VADEMECUM PER L'IMPLEMENTAZIONE DELLE LINEE GUIDA SULLA FORMAZIONE, GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Ottobre 2022

Sommario

PREFAZIONE 3
OBIETTIVI DEL VADEMECUM 4
INDICE DELLE ABBREVIAZIONI 5
LA CATEGORIZZAZIONE DEI RUOLI E CORRISPONDENTI 6
PUBBLICA AMMINISTRAZIONE ITALIANA (PAI) PRESENTE SU IPA 6
PERSONA FISICA (PF) 8
PERSONA GIURIDICA (PG) 9
PUBBLICA AMMINISTRAZIONE ESTERA (PAE) 10
LA CATEGORIZZAZIONE DEI FASCICOLI 11
GESTIONE DELLA METADATAZIONE 13
IL SIGILLO 14
LE NUOVE REGOLE DI INTEROPERABILITÀ TRA PP.AA. 16
LE REGOLE DI PROCESSAMENTO 17
RACCOMANDAZIONI PER UN CORRETTO PROCESSO DI GESTIONE DOCUMENTALE COERENTE CON IL QUADRO NORMATIVO 19
LA "NUOVA" SEGNATURA 20
IL SERVIZIO WEB PER L'INTEROPERABILITÀ TRA LE PP.AA. 22
L'ANNULLAMENTO DI UNA REGISTRAZIONE DI PROTOCOLLO 25
L'INVIO IN CONSERVAZIONE DEI REGISTRI GIORNALIERI DI PROTOCOLLO 26
MAPPATURA DEI METADATI PREVISTA DALL'ALLEGATO 5 ALLE LINEE GUIDA SULLA FORMAZIONE, GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI, CON RIFERIMENTO AL DOCUMENTO AMMINISTRATIVO INFORMATICO APPLICATO AL VERSAMENTO DEI REGISTRI GIORNALIERI DI PROTOCOLLO 28

PREFAZIONE

Le nuove Linee Guida AgID sul documento informatico, entrate in vigore il 1 gennaio 2022, hanno contribuito a rafforzare ed omogenizzare il quadro normativo di riferimento per la produzione, gestione e conservazione dei documenti informatici. La loro corretta applicazione richiede un forte impegno da parte di tutte le pubbliche amministrazioni che sono chiamate a rendere effettivi e consolidati i principi enunciati nel Codice dell'Amministrazione Digitale.

Al fine di approfondire il contesto di applicazione delle norme, l'Agenzia per l'Italia Digitale si è fatta promotrice dell'attivazione di un tavolo di lavoro, in sostanziale continuità con il Gruppo di lavoro sui Poli di Conservazione che nel giugno 2021 aveva prodotto il documento *Definizione di un modello di riferimento per i Poli di conservazione.* Il mandato del nuovo tavolo è stato quello di indagare sui diversi aspetti innovativi delle Linee Guida.

Per rendere più agevole l'approfondimento dei diversi ambiti e per velocizzare la produzione dei documenti conclusivi, il Gruppo si è ulteriormente suddiviso in tre sottogruppi che hanno curato rispettivamente:

Gruppo 1: Metadati, segnatura di protocollo e interoperabilità

Gruppo 2: Conservazione di basi di dati

Gruppo 3: Interoperabilità tra erogatori di servizi di conservazione

Il Gruppo 1 ha, inoltre, approfondito le problematiche legate all'applicazione delle Linee Guida mediante la somministrazione di una indagine conoscitiva rivolta ad un campione di Enti Pubblici.

In attesa dei riscontri acquisiti dal questionario, che si ritiene potranno fornire un quadro di contesto aderente alla situazione reale, si è considerato opportuno elaborare un primo documento di approfondimento, suscettibile certamente di integrazioni e modifiche, che potesse stimolare un confronto sulle diverse esperienze e dare utili spunti di riflessione agli Enti interessati.

Le Linee Guida rappresentano un riferimento normativo nel percorso, complesso e sfidante, per la transizione al digitale, che è a sua volta un aspetto, altrettanto sfidante, per la crescita delle Amministrazioni Pubbliche. La condivisione delle risorse e le sinergie possono rendere meno oneroso il percorso e più realizzabili gli obiettivi del legislatore.

OBIETTIVI DEL VADEMECUM

Il processo di adeguamento alle LLGG richiede una attenta valutazione degli impatti organizzativi e delle soluzioni tecniche da implementare per non ritardarlo.

Lo scopo primario di questa pubblicazione è di fornire suggerimenti a supporto delle Amministrazioni nell'applicazione della normativa di contesto in vigore dal 1° gennaio 2022.

L'esperienza dei primi mesi di applicazione delle LLGG nell'ambito delle pubbliche amministrazioni ha fatto emergere alcuni punti di snodo rilevanti per la loro corretta interpretazione e la susseguente implementazione nei sistemi di protocollo informatico, gestione documentale e conservazione a norma.

Con le note di seguito esposte, si intende, quindi, fornire elementi tecnici di dettaglio operativo, che possano ricondurre, nell'ambito della pubblica amministrazione, ad una applicazione coerente e uniforme delle regole tecniche.

L'attenzione principale sarà rivolta all'allegato 5 (*I metadati*), con particolare riferimento al documento amministrativo informatico e alle aggregazioni documentali informatiche, e all'allegato 6 (*Comunicazione tra AOO di Documenti Amministrativi Protocollati*), con particolare riferimento, in questo caso, alle regole di processamento, al sigillo, al "nuovo" segnatura.xml e alle procedure di interoperabilità.

INDICE DELLE ABBREVIAZIONI

AOO Area Organizzativa Omogenea

AGID Agenzia per l'Italia Digitale

CAD Codice dell'Amministrazione Digitale

DPCM Decreto del Presidente del Consiglio dei ministri

GPS Gestori di Pubblici Servizi

HTTP HyperText Transfer Protocol

IPA Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi

LLGG Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

MTOM Message Transmission Optimization Mechanism

PAI Pubblica Amministrazione Italiana

PAE Pubblica Amministrazione Estera

PdV Pacchetto di Versamento

PF Persona Fisica

PG Persona Giuridica

P.A. Pubblica Amministrazione

PP.AA. Pubbliche Amministrazioni

REM Registered Electronic Mail

REST Representational State Transfer

SLA Service Level Agreement

SOAP Simple Object Access Protocol

UOR Unità Organizzativa Responsabile

URI Uniform Resource Identifier

URL Uniform Resource Locator

W3C World Wide Web Consortium

XML eXtensible Markup Language

XSD XML Schema Definition

LA CATEGORIZZAZIONE DEI RUOLI E CORRISPONDENTI

Nell'ambito dell'allegato sei alle LLGG è prevista, tra le altre, la necessità di configurare opportunamente i corrispondenti (*mittente e destinatario*), al fine di poterli meglio gestire anche nel file segnatura.xml.

Le categorie previste dall'allegato sei alle LLGG sono:

- Pubblica Amministrazione Italiana (PAI);
- Persona Fisica (PF);
- Persona Giuridica (PG);
- Pubblica Amministrazione Estera (PAE).

Le suddette categorie (insieme ad altre) sono presenti anche nell'allegato cinque alle LLGG, con riferimento ai ruoli che entrano a far parte del processo di formazione, gestione e conservazione del documento informatico.

Le informazioni associate ai ruoli (all.5) e ai corrispondenti (all.6) sono fondamentalmente le stesse, con alcune piccole differenze, derivanti dal diverso scopo a cui sono destinati i suddetti allegati:

- l'allegato cinque alle LLGG descrive **i ruoli** rivestiti dai vari soggetti nel processo di formazione, gestione e conservazione del documento informatico;
- l'allegato sei fornisce indicazioni relative ai **soggetti interessati** dalla trasmissione e ricezione dei documenti informatici tra le AOO delle PP. AA..

Di seguito sarà dato maggior risalto a quanto indicato nell'allegato 6 poiché l'allegato 5 è maggiormente legato ai processi interni di ciascuna AOO e, pertanto, talune informazioni, possono essere necessarie in specifici contesti e in altri no, mentre la trasmissione e ricezione rimane un processo standardizzato.

In ogni caso, quanto previsto dagli allegati 5 e 6 alle LLGG ha richiesto l'aggiornamento delle componenti informatiche dei soggetti coinvolti ai fini della corretta implementazione del processo di formazione, gestione e conservazione dei documenti informatici nonché per la trasmissione degli stessi.

Ciascuna delle categorie sopra elencate deve avere una serie di metadati associati, che verranno di seguito descritti.

PUBBLICA AMMINISTRAZIONE ITALIANA (PAI) PRESENTE SU IPA

I dati dei corrispondenti presenti in questa tipologia possono essere scaricati direttamente dall'Indice dei domicili digitali delle Pubbliche Amministrazioni (IPA) mediante il download dei dati disponibili (https://indicepa.gov.it/ipa-dati/) oppure utilizzando i servizi web messi a disposizione (https://www.indicepa.gov.it/ipa-portale/dati-statistiche/web-service).

Da ciò ne deriva una semplificazione procedurale, poiché, le informazioni così raccolte, di norma, non richiedono manutenzione (è pertanto necessario prelevare frequentemente i dati dal sito IPA, in quanto le PP.AA. devono mantenere aggiornate le informazioni di pertinenza).

Le informazioni da gestire sono le seguenti:

- **Denominazione AOO**

  È la denominazione della P.A. presente su IPA.

- **Codice IPA Amministrazione**

  È il codice IPA della P.A. a cui quel corrispondente PAI appartiene.

- **Codice Univoco AOO**

  È il codice univoco dell'AOO e generato da IPA e dal 1° gennaio 2022 deve essere utilizzato nella segnatura di protocollo. È buona pratica, se si è in possesso di tale informazione, inserirla nel file *segnatura.xml*.

- **Indirizzo digitale di riferimento**
  - URL del servizio web previsto dall'allegato sei alle LLGG;
  - casella di posta elettronica certificata;
  - casella di posta elettronica.

- **Eventuale indirizzo postale:**

  da utilizzare nel caso di assoluta impossibilità di trasmissione per via telematica.

Per quanto attiene agli indirizzi digitali, è necessario puntualizzare che la categoria PAI deve essere sempre popolata con l'URL del servizio web (obbligatorio a partire dal 1° gennaio 2022, data di entrata in vigore delle LLGG) e con la casella di posta elettronica certificata.

In presenza dell'URL del servizio web, l'applicativo che gestisce la trasmissione dei documenti deve, automaticamente, inibire l'utilizzo dei canali "tradizionali" eventualmente presenti, indirizzando la comunicazione verso il servizio web esposto (si dà per scontato, in questo caso, che anche la AOO Mittente abbia attivato il servizio web).

L'allegato 6 alle LLGG prevede anche informazioni da utilizzare nel file segnatura.xml, associate alla categoria PAI, dichiarate non obbligatorie.

Gli altri dati dichiarati non obbligatori sono i seguenti:

- **Codice Fiscale dell'Amministrazione.**

- **Contatti dell'Amministrazione:**

  se presente, il campo deve essere valorizzato con almeno uno dei seguenti dati:
  - indirizzo postale;
  - indirizzo telematico;
  - contatto telefonico.

- **Contatti AOO:**

  se presente, da valorizzare come già descritto in Contatti dell'Amministrazione.

- **Codice IPA UOR:**

  il codice IPA associato alla UOR di riferimento della AOO a cui viene trasmesso il documento.

- **Contatti UOR:**

  se presente, da valorizzare come già descritto in Contatti dell'Amministrazione.

- **Persona Fisica:**

  se presente, deve essere descritta come la categoria generale Persona Fisica.

L'introduzione della categoria PAI comporta un problema per la comunicazione verso Pubbliche Amministrazioni che hanno distribuito caselle di posta elettronica ad articolazioni di secondo/terzo o altro livello e che non hanno pubblicato tali indirizzi sull'IPA.

A questo proposito deve essere segnalato che la comunicazione diretta verso articolazioni di AOO non esposte sull'IPA rimane una comunicazione impropria poiché l'interscambio di documenti tra PP.AA. deve avvenire tra AOO oppure tra AOO e UOR e/o UOR e UOR, censite su IPA.

Quanto ora detto viene ulteriormente rafforzato dalla previsione di effettuare la comunicazione tramite servizio web, piuttosto che tramite casella di posta elettronica certificata.

Per quanto sopra è necessario verificare l'attuale stato di pubblicazione delle AOO e delle UOR su IPA, al fine di evitare richieste da parte di UOR di ricevere direttamente comunicazioni a loro afferenti senza essere correttamente censite su IPA.

Le PP.AA. non devono adottare soluzioni, non previste dalla norma, quali, ad esempio, la categorizzazione della UOR di cui trattasi nella categoria non corretta (tipicamente PG o PF).

PERSONA FISICA (PF)

Per la definizione del tipo di soggetto PERSONA FISICA, i dati più rilevanti sono:

- **Nome;**
- **Cognome.**
- **Indirizzo digitale di riferimento:**

  almeno uno dei seguenti dati:

  - casella di posta elettronica certificata;
  - casella di posta elettronica.

- **Eventuale indirizzo postale:**

  va utilizzato nel caso di impossibilità di trasmissione per via telematica.

L'allegato 6 alle LLGG prevede anche la possibilità di indicare le seguenti informazioni:

- **Titolo;**
- **Codice Fiscale.**
- **Contatti:**

  se presente, il campo deve essere valorizzato con almeno uno dei seguenti dati:

- indirizzo postale;
- indirizzo telematico;
- contatto telefonico.

Qualora la categoria PF venga utilizzata per descrivere un ruolo interno alla AOO, l'allegato cinque alle LLGG prevede l'obbligatorietà di indicare la:

- **Denominazione Amministrazione/Codice IPA;**
- **Denominazione Amministrazione AOO/Codice IPA AOO.**

PERSONA GIURIDICA (PG)

Per la definizione del tipo di soggetto PERSONA GIURIDICA, i dati più rilevanti sono:

- **Denominazione**
- **Indirizzo digitale di riferimento:**

  almeno uno dei seguenti dati:
  - casella di posta elettronica certificata;
  - casella di posta elettronica.
- **indirizzo postale:**

  va utilizzato nel caso di assoluta impossibilità di trasmissione per via telematica.

Anche per le persone giuridiche sono previsti alcuni dati opzionali:

- **Partita IVA/Codice Fiscale;**
- **Contatti Persona Giuridica:**

  se presente, da valorizzare con almeno uno dei seguenti dati:
  - indirizzo postale;
  - indirizzo telematico;
  - contatto telefonico.
- **Persona Fisica:**

  se presente, deve essere descritta come la categoria generale Persona Fisica.

Per la descrizione di una PERSONA GIURIDICA l'allegato cinque alle LLGG prevede un solo dato obbligatorio (la denominazione).

Tuttavia, ai fini di una corretta gestione di trasmissione, è necessario disporre anche dei riferimenti digitali e/o postali.

PUBBLICA AMMINISTRAZIONE ESTERA (PAE)

Per una Pubblica Amministrazione Estera i dati obbligatori sono due:

- **Denominazione;**
- **Indirizzo digitale di riferimento.**

Tale indirizzo potrebbe essere una casella di posta elettronica ovvero una casella di posta elettronica certificata, se l'Amministrazione Estera se ne è dotata avendola acquisita in Italia, ovvero un servizio REM, quando sarà disponibile.

Sia l'allegato 5 che l'allegato 6 alle LLGG prevedono l'uso anche del seguente dato non obbligatorio:

- **Denominazione Ufficio:**

mentre l'allegato sei alle LLGG prevede, in aggiunta, l'uso del dato non obbligatorio:

- **Contatti dell'Amministrazione Estera**

e, qualora sia presente va valorizzato con uno dei seguenti dati:

  - indirizzo postale;
  - indirizzo telematico;
  - contatto telefonico.

LA CATEGORIZZAZIONE DEI FASCICOLI

Le LLGG prevedono l'obbligo di indicare, per ciascun fascicolo la relativa tipologia.

Sono indicate cinque diverse tipologie:

- **affare**

  comprende i documenti relativi a una competenza non proceduralizzata, ma che, nella consuetudine amministrativa, la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.

- **attività**

  comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice, che implica risposte obbligate o meri adempimenti, per la quale, quindi, non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.

- **persona fisica**

  comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.

- **persona giuridica**

  comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte

- **procedimento amministrativo**

  comprende una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo

Da questa elencazione è possibile vedere che non si tratta di meri formalismi, ma, invece, di una ben precisa organizzazione archivistica che deve essere effettuata nell'ambito dell'archivio dell'Ente, gestito attraverso il sistema.

Punto di partenza essenziale per perseguire gli obiettivi sinteticamente descritti, è il piano di classificazione (T*itolario*) e relativo piano di organizzazione delle aggregazioni documentali che diventa l'elemento trainante della successiva attività gestionale e archivistica.

Tra le diverse tipologie di fascicolo quella che può determinare una maggiore difficoltà realizzativa è la tipologia del fascicolo "procedimento amministrativo" che ha associati ad essa una serie di dati la cui reperibilità all'utente del sistema potrebbe aumentarne la complessità procedurale:

- la materia, l'argomento o la struttura per la quale sono stati catalogati i procedimenti amministrativi;
- la denominazione del procedimento;
- l'URI di pubblicazione del catalogo dei procedimenti amministrativi;
- le fasi del procedimento, a sua volta suddivise in fase preparatoria, consultiva, decisoria o deliberativa, integrazione dell'efficacia, e, per ogni fase, la data di inizio e di fine.

Va tenuto in considerazione che la corretta individuazione della tipologia di appartenenza di un fascicolo è una attività delicata e, a volte, complessa. Pertanto, soprattutto per quelle categorie di più difficile differenziazione (come, ad esempio, affare, attività e procedimento amministrativo) possono anche essere impartite disposizioni per una semplificazione concettuale ed operativa, evitando di utilizzare una o più delle categorie proposte.

È opportuno, nel caso, che le indicazioni fornite agli utenti del sistema documentale, vengano riportate anche nel Manuale di gestione.

In realtà, come apparirà sempre più evidente, tutto l'impianto delle nuove LLGG è improntato a sottolineare l'importanza della gestione archivistica dei documenti, con un occhio particolarmente attento ai successivi processi di conservazione a norma della documentazione, come previsto dal Codice dei Beni Culturali. In quest'ottica sono opportune, da un lato, progressive azioni di sensibilizzazione degli utenti e, dall'altro lato, una (ri)organizzazione dei processi archivistici della propria AOO, anche puntando ad una maggiore centralizzazione presso i servizi di gestione documentale, intesi in senso stretto, di alcune funzioni di difficile attribuzione al singolo utente, spesso sprovvisto della necessaria visione, idonea alla corretta gestione archivistica del documento in trattazione.

In pratica gli Uffici dei servizi di gestione documentale dovrebbero divenire sempre più il fulcro centrale della gestione dell'archivio dell'Ente di riferimento, con strumenti più incisivi rispetto al recente passato e, infine, con una visione coerente e unitaria discendente dalle disposizioni che saranno impartite attraverso i cinque documenti fondamentali per la gestione documentale:

- Manuale di Gestione;
- Manuale della Conservazione;
- Piano di Conservazione;
- Titolario;
- Piano di Organizzazione delle aggregazioni documentali informatiche.

GESTIONE DELLA METADATAZIONE

L’allegato 5 alle LLGG prevede la produzione dei metadati secondo un formato ben definito.

Per i documenti amministrativi informatici si renderà necessario effettuare la metadatazione di ogni file (documento primario ed eventuali allegati). I metadati afferenti i singoli file sono sostanzialmente statici, con l’eccezione della eventuale necessità di gestire il versionamento, previsto dall’allegato 5.

I metadati possono essere gestiti memorizzandoli all'interno di file .XML ovvero possono essere elaborati nel momento in cui viene fatta la richiesta di accesso a questa informazione.

La gestione delle diverse versioni potrebbe essere risolta anche attraverso una opportuna identificazione dei diversi file, aggiungendo, ad esempio, un suffisso o un prefisso, relativo alla versione come pure si potrebbe adottare una regola di denominazione dei file che associ ciascun documento al relativo file di metadati attraverso lo stesso nome di identificazione.

Per quanto attiene ai metadati delle aggregazioni documentali, sussiste una oggettiva dinamicità delle informazioni da gestire. Pertanto, è consigliabile una gestione dei metadati generandoli a richiesta, nel momento in cui l’operatore ne ha necessità.

IL SIGILLO

Una delle principali varianti apportate al file segnatura.xml è la necessità di apporre il sigillo su di esso.

Con tale procedura si risolve uno dei problemi presenti nelle precedenti regole tecniche, ovvero la garanzia dell'integrità del file segnatura.xml, oltre alla certezza del mittente.

La reperibilità dei sigilli è piuttosto semplice, poiché in genere sono servizi disponibili presso ciascun erogatore di firme digitali.

Tuttavia, è necessario prendere in considerazione alcuni aspetti organizzativi:

La richiesta del sigillo deve essere effettuata da una persona fisica, in nome e per conto dell'organizzazione richiedente, con le relative deleghe, individuata con atto interno.

È opportuno valutare quale sia il numero dei sigilli da richiedere.

Infatti, nelle PP.AA. costituite da una sola AOO serve ovviamente un unico sigillo, ma, nelle PP.AA. dove, invece, le AOO sono molteplici, potrebbe essere opportuno che ciascuna AOO sia dotata del proprio sigillo. Ciò, darà la certezza della AOO Mittente nei messaggi inviati.

D'altro canto, bisogna tenere in mente che la gestione centralizzata di un sigillo per ciascuna AOO richiede un'organizzazione procedurale più articolata e potrebbe avere anche un impatto, sia pure di modesta entità, sui costi.

Le LLGG, su questo aspetto, lasciano la scelta all'autonomia delle singole Amministrazioni. Per questo diventa necessario bilanciare gli aspetti organizzativi e quelli funzionali. Ad esempio, nel caso di richiesta di un singolo sigillo per la singola P.A.er la singola P.A. da associare a tutte le AOO di quella P.A., la scelta comporta una gestione centralizzata delle credenziali necessarie all'uso del sigillo.

Nel caso di richiesta di un sigillo per ciascuna AOO, la scelta comporta l'individuazione delle persone richiedenti e la successiva gestione amministrativa di tali richieste.

In ogni caso il modello organizzativo individuato deve essere descritto all'interno del Manuale di gestione.

Una volta che il sigillo è stato acquisito, le relative credenziali devono essere inserite all'interno del sistema utilizzante, in modo sicuro, da parte del titolare.

Dopo aver attivato la funzione, le credenziali devono comunque essere protette da accessi non autorizzati.

Il sigillo deve essere utilizzato nell'ambito del segnatura.xml a partire dal 1° gennaio 2022, anche nel caso in cui il canale di comunicazione tra AOO sia la posta elettronica.

L'Appendice C dell'Allegato 6 alle LLGG prevede una specifica deroga temporanea con la quale, nelle more dell'applicazione della comunicazione tra AOO tramite cooperazione applicativa, l'utilizzo della posta elettronica risulta immutata rispetto a quanto indicato nella Circolare AGID 60/2013.

Tuttavia, *per permettere l'univocità della segnatura di protocollo indicata nell'Appendice A di seguito è riportato l'XML Schema da utilizzarsi per la generazione dei file da prevedersi come body part dei messaggi scambiati tramite posta elettronica:*

• *Segnatura.xml avente un root element di tipo "SegnaturaInformatica";*

Da quanto sopra segnalato, il processo di comunicazione tra AOO via posta elettronica sarà ancora governato dalle regole della Circolare AGID 60/2013 mentre l'interoperabilità tramite metadatazione con quanto previsto dall'Allegato 6 alle LLGG (il file segnatura.xml deve avere un root element di tipo "SegnaturaInformatica").

Andando ancora più nel dettaglio, con riferimento ai paragrafi dall'allegato 6 alle LLGG, quelli più direttamente connessi con le modalità di gestione della comunicazione vanno applicati in modo indipendente dal canale di comunicazione utilizzato (paragrafo 2), mentre quelli più direttamente connessi con l'impiego della cooperazione applicativa (paragrafo 3), troveranno attuazione nel momento in cui tale strumento sarà utilizzato.

La conclusione è quella già indicata: il sigillo deve essere apposto nel file segnatura.xml indipendentemente dal canale di comunicazione utilizzato.

Sussiste un'unica differenza: la verifica del sigillo da parte della AOO destinataria, nel caso di comunicazione tramite cooperazione applicativa, deve essere obbligatoriamente effettuata mentre tale obbligo non sussiste quando si utilizza la posta elettronica.

Tuttavia, la verifica del sigillo è raccomandata anche in quest'ultimo caso, utilizzando il file Eccezione.xml avente un root element di tipo "NotificaEccezione", segnalato nell'Appendice C dell'Allegato sei alle LLG, per segnalare eventuali problemi riscontrati.

LE NUOVE REGOLE DI INTEROPERABILITÀ TRA PP.AA.

Una delle implementazioni di maggior impatto e più innovative introdotte con le LLGG, riguarda l'interoperabilità tra le Aree Organizzative Omogenee (AOO).

Nel dettaglio, si tratta della terza rivisitazione dell'argomento.[1]

D'altra parte, le modalità di comunicazioni tra le AOO sono un aspetto molto rilevante, anche dal punto di vista dell'efficienza, nell'economia generale di gestione del sistema di protocollo informatico e gestione documentale.

In estrema sintesi, di seguito i passaggi più importanti:

- la comunicazione tra AOO deve avvenire, prioritariamente, attraverso servizi web;
- il file di accompagnamento di un documento protocollato (segnatura.xml) è stato aggiornato;
- per dare certezza della AOO/Amministrazione mittente, ciascun file segnatura.xml dovrà essere firmato con un sigillo elettronico;
- prima di far partire un documento è necessario che la AOO Mittente effettui una serie di controlli e segua un ben definito processo elaborativo;
- La AOO Destinataria può effettuare ulteriori controlli, e se necessario, generare una serie di ricevute di mancata protocollazione che vanno inviate alla AOO Mittente
- è necessario garantire elevati livelli di servizio (SLA) per la funzionalità del servizio web esposto per l'interoperabilità e, in caso di malfunzionamento, garantire una soluzione alternativa di colloquio;
- per le amministrazioni che al 1° gennaio 2022, erano inadempienti, era stato autorizzato temporaneamente il protocollo di comunicazione alternativo via PEC.

Di seguito saranno approfonditi alcuni dei punti sopra delineati.

[1] Inizialmente, la materia era regolamentata dalla Circolare AIPA/CR/28 del 7 maggio 2001. In seguito, è stata pubblicata la Circolare AGID n. 60 del 23 gennaio 2013. Infine, abbiamo le LLGG aggiornate al maggio 2021.

LE REGOLE DI PROCESSAMENTO

Nelle precedenti regole tecniche le modalità di produzione di un documento informatico in uscita non erano puntualmente indicate, lasciando ampia discrezionalità in questo campo.

L'allegato 6 alle LLGG introduce delle precise regole di processamento, per la formazione, la protocollazione e la preparazione di un documento informatico per garantire l'interoperabilità tra AOO.

Per poter produrre un documento sono previsti cinque passaggi:

1. **Formazione del *documento principale* ed eventuali *allegati***

   Effettuata secondo le regole previste dalle LLGG. Dal punto di vista pratico non differisce molto da quanto si faceva in precedenza (al netto della necessità di creare i file di metadati e della necessità di utilizzare i formati previsti nelle LLGG stesse). Sembra utile ribadire che la formazione del documento principale e degli eventuali allegati si conclude con la firma elettronica degli stessi.

2. **Calcolo dell'impronta del *documento principale* e degli eventuali *allegati***

   Il calcolo dell'impronta (digest) di un file era già previsto anche nelle precedenti regole tecniche, seppure la gestione di tale dato attualmente, viene resa più stringente e più ampia.

3. **Generazione del numero di protocollo da assegnare al *messaggio di protocollo.***

   È il momento cardine del processo di protocollazione di un documento.

4. **Formazione della *segnatura di protocollo* che DEVE rispettare l'XML Schema indicato nelle LLGG utilizzando le impronte del documento principale e degli eventuali allegati, create al passo 2.**

   La novità di maggior impatto è rappresentata dalla nuova metadatazione del file segnatura.xml prevista dalle LLGG rispetto alla preesistente Circolare AGID n.60.

5. **Apposizione di un "sigillo elettronico qualificato" alla *segnatura di protocollo* per garantire l'integrità e autenticità**

   Si tratta di un'altra delle maggiori novità.

Deve essere tenuto in considerazione il vincolo aggiuntivo imposto dalle regole tecniche: gli ultimi tre passaggi devono essere **atomici**. Pertanto, le tre operazioni sono eseguite in maniera indivisibile. Da un punto di vista logico: o sono portate a termine tutte o non ne risulta eseguita nessuna.

In sintesi, se uno qualunque dei tre passaggi finali non ha esito positivo, la trasmissione deve essere interrotta e ripetuta.

Inoltre, la necessità di dover effettuare i passaggi 3, 4 e 5 delle regole di processamento in modalità atomica può introdurre un fattore di criticità prestazionale nei sistemi che gestiscono una consistente numerosità di protocolli, in modo particolare per l'eventuale tempistica di apposizione del sigillo.

Pertanto, è opportuno valutare, in sede di sottoscrizione dei contratti di fornitura del sigillo, la richiesta di SLA adeguati e/o adottare soluzioni tecnico-organizzative correlate alle modalità di trasmissione.

Le nuove regole di processamento rendono più rigorosa la procedura di protocollazione dei documenti informatici, ai quali deve essere associata la segnatura di protocollo (l'apposizione riguarda solo documenti analogici). In un ambito digitale i sistemi di protocollo informatico e gestione documentale devono consentire la visualizzazione della segnatura di protocollo in modo semplice.

Tuttavia, questa soluzione non risolve l'intera tematica, in quanto il documento informatico può essere utilizzato al di fuori del sistema documentale di pertinenza e, in questo caso, l'assenza della stringa di protocollo impressa su di esso può rappresentare un fattore di criticità.

Fermo restando il rispetto delle regole tecniche, che consentono di evitare qualunque tipo di problema connesso con la corretta procedura di protocollazione di un documento, nulla vieta di associare al documento originale una cosiddetta *copia di cortesia* dello stesso documento che porterà stampigliata la segnatura di protocollo e l'indicazione che si tratta di un documento non opponibile a terzi.

Nel caso di comunicazioni rivolte a privati ed aziende il canale preferenziale di comunicazione è la posta elettronica (certificata o non) e, pertanto, la trasmissione della *copia di cortesia* è sempre possibile poiché il destinatario potrebbe non essere provvisto di strumenti idonei alla gestione della segnatura di protocollo.

Per contro, proprio per agevolare i corrispondenti che disponessero di strumenti adeguati, è consigliabile associare alla comunicazione il file segnatura.xml, completo di sigillo, anche se la comunicazione non è rivolta a PP. AA..

Nel caso di comunicazione tra AOO tramite servizio web, l'invio della copia di cortesia è inutile e non è compatibile con le regole tecniche.

Le regole di processamento sopra descritte riguardano la protocollazione di un documento ma devono intendersi valide anche nel caso di numerazione dei documenti attraverso registri particolari, albi, elenchi ecc...

L'allegato 6 alle LLGG prevede la possibilità per la AOO destinataria di effettuare quattro tipi di verifiche su quanto ricevuto e nel caso di anomalie DEVE segnalare alla AOO mittente l'anomalia riscontrata, secondo il formato previsto.

I quattro possibili controlli riguardano tutti i file pervenuti (documento principale e allegati) e l'obbligo di invio di segnalazione scatta se almeno uno dei file ricevuti risulta:

- non leggibile;
- con firma e la validazione della stessa fallisce;
- con marca temporale e la validazione della stessa fallisce;
- con sigillo elettronico e la validazione dello stesso fallisce;

L'effettuazione dei controlli sopra elencati è fortemente raccomandata quale garanzia di una corretta interoperabilità tra AOO.

RACCOMANDAZIONI PER UN CORRETTO PROCESSO DI GESTIONE DOCUMENTALE COERENTE CON IL QUADRO NORMATIVO

A volte, si verificano casi in cui l'uso del sistema di gestione documentale non è aderente al quadro normativo vigente.

Uno di questi casi è la produzione di un documento che abbia tra i suoi destinatari una o più PP.AA. e, in aggiunta, anche privati cittadini e/o aziende.

Appare evidente che in una situazione del genere avremo una trasmissione su più canali:

- verso le PP.AA. tramite servizio web, secondo le indicazioni dell'allegato sei LLGG;
- verso le aziende con la casella di posta elettronica certificata, secondo il DPCM 22 luglio 2011 "Comunicazioni con strumenti informatici tra imprese e amministrazioni pubbliche, ai sensi dell'articolo 5-bis del Codice dell'amministrazione digitale";
- verso il privato tramite casella di posta.

Malgrado la trasmissione avvenga su più canali, il file segnatura.xml dovrà essere sempre e soltanto uno, comprendendo al suo interno tutti i destinatari del documento. Produrre diversi file segnatura.xml a fronte di un'unica registrazione di protocollo non è coerente con il quadro normativo nel suo complesso.

Non è coerente neppure una trasmissione differenziata della numerosità degli allegati associati ad una medesima registrazione di protocollo a diversi destinatari.

Ciascuna trasmissione deve garantire la coerenza tra quanto contenuto nella registrazione di protocollo e quanto trasmesso ai destinatari.

LA "NUOVA" SEGNATURA

A far data dal 1° gennaio 2022 è obbligatorio l'uso del *xml schema* così come definito nell'appendice C dell'allegato 6 alle LLGG, con particolare riferimento all'uso del sigillo.

Per quanto sopra le PP.AA. che utilizzano formati antecedenti sono inadempienti e, come tali, soggetti a sanzioni ai sensi dell'art.18bis del CAD.

In particolare, si rammenta che Segnatura.xml deve avere un *root element* di tipo "SegnaturaInformatica".

Quando si effettua la trasmissione tramite servizio web, si suggerisce di utilizzare il seguente esempio:

```
<Segnatura prot:lang="it" prot:versione="3.0.0"
       xmlns:prot="http://www.agid.gov.it/protocollo/"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:type="prot:SegnaturaInformaticaType" >

     <prot:Intestazione>
                  .....
       </prot:Intestazione>
                   .....
     <ds:Signature Id="ID" xmlns="http://www.w3.org/2000/09/xmldsig#">
                   .....
     </ds:Signature>
</Segnatura>
```

e, di conseguenza, nel pacchetto SOAP,

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
        .....
  </soap:Header>
  <soap:Body                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
   <MessaggioInoltro xmlns="http://tempuri.org/">
     <Segnatura prot:versione="3.0.0" prot:lang="it"
           xmlns:prot="http://www.agid.gov.it/protocollo/"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:type="prot:SegnaturaInformaticaType" >
```

```
        <prot:Intestazione>
                    .....
        </prot:Intestazione>
                    .....
         <ds:Signature Id="ID" xmlns="http://www.w3.org/2000/09/xmldsig#">
                    .....
         </ds:Signature>
     </Segnatura>
     ...
   </MessaggioInoltro>
  </soap:Body>
</soap:Envelope>
```

In questa soluzione, per evitare duplicazioni di formati, dovrebbe essere utilizzato il formato sopra indicato, anche nel caso di trasmissione via PEC.

I sistemi riceventi devono pertanto essere predisposti a gestire il formato sopra indicato.

A far data dal 1° gennaio 2022 il codice identificativo delle AOO da utilizzare nei rapporti di interoperabilità e nella segnatura di protocollo è il cosiddetto Codice Univoco AOO, assegnato da IPA automaticamente.

Tale codice è una stringa di sette caratteri alfanumerici che si contraddistingue per avere come primo carattere una A.

I preesistenti codici AOO vengono ridenominati codici AOO interni (alle singole PP.AA.).

Qualora, nell'ambito delle singole Amministrazioni, il codice interno delle AOO risultasse ancora rilevante, i sistemi applicativi proporranno la corretta decodifica tra Codice Univoco e Codice Interno.

Una delle possibili tematiche che emerge nell'ambito dell'interoperabilità tra AOO è la rappresentazione dell'impronta dei documenti associati al file segnatura.xml.

L'allegato 6 indica che la codifica deve essere effettuata in *base64.*

Utilizzando uno degli algoritmi più diffusi, lo SHA256, si ottiene un *output* di 256 bit, che codificato in *base64* produce una stringa (rappresentazione dell'impronta) di 44 caratteri (6 bit per carattere + caratteri di riempimento).

IL SERVIZIO WEB PER L'INTEROPERABILITÀ TRA LE PP.AA.

La tecnologia per il servizio web di interoperabilità è SOAP in quanto, in una indagine effettuata da AGID, antecedente alla redazione delle LLGG, è stata riscontrata un'ampia diffusione di tale protocollo di comunicazione.

Con l'aumento delle PP.AA. che usano la tecnologia c.d. REST si potrà procedere con l'estensione dei servizi web in tale tecnologia.

Le PP.AA., per rendere disponibili i propri servizi, devono inserire *l'end point* (l'indirizzo, URI, dove sono esposti i due servizi indicati nell'allegato 6: ovvero l'end-point dal quale richiamare le funzioni lato mittente e le funzioni lato destinatario) all'interno dell'Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi.

Nel paragrafo 3.1.1 *Inoltro di un messaggio protocollato* dell'allegato 6 alla lettera C, è previsto che l'AOO Destinataria DEVE verificare la ricevibilità del messaggio di protocollo ricevuto, ed in caso negativo DEVE restituire l'anomalia 000_Irricevibile e l'indicazione della motivazione di irricevibilità. I possibili casi di irricevibilità devono essere indicati nel Manuale di gestione.

A titolo di esempio si segnala l'opportunità di indicare i formati gestiti (tra quelli previsti dall'allegato due alle LLGG) e l'indicazione della massima dimensione dei documenti accettati.

Il tema del dimensionamento dei file allegati al messaggio che è possibile trasmettere e/o ricevere rimane rilevante, avendo impatti sull'interoperabilità tra AOO.

Sia la precedente Circolare AGID n.60 che l'allegato 6 alle LLGG prevedono la possibilità di superare eventuali problemi legati alla dimensione degli allegati utilizzando riferimenti esterni, indicati nel file segnatura.xml, attraverso i quali recuperare i documenti informatici.

Nell'allegato 6 alle LLGG, il dato di riferimento è denominato Collocazione Telematica, che esplicita un riferimento telematico per recuperare la risorsa. Tale recupero avviene tramite la richiesta HTTP GET con autenticazione conforme all'RFC 7617, su canale di trasporto TLS.

Le informazioni che è possibile indicare sono:

- il server che espone la risorsa;
- il riferimento alla risorsa da recuperare;
- il numero di millisecondi di disponibilità della risorsa;
- la user-id comunicata dalla AOO Mittente;
- la password comunicata dall'AOO Mittente.

Malgrado l'efficacia di tale meccanismo deve essere considerata la raggiungibilità della risorsa che potrebbe non essere disponibile per il destinatario, ad esempio, per tematiche di sicurezza legate agli instradamenti della connettività delle diverse Amministrazioni.

L'uso di tale possibilità deve essere calibrato alle effettive necessità e nei casi di impiego rilevante potrebbe essere utile un raccordo preventivo tra la AOO Mittente e quella Destinataria.

Va anche considerato che, già di per sé, l'impiego del servizio web, previsto come canale principale di interoperabilità, supera i precedenti limiti imposti dall'impiego della posta elettronica su tale tematica.

In ogni caso, il dimensionamento della documentazione deve sempre essere valutato con attenzione. Allegati voluminosi richiedono maggiori risorse sia in termini di memorizzazione sia in termini di tempo di *upload/download* e di occupazione di banda e questi aspetti sono da considerare per ogni accesso che si effettua sui file interessati.

Eventuali limiti introdotti applicativamente devono essere segnalati nel Manuale di gestione e il destinatario deve indicare la massima dimensione degli allegati accettata; nell'eventualità di restituzione al mittente del messaggio ricevuto, dovrà utilizzare quanto previsto per l'anomalia *000_Irricevibile*.

Sempre nel Manuale di gestione devono essere descritti i servizi web che sono esposti.

Si riporta quanto previsto nell'allegato 6 per l'inoltro di binary data nei messaggi SOAP: "…*deve essere utilizzato il W3C Message Transmission Optimization Mechanism (MTOM, le cui specifiche sono disponibili al link https://www.w3.org/TR/soap12-mtom/).*

Le AOO Mittente e AOO destinatarie assicurano il non ripudio della comunicazione, provvedendo alla firma dei messaggi scambiati ed loro trasporto su canale TLS tramite SOAP coerentemente alla specifica WS-Security, così come previsto dal profilo "Soluzioni per la non ripudiabilità della trasmissione" indicato nel documento operativo "Profili di interoperabilità" delle "Linea di indirizzo sull'interoperabilità tecnica delle Pubbliche Amministrazioni" emanate da AgID con Circolare 1/2020 (vedasi al riguardo https://trasparenza.agid.gov.it/archivio28_provvedimenti-amministrativi_0_122346_725_1.html)."

Quando una AOO è pronta a comunicare con altre AOO tramite servizio web, deve inserire l'end point, come già più sopra descritto, nello specifico campo previsto in IPA.

Tramite questa informazione AGID effettuerà anche il monitoraggio dell'adeguamento delle PP.AA. alle indicazioni dell'allegato sei delle LLGG.

L'obiettivo deve essere quello che nel breve/medio periodo la comunicazione tra AOO avvenga esclusivamente tramite servizio web.

È necessario inserire correttamente tale informazione: un *end point* errato comporterà, evidentemente, l'impossibilità di ricevere comunicazione da parte di altre AOO.

In ogni caso, come regola minimale, vanno scartati per la comunicazione tra AOO eventuali *end point* privi del prefisso *https:*

Un altro punto di rilievo è la modalità di trasmissione del documento protocollato in quanto la segnatura, in particolare, caratterizza il documento protocollato.

La segnatura è inserita nel *body* SOAP per facilitare il formato dell'oggetto.

Il paragrafo 3.3 dell'allegato 6 delle LLGG affronta un argomento di rilievo quale le procedure da seguire nel caso di disservizi nel flusso di comunicazione, presumibilmente imputabili alla AOO Destinataria. Il paragrafo di cui trattasi prevede quattro passaggi successivi:

A. L'AOO Mittente recupera dall'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) i riferimenti della AOO Destinataria.
B. L'AOO Mittente procede a segnalare l'anomalia riscontrata contattando l'AOO Destinataria ad uno dei riferimenti individuati al punto A.
C. Qualora l'anomalia segnalata determini un disservizio bloccante, l'AOO Destinataria DEVE individuare e fornire all'AOO Mittente modalità alternative per garantire l'operatività del

servizio nelle more della risoluzione del disservizio, ed il periodo stimato di ripristino del servizio.

D. L'AOO Mittente in caso di disservizio bloccante DEVE adoperare la modalità alternativa fornita dalla AOO Destinataria per ottemperare alle proprie esigenze di comunicazione, fino alla scadenza del periodo di ripristino del servizio comunicato l'AOO Destinataria.

Al fine di rendere la procedura sopra descritta efficace, si segnala l'opportunità, da parte degli Enti che attivano la comunicazione via servizio web, di pubblicare all'interno del proprio Manuale di Gestione:

- la modalità alternativa di comunicazione che le AOO mittenti dovranno utilizzare in caso di malfunzionamento del servizio web: in tal modo il ripristino della comunicazione sarà più tempestivo e facilitato;
- il numero di tentativi che verranno effettuati dopo la prima mancata risposta da parte del servizio web del destinatario, prima di attivare la procedura di gestione dei disservizi. Le LLGG prevedono, in tale casistica, una politica di trasmissione con N tentativi e backoff incrementale del tipo 2(elevato)N ore. Il valore N deve essere 1 <= N <= 3.

L’ANNULLAMENTO DI UNA REGISTRAZIONE DI PROTOCOLLO

Nell’ambito dell’allegato 6 paragrafo 3.1.2, si fa riferimento alla richiesta di annullamento protocollazione destinatario ma si tratta di una difformità di tipo lessicale: infatti non si tratta di una *richiesta* ma di una **notifica** di annullamento. Malgrado tale difformità il meccanismo previsto mantiene la sua operatività.

Sempre nel paragrafo 3.1.2 viene previsto, tra le altre:

l’AOO Mittente deve inoltrare la notifica di annullamento riportando il riferimento al provvedimento che determina il presupposto amministrativo per l’annullamento

mentre, nel paragrafo 3.1.3, viene previsto, tra le altre:

l’AOO Destinataria deve inoltrare la notifica di annullamento riportando il riferimento al provvedimento che determina il presupposto amministrativo per l’annullamento

Si suggerisce di attivare un registro particolare, nell’ambito del sistema di gestione documentale dove raccogliere i provvedimenti di cui ai due paragrafi sopra riportati. In tal modo si avrà una raccolta ordinata di tali provvedimenti e un sicuro riferimento ai medesimi. In alternativa è possibile registrare i provvedimenti di annullamento nel registro generale.

L'INVIO IN CONSERVAZIONE DEI REGISTRI GIORNALIERI DI PROTOCOLLO

L'entrata in vigore delle LLGG modifica alcuni dettagli di gestione operativa dei registri giornalieri di protocollo.

Il registro giornaliero di protocollo, mantenendo le sue peculiari caratteristiche di documento che gode di fede privilegiata (se gestito secondo quanto previsto dalle norme) ricade nella tipologia di documento amministrativo informatico e come tale, deve essere accompagnato da classificazione, fascicolazione e metadatazione ai sensi dell'allegato cinque delle LLGG.

AGID, con un documento dell'1 ottobre 2015, aveva indicato 18 metadati che dovevano accompagnare la conservazione dei registri giornalieri di protocollo:

1. **Identificativo univoco e persistente;**
2. **Data di chiusura** *(data di creazione del registro)***;**
3. **Soggetto produttore** *(Operatore che ha prodotto il Registro - Nome, Cognome, Codice fiscale; qualora il registro è generato automaticamente dal sistema informatico, il nome dell'operatore può essere sostituito dall'indicazione della denominazione di tale sistema);*
4. **Soggetto produttore 2** *(Operatore che ha prodotto il Registro - Nome, Cognome, Codice fiscale);*
5. **Destinatario** *(Nome, Cognome, Codice fiscale se disponibile)***;**
6. **Impronta del documento informatico;**
7. **Codice identificativo dell'amministrazione** *(codice IPA);*
8. **Denominazione dell'amministrazione;**
9. **Codice identificativo dell'area organizzativa omogenea;**
10. **Responsabile** *(Responsabile della gestione documentale o Responsabile del servizio per la tenuta del protocollo informatico - Nome, Cognome, Codice fiscale*);
11. **Oggetto** *(descrizione della tipologia di registro; ad es. "Registro giornaliero di protocollo", "Registro giornaliero delle modifiche di protocollo", ecc.);*
12. **Codice identificativo del registro;**
13. **Numero progressivo del registro;**
14. Anno;
15. Numero della prima registrazione effettuata sul registro;
16. Numero dell'ultima registrazione effettuata sul registro;
17. Data della prima registrazione effettuata sul registro;
18. Data dell'ultima registrazione effettuata sul registro**.**

I metadati **in grassetto** trovano corrispondenza con analoghi metadati previsti nell'allegato cinque alle LLGG.

Per gli altri metadati, qualora si decidesse di continuarne la gestione, nell'ambito di quanto previsto dal già citato all.5 LLGG., devono essere riportati nel Manuale di gestione.

Come qualunque altro documento amministrativo informatico, l'immodificabilità e l'integrità del registro giornaliero di protocollo vengono garantite secondo le indicazioni fornite nel paragrafo 2.1 delle LLGG.

Normalmente l'integrità e l'immodificabilità si ottengono seguendo le indicazioni del paragrafo 3.1.6, Requisiti minimi di sicurezza dei sistemi di protocollo informatico, attraverso la trasmissione, entro la giornata lavorativa successiva, al sistema di conservazione.

Qualora, per un qualunque motivo, non riesca l'invio in conservazione entro la giornata lavorativa successiva, in attesa del ripristino della trasmissione in conservazione, è consigliabile firmare digitalmente o apporre il sigillo al registro.

Al fine di fornire un esempio concreto di attuazione di quanto sopra indicato, si fornisce l'elenco dei metadati che dovrebbero far parte di un Pacchetto di versamento di un registro giornaliero di protocollo a seguito dell'entrata in vigore delle LLGG.

Per ciascun dato viene fornito il corrispondente XSD riferito all'allegato cinque alle LLGG, relativo al Documento Amministrativo Informatico.

Per i metadati non previsti nel predetto allegato si fornisce un possibile esempio applicativo.

MAPPATURA DEI METADATI PREVISTA DALL'ALLEGATO 5 ALLE LINEE GUIDA SULLA FORMAZIONE, GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI, CON RIFERIMENTO AL DOCUMENTO AMMINISTRATIVO INFORMATICO APPLICATO AL VERSAMENTO DEI REGISTRI GIORNALIERI DI PROTOCOLLO

Definizione del metadato IdDoc

(element xsd: IdDoc)

Impronta crittografica del documento (Impronta e Algoritmo)

Identificativo

Definizione del metadato Modalità di formazione

(element xsd: ModalitaDiFormazione)

In riferimento alle modalità di formazione previste al paragrafo 2.1.1 delle LLGG:

a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato due alle LLGG;

b) non applicabile;

c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Definizione del metadato Tipologia documentale

(element xsd: TipologiaDocumentale)

Esempio: registro giornaliero di protocollo generale

Definizione del metadato Dati di registrazione

(element xsd: DatiDiRegistrazione)

Tipologia di flusso I

Tipo di registro Protocollo Ordinario/Protocollo Emergenza Repertorio/Registro

Data registrazione (si intende quella di produzione del registro)

Numero Documento (inserire l'identificativo)

Codice registro

Definizione del metadato Soggetti

(element xsd: Soggetti)

Ruolo (Responsabile della gestione Documentale o Responsabile del servizio di protocollo)

Persona Fisica

Definizione del metadato Chiave descrittiva

(element xsd: ChiaveDescrittiva)

Oggetto (esempio: Registro Giornaliero di protocollo generale)

Definizione del metadato Allegati

(element xsd: Allegati)

Numero allegati: 0

Definizione del metadato Classificazione

(element xsd: Classificazione)

Indice di classificazione

Descrizione

Definizione del metadato Riservato

(element xsd: Riservato)

Falso

Definizione del metadato Identificativo del formato

(element xsd: IdentificativoDelFormato)

Formato come da allegato 2 delle Linee Guida

Prodotto Software, quando rilevabile (nel caso Nome Prodotto, versione prodotto, produttore)

Definizione del metadato Verifica

(element xsd: Verifica)

Firmato Digitalmente vero/falso

Sigillato Elettronicamente vero/falso

Marcatura temporale vero/falso

Definizione del metadato Identificativo dell'Aggregazione documentale

(element xsd: Agg)

Identificativo del fascicolo

Definizione del metadato Identificativo del Documento Primario

(element xsd: IdIdentificativoDocumentoPrimario)

IdDoc del documento primario

Definizione del metadato Nome del documento\file

(element xsd: NomeDelDocumento)

Nome del file

Definizione del metadato Versione del documento

(element xsd: VersioneDelDocumento)

1

Definizione del metadato Tracciature modifiche documento

(element xsd: TracciatureModificheDocumento)

NON APPLICABILE ALLA TIPOLOGIA DOCUMENTALE REGISTRI GIORNALIERI DI PROTOCOLLO

Definizione del metadato Tempo di conservazione

(element xsd: TempoDiConservazione)

Numero di anni (deve essere 9999)

Definizione del metadato Note

(element xsd: Note)

Testo libero (opzionale)

Definizione del Metadato Registro giornaliero di protocollo

Numero della prima registrazione effettuata sul registro

Numero dell'ultima registrazione effettuata sul registro

Data della prima registrazione effettuata sul registro

Data dell'ultima registrazione effettuata sul registro.

Per gli ultimi quattro metadati proposti, non presenti negli esempi presenti nell'allegato cinque alle LLGG, si fornisce il seguente esempio:

```
<xs:element                                          name="registroGiornaliero"
type="registroGiornalieroType"></xs:element>

<xs:complexType name="registroGiornalieroType">

       <xs:element       name="inizioIntervallo"       type="estremoProtocollo"
use="required"/>

       <xs:element        name="fineIntervallo"        type="estremoProtocollo"
use="required"/>

</xs:complexType>


<xs:complexType name="estremoProtocollo">

       <xs:element name="numero" type="string" use="required"/>

       <xs:element name="dataCreazione" type="date" use="required"/>

</xs:complexType>
```