Manuale di Conservazione

eGlue S.r.l.
Sede legale: via degli Alpini 34 - 20090 Segrate (MI)
Sede direzionale: Via Cassanese 224 - Palazzo Raffaello B piano 6, 20090 Segrate (MI)
C.F. P.IVA 07334940157 - Capitale Sociale Euro 400.000,00 i.v.
Ufficio del Registro di Milano (MI) - n. R.E.A. 1156916
Tel. (+39) 02.36.68.44.1 - Fax (+39) 02.26.51.00.34 – www.eglue.it

Il presente Manuale è pubblicato nell'elenco dei Conservatori Accreditati sul sito istituzionale dell'Agenzia per l'Italia Digitale (AgID) www.agid.gov.it

Indice del documento

Emissione del documento			
Azione	**Data**	**Nominativo**	**Funzione**
Redazione	01/07/2019	Sebastiano Sighinolfi	Responsabile della funzione archivistica di conservazione
Verifica	08/07/2019	Davide Aprea	Responsabile del trattamento dei dati personali
Verifica	12/7/2019	Davide Coletto	Delegato Responsabile dello sviluppo e della manutenzione del sistema di conservazione LegalSolutionDOC di 2C Solution SRL
Approvazione	12/7/2019	Luca Mantovani	Responsabile del servizio di conservazione – Presidente

Registro delle versioni			
Rev.	**Data emissione**	**Modifiche apportate**	**Osservazioni**
1.0	08/04/2015	Prima emissione secondo lo schema AgID del 16 gennaio 2015	
1.1	01/07/2019	Revisione per l'accreditamento AgID ai sensi dell'art. 44-bis del decreto legislativo 7 marzo 2005, n. 82 e s.m.i. (CAD)	
1.2	05/02/2020	Integrazione tipologie di Pacchetto di Distribuzione nel paragrafo 6.4	

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente Manuale di Conservazione del servizio *eGlue Suite*, erogato e gestito dal Conservatore eGlue S.r.l., è adottato secondo le disposizioni dell'art. 8 del DPCM 3 dicembre 2013.

Il servizio di conservazione eGlue Suite utilizza il sistema *LegalSolutionDOC* di proprietà di 2C SOLUTION S.R.L., società sottoposta a controllo e direzione da parte di Namirial SPA, che è in grado di gestire l'intero processo di conservazione dei documenti informatici in conformità alla normativa vigente.

Il documento illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, le procedure, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica nel tempo del funzionamento del sistema di conservazione.

Il presente documento e gli eventuali ulteriori documenti rilasciati quali "specifiche forniture del servizio di conservazione" sono custoditi presso la sede del Conservatore. Il documento è identificato attraverso il livello di revisione e la data di emissione. Il Conservatore esegue periodicamente un controllo di conformità del processo di erogazione del servizio di conservazione e, ove necessario, aggiorna il documento in oggetto anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

Il Manuale di Conservazione, depositato e pubblico presso l'Agenzia per l'Italia Digitale, è un documento informatico prodotto nel formato PDF/A, su cui è apposta la firma digitale del Responsabile del Servizio di Conservazione e Rappresentante Legale ed è conservato secondo le disposizioni della normativa vigente, al fine di assicurarne l'origine, la data certa e l'integrità del contenuto dalla sua emissione e per tutto il periodo di conservazione.

Il presente Manuale di Conservazione è collegato ai documenti riportati nella successiva tabella, che entrano più nel dettaglio in diversi aspetti del sistema e del servizio di conservazione e costituiscono parti integranti e sostanziali del Manuale della Conservazione.

Documenti collegati	
Specificità del Contratto	Rappresenta il documento che contiene le specifiche condizioni del servizio di conservazione (SPECIFICITÀ DEL CONTRATTO) ed è parte integrante e sostanziale del contratto di servizi sottoscritto tra le parti e del Manuale di Conservazione. In genere denominato "Scheda Servizio" o "Richiesta di attivazione". Redatto dal Conservatore sulla base delle informazioni condivise con il Titolare dei documenti, contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fasi del servizio (attivazione, versamento, conservazione, post-produzione, distribuzione) oltre ai livelli di Servizio (SLA); tale documento è redatto in fase di analisi, prima del collaudo e della produzione del primo processo di conservazione.
Piano per la Sicurezza	Rappresenta il documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito del servizio di conservazione.

Torna al sommario

2 TERMINOLOGIA

2.1 Glossario

Glossario dei termini	
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di dichiarazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento
Aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archiviazione	Processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo che permette una loro classificazione (indicizzazione) ai fini della ricerca e consultazione
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticazione del documento informatico	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati correlati e registrati tra loro
Certificato qualificato	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva
Certification Authority (CA)	Il soggetto che secondo quanto disposto dall'art. 27 del CAD presta servizi di certificazione delle firme elettroniche qualificate o che fornisce altri servizi connessi con queste ultime, quali ad esempio quello delle marche temporali

Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Comunità di riferimento	Un gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere l'informazione conservata. Una comunità di riferimento può essere composta anche da più comunità di utenti
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'art. 12 del DPCM 3 dicembre 2013
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Dispositivo sicuro per la creazione della firma:	I dispositivi sicuri per la generazione della firma qualificata che devono essere dotati di certificazione di sicurezza secondo l'art. 35 del CAD
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno

	specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica
Firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
Firma elettronica qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Formazione	l processo atto ad assicurare l'autenticità dell'origine e l'integrità del contenuto dei documenti informatici, con apposizione della firma digitale su ciascun singolo documento e/o della marca temporale ai fini di associare una data certa elettronica ove richiesto
FTP Server	Programma che permette di accettare connessioni in entrata e di comunicare in maniera sicura con un Client attraverso il protocollo FTP
Funzioni archivistiche	Funzioni per la conservazione delle informazioni (acquisizione, archiviazione, gestione dei dati, accesso, distribuzione)
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Identificazione informatica	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso

IDM	Strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
Indice del Pacchetto di Archiviazione	Struttura dell'insieme dei dati a supporto del processo di conservazione, riferita allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010)
Indice del Pacchetto di Versamento	Struttura dell'insieme dei dati a supporto del processo di versamento del pacchetto di versamento (PdV), ispirata allo standard internazionale OAIS ISO 14721:2012 e definita nello specifico dal Conservatore in accordo con il produttore dei documenti
Indice del Pacchetto di Distribuzione	Struttura dell'insieme dei dati a supporto del processo di distribuzione del pacchetto di distribuzione (PdD), ispirata allo standard internazione OAIS ISO 14721:2012 e definita nello specifico dal Conservatore in accordo con il produttore dei documenti
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite sul sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'art. 8 del DPCM 3 dicembre 2013, regole tecniche in materia di sistema di conservazione.
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3 dicembre 2013

Originali non unici	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013 e secondo le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto di scarto	Pacchetto contenente i documenti da scartare dal Sistema di conservazione perché hanno raggiunto il loro termine temporale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
Piano per la sicurezza	È il documento aziendale che analizza il contesto in cui l'azienda opera riportando i fattori interni ed esterni che lo influenzano ed evidenzia le principali criticità legate alla gestione della sicurezza delle informazioni gestite
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 9 delle regole tecniche sul sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'art. 7, c. 1, del DPCM 3 dicembre 2013 e che opera presso il Produttore
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
Responsabile del servizio di conservazione	Soggetto persona fisica nominato responsabile del servizio di conservazione con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile della funzione archivistica di conservazione	Soggetto persona fisica nominato responsabile della funzione archivistica di conservazione con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)

Responsabile del trattamento dei dati personali	Soggetto persona fisica nominato responsabile del trattamento dei dati personali del servizio di conservazione con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Responsabile della sicurezza dei sistemi per la conservazione	Soggetto persona fisica nominato responsabile della sicurezza dei sistemi per la conservazione con l'assegnazione delle attività indicate nel documento dell'Agenzia per l'Italia Digitale sui profili professionali richiamati dalla Circolare n. 65/2014 (G.U. n. 89 del 16/04/2014)
Riferimento temporale	Informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Service Level Agreement	È l'accordo tra produttore e responsabile del servizio di conservazione sui livelli di servizio da garantire ed indica i giorni entro cui devono essere conservati i documenti nel Sistema di conservazione
Sessione di distribuzione	Sessione telematica per la consegna (distribuzione) di uno o più Pacchetti di Distribuzione dall'Ente Conservatore all'Ente Produttore, sulla base di un modello-dati per i formati ed i contenuti definito e concordato tra le parti.
Sessione di ricerca	Una sessione telematica avviata da un Utente di un sistema di conservazione, durante la quale l'Utente usa gli Strumenti di Ricerca del sistema per individuare e consultare gli oggetti digitali in esso presenti.
Sessione di versamento	Sessione telematica per la consegna (versamento) di uno o più pacchetti di Versamento dall'Ente Produttore all'Ente Conservatore, sulla base di un modello-dati per i formati ed i contenuti definito e concordato tra le parti.
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'art. 44 del Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005, n. 82 e successive modifiche ed integrazioni)
Titolare	La persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Validazione temporale	Il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi
Versamento agli archivi di stato	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

Torna al sommario

2.2 Acronimi

Acronimi	
AE	Agenzia delle Entrate
AgID	Agenzia per l'Italia Digitale (già DigitPA e CNIPA)
CAD	Codice dell'Amministrazione Digitale
CNIPA	Centro Nazionale per l'Informatica della Pubblica Amministrazione, ora AgID
FTP	File Transfer Protocol
SFTP	SSH File Transfer Protocol o SFTP è un protocollo di rete che prevede il trasferimento dei dati e funzionalità di manipolazione. Usato con protocollo SSH-2 per il trasferimento dei file sicuro.
IDM	Identity Management
IPA	Indice delle Pubbliche Amministrazioni
IPdA	Indice del Pacchetto di Archiviazione
IPdD	Indice del Pacchetto di Distribuzione (o Rapporto di distribuzione)
IPdV	Indice del Pacchetto di Versamento
ISO	International Organization for Standardization
OAIS	Open Archival Information System, ISO 14721:2012
PdD	Pacchetto di Distribuzione
PdS	Pacchetto di Scarto
PdV	Pacchetto di Versamento
RdV	Rapporto di Versamento
SdI	Sistema d'Interscambio per la fatturazione elettronica PA per lo scambio delle fatture e delle relative notifiche/ricevute ai sensi del DM 3 aprile 2013, n. 55
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SLA	Service Level Agreement
TSA	Time Stamping Authority
SdC	Sistema di Conservazione
SOC	Security Operations Center

Torna al sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Nel presente paragrafo è riportata la principale normativa di riferimento per l'attività di conservazione a livello nazionale, ordinata secondo il criterio della gerarchia delle fonti:

Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;

Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;

Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;

Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);

Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;

Circolare AgID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Regolamento europeo eIDAS 910/2014/EC del 24 luglio 2014 – regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni

ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

La normativa specifica relativa alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione è riportata nel documento "Specificità del Contratto".

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento a cui l'attività di conservazione si riferisce, elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014, come indicato nelle regole tecniche di cui al DPCM 3 Dicembre 2013.

ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

UNI 11386:2010 Standard SInCRO - Supporto all' Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

UNI ISO 15489 Informazioni e documentazione – Gestione dei documenti di archivio (record).

Torna al sommario

4 RUOLI E RESPONSABILITÀ

Il servizio di conservazione descritto nel presente manuale, come prescritto dall'art. 5 del DPCM 3 dicembre 2013, descrive l'adozione del modello organizzativo governato dal conservatore eGlue che coinvolge soggetti, strutture e/o funzioni deputate al versamento, all'implementazione, all'erogazione del processo, alla gestione e al controllo del sistema di conservazione di documenti informatici.

Il servizio di conservazione *eGlue Suite*, gestito dal Conservatore **eGlue** e dal suo Responsabile del Servizio di Conservazione, è basato su un modello organizzativo di riferimento definito formalmente nei ruoli e nelle responsabilità dei vari attori coinvolti nel processo di conservazione dei documenti informatici, come riportato nella tabella successiva, in conformità ai ruoli e alle attività ad essi associati indicati nel documento "Profili professionali" pubblicato da AgID sul proprio sito istituzionale.

In particolare, per il servizio di conservazione di documenti informatici, eGlue ha adottato un modello **SaaS** per cui con la propria struttura organizzativa eroga il servizio ai propri Clienti utilizzando una istanza completamente dedicata ad eGlue del sistema *LegalSolutionDOC* gestita dal conservatore accreditato 2C SOLUTION S.r.l. afferente al gruppo Namirial Spa.

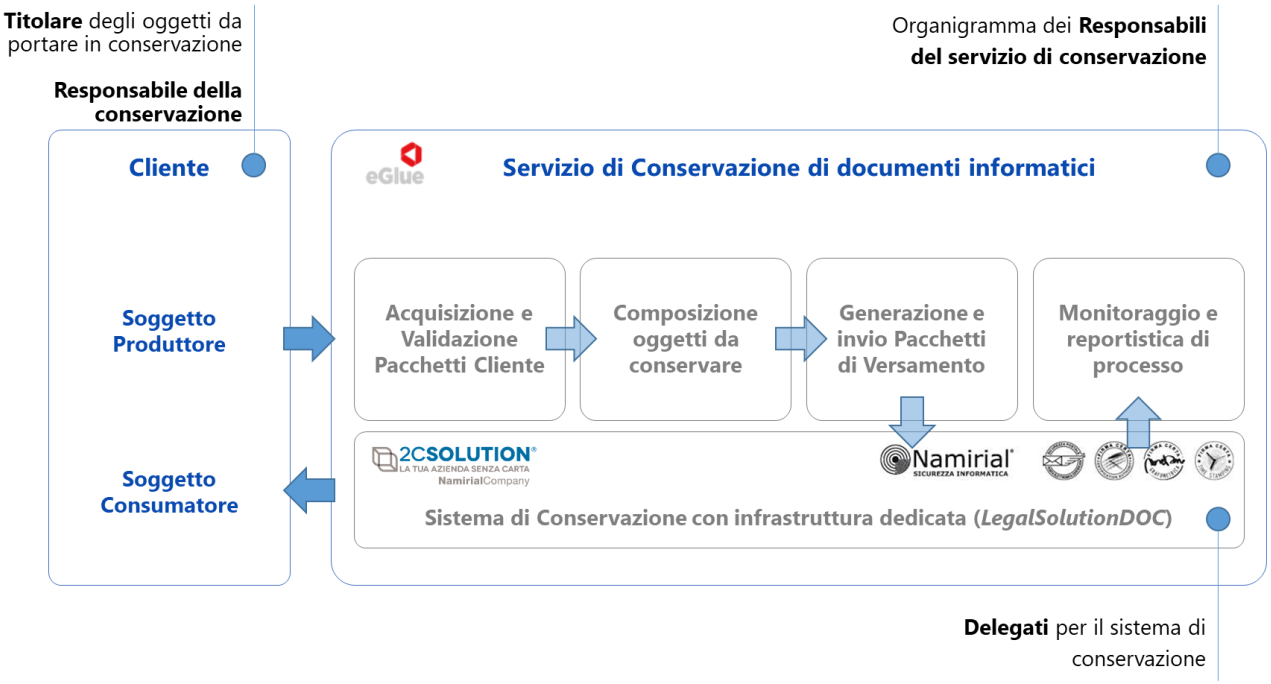


Figura 1 – Schema di processo e responsabilità del servizio di conservazione

Il servizio di conservazione eGlue Suite riprende il modello di riferimento OAIS (Open Archival Information System) recepito come standard ISO 14721:2005/2014.
Il modello definisce il ruolo degli attori, i Produttori e i Consumatori, che insieme costituiscono la Comunità Designata, cioè l'insieme di soggetti che interessati e destinatari del processo di conservazione, e le relazioni di questi con il Responsabile del Servizio di Conservazione (Management) che gestisce il sistema di conservazione.

Il servizio di conservazione di eGlue prevede la gestione di pacchetti informativi preposti a collegare i contenuti informativi e le informazioni rilevanti per la conservazione e si distinguono in base alle diverse fasi di gestione del processo di conservazione:

- Pacchetto Cliente (*Customized Submission Information Package* – Custom SIP), che viene inviato dal Titolare o Soggetto Produttore al servizio di conservazione eGlue Suite per trasferire i contenuti da portare in conservazione (Content Information) e i meta-dati (Preservation Description Information) necessari ad individuare univocamente e preservare i contenuti associati;
- Pacchetto di Versamento (*Submission Information Package* – SIP) che viene trasmesso nella fase di versamento al sistema di conservazione;
- Pacchetto di Archiviazione (*Archival Information Package* – AIP) che viene generato a partire dal SIP in fase di accettazione e poi diventa oggetto diretto della conservazione;
- Pacchetto di Distribuzione (*Dissemination Information Package* – DIP) che viene generato a partire dall'AIP per essere distribuito alla Comunità Designata per la fruizione.

Il Conservatore eGlue ed il Titolare hanno la facoltà di negoziare il formato e i criteri di validazione del Pacchetto Cliente affinché sia garantito il contenuto informativo minimo necessario per la corretta composizione del Pacchetto di Versamento verso il sistema di conservazione da parte di eGlue in qualità di Produttore.
Il documento Specificità del Contratto – Scheda Servizio raccoglie le specifiche tecniche concordate in termini di formato e contenuto del Pacchetto Cliente e di canale sicuro di trasmissione a cui il Soggetto Produttore deve attenersi per generare e trasferire al Conservatore eGlue i pacchetti informativi.
Il Soggetto Produttore deve verificare il buon esito del trasferimento e risolvere eventuali anomalie che impediscano al Conservatore eGlue di alimentare in modo corretto ed esaustivo il sistema di conservazione.

Si precisa che il nominativo ed i riferimenti del Responsabile della conservazione del cliente sono indicati nell'allegato "Specificità del contratto" nel quale sono anche riportate le attività affidate al Responsabile del servizio di conservazione.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo (dal – al)
Responsabile del servizio di conservazione	Luca Mantovani	-Definizione ed attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; -definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; -corretta erogazione del servizio di conservazione all'ente produttore; -gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	12/01/2015 - oggi

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo (dal – al)
Responsabile della funzione archivistica di conservazione	Sebastiano Sighinolfi	-Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; -definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; -monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; -collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	01/07/2019 - oggi
Responsabile del trattamento dei dati personali	Davide Aprea	-Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; -garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	01/07/2019 - oggi
Responsabile della sicurezza dei sistemi per la conservazione	Alessandro Petrini	-Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; -segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	01/07/2019 - oggi
Responsabile dei sistemi informativi per la conservazione	Alessandro Petrini	-Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; -monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; -segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e	01/07/2019 - oggi

		pianificazione delle necessarie azioni correttive; -pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; -controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Sebastiano Sighinolfi	-Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; -pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; -monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; -interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; -gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	01/07/2019 - oggi

4.1 Deleghe

In virtù della partnership fra eGlue e 2C Solution basata sull'impiego da parte di eGlue di una istanza dedicata della soluzione LegalSolutionDOC, sono state definite le seguenti deleghe, regolate dall'accordo quadro in essere fra eGlue e 2C Solution. Per ciascuna delega viene indicata l'attività delegata.

- Supporto al Responsabile del servizio di conservazione: 2C SOLUTION SRL con la sua struttura organizzativa
    - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;
    - corretta erogazione del servizio di conservazione al soggetto produttore.

- Supporto al Responsabile della sicurezza dei sistemi per la conservazione: 2C SOLUTION SRL con la sua struttura organizzativa
    - Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;
    - Segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

- Supporto al Responsabile dei sistemi informativi per la conservazione: 2C SOLUTION SRL con la sua struttura organizzativa
    - Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;
    - Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;
    - Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.

- Supporto al Responsabile dello sviluppo e della manutenzione del sistema di conservazione: 2C SOLUTION SRL con la sua struttura organizzativa
    - Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;
    - Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;
    - Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;
    - Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;
    - Gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

eGlue considera il miglioramento continuo delle performance dei propri processi e servizi, nonché del Sistema della Sicurezza delle informazioni, uno degli strumenti strategici attraverso il quale conseguire gli obiettivi del proprio business, costituito dalla fornitura di risorse e professionalità e quindi di una struttura organizzativa a supporto per la progettazione, sviluppo, gestione, erogazione e commercializzazione dei propri servizi.

In particolare, eGlue ha definito un insieme di politiche e obiettivi per gestire in maniera integrata e proattiva gli aspetti della propria attività che riguardano la Qualità, l'Ambiente, la Sicurezza delle Informazioni e la Sicurezza delle Tecnologie.
La gestione Integrata è volta ad **affrontare** i **rischi** connessi al **business** di eGlue ed in particolare a **garantire** che:

- Le esigenze/aspettative dei clienti vengano soddisfatte da prodotti/servizi di qualità;
- L'attività dell'azienda sia rispettosa dell'ambiente, nell'ottica della sostenibilità ambientale;
- Sia in atto una gestione sicura delle informazioni, come aspetto rilevante del servizio offerto;
- Il lavoro delle persone si svolga in condizioni di sicurezza.

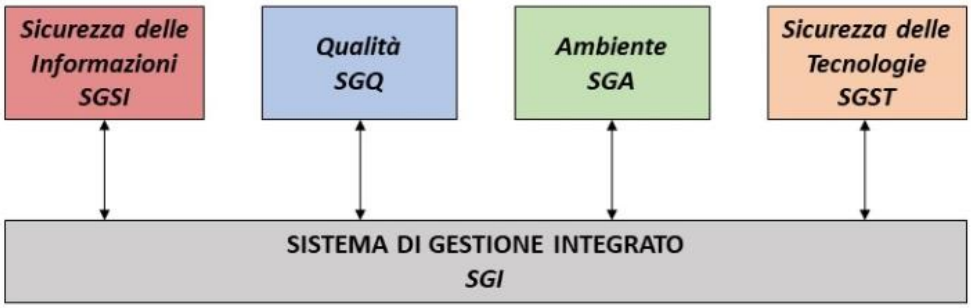


Figura 2– Sistema di Gestione Integrato di eGlue

L'ambito di applicazione della **Gestione Integrata** comprende **tutti i servizi** di **eGlue**, descritto nel modo seguente:
Progettazione, sviluppo ed erogazione di servizi gestiti per la composizione, la distribuzione digitale e la fruizione interattiva, la dematerializzazione, la fatturazione elettronica, la conservazione sostitutiva a norma, la stampa digitale, il confezionamento e la conservazione fisica di comunicazioni e documenti di business.

Rispetto a questo ambito eGlue detiene le seguenti certificazioni.

ISO9001:2015	Requisiti standard sistema gestione qualità (SGQ)
ISO14001:2015	Requisiti standard sistema gestione ambientale (SGA)
ISO27001:2013	Requisiti standard sistema gestione sicurezza informazioni (SGSI)
FSC-STD-40-004 V3-0	Requisiti standard catena di custodia (CoC)

La **Gestione Integrata** promuove il **principio del miglioramento continuo** a **tutte le funzioni** e **livelli** dell'organizzazione.

Il servizio di conservazione dei documenti informatici di eGlue adotta un **modello SaaS** secondo cui la propria struttura organizzativa eroga il Servizio ai propri Clienti, mentre l'infrastruttura a supporto del Servizio è completamente dedicata e gestita dal conservatore accreditato 2C Solution.
I principi del Sistema di Gestione Integrato di eGlue recepiscono quindi le certificazioni di 2C Solution che comprendono

- Il proprio **Sistema di Gestione della Sicurezza delle Informazioni** nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione (certificazione **ISO/IEC 27001:2013),** in particolare nel perimetro "*Progettazione ed erogazione di servizi gestiti in modalità Saas, Paas e on premise in ambito Enterprise Content Management e paperless business (Business Process Management, acquisizione e trasmissione dei documenti, fatturazione elettronica, formazione documenti, gestione archiviazione e conservazione a Norma di documenti informatici)*";
- Il **Sistema di Gestione della Qualità** secondo la norma **UNI EN ISO 9001:2008**, che comprende il perimetro predetto.

Torna al sommario

5.1 Organigramma

Di seguito l'organigramma adottato dall'organizzazione eGlue per la gestione del servizio di conservazione di documenti informatici:

Figura 3 – Organigramma del servizio di conservazione

Le funzioni aziendali coinvolte nel servizio di conservazione dei documenti informativi sono:

- Sales: ha la responsabilità dei contenuti contrattuali che regolamentano il servizio;
- Service Management: supporta la funzione Sales nella definizione dei contenuti specifici del servizio da allegare al contratto ed è responsabile del servizio nei confronti del cliente una volta che è attivato;

- Service Delivery: è l'unità organizzativa che configura gli asset del servizio di conservazione rispetto ai requisiti specifici contenuti nella scheda servizio;
- Service Operation: ha la responsabilità della corretta esecuzione del servizio;
- Demand: è la funzione che presiede l'analisi e la progettazione funzionale dei requisiti evolutivi del servizio di conservazione;
- Development: ha la responsabilità degli sviluppi sul sistema di conservazione;
- IT & Security: determina i requisiti aziendali in termini di infrastruttura e sicurezza ed è responsabile della verifica sulla loro corretta applicazione;
- Compliance: determina i requisiti aziendali in termini di qualità nell'erogazione del servizio e contribuisce alla verifica della loro corretta applicazione.

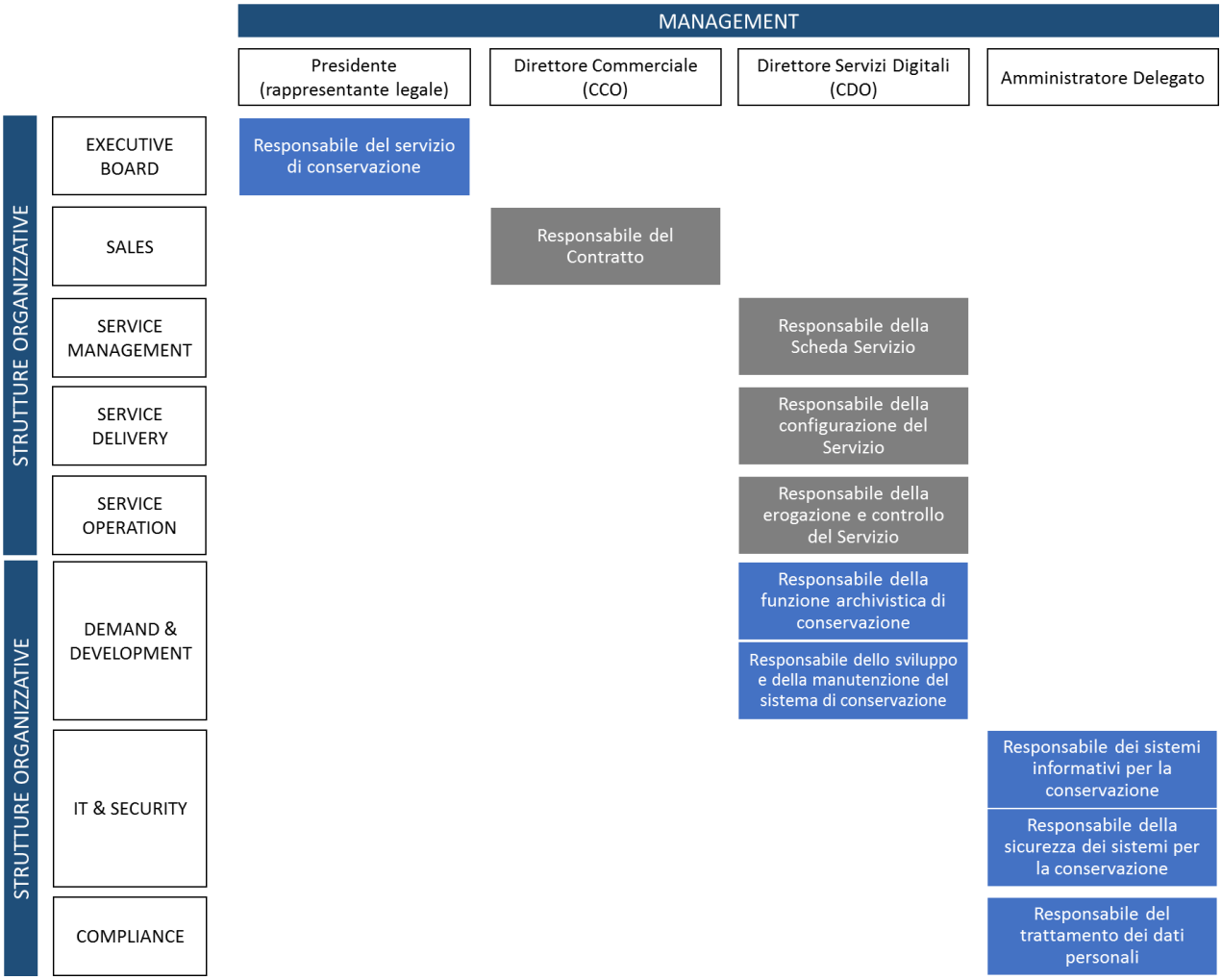


Figura 4 – Funzioni aziendali e responsabilità per il servizio di conservazione

Torna al sommario

5.2 Strutture organizzative

Il servizio di conservazione eGlue Suite presenta un ciclo di vita caratterizzato da tre fasi principali: **attivazione, produzione e post-produzione.**

Figura 5 – Fasi del servizio di conservazione

In ciascuna fase del servizio sono previste delle sotto fasi principali:

Attivazione	Predisposizione e condivisione della "Scheda Servizio Cliente Specificità di Contratto" per la definizione dei requisiti di servizio Cliente
	Configurazione servizio di conservazione
	Collaudo e sua validazione

La fase di **Attivazione** del servizio viene avviata in caso di formale accettazione dell'offerta e delle condizioni contrattuali di servizio da parte del Produttore dei documenti, inclusi gli atti di nomina sottoscritti tra le parti per svolgere il ruolo di Responsabile della Conservazione e Responsabile del Trattamento dei dati.

L'**Area Sales** di eGlue, owner del processo di vendita del servizio e del completamento dell'accordo tra le parti, invia tramite sistema aziendale di tracciatura delle opportunità commerciali la richiesta di attivazione operativa del Cliente all'**Area Service Management** che, presa in carico l'attività, contatta il Cliente e predispone la "*Scheda Servizio Cliente - Specificità del Contratto*".
Questo documento è fondamentale per l'erogazione del servizio ad un determinato Cliente (produttore dei documenti) ed è parte integrante del contratto di servizio e del manuale, redatto dal Conservatore sulla base delle informazioni condivise con il produttore dei documenti (Cliente) e contenente i requisiti essenziali del servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fasi in cui si articola (attivazione, versamento, conservazione, post-produzione, distribuzione) oltre ai livelli di Servizio (SLA) ed alla pianificazione della fase di collaudo e produzione; tale documento è redatto in fase di analisi, prima del collaudo e del primo processo produttivo di conservazione.
In caso di specifica assistenza richiesta dal produttore dei documenti relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche, l'Area di Service Management gestisce la richiesta con il Cliente e richiede un intervento di assistenza all'area **Demand**, che pertanto s'interfaccia con l'ente produttore al fine di definire correttamente la modalità da inserire in Scheda Servizio Cliente. Una volta definito l'intervento di sviluppo necessario al fine di soddisfare la richiesta specifica del cliente, l'area **Demand** ingaggia la funzione **Development** per la realizzazione dell'intervento.

La predisposizione della corretta definizione iniziale dei requisiti e quindi la conformità alla normativa vigente in materia di sistemi di conservazione, con anche l'individuazione degli adempimenti correlati, è assicurata in fase di analisi dalla predisposizione della Scheda Servizio Cliente, con il controllo e la supervisione da parte

del **Demand** che esprime il **Responsabile della funzione archivistica di conservazione, del Responsabile del trattamento dei dati personali** (in caso di necessità) e del **Responsabile del servizio di conservazione** che ha in carico l'approvazione finale.

Successivamente, il processo prevede che ad ogni variazione del Servizio (Change Process), la Scheda Servizio debba essere aggiornata e nuovamente condivisa tra le parti.

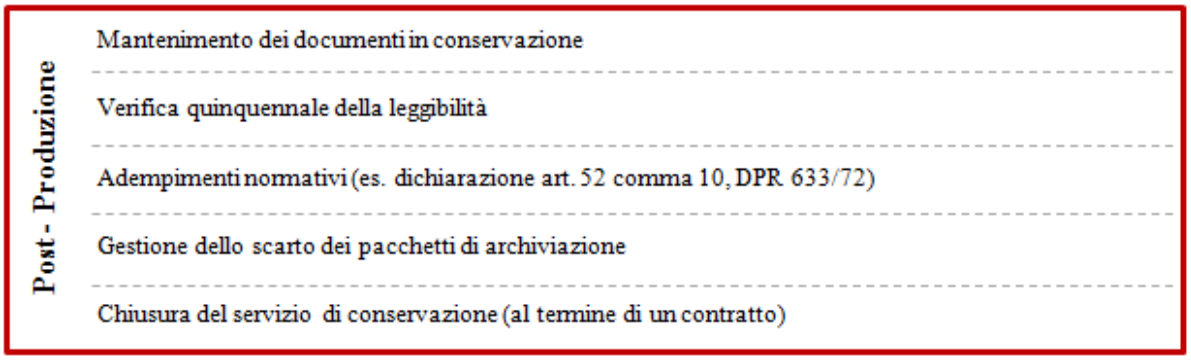
Predisposta e condivisa la Scheda Servizio Cliente, validata dal Responsabile del servizio di conservazione e dal Cliente, l'area di Service Management ingaggia l'**Area di Service Delivery** che avvia le attività di configurazione del servizio nella piattaforma eGlue Suite al fine di eseguire il collaudo.
Prima viene eseguito un collaudo interno (verifica interna dell'Area di Delivery delle configurazioni eseguite in coerenza con quanto concordato dalla *Scheda Servizio Cliente - Specificità del Contratto*) e poi si esegue, previa pianificazione, il collaudo con il Cliente. Le modalità del collaudo sono indicate nella scheda di servizio; a seguito del collaudo e della sua validazione formale da parte del cliente si procede con la successiva fase di messa in produzione.

Produzione	Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico
	Generazione dei rapporti di versamento
	Preparazione e gestione dei pacchetti di archiviazione
	Erogazione in alta disponibilità, replica geografica dei dati e procedure di backup
	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta

L'area organizzativa di **Service Operation** si occupa di presidiare, controllare e monitorare il corretto funzionamento dei sistemi per la sua erogazione tramite l'ausilio di esiti, monitor, report ed altri strumenti di controllo (sistema di monitoraggio delle eGlue Suite). Il sistema di conservazione viene controllato e monitorato attraverso i sistemi di monitoraggio forniti da 2C Solution per l'istanza dedicata al servizio di eGlue.

Inoltre, l'Area di Service Operation presidia gli asset di infrastruttura e la corretta esecuzione del processo, dalla fase di presa in carico, al controllo di coerenza, dalla generazione del rapporto di versamento, alla preparazione e gestione dei pacchetti di archiviazione, fino alla preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta dell'utente.
In particolare, il **Responsabile dei sistemi informativi per la conservazione** ha l'ownership delle attività di controllo degli asset e di monitorare il corretto svolgimento del servizio. In caso di riscontro di incident viene attivato il processo di gestione e risoluzione dell'incident attraverso la creazione di un ticket al fine di tracciare l'accaduto e risolvere l'anomalia. Eventuali incident di rilievo e difformità sono segnalate al **Responsabile del servizio di conservazione** attraverso apposita procedura riportata nel paragrafo 9.3.1 e ricompresa nel sistema di gestione aziendale conforme allo standard ISO/IEC 27001:2013.

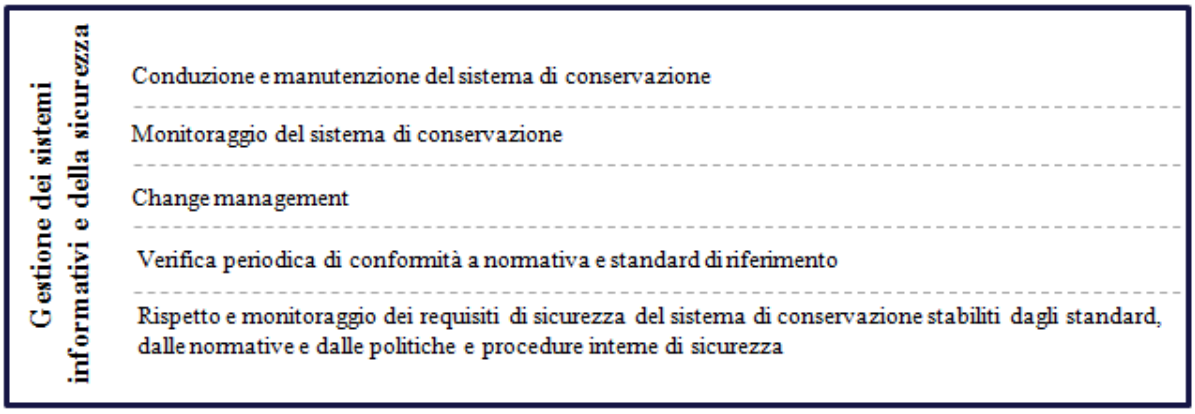
Completato con esito positivo il processo produttivo della conservazione dei documenti, il servizio per un determinato Cliente deve essere mantenuto nel tempo anche nella fase di post-produzione, per tutta la durata contrattuale concordata, garantendo ai documenti ed ai pacchetti informativi integrità, autenticità dell'origine, leggibilità, disponibilità e reperibilità, sicurezza e riservatezza.



Il mantenimento dei documenti e dei pacchetti generati nel processo di conservazione è garantito dalle attività dell'**Area di Service Operation** che presidiano il funzionamento del sistema sia dal punto di vista infrastrutturale che applicativo in collaborazione con le strutture operative di monitoraggio di 2C Solution.
Durante la fase di post-produzione la struttura organizzativa di eGlue supporta gli adempimenti previsti dalla normativa (a titolo di esempio non esaustivo la dichiarazione art. 52, decimo comma, D.P.R. 633/72).

Infine, scaduto il periodo di conservazione, concordato contrattualmente tra produttore dei documenti e Responsabile della conservazione, viene avviata la procedura di Scarto concordata, con la produzione dei Pacchetti di Scarto e la verbalizzazione dello scarto e della chiusura del servizio. Owner di queste attività sono l'Area di Service Management e di Service Operation.
Prima dell'avvio dello scarto e della procedura di chiusura del Servizio, che si conclude con una verbalizzazione dell'attività, viene comunicato al produttore l'avvio dello scarto entro 30 gg al fine di fornirgli un periodo transitorio per richiedere formalmente l'estensione (prolungamento) del periodo di conservazione. Inoltre, come da disposizioni del codice dei beni culturali (D. Lgs. 22 gennaio 2004, n.42) nel caso di enti pubblici o privati dichiarati di notevole interesse storico, per effettuare lo scarto verrà richiesta l'autorizzazione preventiva alla Soprintendenza Archivistica da parte del Produttore

Infine, in tutte le predette fasi del servizio di conservazione eGlue Suite ed in generale in tutte le attività in carico ad un Conservatore è necessario garantire la **Gestione dei sistemi informativi e della sicurezza a supporto del servizio**.



Tale obiettivo viene perseguito dall'organizzazione eGlue attraverso la definizione di compiti, ruoli e responsabilità come descritto nel presente manuale, attraverso verifiche ed audit periodici e tramite l'ausilio di strumenti per il controllo ed il monitoraggio. Le procedure definite all'interno del Sistema di Gestione per la Sicurezza delle Informazioni sono gli strumenti primari anche ai fini dell'analisi del rischio, della pianificazione e quindi ai fini dell'adozione di misure per la prevenzione, la manutenzione ed il miglioramento continuo del servizio.
Attori primari dell'attuazione della gestione dei sistemi informativi e della sicurezza sono i responsabili definiti nell'organigramma per la conservazione, che di concerto devono garantire l'obiettivo aziendale e gestire la compliance ed il miglioramento della qualità del servizio.

Torna al sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il funzionamento del sistema di conservazione *LegalSolutionDOC* è basato sulla compliance alle regole tecniche di cui al DPCM 3 dicembre 2013 ed allo standard ISO 14721:2012 OAIS (Open Archival Information System), modello di riferimento di sistema informativo per l'archiviazione e la conservazione degli oggetti digitali.
Alla base del funzionamento del predetto modello OAIS e quindi delle regole tecniche vigenti vi è il concetto di informazione da conservare e quindi di pacchetto informativo.
Il versamento dei pacchetti (contenenti documenti e dati) al Sistema *LegalSolutionDOC* da parte di eGlue e ogni distribuzione di documenti dal Sistema ad un Utente autorizzato avvengono infatti nella forma di una o più trasmissioni distinte (sessioni) ovvero tramite lo scambio (versamento o distribuzione) di pacchetti informativi.

Il Responsabile del Servizio di Conservazione e Conservatore eGlue, ispirandosi ai principi dello standard OAIS, utilizza nel Sistema di Conservazione e nelle fasi fondamentali del processo i pacchetti informativi intesi come contenitori astratti contenenti due tipologie di informazioni:
- contenuto informativo;
- informazioni sulla Conservazione (PDI).

Contenuto informativo
L'insieme delle informazioni che costituisce l'obiettivo originario della conservazione; è un *Oggetto informativo* composto dal suo *Oggetto dati* e dalle sue *Informazioni di rappresentazione*:

- Oggetto dati: oggetto digitale composto da un insieme di sequenze di bit;
- Informazioni sulla rappresentazione: informazioni che rappresentano un Oggetto dati ovvero lo associano a concetti più significativi (es: formato). Include le Information properties, ovvero le informazioni significative che devono essere mantenute nel tempo (es.: alcuni elementi della formattazione, ecc.)

Informazioni sulla Conservazione (PDI Preservation Description Info):
Informazioni necessarie per un'adeguata conservazione del Contenuto informativo: sono fornite dai metadati e possono essere classificate in:

- *Informazioni sulla provenienza* (documentano la storia del Contenuto informativo: ad esempio forniscono informazioni sull'origine/sulla fonte del Contenuto informativo e su chi ne ha curato la custodia sin dalla sua origine).
- *Informazioni sull'identificazione* (identificano e se necessario descrivono uno o più meccanismi di attribuzione di identificatori al Contenuto informativo).
- *Informazioni sull'integrità* (informazioni che garantiscono che il Contenuto informativo non sia stato alterato senza una documentazione dell'evento).
- *Informazioni sul contesto* (informazioni che documentano le relazioni del Contenuto informativo con il suo ambiente, inclusi i motivi della creazione del Contenuto informativo e il modo in cui è in relazione con altri Contenuti informativi).
- *Informazioni sui diritti di accesso* (informazioni che possono identificare i limiti di accesso al contenuto informativo, inclusi i termini di licenza, le restrizioni legali e i sistemi di controllo).

Il Contenuto informativo e le Informazioni sulla conservazione sono incapsulati e identificabili mediante le Informazioni sull'Impacchettamento, ovvero informazioni usate per collegare e identificare le componenti di un pacchetto informativo (Contenuto informativo e Informazioni sulla conservazione).

Il pacchetto informativo, infine, può essere trovato nel sistema di conservazione tramite le informazioni descrittive ovvero l'insieme delle informazioni – composto essenzialmente dalla Descrizione del pacchetto – necessarie all'utente per ricercare, richiedere e recuperare le informazioni conservate dal Sistema.

Affinché la conservazione dell'oggetto informativo avvenga correttamente il Sistema *LegalSolutionDOC* è basato, quindi, su un modello che permette di identificare e comprendere l'oggetto-dati e le relative informazioni sulla rappresentazione, che contengono informazioni sia di natura sintattica che semantica.

Torna al sommario

6.1 Oggetti conservati

Nel documento "Specificità del Contratto" concordato tra Conservatore eGlue e Cliente sono elencate e descritte le tipologie di documenti sottoposte a conservazione per quel determinato Cliente e le relative politiche di conservazione.
In particolare, tali politiche di conservazione relative agli oggetti conservati riguardano per ciascuna tipologia documentale:

- La natura e l'oggetto della tipologia documentale;
- L'elenco e la descrizione dei formati (comprensivi della relativa versione) dei file utilizzati;
- L'indicazione dei visualizzatori relativi ai formati gestiti, necessari per garantire la leggibilità nel tempo dei documenti conservati;
- L'elenco e la descrizione dei metadati associati ai documenti;
- Il periodo di conservazione;
- I livelli di servizio (SLA) concordati con l'ente produttore;
- Altre politiche (regole) che caratterizzano il processo di conservazione.

Le tipologie di documenti che caratterizzano gli oggetti digitali da versare nel sistema di conservazione *LegalSolutionDOC* sono definite attraverso le attività di analisi e di classificazione documentale nella fase di prevendita ed attivazione del servizio.
La descrizione delle tipologie documentali, con l'indicazione della loro natura, dei formati, dei metadati obbligatori e dei metadati opzionali, delle regole e della durata di conservazione (piano di conservazione e successivo scarto) sono riportate nel dettaglio in una tabella per ciascuna tipologia nel documento allegato "Specificità del Contratto" e sono peculiari di ciascun produttore dei documenti e di ciascuna tipologia documentale.

Di seguito, si riporta un esempio di draft della tabella da compilare nel documento "Specificità del Contratto" del servizio di conservazione di eGlue.

1	**CLASSE DOCUMENTALE**		**……**
1.1	**Codice della tipologia nel Sistema di conservazione**		……..
1.2	**Natura di documento informatico amministrativo**		Sì o No
1.3	**Apposizione della firma digitale su ciascun singolo documento eseguita da eGlue (nella fase di formazione)**		Sì o No
1.4	**Apposizione della marca temporale su ciascun singolo documento eseguita da eGlue (nella fase di formazione)**		Sì o No
1.5	**Metadati**	*In questa sezione della tabella sono inseriti tutti i metadati associati alla specifica tipologia documentale, indicandone la loro descrizione ed il loro valore (stringa, numero, data).* *Per ciascun metadato si dichiara se è un metadato "obbligatorio" in quanto richiesto dalla normativa vigente a seconda della natura della tipologia documentale ovvero in quanto richiesto dall'accordo tra ente produttore ed ente conservatore.*	
1.6	**Presenza di fascicolo informatico o aggregazione documentale**		Sì o No
1.7	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**		…..
1.8	**Durata di conservazione richiesta**		Esempio: 10 anni
1.9	**Formato del file**		…

I formati dei files contenuti nel Pacchetti di Versamento devono essere conformi all'elenco dei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013.
I formati associati alla tipologia documentale sottoposta a conservazione sono dichiarati nella tabella precedente nella fase di analisi antecedente l'attivazione del servizio di conservazione.

Il sistema di conservazione *LegalSolutionDOC* verifica nella fase di presa in carico per l'accettazione e l'individuazione dello specifico Mimetype che i documenti siano adeguati al seguente elenco dei formati ammessi.

Formato del file	Proprietario	Estensione	Standard	Mimetype	Visualizzatore	Produttore del visualizzatore
PDF	Adobe Systems - www.adobe.com	.pdf	ISO32000-1	application/ pdf	Adobe Reader	Adobe Systems www.adobe.com
PDF/A	Adobe Systems - www.adobe.com	.pdf	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	application/ pdf	Adobe Reader http://www.pdfa.org/doku.php	Adobe Systems - www.adobe.com
XML	W3C	.xml		application/ xml text/xml	Mozilla - Chrome - Internet Explorer	Firefox - Google - Microsoft
TXT	Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata	.txt			Mozilla - Chrome - Internet Explorer	Firefox - Google - Microsoft

Formato del file	Proprietario	Estensione	Standard	Mimetype	Visualizzatore	Produttore del visualizzatore
TIFF	Aldus Corporation in seguito acquistata da Adobe	.tif	-	image/tiff	Vari visualizzatori di immagini	
JPG	Joint Photographic Experts Group	.jpg, .jpeg	ISO/IEC 10918:1	image/jpeg	Vari visualizzatori di immagini	Per maggiori informazioni sul formato www.jpeg.org
EML	Vari	.eml	RFC2822		Client di posta elettronica supportano la visualizzazione di file eml	Vari
OOXML	Microsoft	.docx, .xlsx, .pptx	ISO/IEC DIS 29500:2008	-		Tale formato deve garantire alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML
ODF	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odb	ISO/IEC 26300:2006	application/ vnd.oasis.opendocument.text		www.oasis-open.org

In tutti i casi riportati in tabella, eGlue s'impegna a versare al sistema di conservazione *LegalSolutionDOC* documenti privi di codici eseguibili o macro istruzioni o privi di qualsiasi causa, anche non visibile all'utente, che ne possa alterare il contenuto.

Infine, gli oggetti da conservare sono versati al sistema di conservazione da eGlue all'interno di Pacchetti Informativi denominati Pacchetti di Versamento e descritti nel paragrafo successivo.

Torna al sommario

6.2 Pacchetto di Versamento

Il Pacchetto di Versamento (PdV) del sistema di conservazione *LegalSolutionDOC* è costituito da un contenitore (archivio) nel formato zip compresso, contenente:

- I documenti oggetti da conservare (*Content Information*), eventualmente firmati digitalmente (nello standard di firma CAdES ".p7m" ovvero nello standard PAdES ovvero XAdES) o eventualmente marcati temporalmente (nello standard di validazione temporale CAdES-T ovvero nello standard PAdES-T ovvero XAdES-T);
- Un file Indice IPdV (Indice del Pacchetto di Versamento) ovvero le *Preservation Description Information*, finalizzato alla descrizione dell'oggetto della conservazione e che secondo lo standard ISO 14721:2012 OAIS permette di identificare il produttore, di contenere i dati descrittivi ed informativi sull'impacchettamento ed i dati descrittivi e di rappresentazione di ciascun documento contenuto nel pacchetto.

Il file Indice del Pacchetto di Versamento (IPdV) è un file nel formato XML, che in conformità allo standard UNI SINCRO 11386:2010 assicura:

- L'identificazione del soggetto che ha prodotto il Pacchetto di Versamento;
- L'identificazione dell'applicativo che lo ha prodotto;
- La definizione della tipologia documentale (a cui appartengono i documenti inclusi nel pacchetto) ed eventuali messaggi del Responsabile del Servizio di Conservazione;
- La definizione dei documenti inclusi nel pacchetto, con le relative informazioni quali: nome file, hash calcolato, indici e relativi valori, messaggi del Responsabile del Servizio di Conservazione, ecc.

Il file Indice del Pacchetto di Versamento (IPdV) può essere eventualmente firmato digitalmente dal Produttore dei documenti. Di seguito la rappresentazione grafica del file XSD dell'Indice del Pacchetto di Versamento del sistema *LegalSolutionDOC*:

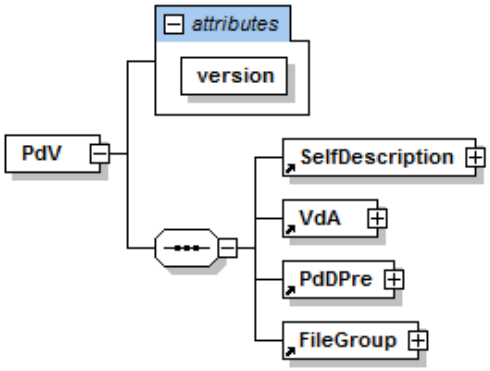


Figura 6 – Struttura dell'Indice IPdV suddiviso nelle componenti principali

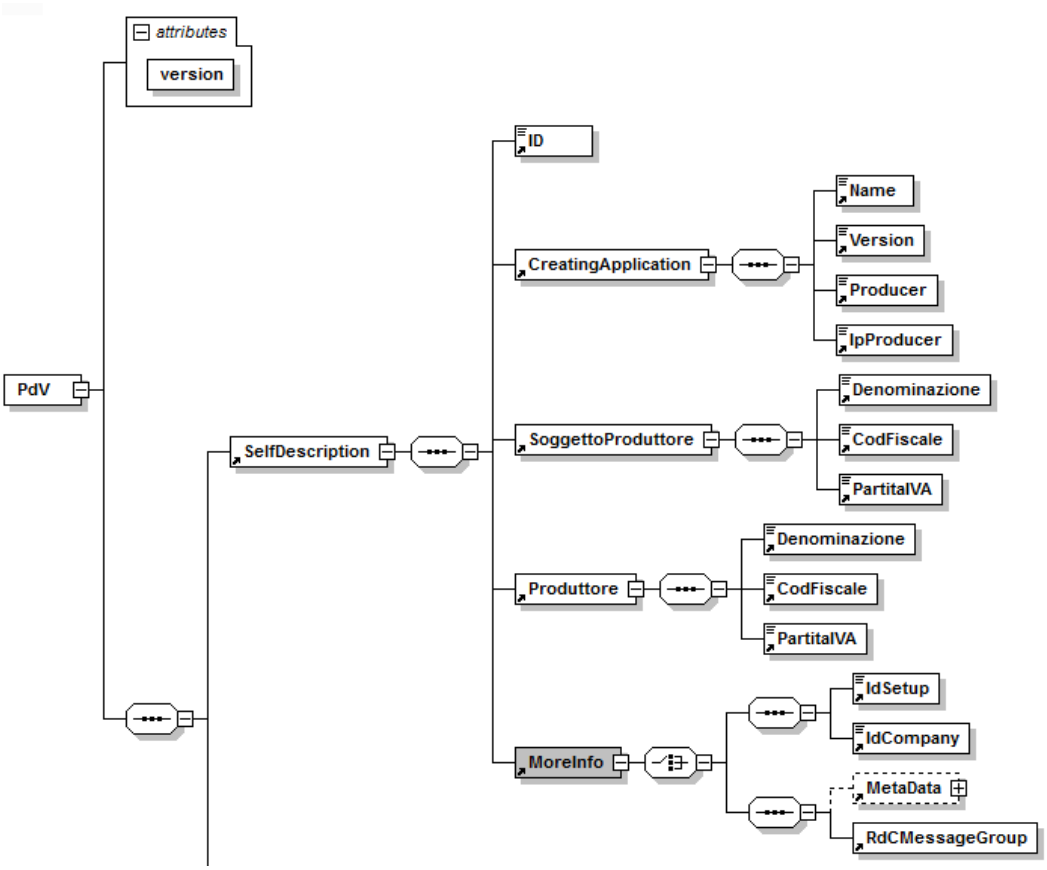


Figura 7 – Struttura Indice PdV sezione (SelfDescription)

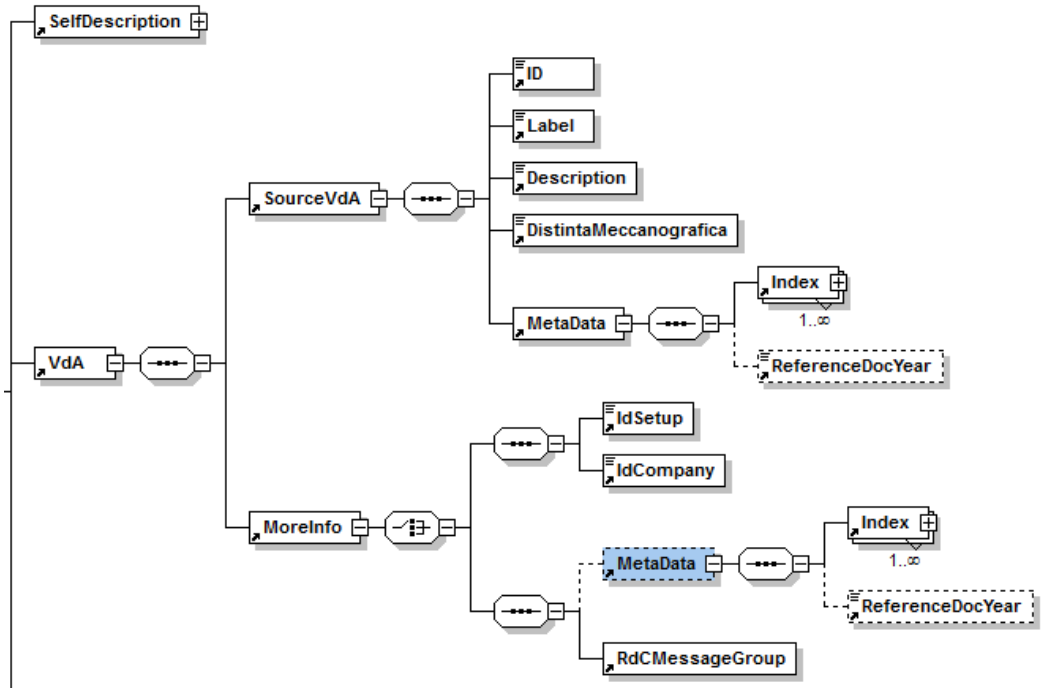


Figura 8 – Struttura Indice PdV (Sezione VdA)

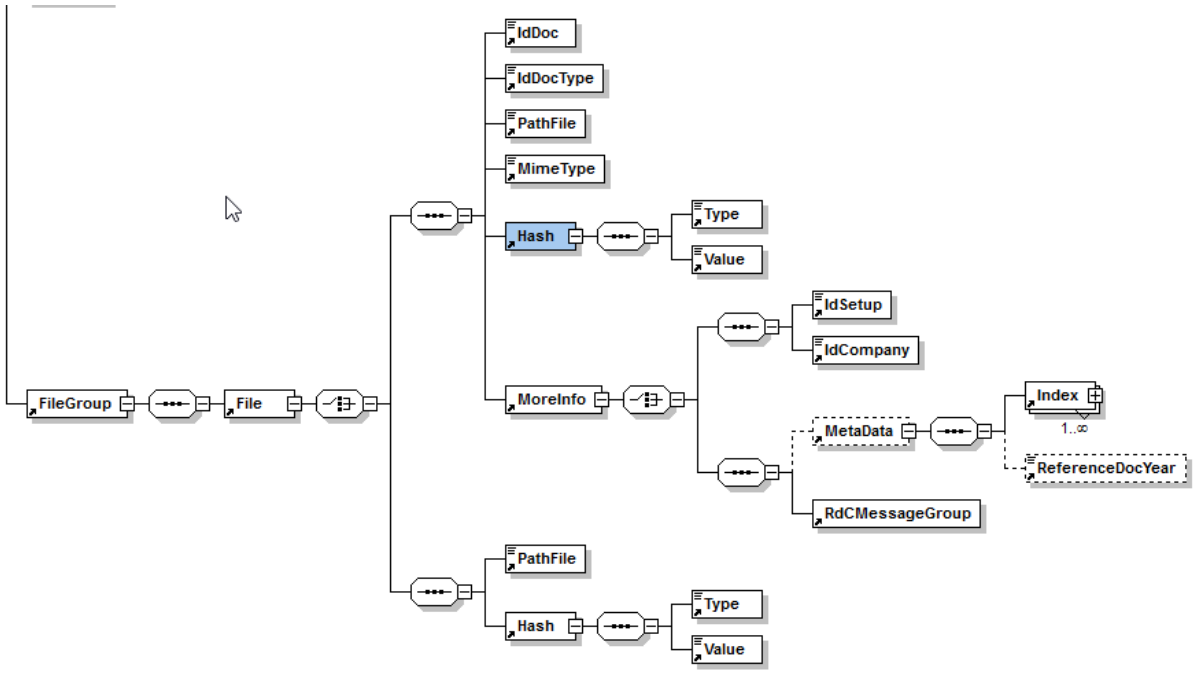


Figura 9 – Struttura Indice PdV (Sezione FileGroup)

Le eventuali personalizzazioni sul Pacchetto di Versamento e sulla sessione di versamento sono descritte e concordate tra le parti nel documento "Specificità del contratto".

Torna al sommario

6.3 Pacchetto di Archiviazione

Il Pacchetto di Archiviazione (PdA) generato nel processo di conservazione del sistema *LegalSolutionDOC* è una specializzazione del Pacchetto Informativo ed è composto dalla trasformazione di uno o più Pacchetti di Versamento secondo le modalità riportate nel presente manuale di conservazione.

Un Pacchetto di Archiviazione (PdA) è un contenitore informativo che contiene:

- Gli oggetti informativi individuati per la conservazione (quindi i documenti, i fascicoli elettronici o le aggregazioni documentali sottoposti al processo di conservazione a lungo termine);
- Un Indice del Pacchetto di Archiviazione (IPdA) che rappresenta le Informazioni sulla Conservazione.

In particolare, la struttura dati dell'IPdA del sistema *LegalSolutionDOC* fa riferimento allo standard nazionale SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

L'IPdA è l'evidenza informatica nel formato XML associata ad ogni PdA, contenente un insieme di informazioni descritte nelle regole tecniche in materia, in cui è riportata nel dettaglio la struttura dati prevista. Su ciascun IPdA viene apposta una marca temporale e la firma digitale del Responsabile del Servizio di Conservazione.

La struttura dati del PdA del sistema *LegalSolutionDOC* completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO.

- **SelfDescription** (1)*: Descrizione generale del pacchetto
  - **Id**: Identificativo univoco del PdA generato dal Sistema di conservazione (Id PdA generato dal data base)
  - **CreatingApplication** (1):
    - **Name**: Servizio di conservazione di eGlue
    - **Version**: Versione del sistema di conservazione
    - **Producer**: Proprietario del sistema di conservazione
  - **SourceIdC** (0-n)
    - **ID**: Id del pacchetto archiviazione (PdA) precedente
    - **Path**: Percorso relativo del IPdA (SInCRO) del pacchetto precedente
    - **Hash**: Valore restituito dalla funzione applicandola al file IPdA del pacchetto precedente, contiene l'attributo "function" che identifica la funzione di Hash utilizzata per il calcolo.
  - **Moreinfo (1)**
    - **EmbeddedMetadata**: Riferimenti dell'azienda a cui si riferisce il processo di Conservazione
      - **SoggettoProduttore**
        - **IdSetup**: Id Cliente nel sistema di conservazione
        - **IdAzienda**: Id azienda nel sistema di conservazione
        - **Denominazione**: Ragione Sociale dell'azienda
        - **CodFiscale**: Codice Fiscale dell'azienda
        - **PartitaIVA**: Partita IVA dell'azienda
      - **Produttori**
        - **Produttore**
          - **Denominazione**: Ragione Sociale eGlue
          - **CodFiscale**: Codice Fiscale eGlue
          - **PartitaIVA**: Partita IVA eGlue
          - **IdPdV_Versati**: lista dei pacchetti di versamento
            - **IdPdV**: Id del pacchetto di versamento
      - **VersionIPdA**: La versione dell'IPdA
- **VdC** (1):
  - **ID**: Identificativo univoco del PdA generato dal Sistema di conservazione (Id PdA generato da Data Base)
  - **MoreInfo** (1)
    - **EmbeddedMetadata**: Elenco dei PdV inclusi all'interno del PdA
      - **PdVGruppo**
        - **PdV**
          - **IdPdV**: Id del PdV restituito dal Sistema di conservazione al termine della presa in carico
          - **FunzioneHash**: Funzione di hash utilizzata per calcolare hash dell'IPdV
          - **Hash**: Valore restituito dalla funzione di hash applicata al file IPdV

- **RdCMessageGroup**: Eventuali comunicazioni tra il produttore, il Responsabile della Conservazione o il Responsabile del Servizio di Conservazione relative al PdV.

➢ **FileGroup (1-n):**
- **Label**: Nome della tipologia documentale
- **File**: Definizione del file comprensiva di codifica, estensione e formato (MimeType)
  - **ID**: Id del documento (univoco all'interno del Sistema di Conservazione))
  - **Path**: Indirizzo logico del file rappresentato da un URI (individua il file all'interno dello storage)
  - **Hash**: Funzione di hash utilizzata e valore restituito dalla funzione applicandola al file oggetto della Conservazione
  - **MoreInfo**:
    - **EmbeddedMetadata**
      - **File** (1)
        - **IdDoc**: Id del documento assegnato dal Produttore ed è univoco all'interno di una tipologia documentale per l'azienda.
        - **Indici** (1)
          - **Indice** (1-n)
            - **Nome**: Nome del campo indice (metadato)
            - **Valore**: Valore del campo indice (metadato)
        - **AnnoRiferimentoDoc**: Anno di riferimento per il documento
        - **Oggetto**: Il campo oggetto del documento viene calcolato in automatico dal sistema, in funzione alle regole definite in fase di versamento. Metadato funzionale a riassumere brevemente il documento e comunque a chiarirne la natura.
        - **RdCMessageGroup**: Eventuali comunicazioni tra il produttore ed il Responsabile del Servizio di Conservazione relative al file.

- **MoreInfo**
  - **EmbeddedMetadata**
    - **Tipologia** (1)
      - **IdTipologia**: Id della Tipologia documentale a cui appartiene il documento
      - **Indici** (1)
        - **Indice (1-n)**
          - **Numero**: Numero indice. Posizione del campo indice (metadato) all'interno della definizione della Tipologia
          - **Nome**: Nome del campo indice (metadato)
          - **Richiesto**: Indica se il valore dell'indice (metadato) è obbligatorio (Possibili valori: True, False)

- **RegEx**: Eventuale espressione di validazione per il valore dell'indice (metadato)
- **IndexType**: Tipo di dati del metadato (Possibili valori: stringa, intero, data)
- **IndexFormatString**: Formato del tipo di dato

➢ **Process (1)**

- **Agent** (1-n): Definizione dei soggetti che fanno parte del processo di Conservazione (vedere l'Allegato 4 delle Regole tecniche in materia di sistema di conservazione: Specifiche tecniche del Pacchetto di Archiviazione)
  - **AgentName**
    - **NameAndSurname** oppure FormalName.
      - **FirstName**: Nome soggetto
      - **LastName**: Cognome soggetto
      - **FormalName**: Denominazione o ragione sociale
    - **Agent_ID** (1-n): Id univoco del soggetto che interviene nel processo di produzione del pacchetto di Archiviazione (Cod. Fiscale o Partita IVA). Se il soggetto appone la firma, allora uno di questi campi riporta l'Id del certificato digitale del soggetto.
  - **MoreInfo** (0-n)
    - **EmbeddedMetadata**
      - **Soggetto** (1-n)
        - **Mansione**: La descrizione della mansione riferita al soggetto
- **TimeReference** (1)
  - **TimeInfo**: Data in cui è stata prodotto il file indice. Corrisponde entro certi limiti temporali (richiesti dal processo di firma e marca del file) alla data di rilascio della marca temporale.
- **LawAndRegulations**: Riferimento alla norma di riferimento: *Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*

* Il numero indicato tra parentesi precisa il numero di ricorrenze che l'elemento può assumere all'interno dell'IPdA: ad es. "(1)" specifica che l'elemento può ricorrere una sola vola; "(1-n)" specifica che può ricorrere 1 o più volte.

Torna al sommario

6.4 Pacchetto di Distribuzione

Un Pacchetto di Distribuzione (PdD) del sistema *LegalSolutionDOC* **a garanzia dell'interoperabilità e trasferibilità ad altri conservatori,** può essere richiesto dall'utente secondo le seguenti modalità:

- **PdD distribuito a seguito di ricerca di un singolo documento**, in risposta alla richiesta dell'Utente, il pacchetto contiene il file richiesto e il file indice SinCRO dell'intero PDA.
- **PdD distribuito a seguito di ricerca di più documenti, anche appartenenti a più PdA**, in risposta alla richiesta dell'Utente, il pacchetto contiene tutti i file richiesti e i relativi file SinCRO dell'intero PDA di tutti i pacchetti.

- **PdD distribuito in risposta alla richiesta cessazione del servizio**, in tal caso il PdD contiene uno o più PDA, suddivisi per tipologia documentale, anno Rif. Doc.

Il PdD è costituito da un contenitore compresso (ad esempio zip) che contiene i seguenti elementi:

- ✓ I **documenti** (oggetti digitali conservati nel sistema) richiesti dall'Utente.
- ✓ **Uno o più files IPdA** firmati digitalmente dal Responsabile del Servizio di Conservazione e marcati temporalmente associati ai predetti documenti richiesti dall'Utente.
- ✓ **File indice del PdD (IPdD)**: file XML ispirato allo standard UNI SINCRO 11386:2010 e firmato digitalmente dal Responsabile del Servizio di Conservazione, che contiene l'hash dell'IPdA, l'hash di ogni singolo file (documento richiesto o presente all'interno di un PdV richiesto), Super Impronta (se presente).
- ✓ La **Super Impronta** (opzionale, se presente) generata per il produttore (Azienda) a cui si riferiscono i documenti [ad esempio, presente per tutti i documenti con rilevanza tributaria oggetto di conservazione, propedeutica alla comunicazione dell'impronta dell'Archivio secondo il Provvedimento Attuativo Agenzia delle Entrate n. 2010/143663 del 25 ottobre 2010, abrogato con l'entrata in vigore del DM 17 Giugno 2014].

Per ogni PdD generato viene archiviato il file indice (IPdD) all'interno del Sistema di conservazione, per la tracciatura formale delle richieste di documenti da *LegalSolutionDOC*. Questo file indice contiene al suo interno:

- ✓ Id del PdD, generato in seguito al salvataggio su Data Base
- ✓ Data della generazione del PdD (in formato UTC)
- ✓ Azienda a cui si riferisce il PdD (Rag. Sociale, Id setup, Id azienda, Cod. Fiscale, Partita IVA)
- ✓ L'utente che ha richiesto il PdD (Nome, Cognome, Codice Fiscale e/o Partita IVA)
- ✓ Responsabile del Servizio di Conservazione (Nome, cognome, Cod. Fiscale e/o Partita IVA)
- ✓ Operatore conservazione delegato della conservazione.
- ✓ Responsabile del servizio di conservazione.
- ✓ L'indirizzo IP da cui è arrivata la richiesta di generazione
- ✓ PdA consegnati (Id PdA, Hash, Funzione di hash utilizzata, Uri file nel Sistema di conservazione e nel PdD)
- ✓ La lista dei file richiesti (Id documento, Id tipologia, Nome tipologia, Nome file, Hash file, Funzione di hash utilizzata, Uri file nel Sistema di conservazione e nel PdD).

Di seguito viene riportata la struttura dati del pacchetto di distribuzione, secondo lo standard SInCRO.

- **DescGenerale,** Informazioni del richiedente, del Responsabile del Servizio di Conservazione e del sistema di conservazione
  - **ID**, Id del documento estratto dal Sistema di conservazione
  - **IdSetup,** Il codice Cliente associato al produttore
  - **IdAzienda**, L'id dell'azienda di riferimento nel sistema documentale
  - **RagSociale**, La ragione sociale del produttore dei documenti

- **CodFiscale**, Il codice fiscale del produttore dei documenti
- **PartitaIVA,** La partita Iva del produttore dei documenti
- **DataGenerazione**, La data in formato UTC riferita alla produzione del PdD
- **Richiedente,** Dati anagrafici del richiedente
  - **Nome**, Il nome del richiedente
  - **Cognome**, Il cognome del richiedente
  - **CodiceFiscale**, Il codice fiscale del richiedente
  - **PartIVA,** La partita IVA del richiedente
- **Soggetti** La lista dei soggetti coinvolti nel processo di conservazione
- **Soggetto,** Dati anagrafici e ruolo del soggetto.
  - **Nome**, Nome del Soggetto
  - **Cognome**, Cognome del Soggetto
  - **RagSociale,** Denominazione del soggetto in caso di soggetto giuridico
  - **Ruolo,** Il ruolo svolto nel processo
  - **CodFiscale**, Codice Fiscale del Responsabile del Servizio di Conservazione
  - **PartIVA**, Partita IVA del Responsabile del Servizio di Conservazione
- **SdC,** Indicazioni anagrafiche del sistema di conservazione
  - **Nome**, Denominazione del sistema di conservazione
  - **Versione**, Versione del sistema di conservazione

- **PdAGruppo,** Descrizione del PdA estratto
  - **PdA,** descrizione del pacchetto di archiviazione
    - **Id**, Id del pacchetto di archiviazione (identificativo univoco del data base)
    - **FunzioneHash**, il tipo di algoritmo usato per calcolare l'hash
    - **Hash**, Il valore di hash ottenuto dal PdA
    - **UrlFile,** Percorso relativo dell'IPdA all'interno del pacchetto di distribuzione
    - **FileGruppo**, descrizione dei file estratti
      - **File**
        - **IdDoc,** id del documento nel sistema documentale o altro sistema
        - **PathFile,** Il nome file
        - **AnnoRiferimentoDoc**, anno di riferimento dell'oggetto conservato
        - **FunzioneHash**, il tipo di funzione di hash usata per calcolare il valore
        - **Hash**, Il valore hash del file considerato.
        - **UrlFile,** Percorso relativo del file all'interno del pacchetto di distribuzione

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nel documento "*Specificità del contratto*".

Torna al sommario

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione implementato dal sistema *LegalSolutionDOC* è governato in tutte le sue fasi dall'**entità di Amministrazione del sistema** che interagisce con le altre entità del Sistema, con eGlue e con gli Utenti e le eventuali Comunità di riferimento (Gruppi di Utenti) ed è governata dal **Responsabile del servizio di Conservazione** (ruolo ricoperto dal Conservatore eGlue S.r.l. ed espletato attraverso la struttura organizzativa descritta nel presente manuale).

Il Responsabile del servizio di Conservazione, in conformità ai compiti previsti dall'art. 7 del DPCM 3 Dicembre 2013, in virtù delle deleghe descritte nella struttura organizzativa, gestisce i servizi e le funzioni per l'operatività complessiva del sistema *LegalSolutionDOC.*
Nel seguito viene rappresentato il processo di conservazione implementato nel sistema di conservazione *LegalSolutionDOC* in conformità all'art. 8 del DPCM 3 Dicembre 2013.

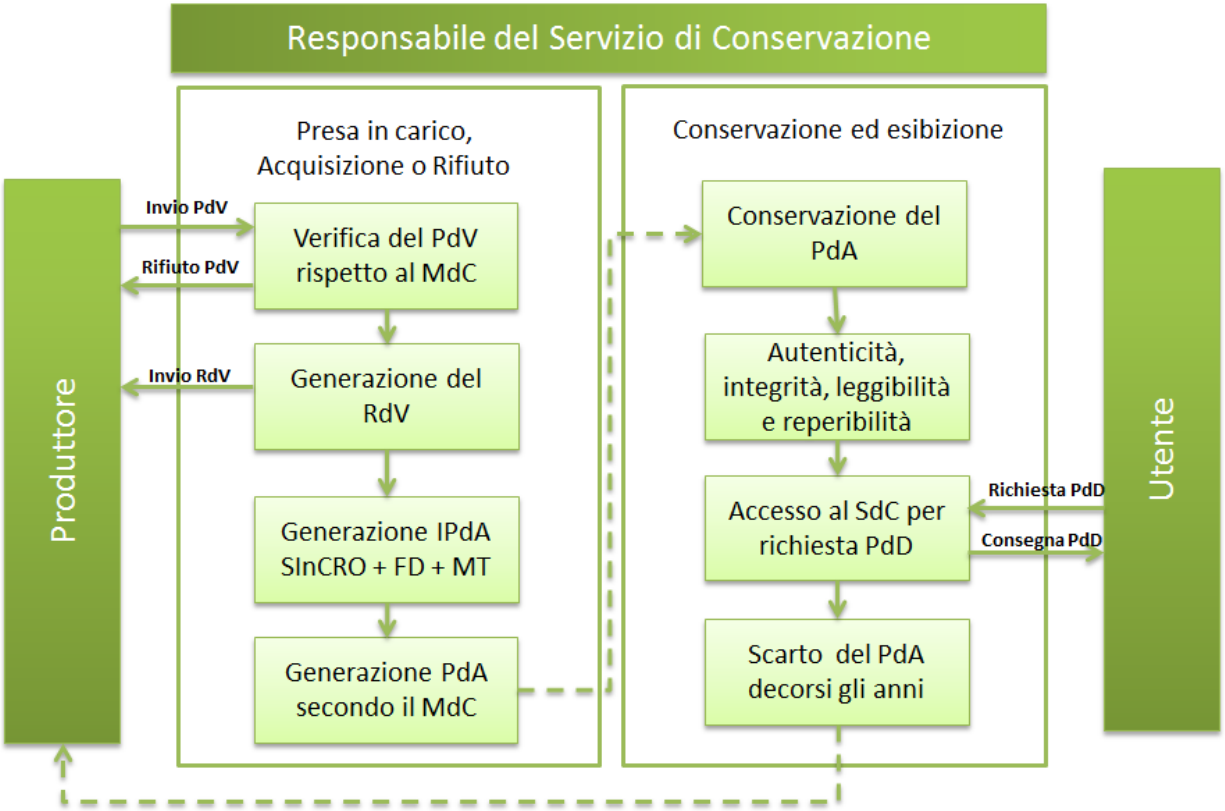


Figura 10 – Processo di conservazione in LegalSolutionDOC

Per ciascuna delle seguenti fasi del processo viene riportata nel seguito una descrizione esaustiva.

Torna al sommario

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Il sistema *LegalSolutionDOC* prevede le seguenti modalità di trasmissione dei PdV da parte dell'Ente Produttore verso l'Ente Conservatore:

- Tramite Web Services (processo sincrono)
- Tramite sFTP e successivo caricamento all'interno di *LegalSolutionDOC* (processo asincrono)

La presa in carico del PdV può avvenire in due modalità:

Sincrona
- Trasferimento via web services
- Check effettuati per il PdV in fase di presa in carico
- Risposta web services (esito presa in carico).

Asincrona
- Trasferimento PdV nella cartella dedicata SFTP
- Presa in carico da Job Schedulato
- Inserimento nel Sistema di conservazione
- Check effettuati per il PdV in fase di presa in carico
- Creazione del file "Esito di presa in carico".

Crittografia delle Informazioni trasmesse
Entrambe le modalità di versamento garantiscono la sicurezza e riservatezza dei dati trasmessi grazie alla crittografia del canale adottato (HTTPS o sFTP).
Il canale HTTPS integra sul protocollo base HTTP la crittografia di tipo Transport Layer Security (SSL/TLS), questa tecnica aumenta il livello di protezione contro gli attacchi. Il certificato digitale utilizzato per la connessione HTTPS è fornito e garantito da GlobalSign.
Il protocollo sFTP prevede il trasferimento dei dati usando il protocollo SSH-2 che garantisce la cifratura delle informazioni trasmesse.

Le specifiche ed il modello-dati adottati per il PdV sono i medesimi e la presa in carico per entrambe le modalità si conclude con il rilascio da parte del sistema *LegalSolutionDOC* di un file "Esito di presa in carico" contenente:

- Un identificativo Id (GUID) assegnato al PdV in caso di caricamento con esito positivo in modo da identificarlo in maniera univoca nel sistema di conservazione in tutto il ciclo di vita del servizio;
- Una Eccezione, se si sono verificati degli errori durante il caricamento.

In particolare, nella modalità sFTP l'esito restituito dalla presa in carico è un file testuale che viene depositato in una cartella di output predefinita.

I sistemi per la presa in carico dei pacchetti di versamento sono tutti in alta disponibilità e garantiscono la ridondanza dei dati.

Inoltre, nel sistema *LegalSolutionDOC* sono attive procedure per la generazione di backup dei PdV versati dal produttore. Le politiche di salvataggio e backup possono essere definite a livello di classe documentale, tale

impostazione consente di specificare quanto tempo la copia di sicurezza del PdV debba essere mantenuta nello storage dedicato ai PdV.

Lo storage che mantiene le copie di backup è costituito da 3 repliche, due sul sito primario e una sul sito DR: questa architettura garantisce l'alta affidabilità e il recupero a seguito di un disastro.
Pertanto, in caso di necessità, il recupero dei dati dei PdV ancora non trasformati in PdA dal sistema, avviene in accordo con il produttore, il quale può richiederlo attraverso un ticket di richiesta all'area di Assistenza. La richiesta smistata all'area tecnico-operativa di 2C Solution permette di attivare il "restore" delle copie dei PdV mantenute nell'area di storage dedicata, al fine di ricreare il processo di acquisizione dei PdV e quindi dare il via ad un nuovo processo di presa in carico.

Tutti le attività di presa in carico dei singoli PdV vengono tracciate tramite il sistema di Log Management integrato nel sistema di conservazione. I log vengono mantenuti per tutto il periodo di conservazione degli oggetti versati.
Periodicamente vengono effettuati i controlli di coerenza sui PdV che comprendono controlli di numerosità e altri controlli eventualmente necessari; tutte le attività di controllo vengono tracciate e mantenute sul SdC consentendo di generare report a cadenza impostabile che a loro volta possono essere conservati a sistema.

Ulteriori eventuali specifiche concordate tra Cliente e Conservatore eGlue in merito alla sessione di versamento, alla generazione e trasformazione dei PdV, al modello-dati del PdV e alla presa in carico del PdV, sono dettagliate nel documento di "Specificità del Contratto".

Torna al sommario

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Nel processo di presa in carico dei PdV nel sistema di conservazione, il sistema *LegalSolutionDOC* effettua una serie di controlli di coerenza su ciascun PdV e sugli oggetti in esso contenuti e genera un **esito di presa in carico**.

I controlli eseguiti dal Sistema sui PdV trasmessi sono i seguenti:
(**Bloccante**) Verifica che il pacchetto di versamento contenga l'IPdV ed i files (non viene effettuato dal metodo web services checkIndicePdV);
(**Bloccante**) Controllo validità del file IPdV con il file schema XSD;
(**Bloccante**) Controllo che il soggetto che ha formato ed è titolare dei documenti definito nell'IPdV sia presente e configurato nel Sistema di Conservazione e che per questo soggetto ci sia un soggetto Responsabile del Servizio di Conservazione configurato nel sistema;
(**Bloccante**) Controllo che il numero di files presenti nel PdV corrisponda al numero di files dichiarati nell'IPdV (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
Nel caso specifico della tipologia documentale distinta meccanografica il numero di files presenti nell'indice del pacchetto di versamento deve coincidere con il numero di documenti presenti nel singolo documento distinta contenuto nel PdV. Il sistema controlla che tutti i files indicizzati all'interno dell'IPdV, abbiano una corrispondenza con i documenti contenuti nella distinta;
(**Bloccante**) Controllo che i nomi dei files presenti nel PdV corrisponda ai files definiti nell'IPdV (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
(**Bloccante**) Controllo che il MimeType dei files definito nell'IPdV sia stato specificato;

(**Bloccante**) Verifica che i formati dei files contenuti nel PdV siano nei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013 e dalla tabella di seguito riportata

Tipo file	Tipo MIME	Codifica	Note
PDF, PDF/A	application/pdf, application/x-pdf, application/x-bzpdf, application/x-gzpdf	Binario	
TIFF	image/tiff, image/tiff-fx	Binario	
JPG-JPEG	image/jpeg	Binario	
TXT	text/plain	8 bit	
EML (Messaggio di Posta elettronica)	RFC 2822/MIME (text/plain, message/rfc822, multipart/alternative, text/html)	8 bit	
XML	application/xml, text/xml	8 bit	
ODT	application/vnd.oasis.opendocument.text	Binario	
FODT	application/vnd.oasis.opendocument.text	Binario	
DOCX	application/vnd.openxmlformats-officedocument.wordprocessingml.document	Binario	
ODS	application/vnd.oasis.opendocument.spreadsheet	Binario	
FODS	application/vnd.oasis.opendocument.spreadsheet	Binario	
XLSX	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Binario	
ODP	application/vnd.oasis.opendocument.presentation	Binario	
FODP	application/vnd.oasis.opendocument.presentation	Binario	
PPTX	application/vnd.openxmlformats-officedocument.presentationml.presentation	Binario	
ODG	application/vnd.oasis.opendocument.graphics	Binario	
FODG	application/vnd.oasis.opendocument.graphics	Binario	

(**Bloccante**) Verifica della presenza di files nell'IPdV con Id documento NON specificato;
(**Bloccante**) Verifica della presenza di files nell'IPdV con lo stesso Id documento;
(**Bloccante**) Se l'IPdV è firmato il sistema verifica che la firma sia valida, se non è firmato NON lo verifica (il predetto controllo non viene effettuato dal metodo web services checkIndicePdV).

Per ogni documento definito nell'IPdV si effettuano i seguenti controlli:
(**Bloccante**) Verifica che la tipologia definita per il documento corrisponda a quella definita per l'IPdV (campo: SourceVdA);
(**Bloccante**) Verifica che il numero di metadati definiti per il documento corrisponda a quelli definiti all'interno della tipologia configurata nel sistema di conservazione (definita nell'IPdV nella sezione SourceVdA);
(**Bloccante**) Verifica che il nome e l'ordine dei metadati definiti per il documento corrisponda a quanto definito all'interno della tipologia configurata nel sistema di conservazione (definita nell'IPdV nella sezione SourceVdA);
(**Bloccante**) Verifica della presenza del valore per i metadati obbligatori, seguendo lo schema dei metadati (inserito nel PdV nella sezione SourceVdA);
(**Bloccante**) Validazione del valore per i metadati in base all'eventuale espressione regolare definita, seguendo lo schema dei metadati (inserito nel PdV nella sezione SourceVdA);
(**Bloccante**) Verifica che non ci siano documenti con lo stesso Id documento, all'interno del Sistema di Conservazione, per la tipologia associata all'azienda;

(**Bloccante**) Verifica degli Hash dei file con il valore inserito nel PdV (Il predetto controllo non viene effettuato dal metodo web services checkIndicePdV);
(**Bloccante**) Verifica della validità della firma sul file (opzionale); il predetto controllo non viene effettuato dal metodo web services checkIndicePdV.
(**Bloccante**) Verifica dell'anno di riferimento documento: deve essere lo stesso per tutti i documenti (definito dell'IPdV nella sezione FileGroup/File/MoreInfo/MetaData/ReferenceDocYear)

Ulteriori personalizzazioni sui controlli eseguiti sono riportati nella "Specificità del Contratto".

Se le verifiche di coerenza eseguite nella fase di presa in carico sono positive il PdV viene preso in carico dal Sistema di Conservazione, altrimenti l'esito di presa in carico ne evidenzia il rifiuto definitivo.

Nella fase di verifica di coerenza del PdV, i risultati dei controlli elencati in precedenza vengono tutti registrati all'interno della funzionalità di LOG Management del Sistema con la registrazione di un time stamp (riferimento temporale). Periodicamente vengono effettuate verifiche sui log dei controlli effettuati e tali verifiche vengono annotate all'interno del SdC, dove periodicamente è possibile ricavare un report dei controlli effettuati.

Inoltre, l'esito di presa in carico generato dal sistema di conservazione *LegalSolutionDOC* contiene un riferimento temporale e, come meglio specificato nel paragrafo successivo, il Rapporto di Versamento (RdV) generato dal sistema contiene il Tag "<DataGenerazione>" ed è firmato digitalmente dal Responsabile del Servizio di Conservazione. Il riferimento temporale associato al Rapporto di Versamento rappresenta quindi un'informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC) che identifica la data di formazione del RdV.

Per quanto riguarda i riferimenti temporali si evidenzia che l'orologio di sistema di tutti gli elaboratori impiegati nel servizio di conservazione di documenti informatici sono sincronizzati con i segnali di tempo campione generati dall'Istituto Nazionale di Ricerca Metrologica (INRIM) in Torino (www.inrim.it). Questo permette al server di firma massiva di mantenere un tempo di sistema che si discosta dal tempo campione dell'istituto metrologico primario INRIM con un errore sicuramente inferiore al minuto.

Torna al sommario

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

In caso di presa in carico, il sistema di conservazione *LegalSolutionDOC* esegue, con una schedulazione periodica il cui timing è configurabile per ciascun Soggetto Produttore dei documenti, eventuali ulteriori controlli di continuità (se previsti nel documento Specificità del Contratto) e genera un rapporto, il **Rapporto di Versamento (RdV)**, quale esito di tutte le verifiche effettuate sul PdV dalla sua ricezione.

Il Rapporto di Versamento previsto dalle regole tecniche (DPCM 3 Dicembre 2013) ha lo scopo di formalizzare l'acquisizione degli oggetti da conservare inviati tramite un PdV dal Produttore dei documenti. Tale rapporto, come previsto dalla normativa, viene generato anche automaticamente dal sistema *LegalSolutionDOC* e può contenere uno o più pacchetti di versamento.

Il Rapporto di Versamento generato da *LegalSolutionDOC* viene firmato digitalmente dal Responsabile del Servizio di Conservazione. Alla firma, inoltre, è associato un riferimento temporale che identifica la data di formazione del documento informatico RdV. Il riferimento temporale e riferito al Tempo Universale Coordinato (UTC).

Per ogni Soggetto Produttore possono essere generati uno o più RdV per ogni schedulazione, in quanto:

- ogni RdV si riferisce ad una sola tipologia documentale;
- per ogni Produttore è possibile definire il numero massimo di PdV da includere all'interno di un rapporto RdV per evitare di includere un numero elevato di PdV per RdV.
- Il RdV è costituito da un file XML dove all'interno vengono riportate le seguenti informazioni:
- Indicazioni della versione del Sistema di Conservazione
- Indicazioni ed autenticazione del Produttore dei documenti in riferimento al sistema di Conservazione
- Riferimenti dell'utente che ha trasmesso il PdV
- Data di Generazione del RdV
- Riferimenti del Responsabile del Servizio di Conservazione associato al produttore dei documenti
- Riferimenti del Responsabile della conservazione
- Riferimento del Delegato Conservatore
- Numero di PdV inclusi nel RdV
- Numero totale dei files contenuti nei PdV inclusi all'interno del RdV
- La funzione di Hash con cui è stato generato l'hash del IPdV
- Hash del/i IPdV considerato/i nel RdV
- L'indirizzo IP della macchina dove è stato generato il PdV
- La lista dei messaggi del RdC contenuti nel/nei pacchetto/i di versamento collegato/i al file

L'esito dei check una volta ricevuto il PdV da parte del Sistema di conservazione.
Il rapporto di versamento, generato nel formato XML, viene firmato dal Responsabile del Servizio di Conservazione e conservato periodicamente nel sistema di conservazione *LegalSolutionDOC*.
Ulteriori eventuali specifiche sulla generazione del RdV ed il modello dati dello stesso sono dettagliate nella "Specificità del Contratto."

Il Rapporto di Versamento (RdV) generato secondo lo standard UNI SInCRO 11386:2010, che formalizza il buon esito del versamento dei pacchetti da parte del produttore dei documenti, una volta l'anno viene posto in conservazione a norma.

Periodicamente vengono effettuati dei controlli sui RdV generati e inviati, tali verifiche vengono annotate all'interno del SdC. Tali annotazioni vengono inoltre riportate sui report periodici prodotti ai fini dell'archiviazione.

Torna al sommario

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Durante le verifiche di coerenza possono essere riscontrate le seguenti anomalie che generano il rifiuto dei pacchetti di versamento:

- PdV non contiene l'IPdV ed i documenti;
- File IPdV non valido rispetto allo schema XSD;

- Identificazione del Produttore dei documenti e non corrispondenza nel sistema di conservazione;
- Assenza di un Responsabile del Servizio di Conservazione nel Sistema di conservazione per il produttore dei documenti a cui il PdV si riferisce;
- Numero di files presenti nel PdV non corrispondente al numero di files dichiarati nell'IPdV;
- Nomi dei files presenti nel PdV non corrispondenti ai nomi files definiti nell'IPdV;
- Verifica tipo MIME dichiarato nell'IPdV (MimeType tra quelli ammessi per la conservazione dei files);
- Verifica formati dichiarati nell'IPdV (formati tra quelli ammessi per la conservazione dei files);
- Presenza di files nell'IPdV con Id documento non specificato;
- Presenza di files nell'IPdV con lo stesso Id documento;
- Verifica della validità della firma digitale solo se il IPdV è firmato;
- Verifica che la tipologia documento nel sistema di conservazione corrisponda a quella definita per l'IPdV (campo: SourceVdA);
- Verifica che la tipologia documentale configurata nel Sistema di conservazione corrisponda a quella dichiarata nel'IPdV (campo: SourceVdA);
- Verifica che i metadati configurati per quella tipologia documentale nel sistema di conservazione corrispondano a quelli dichiarati nel'IPdV (campo: SourceVdA);
- Verifica che il nome e l'ordine dei metadati configurati per quella tipologia documentale nel sistema di conservazione corrispondano a quelli dichiarati nell'IPdV (campo: SourceVdA);
- Verifica della presenza dei metadati settati come obbligatori nell'IPdV (campo: SourceVdA);
- Verifica dell'eventuale espressione regolare dei metadati dichiarati nell'IPdV (campo: SourceVdA);
- Verifica che non ci siano documenti con lo stesso Id documento, all'interno del Sistema di Conservazione, per la medesima tipologia documentale associata ad un determinato produttore dei documenti;
- Verifica corrispondenza degli hash (impronte) dei documenti calcolati dall'ente conservatore con l'hash dichiarato nell'IPdV dall'ente produttore;
- Verifica della validità della firma sul singolo documento. Il controllo della verifica sui documenti firmati può essere opzionale ed attivabile solo sui documenti firmati.

Ulteriori controlli possono essere eseguiti in merito al rispetto della continuità della numerazione o all'ordinamento cronologico, eventualmente generando ulteriori anomalie riportate nel Rapporto di Versamento, ma ciò è concordato tra Soggetto Produttore e Conservatore nel documento "Specificità del Contratto".

Il sistema di conservazione, successivamente alla sua generazione, prevede la possibilità di inoltro al produttore dei documenti del RdV tramite e-mail o messa a disposizione via sFTP o tramite chiamata web service.
La modalità di consegna del RdV dal sistema di conservazione al produttore prevede la creazione di un pacchetto contenitore, contenente il file RdV firmato dal Responsabile del Servizio di Conservazione, il file RdV non firmato per una più agevole elaborazione del file da un eventuale sistema informativo ed un file XSLT per la semplice visualizzazione tramite browser.

É inoltre possibile richiedere il RdV direttamente accedendo dall'interfaccia web di consultazione in *LegalSolutionDOC* da parte di un utente autorizzato dal produttore dei documenti.
Periodicamente il Responsabile del Servizio di Conservazione conserva in conformità alla normativa vigente tutti i RdV generati, che rimangono sempre a disposizione per la consultazione ed esibizione. Si evidenzia che nel sistema di conservazione *LegalSolutionDOC* è prevista una procedura per permettere al Responsabile del Servizio di Conservazione, su esplicita richiesta del produttore, di annullare dei PdV già acquisiti solo se non

fanno parte di un processo di conservazione già completato (Pacchetto di Versamento già incluso in un PdA firmato e marcato).
L'annullamento dei PdV avviene tramite interfaccia Web attraverso una specifica funzionalità accessibile solo tramite il sistema di ticketing di 2C Solution.
Tali pacchetti, se annullati attraverso l'interfaccia web, resteranno comunque salvati e disponibili nel Sistema di conservazione ma nello stato annullato e quindi non potranno più essere selezionati per la successiva fase di generazione dell'IPdA.
L'operazione di annullamento dal processo di conservazione di un PdV viene comunicata al produttore dei documenti all'interno del successivo RdV per esso generato.
In conclusione, nel presente paragrafo e nel paragrafo 7.2 sono stati descritti i controlli eseguiti dal servizio *LegalSolutionDOC* sui PdV ricevuti in cui si è descritto che le anomalie rilevate sui PdV vengono tracciate negli esiti di presa in carico e nel rapporto di versamento (RdV).
La comunicazione al Produttore delle anomalie riscontrate dai predetti controlli avviene, pertanto, attraverso la consegna o messa a disposizione degli esiti di presa in carico e dei rapporti di versamento.
Il sistema di conservazione consente al Produttore di avere a disposizione gli esiti di presa in carico tramite dialogo applicativo web services o tramite sFTP nella cartella di destinazione "RX" definita tra le parti nel documento "Specificità del Contratto".

Si riporta un esempio di generazione del file *Esito di presa in carico (*estensione *.esito)* messo a disposizione del Produttore:

```
<?xml version="1.0" encoding="utf-8"?>
<EsitoPresaInCarico>
<NomeFile><![CDATA[Files.zip]]></NomeFile>
<DataVersamento>2014-09-11T07:58:01Z</DataVersamento>
<Id>000000001_2014</Id>
<IdPdV>54115609b84ac914886a905b</IdPdV>
<HashIPdV>B6D3163419584386155E39810111ED69BF8D7166FF38502A451371DB42DA0186</HashIPdV>
<FunzioneHashIPdV>SHA-256</FunzioneHashIPdV>
<CodFiscale>COD_FISCALE</CodFiscale>
<PartitaIVA>IT:PARTITA_IVA</PartitaIVA>
<Errori />
</EsitoPresaInCarico>
```

Gli elementi presenti nel file di esito hanno il seguente significato:

NomeFile: Nome file del pacchetto di versamento (Archivio Zip o Non Zip).
DataRicezione: Data e ora in cui è stato ricevuto il PdV.
Id: Progressivo (es.: Guid) generato dal Sistema Documentale, oppure dal sistema che ha prodotto il PdV. Viene inserito all'interno dell'IPdV da parte del produttore.
IdPdV: Id univoco del PdV assegnato dal Sistema di conservazione.
HashIPdV: Hash del file IPdV.
FunzioneHashIPdV: Funzione di hash con cui è stata calcolato l'hash dell'IPdV.
CodFiscale: Codice Fiscale del produttore ricavato dal PdV.
PartitaIVA: Partita Iva del produttore ricavata dal PdV.

Si riporta un esempio di possibili errori che possono essere riscontrati dai controlli del sistema di conservazione *LegalSolutionDOC*:

<Errori>
<Errore><![CDATA[Il file indice PdV contiene 1 files, mentre nel pacchetto sono presenti 2 files.]]></Errore>
<Errore><![CDATA[Il file NON è presente nel file indice PdV, ma è presente nel pacchetto. Nome file: 1.pdf]]></Errore>
</Errori>

La generazione e la consegna degli esiti di presa in carico sono tutte azioni registrate nel Log management System del sistema di conservazione *LegalSolutionDOC* con un riferimento temporale.

Il sistema 2C Solution consente ad eGlue di avere a disposizione i Rapporti di Versamento con le seguenti modalità:

- attraverso **comunicazione via PEC o mail ordinaria**, secondo l'indirizzo di posta elettronica configurato nel Sistema di conservazione *LegalSolutionDOC* nella anagrafica del Produttore (servizio configurato su richiesta del Cliente e concordato nel documento di Specificità del Contratto); la e-mail viene formattata in modo automatico dal Sistema e in allegato viene inserito il RdV firmato dal Responsabile del Servizio di Conservazione e il file non firmato (per una più agevole elaborazione del file da parte di un eventuale sistema di terze parti). Viene inoltre fornito un file XSLT per la visualizzazione agevole tramite browser;
- tramite **chiamata al webservice del sistema di conservazione**, secondo le modalità specificate nel documento *LegalSolutionDOC* SDK;
- tramite **accesso alla piattaforma web del Sistema di conservazione *LegalSolutionDOC*** da parte di un utente autorizzato.

Anche in questo caso tutte le azioni sono tracciate nel Log management System del sistema di conservazione *LegalSolutionDOC* con un riferimento temporale.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

La generazione dell'IPdA avviene secondo le specifiche dell'Allegato 4 del DPCM 3 Dicembre 2013 e secondo il modello dati definito dallo standard SInCRO – Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.
La generazione dell'IPdA corrisponde alla chiusura definitiva del processo di conservazione a norma. Questa procedura viene avviata nel sistema *LegalSolutionDOC* tramite un job configurato all'interno dell'entità funzionale schedulatore dei processi presente nel sistema, sulla base delle regole di conservazione configurate nel sistema per il produttore dei documenti.
Una volta generato l'IPdA viene apposto su di esso la firma digitale del Responsabile del Servizio di Conservazione ed una marca temporale, quindi i Pacchetti di Versamento inclusi nel PdA non potranno più essere modificati.
La firma digitale e la marca temporale sono emesse da Namirial S.p.A., rispettivamente in qualità di Certification Authority (CA) e di Time Stamping Authority, in conformità alla normativa vigente. Il sistema, anche nel caso della generazione dei PdA, registra i log per la tracciatura delle azioni effettuate sui pacchetti di archiviazione.

La procedura di ripristino in caso di corruzione o perdita dei dati dei PdA prevede la gestione dell'incident con livello di priorità massima ed il ripristino attraverso l'utilizzo del PdA copia di backup da parte del team preposto, secondo il piano operativo esposto nella documentazione sulla continuità operativa gestita per la certificazione ISO 27001:2013.
Eventuali casi specifici in cui è necessario adottare metodi di crittografia per proteggere i dati conservati nei PdA sono descritti nel documento "Specificità del contratto" che rappresenta l'accordo sulle condizioni di servizio specifiche tra Conservatore e Titolare (Soggetto Produttore).

Periodicamente vengono effettuati dei controlli sui PdA prodotti; tali verifiche vengono inserite come annotazione sul sistema di conservazione e riportati sui report che vengono mantenuti in archiviazione.

Torna al sommario

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

In risposta ad un ordinativo (richiesta dell'Utente) tramite l'interfaccia di ricerca documenti di *LegalSolutionDOC*, il sistema di conservazione fornisce all'Utente richiedente tutto o parte o una raccolta di Pacchetti di Archiviazione, sotto forma di Pacchetto di Distribuzione (PdD).

L'Utente può ricercare da interfaccia web, attraverso l'inserimento di apposite chiavi di ricerca, i documenti come output della ricerca, su cui poi richiedere la distribuzione del relativo PdD attraverso un pulsante "Genera Pacchetto di Distribuzione"; in alternativa un'utenza applicativa autorizzata può richiedere un PdD tramite chiamata web service. Il PdD distribuito dal sistema *LegalSolutionDOC* contiene tutte le evidenze di un singolo documento o quelle di un sottoinsieme di documenti conservati, a seconda della tipologia di PdD richiesta.

A fronte della richiesta di PdD da parte di un utente, il sistema restituisce tramite canale crittografato (protocollo HTTPS) il pacchetto PdD in formato di cartella compressa .zip al cui interno sono messi a disposizione tutti i file necessari. Le tipologie di Pacchetti di Distribuzione ed i modelli dati sono descritti nel paragrafo 6.4 del presente manuale.
L'utente può richiedere la generazione di più PdD e ogni azione di richiesta e messa a disposizione del PdD viene tracciata con un identificativo univoco all'interno del sistema di Log Management System di *LegalSolutionDOC*, con la registrazione di un riferimento temporale.
Lo storage che mantiene i Pacchetti di Archiviazione e dei Pacchetti di Distribuzione è costituito da tre repliche, due sul sito primario e una sul sito DR: questa architettura garantisce l'alta affidabilità e il recupero dei dati a seguito di corruzione o perdita dei dati.

Torna al sommario

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

L'utente autorizzato ad accedere al sistema di conservazione *LegalSolutionDOC* tramite le sue credenziali può eseguire le ricerche attraverso una interfaccia web e tramite l'ausilio di una serie di chiavi di ricerca (metadati) predefinite.

Una volta ottenuto l'output della ricerca, l'utente ha la possibilità di richiedere la distribuzione di un PdD o più semplicemente può eseguire la richiesta di download dei duplicati dei documenti informatici conservati, per singolo documento o per range di documenti.
La richiesta e l'ottenimento di un duplicato di un documento informatico conservato può essere avanzata anche attraverso chiamate web service da un utente autorizzato.
Inoltre, attraverso il sistema di ticketing aziendale e secondo quanto concordato nel documento "Specificità del Contratto", l'utente può inoltrare richiesta in merito alla necessità di ricevere duplicati. Il Conservatore eGlue potrà in tal caso mettere a disposizione tutti i duplicati richiesti dall'utente secondo la modalità concordata (ad esempio sFTP) in un pacchetto contenitore.

Vi sono casi in cui è necessaria la produzione di una copia informatica con attestazione di conformità da parte di un pubblico ufficiale:

- Per adeguare il formato del documento all'evoluzione tecnologica attivando un processo di riversamento sostitutivo a seguito dei controlli da parte del Responsabile del Servizio di Conservazione;
- Su esplicita richiesta dell'utente in quanto eventualmente concordato nel documento Specificità del Contratto.

Nel primo caso l'ownership dell'attività è in carico al Responsabile del Servizio di Conservazione che secondo un piano preventivo di controlli esegue le verifiche di integrità, di leggibilità e di adeguatezza della rappresentazione informatica dei documenti all'evoluzione tecnologica.
Il processo, completamente tracciato nei Log Management System e presidiato operativamente dall'Area di Assistenza Dematerializzazione e Sicurezza Digitale di 2C Solution, richiede la gestione di un riversamento sostitutivo, ovvero il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, modificando la loro rappresentazione informatica, garantendo il mantenimento dell'integrità del contenuto.
Proprio per la garanzia della conformità del contenuto nel passaggio da una rappresentazione informatica ad un'altra, più aggiornata tecnologicamente, è necessario nel processo l'intervento del pubblico ufficiale. La procedura prevede la messa a disposizione dei documenti originali e dei documenti copia al pubblico ufficiale, che una volta verificata l'immodificabilità del contenuto, appone la firma digitale su un file denominato "attestazione di conformità".
Questo documento viene posto in conservazione nel sistema *LegalSolutionDOC* come allegato integrativo (collegamento tramite hash tra i PdA) assieme al documento copia conforme e poi entrambi conservati. Tutte le evidenze dell'operazione eseguita vengono mantenute nel tempo dal Responsabile del Servizio di Conservazione.
Si evidenzia che la scelta di formati idonei, previsti e consigliati dalla normativa vigente (ad esempio il formato PDF/A) da parte del Responsabile del Servizio di Conservazione e del Titolare dei documenti è la scelta perseguita come prevenzione e minimizzazione dei rischi legati all'obsolescenza tecnologica.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Superato il periodo di conservazione di pacchetti e documenti concordato tra Conservatore eGlue e Cliente, il sistema *LegalSolutionDOC* deve implementare la procedura di scarto dei pacchetti di archiviazione.

Il sistema notifica (via mail/pec) al produttore con 30 gg di anticipo l'avvio della funzione di scarto per determinati PdA dandone quindi informativa secondo la normativa vigente e fornendo le informazioni necessarie al produttore per valutare l'eventuale richiesta di estensione del periodo di conservazione.
In caso di superamento della scadenza prefissata ed in assenza di richiesta di estensione, il job della procedura di scarto si attiva e produce dei Pacchetti di Scarto (PdS) in relazione ai PdA oggetto della procedura. L'operazione è tracciata nel sistema e viene prodotto un file Indice del Pacchetto di Scarto (IPdS) nel formato UNI SInCRO 11386:2010 firmato digitalmente dal Responsabile del Servizio di Conservazione che grazie al file XSLT può essere visualizzato dal Produttore dei documenti o altri soggetti interessati per la verifica della corretta procedura eseguita.
In ultimo, nel sistema *LegalSolutionDOC* viene registrato se la gestione della procedura di scarto è relativa ad archivi pubblici o privati che rivestono interesse storico particolarmente importante secondo (D.Lgs. 22 gennaio 2004, n.42); in questo caso si attiva un alert e la procedura di scarto del pacchetto di archiviazione avviene solo previa autorizzazione della Soprintendenza Archivistica del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia e secondo gli accordi definiti nel documento "Specificità del Contratto".

Torna al sommario

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

La principale struttura-dati a garanzia dell'interoperabilità è il Pacchetto di Archiviazione generato secondo le regole tecniche in materia di sistema di conservazione e secondo lo standard nazionale UNI SINCRO 11386:2010.
La sua distribuzione attraverso la richiesta di uno o più Pacchetti di Distribuzione (PdD) tramite diverse funzionalità e modalità (interfaccia web, web service, sFTP, ecc.) messe a disposizione dal sistema *LegalSolutionDOC* garantisce la corretta trasferibilità da parte del produttore ad altro conservatore.
Nel caso di riconsegna di tutti i PdA conservati (ad esempio per la chiusura del servizio o per la cessazione anticipata del servizio secondo quanto concordato contrattualmente), il Cliente potrà richiedere la loro distribuzione al sistema *LegalSolutionDOC*, selezionando la richiesta tramite dei filtri da interfaccia web e l'apposita funzionalità.
Ogni PdD contiene un Indice del PdD, generato secondo lo standard UNI SInCRO 11386:2010 e firmato dal Responsabile del Servizio di Conservazione, che rappresenta un rapporto (verbale) della distribuzione eseguita. Il PdD contiene anche il file XSLT per la corretta visualizzazione dell'IPdD.
Nel caso in cui il Cliente richieda una personalizzazione del servizio di distribuzione con l'esecuzione di attività aggiuntive per la migrazione o per l'interfacciamento diretto di eGlue/2C Solution con altri Conservatori ai fini della trasferibilità, le attività saranno eseguite da eGlue/2C Solution sulla base di quanto concordato nella "Specificità del Contratto" con il Cliente stesso.

Il sistema *LegalSolutionDOC* è in grado di acquisire pacchetti di versamento/pacchetti di archiviazione conformi con la struttura UNI SINCRO 11386:2010 nel caso di subentro su archivi gestiti da altro Conservatore che abbia adottato tale standard per la generazione dell'IPdA.

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE

Il servizio di conservazione della piattaforma eGlue Suite si basa su due processi distinti, integrati e sequenziali fra loro. Il primo prevede la ricezione del pacchetto cliente e la sua trasformazione nel pacchetto di versamento ed è eseguito da componenti applicative di eGlue, il secondo esegue il processo di conservazione ed è realizzato dal sistema di conservazione *LegalSolutionDOC* creato da 2C Solution.

Torna al sommario

8.1 Componenti Logiche

Dal punto di vista logico la piattaforma eGlue Suite è costituita da una serie di moduli funzionali orchestrati da un motore di workflow che viene configurato in modo personalizzato in funzione del processo di lavorazione da realizzare per ogni Cliente.

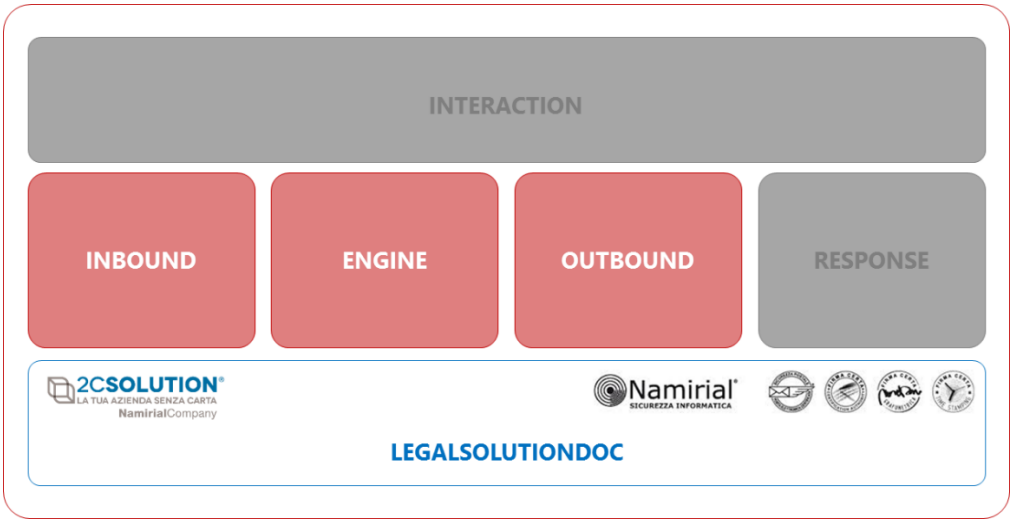


Figura 11 – Architettura funzionale "eGlue Suite"

Il modulo **Inbound** è l'interfaccia primaria verso cui il Cliente trasferisce i materiali da elaborare sulla piattaforma (pacchetto cliente). In questa fase è possibile eseguire i controlli di congruità predefiniti, le normalizzazioni ed eventuali arricchimenti previsti nelle specifiche del servizio. Eventuali errori intercettati in fase di elaborazione e determinati da non conformità dei materiali conferiti sono notificate tempestivamente al Cliente tramite e-mail o feedback applicativi di sistema e/o in alcuni casi direttamente dal Referente Operativo o suo delegato.

Il modulo di **Engine** racchiude l'insieme dei servizi di coordinamento dei processi (workflow) e della produzione informatica degli oggetti che compongono il pacchetto di versamento in ottemperanza alle specifiche previste nella Scheda Servizio. In questa fase vengono creati i documenti informatici a norma attraverso l'apposizione della firma digitale remota massiva, utilizzando certificati digitali emessi e custoditi su HSM dalla Certification Authority Namirial.

Il modulo di **Outbound** prevede la composizione del Pacchetto di Versamento arricchito con le informazioni di processo previste del canale di distribuzione da ingaggiare (sFTP / https) ed il suo instradamento ai gateway di destinazione. Ogni gateway ha una trasmissione controllata dei documenti che permette di gestire gli esiti

e gli eventuali errori di trasmissione, applicando regole specifiche condivise con il destinatario, nella fattispecie 2C Solution.

Il **sistema di conservazione *LegalSolutionDOC*** è una soluzione informatica sviluppata e mantenuta da 2C Solution per la conservazione a norma dei documenti informatici, conforme con le disposizioni tecniche del DPCM 03 Dicembre 2013.

L'infrastruttura di erogazione del servizio di conservazione dei documenti informatici *LegalSolutionDOC* è stata concepita, organizzata e sviluppata in modo che le varie fasi di lavoro risultino atomiche e che il flusso di lavoro sia modulare e scalabile, sfruttando tecnologie oggi conosciute come BigData, quindi utilizzando database NoSQL e Object Storage.
Le sue componenti logiche e tecnologiche descritte di seguito sono state installate e configurate in modo esclusivo per eGlue.

La piattaforma eGlue Suite è inclusa nell'ambito della certificazione ISO 27001:2013 conseguita da eGlue. Si rimanda alla documentazione tecnica del SGSI per la valutazione delle misure di sicurezza applicate in maniera preventiva e reattiva.

Torna al sommario

8.2 Componenti Tecnologiche

Nel complesso, il servizio di conservazione di eGlue può essere suddiviso in due insiemi di componenti tecnologiche: l'insieme delle componenti preposte alla trasformazione del Pacchetto Cliente nel Pacchetto di Versamento e l'insieme delle componenti del sistema di conservazione *LegalSolutionDOC*.

Lo schema delle componenti di eGlue è rappresentato nella figura seguente ed i principali elementi sono:

- *SFTP*, Il servizio di FTP che ha il compito di ricevere i Pacchetti Cliente da trasformare in Pacchetti di Versamento, processo asincrono
- *Workflow*, applicativo Windows Workflow Foundation per l'orchestrazione dei processi di elaborazione
- *Composition*, insieme di applicazioni dedicate alla formazione dei documenti oggetto di conservazione nei formati consentiti; ad esempio, per il processo di composizione documentale eGlue utilizza la piattaforma Inspire di Quadient
- *Servizio di Firma*, black box Namirial per la firma digitale
- *COS Service*, applicazione eGlue per la business logic e la validazione degli elementi destinati alla conservazione
- *Database*, tecnologia Microsoft SQL Server
- *Repository*, contenitore documentale per le varie fasi di lavorazione, tecnologia NetApp.

Tutte le componenti hardware sono in alta affidabilità e soggette a monitoraggio proattivo.

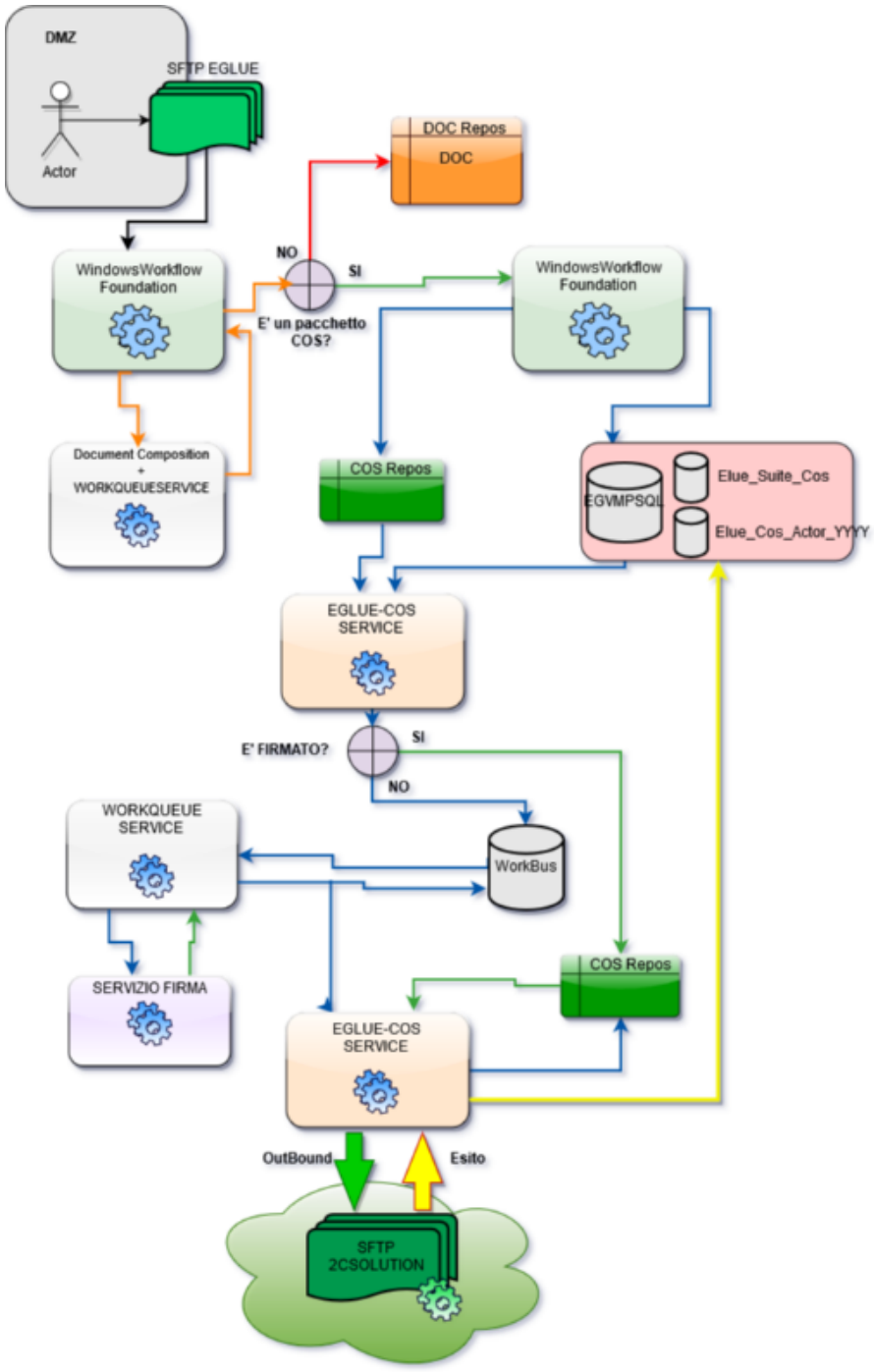


Figura 12 – Diagramma tecnologico del processo di alimentazione del Sistema di Conservazione

Le principali componenti del sistema di conservazione di documenti informatici *LegalSolutionDOC* possono essere schematizzate dalla seguente rappresentazione grafica.

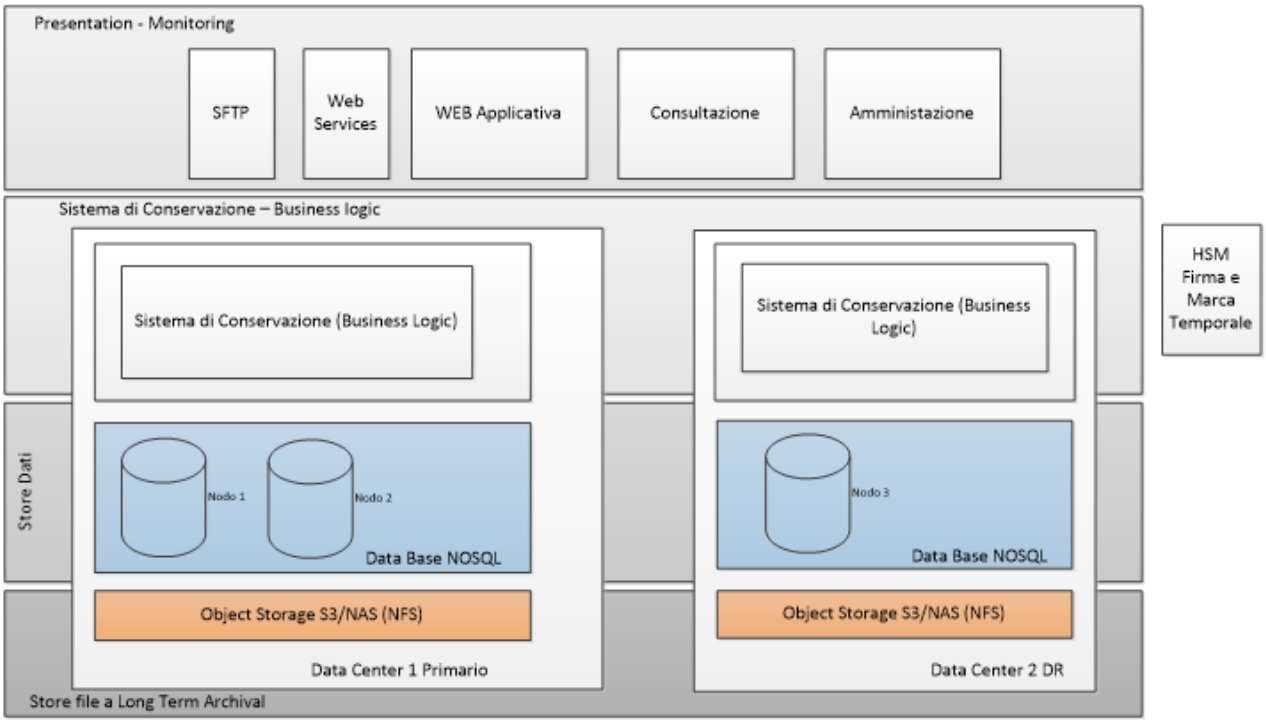


Figura 13 – Architettura del Sistema di Conservazione

Come rappresentato in figura la soluzione è basata su una struttura multi-tier e più livelli:

Presentation - Monitoring: la soluzione è stata progettata per garantire una veloce scalabilità, il livello presentation costituisce l'interfaccia dove i produttori e gli amministratori di sistema possono operare e gestire il sistema di conservazione, vediamo in dettaglio le singole componenti:

- *SFTP*, il servizio di FTP che ha il compito di ricevere i PdV da parte dei produttori, processo asincrono.
- *Web Services*, l'interfaccia web esposta su protocollo SOAP che consente ai produttori tramite l'integrazione con i loro sistemi di trasferire direttamente i PdV con processi sincroni. Il Web Services inoltre espone le funzionalità di ricerca dei documenti e le funzionalità di generazione dei PdD.
- *Web Applicativa/Consultazione/Amministrazione*, costituisce il client di gestione web del sistema di conservazione, in questa web application e possibile gestire la configurazione del sistema di conservazione, definizione dei soggetti produttori, configurazione dei soggetti per i processi di conservazione, definire le classi documentali e i rispettivi metadati, definire le policy di accesso o gli utenti che dovranno consultare i documenti.

Sistema di Conservazione - Business Logic: Lo strato di Business Logic integrata nel servizio di Conservazione, implementa tutti i processi del sistema di conservazione, dalla gestione di ogni singolo pacchetto (PdV, PdA, PdD) rapporti di versamento, i log del processo di conservazione, e l'interfaccia con il database e lo storage dei dati.

Store Dati: *LegalSolutionDOC* utilizza un data base NoSQL per lo storage dei dati, con una struttura a tre nodi replicati, due nodi sul sito primario e un terzo nodo sul sito DR. Tale struttura consente oltre a gestire una scalabilità orizzontale del sistema, una grande affidabilità e SLA di servizio molto alti. Ognuno dei tre nodi dati quindi è replicato a livello applicativo e tale replica garantisce sia la salvaguardia delle informazioni trattate sia la continuità operativa del servizio e la disponibilità dei documenti e dati, qualora uno tre nodi non dovesse essere operativo.

Store file e Long Term Archival: per lo storage dei file *LegalSolutionDOC* utilizza un sistema di storage basato su tecnologia Object Storage su tre nodi. Anche per la gestione dello storage dei file è utilizzata un'architettura a 3 nodi, 2 nodi dati sul primario e 1 nodo dati sul DR, al fine di garantire l'alta affidabilità e SLA nell'ordine del 99,99 sulla perdita delle informazioni. Il gruppo di server distribuiti, interconnessi tra loro, dove sono conservati gli oggetti digitali della conservazione è ubicato nel territorio nazionale.

Dalla struttura di erogazione del servizio (struttura primaria), è previsto un collegamento diretto, cifrato e privato, verso la struttura di Disaster Recovery. Tale struttura è logicamente suddivisa, come la struttura primaria.

Maggiori dettagli sulle componenti tecnologiche sono riportati nella documentazione del Sistema di Gestione della Sicurezza certificato ISO/IEC 27001:2013 di 2C Solution.

Torna al sommario

8.3 Componenti Fisiche

Il sistema di conservazione *LegalSolutionDOC* è installato ed eroga i servizi su data center ASCO TLC.

- **Sito Primario**, situato su datacenter di ASCO TLC a Santa Lucia (TV) con tutte le componenti necessarie in HA e collegato tramite connettività descritta sotto.
- **Sito Secondario DR,** su datacenter a San Vendemiano (TV) di ASCO TLC, gestito e amministrato tramite interfaccia VMWare da 2C SOLUTION, con le componenti necessarie per la ripartenza dei servizi in modo completamente automatico. Il data center è conforme ai principali standard di sicurezza internazionale ed in particolare implementa un sistema di gestione della sicurezza delle informazioni certificati ISO 27001.
- **Sito Ausiliario DR**, AWS Amazon gestito e amministrato tramite interfaccia di gestione Amazon, il data center è conforme ai principali standard di sicurezza internazionale ed in particolare implementa un sistema di gestione della sicurezza delle informazioni certificata ISO 27001.

L'architettura di rete che compone il sistema informativo di ASCO TLC è strutturata secondo lo schema "Network Fully Connected / Any to Any" completamente ridondato.

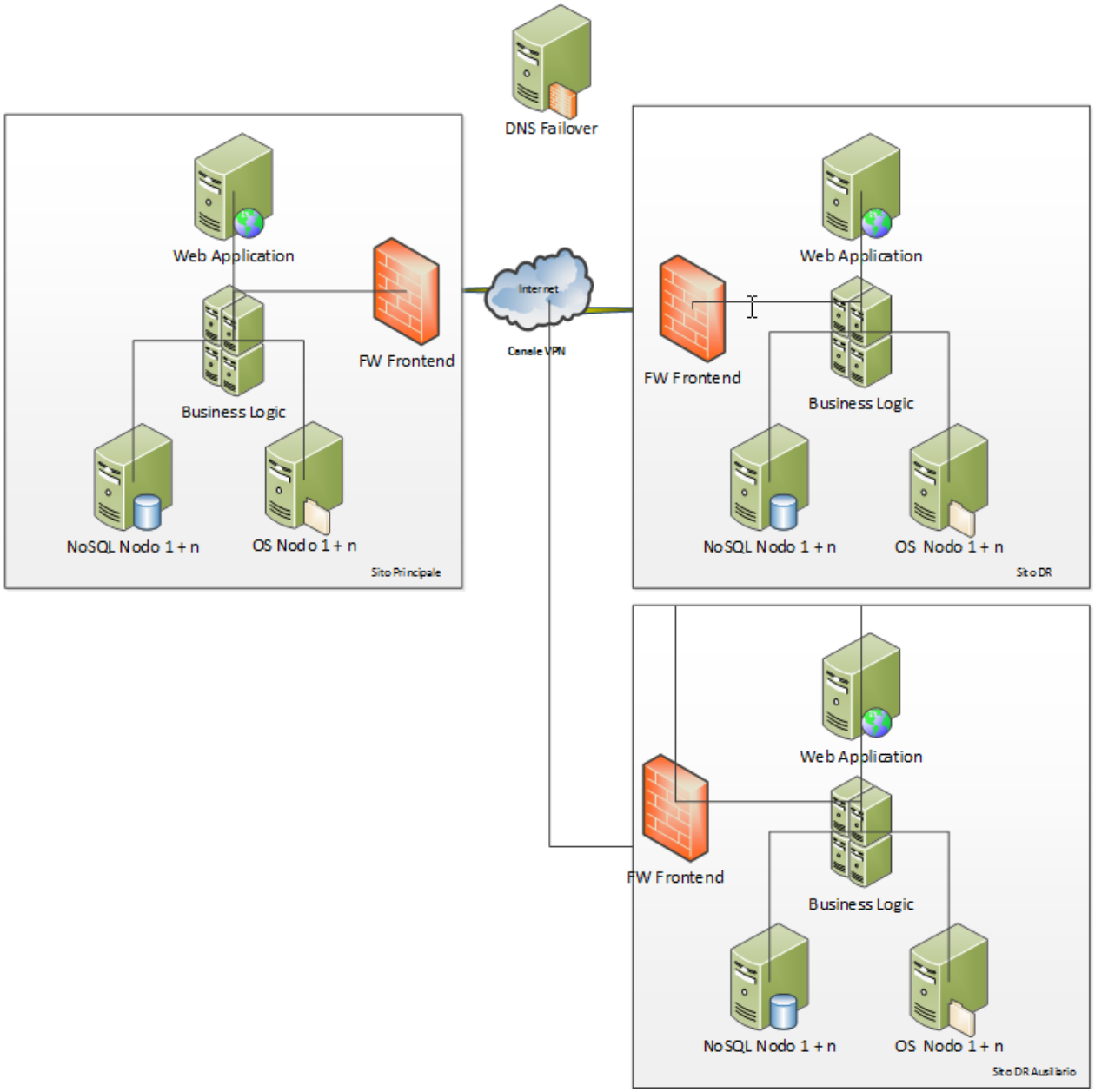


Figura 14 – Architettura Data center Primario e DR

La distanza dei siti elaborativi Santa Lucia (TV), San Vendemiano (Disaster Recovery) e i siti ausiliari EU-west-1 (Ireland) e EUcentral-1 (Francoforte) i quali erogano i servizi informatici di produzione per il business di 2C Solution, evidenzia quanto segue.

Distanza in linea d'aria:

- eGlue sito "Alpini" (Produzione) – 2C Solution (Outsourcer) -> 218 km
- 2C Solution (Outsourcer) – Santa Lucia (TV) (Conservazione) -> 70 Km
- Santa Lucia (TV) (Conservazione) – San Vendemiano (TV) (DR) -> 30 km
- Santa Lucia – EU-central-1/Francoforte (Ausiliario) -> 800 Km
- Santa Lucia – EU-west-1/Ireland (Ausiliario) -> 2.212 Km

Per gli approfondimenti ed il dettaglio in relazione alle componenti fisiche ed alla continuità operativa si rimanda alla documentazione relativa al sistema di gestione della sicurezza informatica, certificato ISO/IEC 27001:2013.

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Il conservatore eGlue, con il supporto e le opportune deleghe verso 2C Solution, ciascuno per la parte di propria competenza, ha provveduto ad istituire un sistema di governo e presidio del servizio con lo scopo di:

- garantire la riservatezza, l'integrità, la leggibilità, la reperibilità e la disponibilità dei documenti e dati nel sistema;
- formalizzare e garantire i requisiti del sistema in conformità alla normativa vigente;
- manutenzione del servizio;
- ottimizzare la gestione dell'incident management;
- valutare i livelli di rischio e di continuità operativa;
- monitorare i livelli di sicurezza;
- gestire operativamente le attività di sicurezza (incidenti, prevenzione frodi, gestione della comunicazione in emergenza, ecc.).

Conduzione e manutenzione del sistema di conservazione

I requisiti di sicurezza (sicurezza fisica, sicurezza logica e sicurezza organizzativa) adottati nella conduzione e manutenzione del sistema di conservazione, nelle politiche di gestione dell'incident management e della continuità operativa del servizio di conservazione sono specificati e riportati nel piano della sicurezza e nella documentazione del sistema di gestione della sicurezza.
2C Solution mantiene un registro cronologico delle componenti della piattaforma software *LegalSolutionDOC*, comprensivo di tutte le release, inoltre registra le diverse release di sistema operativo e di applicativi utilizzati nell'intero processo di conservazione nell'arco degli anni al fine di rendere comunque disponibili e fruibili nel tempo i documenti ed i dati relativi al servizio.
La procedura dei rilasci del software è una procedura che segue i requisiti imposti dalla certificazione ISO/IEC 27001:2013.

Per quanto riguarda l'organizzazione del supporto verso il cliente, eGlue ha definito con 2C Solution una struttura operativa di assistenza con competenze specifiche sia di processo che di prodotto:

- **Help Desk 1° Livello**, sono operatori dell'area di Service Operation di eGlue che ricevono il primo contatto da parte dell'Utente in caso di necessità attraverso il sistema di ticketing di eGlue, riescono a dare supporto su tematiche relative all'utilizzo della piattaforma, al processo, al servizio, ecc. Se il supporto non riesce a soddisfare la richiesta viene ingaggiato l'Help Desk di 2° Livello, attraverso lo strumento di ticketing SysAid che a seconda della catalogazione del ticket istanzia rispettivamente l'Area di Assistenza Dematerializzazione e Sicurezza Digitale, l'Area di Sviluppo software o l'Area di Produzione di 2C Solution;
- **Help Desk 2° Livello**, prende in carico la richiesta dall'Help Desk di primo livello e provvede alla gestione della problematica secondo la propria competenza ed eventualmente in team con altre competenze multidisciplinari.

Gestione e conservazione dei log

Il sistema di conservazione integra applicativamente la tracciatura tramite un sistema di log di tutte le chiamate/eventi sul sistema. I log sono conservati per dieci anni nel sistema di conservazione.
I dati tracciati sono:

- Livello LOG: indica il tipo di informazione tracciata, Debug, Warning, Info.
- Messaggio: informazioni descrittive dell'operazione eseguita.
- Note: i parametri applicativi inviati per l'operazione considerata
- Operazione: la descrizione dell'evento applicativo eseguito
- Utente: il nome dell'utente che ha richiesto l'operazione
- Indirizzo IP: l'eventuale indirizzo IP da dove proviene la richiesta
- Data Creazione: la data di creazione del Log.

Monitoraggio del sistema di conservazione

Il sistema di conservazione *LegalSolutionDOC* implementa numerosi sotto processi dediti al controllo e al monitoraggio del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al personale incaricato dal Responsabile del Servizio di Conservazione.
Tutte le componenti del sistema sono dotate di un proprio file di log nel quale sono tracciate tutte le operazioni eseguite dal componente e le altre informazioni che permettono di tenere traccia delle attività svolte e facilitare la diagnosi di eventuali anomalie e/o incident.
eGlue ha accesso ai log del sistema di conservazione tramite il pannello di controllo amministrativo del sistema di monitoring SysAid.
Il sistema di monitoring adottato SysAid è descritto più dettagliatamente nel Capitolo 9.1.

Change management

eGlue gestisce il processo di change management sul sistema di conservazione LegalSolutionDOC attraverso la piattaforma di ticketing SysAid. Le richieste di modifica sono istanziate dalla funzione Demand e Development di eGlue e vengono gestiti dall'Area di Assistenza Dematerializzazione e Sicurezza Digitale di 2C Solution.

Il processo viene avviato a fronte dell'aggiornamento e la condivisione di una nuova versione della "Specificità del Contratto".

Tale documento recepisce le specifiche di modifica sul servizio e solo se espressamente accettato e condiviso dal Cliente, permette di attivare la successiva fase implementativa del change (dall'analisi al collaudo e fino alla messa in produzione).
Il change management dell'infrastruttura di erogazione del servizio, invece, è gestito da 2C Solution secondo la proceduta definita dal proprio SGSI ISO/IEC 27001:2013.

Verifica periodica di conformità a normativa e standard di riferimento
Con periodicità almeno semestrale, il Responsabile del servizio di Conservazione di eGlue effettua un riesame generale del servizio insieme ai soggetti incaricati nell'organigramma per la conservazione, al fine di accertare la conformità del sistema al livello di servizio atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, ecc.).
Con periodicità almeno annuale, in accordo con le funzioni interne, il Responsabile del Servizio di Conservazione pianifica processi di audit che coinvolgono aspetti normativi, di processo, organizzazione, tecnologici e logistici, anche con l'intervento di consulenze specifiche.

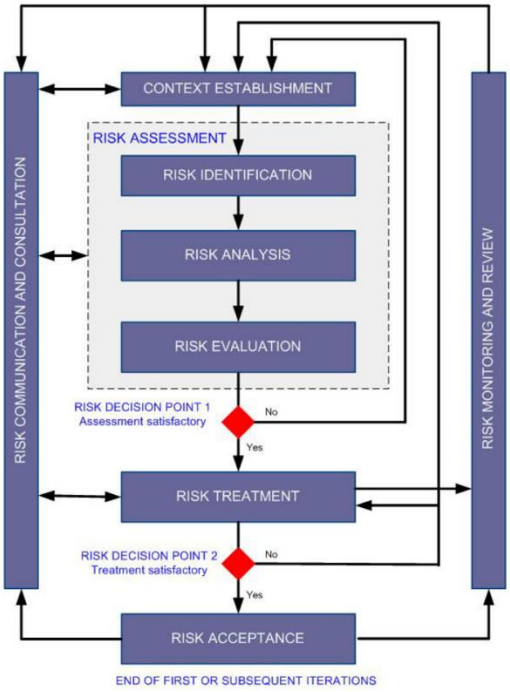
L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto con i produttori dei documenti, alla documentazione generale del servizio, ai principi che ispirano il sistema qualità e al presente manuale.
Periodicamente sono, inoltre, eseguite delle verifiche di audit sulle funzionalità del sistema di conservazione, principalmente su:

- Verifica funzionalità di creazione e mantenimento dei rapporti di versamento, dei pacchetti di archiviazione, ecc.
- Verifica funzionalità di distribuzione di pacchetti e documenti ai fini di esibizione e produzione delle copie;
- Mantenimento e disponibilità di un archivio del software dei programmi in gestione nelle eventuali diverse versioni, per permettere il ripristino;
- Verifica della corretta configurazione delle varie anagrafiche (produttore, responsabile della conservazione, altri soggetti, classi documentali, metadati, privilegi utenti, ecc.)
- Verifica del corretto funzionamento delle procedure di sicurezza utilizzate per garantire l'apposizione della firma digitale e della validazione temporale;
- Verifica sulla corretta predisposizione e mantenimento della documentazione relativa alla conservazione, anche a fronte di variazione delle condizioni di servizio o a eventi di cui si deve tenere traccia, quali adeguamenti normativi, evoluzioni tecnologiche, subentro di personale in attività previste dalla conservazione, evoluzioni tecnologiche e software, ecc.

Le attività di verifica sono svolte da eGlue e 2C Solution e sono riepilogate in un verbale di audit.

Gestione della sicurezza e valutazione del rischio

La gestione della sicurezza si basa in primo luogo sulla gestione dei rischi a cui sono sottoposti gli asset di eGlue. Il processo di gestione del rischio è basato interamente sui requisiti descritta nella ISO 27005:2013.



Identificazione del contesto

Il contesto del processo di risk management per la sicurezza delle informazioni coincide con l'ambito dell'information security policy. Questo processo è applicato a tutti gli aspetti critici come la valutazione del rischio per nuovi elementi come un nuovo servizio o infrastruttura, oppure nell'adozione di nuovi fornitori (ad es. fornitori in cloud).

Gli aspetti valutati sono:

- Sistemi sorgente: tutti quei sistemi che rappresentano la sorgente dei dati e delle informazioni che verranno direttamente o indirettamente trattate. Ad es. l'Active Directory è una sorgente per le identità degli utenti;
- Dati trattati: tutti i dati trattati devono essere classificati secondo la policy corrispondente del SGSI di eGlue;
- Componenti software: tutte le applicazioni o in generale software che prendono parte al trattamento dei dati o delle policy che li riguardano (ad es. permessi di accesso, proprietari etc)
- Componenti hardware: tutti i componenti hardware che entrano in gioco nel trattamento delle informazioni in maniera diretta o indiretta (ad es. server, workstation, storage etc)
- Servizi IT: tutti i servizi usati durante il trattamento dei dati ma che non ne fanno parte in maniera esclusiva (ad es. il servizio DNS, o la posta elettronica etc).

La nomenclatura degli asset e la classificazione dei dati deve essere conforme alle politiche del SGSI di eGlue.

Risk assessment
La parte di risk assessment si compone di tre sotto processi che sono:

- L'identificazione dei rischi
- L'analisi dei rischi
- La valutazione dei rischi.

Approvazione dell'assessment
La valutazione dell'assessment consiste in una approvazione da parte del CISO e del comitato di sicurezza. Il CISO deve approvare la valutazione della classe di rischio del contesto esaminato. Se il CISO approva la valutazione iniziale si può passare alla stesura del piano di trattamento del rischio, in caso contrario occorre correggere la valutazione integrando nuove informazioni al processo o al contesto.

Trattamento del rischio
La valutazione, o classificazione, ottenuta per ogni rischio individua anche il tipo di trattamento accettabile per quel tipo di rischio. Come descritto nella policy SGI_RM_Policy_Risk_Management è obbligatorio mitigare o evitare rischi critici o molto alti. I rischi bassi possono essere trascurati.

Approvazione del trattamento
I trattamenti individuati per i rischi elencati nel risk assessment devono essere approvati dal CISO e dal Comitato di Sicurezza. Nel caso in cui questi non siano approvati occorre analizzare nuovamente i rischi e valutare gli input forniti dal CISO. L'approvazione avviene in modo formale tramite report.

Accettazione del rischio residuo
La fase di accettazione del rischio è una formalità che spetta al CISO e al Comitato della Sicurezza. Questi organi devono accettare il rischio residuo che si ottiene valutando gli stessi rischi in fase di assessment ma tenendo conto delle misure di mitigazione implementate nella fase di trattamento.

2C Solution implementa tutte le misure di sicurezza volte a garantire la riservatezza, l'integrità e la disponibilità di dati e servizio di conservazione.
eGlue ha provveduto a sviluppare un set di controlli preventivi per misurare il livello di protezione del servizio di conservazione. I controlli vengono effettuati periodicamente sotto forma di audit per verificare il livello di protezione e garantire un monitoraggio degli eventuali piani di rimedio stabiliti con 2C Solution.

Si rimanda alla documentazione relativa al SGSI, certificato ISO/IEC 27001:2013 di eGlue per gli approfondimenti necessari.

Torna al sommario

9 MONITORAGGIO E CONTROLLI

La strategia adottata da eGlue in collaborazione con 2C Solution prevede che la pianificazione, la struttura organizzativa a supporto e gli strumenti di continuità operativa sviluppati comprendano tutte le misure funzionali, tecnologiche, organizzative e infrastrutturali necessarie per assicurare qualità, sicurezza e affidabilità ai servizi erogati per il cliente.

Per il raggiungimento di questo obiettivo sono essenziali le procedure e gli strumenti di monitoraggio e controllo descritti di seguito.

Torna al sommario

9.1 Procedure di monitoraggio

Il servizio di conservazione di documenti informatici *LegalSolutionDOC* viene costantemente controllato da un sistema di monitoring che rileva malfunzionamenti, anomalie ma anche situazioni critiche che rischiano di degenerare e causare problemi di funzionamento dei moduli che compongono l'intero sistema.

L'area organizzativa di Produzione e di Sviluppo Software di 2C Solution sono responsabili dell'infrastruttura e dei sistemi, pertanto effettuano il monitoring on-line e le attività di controllo delle componenti applicative e di impianto con cui vengono erogati i servizi, tramite gli indicatori e i controlli identificati sul Sistema di Gestione della Sicurezza delle Informazioni.

In particolare, 2C Solution effettua le attività di controllo avvalendosi della piattaforma **SySAid** sistema di asset management e ticketing, il quale al verificarsi di un evento anomalo legato alle risorse hardware o ai servizi applicativi crea ticket in automatico e li assegna al Responsabile dei sistemi informativi o altro operatore deputato, il quale entro un tempo prestabilito (SLA servizio) deve effettuare le opportune manutenzioni per chiudere l'anomalia, il sistema inoltre prevede delle policy di escalation verso i supervisori nel caso in cui il ticket non venga preso in carico nei tempi prefissati. Il ticket una volta lavorato viene chiuso dall'operatore inserendo le attività effettuate per chiudere l'incidente. Tutti i ticket gestiti rimangono storicizzati nel sistema e costituiscono la base per la creazione dei report di monitoraggio e controllo.

Oltre al sistema SysAid, 2C SOLUTION si è dotata di un software per il monitoraggio degli eventi di sicurezza e continuità operativa sui servizi essenziali del sistema di conservazione, tale software **QRadar** di IBM viene utilizzato dal SOC operato dalla società Yarix di Montebelluna che monitora 24h ore al giorno 365 gg anno il sistema a al verificarsi di eventuali eventi critici contatta il personale preposto di 2C Solution per mitigare eventuali problemi di sicurezza e continuità operativa.

Gli accordi tra eGlue e 2C Solution prevedono che con periodicità mensile venga generato un report dal SOC per consentire al titolare del servizio di poter monitorare la sicurezza della piattaforma dedicata ad eGlue e che tutti i parametri fondamentali risultino entro i valori stabiliti e concordati.

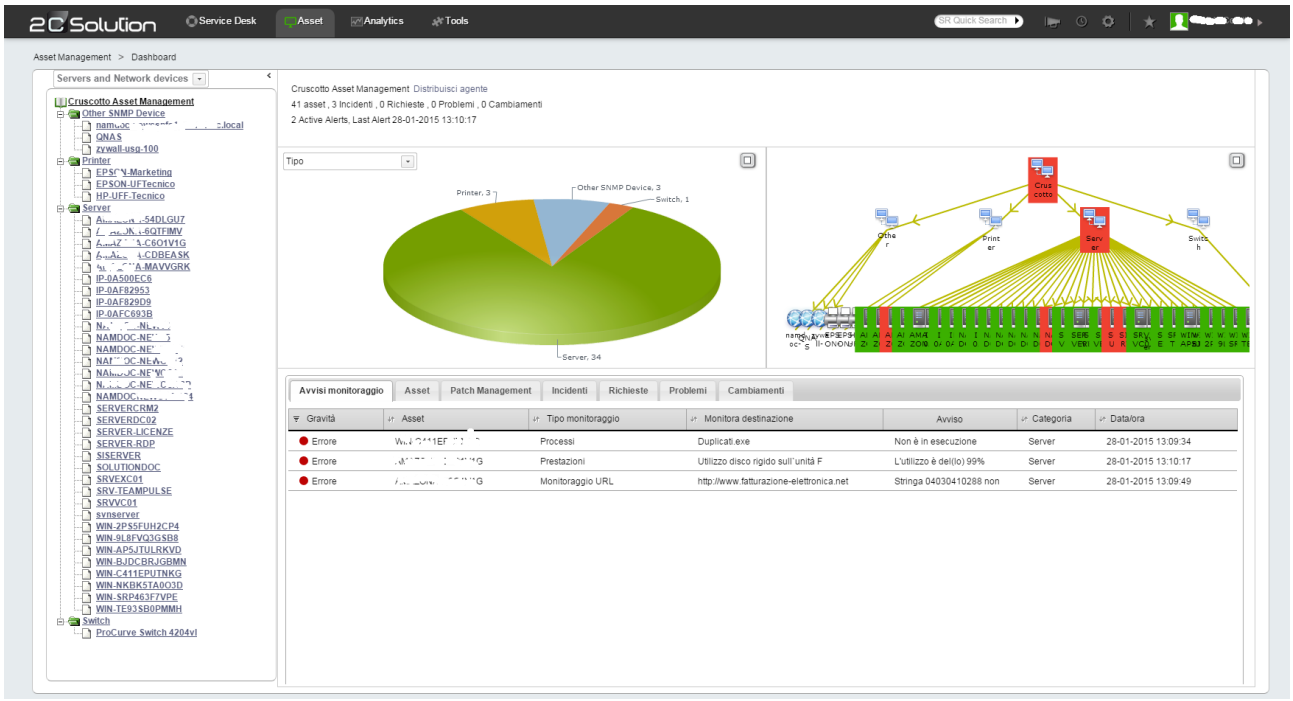


Figura 15 – Sistema di Asset Management SysAid Dashborad di controllo

Gli utenti del sistema di conservazione *LegalSolutionDOC* usano la stessa piattaforma per aprire i ticket per richiedere supporto all'help desk del servizio. Tali ticket riportano tutte le fasi di gestione del ticket:

- presa in carico della richiesta
- assegnazione
- tutti i messaggi scambiati con l'operatore
- la chiusura del ticket
- le attività effettuate
- il sistema inoltre tiene traccia delle date e ore di gestione.

Il sistema di monitoraggio mantiene i ticket salvati nel proprio data base almeno per dieci anni.

In particolare, attraverso il sistema di SysAid, vengono controllati costantemente:

- processi e web services
- la raggiungibilità del servizio da parte dell'utente
- processi di acquisizione documentali (PdV)
- servizio sFTP
- servizi di scheduling (es. processi generazione RdV, PdA, PdD, ecc.)
- servizi di supporto (es. antivirus, servizio di firma, servizio di time stamping)
- occupazione, latenza e performance storage
- processi, transazioni e performance DB
- log del sistema di gestione delle repliche del DB
- servizio di pubblicazione web
- log servizio di pubblicazione web

- log di sistema e funzionalità risorse
- log di procedura e consistenza
- servizio di rotazione legale dei log
- processi backup, replica geografica e DR
- funzionamento sistema di backup e DR
- funzionamento e performance HSM.

Il sistema di gestione degli asset e log management SysAid. rileva grazie all'installazione di un agent sulle macchine di produzione del servizio di conservazione i seguenti dati:

- accesso amministratori di sistema
- hardware e software installato sul server
- uso della CPU, RAM, SPAZIO disco monitorato con intervalli di 5 minuti.

Il sistema inoltre genera in automatico dei report inviati periodicamente al Responsabile dei sistemi informativi e al responsabile della sicurezza. Il dettaglio degli indicatori è riportato nella documentazione del SGSI ISO/IEC 27001:2013.

Ulteriori ed eventuali procedure aggiuntive di monitoraggio e controllo richieste dal Soggetto Produttore sono descritte nell'allegato documento "Specificità del contratto".

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il processo di verifica dell'integrità dei pacchetti informativi e dei documenti nell'ambito del servizio prevede:

- la verifica di corrispondenza sul numero documenti (verifica tra il numero di documenti effettivi presenti nel sistema di conservazione e il numero dei records presenti all'interno della struttura del DB per un determinato produttore);
- Il controllo dell'integrità degli strumenti di validazione apposti sui documenti e sugli Indici dei pacchetti (verifica della firma e della marca temporale su una percentuale prescelta rispetto al totale dei documenti ed indici XML (IPdA) presenti all'interno del sistema di conservazione per un determinato produttore dei documenti).

Per quanto riguarda la verifica di leggibilità, nel sistema di conservazione *LegalSolutionDOC* sono attivi degli automatismi che periodicamente effettuano una serie di controlli su base campionaria estratta tramite un algoritmo pseudocasuale considerando l'insieme degli Id presenti nell'insieme dei documenti conservati. Il campione prodotto da sottoporre a verifica è tale per cui nell'arco dei 5 anni sia garantita la verifica di un campione significativo che rappresenti la totalità dei documenti conservati per ciascun produttore. I controlli eseguiti su questi documenti sono i seguenti:

- verifica di integrità: attraverso il calcolo automatico dell'hash del documento e relativa comparazione con l'hash registrato in fase di creazione del PdA;
- verifica human-readable: sull'insieme dei documenti estratti per la verifica di integrità verrà ulteriormente creato un sottoinsieme di documenti nella percentuale del 1% visualizzati da un operatore delegato che verificherà se il documento è correttamente leggibile ad occhio umano.

A seguito di ogni operazione di controllo verrà prodotto un verbale di controllo firmato digitalmente dal Responsabile del servizio di Conservazione e conservato nel sistema di conservazione *LegalSolutionDOC*. Ulteriori ed eventuali procedure aggiuntive richieste dal Soggetto Produttore sono descritte nell'allegato Documento "Specificità del contratto".

Gli accordi tra eGlue e 2Csolution prevedono che il fornitore generi con cadenza periodica un report di integrità dei 5 anni.

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

eGlue gestisce le anomalie considerando il loro grado di gravità sull'erogazione e stato di salute dei servizi erogati ai propri clienti. Per tale motivo sono applicati due processi distinti a seconda della gravità della situazione che sono: incident management e disaster recovery.

9.3.1 Gestione degli incidenti

La figura seguente mostra il flusso del processo per la gestione degli incidenti.

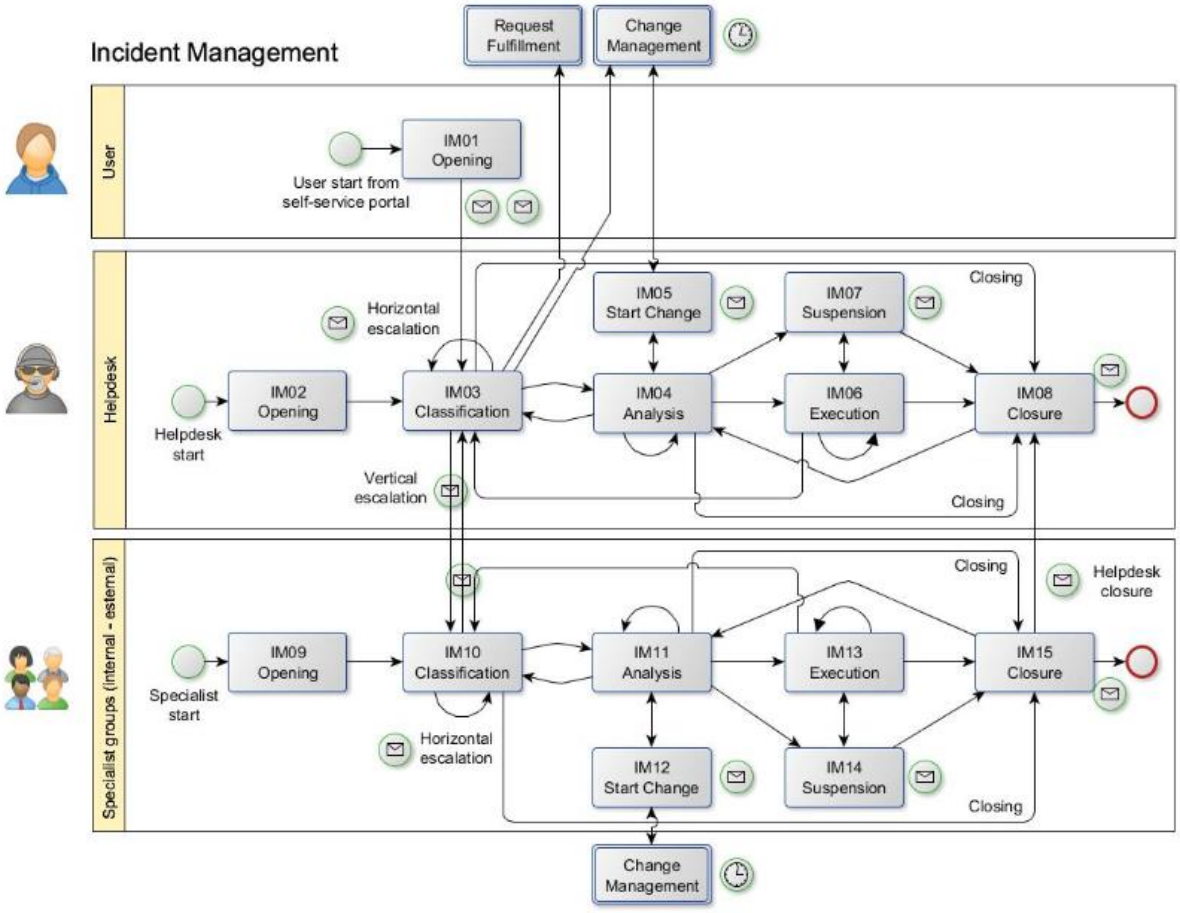


Figura 16 – Processo di incident management

Di seguito la descrizione delle fasi:

- IM01: l'utente apre un incident
- IM02: l'help desk apre un incident
- IM03: l'help desk classifica l'incidente
- IM04: l'help desk effettua una prima analisi dell'incidente
- IM05: l'help desk apre un change se l'analisi lo richiede
- IM06: (se possibile) l'help desk esegue una procedura per la risoluzione dell'incidente
- IM07: l'help desk sospende la risoluzione dell'incident se richiesto
- IM08: l'help desk chiude l'incident se considerato risolto
- IM09: il gruppo specialistico apre un ticket per un incident
- IM10: il gruppo specialistico classifica l'incident
- IM11: il gruppo specialistico analizza l'incident
- IM12: Il gruppo specialistico richiede un change per la risoluzione dell'incident
- IM13: il gruppo specialistico esegue una procedura per la risoluzione dell'incident
- IM14: IL gruppo specialistico sospende la risoluzione dell'incident
- IM15: il gruppo specialistico chiude l'incident

Le fasi di analisi svolte dai gruppi di supporto o di specialisti prevedono l'eventuale segnalazione al DPO di eGlue nel caso in cui si possa evidenziare un eventuale rischio di riservatezza dei dati.

Il workflow di Incident Management gestisce le richieste di supporto inoltrate dagli utenti a seguito di malfunzionamenti dei servizi IT. Le richieste vengono inviate dagli utenti tramite il sistema di ticketing, sono prese in carico dall'help desk e se necessario possono essere inoltrate agli specialisti interni o esterni (escalation orizzontale e verticale).

9.3.2 Gestione dei casi disastrosi

Il Piano di continuità operativa di eGlue prevede che il DR del servizio di conservazione si basi, dal punto di vista tecnologico, sulle soluzioni implementate da 2C Solution che ospita il sistema di conservazione.
Da un punto di vista della governance del DR, eGlue e 2C Solution hanno stabilito un protocollo di comunicazione da attivare nei casi in cui 2C dovesse attivare il piano di DR ed eseguire il ripristino dei servizi di conservazione.

Di seguito sono riportate le fasi del piano di disaster recovery:

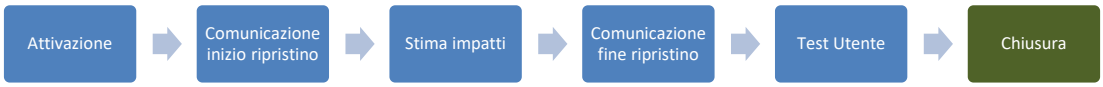


Figura 17 – Fasi del piano di disaster recovery di eGlue

Le fasi sono eseguite in questo ordine e con questi tempi:

- **Attivazione**
  - Scopo: gestione comunicazione verso 2C Solution
  - Responsabile: DR Manager
  - Durata: 1 ora

- **Comunicazione inizio ripristino**
  - Scopo: gestione della comunicazione verso i clienti e stakeholders
  - Responsabile: DR Manager
  - Durata: 1 ora
- **Stima**
  - Scopo: valutazione della stima degli impatti dall'indisponibilità del servizio rispetto agli SLA stabiliti con i clienti di eGlue
  - Responsabile: DR Manager
  - Durata: 4 ore
- **Comunicazione fine ripristino**
  - Scopo: gestione della comunicazione ricevuta da 2C Solution in merito alla chiusura della fase di ripristino
  - Responsabile: DR Manager
  - Durata: 1 giorno
- **Test eGlue**
  - Scopo: esecuzione dei test utente eGlue per verificare la corretta funzionalità dell'intero servizio di conservazione
  - Responsabile: DR Manager
  - Durata: 4 ore
- **Chiusura**
  - Scopo: raccolta dei log e comunicazioni a clienti e fornitori del livello di operatività raggiunto
  - Responsabile: DR manager
  - Durata: 4 ore

Questo piano viene, ovviamente, scatenato e sincronizzato con il piano di DR di 2C Solution per il servizio LegalSolutionDOC.

Al fine di mantenere l'allineamento dei rispettivi piani di ripristino, eGlue e 2C Solution hanno stabilito degli audit periodici del sistema di DR che include un report periodico inclusivo dello stato di performance del sistema di DR. Inoltre, eGlue opera un audit nel sito di 2C Solution al fine di verificare personalmente che i test di DR vengano effettuati periodicamente e con successo, e che tutte le componenti del sistema siano continuamente riviste e aggiornate.

Torna al sommario