

Manuale di Conservazione DigiDoc di Engineering Ingegneria Informatica

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	08/05/2018	Martinucci Valentina	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
	08/05/2018	Mancini Barbara	Responsabile funzione archivistica di conservazione
Verifica	09/05/2018	Nigro Cosimo	Responsabile servizio di conservazione
	09/05/2018	Cafiso Giuseppe	Responsabile Sicurezza dei sistemi per la conservazione
Approvazione	09/05/2018	Pizzonia Mario Carmelo	Responsabile ECM Competence Center

REGISTRO DELLE VERSIONI

N°Ver/Rev/ Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	09/06/2015	Prima versione	
1.1	03/07/2015	Modificato paragrafo 5.2 : inserita delega Marten Canavesio	
1.2	22/09/2015	Modifiche e integrazioni richieste da AgID in fase di accreditamento.	
1.3	8/01/2016	Eliminato il cap. 4 “Certification e time stamping authority” e adeguato al nuovo schema AgID	
1.4	19/05/2017	§ 5 modificate figure 2 e 3 relative alla strutture organizzative § 6.2 Modificati canali comunicazione	Non inviate in AGID in quanto prima dell’invio sono state rilevate delle osservazioni da parte di DNV

1.5	28/06/2017	§3.2 aggiornata standard di riferimento §§ 5.4, 8.3, 9.1 Adeguamenti per modifiche Organizzative precisando la distinzione tra le attività di responsabilità di Engineering Ingegneria Informatica S.p.A. e quelle in carico al fornitore Engineering.MO S.p.A. §8.3 aggiornata normativa di riferimento componenti fisiche	
1.6	19/07/2017	Recepita le indicazione di AgID in merito alla sostituzione del termine “Lotto” e “Volume di conservazione”	
1.7	21/08/2017	Recepita la variazione della denominazione Sociale di Engineering.mo SpA in Engineering D.HUB SpA	
1.8	08/05/2018	§1 Recepita l’incorporazione di Infogroup in Engineering Ingegneria Informatica Corretti i riferimenti alla norma 14721:2012	

INDICE DEL DOCUMENTO

1.	SCOPO E AMBITO DEL DOCUMENTO	6
2.	TERMINOLOGIA (GLOSSARIO E ACRONIMI).....	7
2.1	Acronimi	7
2.2	Glossario.....	8
3.	NORMATIVA E STANDARD DI RIFERIMENTO	18
3.1	Normativa di riferimento	18
3.2	Standard di riferimento	19
4.	RUOLI E RESPONSABILITA'	20
4.1	Il Responsabile del servizio di conservazione	22
4.1.1	<i>Dati anagrafici del Responsabile del servizio di Conservazione.....</i>	<i>24</i>
4.2	Formazione.....	24
4.3	Delegati del Responsabile del servizio di Conservazione	25
4.4	Coinvolgimento di altri pubblici ufficiali.....	25
5.	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE.....	27
5.1	Organigramma.....	27
5.2	Strutture organizzative.....	28
5.3	Focus sul Centro di Competenza ECM (Enterprise Content Management)	29
5.4	Focus sui servizi erogati da Engineering D.HUB	30
6.	OGGETTI SOTTOPOSTI A CONSERVAZIONE	31
6.1	Oggetti conservati	31
6.2	Pacchetto di versamento.....	31
6.3	Pacchetto di archiviazione.....	33
6.4	Pacchetto di Distribuzione	33
6.5	Formati	34
6.6	Metadati conservati	34
6.7	Tempi di conservazione.....	35
6.8	Peculiarità e gestione delle eccezioni.....	35
7.	IL PROCESSO DI CONSERVAZIONE.....	37
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	37
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti	39
7.2.1	<i>Controllo impronta del pacchetto di versamento.....</i>	<i>39</i>
7.2.2	<i>Controllo dell'identità del soggetto produttore del pacchetto.....</i>	<i>39</i>
7.2.3	<i>Controllo delle Firme Digitali.....</i>	<i>40</i>
7.2.4	<i>Controllo dei Formati digitali</i>	<i>41</i>
7.2.5	<i>Controllo della Presenza di Macro e Codice Eseguitibile</i>	<i>43</i>

7.2.6	Controllo dei Metadati	44
7.2.7	Controllo Impronta.....	45
7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico ..	45
7.3.1	Rinnovo marche temporali in scadenza	45
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	46
7.5	Preparazione e gestione del pacchetto di archiviazione	46
7.5.1	Creazione Indice di Conservazione	47
7.6	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.....	48
7.6.1	Funzionalità di ricerca	48
7.6.2	Funzionalità di esibizione	50
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	53
7.8	Scarto dei pacchetti di archiviazione	54
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	55
7.10	Riversamento diretto e sostitutivo.....	55
7.10.1	Riversamento diretto	55
7.10.2	Riversamento sostitutivo.....	55
8.	IL SISTEMA DI CONSERVAZIONE	57
8.1	Componenti Logiche.....	57
8.2	Componenti Tecnologiche.....	57
8.2.1	Software di base.....	57
8.2.2	Framework di sviluppo utilizzati.....	58
8.2.3	Scalabilità.....	58
8.3	Componenti Fisiche	60
8.4	Procedure di gestione e di evoluzione	62
9.	MONITORAGGIO E CONTROLLI.....	71
9.1	Procedure di monitoraggio.....	71
9.2	Verifica di integrità degli archivi	72
9.3	Soluzioni adottate in caso di anomalie.....	73

INDICE DELLE FIGURE

Figura 1 – Strutture Organizzative	27
Figura 2 – Strutture Organizzative Servizio di Conservazione	28
Figura 3 – Relazioni tra Responsabile della conservazione e strutture Organizzative	28
Figura 4 – Versamento del documento nel sistema di conservazione	38
Figura 5 - Visualizzazione documento	50
Figura 6 - Configurazione del sistema con un 1° livello di scalabilità	59
Figura 7 - Configurazione del sistema con un 2° livello di scalabilità	59
Figura 8 - Configurazione ambienti di collaudo e produzione.....	60
Figura 9: Organizzazione dell'Operation Center	72

1. SCOPO E AMBITO DEL DOCUMENTO

Engineering Ingegneria Informatica dispone di due differenti servizi di Conservazione Digitale, uno denominato DigiDoc e l'altro denominato DigiBox (sistema ereditato dall'incorporazione di Infogroup); il presente documento costituisce il manuale di conservazione di DigiDoc adottato da Engineering Ingegneria Informatica S.p.A., nel seguito indicato come Eng, per il processo di conservazione della documentazione digitale ai sensi della vigente normativa in materia elencata nell'apposito capitolo del presente documento.

Il manuale comprende tutte le informazioni previste dall'Agenzia per l'Italia Digitale per quanto concerne le tipologie documentali oggetto di conservazione presso Eng: all'ampliarsi e/o al variare di tali tipologie il manuale verrà aggiornato per recepire tutte le informazioni aggiornate relative al trattamento delle tipologie oggetto di conservazione.

Si precisa che alcuni argomenti che riguardano aspetti delle specifiche forniture del servizio di conservazione non saranno inseriti nel presente manuale, ma saranno sviluppati nel documento "Specificità del contratto" / "Proposta tecnica" in coerenza e/o facendo riferimento alla documentazione contrattuale prevista dal contratto di servizio stipulato da Eng con la propria clientela.

[Torna al sommario](#)

2. TERMINOLOGIA (GLOSSARIO E ACRONIMI)

2.1 Acronimi

Acronimo	Definizione
ACL	Access Control List
AIP	Archival Information Package (ex OAIS), ovvero il pacchetto di archiviazione ex DPCM 3 Dicembre 2013
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale, ovvero D.lgs 7 marzo 2005, n.82 e successive modificazioni e integrazioni
CAdES	CMS (Cryptographic Message Syntax) Advanced Electronic Signatures
CNS	Carta Nazionale dei Servizi provvista almeno del certificato di autenticazione (recante il codice fiscale del titolare)
DB	Database
DIP	Dissemination Information Package (ex OAIS), ovvero il pacchetto di distribuzione DPCM 3 Dicembre 2013
DPCM	Decreto del Presidente del Consiglio dei Ministri
DigiDoc	È il sistema utilizzato da Eng per erogare il servizio di Conservazione
GUI	Graphical User Interface
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
HSM	Hardware Security Module
ORM	Object-relation Mapping
OAIS	Open Archival Information System, standard ISO 14721:2012
PAdES	PDF Advanced Electronic Signatures
PEC	Posta Elettronica Certificata
PdV	Pacchetto di Versamento
RdV	Rapporto di Versamento
PdA	Pacchetto di Archiviazione
IdC	Indice di Conservazione

Responsabile della conservazione	E' il soggetto responsabile dell'insieme delle attività elencate dall'art. 7 comma 1 delle Regole tecniche. Viene designato dal Titolare all'interno della propria struttura organizzativa nelle pubbliche amministrazioni deve essere ricoperto obbligatoriamente da un dirigente o funzionario formalmente designato (art. 7 comma 3 delle Regole tecniche).
Responsabile del servizio di conservazione	E' la persona designata da Eng a gestire il sistema di conservazione affidato in outsourcing alla società dal Titolare dei documenti informatici. L'attività del responsabile consiste nel gestire ed erogare il servizio di conservazione come definito nell'accordo di servizio e nel presente Manuale di Conservazione utilizzando strumenti e metodi aggiornati tecnicamente e conformi alla normativa vigente.
SdI	Sistema di Interscambio (per le fatture elettroniche destinate alle pubbliche amministrazioni)
SIP	Submission Information Package (ex OAIS), ovvero il pacchetto di versamento DPCM 3 Dicembre 2013
Soggetto Produttore	Il titolare dei documenti. E' il soggetto o l'ente che produce i documenti che vengono affidati al soggetto al quale è affidato il processo di Conservazione
SSO	Single Sign On
TSA	TimeStamping Authority
UI	User Interface
UO	Unità organizzativa (cfr glossario)
URI	Uniform Resource Identifier
XAdES	XML Advanced Electronic Signatures

[Torna al sommario](#)

2.2 Glossario

Obiettivo di questo glossario è quello di definire il significato con il quale alcuni termini “chiave” ricorrenti saranno utilizzati all'interno del presente documento. Le definizioni, nel rispetto della terminologia tecnica di riferimento e delle prescrizioni normative, sono quelle effettivamente utilizzate all'interno del sistema di conservazione.

Termine	Definizione
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

Termine	Definizione
	conservazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
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
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
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del Testo Unico
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
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 registrati e correlati tra loro
CAD	Decreto legislativo 7 Marzo 2005, n. 82 e successive modificazioni e integrazioni
CADES	CMS Advanced Electronic Signatures – Formato di firma che può essere apposto su qualsiasi tipo di file. Genera una busta genera una busta crittografica contenente il file originale. Si presenta come un file la cui estensione è p7m

Termine	Definizione
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto dall'AgID il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Certificato di firma	Certificato destinato alla generazione delle firme apposte ai documenti digitali.
Certificato di marcatura temporale	Certificato destinato alla generazione di marche temporali.
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'AgID, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Conservazione	Insieme delle attività finalizzate a definire ad attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Coordinatore della gestione documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50, comma 4 del Testo Unico nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
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'articolo 12 delle Regole tecniche per il sistema di conservazione
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
DOI	Digital Object Identifier
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Esibizione	Operazione che consente di visualizzare un

Termine	Definizione
	documento conservato e di ottenerne copia
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Sequenza di simboli binari, ossia di 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 CAD
Firme multiple	Firme digitali apposte da diversi sottoscrittori allo stesso documento.
Firme parallele	Firme apposte da differenti soggetti al medesimo documento digitale utilizzando una sola busta crittografica.
Firme verticali	Firme apposte da differenti soggetti, l'una ad un documento firmato in precedenza da un altro soggetto, creando delle buste crittografiche innestate l'una dentro l'altra.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
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
Immodificabilità	Caratteristica che rende il contenuto del

Termine	Definizione
	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	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione ad una sequenza informatica d'origine di un'opportuna funzione di hash
Indice di conservazione	Evidenza informatica che elenca in forma strutturata – xml - le impronte, gli identificativi e le informazioni descrittive dei documenti digitali sottoposti insieme a processo di conservazione a norma. Tale file è conforme al <i>UNI 11386:2010 Standard SinCRO</i> ed è firmato digitalmente dal responsabile del servizio di conservazione e marcato temporalmente.
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 delle Regole tecniche, 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 le 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
ISBN	International Standard Book Number
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 su di un 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. 9 delle Regole tecniche del sistema di

Termine	Definizione
	conservazione
Manuale di gestione	Strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico DPCM 31 ottobre 2000 e successive modificazioni e integrazioni
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale. La marca temporale può essere solamente rilasciata da una <i>Time Stamping Authority</i>
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 delle Regole Tecniche del sistema di conservazione
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento
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 informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche solo i metadati riferiti agli oggetti da conservare
PAdES	PDF Advanced Electronic Signatures– Formato di firma che può essere apposto esclusivamente sul tipo di file pdf.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale

Termine	Definizione
	di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'art. 68 del Testo Unico
Piano generale della sicurezza	Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Posta elettronica certificata	Sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici
Presenza 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'art. 10 delle Regole tecniche del sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha firmato 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 il 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

Termine	Definizione
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro particolare	Registro informatico di particolari tipologie di atti o documenti nell'ambito della pubblica amministrazione previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del Testo Unico, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione
Responsabile del servizio di conservazione	Soggetto a cui sono affidati, dal responsabile della conservazione, l'insieme delle attività elencate nell'art. 7 delle Regole tecniche del sistema di conservazione
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 dei dati personali
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Riferimento temporale	Informazione contenente la data e l'ora con

Termine	Definizione
	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
Scheda documento	Aggregato logico costituito da uno o più documenti digitali e/o analogici che sono considerati come un tutto unico e come tali costituiscono l'oggetto di una singola descrizione: nel caso in cui sia formata da più documenti uno di essi si configura come "primario" e gli altri sono gli "allegati" che trovano il loro significato compiuto solo in relazione al primario. E' l'unità minima, concettualmente non divisibile, di cui è composto l'archivio.
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'art. 44 del CAD
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del Testo Unico; per i privati è il sistema che consente la tenuta di un documento informatico
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
Tag	Marcatori (etichette) per assegnare una semantica al testo nei file xml
Testo Unico	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e successive modificazioni
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche alla base dati

Termine	Definizione
Unità di aggregazione	Aggregato logico di schede documento collegate tra loro che si forma nell'archivio corrente e che può costituire un'unità di versamento in conservazione. Il fascicolo che scaturisce da un procedimento amministrativo è il caso più comune di unità di aggregazione, altri esempi sono costituiti dalle serie tipologiche (delibere, contratti ecc).
Unità organizzativa	Qualsiasi articolazione di un'Area Organizzativa Omogenea, ovvero un nodo della struttura gerarchica – mappa organizzativa - in cui si organizza un'Amministrazione
URI	Uniform Resource Identifier
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
Versamento agli Archivi di Stato	Operazione con cui il Responsabile del servizio di 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](#)

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

- 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, comma 3, 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;
- 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.

[Torna al sommario](#)

3.2 Standard di riferimento

Di seguito sono riportati gli standard ai quali si fa riferimento per il Manuale di Conservazione:

- 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 15836-1:2017 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- Moreq - Model Requirements for Electronic Records Management
- Pronom - registro internazionale sui formati idonei alla conservazione a lungo termine

[Torna al sommario](#)

4. RUOLI E RESPONSABILITA'

Il sistema di conservazione DigiDoc, gestito dal Responsabile del Servizio di Conservazione di Engineering, 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.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile del servizio di conservazione	Nigro Cosimo	Definizione e 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.	Giugno 2015
Responsabile Sicurezza dei sistemi per la conservazione	Cafiso Giuseppe	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.	gennaio 2015
Responsabile funzione archivistica di conservazione	Mancini Barbara	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	Giugno 2015

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
		<p>documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;</p> <p>definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;</p> <p>monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;</p> <p>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.</p>	
Responsabile trattamento dati personali	Nigro Cosimo	<p>Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;</p> <p>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</p>	Gennaio 2010
Responsabile sistemi informativi per la conservazione	Carrozzo Massimo	<p>Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;</p> <p>monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;</p> <p>segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;</p> <p>pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;</p> <p>controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del</p>	Giugno 2015

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
		servizio di conservazione.	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Martinucci Valentina	<p>- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;</p> <p>pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione;</p> <p>monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;</p> <p>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;</p> <p>gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.</p>	Giugno 2015

[Torna al sommario](#)

4.1 Il Responsabile del servizio di conservazione

Nel presente paragrafo sono dettagliate le competenze del Responsabile del servizio di conservazione secondo quanto previsto dal decreto [8].

- Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove

- necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
 - adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 decreto [8];
 - assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
 - assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
 - provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
 - predispose il manuale di conservazione di cui all'art. 8 del decreto [8] e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
 - Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
 - Archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
 1. descrizione del contenuto dell'insieme dei documenti;
 2. estremi identificativi del responsabile del servizio di conservazione;
 3. estremi identificativi delle persone eventualmente delegate dal responsabile del servizio di conservazione, con l'indicazione dei compiti alle stesse assegnati;
 4. indicazione delle copie di sicurezza;
 - Mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
 - Verifica la corretta funzionalità del sistema e dei programmi in gestione;
 - Adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione e delle copie di sicurezza dei supporti di memorizzazione;
 - Richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
 - Definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
 - Verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

Il responsabile del servizio di conservazione può delegare in tutto o in parte le proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate.

Il responsabile del servizio di conservazione richiede l'intervento del Pubblico Ufficiale nei casi previsti, assicurando allo stesso l'assistenza e le risorse necessarie all'espletamento delle attività al medesimo attribuite.

Il Responsabile del servizio di Conservazione non è responsabile del contenuto dei singoli documenti né degli indici (attributi) associati a ciascun Documento. La conformità dei documenti trasmessi ai corrispondenti originali è assicurata da formale autorizzazione alla Conservazione da parte del Produttore, eseguita mediante la sottoscrizione del contratto per la fornitura del servizio.

Il responsabile del servizio di conservazione è tenuto ad operare d'intesa con:

- il responsabile del trattamento dei dati personali
- il responsabile della sicurezza
- il responsabile dei sistemi informativi
- il coordinatore della gestione documentale, salvo che il ruolo sia ricoperto dallo stesso responsabile del servizio di conservazione
- i responsabili designati per ciascuno dei sistemi/applicativi abilitati a versare in conservazione la documentazione: per poter versare in conservazione ciascun sistema/applicativo deve essere a ciò abilitato attraverso apposita procedura che prevede di poter indicare il responsabile di riferimento del sistema/applicativo quale figura che il RdC può interpellare per qualsiasi problematica inerente la documentazione versata in conservazione dal sistema/applicativo stesso; qualora tale responsabile non sia designato il coordinatore della gestione documentale e il responsabile del cliente che ha versato la documentazione sono i soggetti tenuti a fornire al RdC tutte le informazioni richieste

[Torna al sommario](#)

4.1.1 Dati anagrafici del Responsabile del servizio di Conservazione

Nel presente paragrafo sono riportati i dati anagrafici, del responsabile del servizio di conservazione attualmente in carica; sono altresì riportati i dati "storici" di tutti i responsabili della conservazione che si sono avvicendati nel tempo.

Con decorrenza dal 03 giugno 2015

il responsabile del servizio di conservazione attualmente in carica, come da apposita nomina, è

cognome NIGRO nome COSIMO

nato a SAN VITO DEI NORMANNI Prov. (BR) il 25/10/1965

cod. fiscale NGRCSM65R25I396M

[Torna al sommario](#)

4.2 Formazione

Per il responsabile del servizio di conservazione e suoi delegati è previsto uno piano di formazione in linea con le guide aziendali allo scopo di adeguare il percorso formativo alle nuove eventuali esigenze di legge e di business. Tale percorso prevede la partecipazione ad eventuali corsi di aggiornamento e seminari periodici sul tema della conservazione digitale, corsi di formazione sulla sicurezza delle informazioni e sulla privacy.

[Torna al sommario](#)

4.3 Delegati del Responsabile del servizio di Conservazione

I delegati del responsabile del servizio di conservazione sono nominati a cura del responsabile stesso e la loro nomina decade automaticamente con la revoca o decadenza del responsabile che li ha nominati.

La nomina dei delegati avviene attraverso un documento sottoscritto dal responsabile del servizio di conservazione, e, per accettazione, dal/i delegati nominati; tale documento viene conservato all'interno dello stesso sistema di conservazione.

La delega può essere:

- di tutte le funzioni del responsabile (fatta comunque salva la facoltà di delegare altri) o solo di alcune, da dettagliare;
- a tempo determinato oppure indeterminato

tutti questi elementi devono essere esplicitamente riportati nel documento di delega pena la non validità della delega stessa.

L'elenco dei delegati sono riportati nell'allegato 5 del presente manuale.

La delega come responsabile del servizio di conservazione può in qualsiasi momento essere revocata dal responsabile del servizio di conservazione formalizzando la revoca nelle stesse forme e modalità della delega (salvo che ovviamente la revoca non deve essere sottoscritta dal/i delegati ma solo dal responsabile del servizio di conservazione); parimenti un delegato ha facoltà di dimettersi/rinunciare alla delega e le dimissioni risultano esecutive a decorrere da 30 giorni dalla presentazione formale – a protocollo generale o alla casella PEC dedicata al sistema di conservazione - del documento di dimissioni/rinuncia (in formato analogico o digitale) sottoscritto dal delegato dimissionario/rinunciatario.

Sia in caso di revoca che di dimissioni/rinuncia è a cura del responsabile del servizio di conservazione mettere in conservazione il documento di revoca/dimissioni/rinuncia, ed aggiornare l'allegato inserendo il termine della delega, il motivo del termine, e gli estremi - id. nel sistema di conservazione ed impronta - del documento che formalizza la fine della delega.

[Torna al sommario](#)

4.4 Coinvolgimento di altri pubblici ufficiali

Qualora il coinvolgimento di pubblici ufficiali che non siano quelli che ricoprono i ruoli di cui ai § 4.1 e 4.3 dovesse rendersi necessario esso andrà formalizzato a cura del responsabile del servizio di conservazione o suo delegato (dotato di opportuna delega), con modalità del tutto analoghe alla nomina dei delegati del responsabile del servizio di conservazione, ed in particolare con l'obbligo di indicare nel documento di formalizzazione dell'incarico al/i pubblici ufficiali le motivazioni e l'ambito di pertinenza dell'intervento richiesto.

L'incarico del pubblico ufficiale, anche se a tempo indeterminato, decade automaticamente con la revoca o decadenza del responsabile del servizio di conservazione o suo delegato che ha formalizzato l'incarico (attraverso sottoscrizione digitale del relativo documento).

Il presente paragrafo riporta gli estremi degli eventuali incarichi a pubblici ufficiali che non siano quelli che ricoprono i ruoli di cui ai § 4.1 e 4.3, ovvero almeno:

- i dati anagrafici necessari ad identificare il pubblico ufficiale (cognome e nome, codice fiscale, luogo e data di nascita);

- il ruolo del pubblico ufficiale e gli estremi dell'amministrazione pubblica in cui ricopre tale ruolo;
- il periodo di validità dell'incarico (senza estremo superiore se l'incarico è ancora in essere ed è a tempo indeterminato);
- le motivazioni e l'ambito di pertinenza dell'incarico al pubblico ufficiale;

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Nella figura che segue sono riportate le strutture organizzative di Engineering Ingegneria Informatica S.p.A. nel suo complesso:

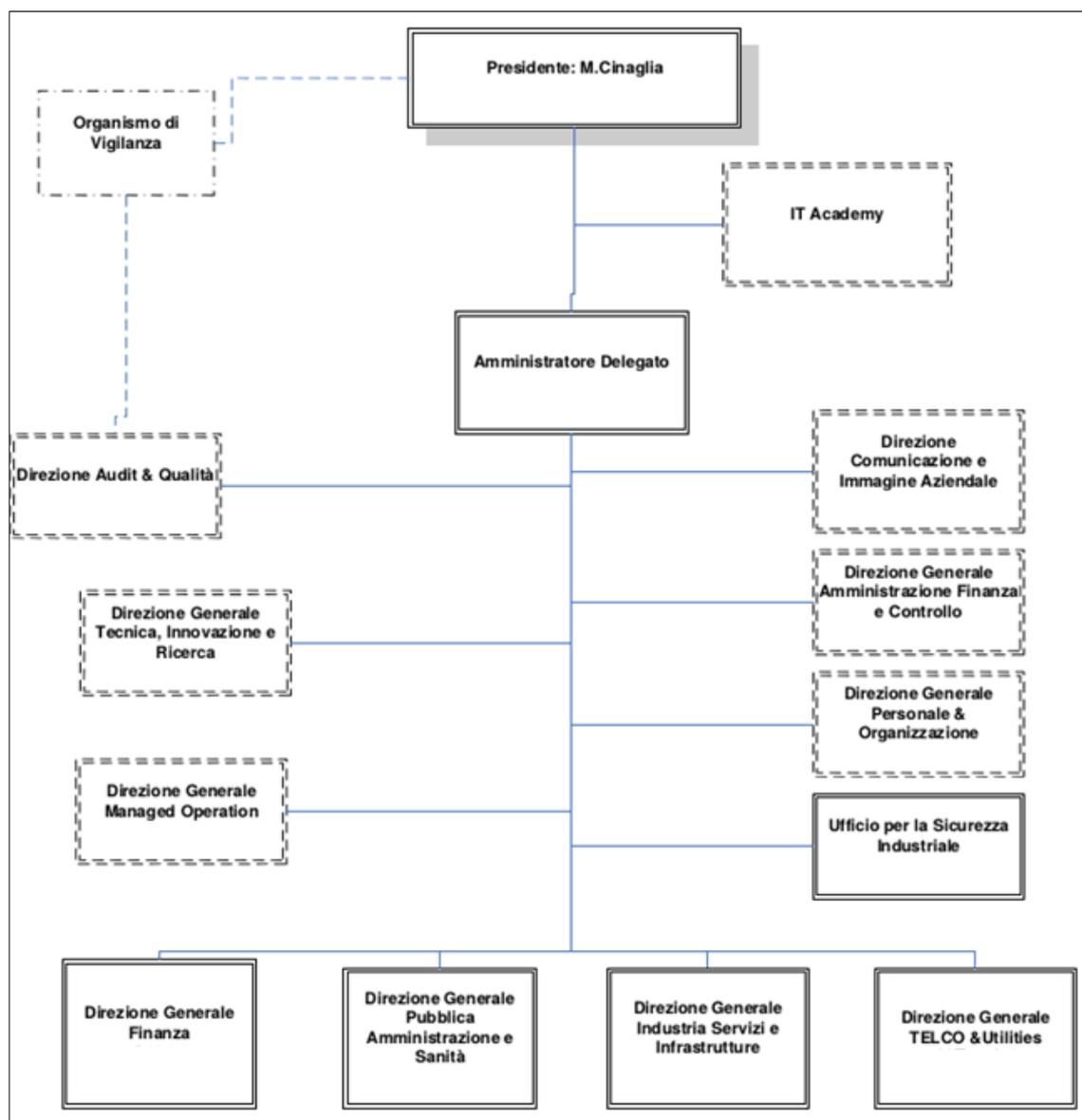


Figura 1 – Strutture Organizzative

Nella figura che segue sono riportate le strutture organizzative di Engineering Ingegneria Informatica S.p.A. coinvolte nel processo di conservazione:

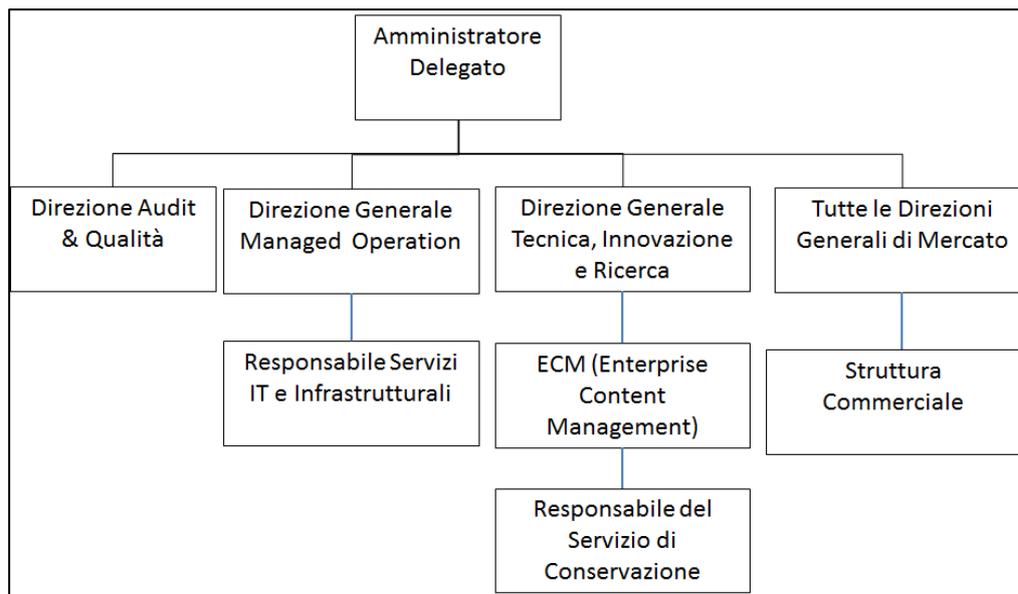


Figura 2 – Strutture Organizzative Servizio di Conservazione

Nella figura che segue sono riportate le strutture organizzative di Engineering Ingegneria Informatica S.p.A. ed Engineering D.HUB, che si relazionano con il responsabile del servizio di conservazione:

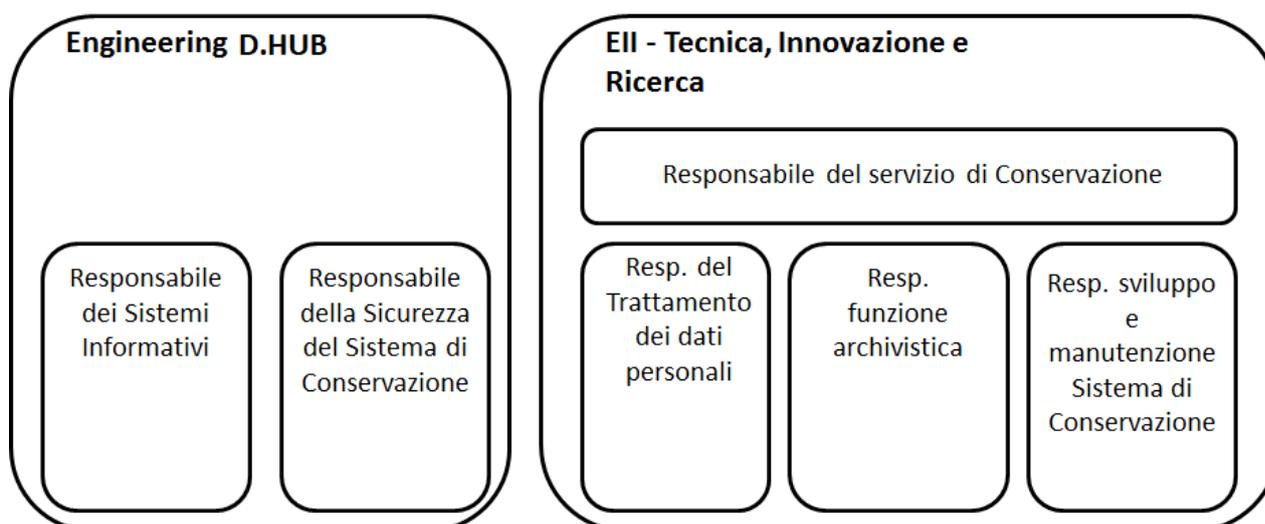


Figura 3 – Relazioni tra Responsabile della conservazione e strutture Organizzative

[Torna al sommario](#)

5.2 Strutture organizzative

Compiti delle strutture organizzative individuate nel capitolo precedente ad esclusione delle strutture che fungono da:

- Amministratore Delegato, nomina il responsabile del servizio di conservazione e le altre figure professionali indicate nel capitolo 5;

- Direzione Audit & Qualità, gestisce il sistema di gestione della qualità e sicurezza redatto secondo le normative ISO 9001 e ISO 27001. La funzione si occupa inoltre di verificare periodicamente la conformità a normativa e standard di riferimento;
- Team del Responsabile del servizio di conservazione, è il team che comprende tutti i ruoli già indicati al capitolo 5 e loro eventuali delegati e si occupa di attivare il servizio di conservazione, censire il Titolare nel sistema di conservazione, concordare col Titolare o con il suo Responsabile della Conservazione, documenti, metadati, tempistiche, regole di validazione, tempistiche e parametri di conservazione, fornire supporto ai Titolari che ne facciano richiesta anche sui loro sistemi per verificare e configurare le applicazioni di trasferimento dei documenti da conservare nel rispetto dei permessi ottenuti dai Titolari medesimi, configurare i metadati e le regole di validazione, le tempistiche e i parametri di conservazione nel sistema di conservazione; definire col Titolare e censire nel sistema di conservazione l'elenco degli utenti autorizzati ad accedere al sistema ed i loro limiti di accesso e utilizzo, erogare il servizio di assistenza ai Titolari del servizio di conservazione, monitorare il sistema di conservazione relativamente all'acquisizione e all'elaborazione dei documenti;
- Responsabile dei servizi IT e infrastrutturali, si occupa della gestione delle componenti hardware e software del sistema di conservazione;
- Struttura commerciale, si occupa di definire i parametri contrattuali e raccogliere la firma dei Titolari sulla richiesta di attivazione del servizio di conservazione;
- Direzione Tecnica, Innovazione e Ricerca, si occupa di gestire lo sviluppo, la correzione di eventuali anomalie, il change management, il rilascio ed il monitoraggio del software del sistema di conservazione, acquisire, verificare e gestire i PdV ricevuti, predisporre il rapporto di versamento per i PdV presi in carico, predisporre il rapporto di rifiuto per i PdV rifiutati; preparare e gestire i PdA tramite applicazioni automatizzate, preparare e gestire i PdD ai fini dell'esibizione e della produzione di duplicati informatici e copie informatiche su richiesta tramite applicazioni automatizzate, verificare integrità e leggibilità dei documenti del sistema di conservazione tramite applicazioni automatizzate.

[Torna al sommario](#)

5.3 Focus sul Centro di Competenza ECM (Enterprise Content Management)

La mission del Centro di competenza ECM di Engineering è fornire soluzioni e servizi per trasformare le informazioni in patrimonio aziendale, supportando i clienti nella selezione degli strumenti migliori per soddisfare i requisiti individuati nei progetti.

Tale centro di competenza fornisce soluzioni e servizi per trasformare contenuti analogici e digitali di un'organizzazione in un patrimonio informativo pienamente fruibile con strumenti di groupware, content, document, workflow e knowledge management. Dispone di competenze sull'intero ciclo di vita documentale, dalla creazione del documento fino alla sua archiviazione, sia dal punto di vista di gestione del processo organizzativo che della normativa; nel centro operano professionisti certificati sulle principali tecnologie di riferimento di mercato e/o open source (pacchetti e piattaforme quali EMC Documentum, IBM FileNet, Alfresco, DRUPAL, OpenCMS, ecc.). All'interno di tale centro di competenza è presente una struttura dedicata alla Dematerializzazione e Conservazione che fornisce conoscenze di alto livello non solo sulla "conservazione a norma", ma anche sui temi organizzativi, normativi e di responsabilità giuridica. Sono presenti risorse esperte con competenze sul modello OAIIS (Open Archival Information System).

[Torna al sommario](#)

5.4 Focus sui servizi erogati da Engineering D.HUB

L'azienda Engineering D.HUB, dispone di soluzioni verticali ed eroga servizi utilizzando la propria rete di Data Center..

I principali servizi offerti da Engineering D.HUB sono:

- gestione centralizzata e distribuita di piattaforme tecnologiche eterogenee
- strutture organizzative di Enterprise Monitoring Center e di Server, Storage & Network Management;
- hosting e housing;
- gestione dei posti di lavoro e degli utenti con servizi di “fleet management”, “service desk” e “help desk”;
- soluzioni e servizi per la gestione di progetti complessi di aggiornamento tecnologico, ottimizzazione di risorse elaborative, implementazione di soluzioni specifiche, come re-hosting di ambienti mainframe, server consolidation & virtualization, disaster recovery;
- application management, business process outsourcing, facility management;
- servizi professionali di consulenza tecnologica, progettuale e metodologica.

[Torna al sommario](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Il servizio offerto da Eng permette potenzialmente il trattamento e la conservazione di qualunque tipologia di documento. Il cliente che intende usufruirne, deciderà per quali tipologie documentali attivare il servizio di conservazione e, una volta comunicatele a Eng, collaborerà col il team DigiDoc nelle operazioni di definizione del relativo trattamento.

Per ogni caso specifico, ossia per ogni Soggetto Produttore i cui documenti vengano presi in carico, Eng individua le classi documentali e i dati o attributi specifici da associare a ciascuna di esse. In questa fase, con le scadenze da concordare; saranno ad esempio precisati i tempi di conservazione, la periodicità di invio dei documenti al sistema di conservazione, l'intervallo di tempo intercorrente tra la presa in carico e la chiusura del pacchetto.

La classe documentale racchiude tutte le caratteristiche comuni ad uno specifico tipo di documento da sottoporre a conservazione, definendone quindi le informazioni indispensabili per qualificarlo ed identificarne gli elementi distintivi. L'elenco e le caratteristiche delle classi documentali vengono precisate di caso in caso, in collaborazione con il Soggetto Produttore; a titolo esemplificativo, tuttavia, le classi più comunemente trattate sono documenti del ciclo attivo (Fatture Clienti, DDT Attivi, Libri e Registri, etc.), del ciclo passivo (Fatture di Acquisto, DDT Passivi, etc.) e documenti del lavoro (LUL).

Il dettaglio delle informazioni sopra indicate, concordate con il soggetto Produttore, sono descritte nello specifico accordo di servizio.

[Torna al sommario](#)

6.2 Pacchetto di versamento

Il Pacchetto di versamento è il pacchetto informativo proveniente dal soggetto produttore e versato nel sistema di conservazione. Le modalità di versamento sono concordate e descritte nell'accordo di servizio.

Fra i diversi aspetti da concordare, i principali sono:

- le tipologie di documenti da conservare,
- metadati,
- eventuali informazioni extra,
- i formati da adottare per ogni classe/tipo di documento,
- le modalità e canali di trasferimento dei documenti nell'archivio (https, ftps).

Il responsabile del servizio di conservazione coordina l'intero processo e si accerta del rispetto delle regole fissate negli specifici accordi di servizio. Viene verificata la presenza dei metadati minimi che il soggetto produttore deve associare alle tipologie documentali informatiche che si accinge a versare nel sistema. Sono conservati i seguenti oggetti: Documenti informatici, documenti amministrativi informatici e fascicoli informatici e per ciascuno di queste tipologie di oggetti sono previsti determinati requisiti minimi.

Per il documento informatico sono previsti i seguenti metadati minimi:

- identificativo univoco e persistente
- data di chiusura
- oggetto (sintesi del contenuto di un documento)

- soggetto che ha formato il documento
- impronta

Per il documento amministrativo informatico, specifico per le pubbliche amministrazioni sono previsti i seguenti metadati minimi:

- codice identificativo dell'amministrazione (codice IPA)
- codice identificativo dell'area organizzativa omogenea (codice IPA)
- codice identificativo del registro
- data di protocollo
- progressivo di protocollo
- impronta.

Per il fascicolo amministrativo sono previsti i seguenti metadati minimi:

- identificativo
- oggetto
- responsabile del procedimento
- elenco dei documenti contenuti nel fascicolo

Il pacchetto di versamento è corredato dal un file xml - SIPManifest.xml, il cui schema è fornito nell'allegato Allegato1 - SIPManifest (Indice di Versamento).pdf - che contiene sia le descrizioni della documentazione che i puntatori e le impronte dei file che compongono la documentazione digitale da inviare in conservazione. In caso di documentazione già inviata in conservazione e di cui si devono solo aggiornare dati e/o file, per le unità di descrizione - schede documento, unità di aggregazione di documenti ecc - e i documenti digitali da aggiornare basta specificare i tag relativi ai dati e/o file da aggiornare. Occorre considerare che la valorizzazione dei tag all'interno delle CustomInfo sostituisce i valori precedentemente specificati per lo stesso item.

La responsabilità del produttore è quella di provvedere e monitorare il corretto funzionamento dell'integrazione tra i sistemi producer e il sistema di conservazione.

E' altresì a cura del produttore fare quanto necessario per assicurarsi che:

- tutta la documentazione venga inviata in conservazione correttamente "tipizzata" nel pacchetto di versamento secondo quanto specificato nell'accordo di servizio, cosicché dalla tipologia specificata il sistema di conservazione sia in grado di impostare correttamente sia il termine entro cui obbligatoriamente deve essere effettuato il processo di conservazione che il termine fino cui decorre l'obbligo di conservazione della documentazione;
- tutta la documentazione sia inviata al sistema di conservazione in tempo utile affinché la conservazione possa avvenire nel rispetto delle tempistiche imposte dalla normativa vigente e secondo quanto concordato negli accordi di servizio;
- la documentazione venga inviata in conservazione corredata almeno dei metadati obbligatori previsti dal profilo specifico della tipologia documentale specificata.

Per quanto concerne gli allegati delle fatture

- nel caso delle fatture attive in base alle nuove regole tecniche della fatturazione elettronica gli eventuali allegati, recanti ad esempio il dettaglio di ciò che viene fatturato, sono inglobati all'interno della fatturaPA (embedded in base 64 nell'xml della fattura stessa), e dato che la fattura è firmata digitalmente sono inviati in conservazione come parte integrante del documento xml

principale della fattura (esattamente come ricevuti dal SdI); tuttavia per garantire una maggior leggibilità vengono anche versati in conservazione come documenti distinti (allegati) della scheda documento della fattura, “estraendoli” dall’xml firmato in cui sono inglobati;

- nel caso delle fatture attive è previsto che eventuali allegati a corredo della fattura siano descritti nel pacchetto di versamento come documenti allegati della scheda documento di cui la fattura è il documento principale

Per quanto concerne eventuali ricevute/notifiche provenienti o inviate al SdI a fronte di una data fattura passiva o pacchetto di archiviazione ricevuto, esse vengono versate in conservazione come schede documento distinte dalla fattura o pacchetto di archiviazione a cui fanno riferimento, creando una relazione con la scheda documento della fatturaPA cui sono relative (attraverso gli appositi tag di relazione tra schede documento previsti dal tracciato xsd del pacchetto di versamento).

[Torna al sommario](#)

6.3 Pacchetto di archiviazione

L’elaborazione del pacchetto di versamento verifica dati e file dei documenti versati al fine di stabilire quali dei documenti del pacchetto possano esser presi in carico da DiGiDoc e quali vadano rifiutati (vi può essere anche una presa in carico parziale). Al termine di questa elaborazione i risultati e i dettagli dei controlli effettuati su tutti i documenti del pacchetto, sia quelli accettati che quelli rifiutati, sono riportati nel rapporto di versamento (SIPResult.xml, il cui schema è fornito nell’allegato Allegato2 - SIPResult (Rapporto di Versamento).pdf) che viene restituito al versatore e al tempo stesso diviene esso stesso oggetto di conservazione in DiGiDoc.

Il Pacchetto di Archiviazione (PdA) o Archival Information Package (AIP) secondo la terminologia OAIS, viene generato dal sistema a conclusione del processo di verifica e presa in carico degli item – schede documento e unità di aggregazione – del PdV e si ottiene dalla trasformazione di uno o più pacchetti di versamento. Esso contiene:

- I documenti conservati nel formato utilizzato all’atto del versamento;
- Il file indice IPdA firmato e marcato temporalmente: esso è un file XML formato secondo le regole tecniche definite nella norma UNI 11386:2010 Standard SInCRO - Supporto all’Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali; nella sezione MoreInfo prevista dallo standard contiene per ciascun documento del PdA:
 - il corrispondente tag *Item* del SIPManifest.xml con cui il documento è stato versato in conservazione (per dettagli si rimanda all’allegato *Allegato1 - SIPManifest (Indice di Versamento).pdf*);
 - il corrispondente tag del *Item* del SIPResult.xml, ovvero il rapporto di versamento, contenente l’esito dei controlli effettuati sul documento (per dettagli si rimanda all’allegato *Allegato2 - SIPResult (Rapporto di Versamento).pdf*).

[Torna al sommario](#)

6.4 Pacchetto di Distribuzione

Il Pacchetto di distribuzione (PdD) o Dissemination Information Package (DIP) secondo la terminologia OAIS, consente di rispettare l’obbligo di esibizione dei documenti conservati; esso viene generato dal Sistema a partire dai Pacchetti di archiviazione conservati ed è finalizzato a mettere a disposizione degli Utenti, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione. Un pacchetto di distribuzione può coincidere con un pacchetto di archiviazione, ma è possibile gestire la

produzione di pacchetti di distribuzione specifici in relazione a particolari esigenze. In relazione alle sue caratteristiche e agli utilizzi a cui è destinato, il Pacchetto di distribuzione può essere generato al momento della richiesta da parte di un Utente e non conservato nel Sistema.

[Torna al sommario](#)

6.5 Formati

Negli accordi di servizio è definito l'elenco dei formati dei documenti che il soggetto produttore vuole conservare nell'archivio digitale.

Qui di seguito l'elenco dei principali formati ammessi:

	FORMATO	ESTENSIONE	MIMETYPE
Bmp	File bitmap	bmp	image/bmp
Doc	Microsoft Word	doc	application/msword
docx	Microsoft Word 2007	docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Gif	Graphics Interchange Format (GIF)	gif	image/gif
Jpeg	Joint Photographic Experts Group	jpg	image/jpeg
jpeg2000	Joint Photographic Experts Group	jp2	image/jp2
Odg	OpenDocument Drawing	odg	application/vnd.oasis.opendocument.graphics
Odp	OpenDocument Presentation	odp	application/vnd.oasis.opendocument.presentation
Ods	OpenDocument Spreadsheet	ods	application/vnd.oasis.opendocument.spreadsheet
Odt	OpenDocument Text Document	odt	application/vnd.oasis.opendocument.text
Ots	OpenDocument Spreadsheet Template	ots	application/vnd.oasis.opendocument.spreadsheet-template
Ott	OpenDocument Text Template	ott	application/vnd.oasis.opendocument.text-template
Pdf	Portable Document Format	pdf	application/pdf
Plaintext		txt	text/plain
Png	Portable Network Graphics	png	image/png
Ppt	Microsoft Power Point	ppt	application/powerpoint
pptx	Microsoft Power Point 2007	pptx	application/vnd.openxmlformats-officedocument.presentationml.presentation
Project	Microsoft Project	mpp	application/vnd.ms-project
Ps	postscript	ps	application/postscript
Rtf	Rich Text Format	rtf	text/richtext
Tar	Tape archive (TAR)	tar	application/x-tar
Tiff	Tagged Image File	tiff	image/tiff
Wav	Audio file	wav	audio/wav
xls	Microsoft Excel	xls	application/excel
xlsx	Microsoft Excel 2007	xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Xml	eXtensible Markup Language	xml	application/xml
Zip	Archivio compresso (zip, gzip, gz, tgz)	zip	application/x-compressed
eml	email	eml	message/rfc822

[Torna al sommario](#)

6.6 Metadati conservati

Il sistema di conservazione consente di gestire tutti i metadati obbligatori previsti dalla normativa vigente ai quali vanno aggiunti quelli presenti negli accordi specifici. Per quanto riguarda le fatture, ad oggi, tenuto conto della normativa vigente, i dati obbligatori da fornire in sede di versamento in conservazione delle fatture e degli altri documenti afferenti ai cicli di fatturazione attivo e passivo (acconti, note di credito, note di debito ecc) sono i seguenti:

- indicazione se documento relativo al ciclo attivo o passivo;
- tipologia del documento, dalla quale vengono ricavati il termine entro cui il documento deve essere messo in conservazione e il termine fino a cui deve essere conservato;
- cognome e nome o denominazione dell'emittente e cognome e nome o denominazione del destinatario;
- codice fiscale e/o eventuale altro identificativo fiscale (es. partita IVA) del emittente/destinatario del documento (a seconda se documento del ciclo passivo o attivo);
- data di emissione della fattura;

- periodo fiscale, numero della fattura e sezionale (vale a dire il registro di numerazione, gestito come dato separato dal n.ro solo nel caso delle fatture attive)

Sia i dati obbligatori di cui sopra che i seguenti dati opzionali:

- importo della fattura
- valuta della fattura

sono stati configurati nel Sistema di Conservazione nel profilo specializzato per i documenti dei cicli di fatturazione attivo e passivo e pertanto vanno/possono essere specificati nel pacchetto di versamento dei documenti afferenti a ciclo attivo e passivo di fatturazione (una volta indicata la tipologia documentale), nei tag AttributoCustom del tag relativo al documento principale della scheda documento.

Essendo specificati nei dati di descrizione del pacchetto di versamento questi dati sono altresì fruibili come chiavi di ricerca delle fatture conservate.

[Torna al sommario](#)

6.7 Tempi di conservazione

Il sistema di conservazione consente di gestire i tempi entro cui è necessario mettere in conservazione e quelli per cui è necessario conservare i documenti. Tali informazioni sono fornite dal produttore all'atto del versamento oppure sono indicati negli accordi di servizio ed associati alle specifiche tipologie documentali.

Tali informazioni relativamente ai documenti dei cicli di fatturazione attivo e passivo sono configurati nel sistema di conservazione su tutte le tipologie documentali interessate. Pertanto nei pacchetti di versamento contenenti i documenti dei cicli di fatturazione attivo e passivo i sistemi produttori non specificano il termine di conservazione né il termine entro cui il documento deve essere sottoposto a conservazione : dalla tipologia dei documenti, in particolare dal fatto che afferiscano al ciclo passivo o a quello attivo di fatturazione, il sistema determina in automatico il tempo di conservazione e il termine entro cui è indispensabile che il processo di conservazione del documento sia perfezionato (con la firma e marca temporale dell'Indice di Conservazione contenente l'impronta e i dati del documento). Ciò detto è responsabilità fondamentale del produttore indicare correttamente la tipologia documentale: in caso di mancata o errata attribuzione della tipologia il sistema di conservazione non potrà procedere all'avvio e mantenimento della conservazione secondo le corrette tempistiche.

Il tempo di conservazione di tutte le tipologie documentali dei cicli attivo e passivo di fatturazione è configurato a 10 anni.

[Torna al sommario](#)

6.8 Peculiarità e gestione delle eccezioni

Nel caso di fatture attive, i documenti afferenti ad un certo registro (o sezionale) e periodo fiscale devono essere sottoposti a conservazione senza soluzione di continuità, ovvero non devono esserci "buchi" nella numerazione progressiva in quel registro e quell'anno fiscale. Qualora vi siano dei "buchi" la conservazione può essere "forzata" ma i "buchi di numerazione" vanno opportunamente motivati e documentati a cura dei responsabili dei processi di produzione e di conservazione delle fatture.

Per soddisfare questo requisito il Sistema di Conservazione prevede meccanismi di controllo ad hoc in fase di creazione degli Indici di Conservazione, mentre il versamento in conservazione può avvenire anche senza rispettare la non soluzione di continuità nelle numerazioni dei registri delle fatture attive. Quando il sistema procede alla chiusura, automaticamente o su richiesta, dei pacchetti di conservazione e

alla creazione automatica dei relativi Indici di Conservazione verifica se nel pacchetto vi sono documenti del ciclo attivo di fatturazione, nel qual caso controlla che:

1. per ogni registro (o sezionale) e anno delle fatture attive presenti nel pacchetto, tutti i numeri precedenti al minore presente nel pacchetto siano già in conservazione (ovvero in un Indice di Conservazione già firmato e marcato temporalmente);
2. per ogni registro e anno delle fatture attive presenti nel pacchetto, vi siano tutte le fatture con numeri compresi tra il minore e il maggiore di quelli presenti per il dato registro e anno

Se questi controlli non vengono superati il file Indice non viene creato e il pacchetto non viene chiuso; viene invece corredato in automatico di un messaggio che dettaglia il motivo per cui la chiusura del pacchetto non è stata possibile: il messaggio appare in evidenza al RdSC quando procede all'attività ordinaria di verifica dei pacchetti da firmare. Il RdSC deve allora verificare se le fatture mancanti, al fine di garantire la non soluzione di continuità della numerazione, sono in altri pacchetti aperti o sono ancora "da consolidare" (ovvero accettate dal sistema di conservazione ma non ancora inserite in un pacchetto) e nel caso la/le trovi procede a spostarle nel pacchetto di cui è fallita la chiusura, dopodiché procede ad una normale chiusura. Diversamente il RdSC è tenuto a verificare insieme al produttore – vale a dire la persona che ha la responsabilità del sistema/applicativo che ha versato le fatture, e qualora questi non sia designato, il coordinatore della gestione documentale e il/i responsabili del cliente cui fanno capo le fatture - il motivo per cui le fatture mancanti non risultino ancora versate in conservazione:

- a) qualora il versamento della/e fatture mancanti non possa essere effettuato per motivate ragioni, che in ultima analisi possono essere solo l'errore umano o applicativo/di infrastruttura informatica che abbia prodotto la mancanza o perdita della fattura anche nel sistema produttore, ciò andrà debitamente documentato dal RdSC, in base alle indicazioni fornite dal produttore; inserite queste motivazioni in apposito form il RdSC può forzare la chiusura del pacchetto nel cui Indice di Conservazione, poi firmato dal RdSC, verranno automaticamente riportate sia le ragioni che impedivano la chiusura che le motivazioni della forzata chiusura compilate a cura del RdSC
- b) qualora le fatture mancanti siano rintracciate all'interno del sistema produttore che non ha ancora proceduto a versarle in conservazione o le ha versate ma senza riuscire a farle prendere in carico al Sistema di Conservazione a causa di errori commessi nella formazione del pacchetto di versamento e mai sanati, è responsabilità del produttore effettuare il versamento in modalità corretta e responsabilità del RdSC fornire al produttore tutto il supporto necessario e verificare che il versamento avvenga tempestivamente e vada a buon fine.

[Torna al sommario](#)

7. IL PROCESSO DI CONSERVAZIONE

DigiDoc adotta lo standard ISO 14721:2012, comunemente noto come OAIS (Open Archival Information System), che costituisce lo standard di riferimento per qualsiasi sistema si occupi di digital preservation.

La soluzione, nel pieno rispetto della normativa in materia e degli standard internazionali di riferimento, assicura la gestione di tutti i processi inerenti la conservazione quali:

- Processo di Amministrazione: preparazione dell'ambiente, intendendo con ciò la messa a punto del contesto operativo, finalizzata alla predisposizione degli elementi necessari alla creazione, gestione, archiviazione e conservazione dei documenti (massimario di scarto, formati, metadati associati ai documenti ...);
- Processo di Invio in Conservazione: trasferimento del documento al Sistema di Conservazione.
- Processo di Controllo: verifica che il documento abbia i requisiti per essere accettato dal sistema di conservazione
- Processo di Conservazione e fruizione della memoria digitale.
- Processo di Consultazione: ricerca della documentazione conservata da parte di soggetti abilitati.

Le funzionalità gestite dal sistema permettono di garantire:

- l'identificazione certa del soggetto che ha formato il documento e dell'AOO di riferimento
- l'integrità del documento
- la leggibilità e l'agevole reperibilità dei documenti e dei relativi metadati
- il rispetto della normativa nazionale sulla conservazione , con adeguamento alla variazione delle norme
- la prevenzione della obsolescenza hw e sw, attraverso adeguamenti continui dell'HW e del SW e attraverso riversamenti sostitutivi dei documenti digitali;
- il rispetto del trattamento dei dati e della tutela dei dati tramite la registrazione e conservazione - in un sistema di audit unico in grado di restituire dati di sintesi, ma interrogabili a più livelli di dettaglio - il tracciamento di ogni accesso, variazione e intervento sul sistema: accessi, modifiche tecnologiche, aggiornamenti dei metadati e dei documenti digitali.
- Il “mantenimento in vita” delle firme digitali dei documenti, tramite l'apposizione e il rinnovo delle marche temporali;
- l'ampliamento e l'aggiornamento della lista dei formati digitali ammessi;
- la ricezione, il mantenimento, l'aggiornamento e la conservazione di tutti i metadati relativi alla documentazione dell'archivio.

[Torna al sommario](#)

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

Il processo di invio in conservazione inizia con l'invocazione da parte di un sistema/applicativo del Soggetto Produttore del web service di SendSIP esposto da DigiDoc.

Tale servizio prevede l'invio in conservazione di una collezione di uno o più documenti o aggregati di documenti attraverso un attachment, il Submission Information Package (SIP) di OAIS, che è un file compresso – zip o tar.gz – contenente:

- un file xml *SIPManifest.xml* (eventualmente firmato digitalmente) che contiene sia i metadati del/i documenti e loro aggregati (fascicoli, serie ecc) da inviare in conservazione, sia le impronte e gli URI (percorsi relativi all'interno del file archivio) dei file associati ai documenti;
- i file che compongono i documenti digitali da inviare in conservazione (che possono essere o meno firmati digitalmente).

Per ogni *item* – i.e. documento o aggregato di documenti – presente nel SIP il sistema del *Soggetto Produttore* deve specificare nel *SIPManifest.xml* un identificativo univoco attraverso cui può richiederne in seguito degli aggiornamenti o l'esibizione. Infatti lo stesso servizio di SendSIP consente anche di inviare ad DIGIDOC solo degli aggiornamenti dei metadati (ad esempio il tempo di conservazione) e/o dei file della documentazione già inviata in conservazione. In questo caso l'attachment contiene solo il *SIPManifest.xml*, se si devono rettificare, aggiornare o versionare solo dei metadati, ed eventualmente anche i file da rettificare o versionare. Peraltro l'identificativo che il *Soggetto Produttore* deve specificare per ogni item (univoco solo limitatamente a quelli degli item inviati dal dato sistema) serve anche affinché DIGIDOC possa controllare se un dato sistema ha già inviato un dato item in modo da non accettarlo in conservazione qualora quel *Soggetto Produttore* lo stia inviando una seconda volta (senza indicare che si tratta di un aggiornamento).

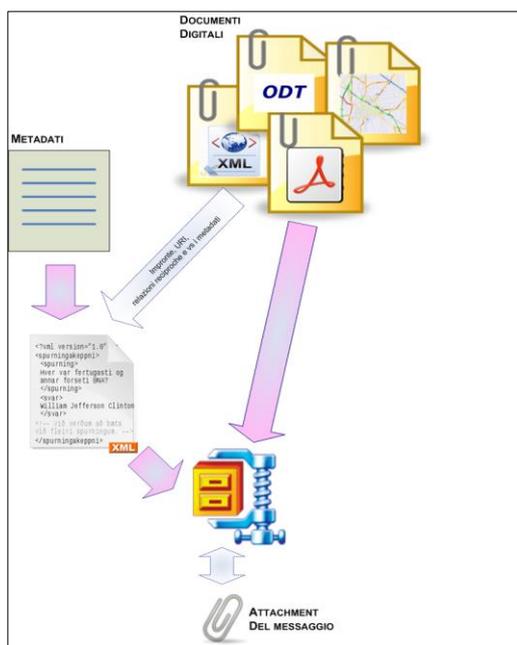


Figura 4 – Versamento del documento nel sistema di conservazione

Gli estremi di ciascun SIP ricevuto, tra cui il produttore e l'identificativo univoco assegnatogli dal produttore, sono memorizzati in apposita tabella di DiGidoc insieme al numero di registrazione, in apposito registro dei SIP, assegnatogli da DiGiDoc stesso. Associato a questo record viene archiviato e avviato alla conservazione il corrispondente *SIPManifest.xml*.

In automatico viene anche prodotto giornalmente e avviato alla conservazione il file PDF/A del registro di tutti i SIP ricevuti (comprensivo delle impronte dei *SIPManifest.xml*): essendo un registro tenuto secondo i crismi di un registro di protocollo esso provvede l'apposizione di un riferimento temporale certo sul SIP.

Sia i file che le strutture dati dei SIP sono oggetto delle procedure di back-up adottate per tutti i dati e i file archiviati in DiGiDoc.

Una volta che il pacchetto di versamento è stato preso in carico dal Sistema di Conservazione, il sistema produttore riceve un ticket attraverso cui può in seguito richiedere l'esito dell'invio di quel SIP, vale a dire il rapporto di versamento: stato di trasmissione/elaborazione e dettaglio dell'elaborazione, ovvero cosa è stato accettato in conservazione e cosa no e perché. Infatti il processo di invio in conservazione della documentazione nel suo complesso prevede una modalità di interazione che è asincrona, dato che i documenti inviati in un unico SIP possono essere molti o di dimensioni ragguardevoli e che la verifica del SIP da parte del Sistema di Conservazione può richiedere un certo tempo di elaborazione.

[Torna al sommario](#)

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

Quando la documentazione inviata in conservazione arriva al modulo di elaborazione dei pacchetti di versamento, il modulo si occupa per prima cosa di effettuare i controlli dei metadati e dei file del SIP pervenuto: la documentazione che non supera i controlli "bloccanti" non può essere ammessa in conservazione. Il sistema DiGiDoc compie le seguenti classi di controlli dettagliati nei seguenti paragrafi:

- Controllo dell'identità del soggetto produttore del pacchetto;
- Controllo delle Firme Digitali;
- Controlli dei Formati digitali;
- Controllo della Presenza di Macro e Codice Eseguitabile;
- Controllo dei Metadati;
- Controllo impronta.

[Torna al sommario](#)

7.2.1 Controllo impronta del pacchetto di versamento

Per evitare eventuali alterazioni, al produttore del pacchetto di versamento viene richiesto di inserire l'impronta. Il sistema DiGiDoc, all'atto del versamento, calcola l'impronta e la confronta con quella inserita dal produttore. Se le due stringhe non coincidono, il pacchetto viene rifiutato.

[Torna al sommario](#)

7.2.2 Controllo dell'identità del soggetto produttore del pacchetto

Il versamento di un pacchetto può avvenire solo fornendo una coppia di credenziali – userid e password – che vanno specificate nell'header del messaggio con cui il pacchetto viene inviato a DiGiDoc: tali credenziali sono state precedentemente generate e memorizzate da DiGiDoc associandole ai dati anagrafici – denominazione, codice fiscale, partita IVA, codice IPA se trattasi di PA ecc - del soggetto produttore a cui sono state rilasciate. Inoltre nel SIPManifest.xml sono previsti come dati obbligatori – si veda Allegato1- SIPManifest (Indice di Versamento).pdf per maggiori dettagli – i dati identificativi del soggetto che ha prodotto il pacchetto. Quando riceve un pacchetto di versamento il primo controllo effettuato da DiGiDoc è quello relativo alle credenziali di autenticazione inviate e subito dopo quello che il soggetto produttore specificato nel SIPManifest.xml sia quello corrispondente alla credenziali verificate.

[Torna al sommario](#)

7.2.3 Controllo delle Firme Digitali

I controlli sulla/e firme digitali e sulle relative marche temporali, sono i seguenti:

- la firma non deve precludere la leggibilità del documento, per cui se il documento firmato è una busta crittografica quale una busta p7m o CAdES, la busta deve poter essere aperta: il mancato superamento di tale controllo impedisce l'accettazione in conservazione;
- le eventuali marche temporali associate alle firme devono essere valide, ovvero: integre, di formato ammesso dalla normativa, emesse da una TSA accreditata da AgID, firmate da un certificato valido e non revocato né sospeso alla data della marca, non ancora scadute: qualora alcuni di questi controlli non siano superati ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- la busta crittografica deve essere in uno dei formati ammessi dalla normativa italiana (quella in vigore alla data del riferimento temporale associato al documento firmato - una marca temporale o una data, quale la data di protocollo del documento, associata al documento digitale nel SIPManifest – ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo) e deve risultare integra: il mancato superamento di tale controllo impedisce l'accettazione in conservazione;
- i certificati di firma devono essere attendibili, ovvero emessi da CA accreditate da AgID: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- i certificati di firma non devono risultare scaduti alla data del riferimento temporale associato al documento firmato ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- i certificati di firma non devono risultare revocati o sospesi alla data del riferimento temporale associato al documento firmato ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento.

Il Sistema di Conservazione è in grado di verificare tutti i tipi e i formati di firme digitali e marche temporali ammessi dalla normativa italiana, e si adegua nel tempo ad ogni cambio normativo in materia di firma digitale.

Dunque ad oggi è in grado di verificare:

- controfirme, firme parallele e firme multiple
- le buste crittografiche: p7m (PKCS#7 e CAdES); PDF (PAdES); XML (XAdES)
- le modalità di imbustamento (enveloped, enveloping, detached)
- le eventuali marche temporali associate alle firme, di qualunque dei formati ammessi (tsr, tsd, tst), sia detached che embedded nella busta crittografica.

Trattandosi di un sistema pensato per la conservazione a lungo termine, e che quindi ha un'attesa di vita molto lunga, è progettato per poter effettuare controlli diversi sui tipi e i formati di firme e marche accettati, a seconda del riferimento temporale dei documenti: in questo modo tiene conto del fatto che ciò che è stato validamente firmato secondo la normativa vigente quando la firma è stata apposta, può non essere conforme alla norma vigente al momento del suo invio in conservazione.

Il sistema traccia tutti i controlli effettuati e i relativi esiti (corredandoli del timestamp in cui li ha effettuati). In particolare dato che il servizio di verifica firma restituisce tutti i dati ottenuti dall'analisi

della busta crittografica - superamento o meno dei vari gradi di validità; estremi degli intestatari dei certificati di firma e delle CA che li hanno emessi; timestamp delle eventuali marche temporali associate; tipo di busta crittografica ecc – tutti questi dati vengono memorizzati nel pacchetto di archiviazione del documento.

Da notare in particolare che il servizio di verifica delle firme digitali:

- consente di specificare un riferimento temporale – quale una data di registrazione a protocollo – rispetto al quale deve essere effettuata la verifica della firma: in questo modo viene soddisfatto il requisito di legge che prevede di considerare altri riferimenti temprali, oltre alle marche, come riferimenti temporali opponibili a terzi;
- quando la verifica della firma viene fatta rispetto ad una data passata, indicata da un marca temporale o da un altro riferimento temporale, il sistema valuta la validità del formato della busta crittografica rispetto a quella data (ad esempio una busta p7m non CADES che utilizza ancora l’algoritmo SHA-1 per il calcolo dell’impronta può risultare comunque valida purché riferita ad una data antecedente 30/6/2010);
- anche il periodo di validità delle marche temporali viene valutato rispetto alla loro data di emissione (la norma ha cambiato nel tempo il periodo di validità minimo richiesto alle TSA);
- grazie ad un archivio storico di CRL che viene man mano incrementato – ogni qual volta, nel verificare una firma, si scarica o si aggiorna una CRL – è in grado di verificare lo stato di revoca e sospensione di un certificato di firma a cui sia associato un riferimento temporale così addietro nel tempo che la relativa CRL non è più pubblicata (la norma impone alle CA di mantenere le CRL solo fino allo scadere dei certificati con cui sono stato firmati i certificati di firma che rimandano alle CRL).

[Torna al sommario](#)

7.2.4 Controllo dei Formati digitali

Su ciascun documento digitale inviato in conservazione il sistema di conservazione effettua il controllo del formato: se il formato non è riconosciuto o non è tra quelli ammessi l’intera scheda documento cui appartiene il documento digitale non viene accettata in conservazione. Tale controllo si basa sul contenuto del file e non sull’estensione del nome file (che potrebbe non essere indicata o peggio essere discordante rispetto al formato effettivo del file). In particolare nel caso di documenti che sono buste crittografiche - p7m, tsd, m7m - il formato che viene riconosciuto è quello del documento con il contenuto informativo depurato della/e eventuali buste crittografiche: il sistema prima procede allo “sbustamento” (se necessario anche ricorsivamente) ed una volta che è arrivato ad un file che non è più una busta crittografica procede al riconoscimento del formato di quel file.

Il servizio di verifica formati del Sistema di Conservazione è ad oggi in grado di riconoscere con un buon grado di affidabilità i seguenti formati:

- PDF e PDF/A;
- tutti i formati della suite MS Office (inclusi Power Point, Visio e Project);
- tutti i formati della suite Open Office;
- RTF;
- formati immagine tiff, bmp, jpeg e jpeg2000, png, gif, pdf immagine;
- xml, ascii (txt, csv, ecc);
- formati audio e video quali wave, aiff;
- gli archivi compressi zip

- mail in formato eml

Il formato eml di fatto è un formato archivio/busta che a loro volta contengono delle parti con dei loro formati. Quindi quando vengono verificati, come nel caso delle buste crittografiche, il servizio di verifica formato va a verificare anche i contenuti del file archivio e delle parti della busta eml (attachment e body): se questi sono riconosciuti e ammessi il file archivio o eml è ammissibile in conservazione, altrimenti no. E' anche gestita la verifica ricorsiva dei formati dei file contenuti se nel file archivio/eml vi sono dei file/attachment che sono a loro volta file archivio o e-mail. Il fatto che il servizio di verifica formato sia in grado di riconoscere e verificare il contenuto di questi formati "contenitore", anche nel caso di annidamenti di buste, mette il Sistema di Conservazione nella condizione di poter accettare in conservazione:

- e-mail firmate;
- ricevute PEC, ovvero e-mail che in genere contengono a loro volta, come attachment, l'e-mail di cui sono la ricevuta: possono essere documenti che è importante conservare in quanto a norma di legge costituiscono un riferimento temporale opponibile a terzi (riferimento utilizzabile per esempio per il documento firmato che è stato inviato in uscita tramite PEC e il cui invio ha dato luogo a quella ricevuta);
- archivi compressi per i quali esiste solo una descrizione complessiva, come documento semplice, e non quelle singoli file componenti.

Una volta che il formato di un documento inviato in conservazione è stato riconosciuto viene sottoposto ad un filtro ulteriore che analizza il formato utilizzando detector diversi e specifici a seconda del formato riconosciuto: attraverso tale analisi il Sistema di Conservazione può determinare la versione del formato, laddove prevista e altre utili informazioni, che andranno ad arricchire i metadati dell'AIP del documento (in particolare la sezione delle informazioni di stabilità, come definite da OAIS).

Tenuto conto che i formati ad oggi riconosciuti dal Sistema di Conservazione, in un'ottica di conservazione a lungo termine, non sono tutti ugualmente idonei alla conservazione, i formati che effettivamente il sistema di conservazione accetterà e che saranno indicati negli accordi di servizio seguiranno formati caratterizzati dai seguenti aspetti:

- aperti
- ben documentati
- standard, possibilmente de-jure
- non proprietari
- largamente diffusi
- indipendenti dalla piattaforma
- che permettono di includere nei file l'insieme di metadati - self-documentation - che ne descrivono il contenuto e il processo di produzione, fornendo anche i dettagli tecnici per la loro rappresentazione negli ambienti tecnologici del futuro
- che non possano contenere macroistruzioni o per i quali siano disponibili strumenti efficaci per rilevare con sufficiente sicurezza la presenza di macroistruzioni
- che non prevedano meccanismi tecnici di protezione e di limitazione sull'utilizzo
- accessibili e robusti
- caratterizzati da un'elevata stabilità (backward e forward compatibility)

E' buona norma considerare che i formati per cui siano disponibili viewer o reader solo per una o poche piattaforme, anche se non vietati e quindi inseribili nel set dei formati ammessi, andranno comunque

evitati quanto più possibile, perché utilizzarli corrisponderebbe a creare una limitazione forte sulla capacità dei sistemi e client fruitori di riprodurre i documenti, e di conseguenza sulla capacità del sistema di conservarli.

Infine si è stabilito che tra i formati che non devono comunque essere accettati in conservazione, vi siano quelli per i quali, sui registri internazionali di formati – quali UDFR e PRONOM – sia indicata una data di obsolescenza o di prevista/avvenuta cessazione di supporto. E' responsabilità del RdSC ed eventuali suoi delegati verificare gli aggiornamenti dei formati in suddetti registri al fine di configurare correttamente il set di formati ammessi in conservazione, procedere ad eventuali procedure di riversamento di quanto già conservato in quel formato nonché dare indicazioni ai produttori e in particolare al coordinatore della gestione documentale in merito a quali formati abbandonare perché a rischio di obsolescenza.

Una volta che il formato di un documento inviato in conservazione è stato riconosciuto viene sottoposto ad un filtro ulteriore che analizza il formato utilizzando detector diversi e specifici a seconda del formato riconosciuto.

Nel dettaglio del formato sono inoltre presenti:

- tutti i dati previsti per la descrizione dei formati nei registri internazionali quali PRONOM e UDFR;
- l'identificativo – obbligatorio - assegnato al formato in uno dei registri appena menzionati.

[Torna al sommario](#)

7.2.4.1 Funzionalità di configurazione

Il sistema consente di configurare per ciascun formato ammesso i seguenti dati di dettaglio:

- nome ed eventuale versione del formato: è questa la coppia che lo identifica univocamente tra tutti gli altri formati censiti;
- estensione principale dei file del dato formato: tale estensione sarà quella che verrà aggiunta in automatico ai nomi dei file accettati in conservazione qualora i nomi originali specificati nel tracciato di versamento/trasferimento non abbiano estensione o ne abbiano una ma non congruente con quella/e previste per il formato effettivo dei file;
- lista dei viewer/reader che sono utilizzabili per il rendering dei file del dato formato.

[Torna al sommario](#)

7.2.5 Controllo della Presenza di Macro e Codice Eseguitabile

Sui documenti digitali inviati in conservazione sono effettuati i controlli per verificare la presenza di parti variabili – macro – e codice eseguibile/dinamico; infatti questi elementi, qualora presenti, non solo danno luogo a sottoscrizione non valida se il file è firmato digitalmente, ma rendono comunque il documento non ammissibile in conservazione in quanto perde le sue caratteristiche di documento così come sancito dalla norma: non è un documento un oggetto che non si presenta sempre uguale nel tempo. Inoltre le macro e il codice eseguibile/dinamico sono i principali veicoli di virus e altri elementi potenzialmente nocivi, se non per il sistema di conservazione in sé, quantomeno per i client che dovessero richiedere l'esibizione di documentazione contenente malware.

Il controllo della presenza di macro viene effettuato su tutti i formati MS Office e Open Office che sono quelli che contemplano tale rischio, mentre la presenza di parti di codice eseguibile o dinamico (ad esempio javascript) viene verificata sul formato pdf che la consente (salvo se PDF/A).

[Torna al sommario](#)

7.2.6 Controllo dei Metadati

Per garantire la qualità dei metadati contenuti nel SIPManifest, il SIP Manager è in grado di effettuare sui metadati di ogni item tutti i seguenti tipi di controlli:

- di obbligatorietà: verifica la presenza di taluni metadati (o loro combinazioni) in assenza dei quali l'item non può essere accettato in conservazione;
- di correttezza sintattica: effettua controlli formali – di tipo e formato, di appartenenza ad un certo range/set predefinito di valori ecc – su tutti i metadati;
- di coerenza interna: verifica che non vi siano incongruenze tra i metadati all'interno dello stesso SIPManifest (ad esempio: verifica che le date dei documenti di un certo fascicolo non vadano oltre la data di chiusura specificata per il fascicolo);
- di coerenza con il contesto archivistico e organizzativo dell'ente: può essere configurato per verificare che i metadati che riconducono la documentazione versata al contesto amministrativo, organizzativo e archivistico dell'ente – classificazione, tipologia documentale, ufficio/struttura che ha prodotto il dato fascicolo, tipo del procedimento da cui è scaturito il fascicolo ecc – siano coerenti con il contesto stesso, così come è stato definito a sistema (se è stato definito); può verificare altresì che il sistema del Soggetto Produttore utilizzi solo quelle parti degli strumenti archivistici - voci del piano di classificazione, tipologie documentarie ecc. – che gli sono consentite (qualora siano definite delle limitazioni in tal senso)
- di unicità: il SIP Manager è anche in grado di verificare, sulla base di alcuni dati del SIPManifest che fanno parte delle informazioni di identificazione di OAIS, se un certo documento o unità di aggregazione di documenti è già stato inviato in conservazione o risulta descritto più volte nello stesso SIPManifest (nel qual caso può dar luogo ad un errore bloccante o solo ad un avvertimento)

Il nucleo base dei controlli sui metadati è prestabilito per tutti gli enti che utilizzano DIGIDOC: si tratta dei controlli che sono indispensabili a garantire la corretta conservazione della documentazione, così come regolata dalle norme e intesa e realizzata dal sistema. A questo nucleo base di controlli ogni ente può aggiungerne altri, anche specializzati per le diverse tipologie documentali, in modo da rafforzare e modulare il filtro di ciò che DIGIDOC può prendere in carico.

Le obbligatorietà/vincoli del nucleo base di controlli sui metadati sono i seguenti:

- è obbligatorio specificare un identificativo (univoco per il sistema che invia) per ogni documento o aggregato di documenti
- è obbligatorio specificare un'etichetta/segnetura per ogni documento o aggregato di documenti (nel caso di documento protocollato potrebbero essere gli estremi di protocollo, nel caso di un fascicolo archivistico la sua segnetura basata sulla classifica e l'anno di apertura)
- è obbligatorio specificare un'intitolazione ovvero una descrizione/oggetto per ogni aggregato di documenti o singolo documento
- è obbligatorio specificare almeno un riferimento cronologico (data di acquisizione/produzione/registrazione a protocollo; data/anno di apertura o chiusura del fascicolo ecc) per ogni documento o aggregato di documenti
- è obbligatorio specificare una tra tipologia, classifica o procedimento amministrativo che ha dato luogo alla documentazione, ovvero specificare il tempo o termine di conservazione se non

desumibile da nessuno degli elementi precedenti. Se il tempo è specificato sul documento o aggregato inviato, non può essere inferiore ma solo superiore a quello stabilito da eventuali regole del massimario di selezione e scarto applicabili a quel documento o aggregato.

Inoltre ai dati del nucleo minimo richiesto, nel caso di documentazione tributaria o fiscalmente rilevante come le fatture si aggiungono i dati già indicati al § 6.6.

[Torna al sommario](#)

7.2.7 Controllo Impronta

Il sistema calcola l'impronta dei file e la confronta con quella dichiarata nel SipManifest.xml. Se le due stringhe non coincidono, viene segnalato nel rapporto di versamento.

[Torna al sommario](#)

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

Gli audit dei controlli effettuati, con dettaglio di esiti ed eventuali risultati (ad esempio nel caso della verifica della validità delle firme, tra i risultati vi sono i dati dei certificati di firma) vengono memorizzati per tutti gli item del SIP, sia quelli accettabili che quelli rifiutati, andando a costituire il “rapporto di versamento” SIPResult.xml, il cui schema è fornito nell'allegato Allegato2 - SIPResult (Rapporto di Versamento).pdf. Il rapporto viene esso stesso archiviato e avviato alla conservazione per tempo illimitato. Come detto in precedenza anche il SIPManifest.xml viene archiviato e avviato alla conservazione, il tutto al fine di attestare nel tempo il flusso di tutto ciò che è arrivato in conservazione e come tale flusso è stato trattato. Più precisamente il rapporto di versamento SIPResult.xml viene archiviato collegandolo al relativo pacchetto di versamento attraverso l'inserimento della sua impronta, data e ora di generazione e URI nella stessa tabella di archiviazione dei dati dei SIP. Analogamente al SIP anche il rapporto di versamento, non appena generato, viene sottoposto a registrazione in apposito registro dei rapporti di versamento che quotidianamente viene prodotto in formato PDF/A e avviato alla conservazione.

E' a cura del sistema produttore che ha inviato il SIP richiedere, attraverso polling, il rapporto di versamento di ciascuno dei SIP inviati fintantoché essi non risultino disponibili, ed è altresì responsabilità del RdSC e suoi delegati accertarsi della corretta e tempestiva (compatibilmente con il carico di lavoro del sistema di conservazione) produzione dei rapporti di versamento di ogni SIP ricevuto nonché della loro messa in conservazione unitamente al SIPManifest.xml.

DigiDoc esegue appositi controlli sui documenti versati propedeutici all'accettazione del documento in conservazione di seguito descritti.

[Torna al sommario](#)

7.3.1 Rinnovo marche temporali in scadenza

DigiDoc prevede un controllo periodico dei pacchetti per verificare se le marche temporali apposte sugli Indici di Conservazione firmati vanno rinnovate perché prossime alla naturale scadenza.

A valle di questa verifica per ogni Indice di Conservazione la cui marca temporale è in scadenza DigiDoc può:

- a) rinnovare la marcatura in modo automatico, richiedendo una nuova marca ad una delle TSA accreditate: la marca viene apposta sull'Indice di Conservazione già firmato e marcato, in modo da garantire la non soluzione di continuità del processo di conservazione;
- b) far rifirmare e marcare l'Indice già firmato e marcato

Nello scenario b) apposita GUI pone i pacchetti da rimarcare, previa nuova firma, all'evidenza dell'RdSC.

[Torna al sommario](#)

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

Se un pacchetto di versamento non supera uno dei controlli previsti, viene rifiutato e non viene caricato nel sistema. I seguenti controlli, se non vengono superati, generano uno scarto del pacchetto:

- Verifica impronta del pacchetto;
- Apertura della busta crittografica dei file firmati;
- Conformità del formato della busta crittografica dei file firmati alla normativa italiana;
- Formati dei documenti digitali.

Viene prodotto un report dello scarto in cui viene riportato il timestamping in cui è avvenuto il controllo ed un dettaglio dei controlli effettuati ed il loro esito. Tale report viene inviato al referente tecnico indicato dal produttore.

[Torna al sommario](#)

7.5 Preparazione e gestione del pacchetto di archiviazione

I documenti contenuti nel SIP che superano tutti i controlli (salvo quelli eventualmente "elusi" dal Soggetto Produttore) entrano nel sistema di conservazione.

Per facilitare la verifica, il contenuto degli elenchi è presentato nelle seguenti sezioni distinte:

- Unità di conservazione;
- Unità archivistiche;
- "documenti sciolti": unità documentarie non versate all'interno di un'unità archivistica in esso contenuti

I documenti digitali accettati vengono consolidati attraverso l'aggregazione dei documenti stessi in insiemi logici chiamati pacchetti in consolidamento (ovvero pacchetti non ancora chiusi, vedi § successivo). Già al momento dell'accettazione in conservazione per ogni scheda documento e ogni unità di aggregazione sia tutti i dati presenti nel SIPManifest.xml che quelli frutto dei controlli vengono "impacchettati" in xml, a formare i pacchetti di archiviazione, e in questa forma archiviati sullo storage del sistema di conservazione. Sul database relazionale vengono memorizzati i puntatori ai pacchetti di archiviazione conservati su storage. Al tempo stesso i dati di descrizione di ciascun item versato e accettato vengono inseriti nella banca dati relazionale del Sistema di Conservazione.

E' possibile configurare:

- sia i trigger di innesco automatico della creazione degli Indici di Conservazione, quali i seguenti:

- quando si raggiunge la soglia minima di giorni dallo scadere del termine entro cui la documentazione deve essere messa in conservazione perché scadono i certificati delle firme digitali apposte;
- per rispettare dei termini stabiliti dalla norma (ad esempio nel caso di documentazione fiscalmente rilevante quali le fatture e i libri contabili che va messa in conservazione entro un certo lasso di tempo a partire dalla data di emissione/produzione);
- quando sono stati accumulati un determinato numero o una determinata dimensione di documenti;
- con una certa cadenza temporale, ad esempio settimanale o mensile;
- sia i vincoli da rispettare nella creazione dei pacchetti quali
 - se fare pacchetti omogenei per certe tipologie o formati digitali di documenti;
 - se creare pacchetti che contengono documentazione i cui termini di conservazione devono restare entro un certo range (in modo tale che tutta la documentazione del pacchetto diventi scartabile in un intervallo temporale relativamente ristretto).

Quando c'è un nuovo documento “da consolidare” il sistema verifica se c'è un pacchetto ancora in consolidamento in cui quel documento può essere inserito tenuto conto dei vari criteri di formazione dei pacchetti: se non c'è ne istanzia uno nuovo e vi inserisce il documento. In questo processo di consolidamento, se nei metadati del documento è specificata, in apposito tag del SIPManifest, l'appartenenza ad un aggregato, ad esempio un fascicolo, il sistema di conservazione cerca di mantenerlo “unito” nella formazione dei pacchetti, cercando di mettere nello stesso pacchetto tutti i documenti relativi allo stesso aggregato (compatibilmente con gli altri criteri di creazione pacchetti configurati). Lo stesso fa per i documenti relativi alla medesima scheda documento (es file principale di una registrazione di protocollo e suoi allegati).

[Torna al sommario](#)

7.5.1 Creazione Indice di Conservazione

L'attività di chiusura dei pacchetto in consolidamento, ovvero di creazione dei relativi Indici di Conservazione conformi al UNI 11386:2010 Standard SInCRO, è svolta per lo più in modo automatico, ma se necessario, in rari casi, può essere forzata manualmente dal RdSC o suo delegato. La chiusura manuale dei pacchetti si rende necessaria ad esempio se essi contengono documentazione fiscalmente rilevante con numerazione progressiva interrotta.

Quando viene predisposto l'Indice di Conservazione, il pacchetto cambia stato da “in consolidamento” a “chiuso”: non vi si possono più aggiungere documenti e il file xml dell'Indice, una volta completato, è disponibile in apposita interfaccia WEB per essere firmato e marcato temporalmente dal RdSC o suo delegato.

La chiusura manuale di un pacchetto può comunque essere fatta in qualsiasi momento dal RdSC o suo delegato; egli dispone di un'apposita GUI attraverso cui non solo vede e può chiudere manualmente tutti i pacchetti in consolidamento ma può anche procedere a mano a modificare la composizione – i documenti – dei pacchetti in consolidamento o a creare nuovi pacchetti.

Negli indici di conservazione, oltre alle impronte e ai dati identificativi dei documenti digitali vengono riportati:

- gli URI che puntano allo stream dei componenti digitali di ciascun documento sullo storage del sistema: l'URI permette il reperimento certo dei file ma non è un path assoluto, cosicché qualora i

file dovessero essere riversati (riversamento diretto) su altro storage l'URI può non cambiare, il che costringerebbe a riformare e certificare nuovamente i PdA contenenti quei documenti;

- nel tracciato dell'Indice per ogni documento viene riportato l'XML che costituisce il pacchetto di archiviazione della scheda documento di appartenenza (quello anche archiviato su storage): in questo modo, attraverso la firma e marcatura, viene anche congelata la situazione dei dati del documento alla data di inizio della conservazione. Qualora i dati di un documento fossero aggiornati a seguito dell'invio di un SIP con aggiornamento dei dati del documento, i dati aggiornati verranno riportati nella banca dati relazionale e nell'AIP conservato su storage, mentre l'Indice di Conservazione attraverso cui è conservato il documento resterà invariato, quale fotografia dello stato del documento al momento dell'avvio della conservazione.

[Torna al sommario](#)

7.5.2 Certificazione PdA (firma e apposizione riferimento temporale)

La fase di certificazione del PdA ha come scopo quello di completare il processo di conservazione perfezionando l'Indice di Conservazione attraverso l'apposizione della firma digitale del RdSC e l'apposizione di un riferimento temporale.

Le attività di certificazione dei PdA consistono pertanto in questi passaggi:

- individuazione da parte del Sistema di Conservazione dei PdA chiusi che devono essere firmati
- segnalazione della lista al Responsabile del servizio di conservazione. Questa operazione può avvenire tramite notifica al Responsabile via posta elettronica.

Una volta che il Responsabile del servizio di conservazione o suo delegato ha firmato il PdA, se il PdA che in base alla normativa vigente prevede una seconda firma dell'Indice di Conservazione (da parte di un notaio o di un pubblico ufficiale), il Sistema di Conservazione gestisce anche questa casistica e inserisce il PdA che manca della seconda firma in un apposito elenco di PdA in attesa della seconda firma.

Quando sull'Indice di Conservazione viene apposta una delle firme previste nella busta crittografica viene inserito il riferimento temporale – signing time – che attesta quando è stata effettuata la firma. Il tipo di firma che viene apposta è CADES-BES con profilo specifico della conservazione a lungo termine.

A questo punto il processo di conservazione è concluso ai sensi di quanto previsto dalla norma.

[Torna al sommario](#)

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

7.6.1 Funzionalità di ricerca

Le GUI del portale DiGiDoc consentono di ricercare la documentazione presa in carico da DiGiDoc attraverso tutti i dati specificati nel pacchetto di versamento nonché attraverso i dati acquisiti dai documenti durante il loro ciclo di vita in DiGiDoc (data di versamento in conservazione, data di accettazione in conservazione, data inizio conservazione ecc).

Le GUI di ricerca sono progettate e realizzate per offrire un accesso:

- sicuro
- semplice
- guidato

- adeguato alle esigenze

La sicurezza dell'accesso è garantita attraverso:

- accesso autenticato alle GUI del portale
- gestione delle richieste di accesso alla documentazione e del relativo iter
- gestione di diversi livelli di sicurezza sulla documentazione.

Attraverso questi meccanismi il sistema garantisce che ognuno acceda solo alla documentazione e alle informazioni cui è autorizzato.

La semplicità dell'accesso è principalmente ottenuta attraverso l'adozione del motore di indicizzazione con cui vengono indicizzati sia il testo dei documenti digitali (eventualmente anche quelli cartacei, previa loro digitalizzazione e sottomissione a processo di OCR) che i metadati (almeno quelli più significativi): in questo modo in una modalità semplice e intuitiva – per così dire google like – è possibile effettuare una ricerca per parole che agisce sia sui metadati che sul contenuto dei documenti (ricerca full-text). Al tempo stesso DIGIDOC permette di adeguare la modalità di accesso alle esigenze di chi ricerca: infatti consente di impostare filtri di ricerca “strutturati” – con operatori di uguaglianza, somiglianza, maggiore, minore, compreso tra, valorizzato e non valorizzato - su tutti i principali metadati della documentazione conservata, inclusi quelli specifici di certe tipologie documentali.

Permette altresì di ricercare la documentazione navigando le diverse strutture gerarchiche – piano di classificazione, articolazione dell'archivio in serie, sottoserie ecc, indici tematici, organigramma dell'Ente produttore – secondo cui la documentazione è organizzata o alle quali si raccorda.

Dalla lista dei risultati che rispondono ai criteri di ricerca impostati, è possibile accedere al dettaglio dei singoli documenti visualizzando:

- il/i file che compongono il documento
- i metadati trasmessi dal versatore
- i metadati calcolati dal sistema in fase di versamento
- l'esito dei singoli controlli eseguiti
- le informazioni del PdA di appartenenza del documento (stato del PdA, descrizione, data creazione, etc)

L'accesso ai documenti è riservato agli utenti autorizzati, secondo le regole impostate nel sistema.

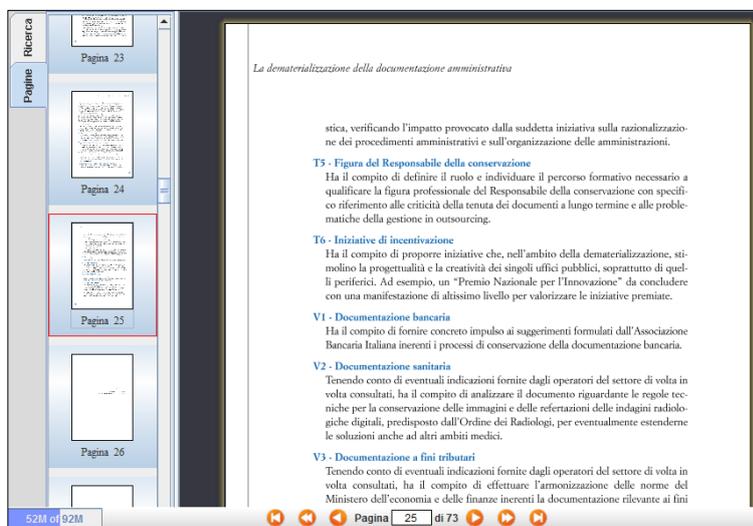


Figura 5 - Visualizzazione documento

[Torna al sommario](#)

7.6.2 Funzionalità di esibizione

Per l'esibizione dei documenti conservati nelle forme prescritte dalla norma il sistema di conservazione ad oggi provvede:

- in cooperazione applicativa, dei web service che in modo completamente automatizzato consentono di recuperare uno o più documenti conservati da parte del sistema/applicativo che li ha versati in conservazione o altri applicativi con opportuni diritti di accesso, unitamente, se richiesti, alle prove di conservazione (Indice di Conservazione firmato e marcato) e/o all'attestato di conformità all'originale conservato e/o ai viewer/reader necessari alla lettura dei componenti digitali dei documenti;
- attraverso le web GUI con cui RdSC e suoi delegati nonché personale abilitato dei soggetti produttori possono visionare la documentazione conservata.

[Torna al sommario](#)

7.6.2.1 Esibizione in cooperazione applicativa

Si tratta della modalità tramite cui i sistemi o applicativi che hanno inviato in conservazione i loro documenti possono ottenere dal Sistema di Conservazione, in cooperazione applicativa, l'esibizione di uno o più documenti conservati.

Tale modalità di esibizione viene implementata attraverso servizi – web services – in cui i DIP restituiti sono realizzati ancora una volta come dei file archivio – zip o tar.gz - che contengono:

- un file manifest.xml con i metadati del documento e i puntamenti ai suoi componenti digitali
- i componenti digitali del documento

L'esibizione tramite cooperazione applicativa prevede di poter specificare le seguenti opzioni:

- indicazione se deve essere inserito nel DIP anche il viewer o reader relativo al formato del documento (per un dato sistema operativo specificato)
- indicazione se è richiesto anche l'Indice di Conservazione attestante che il documento è conservato secondo norma
- indicazione se è richiesta anche la ricevuta di conformità all'originale conservato

Qualora siano stati richiesti il viewer/reader e/o l'Indice di conservazione e/o la ricevuta di conformità anch'essi vengono inseriti nell'archivio compresso che implementa il DIP.

L'esibizione tramite cooperazione applicativa può essere fatta per più documenti con un'unica invocazione del servizio. Infatti nella richiesta di esibizione si può indicare anche:

- una lista di documenti
- uno o più aggregati di documenti (fascicoli, cartelle, serie ecc)

al fine di ottenere che il DIP restituito contenga metadati e componenti digitali di tutti i documenti della lista, ovvero di tutti i documenti appartenenti alla/e aggregazioni di documenti specificate.

Per l'esibizione in cooperazione applicativa è prevista una duplice modalità di interazione per il sistema/applicativo che sottomette la richiesta:

- sincrona, quando il richiedente resta in attesa della risposta contenente il DIP. Consente l'esibizione di un solo documento alla volta, ed è ammessa solo per documenti di dimensione inferiore ad una soglia prestabilita; qualora la dimensione del documento richiesto superi il valore soglia la richiesta viene respinta.
- asincrona, quando a fronte dell'invocazione del servizio il richiedente ottiene solo un ticket di richiesta con il quale, in un momento successivo, va a richiedere lo stato della sua richiesta e l'eventuale risultato – il DIP – qualora la richiesta sia stata evasa.

L'xml di richiesta delle due modalità, con le possibili opzioni previste, sono rispettivamente i tag RequestEsibizioneSync e RequestEsibizioneAsync dell'xsd RequesteEsibizione.xsd la cui documentazione di dettaglio è nell'allegato *Allegato3 - RequestEsibizione.pdf*

L'xml di risposta nelle due modalità nonché quello del manifest del DIP (nel caso di esibizione asincrona), sono rispettivamente descritti dai tag ResponseEsibizioneSync, ResponseEsibizioneAsync, ResponseGetDIP e DIP dell'xsd ResponseEsibizione.xsd la cui documentazione di dettaglio è nell'allegato *Allegato4 - ResponseEsibizione.pdf*

[Torna al sommario](#)

7.6.2.2 Esibizione on-line

Questa modalità di esibizione prevede che dalle GUI web di DigiDoc si visualizzi il documento direttamente all'interno della pagina web. Tale modalità di esibizione è disponibile solo per i documenti in formati pdf o formati Office e ascii convertibili in PDF: infatti prevede la conversione in pdf effettuata a carico del sistema di conservazione.

Se il documento è firmato digitalmente e in particolare se si tratta di una busta crittografica di tipo p7m o tsd o m7m, il sistema esibisce il contenuto della busta depurato della/e firme digitali: di ciò viene data evidenza all'utente che a fianco dell'area in cui visualizza il documento vede le informazioni sulle firme ad esso associate: stato di validità (con dettaglio relativo ai vari livelli di controllo della validità); estremi dei certificati di firma; date ed estremi delle eventuali marche temporali presenti nella busta. Peraltro le informazioni sulle firme e sulle marche temporali apposte sul documento vengono mostrate anche in caso di buste crittografiche pdf (PadES) e xml (XAdES) come pure in caso di firma e/o marche detached.

Questa modalità di esibizione è pensata per allargare la fruibilità dei documenti nei casi in cui:

- per il client non vi sia un viewer/reader in grado di restituirgli il documento nel formato originale;
- l'utente che chiede la visualizzazione non voglia o non possa installare sul proprio client il viewer o reader necessario alla restituzione del documento digitale nel formato originale in cui è conservato

Quando viene utilizzata questa modalità di visualizzazione, se il formato di conservazione del file non è pdf, il sistema dà evidenza del fatto che si tratta di una copia non conforme all'originale conservato e riporta tutte le informazioni del formato originale di conservazione (mimetype, eventuale versione ecc.).

[Torna al sommario](#)

7.6.2.3 Esibizione tramite download da web GUI

Questa modalità di esibizione viene attivata dalla stessa interfaccia web da cui che consente l'esibizione on-line del documento (illustrata nel § precedente). In questo caso però il documento digitale non viene visualizzato all'interno di una pagina web, bensì previo scarico – download – del/i file che lo compongono: dopo di che il client che li ha scaricati può visualizzarli off-line.

7.6.2.4 Esibizione di singolo documento

Laddove viene reso disponibile il download del/dei file del documento vengono date le seguenti possibilità/opzioni:

- link attraverso cui scaricare anche il viewer o reader corrispondente al formato del documento: se per il dato formato DigiDoc dispone di più viewer o reader per diverse piattaforme e sistemi operativi, vengono forniti altrettanti link, indicando per ognuno la piattaforma a cui si riferisce. Da notare che in caso di documenti che siano buste crittografiche p7m, tsd o m7m, il sistema propone lo scarico del/i viewer o reader relativi al formato del file contenuto nella busta crittografica
- in caso di documento firmato digitalmente che sia una busta crittografica p7m, tsd o m7m, vengono forniti due link, uno per scaricare la busta e uno per scaricarne il contenuto depurato delle firme (il file “sbustato”)
- nel caso di documenti con firme e/o marche temporali *detached* o comunque formati da più componenti digitali (i.e. più file) il sistema dà un'opzione per scegliere se effettuare lo scarico di tutti i componenti digitali come un unico file archivio (zip o tar, a scelta)
- scelta se scaricare o meno anche il file xml “Indice di Conservazione”, firmato dal Responsabile del servizio di conservazione (o suo delegato) e marcato temporalmente, attestante la conservazione a norma del documento
- per alcuni formati viene data la possibilità, esattamente come nella visualizzazione on-line, di ottenere il documento digitale convertito in formato PDF o PDF/A - che non è quello di conservazione - e di scaricare quest'ultimo: in questo caso l'utente viene avvertito che si tratta di una versione in formato diverso da quello di conservazione
- il sistema consente di scaricare la ricevuta di “conformità all'originale conservato” del documento, ovvero un PDF/A che contiene: i riferimenti dell'Ente produttore; gli estremi e i principali dati descrittivi del documento; un timbro digitale – codice a barre bidimensionale - contenente le impronte del/dei componenti digitali del documento

[Torna al sommario](#)

7.6.2.5 Esibizione tramite Stampa

Anche questa modalità di esibizione è messa a disposizione dalle GUI web di DigiDoc: laddove sono rese disponibili l'esibizione online e il download del/dei file del documento (esibizione tramite download) è data anche una funzione per effettuarne la stampa: selezionandola il sistema attiva la stampa dei file sul client – purché questo sia già dotato dei programmi necessari ad aprire e mandare in stampa quei file – ed eventualmente, se richiesto, la fa seguire dalla stampa della ricevuta di conformità.

L'esibizione tramite stampa, come quella tramite download, può essere effettuata anche contestualmente per più documenti: una volta effettuata la selezione dei documenti di interesse, con un'unica operazione, si può richiedere la stampa su carta di tutti i documenti selezionati (e delle relative ricevute di conformità).

[Torna al sommario](#)

7.6.2.6 Esibizione telematica

DigiDoc prevede anche l'esibizione telematica dei documenti attraverso canale e-mail, PEC o ordinaria.

La richiesta di esibizione telematica si effettua dalla stessa interfaccia web dalla quale si richiamano le modalità di esibizione on-line e tramite download e tramite stampa.

Per chi effettua la richiesta deve essere noto un indirizzo e-mail a cui indirizzare l'esibizione, o altrimenti il richiedente deve fornirlo al volo nel momento in cui sottometta la richiesta di esibizione.

L'esibizione via e-mail avviene attraverso caselle e-mail, ordinarie o di PEC, che sono state messe a disposizione di DigiDoc. L'esibizione via e-mail è disponibile solo per i documenti la cui dimensione è inferiore ad una soglia prestabilita (una dimensione ragionevole per l'allegato di una e-mail). Infatti l'e-mail di esibizione contiene come allegati:

- i file che compongono il documento;
- la ricevuta di conformità, se richiesta;
- un Manifest.xml con i metadati del documento, se richiesto.

Il corpo della mail spiega il significato di ciascun allegato, mentre il suo oggetto riporta gli estremi identificativi del documento e la data e ora in cui ne è stata richiesta l'esibizione.

[Torna al sommario](#)

7.6.2.7 Esibizione di copia conforme all'originale conservato a norma

Il rilascio di copia conforme di un documento conservato viene realizzata da DigiDoc attraverso la produzione della "ricevuta di conformità all'originale conservato", ovvero un PDF/A recante, oltre che la dichiarazione di conformità all'originale conservato, anche un timbro digitale contenente la/le impronte dei file che compongono il documento. Tale timbro è realizzato come codice a barre bidimensionale: sono disponibili SW freeware che consentono di interpretare il contenuto di questi codici a barre (anche da un'immagine che è la scansione della ricevuta stampata su carta) e quindi di recuperare le impronte del documento riportate nel timbro al fine di verificare che coincidano con le impronte calcolate sulla copia del documento che è stata rilasciata.

Se la ricevuta viene firmata, digitalmente o su carta (una volta stampata), questo vale a fornire quella garanzia di autenticità della stessa che consente di realizzare un rilascio di copia conforme ai sensi di quanto previsto dalla legge.

La firma sarà apposta da un pubblico ufficiale le cui modalità di coinvolgimento sono descritte nel paragrafo 4.4. Per ogni cliente, nel contratto di affidamento, viene regolamentata l'attività del pubblico ufficiale.

[Torna al sommario](#)

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

Dalle web GUI che DiGiDoc mette a disposizione è possibile selezionare uno o più documenti e aggregati di documenti al fine di richiedere un pacchetto di distribuzione contenente tutta la documentazione selezionata. Una volta acquisita la richiesta DiGiDoc attiva in modo asincrono l'elaborazione del DIP richiesto e quando questo è pronto rende scaricabile il DIP da apposita GUI in cui il richiedente consulta lo stato delle richieste di esibizione effettuate. Il DIP è un archivio compresso che oltre ai documenti richiesti contiene un file indice conforme allo schema documentato in *Allegato4 - ResponseEsibizione.pdf*

Nei casi previsti dalla normativa, la firma sarà apposta da un pubblico ufficiale le cui modalità di coinvolgimento sono descritte nel paragrafo 4.4. Per ogni cliente, nel contratto di affidamento, viene regolamentata l'attività del pubblico ufficiale.

[Torna al sommario](#)

7.8 Scarto dei pacchetti di archiviazione

Un obiettivo importante per il sistema è quello di dare supporto, oltre che alla conservazione, anche al processo di selezione e scarto di ciò che non deve più essere conservato perché sono trascorsi i tempi di conservazione stabiliti.

Salvo casi particolari in cui il tempo di conservazione è esplicitato sul singolo documento o aggregazione di documenti al momento dell'invio in conservazione, in generale il tempo di conservazione della documentazione non è esplicitato e viene determinato dal sistema sulla base del massimario di selezione e scarto che stabilisce le regole e i tempi di conservazione agganciandoli ad uno o più dei seguenti dati di definizione del contesto:

- tipologie dei documenti e loro aggregati;
- voci del piano di classificazione;
- tipologie dei procedimenti da cui scaturiscono i fascicoli.

Da notare che laddove non specificato e non ricavabile dalle regole configurate il tempo di conservazione della documentazione viene considerato implicitamente “per tempo illimitato”.

Così determinato il tempo di conservazione, DigiDoc è in grado di fornire una proposta di scarto che può essere modulata opportunamente istruendo DigiDoc in merito alla “granularità” dello scarto che si vuole effettuare:

- intere unità di aggregazione (fascicoli o serie)
- singoli documenti.

A partire dalla proposta predisposta in automatico l'archivista redige la proposta di scarto definitiva e la sottomette alla Sovrintendenza per autorizzazione. La Sovrintendenza verifica la documentazione contenuta nella proposta e seleziona quella di cui autorizzare lo scarto.

Nel caso la documentazione candidata allo scarto sia di particolare interesse culturale, DiGiDoc prevede di poter richiedere ed acquisire un'ulteriore autorizzazione allo scarto da parte del Ministro dei Beni e delle attività culturali e del turismo.

Quando viene acquisita l'autorizzazione allo scarto, gli AIP e i documenti digitali corrispondenti alla documentazione scartata vengono rimossi dallo storage; quanto ai metadati della documentazione scartata memorizzati su RDBMS essi vengono spostati in aree logiche – i.e. tabelle – dedicate alla documentazione scartata e

- perdono le informazioni di stabilità e di pacchetto (diventano inutili dal momento che i documenti digitali vengono fisicamente eliminati), e nelle informazioni di pacchetto vengono aggiunte le informazioni relative all'autorizzazione allo scarto
- perdono le informazioni di rappresentazione (ormai inutili, a fronte dell'eliminazione fisica dei documenti)
- acquisiscono delle nuove informazioni, quelle relative allo scarto (data, autorizzato da chi).

[Torna al sommario](#)

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

Il sistema DiGiDoc rispetta lo standard OAIS; pertanto è in grado di esportare secondo lo schema documentato in *Allegato4 - ResponseEsibizione.pdf* i pacchetti di archiviazione conservati in pacchetti seguendo le regole che permettono la loro importazione in un altro sistema aderente allo standard OAIS.

Allo stesso modo il sistema DiGiDoc è in grado di importare e archiviare pacchetti di distribuzione generati da altri sistemi aderente allo standard OAIS.

L'esportazione dei pacchetti di conservazione può essere effettuata su supporto elettronico in formato ZIP. Il cliente può scaricare i pacchetti utilizzando un'interfaccia WEB messa a disposizione dal sistema DiGiDoc.

[Torna al sommario](#)

7.10 Riversamento diretto e sostitutivo

DiGiDoc prevede le funzionalità di riversamento diretto e sostitutivo che servono a garantire la conservazione della documentazione anche nel medio e lungo termine e che sono implementate secondo quanto previsto dalle normative in vigore.

[Torna al sommario](#)

7.10.1 Riversamento diretto

DiGiDoc prevede le funzioni che consentono al Responsabile del servizio di conservazione, su propria iniziativa o su richiesta di un soggetto produttore, di schedare il riversamento diretto di tutti i documenti che risiedono su un certo storage / dispositivo di memorizzazione piuttosto che di una particolare selezione di documenti: dovrà naturalmente indicare quale/i sono i nuovi supporti fisici di memorizzazione. Tali funzioni consentono anche, dove i supporti di memorizzazione di provenienza lo consentano, di specificare se il riversamento deve spostare i documenti al nuovo supporto di memorizzazione o piuttosto farne una copia mantenendo quella sul vecchio supporto.

Tutte le informazioni relative ai riversamenti diretti che un documento ha subito durante la sua conservazione in DIGIDOC vengono man mano ad arricchire il set di metadati contenuti nell'AIP del documento.

[Torna al sommario](#)

7.10.2 Riversamento sostitutivo

Secondo quanto specificato dalle normative, il riversamento sostitutivo è il "processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica" (Delibera CNIPA 11/2004 art. 1 comma 1).

Nel momento in cui un formato diventa obsoleto, ovvero quando è prossimo a non essere più leggibile, vengono messe a disposizione del Responsabile del servizio di conservazione delle funzioni di riversamento sostitutivo atte a migrare ad altro formato i documenti già conservati a norma che hanno il formato obsoleto.

Tutte le informazioni relative ai riversamenti sostitutivi, come già quelle relative ai riversamenti diretti, che un documento ha subito durante la sua conservazione in DIGIDOC vengono man mano ad arricchire il set di metadati contenuti nell'AIP del documento (oltre che essere memorizzate negli audit trail generali del sistema): in particolare di ogni riversamento sostitutivo vengono memorizzati nell'AIP i

formati originale e di destinazione e gli eventuali dettagli sul formato originale (versione, rischi connessi ecc).

[Torna al sommario](#)

8. IL SISTEMA DI CONSERVAZIONE

Le componenti del sistema di conservazione di seguito descritte sono intese sia per gli ambienti di collaudo che per quelli di produzione che sono separati e indipendenti.

8.1 Componenti Logiche

I processi sopra illustrati corrispondono ad altrettanti gruppi di servizi applicativi previsti dalla soluzione DigiDoc:

- **DigiDocWePo (versamento):** permettono l'invio della documentazione, sia singoli documenti che loro eventuali aggregazioni, al sistema di conservazione nonché l'aggiornamento di quanto già inviato in precedenza;
- **DigiDocCtrl:** svolgono i controlli sulla documentazione inviata in conservazione, necessari per l'accettazione da parte del sistema di conservazione. Sono controlli sia sui dati di descrizione che sui componenti digitali (file) da conservare, in particolare sui loro formati e su eventuali firme digitali e marche temporali;
- **DigiDocCons:** comprendono le funzionalità espressamente richieste dalla normativa italiana per la Conservazione dei documenti;
- **DigiDocWeCS:** consentono le ricerche su tutto il materiale conservato nel sistema, sfruttando tutti i dati di descrizione della documentazione conservata come chiavi di ricerca;
- **DigiDocMoEs:** permettono di verificare la corretta funzionalità del sistema in tutti i suoi aspetti e componenti, consentendo al Responsabile del servizio di Conservazione ed eventuali autorità di vigilanza di assolvere ai propri compiti di verifica ordinaria e straordinaria;
- **DigiDocAdmi:** trasversali a tutto il sistema, consentono di aggiornare e storicizzare strumenti e dati di definizione del contesto che sono funzionali alla descrizione degli archivi (es. organigrammi, piani di classificazione, tipologie documentali, massimari di selezione e scarto)

L'architettura applicativa di DigiDoc, coerentemente con il modello di sviluppo a servizi (SOA), si compone di moduli separati, seppur interdipendenti, che a loro volta composti da servizi e funzionalità applicative, permettono di gestire i processi identificati. Questa separazione consente di installare le varie componenti su sistemi fisici differenti.

[Torna al sommario](#)

8.2 Componenti Tecnologiche

Schema e descrizione delle componenti tecnologiche (strumenti informatici a supporto delle funzionalità del sistema di conservazione) che implementano il sistema di conservazione.

8.2.1 Software di base

Ambiente
Java Runtime
SQL
JDK e JRE Compatibility level

[Torna al sommario](#)

8.2.2 Framework di sviluppo utilizzati

Nome	Utilizzo
JAX-WS (Java API for XML Web Services)	Per realizzare web-service – SOAP e REST – e client che utilizzano XML per comunicare
Jersey	Per realizzare web-service REST e i relativi client (è l'implementazione di riferimento della specifica JAX-RS)
Smart GWT	Framework di base per la realizzazione delle web UI: si occupa del rendering del framework ajax GWT appoggiandosi alle librerie Smartclient
Spring	Per realizzare i componenti come applicazioni java enterprise facilmente configurabili e altamente riusabili
Hibernate	ORM utilizzato per l'accesso al database

[Torna al sommario](#)

8.2.3 Scalabilità

Adottando una politica di scalabilità orizzontale sulla configurazione base il sistema viene configurato in più nodi applicativi bilanciati da un load Balancer, in modo da distribuire il carico su più nodi e fornire meccanismi di fault avoidance, oltre che rendere il sistema più affidabile e ridurre il down-time dello stesso.

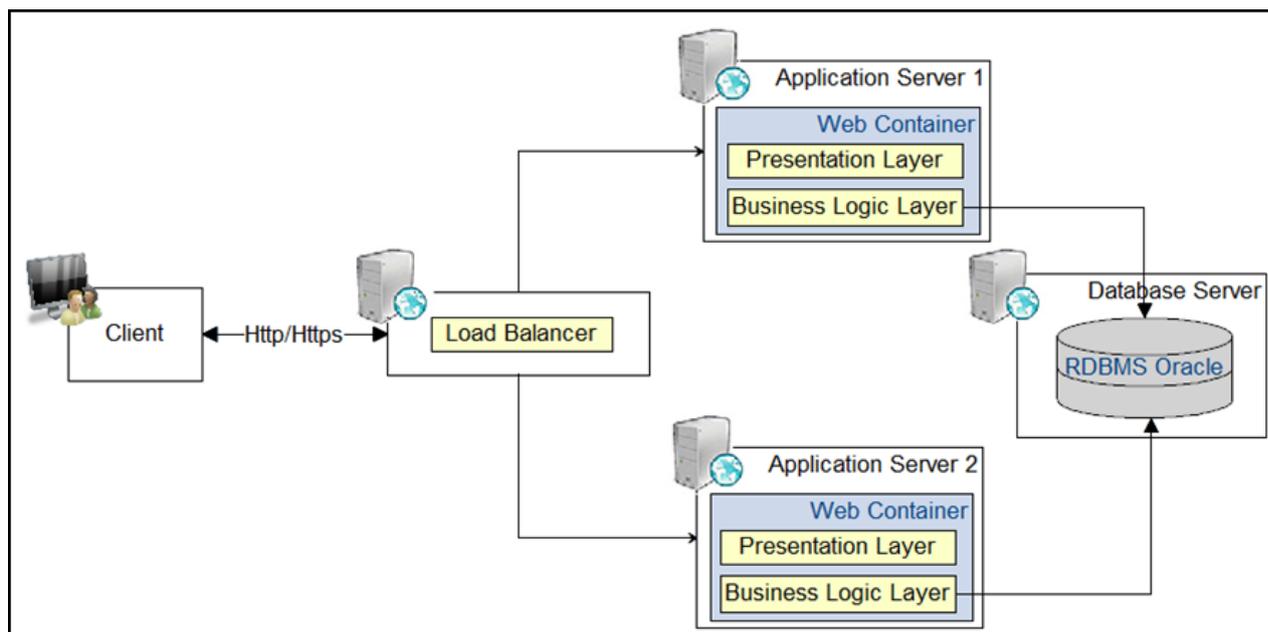


Figura 6 - Configurazione del sistema con un 1° livello di scalabilità

Tale suddivisione non comporta nessuna modifica all'applicativo, ma occorre solamente configurare il load balancer in modo che punti ai vari nodi application server. Sui nodi application server sono installati sia il presentation layer che il business logic layer di tutti i componenti del sistema.

Passando ad un livello ulteriore di scalabilità orizzontale si passa ad una configurazione come quella illustrata nella figura successiva: anche in questo caso il sistema viene scalato senza dover modificare alcuna parte dell'applicativo, ma solamente modificandone le configurazioni.

In questa configurazione oltre al load balancer e alla divisione dell'applicativo su più nodi vengono suddivisi in nodi distinti il presentation layer dal business logic layer.

La comunicazione tra i due layer avviene tramite web service, principalmente in modalità RESTful, secondariamente anche SOAP.

In questa configurazione le chiamate ai web service del sistema da parte di altre applicazioni o altri moduli esterni creano carico di lavoro solo sugli application server contrassegnati dalla lettera b; viceversa delle chiamate alle web UI dei vari componenti del sistema (in particolare le UI di ricerca ed esibizione della documentazione conservata) vanno a creare carico di lavoro sia sugli application server contrassegnati dalla lettera a che su quelli contrassegnati dalla lettera b.

La configurazione potrebbe essere ulteriormente scalata separando su application server distinti i diversi moduli del sistema (naturalmente quelli che hanno dipendenze da altri verranno installati comprensivi delle librerie jar dei moduli da cui dipendono).

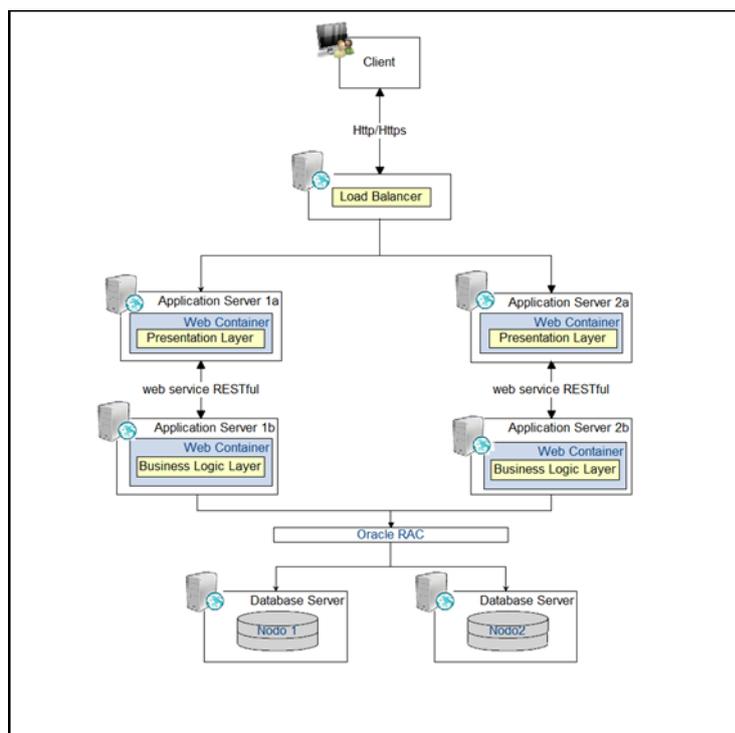


Figura 7 - Configurazione del sistema con un 2° livello di scalabilità

In figura viene anche illustrato come il sistema supporti una soluzione scalata orizzontalmente anche per ciò che riguarda il data layer, ovvero il database: infatti supporta la configurazione Real Cluster Application (RAC), in modo da aumentare la capacità transazionale del database, rendere il sistema più affidabile e ridurre il down-time.

Parimenti anche per lo storage dei file conservati l'architettura applicativa consente di distribuire lo storage su più container fisici (Oracle WCC o altri tipi di storage, anche non veloci ma solo ad alta affidabilità).

[Torna al sommario](#)

8.3 Componenti Fisiche

L'infrastruttura tecnologica necessaria per erogare le attività di conservazione è ospitata nei seguenti data center di Engineering D.HUB:

- Vicenza, Via Vecchia Ferriera 5: Data Center Primario ove risiedono i sistemi di conservazione, strutturato in modo da garantire la sicurezza logica e fisica, nonché i servizi di backup e monitoraggio.
- Pont Saint-Martin (AO), Viale C. Viola 76: Data Center secondario avente le stesse caratteristiche di sicurezza di quello primario ed utilizzato per erogare il servizio di Disaster Recovery (DR).

Il dettaglio degli asset come previsto dalla norma ISO/IEC:27001/2013 è descritto nel sistema ECMDB di Engineering D.HUB.

Gli schemi relativi all'ambiente di produzione e all'ambiente di collaudo sono di seguito riportati.

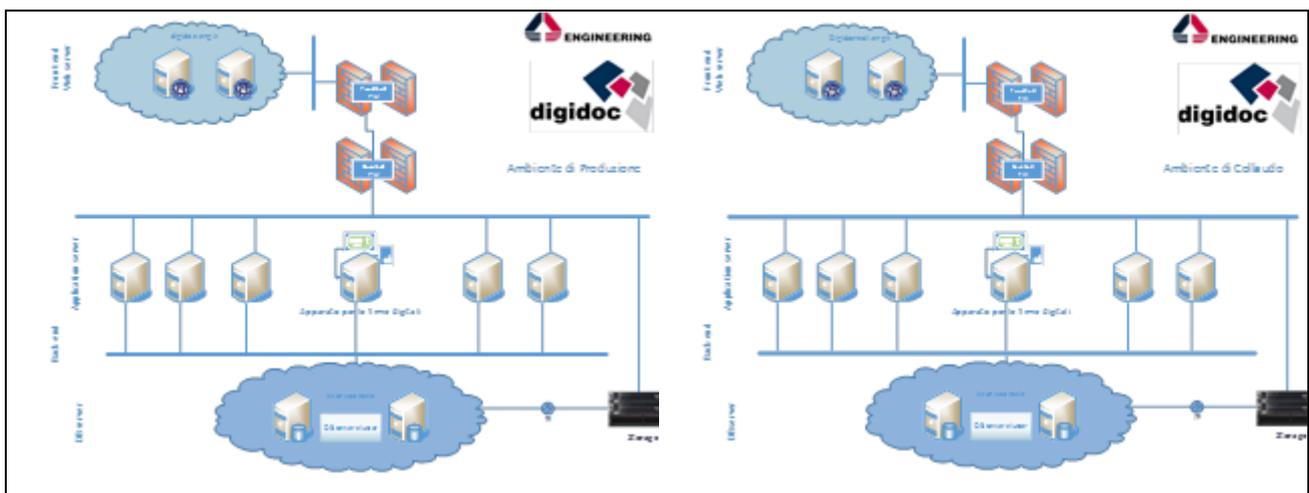


Figura 8 - Configurazione ambienti di collaudo e produzione

Le attività di gestione degli impianti presenti nei Data Center in cui viene erogato il servizio di conservazione, nonché le attività di gestione degli allarmi originati dalle piattaforme di monitoraggio impiantistica sono descritte nella procedura presente nel SGQ “RS08PR05 Procedura Gestione Impianti Data Center”. Tali attività hanno l'obiettivo di assicurare che:

- Gli impianti siano sempre in piena efficienza grazie ad una corretta manutenzione preventiva
- malfunzionamenti o “fault” siano immediatamente segnalati alle funzioni preposte, al fine di consentire un tempestivo avvio delle azioni di ripristino
- siano evidenziate eventuali situazioni critiche, che attestino degrado degli impianti o potenziali incidenti futuri.

In particolare, sono oggetto delle attività di gestione i seguenti impianti:

- Impianti elettrici (GE, UPS, trasformatore, quadri di sala);
- Impianti meccanici (condizionamento, pompaggio acqua, trattamento dell'aria, etc.)

- Impianti antincendio;
- Impianti di sicurezza (anti-intrusione, sorveglianza)

L'architettura degli impianti presenti nei DC delle aziende del Gruppo Engineering che ospitano l'archiviazione, è formalizzata in appositi schemi aggiornati e archiviati (in formato cartaceo e/o elettronico), a cura del Site Manager dello specifico DC.

Dal punto di vista organizzativo, le attività di controllo e gestione degli impianti del DC sono svolte da personale della funzione Infrastrutture DC di D.HUB (Site Manager ed eventuali collaboratori), mentre la parte "operativa" della manutenzione ordinaria/straordinaria è oggetto di apposito appalto a ditte specializzate.)

Gli accordi contrattuali che regolano le attività di manutenzione affidate a ditte esterne sono definiti e gestiti in armonia alla procedura aziendale PGA02 Gestione Ciclo Passivo.

Nei Data Center di Engineering D.HUB che ospitano gli ambienti per la conservazione, sono presenti le seguenti tipologie di infrastruttura:

- Infrastrutture elettriche
- Infrastrutture "meccaniche" (raffreddamento)
- Infrastrutture antincendio
- Infrastrutture di sicurezza

Il "perimetro" degli impianti è delimitato a monte dall'eventuale provider di servizi e a valle dal singolo apparato presente nei DC.

Appartengono alla categoria Infrastrutture Elettriche i seguenti impianti:

- tutte le linee elettriche, sia in bassa tensione (BT) che in media tensione (MT),
- tutti i quadri elettrici (generali e di distribuzione con i relativi rifasatori), sia in asservimento agli apparati come server, dischi, ecc. sia in asservimento ad altre tipologie di impianti sia "servono" al data center (es. impianto elettrico dei condizionatori),
- i sistemi di continuità assoluta (UPS statici e dinamici),
- i gruppi elettrogeni (compreso motore e cisterna carburante),
- le centraline che sovrintendono gli automatismi degli interruttori di potenza elettromeccanici,
- le "celle" di arrivo e partenza,
- i trasformatori MT/BT.

Appartengono alla categoria Infrastrutture Meccaniche tutti quegli impianti che permettono il raffreddamento delle sale tecnologiche:

- i condizionatori ad espansione diretta,
- i gruppi frigo ad acqua (comprese le unità di ventilazione interne alle sale),
- le torri evaporative,
- le pompe e i circuiti idraulici,
- il sistema di trattamento dell'acqua per le torri evaporative,
- le unità di trattamento dell'aria (UTA),
- valvole, termostati, filtri ecc., facenti parte integrante della macchina e relativi al corretto funzionamento degli apparati refrigeranti.

Fanno parte delle Infrastrutture Antincendio, tutti gli impianti di rivelazione e spegnimento:

- gli estintori manuali,
- le bombole di Azoto o Argon,
- i sensori di rivelazione fumi,
- le centraline che sovrintendono il funzionamento sensori di rivelazione fumo,
- l'impianto di estinzione automatica.

Fanno parte delle Infrastrutture di Sicurezza tutti gli impianti che assicurano la sicurezza perimetrale, quali l'impianto di sorveglianza TVCC e gli impianti anti-intrusione (porte allarmate).

Il servizio di manutenzione svolge le attività avvalendosi di figure professionali competenti, in armonia alle normative di Legge vigenti (ad es. DM 37/08, D.Lgs. 81/2008).

Le prestazioni vengono svolte nelle ore e nei giorni compatibili con le operazioni da compiere, senza comunque ostacolare le normali attività di erogazione dei servizi in corso. In caso di necessità di intervento di manutenzione, il DC Site Manager concorda con il personale di manutenzione orari e modalità per intervenire. Nel caso di interventi la cui interferenza con le attività di erogazione dei servizi non può essere evitata, il DC Site Manager concorda orari diversi da quelli di lavoro oppure orari notturni, in modo da minimizzare gli impatti.

E' cura del personale di manutenzione tenere aggiornata tutta la documentazione tecnica relativa alle apparecchiature in manutenzione.

Il Servizio di Manutenzione ha la responsabilità di organizzare il lavoro del proprio personale in garanzia del raggiungimento degli scopi prefissati (formalizzati nei documenti contrattuali che regolano il rapporto con i fornitori del servizio) e il rispetto dei tempi previsti, compresi eventuali turni di reperibilità, soprattutto per garantire un tempestivo intervento in caso di problemi su impianti/dispositivi i cui guasti potrebbero causare disservizi rilevanti, se non riparati prontamente.

Le operazioni di manutenzione da eseguire alle scadenze specificate sono registrate in un apposito calendario annuale riassuntivo (Cronoprogramma), nel quale si riportata la settimana nella quale è previsto l'intervento di manutenzione, l'apparato oggetto della manutenzione e il codice della scheda di manutenzione contenente la lista delle operazioni da effettuare.

Il Cronoprogramma deve essere verificato ed aggiornato ogni qualvolta varia l'architettura degli impianti (e quindi anche la lista degli impianti in manutenzione) e comunque almeno con cadenza annuale.

- Gestione piattaforme di monitoraggio, in termini di riesame delle utenze; I risultati di tali riesami periodici devono essere formalizzati, nella misura in cui vi siano indicazioni per il periodo successivo o qualora costituiscano input all'esecuzione di altri processi aziendali (es. RS02 Processo Gestione Approvvigionamento, MS01 Processo Gestione Misurazioni Analisi Miglioramento).

[Torna al sommario](#)

8.4 Procedure di gestione e di evoluzione

Qui di seguito l'elenco delle procedure riguardanti la sicurezza del sistema di conservazione. Tali procedure fanno parte del Sistema di Gestione per la Qualità di Engineering, sono rese disponibili al personale coinvolto nelle attività sulla intranet aziendale, in considerazione del livello di riservatezza attribuito a ciascun documento.

Ambito	Descrizione sintetica	Nome della procedura
Sistema di Gestione per la Qualità	Manuale della Qualità di Engineering D.HUB e Manuale della Qualità di Engineering Ingegneria Informatica	D.HUB QM01 Manuale Qualità EII QM01 Manuale Qualità
Sistema di Gestione per la Qualità	Visione complessiva ed unitaria dei Processi Aziendali costituenti il Sistema di Gestione per la Qualità	QS01 Processo Gestione Sistema Qualità
Sistema di Gestione per la Qualità	Descrive la struttura documentale della Information Security Policy e le modalità con cui i documenti aziendali sono resi disponibili al personale coinvolto nelle attività, anche in considerazione del livello di riservatezza attribuito a ciascun documento. Alla base dei criteri di accessibilità degli elementi documentali vi è il principio del " <i>need to know, need to use</i> ": in base a tale principio, le informazioni devono essere disponibili esclusivamente per il personale che ha bisogno di conoscerle e di utilizzarle per motivi di lavoro.	QS01P01 Procedura Gestione documentale
Sistema di Gestione per la Qualità	La procedura descrive il flusso di creazione, modifica, rimozione delle utenze di tipo applicativo sulla piattaforma DigiDoc (nei vari ambienti a disposizione), di gestione delle password per garantire tali accessi, nonché indicazioni sugli oggetti e le modalità di gestione dei log applicativi	RS09P01 Procedura Gestione Utenze Applicative DigiDoc
Sistema di Gestione per la Qualità	La procedura descrive le modalità con cui si gestiscono gli interventi correttivi e/o evolutivi sulla piattaforma DigiDoc, in garanzia dell'efficacia dell'intervento stesso, e in modo da assicurarne la tracciatura.	RS09P02 Procedura di Manutenzione Correttiva / Evolutiva DigiDoc
Impostazione, implementazione e gestione della Sicurezza delle Informazioni	Politica per la Sicurezza delle Informazioni: documenti di riferimento per la descrizione generale delle modalità adottate da Engineering ed Engineering D.HUB per la gestione della Sicurezza delle Informazioni. il primo documento è applicabile al	RS08A02 Information Security Policy RS09A01 Information Security Policy – Conservazione Digitale

	<p>perimetro dei servizi erogati da Engineering D.HUB (outsourcing infrastrutturale), mentre il secondo documento si applica al perimetro relativo all'erogazione del servizio di Conservazione dei Documenti Informatici, incluse le attività di manutenzione della Piattaforma DigiDoc.</p> <p>Quanto descritto nel documento è mandatorio sia per i processi che vengono gestiti ed eseguiti interamente all'interno del contesto aziendale, sia per quei processi che prevedono il coinvolgimento di terze parti (es. che coinvolgono Clienti, Partner, Fornitori).</p> <p>I documenti citati forniscono le linee guida e i rimandi a procedure aziendali di dettaglio per la assicurare la Sicurezza delle Informazioni all'interno dei due perimetri di riferimento (Outsourcing Infrastrutturale ed erogazione del Servizio di Conservazione Documenti Digitali). Essi danno evidenza, inoltre, del rispetto delle misure minime previste dal D.Lgs.196/2003.</p>	
<p>Impostazione, implementazione e gestione della Sicurezza delle Informazioni</p>	<p>censimento dei controlli e obiettivi di controllo adottati da Engineering D.HUB (per il perimetro relativo all'Outsourcing Infrastrutturale) e da Engineering Ingegneria Informatica (per il perimetro relativo all'erogazione del Servizio di Conservazione dei Documenti Informatici), per garantire la Sicurezza delle Informazioni, inclusa la motivazione di eventuali esclusioni.</p>	<p>RS08A07 Dichiarazione di Applicabilità</p> <p>RS09A02 Dichiarazione di Applicabilità – Conservazione dei Documenti Informatici</p>
<p>Impostazione, implementazione e gestione della Sicurezza delle Informazioni</p>	<p>Definizione di modalità di comunicazione tra Engineering D.HUB e il Cliente Engineering – DigiDoc durante l'erogazione dei servizi. Garantisce che le informazioni a perimetro siano adeguatamente protette secondo appropriati livelli di riservatezza, la disponibilità delle adeguate istruzioni di lavoro al personale</p>	<p>RS0802P01 Procedura Service Transition</p>

	sulla base del principio "need to know"	
Aspetti Organizzativi	<p>Descrive le Modalità con cui Engineering D.HUB ed Engineering (per il perimetro relativo al Servizio di Conservazione dei Documenti Informatici) interagisce con le Pubbliche Autorità nel caso di circostanze configurabili come reato informatico. Si garantisce che i contatti con le Autorità competenti, in caso di circostanze rilevanti per la Sicurezza delle Informazioni aventi impatto legale, siano gestiti in modo uniforme da una interfaccia ufficialmente incaricata dall'Azienda.</p>	<p>RS0803P02 Procedura Contatti con Autorità</p> <p>RS09A01 Information Security Policy – Conservazione Digitale</p>
Aspetti Organizzativi	<p>Descrive le attività di gestione del personale nel ciclo di vita del rapporto lavorativo per garantire che il personale che sarà coinvolto nella erogazione dei Servizi abbia i requisiti (anche di affidabilità) adeguati per gestire le attività, nel rispetto della Sicurezza delle Informazioni. Il personale deve essere reso consapevole delle proprie responsabilità in termini di sicurezza delle informazioni.</p> <p>È necessario evitare che, al momento della fuoriuscita del personale, siano trattenuti indebitamente asset e informazioni aziendali.</p>	PGP09 Gestione Risorse Umane
Security awareness e professionalità del personale	<p>Descrive le modalità con cui viene garantita la formazione e l'awareness sulla Sicurezza delle Informazioni e su specifici aspetti legati alle procedure aziendali, per il personale coinvolto nei Servizi</p>	PGP02 Procedura Gestione Esigenze Formative
Aspetti Organizzativi	<p>Garantisce che vengano presi adeguati provvedimenti nei confronti di chi commette infrazioni alla sicurezza delle informazioni</p>	CCNL Metalmeccanici
Aspetti Organizzativi	<p>Descrizione delle modalità con cui sono assegnati, modificati e rimossi i privilegi di accesso fisico/logico per locali/sistemi/apparati/applicazioni a perimetro.</p>	RS0803P03 Procedura Gestione Privilegi di Accesso
Aspetti Organizzativi	<p>Assunzione di responsabilità per la sicurezza delle informazioni da parte del</p>	RS08D02 Non Disclosure Agreement

	<p>personale esterno coinvolto nella erogazione di Servizi</p> <p>Il personale deve essere reso consapevole delle proprie responsabilità in termini di sicurezza delle informazioni</p>	
Aspetti Organizzativi	<p>Descrive le modalità di accesso a ciascun DC per garantire che l'accesso ai locali indicati (sale macchine/CED) avvenga solo da parte del personale autorizzato sulla base del principio "need to use", nonchè il controllo degli accessi fisici alle aree ove si trattano informazioni riservate.</p> <p>Garantisce inoltre che, in occasione di carico-scarico merci, non vi siano intrusioni di personale non autorizzato nei locali del perimetro.</p>	RS08A05 Accessi Fisici a Data Center
Gestione controllata accessi fisici e logici	<p>Politiche di tracciatura e conservazione dei log di accesso fisico e logico alle informazioni a perimetro per consentire l'analisi di dati in occasione di eventi critici (manomissioni, accessi non autorizzati, etc.) su asset/locali del perimetro.</p> <p>Definisce i controlli degli accessi fisici alle aree ove si trattano informazioni riservate.</p> <p>Descrive le modalità in cui sono preservati i dati di accesso fisico/logico da modifica, cancellazione, non tracciatura per superamento capienza sul sistema nativo.</p>	RS08A03 Log Management Policy
Gestione controllata accessi fisici e logici	<p>Definisce le regole di utilizzo della dotazione hw/sw in uso al personale e le regole da seguire per lo scambio di informazioni. Definisce l'utilizzo della modalità di connessione wireless in modo che avvenga in modalità sicura solo da parte delle persone autorizzate e in garanzia della RID</p>	<p>RS08A06 Utilizzo servizi informatici e trasmissione informazioni</p> <p>RGP01 Regolamento Uso Risorse Aziendali</p>
Gestione controllata accessi fisici e logici	<p>Elenco delle tecnologie e gli strumenti autorizzati (e quelli espressamente vietati) dal Management a supporto della erogazione dei Servizi erogati da Engineering D.HUB</p>	RS08A04 Tecnologie e Strumenti Autorizzati
Sicurezza dei	<p>Fornisce le indicazioni per identificare,</p>	RS0805P01 Procedura Incident

sistemi e degli asset	classificare, gestire e risolvere le situazioni direttamente individuabili come incidenti di Information Security oppure che, degenerando o aggravandosi, potrebbero diventare tali.	Management
Impostazione, implementazione e gestione della Sicurezza delle Informazioni	<p>Descrive il processo di Change Management per la gestione dei cambiamenti a servizi o a componenti di servizio. L'obiettivo primario di questo processo è quello di gestire i cambiamenti ai servizi ICT o alle componenti di servizio, in maniera sistematica, organica e controllata con la finalità di ridurre, per quanto possibile, i rischi ed eventuali disservizi correlati all'implementazione del cambiamento. Deve essere garantito un adeguato livello di controllo e autorizzazione in occasione di modifiche a servizi o componenti di servizi, aventi impatto anche sulla sicurezza delle informazioni.</p> <p>Il primo documento citato si applica ai servizi di Outsourcing infrastrutturale erogati da Engineering D.HUB, mentre il secondo si applica alle modifiche apportate alla piattaforma Digidoc, nell'ambito dell'erogazione del servizio di Conservazione dei Documenti Informatici.</p>	<p>RS0807 Processo Change Management</p> <p>RS09P02 Procedura di Manutenzione Correttiva / Evolutiva DigiDoc</p>
Sicurezza dei sistemi e degli asset	Modalità con cui si effettua la valutazione, analisi e gestione dei Rischi pertinenti la Sicurezza delle Informazioni	RS0803P01 Procedura Analisi e Gestione Rischi
Sicurezza dei sistemi e degli asset	Individuazione e analisi delle vulnerabilità tecniche di Information Security	RS0803P04 Procedura Vulnerability Assessment e Penetration Test
Sicurezza dei sistemi e degli asset	Descrive il modello logico dell'infrastruttura IT e dei Servizi ICT erogati da Engineering D.HUB che consenta la gestione controllata e sistematica dei configuration item e delle relazioni tra gli stessi, per tutto il loro ciclo di vita. Lo scopo principale è quello di fornire accurate ed aggiornate informazioni di configurazione agli altri processi implementati, in particolare per la gestione	RS0809P01 Procedura Configuration Management

	<p>degli incidenti, dei problemi e dei cambiamenti.</p> <p>Per memorizzare e gestire adeguatamente tutte le informazioni relative agli elementi della configurazione è stato implementato il repository aziendale Engineering Configuration Management Data Base.</p> <p>È così possibile effettuare il censimento degli asset e assegnare gli ownership</p>	
Sicurezza dei sistemi e degli asset	<p>Il processo garantisce che l'accesso fisico e la movimentazione degli asset infrastrutturali avvengano in garanzia della protezione dell'asset stesso e delle informazioni in esso contenute</p>	RS08PR02 Procedura Asset Disposal e Logistica
Sicurezza dei sistemi e degli asset	<p>Definizione di regole per la gestione dei supporti magnetici/elettronici/cartacei ove risiedono informazioni, compresa la loro distruzione quando non più necessari</p>	RS08PR03 Procedura Gestione dei supporti di memorizzazione
Sicurezza dei sistemi e degli asset	<p>La procedura descrive criteri e modalità attraverso i quali viene erogato, da parte della direzione Operation DTM Nord di D.HUB, il servizio di Software Control & Distribution (SC&D).</p> <p>Il servizio, finalizzato alla distribuzione controllata del sw alle sole Postazioni di Lavoro (PdL), si suddivide nei seguenti sottoservizi:</p> <ol style="list-style-type: none"> 1. Software Distribution 2. Patch Management 3. Image Management 4. Antivirus Management 	RS08PR01 Procedura gestione PDL aziendali
Sicurezza dei sistemi e degli asset	<p>Definisce le modalità di gestione dei sistemi in garanzia della sicurezza delle informazioni</p>	RS08PR11 Procedura Gestione Sistemi
Sicurezza dei sistemi e degli asset	<p>descrive il servizio di gestione reti e connettività</p>	RS08PR07 Procedura Network Management
Sicurezza dei sistemi e degli asset	<p>Lo scopo della gestione degli eventi di monitoraggio è conoscere lo stato delle infrastrutture IT e dei servizi erogati rilevando qualsiasi scostamento dal funzionamento normale o atteso. La</p>	RS08PR02 Procedura Monitoring

	<p>procedura descrivere le attività svolte per gestire gli eventi originati dai tool di monitoraggio dell'infrastruttura IT in tutto il loro ciclo di vita. Le attività descritte hanno l'obiettivo di assicurare che eventuali malfunzionamenti o guastidegli apparati IT (ad esempio server, sistemi storage, apparati di rete, reti, backup) siano analizzati tempestivamente al fine di attivare le appropriate procedure di escalation e ripristino del servizio.</p>	
Sicurezza dei sistemi e degli asset	<p>L'adozione di adeguate misure di sicurezza è un prerequisito imprescindibile per la gestione delle infrastrutture IT e l'erogazione dei servizi ai Clienti. Il Patch Mangement è il processo mediante il quale le patch, incluse quelle di sicurezza, sono collezionate, analizzate, verificate ed implementate nell'ambiente IT. La procedura, che rientra nel più vasto ambito di gestione di sistemi, descrive criteri, regole e modalità di esecuzione delle attività finalizzate alla gestione delle patch sui server, costituenti l'infrastruttura IT attraverso la quale vengono erogati servizi ai Clienti sia interni che esterni. Vengono trattati esclusivamente aspetti tecnici ed operativi; sono esclusi temi inerenti le implicazioni legali, le valutazioni di impatto sul business e le strategie di sicurezza (audit, vulnerabilità assessment,...).</p>	RS08PR04 Procedura Patch Management
Sicurezza dei sistemi e degli asset	<p>La procedura descrive i criteri e le modalità di gestione del "servizio schedulazione dei lavori batch</p>	RS08PR12 Procedura Schedulazione Lavori
Sicurezza dei sistemi e degli asset	<p>Descrive le modalità di gestione della manutenzione impianti presenti nei DC</p>	RS08PR05 Procedura Gestione Impianti di Data Center
Sicurezza dei sistemi e degli asset	<p>Definisce le modalità con cui sono effettuati, conservati e utilizzati i dati di backup relativi a Servizi D.HUB</p>	RS08PR08 Procedura Gestione Backup
Gestione della business continuity	<p>L'obiettivo della procedura è di assicurare che le risorse tecniche e i servizi ICT possano essere ripristinati, a fronte di una interruzione totale del servizio, in tempi</p>	RS0814P01 Procedura Service Continuity

	<p>ritenuti accettabili.</p> <p>La procedura di IT Service Continuity Management riguarda gli aspetti di ripristino del servizio nel caso di eventi che comportano fermi di grande rilevanza. In altre parole, l'obiettivo del processo è garantire la continuità del servizi a fronte di eventi qualificabili come "disastri".</p>	
<p>Impostazione, implementazione e gestione della Sicurezza delle Informazioni</p>	<p>Il processo di Capacity Management ha lo scopo di assicurare che esistano le capacità adeguate a soddisfare le esigenze di business attuali e future, in relazione ai servizi che l'Azienda intende erogare nel tempo ai propri Clienti.</p> <p>È necessario garantire un costante monitoraggio dell'utilizzo delle risorse, anche in ottica di pianificazione delle necessità future</p>	<p>RS0811 Processo Capacity Management</p>
<p>Gestione delle terze parti</p>	<p>Descrive la gestione dei fornitori per garantire il rispetto dei requisiti di sicurezza del perimetro nei casi di servizio o porzione di esso affidata a terze parti, gestendo, inoltre, le eventuali modifiche alla fornitura, sempre in garanzia dei requisiti di sicurezza delle informazioni. Rendere le terze parti coinvolte nel perimetro consapevoli dei requisiti dell'org.ne relativamente alla sicurezza delle informazioni</p>	<p>RS02 Processo Gestione Approvvigionamento</p> <p>Condizioni Generali Contratti Acquisizione Prestazioni, art.19</p>
<p>Impostazione, implementazione e gestione della Sicurezza delle Informazioni</p>	<p>Descrive le modalità con cui sono effettuati gli audit interni, anche relativi alla Sicurezza delle Informazioni che devono verificare l'adozione di procedure volte a garantire la gestione controllata delle attività tecniche, in garanzia della sicurezza delle informazioni</p>	<p>MS01P01 Procedura Gestione Audit Interni</p>

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Il servizio è strutturato per fornire servizi continuativi con operatività H24 presidiata, garantendo:

- Implementazione dei sistemi di monitoraggio e relativo aggiornamento
- Rilevazione degli eventi di allarme
- Tracciamento su Sistema di Ticketing
- Applicazione dell'opportuna procedura di fixing o innesco della Procedura di Escalation Operativa / Informativa
- Follow-up del problema in caso di escalation

A supporto delle attività di Monitoring è stato sviluppato un apposito Sistema Informativo ad esclusivo uso del personale tecnico dove sono mantenute e costantemente aggiornate le informazioni riguardanti ogni singolo apparato/sistema monitorato e le procedure da attuare in caso di evento la cui azione correttiva è stata predefinita.

Il servizio di Monitoraggio viene erogato centralmente dall'Operation Centre (OC): esso opera in modalità H24 ed è presidiato da operatori che tengono sotto controllo lo stato dei sistemi; l'obiettivo è il Monitoring Proattivo per rilevare condizioni di criticità e porvi rimedio prima che l'insorgenza del problema generi un disservizio percepibile all'utente.

La Control Room dove risiedono gli operatori è dotata di appositi wall-screen che permettono di rappresentare visivamente lo stato del monitoraggio dell'infrastruttura tecnologica dei clienti

La procedura nelle operazioni di Monitoring prevede che all'insorgere di un allarme gli operatori, dopo aver verificato che l'evento sia stato tracciato sul sistema di Ticketing (la creazione del Ticket avviene in automatico da parte del sistema di Event Management), verificano sulla "Knowledge Base" la corretta procedura da intraprendere e mettono in atto le azioni previste (esecuzione di procedure di recovery, dispatching ad enti interni o esterni codificati, ecc.).

Nel caso l'anomalia non sia risolta a questo livello, o non esista ancora una procedura codificata, l'operatore che ha in carico il problema ne passa le competenze a una struttura di secondo livello interna all'OC che si preoccupa di effettuare una analisi più approfondita (trouble-shooting).

Questo II° livello interno all'OC opera con un presidio 7.00-19.00 e garantisce la copertura h24 in regime di reperibilità. In caso di risoluzione al II° livello il ticket viene chiuso e dopo aver dato riscontro al Cliente la procedura di recovery utilizzata viene inserita/aggiornata sul sistema di Knowledge Management.

Nel caso in cui il problema non possa ancora essere risolto all'interno dell'OC il ticket viene scalato ai competence center specifici (interni ad Engineering, del Cliente o Fornitori terze parti) secondo la natura del problema e in base alle procedure concordate ed il ticket viene inoltrato al gruppo competente.

Nel caso di dispatching a Competence Center (interni, o esterni) il problema rimarrà comunque in carico all'operatore che, ricevuta la notifica di chiusura da parte della struttura tecnica incaricata, verificherà il ripristino delle condizioni di funzionalità e provvederà alla chiusura del ticket (follow-up).

L'organizzazione dell'Operation Center può essere schematizzata come segue:



Figura 9: Organizzazione dell'Operation Center

Per apparati router di proprietà del carrier è richiesto almeno la disponibilità del monitoraggio con il protocollo SNMP.

Per il monitoraggio degli apparati di rete Engineering D.HUB utilizza la suite dei prodotti di Solarwinds.

In aggiunta alla suite Solarwinds vengono utilizzati opzionalmente altri tools quali il Netflow, utilizzato per analizzare il traffico. Mentre Orion NPM indica la percentuale di utilizzo di un link, tramite il protocollo Netflow è possibile identificare informazioni su protocolli o hosts che stanno utilizzando il link o generando traffico e verso quale destinazione, in modo da avere rapidamente una chiara situazione dell'utilizzo di banda. Queste informazioni possono essere utilizzate per definire e gestire (ove previste) le classi di servizio (Class of Services, CoS) della Quality of Service (QoS) riuscendo così a rendere prioritario il traffico ritenuto business.

[Torna al sommario](#)

9.2 Verifica di integrità degli archivi

Il sistema DigiDoc garantisce la conservazione a lungo termine dei documenti mediante funzionalità che verificano periodicamente l'integrità degli archivi. Le verifiche sono relative a:

- Integrità del documento;
- Validità della firma e della marca temporale del Responsabile del Servizio di conservazione;
- Integrità e consistenza dell'archivio;
- Leggibilità dei documenti conservati.

In fase di caricamento di un documento nell'archivio viene verificata la sua integrità confrontando la sua impronta con quella dichiarata nel SipManifest.xml. Tale verifica viene effettuata periodicamente con cadenza almeno annuale confrontando l'impronta memorizzata con quella calcolata per ogni documento. Viene altresì verificata la validità della firma digitale del responsabile del servizio di conservazione e la marca temporale.

Ogni controllo genera un report in formato xml che può essere consultato da parte del Responsabile del servizio di conservazione per attestare l'attività di verifica e per definire le eventuali azioni correttive.

Per garantire la leggibilità dei documenti, il Responsabile della Conservazione almeno una volta ogni cinque anni, sceglie un campione documentale composto da almeno un documento per ciascuna tipologia di documenti ed effettua la verifica tramite il viewer ad esso associato.

Se dalle verifiche dovessero emergere dei problemi, il Responsabile del servizio di conservazione avvierà le procedure atte a garantire il ripristino dei documenti conservati attraverso il riversamento dei documenti secondo quanto indicato nel paragrafo 7.10.

[Torna al sommario](#)

9.3 Soluzioni adottate in caso di anomalie

Con la finalità di raccogliere dati oggettivi per monitorare le attività di gestione degli impianti e delle infrastrutture dei Data Center, il Responsabile Infrastrutture DC, su base trimestrale, raccoglie, dai diversi DC Site Manager, informazioni relative a:

- Anomalie su impianti/infrastrutture verificatesi nel periodo di riferimento: tali informazioni possono essere veicolate attraverso i moduli RS08D12 Registro Anomalie Impianti DC che ciascun Site Manager compila per il proprio DC di riferimento, con il censimento di quanto accaduto nel periodo, in termini di anomalie da manutenzione ordinaria, straordinaria, prove di continuità; tali informazioni consentono di effettuare analisi di tipo statistico, ad esempio trend delle anomalie ricorrenti, o sulle performance dei fornitori del Servizio di Manutenzione nella gestione degli interventi di risoluzione anomalie.

[Torna al sommario](#)