COMUNE DI RIVALTA DI TORINO

ALLEGATO 9

IL SISTEMA DI CONSERVAZIONE ADOTTATO DAL COMUNE DI RIVALTA DI TORINO E IL MANUALE DEL CONSERVATORE AP SYSTEM

INDICE

1. La conservazione dei documenti informatici dell'Ente pag. 3

1.1 Il sistema di conservazione adottato dall'Ente pag. 3

1.2 Il sistema di versamento organizzato dall'Ente pag.4

2. Manuale della conservazione pag. 5

3. Responsabile della conservazione pag. 5

4. Specificità per la conservazione del registro di protocollo informatico pag. 5

5. Gestore del servizio in outsourcing dell'ente pag. 6

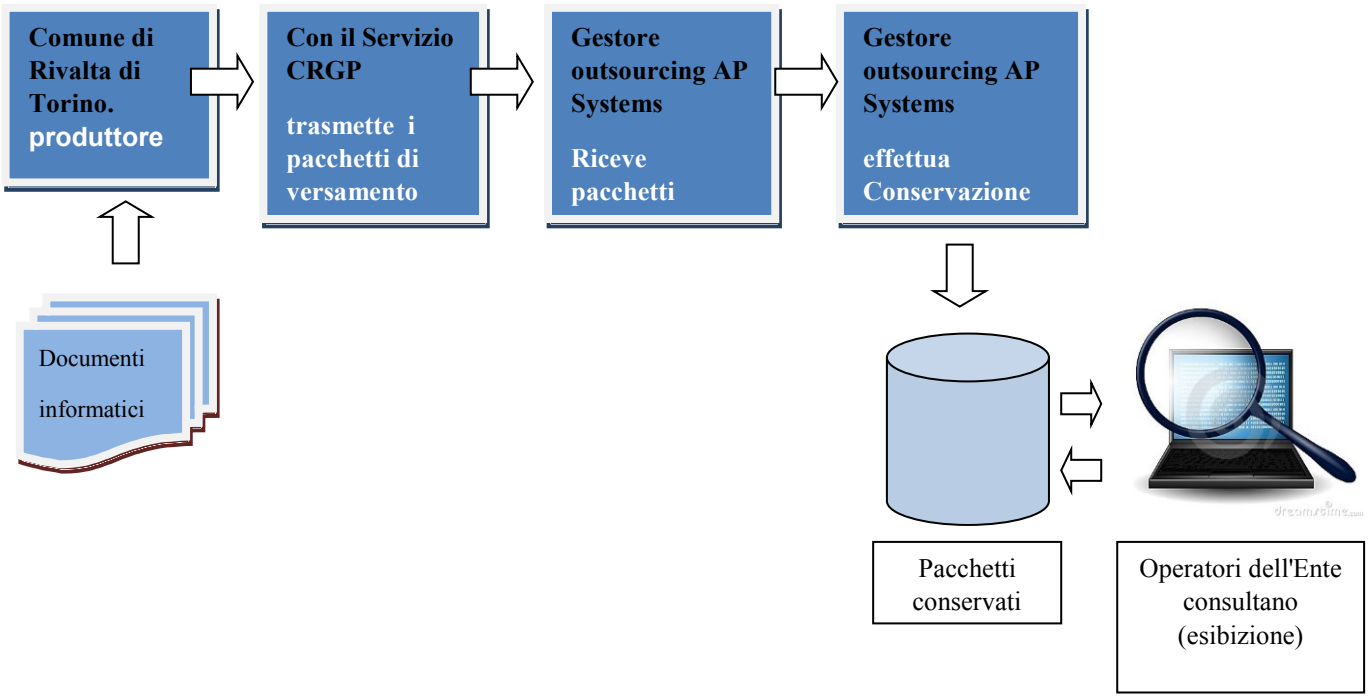
6. Manuale di Conservazione di APSer.Archivio

1. La conservazione dei documenti informatici dell'Ente

1.1 Il sistema di conservazione adottato dall'Ente

Il Comune di Rivalta di Torino affida il servizio di conservazione al conservatore accreditato esterno AP Systems.

Il "ciclo di gestione della conservazione" in outsourcing realizzato dal conservatore accreditato:



Il sistema prevede la "gestione del ciclo della conservazione" dal reperimento dei documenti e la preparazione dei pacchetti di versamento, fino alla conservazione a norma effettuata c/o outsourcer esterno accreditato Ap Systems che viene nominato responsabile della conservazione.

1.2 Il sistema di versamento organizzato dall'Ente

Il sistema di versamento adottato dall'Ente è il sistema Servizio CRGP che consente la gestione completa del flusso di versamento: creazione pacchetti, trasmissione tramite interfaccia al conservatore, archiviazione ricevute e monitoraggio operatività.
Ogni servizio produttore di documenti informatici è anche responsabile del procedimento di trasmissione dei pacchetti di versamento di propria competenza al conservatore esterno.

Modulo adottato: software Servizio CRGP per produzione/trasmissione pacchetti di versamento all'outsourcer Ap Systems.

In particolare, a.p.systems, per la durata del contratto, provvede:

- a gestire il processo di conservazione e garantirne nel tempo la conformità alla normativa vigente;
- a generare e sottoscrivere il pacchetto di distribuzione con firma digitale come previsto dal manuale di conservazione APSer.Archivio
- ad effettuare il monitoraggio della corretta funzionalità del sistema di conservazione APSer.Archivio;
- ad assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- a garantire la conservazione e l'accesso ai documenti informatici da essa conservati, adottando misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, ripristinando la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale del sistema di conservazione APSer.Archivio;
- ad adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione APSer.Archivio;
- a richiedere 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; ogni risorsa, comprese quelle di natura economica, necessaria per l'espletamento delle attività attribuite al pubblico ufficiale dovranno essere garantite e sostenute interamente dall'Ente; pertanto, qualora l'Ente non se ne sia fatto carico direttamente, AP Systems è sin da ora autorizzata ad addebitare all'Ente tutti i costi e le spese, compresi gli onorari inerenti le attività prestate dal Pubblico Ufficiale, qualora la normativa ne richieda obbligatoriamente la presenza;
- ad assicurare agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Inoltre Ap.Systems deve:

- terminare il processo di conservazione dei documenti informatici, entro e non oltre i termini previsti dal DPCM 03 dicembre 2013;
- provvedere, entro i suddetti termini, alla "chiusura" del processo di conservazione mediante l'apposizione di una firma digitale dell'incaricato preposto a tale adempimento e una marca temporale sull'insieme dei documenti ovvero su un'evidenza informatica (Pacchetto di Archiviazione) contenente l'impronta o le impronte dei documenti informatici conservati;
- provvedere, qualora richiesto dall'Ente, all'esibizione dei suoi documenti informatici conservati e delle relative evidenze informatiche che comprovano la corretta conservazione

degli stessi, fornendo appositi pacchetti di distribuzione contenenti gli elementi necessari per valutare la loro autenticità e validità giuridica.

Al solo fine della conservazione digitale del Registro Giornaliero di Protocollo oggetto del SERVIZIO CRGP, l'Ente nomina, ai sensi dell'art. 29 del D.Lgs. n. 196/2003, (Codice in materia di protezione dei dati personali), Ap Systems quale Responsabile esterno del trattamento dei dati necessari all'esecuzione del SERVIZIO CRGP.
In particolare, anche in considerazione del ruolo di Responsabile del Servizio di conservazione così come previsto dall'art. 6, co. 7, del D.P.C.M. 3 dicembre 2013, e dal manuale di conservazione APSer.Archivio, i compiti affidati ad Ap Systems attengono a qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la consultazione, l'elaborazione, la selezione, l'estrazione, l'interconnessione, la comunicazione, la cancellazione e la distruzione di dati.
Ap Systems, inoltre, opererà quale responsabile del trattamento, applicando le misure di sicurezza dalla stessa definite ed implementate ina base alle disposizioni legislative e regolamentari in vigore.

2. Manuale della conservazione

Viene adottato il Manuale della conservazione dell'Outsourcer a cui viene affidato il servizio pubblicato su sito web dell' Agid.

L'Ente definisce nella gestione del manuale di gestione documentale i procedimenti di versamento e di rapporti operativi con il Conservatore esterno.

3. Responsabile della conservazione

L'ente nomina come "Responsabile della conservazione" il Responsabile della conservazione dell'outsourcer Ap Systems a cui affida il servizio.

Il Responsabile della gestione documentale è anche responsabile della conservazione interna, limitatamente alle funzioni di coordinamento e supervisione del sistema realizzato dall'Ente per la gestione delle operazioni di Versamento dei pacchetti da conservare trasmessi al conservatore.
Il Responsabile della conservazione interno tiene i rapporti con il personale dei servizi per le operazioni di versamento.

4. Specificità per la conservazione del registro di protocollo informatico

In adempimento a quanto previsto dal D.P.C.M. 03 dicembre 2013 art. 7 c. 5, l'Ente provvede ad effettuare la conservazione del registro giornaliero di protocollo utilizzando il sistema di conservazione generale dell'Ente.
L'operazione di conservazione del registro di protocollo comprende:

- l'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno;
- la conservazione settimanale del registro di protocollo;
- la trasmissione, al sistema di conservazione ApSer.Archivio, garantendo l'immodificabilità del contenuto.

Il responsabile di protocollo, direttamente o tramite suoi incaricati, provvede tramite specifica funzione programmata del sistema di protocollo alla creazione del pacchetto di versamento del registro di protocollo del giorno precedente, per la verifica e la trasmissione al sistema di conservazione. Lo stesso soggetto e' tenuto al monitoraggio dell'esito positivo delle operazioni di avvenuta conservazione.

5. Gestore del servizio in outsourcing dell'Ente

L'Ente tiene un registro nel quale vengono riportati i riferimenti ai conservatori esterni a cui è affidata la conservazione con le date di incarico e di inizio attività ed eventuale fine incarico.
Tale registro viene mantenuto aggiornato dal Responsabile della gestione documentale.

Manuale di Conservazione

di **APSer.Archivio**

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	16-1-2015	Bassetto Carola	Responsabile del servizio di conservazione
Verifica	16-1-2015	Bassetto Carola	Responsabile del servizio di conservazione
Approvazione	30-1-2015	Bassetto Carola	Responsabile del servizio di conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0 IT	23/09/2010	Prima stesura	
2.0 A IT	30/04/2014	revisione per verifica applicazione regole tecniche ex DPCM 3/12/2013	
2.1 IT	25/08/2014	Revisione per certificazione 27001:2013	
2.2 IT	30/09/2014	revisione per aggiornamento al certificato 27001:2013	
3.0 IT	16/01/2015	revisione per aggiornamento modello organizzativo	

INDICE DEL DOCUMENTO

1 SCOPO E AMBITO DEL DOCUMENTO....4
1.1 allegati....4
2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)....5
3 NORMATIVA E STANDARD DI RIFERIMENTO....11
3.1 Normativa di riferimento....11
3.2 Standard di riferimento....12
4 RUOLI E RESPONSABILITÀ....13
5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE....16
5.1 Organigramma....16
5.1.1 ruolo e compiti del PRODUTTORE....17
5.1.2 ruolo e compiti del CONSERVATORE....18
5.1.3 ruolo e compiti del FRUITORE (utente)....20
5.2 Strutture organizzative....21
5.3 obblighi....22
6 OGGETTI SOTTOPOSTI A CONSERVAZIONE....24
6.1 Oggetti conservati....24
6.1.1 classe documentale....24
6.1.2 Formati dei documenti....25
6.1.2.1 PDF - PDF/A - Portable Document Format....25
6.1.2.2 JPEG - Joint Photographic Experts Group....26
6.1.2.3 OOXML – Open Office XML....26
6.1.2.4 ODF – Open Document Format....26
6.1.2.5 XML - eXtensible Markup Language....26
6.1.2.6 TXT – generico testo....27
6.1.2.7 EML – messaggi di posta elettronica....27
6.1.3 metadati....27
6.2 Pacchetto di versamento....33
6.2.1 Informazioni presenti nell'indice pacchetto di versamento (IPdV)....33
6.2.2 Personalizzazioni del pacchetto di versamento....34
6.3 Pacchetto di archiviazione....35
6.3.1 Informazioni presenti nell'indice pacchetto di versamento....35
6.3.2 Struttura ExtraInfo dell'IPdA....36
6.3.3 Personalizzazioni del pacchetto di archiviazione....37
6.4 Pacchetto di distribuzione....38
6.4.1 Informazioni presenti nell'indice pacchetto di distribuzione....38
6.4.2 Personalizzazioni del pacchetto di distribuzione....38
7 IL PROCESSO DI CONSERVAZIONE....39
7.1 modalità di acquisizione dei pacchetti di versamento per la loro presa in carico....40
7.2 verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti....41

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico 43

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie 43

7.5 Preparazione e gestione del pacchetto di archiviazione 44

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione 45

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti 46

7.8 Scarto dei pacchetti di archiviazione 47

7.9 Annullamento dei pacchetti di versamento 47

7.10 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori 47

8 IL SISTEMA DI CONSERVAZIONE 49

8.1 Componenti logiche, tecnologiche, fisiche 49

8.2 Conduzione e manutenzione del sistema di conservazione 55

8.3 Change Management 55

8.4 Verifica periodica di conformità normativa e standard di riferimento 57

9 MONITORAGGIO E CONTROLLI 57

9.1 Procedure di monitoraggio 57

9.2 Verifica dell'integrità degli archivi 57

9.2.1 Verifica dell'integrità e della consistenza dei pacchetti di archiviazione e degli indici dei documenti generati dal Processo di Conservazione, in carico al RC; 58

9.2.2 Verifica dell'effettiva leggibilità dei documenti informatici inseriti all'interno dei lotti, in carico al RSC. 58

9.2.3 registro delle verifiche periodiche 59

9.3 Soluzioni adottate in caso di incidenti della sicurezza 59

1 SCOPO E AMBITO DEL DOCUMENTO

Da oltre 30 anni a.p.systems rilascia soluzioni ICT per la pubblica amministrazione locale e partecipa attivamente al processo di rinnovo della PA in tema di digitalizzazione.
Oltre a mettere a disposizione una suite applicativa sempre aggiornata sia a livello tecnologico che normativo, a.p.systems ha attivato un centro servizi (denominato APSer) che incontra l'esigenza della PA di digitalizzare ed ottimizzare la propria azione amministrativa riducendo, nel contempo, la relativa spesa.
Tra i molti servizi, APSer offre anche la possibilità di conservare i documenti digitali; il presente manuale descrive il servizio APSer.ARCHIVIO al quale la Pubblica Amministrazione può affidare la conservazione digitale dei propri documenti informatici, ma non analogici, nel pieno rispetto delle normative e regole tecniche vigenti.
Più in generale lo scopo di questo manuale è fornire dettagli sull'organizzazione e le modalità di erogazione del servizio APSer.Archivio, e più precisamente descrive:

- l'*organizzazione* (art. 8 c.2 lett. a, b, et k DPCM 3/12/2013): le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo;
- il modello di funzionamento (art. 8 c.2 lett. c et e DPCM 3/12/2013): come è implementato il processo di conservazione e gli aspetti operativi per arrivare alla produzione del dispositivo contenente la documentazione digitale;
- il *processo* (art. 8 c.2 lett. d, f, i et j DPCM 3/12/2013): il processo di apposizione della Firma Digitale, della Marca Temporale e tutti gli aspetti procedurali inerenti la registrazione dei dispositivi sostitutivi e le procedure di verifica dei documenti e di gestione delle copie di sicurezza
- l'*architettura* e l'*infrastruttura* utilizzata (art. 8 c.2 lett. g DPCM 3/12/2013)
- le *misure di sicurezza* adottate (art. 8 c.2 lett. h et l DPCM 3/12/2013)

1.1 allegati

- schema "Specificità del Contratto" Le specificità di utilizzo di APSer.Archivio da parte di ogni singolo Cliente, come ad esempio l'individuazione delle tipologie di documenti da conservare e le modalità operative per effettuare il loro versamento anche tenendo conto dell'organizzazione informatica dell'Ente, vengono declinate nell'allegato

"*Specificità del Contratto*"; tale allegato viene prodotto e personalizzato con riferimento alle peculiarità descritte nel contratto stipulato con il Cliente, per l'erogazione del servizio. Per questo motivo, tale allegato non fa parte del presente manuale.

- Decreto Presidente del Consiglio dei Ministri 3 dicembre 2013, pubblicato in G.U. suppl.ord. n.20 serie generale n. 59 del 12 marzo 2014

Torna al sommario

2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Fatti salvi i termini di cui all'Allegato 1 DPCM 3/12/2013, riportato quale allegato anche del presente Manuale, di seguito si riportano i termini e gli acronimi utilizzati ripetutamente in questo testo e per i quali non vi è riferimento nel citato allegato.

Glossario dei termini e Acronimi	
accesso	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
accreditamento	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
affidabilità	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
aggregazione documentale informatica	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
AgID	Agenzia per l'Italia Digitale
APS	a.p.systems
APSer	centro servizi di a.p.systems
APSer.Archivio	servizio di conservazione digitale erogato da a.p.systems.
archivio	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
archivio informatico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
area organizzativa omogenea	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
attestazione di conformità delle copie per immagine su supporto informatico di documento analogico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale

Glossario dei termini e Acronimi	
autenticità	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
base di dati	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale
certificatore accreditato	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
ciclo di gestione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
classificazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
Cliente	Ente produttore che affida il servizio di conservazione ad a.p.systems
Codice	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
codice eseguibile	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
conservatore	soggetto esterno che svolge il servizio di conservazione per conto del soggetto produttore
conservatore accreditato	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
conservazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
coordinatore della gestione documentale	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
copia analogica del documento informatico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
copia di sicurezza	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
destinatario	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
CRL	Certificate Revocation List
documento SdC	allegato al contratto di affidamento del servizio di conservazione dal titolo Specificità del Contratto, che descrive gli accordi tecnico-organizzativi tra Produttore e Conservatore con il fine di erogare il servizio nel rispetto delle peculiarità del Cliente affidatario e della norma cogente.
DPCM	decreto del Presidente del Consiglio dei Ministri

Glossario dei termini e Acronimi	
duplicazione dei documenti informatici	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
Ente	Ente Pubblico
esibizione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
estratto per riassunto	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
evidenza informatica	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
fascicolo informatico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
ETSI-TR	European Telecommunications Standards Institute Technical Report
ETSI-TS	European Telecommunications Standards Institute Technical Specification
ESI	Electronic Signatures and Infrastructure
formato	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
funzionalità aggiuntive	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
funzionalità minima	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
funzionalità operative	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
funzione di hash	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
generazione automatica di documento informatico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
ICT	Information and Communication Technology
identificativo univoco	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
IdP:	strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
immodificabilita'	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale

Glossario dei termini e Acronimi	
impronta	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
insieme minimo di metadati del documento informatico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
integrita'	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
interoperabilita'	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
IPdA	file indice del pacchetto di archiviazione
IPdD	file indice del pacchetto di distribuzione
IPdV	file indice del pacchetto di versamento
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISMS	Information security management system
leggibilita'	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
log di sistema	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
Manuale	il presente manuale del servizio di conservazione
manuale di conservazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
manuale di gestione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
memorizzazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
metadati	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
metadato	
OAIS	ISO 14721:2012; Space Data information transfer system……
MIBACT	Ministero dei beni e delle attività culturali e del turismo
PA	Pubblica Amministrazione
pacchetto di archiviazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
pacchetto di distribuzione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
pacchetto di versamento	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale

Glossario dei termini e Acronimi	
pacchetto informativo	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
piano della sicurezza del sistema di conservazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
PdA	pacchetto di archiviazione
PdD	pacchetto di distribuzione
PdV	pacchetto di versamento
piano della sicurezza del sistema di gestione informatica dei documenti	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
piano di conservazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
piano generale della sicurezza	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
presa in carico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
processo di conservazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
produttore	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
RA	responsabile della funzione archivistica di conservazione
rapporto di versamento	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
RC	responsabile della conservazione
registrazione informatica	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
registro di protocollo	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
registro particolare	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
repertorio informatico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
responsabile del trattamento dei dati	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
responsabile della conservazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
responsabile della sicurezza	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
RGD	responsabile della gestione documentale
riferimento temporale	vedi allegato 1 DPCM 3/12/2013,

Glossario dei termini e Acronimi	
	allegato al presente manuale
RSC	responsabile della servizio di conservazione
RSI	responsabile dei sistemi informativi per la conservazione
RSI-Ente	responsabile sistemi informativi dell'Ente
RSM	responsabile sviluppo e manutenzione del sistema di conservazione
RSSC	responsabile sicurezza dei sistemi per la conservazione
RSS-Ente	responsabile della sicurezza dei sistemi informativi dell'Ente
RTP	responsabile del trattamento dei dati personali
scarto	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SHA-256	algoritmo di hash a 256 caratteri sviluppato dalla National Security Agency e pubblicato dal NIST (National Institute of Standards and Technologies) cine standard federale USA.
SinCRO	Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali
sistema di classificazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
sistema di conservazione	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
sistema di gestione informatica dei documenti	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
SLA	service level agreement
staticità	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
testo unico	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
transazione informatica	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
ufficio utente	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
user ID	login e password
UTC	Coordinated Universal Time, ossia il fuso orario di riferimento da cui sono

Glossario dei termini e Acronimi	
	calcolati tutti gli altri fusi orari del mondo
utente	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
versamento degli archivi di stato	vedi allegato 1 DPCM 3/12/2013, allegato al presente manuale
W3C	World Wide Web Consortium, è un'organizzazione non governativa internazionale che ha come scopo quello di sviluppare tutte le potenzialità del World Wide We
XML, linguaggio XML	acronimo di eXtensible Markup Language, è un linguaggio marcatore basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo
ZIP	formato di compressione dei dati che supporta vari algoritmi di compressione, uno dei quali è basato su una variante dell'algoritmo LZW

Torna al sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

Il servizio APSer.Archivio recepisce le indicazioni fornite dall'Agenzia per l'Italia Digitale (Circolare AgID numero 65/2014), e in particolare le "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 CAD" (DPCM 3 dicembre 2013 G.U. n. 59 del 12-3-2014 – Suppl. Ordinario n. 20).

3.1 Normativa di riferimento

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- 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.
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, pubblicato su G.U. del 12/1/2015.

Torna al sommario

3.2 Standard di riferimento

APSer.Archivio svolge il servizio di conservazione con riferimento agli standard elencati nell'allegato 3 delle Regole Tecniche DPCM 3/12/2013 e di seguito richiamati nella versione aggiornata al 1° ottobre 2014.

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic

Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Torna al sommario

4 RUOLI E RESPONSABILITÀ

Il sistema di conservazione nel suo complesso interviene nella fase di produzione e conservazione dei pacchetti di versamento, in quella di recupero ed esibizione dei documenti conservati (es. richiesta di accesso da parte di soggetto avente diritto) ed in quella di tutela dell'archivio conservato. In tale contesto, per sfruttare al meglio la capacità professionale delle parti coinvolte, il modello organizzativo di APSer.ARCHIVIO prevede la distribuzione dei ruoli e del compiti tra il Cliente che produce e gestisce i documenti informatici da conservare e a.p.systems che svolge il ruolo di Conservatore degli stessi.

In seno al Cliente viene assegnato il ruolo di Responsabile della Conservazione (RC), nel rispetto di quanto previsto dalla norma, e, per quanto attiene l'intero sistema, ad esso fanno riferimento tutte le altre figure coinvolte sia del Cliente stesso che di a.p.systems.

In tale contesto, a.p.systems supporta RC con ruoli di competenza per quanto riguarda il *servizio di conservazione*; nella fattispecie, in seno ad a.p.systems vengono svolti i ruoli come indicato nella griglia 1.

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
RSC Responsabile del servizio di	Bassetto Carola	definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo del sistema di	dal 10/01/2007	nessuna

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
conservazione		conservazione; definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; corretta erogazione 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.		
RSSC Responsabile Sicurezza dei sistemi per la conservazione	Cazzato Roberto	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 RSC e individuazione e pianificazione delle necessarie azioni correttive.	dal 31/03/2008	nessuna
RA Responsabile funzione archivistica di conservazione	Ripamonti Alessandro	definizione e gestione dei processi di conservazione (incluse le modalità di trasferimento da parte del Cliente), di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definizione del set di metadati di conservazione dei documenti e dei fascicoli; monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; collaborazione con il Cliente 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.	dal 15/01/2007	nessuna
RTP Responsabile trattamento dati personali	Bassetto Carola	garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; garanzia che il trattamento dei dati affidati dal Cliente avviene nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e riservatezza.	dal 10/01/2007	nessuna

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
RSI Responsabile sistemi informativi per la conservazione	Cazzato Roberto	Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con il Cliente; segnalazione delle eventuali difformità degli SLA al RSC e individuazione e pianificazione delle necessarie azioni correttive. pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al RSC.	dal 31/03/2008	nessuna
RSM Responsabile sviluppo e manutenzione del sistema di conservazione	Bonini Luca	coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; interfaccia con il Cliente 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.	dal 15/01/2007	nessuna

griglia 1 – ruoli e competenze conservatore

I responsabili di ruolo possono avvalersi del supporto di addetti e operatori, formalmente incaricati, per svolgere alcune attività mantenendo comunque la supervisione e la responsabilità del lavoro svolto.

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

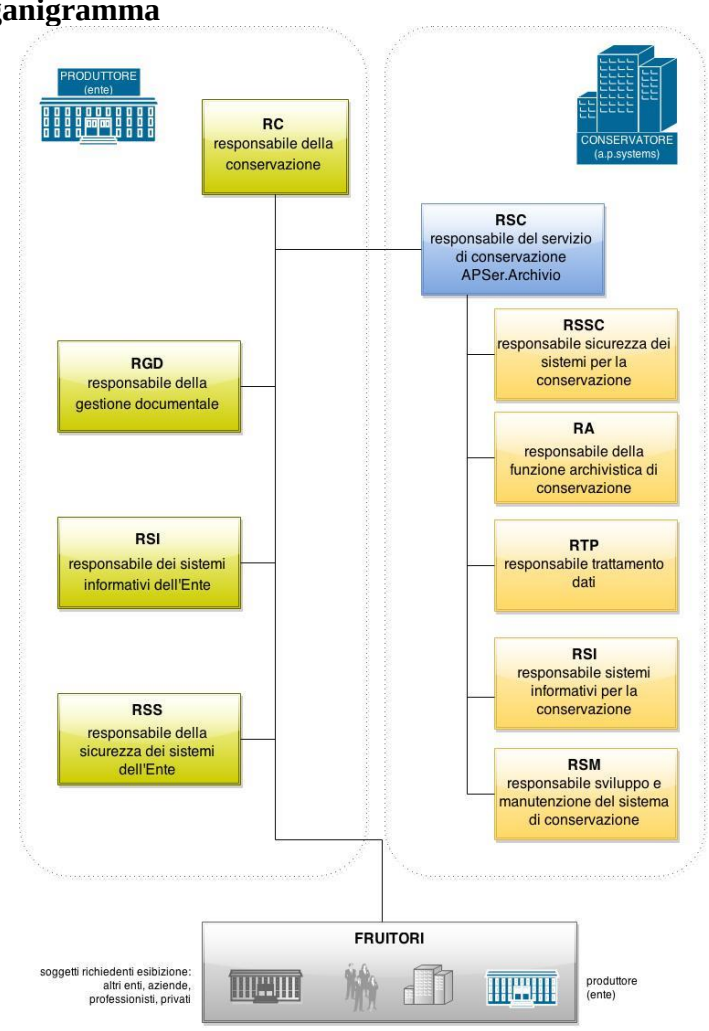


Figura 1- organigramma

Ricorrendo ad APSer.ARCHIVIO, il Cliente produttore dei documenti informatici *affida il servizio della loro conservazione ad a.p.systems*, in applicazione del modello organizzativo previsto dall'art.5 comma 2 lett. b) del DPCM 3/12/2013 e rappresentato dall'organigramma di **Figura 1- organigramma**; il Cliente mantiene la responsabilità della produzione, gestione e conservazione a norma dei propri documenti informatici.

I responsabili RC e RSC si interfacciano per coordinare la cooperazione applicativa e garantire la continuità operativa, tra i sistemi informativi gestionali di RC con quello di conservazione di RSC.

5.1.1 ruolo e compiti del PRODUTTORE

L'Ente è produttore dei documenti informatici e mantiene titolo e responsabilità sulla loro produzione, composizione, contenuto e gestione documentale in applicazione della norma cogente in materia.
Tale osservanza garantisce che il documento, nei modi e tempi dovuti, viene inserito, nei tempi previsti, in un pacchetto di versamento per la sua conservazione.

Con riferimento alla Figura 1- organigramma, il Cliente:

- ai sensi dell'art.7 comma 3 e 4 DPCM 31/12/2013, designa formalmente ad uno tra i suoi dirigenti o funzionari il ruolo di RESPONSABILE DELLA CONSERVAZIONE (RC) limitatamente per
- definire ed attuare le politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;
- gestire le convenzioni, gli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione
- gestire il processo di conservazione garantendone nel tempo la conformità alla norma
- generare e sottoscrivere i pacchetti di distribuzione per versamento e/o esibizione
- assicurare la presenza di un pubblico ufficiale nei casi in cui sia richiesto il suo intervento
- autorizzare il riversamento proposto dal RSC nei casi di incorsa obsolescenza dei supporti di conservazione
- predisporre il manuale di conservazione, per la parte di competenza, e curarne l'aggiornamento periodico in presenza di cambiamenti rilevanti sul piano normativo, organizzativo, procedurale e/o tecnologico
- ai sensi dell'art.6 comma 6 DPCM 3/12/2013, delegare RSC per alcune le funzioni previste a suo carico dalla norma;
- mantiene la RESPONSABILITA' DELLA GESTIONE DOCUMENTALE (ruolo RGD).
- mantiene la RESPONSABILITA' DEI PROPRI SISTEMI

INFORMATIVI usati per produrre e gestire i documenti informatici (ruolo RSI-Ente)

- mantiene la RESPONSABILITA' DELLA SICUREZZA PER LA TUTELA SIA FISICA CHE LOGICA DEI PROPRI SISTEMI INFORMATIVI con i quali vengono prodotti e gestiti i documenti informatici da conservare (ruolo RSS).

Qualora nell'ambito del servizio di conservazione, ricorra l'obbligo che un Pubblico Ufficiale sancisca i passaggi di stato (es. nei casi di passaggio da analogico a digitale del documento), di supporto o qualsiasi altra situazione simile in cui sia necessaria un'autenticazione, questi viene messo a disposizione senza oneri a carico del conservatore da parte del Cliente. Egli agisce utilizzando la piattaforma applicativa di APSer.ARCHIVIO e gli strumenti di validazione digitale e fissazione temporale quali la propria firma digitale e la marca temporale.

5.1.2 ruolo e compiti del CONSERVATORE

a.p.systems, in qualità di conservatore, svolge il servizio di conservazione dei documenti informatici affidatigli dal Cliente nel rispetto della normativa cogente e di quanto stabilito con il Cliente sul piano contrattuale e sul documento SdC. Con riferimento all'organigramma rappresentato in Figura 1, apsystems:

- ricopre il ruolo di CONSERVATORE, ossia svolge il servizio di conservazione dei documenti informatici affidatigli dal Cliente nelle modalità e forme descritte nel documento SdC e nel rispetto del presente Manuale;
- incarica un suo funzionario del ruolo di RESPONSABILE DEL SERVIZIO DI CONSERVATORE (RSC) a cui affida i seguenti compiti svolti per conto del RC
- individuare le caratteristiche ed i requisiti di sistema in funzione della tipologia dei documenti da conservare
- erogare correttamente il servizio di conservazione all'ente produttore;
- generare il rapporto di versamento secondo le modalità descritte nel presente Manuale;
- effettuare il monitoraggio della corretta funzionalità del sistema, anche effettuando verifiche periodiche, a cicli non superiori di 5 anni, sull'integrità degli archivi e della loro leggibilità, e adottare le misure per rilevare tempestivamente eventuali situazioni di degrado nei sistemi di

memorizzazione e registrazione e quindi ripristinarne il funzionamento per garantire la conservazione e l'accesso ai documenti;

- proporre al RC riversamenti su supporti tecnologici diversi nel caso di necessità
- adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione
- assicurare agli organismi competenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e vigilanza
- su richiesta del RC, garantire l'assistenza e le risorse necessarie all'espletamento delle attività attribuite al pubblico ufficiale quando è richiesto il suo intervento
- predisporre il manuale di conservazione, per la parte di competenza, e curarne l'aggiornamento periodico in presenza di cambiamenti rilevanti sul piano normativo, organizzativo, procedurale e/o tecnologico.
- in qualità di soggetto esterno a cui è affidato il servizio di conservazione, dall'Ente gli viene affidato anche il ruolo di RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI (RTP) ai sensi dell'art.6 comma 8 DPCM 3/12/2013 e secondo quanto previsto in materia dal Codice. Nella fattispecie, i compiti in tale ruolo si riassumono in
- garantire del rispetto delle norme vigenti in materia di trattamento dei dati personali;
- garantire che il trattamento dei dati affidati dall'Ente avviene nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza
- svolge la funzione di RESPONSABILE DELLA FUNZIONE ARCHIVISTICA (RA) per le attività di
- definizione e gestione del processo di conservazione per fasi di
- trasferimento, acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti,
- esibizione, accesso e fruizione del patrimonio documentario e informativo conservato;
- definizione del set di metadati di conservazione dei documenti e dei fascicoli
- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione
- collaborazione con l'Ente 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 competenzadefinizione set
- svolge la funzione di RESPONSABILE DEI SISTEMI INFORMATIVI

(RSI) con i quali vengono erogati i servizi di conservazione APSer.ARCHIVIO; in particolare si occupa di

- sovrintendere alla corretta operatività delle componenti hardware e software del sistema di conservazione;
- monitorare il mantenimento dei livelli di servizio (SLA) concordati con l'Ente;
- segnalare le eventuali difformità degli SLA al RCONS, individuare e pianificare le necessarie azioni correttive;
- pianificare lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione;
- controllare e verificare i livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al RC.
- svolge la funzione di RESPONSABILE DELLA SICUREZZA (RSSC) per la tutela sia fisica che logica dei propri sistemi di conservazione; in particolare il ruolo garantisce le seguenti attività:
- 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 RC e RSC
- individuazione e pianificazione delle necessarie azioni correttive in caso di difformità in accordo con RC e RSC.

5.1.3 ruolo e compiti del FRUITORE (utente)

Il fruitore è colui che (tipicamente un soggetto esterno che si rivolge all'Ente) richiede l'esibizione di uno o più documenti conservati.
Egli, per ottenere la copia o la visura del documento di interesse, ha l'obbligo di fare richiesta di esibizione nelle forme previste dal regolamento dell'Ente e dalla norma; di conseguenza, se sussistono i criteri per l'esibizione, l'Ente ha l'obbligo di produrre il pacchetto di esibizione ed APSer.ARCHIVIO di consegnarlo all'Ente che, a sua volta, lo presenta quindi al fruitore.

Torna al sommario

5.2 Strutture organizzative

Per ciascun contratto di conservazione, le attività e le responsabilità dei ruoli che svolgono il servizio sono definite dalla seguente matrice

		RESPONSABILITÀ					
		RSC	RSSC	RA	RTP	RSI	RSM
ATTIVITÀ proprie di gestione dei sistemi informativi	attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	A	C	P	P	P	R
	acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	A	C	R	C	P	P
	preparazione e gestione del pacchetto di archiviazione	C	C	P	C	-	-
	preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	C	C	R	C	-	-
	scarto dei pacchetti di archiviazione	C	C	R	C	-	-
	chiusura del servizio di conservazione a seguito di disdetta contratto	A	C	P	C	P	R

legenda

RC = Responsabile della Conservazione (Ente)

RSC=Responsabile del servizio di conservazione (a.p.systems)
RSSC = Responsabile sicurezza dei sistemi per la conservazione (a.p.systems)
RA = Responsabile della funzione archivistica di conservazione (a.p.systems)
RTP = Responsabile trattamento dei dati (a.p.systems)
RSI = Responsabile sistemi informativi per la conservazione (a.p.systems)
RSM = Responsabile sviluppo e manutenzione del sistema di conservazione (a.p.systems)

A= autorizza
R= responsabile
C= controlla
P= partecipa

Matrice 1

Le responsabilità nella gestione dei sistemi informativi per la conservazione sono definite dalla seguente matrice.

		RESPONSABILITÀ					
		RSC	RSSC	RA	RTP	RSI	RSM
ATTIVITÀ proprie di gestione dei sistemi informativi	conduzione e manutenzione del sistema di conservazione	A	C	R	C	P	P
	monitoraggio del sistema di conservazione	A	C	R	C	P	P
	change management	A	C	P	C	P	R
	verifica periodica di conformità a normativa e standard di riferimento	A	R	P	C	P	P

legenda

RC = Responsabile della Conservazione (Ente)

RSC=Responsabile del servizio di conservazione (a.p.systems)
RSSC = Responsabile sicurezza dei sistemi per la conservazione (a.p.systems)
RA = Responsabile della funzione archivistica di conservazione (a.p.systems)
RTP = Responsabile trattamento dei dati (a.p.systems)
RSI = Responsabile sistemi informativi per la conservazione (a.p.systems)
RSM = Responsabile sviluppo e manutenzione del sistema di conservazione (a.p.systems)

A= autorizza
R= responsabile
C= controlla
P= partecipa

Matrice 2

5.3 obblighi

Il Cliente ha l'obbligo di gestire i propri documenti informatici in accordo a quanto definito nell'ambito della propria organizzazione dai propri regolamenti e dalla norma in vigore in tema di gestione documentale e archivistica; ha inoltre l'obbligo di individuare i documenti che devono essere archiviati, sulla base del proprio regolamento, e di produrre i pacchetti di versamento. Allo stesso modo ha l'obbligo di interfacciarsi all'utente che richiede accesso ai documenti e, se il caso, di predisporre il relativo pacchetto di esibizione.

Il Cliente ha anche l'obbligo di definire, al proprio interno,

- le procedure propedeutiche alla conservazione digitale,

- le responsabilità, funzioni e le attività eventualmente delegate e di mantenere valida e aggiornata la relativa documentazione
- i provvedimenti tecnico-organizzativi da adottare per evitare di arrecare danno alla propria struttura e a terzi.

Infine il Cliente ha l'obbligo di provvedere all'assolvimento di eventuali imposte di bollo dovute sui documenti informatici depositati in conservazione.

a.p.systems ha l'obbligo di garantire la conservazione e l'accesso ai documenti informatici affidatigli nelle forme e modalità previste dal Manuale e dal documento SdC, acquisire i pacchetti di versamento dal Cliente e consegnare quelli di esibizione a fronte delle richieste dello stesso. Ha inoltre l'obbligo di mantenere aggiornato e funzionante il sistema di conservazione sia sotto il profilo tecnologico che normativo.
In qualità di RSC, a.p.systems non ha alcuna responsabilità in merito ai contenuti dei documenti informatici affidatigli per la conservazione: tale responsabilità rimane totalmente a carico del Cliente; inoltre, a.p.systems non non accede e/o tratta alcun contenuto dei documenti informatici affidatigli in conservazione: tale compito rimane in capo al Cliente che svolge per tramite del suo sistema di gestione documentale.

Torna al sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il Cliente, nel proprio manuale di conservazione, individua i documenti per i quali intende avvalersi del servizio di conservazione APSer.ARCHIVIO e ne determina le classi documentali; tali specifiche vengono riprese nel documento SdC ed il RSC ha cura che vengano recepite e attivati i procedimenti informatici per la loro conservazione.

Torna al sommario

6.1 Oggetti conservati

I documenti informatici da sottoporre a conservazione devono essere

- prodotti in uno dei formati accettati dal sistema di conservazione, come di seguito indicato
- associati ad una CLASSE DOCUMENTALE

6.1.1 classe documentale

La classe documentale specifica tutte le caratteristiche relative ad una tipologia di documento da sottoporre a conservazione, individuando le informazioni necessarie a qualificare ed identificare univocamente ogni singolo documento. Ha parametri propri di comportamento ed attributi caratteristici (metadati).
Nel sistema di conservazione APSer.ARCHIVIO, la classe documentale è definita dai seguenti parametri:

- codice identificativo;
- descrizione;
- periodo di conservazione;
- classificazione;
- eventuale fascicolo di attribuzione;
- metadati associati.

A titolo esemplificativo, si riporta di seguito la definizione relativa alla classe documentale denominata "**DETERMINE**" (determinazioni dirigenziale emesse):

DETE;
DETERMINAZIONI;

Indeterminato;
1 – 6 – 0 – Archivio Generale;
XXX/XXXX – DETERMINAZIONI EMESSE ANNO XXXX
Metadati minimi associati:

DATA_ADOZIONE	Data dell'atto
NUMERO_ADOZIONE	Numero dell'atto
OGGETTO	Oggetto dell'atto
CODICE_SETTORE	Codice del progressivo di settore
NUMERO_SETTORE	Numero del progressivo di settore
DATA_PUBBLICAZIONE_INIZIO	Data di inizio pubblicazione dell'atto
DATA_PUBBLICAZIONE_FINE	Data di fine pubblicazione dell'atto
SETTORE_PROPONENTE	Settore che effettua l'atto
UNITA_PROPONENTE	Unità organizzativa che effettua l'atto

6.1.2 Formati dei documenti

I formati idonei alla conservazione devono assolvere all'esigenza che il documento assuma le caratteristiche di immodificabilità e di staticità previste dalle regole tecniche.
In considerazione del fatto che il tempo di conservazione, previsto dalla normativa per le singole tipologie di documenti informatici che si sottopongono a conservazione, può essere indeterminato, APSer.ARCHIVIO ammette la conservazione dei documenti informatici prodotti nei seguenti formati, scelti tra quelli di cui all'allegato 2 del DPCM 3 dicembre 2013.

6.1.2.1 PDF - PDF/A - Portable Document Format

Il PDF (Portable Document Format) è un formato creato da Adobe nel 1993 che attualmente si basa sullo standard ISO 32000. E' stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Nell'attuale versione gestisce varie tipologie di informazioni quali: testo formattato, immagini, grafica vettoriale 2D e 3D, filmati. Un documento PDF può essere firmato digitalmente in modalità nativa attraverso il formato ETSI PAdES.
Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A. Il

PDF/A è stato sviluppato con l'obiettivo specifico di rendere possibile la conservazione documentale a lungo termine su supporti digitali e, tra le sue caratteristiche, ricoprono particolare importanza per la conservazione:

- assenza di collegamenti esterni,
- assenza di codici eseguibili quali javascript ecc.,
- assenza di contenuti crittografati.

Queste caratteristiche rendono il file indipendente da codici e collegamenti esterni che ne possono alterare l'integrità e l'uniformità nel lungo periodo.

6.1.2.2 JPEG - Joint Photographic Experts Group

Dato che il formato JPEG può comportare una perdita di qualità dell'immagine originale questo formato può essere utilizzato per portare in conservazione documenti originariamente reperiti già in questo formato essendo un formato di altissima diffusione a livello informatico e normalmente utilizzato per lo scambio di immagini.
E' invece ammesso a conservazione il formato JPEG con estensione .jp2 (ISO/IEC 15444-1) che può utilizzare la compressione senza perdita di informazione. Il formato JPEG 2000 consente, inoltre, di associare metadati ad un'immagine.

6.1.2.3 OOXML – Open Office XML

E' un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database (estensioni docx, xslx,…). E' ammesso a conservazione in quanto conforme allo standard ISO/IEC 29500:2008

6.1.2.4 ODF – Open Document Format

E' un formato di file, sviluppato da OASIS, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database (estensioni ods, odg,…)
E' ammesso a conservazione in quanto conforme allo standard ISO/IEC 26300:2006.

6.1.2.5 XML - eXtensible Markup Language

Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi. Ad esempio:

- SVG usato nella descrizione di immagini vettoriali
- XBRL usato nella comunicazione di dati finanziari
- ebXML usato nel commercio elettronico
- SOAP utilizzato nello scambio dei messaggi tra Web Service

6.1.2.6 TXT – generico testo

Oltre a XML, per quanto concerne i formati non binari "in chiaro", è universalmente utilizzato il formato TXT.
Sono ammessi alla conservazione i file TXT creati con formati Unicode (es. UTF – 8) in quanto riconosciuti anche nell'ambito W3C.

6.1.2.7 EML – messaggi di posta elettronica

Ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, si utilizza il formato EML conforme allo standard di riferimento RFC 2822/MIME.

6.1.3 metadati

Ciascuna classe documentale è identificata da metadati stabiliti nel documento SdC in relazione ai documenti informatici che il Cliente vuole conservare, quindi in base alle esigenze di identificazione e riconducibilità dei documenti stessi. In ogni caso, per ciascuna classe documentale, APSer.ARCHIVIO garantisce l'uso dei metadati minimi di cui all'allegato 5 del DPCM 3 dicembre 2013 e cioè

documento informatico (metadati minimi)

informazione	utile per	valore ammesso	tipo dato
identificativo	identificare univocamente il documento	qualsiasi	alfanumerico 20 char
data chiusura	data in cui il documento viene reso immodificabile	data	data formato gg/mm/aaaa
oggetto	breve riassunto del contenuto o natura del documento	testo libero	alfanumerico 100 char
soggetto produttore	soggetto che ha autorità e competenza a produrre il documento informatico	nome	alfanumerico 40
		cognome	alfanumerico 40
		codice fiscale	alfanumerico 16
destinatario	soggetto che ha autorità e competenza a ricevere il documento informatico	nome	alfanumerico 40
		cognome	alfanumerico 40
		codice fiscale	alfanumerico 16

documento informatico amministrativo (metadati minimi)

informazione	utile per	valore ammesso	tipo dato
identificativo	identificare univocamente il documento	qualsiasi	alfanumerico 20 char
amministrazione titolare	(segnatura) amministrazione titolare del registro di protocollo	codice IPA	codice IPA
AOO titolare	(segnatura) AOO titolare del registro di protocollo	codice IPA	codice IPA
data di protocollo	(segnatura) data di acquisizione del documento al registro di protocollo	data	data formato gg/mm/aaaa
progressivo di protocollo	(segnatura) numero progressivo di acquisizione del documento al registro di protocollo	da 1 a 9.999.999	numerico 7 char
oggetto	(segnatura) breve riassunto del contenuto o natura del documento	testo libero	alfanumerico 100 char
mitttente	soggetto che ha autorità e competenza a spedire il documento informatico	testo libero	alfanumerico 100 char
destinatario	soggetto che ha autorità e competenza a ricevere il documento informatico	testo libero	alfanumerico 100 char

fascicolo informatico (metadati minimi)

informazione	utile per	valore ammesso	tipo dato
identificativo	identificare univocamente il documento	qualsiasi	alfanumerico 20 char
amministrazione titolare	amministrazione titolare del procedimento che cura la costituzione e la gestione del fascicolo	codice IPA	codice IPA
amministrazioni partecipanti	amministrazioni che partecipano all'iter	codice IPA	codice IPA
responsabile del procedimento	soggetto che ha la responsabilità del procedimento	nome	alfanumerico 40
		cognome	alfanumerico 40
		codice fiscale	alfanumerico 16
oggetto	breve riassunto del contenuto o natura del fascicolo	testo libero	alfanumerico 100 char
documento	elenco degli identificativi dei documenti contenuti nel fascicolo	qualsiasi	alfanumerico 20 char

A titolo esemplificativo, si riportano di seguito i metadati standard utilizzati per le tipologie di documenti più comunemente posti in conservazione.

DETERMINAZIONI, ATTI LIQUIDAZIONE, ORDINANZE:

DATA_ADOZIONE	Data dell'atto
NUMERO_ADOZIONE	Numero dell'atto
OGGETTO	Oggetto dell'atto
CODICE_SETTORE	Codice del progressivo di settore
NUMERO_SETTORE	Numero del progressivo di settore
DATA_PUBBLICAZIONE_INIZIO	Data di inizio pubblicazione dell'atto
DATA_PUBBLICAZIONE_FINE	Data di fine pubblicazione dell'atto
SETTORE_PROPONENTE	Settore che effettua l'atto
UNITA_PROPONENTE	Unità organizzativa che effettua l'atto

DELIBERAZIONI:

DATA_ADOZIONE	Data dell'atto
NUMERO_ADOZIONE	Numero dell'atto
OGGETTO	Oggetto dell'atto
DATA_ESECUTIVITA	Data di esecutività dell'atto
DATA_PUBBLICAZIONE_INIZIO	Data di inizio pubblicazione dell'atto
DATA_PUBBLICAZIONE_FINE	Data di fine pubblicazione dell'atto
SETTORE_PROPONENTE	Settore che effettua l'atto
UNITA_PROPONENTE	Unità organizzativa che effettua l'atto

DOCUMENTO PROTOCOLLATO:

DATA	Data del protocollo generale
NUMERO	Numero del protocollo generale
ENTRATA_USCITA	Entrata/Uscita
OGGETTO	Oggetto
MITTENTI	Elenco mittenti
DESTINATARI	Elenco destinatari
DATA_DOCUMENTO	Data documento originale
NUMERO_DOCUMENTO	Numero documento originale

FATTURA:

NUMERO FATTURA	numero della fattura
DATA FATTURA	data della fattura
CODICE CLIENTE	eventuale codifica del cliente
RAGIONE SOCIALE	ragione sociale
PARTITA IVA	partita Iva
CODICE FISCALE	codice fiscale
IMPORTO	importo in euro della fattura
NUMERO PROTOCOLLO	eventuale numero di protocollazione
DATA PROTOCOLLO	eventuale data protocollazione
NUMERO MANDATO	eventuale numero del mandato di pagamento
DATA MANDATO	eventuale data del mandato
TIPO ATTO AMMINISTRATIVO	eventuale atto amministrativo associato
NUMERO ATTO AMMINISTRATIVO	eventuale numero atto amministrativo associato
DATA ATTO AMMINISTRATIVO	eventuale data atto amministrativo associato

CONTRATTO:

NUMERO CONTRATTO	numero del contratto
DATA ADOZIONE	data del contratto
OGGETTO	oggetto del contratto
CONTRAENTE DESCRIZIONE	ragione sociale del contraente
CONTRAENTE CODICE FISCALE	codice fiscale del contraente
DATA SCADENZA	data di scadenza del contratto
IMPORTO CONTRATTO	eventuale importo in euro del contratto.

Torna al sommario

6.2 Pacchetto di versamento

Il pacchetto di versamento dei documenti informatici da portare in conservazione è composto da un file compresso in formato .zip unito ad un file indice di versamento (di seguito chiamato IPdV), articolato per mezzo del linguaggio formale XML, che ne descrive il contenuto ed i dati relativi alla richiesta di versamento in conservazione.
Esso viene prodotto a cura del Cliente, nel rispetto del presente Manuale, del documento SdC e della norma cogente, e firmato digitalmente con propria firma digitale.

6.2.1 Informazioni presenti nell'indice pacchetto di versamento (IPdV)

Nell'IPdV vengono identificate le seguenti informazioni strutturate:

- Informazioni generali sul pacchetto di versamento

  Vengono riportati i codici identificativi nel pacchetto di versamento (lotto) e la sua descrizione, l'identificazione dell'ente che invia il pacchetto, la dimensione del pacchetto, l'utente di creazione, la data di scadenza del pacchetto e l'impronta del file compresso.

- Informazioni sull'unità documentale sottoposta a conservazione

  Vengono riportati i codici identificativi dell'unità e la sua descrizione, la tipologia di classe documentale, le indicazioni relative ai controlli da eseguire per l'unità e i dati relativi all'utente di inserimento, verifica o annullamento.

- Informazioni sui documenti

  Vengono riportati anno, data e descrizione del documento, l'utente di inserimento, la data di scadenza del pacchetto e l'impronta del file compresso.

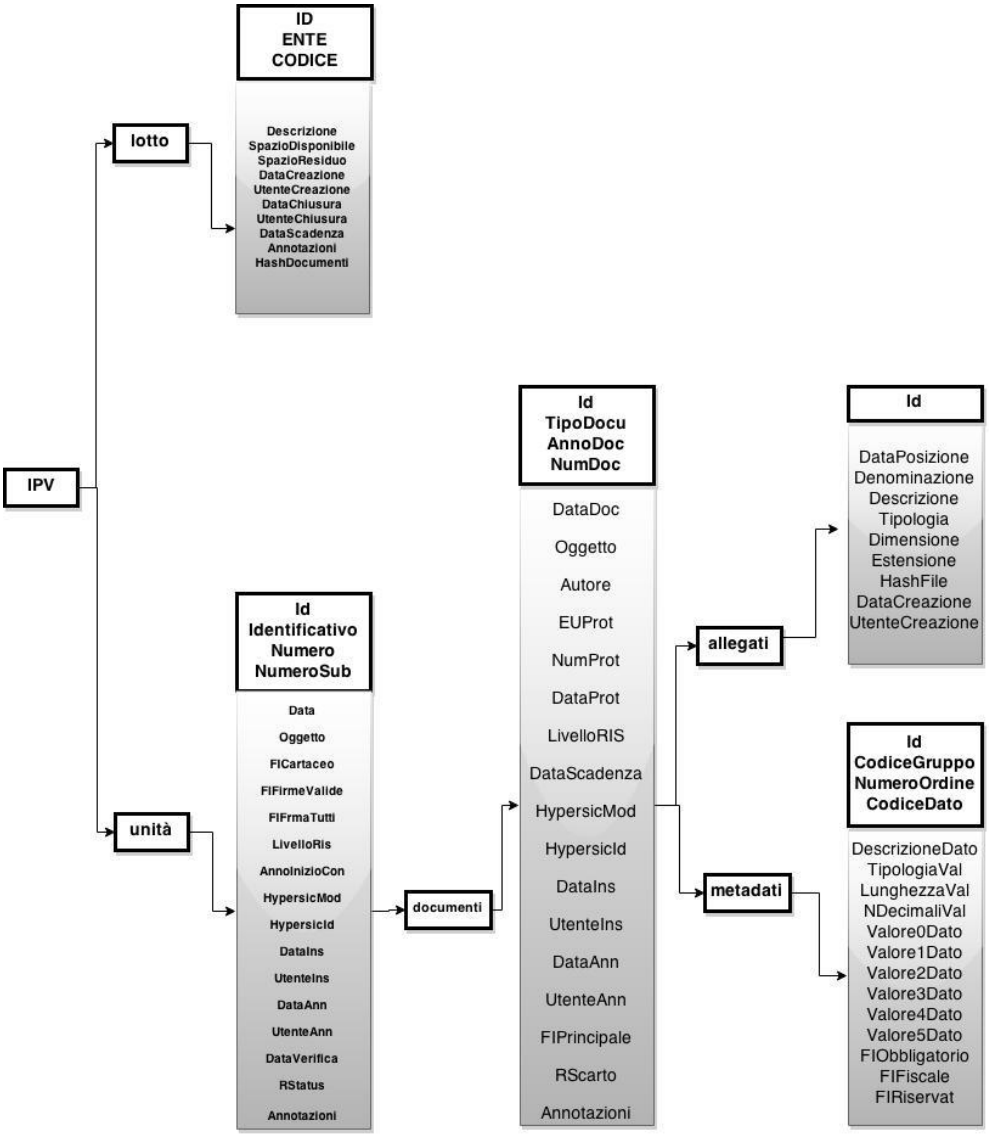
- Informazioni sui file fisici

  Vengono riportati denominazione completa (completa del sistema di indicizzazione adottato dal software di archiviazione), formato, dimensione e impronta del singolo file.

- Metadati

  Vengono riportati i metadati collegati all'unità documentale e la loro valorizzazione.

Si riporta di seguito la rappresentazione grafica dell'IPdV:



6.2.2 Personalizzazioni del pacchetto di versamento

Qualora un contratto preveda l'utilizzo di un pacchetto di versamento diverso da quanto qui descritto, per specificità o esigenze del Cliente, tale variazione viene espressamente descritta nel documento SdC.

Torna al sommario

6.3 Pacchetto di archiviazione

L'archiviazione dei documenti informatici portati in conservazione avviene presso lo storage all'uopo designato. Dei documenti informatici sottoposti a conservazione viene creato un indice del pacchetto di archiviazione (di seguito IPdA) conforme allo standard 'Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010)' ed all'allegato 4 del D.P.C.M. 03/12/2013.

6.3.1 Informazioni presenti nell'indice pacchetto di versamento

All'interno dell'elemento IPdA si trovano le seguenti strutture:

- informazioni generali relative all'indice del pacchetto di archiviazione:

  un identificatore dell'IPdA, il riferimento all'applicazione che l'ha creato ed eventuali riferimenti ad altri IPdA da cui esso;

- informazioni inerenti il Pacchetto di Archiviazione:

  l'identificatore del PdA, eventuali riferimenti ad altri PdA da cui esso stesso deriva, informazioni relative ad una eventuale tipologia/aggregazione (di natura logica o fisica) a cui il PdA appartiene;

- indicazione dei raggruppamenti di uno o più files che sono contenuti nel PdA:

  è possibile raggruppare files sulla base di criteri di ordine logico o tipologico ed assegnare, sia ad ogni raggruppamento che ad ogni singolo file, sia le informazioni di base che, mediante "ExtraInfo", dati definiti dall'operatore. Ogni elemento file contiene la sua impronta attuale, ottenuta con l'applicazione di un algoritmo di hash e un'eventuale impronta ad esso associata precedentemente[1];.

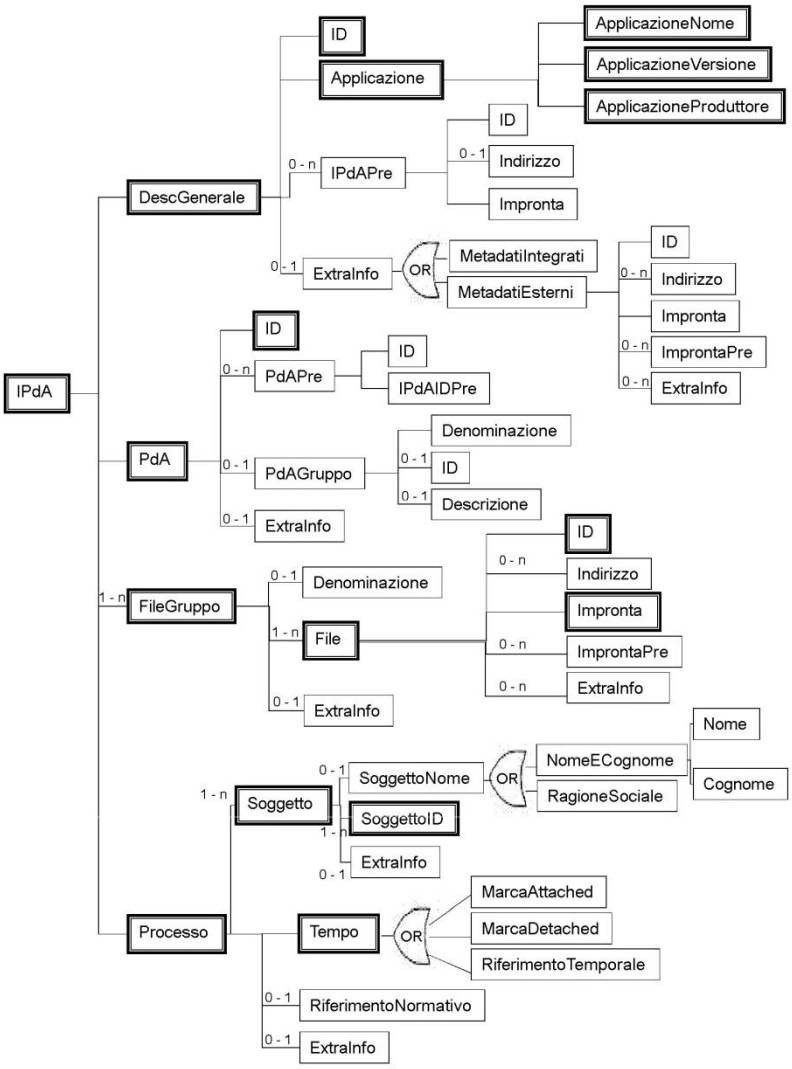
- informazioni relative al processo di produzione del PdA:

  l'indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione del PdA (es. responsabile della conservazione, delegato, pubblico ufficiale ecc.), il riferimento temporale adottato (generico riferimento temporale o marca temporale), l'indicazione delle norme tecniche e giuridiche applicate

[1] tra i molti vantaggi derivanti da questa scelta vi è la possibilità di gestire molto più agevolmente il passaggio da un algoritmo di hash ad uno più robusto, ad esempio perchè quello in uso potrebbe essere divenuto nel tempo meno sicuro.

per l'implementazione del processo di produzione del PdA.

Si riporta di seguito la rappresentazione grafica dell'IPdA:

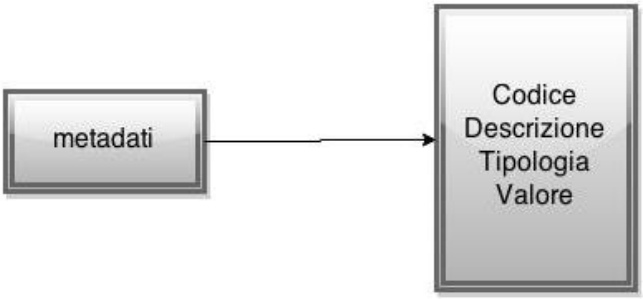


Gli elementi racchiusi nella cornice in grassetto sono obbligatori.

6.3.2 Struttura ExtraInfo dell'IPdA

APSer.Archivio consente la possibilità di produrre PdA con elementi appartenenti a classi documentali differenti tra di loro; per tale motivo viene all'interno delle ExtraInfo legate al FileGruppo, viene inserito l'identificativo dell'aggregazione documentale utilizzata, intesa come

campo chiave univoco del FileGruppo, ed una struttura di metadati legata ai singoli files associati; tale struttura segue la seguente rappresentazione grafica:



6.3.3 Personalizzazioni del pacchetto di archiviazione

Qualora un contratto preveda personalizzazioni del pacchetto di archiviazione, queste possono essere accettate solo se riferite a livello dell'intero pacchetto e, in quest'ambito, vengono inserite nelle ExtraInfo.
La nuova struttura dei dati richiesta deve essere espressamente descritta nel documento SdC.

Torna al sommario

6.4 Pacchetto di distribuzione

In adempimento a quanto prevede la norma, su richiesta del Cliente APSer.Archivio genera il pacchetto di distribuzione da consegnare al Cliente stesso ed un ulteriore pacchetto di distribuzione che viene custodito in una ubicazione differente del servizio di storage come ulteriore copia di backup.

Il pacchetto di distribuzione dei documenti informatici in conservazione è composto da un file compresso in formato .zip contenente copia dei documenti digitali in conservazione unito ad un file indice di distribuzione (di seguito chiamato IPdD), articolato per mezzo del linguaggio formale XML ed avente la medesima struttura dell'indice del pacchetto di archiviazione IPdA. Il pacchetto di distribuzione viene fornito su un supporto removibile.

Eventuali altri pacchetti di distribuzione possono essere richiesti dal Cliente nei termini e costi definiti all'interno del contratto di servizio per la conservazione e del documento SdC.

6.4.1 Informazioni presenti nell'indice pacchetto di distribuzione

All'interno dell'elemento IPdD si trovano le medesime strutture indicate per l'IPdA descritte in precedenza in questo Manuale.

6.4.2 Personalizzazioni del pacchetto di distribuzione

Qualora un contratto preveda personalizzazioni del pacchetto di distribuzione, queste possono essere accettate solo se coincidenti con analoghe modifiche al pacchetto di archiviazione, riferite a livello dell'intero pacchetto e, in quest'ambito, vengono inserite nelle ExtraInfo.
Tale personalizzazione deve essere espressamente indicata nel documento SdC.

Torna al sommario

7 IL PROCESSO DI CONSERVAZIONE

In seguito alla condivisione e configurazione del modello di funzionamento in questo Manuale, a regime, il processo di conservazione prevede diversi percorsi a seconda che l'obiettivo finale sia

- conservare
- esibire
- duplicare o copiare
- scartare
- riversare

i documenti informatici.

Sinteticamente, il processo di conservazione si espleta nelle seguenti fasi:

AZIONE	INPUT	OUTPUT
• Verifica del pacchetto di versamento e generazione del rapporto di versamento	Pacchetto/i di versamento da verificare	Rapporto di versamento
APSer.ARCHIVIO: Presa in carico del pacchetto di versamento; esecuzione di una serie di verifiche formali sulla completezza e sulla correttezza delle informazioni contenute nel file indice ai sensi del presente Manuale e del documento SdC e della corrispondenza dei documenti informatici allegati; generazione del rapporto di versamento, o del rapporto di sospensiva in caso ci siano incongruenze tra file indice e documenti informatici allegati o del ripudio del pacchetto di versamento in caso di anomalie bloccanti.		
• Creazione del pacchetto di archiviazione e chiusura dello stesso	Pacchetto/i di versamento che hanno superato la verifica con esito positivo	Creazione del pacchetto di archiviazione
APSer.ARCHIVIO: Creazione dell'indice del pacchetto di archiviazione IPdA (previsto dall'allegato 4 del DPCM 3 dicembre 2013) e sua conservazione unitamente al pacchetto di archiviazione, firma digitale del pacchetto e dell'indice da parte del RSC e apposizione della marca temporale tramite web-services pubblico messo a disposizione dal certificatore iscritto all'albo.		
• Creazione di pacchetto di distribuzione	Pacchetto/i di archiviazione	Creazione del pacchetto di distribuzione.
APSer.ARCHIVIO: Creazione di una o più copie del pacchetto di distribuzione nel rispetto delle medesime formalità per la generazione del pacchetto di archiviazione.		
• Scarto/Restituzione	Pacchetto/i di archiviazione "scaduti"	cancellazione o restituzione al Produttore
APSer.ARCHIVIO: individuazione dei pacchetti il cui termine ultimo di conservazione è scaduto e ne proposta di cancellazione dagli storage al RC per la necessaria autorizzazione. In assenza di		

AZIONE	INPUT	OUTPUT
autorizzazione o in concomitanza con la conclusione del rapporto contrattuale che ne determina il termine ultimo di conservazione presso APSer.ARCHIVIO, RSC restituisce formalmente i pacchetti al RC.		
• Riversamento	Pacchetto/i di archiviazione da riversare	Spostamento del/i pacchetto/i
APSer.ARCHIVIO: individuazione dei pacchetti che debbono essere trasferiti su diverso dispositivo hardware/software per dare continuità alla caratteristica di usabilità o altra valida motivazione. RSC propone, attraverso l'interfaccia gestionale APSer.ARCHIVIO, il riversamento a RC; RC deve autorizzarlo con firma digitale. Ottenuta tale autorizzazione, APSer.ARCHIVIO genera il nuovo indice e lo conserva unitamente al pacchetto nel nuovo dispositivo, inviando quindi la ricevuta di avvenuto riversamento al RC. Qualora invece l'autorizzazione non venga data da RC, APSer.ARCHIVIO restituisce al RC una ricevuta di diniego al riversamento.		
• Duplicazione/Copia	Documento archiviato	Duplicazione/Copia del documento
APSer.Archivio può rilasciare, su richiesta del Cliente, duplicati informatici secondo tale prassi: ricevuta la richiesta di duplicazione rintraccia il documento e ne predispone un un'estrazione in formato binario con verifica che non siano incorsi errori durante tale operazione. In questo modo si assicura che il documento scaricato contiene la stessa sequenza di bit del documento informatico conservato (ex art. 5 DPCM 14.11.2014). La consegna al Cliente avviene per mezzo di un download. APSer.Archivio non rilascia copie cartacee conformi agli originali digitali conservati, né copie cartacee in generale dei documenti informatici affidatigli in conservazione. APSer.Archivio rilascia duplicati solo su richiesta del Cliente e solo al Cliente; i fruitori, per esercitare il loro diritto di accesso, dovranno far richiesta di consultazione tramite il Cliente.		

Torna al sommario

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

Ogni pacchetto di versamento PdV è inviato dal Cliente ad APSer.ARCHIVIO utilizzando il canale di trasmissione (flusso in cooperazione applicativa, upload, PEC o supporto fisico) stabilito nel documento SdC.

Ogni pacchetto è costituito da:

- un file dati in formato archivio ZIP contenente i documenti da conservare;
- un file indice in formato archivio ZIP contenente:
- identificazione dell'ente richiedente la conservazione;
- identificazione univoca e descrizione del pacchetto di versamento;
- utente e data di creazione del pacchetto di versamento;
- dimensione dell'archivio zip contenente i documenti da conservare e sua

impronta hash generata mediante l'algoritmo SHA-256
- data di scadenza del pacchetto di archiviazione
- tutti i valori degli attributi di ogni singolo documento contenuto nell'archivio ZIP, il suo riferimento (path) all'interno del File dati stesso e sua impronta hash generata mediante l'algoritmo SHA-256.

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

Per ogni pacchetto di versamento vengono verificati i seguenti requisiti:

- conformità del pacchetto di versamento all'hash indicato nel file indice e sua completezza;
- conformità dei formati dei documenti sottoposti a conservazione;
- conformità dei documenti alle impronte indicate nel file indice;
- conformità delle firme digitali apposte sui documenti sottoposti a conservazione e sulla catena di autenticazione;
- validità delle firme al momento del versamento in base alla marca temporale apposta sul pacchetto di versamento;

Per l'intero pacchetto di versamento, nel file Log vengono dettagliatamente indicate

- la conformità o meno del PdV ai controlli
- per ogni singolo documento, le conformità o meno dei controlli di cui ai successivi punti.

In base alla tipologia delle anomalie il pacchetto, o i singoli documenti, possono assumere gli status:

- verifica positiva

  quando nei controlli non vengono rilevate non conformità e RSC può procedere con la creazione del pacchetto di archiviazione.

- verifica con warning

  quando nei controlli vengono rilevate non conformità definite non bloccanti dal Cliente a seconda della classe documentale (ad esempio, la mancanza della firma digitale o un riscontro della stessa sulle CRL nel caso in cui la firma digitale sul documento non sia richiesto). In questo caso il RSC procede comunque alla creazione del pacchetto di archiviazione.

- verifica negativa

  Le seguenti anomalie generano una verifica negativa e causano lo scarto del pacchetto o del singolo documento:

- Hash non corrisponde a quello indicato
- CNIPA - Formato non riconosciuto
- CRL - Certificato revocato
- CRL - Non valida

  Nel caso in cui venga richiesta la conservazione di documenti informatici firmati digitalmente, generano una verifica negativa, e quindi lo scarto del pacchetto o del singolo documento informatico, anche le seguenti anomalie:

- Firma non presente
- Crittografia - Firma non valida
- Certificato - Non valido alla data indicata
- Certificato - Scaduto alla data indicata
- Certificato - Non risulta essere 'NON RIPUDIABILE'.
- Chain - Catena di emissione non valida
- CRL - Non presente
- CRL - Non scaricabile
- CRL - Scaduta
- CRL - Certificato scaduto

  In caso di verifica negativa APSer.Archivio non procede alla formazione del pacchetto di archiviazione ma sospende il PdV in attesa di ricevere i documenti informatici congruenti con l'IPdV; solo quando tutto il PdV ottiene lo status di verifica positiva o verifica con warning allora si procede con la generazione del pacchetto di archiviazione.
  Nel caso in cui lo status negativo riguardi tutti i documenti del PdV allora APSer.Archivio rifiuta il PdV.

Di ciascun passaggio APSer.Archivio invia al RC opportuna segnalazione; le azioni vengono registrate nel file di Log che viene associato al PdV.

Torna al sommario

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

Nel caso in cui il pacchetto abbia superato le verifiche e se ne sia riscontrata la conformità, il Log viene arricchito dei seguenti messaggi:

- pacchetto di versamento conforme alle specifiche;
- formato del documento conforme alle specifiche;
- impronta del documento conforme alle specifiche;
- firma digitale conforme alle specifiche;
- firma digitale valida al momento del versamento;

L'esito delle verifiche effettuate viene inserito in un rapporto di versamento, che viene inviato al Cliente, unitamente ad un file XML che il Cliente può utilizzare per aggiornare il proprio sistema documentale con le indicazioni relative al processo di versamento.
Prima di essere inviato al Cliente, il rapporto di versamento viene firmato digitalmente dal RSC che gli appone anche un riferimento temporale con riferimento al Tempo Universale Coordinato (UTC). La Firma e le Marche Temporali utilizzate sono emesse da un certificatore iscritto all'albo ai sensi delle vigenti disposizioni legislative; in particolare le Marche Temporali vengono apposte tramite web-services pubblici messi a disposizione dal certificatore medesimo.
Copia del file firmato e marcato temporalmente viene salvato su idonei supporti di storage e collazionato con l'operazione di versamento eseguita.

Torna al sommario

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

Nel caso in cui il pacchetto non abbia superato le verifiche e se ne sia riscontrata la non conformità, il log viene arricchito dei seguenti messaggi:

- Hash non corrisponde a quello indicato
- Firma non presente
- CNIPA - Formato non riconosciuto
- Crittografia - Firma non valida
- Certificato - Non valido alla data indicata
- Certificato - Scaduto alla data indicata
- Certificato - Non risulta essere 'NON RIPUDIABILE'.
- Chain - Catena di emissione non valida
- CRL - Non presente

- CRL - Non scaricabile
- CRL - Non valida
- CRL - Scaduta
- CRL - Certificato revocato
- CRL - Certificato scaduto

L'esito delle verifiche effettuate viene inserito in un rapporto di rifiuto, che viene inviato al Cliente unitamente al file indice IPdV ed al log in cui vengono riportati i controlli effettuati e gli esiti.
Prima di essere inviato al Cliente, il rapporto di rifiuto viene firmato digitalmente dal RSC che gli appone anche un riferimento temporale con riferimento al Tempo Universale Coordinato (UTC). La Firma e le Marche Temporali utilizzate sono emesse da un certificatore iscritto all'albo ai sensi delle vigenti disposizioni legislative; in particolare le Marche Temporali vengono apposte tramite web-services pubblici messi a disposizione dal certificatore medesimo.
APSer.Archivio mantiene i PdV rifiutati in un'area dello storage in attesa che venga disposta la loro bonifica da parte del RC; la permanenza in tale area si può protrarre non oltre i 12 mesi, trascorsi i quali RSC provvederà ad applicare il procedimento dell'annullamento. Lo stesso accade se RC dichiara la non risolvibilità delle problematiche riscontrate dalle verifiche del PdV; tale comunicazione, notificata dal RC al RSC nei modi scelti e descritti nel documento SdC, autorizza RSC ad annullare il PdV e a non considerarlo più in futuri controlli.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Il RSC, in caso di esito positivo delle verifiche sul pacchetto di versamento, avvia la procedura automatizzata di conservazione che genera l'indice del pacchetto di archiviazione previsto dall'allegato 4 del DPCM 3 dicembre 2013 e lo conserva unitamente ai documenti informatici sottoposti a conservazione.

Ogni pacchetto di archiviazione è costituito da:

- una serie di file di documenti informatici memorizzati su idonei supporti di storage
- un file indice XML generato con la struttura prevista dall'allegato 4 del DPCM 3 dicembre 2013

Per la generazione del pacchetto di archiviazione, APSer.Archivio svolge automaticamente le seguenti attività per ogni singolo documento informatico posto in conservazione:

- verifica dello status del documento
- salvataggio del file da conservare in idoneo supporto di storage;
- calcolo dell'impronta del file costituente il documento informatico (hash mediante algoritmo SHA-256)
- annotazione, sul file di log relativo alla creazione del pacchetto di archiviazione, delle operazioni svolte e loro esito (corrette o con segnalazione di errori).

Concluso tale iter per tutti i documenti informatici del PdV, APSer.Archivio genera l'indice del pacchetto di archiviazione come descritto a pagina 35, includendo il file di log delle operazioni svolte nelle ExtraInfo legate al processo.

Il RSC firma digitalmente l'IPdA a testimonianza della correttezza delle operazioni eseguite e, successivamente, appone la marca temporale ai fini dell'estensione di validità dei documenti soggetti a conservazione.
Le Marche Temporali apposte dal RSC sono emesse da un certificatore iscritto all'albo ai sensi delle vigenti disposizioni legislative e hanno validità quinquennale.

Torna al sommario

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

Il PdD può essere generato solo su richiesta del Cliente, che allo scopo utilizza l'interfaccia web messa a disposizione da APSer.Archivio (ndr – hyperSIC.Archivio, hyperSIC.PortalArchivio).

Sempre tramite questa interfaccia il RC può ricercare ed eventualmente visualizzare i propri documenti informatici sottoposti a conservazione; a seguito dell'accesso a tale funzionalità il RC può visualizzare la lista di tutte le categorie documentali per le quali effettuare la sua ricerca. Successivamente, selezionando la tipologia di interesse, gli viene proposta una scheda, costruita dinamicamente in base alle caratteristiche della classe documentale, che il RC potrà utilizzare per inserire tutti i parametri in base

ai quali effettuare la ricerca del documento informatico conservato.
Alla conferma APSer.Archivio esegue la ricerca e propone la lista di documenti che rispondono ai parametri selezionati. Per ciascun documento della lista viene mostrato:

- una scheda che consente la visualizzazione di tutte le informazioni disponibili per il documento informatico conservato;
- un link che consente di effettuare un duplicato (download) del documento informatico conservato.

A questo punto il RC seleziona i documenti da includere nel PdD e ne avvia la richiesta di generazione ad APSer.Archivio.
APSer.Archivio, genera quindi il PdD che è costituito da:

- un file dati in formato archivio ZIP contenente i documenti da esibire
- un file indice XML generato con la struttura prevista dall'allegato 4 del DPCM 3 dicembre 2013

Il RSC appone sull'indice del pacchetto di distribuzione la propria firma digitale a testimonianza della correttezza delle operazioni eseguite.
A questo punto il RC riceve, per mezzo del canale di trasmissione concordato nel documento SdC, il PdD che ha richiesto.

Nell'ambito delle potenzialità di ricerca nel proprio archivio conservato, il RC può visualizzare tutte le informazioni disponibili per il documento informatico di interesse e risalire all'intero pacchetto di archiviazione per verificarne anche la validità di Firma Digitale e di Marca Temporale.

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

La produzione di copie o duplicati dei documenti conservati avviene da parte di personale autorizzato del Cliente mediante l'interfaccia web nativa messa loro a disposizione da APSer.ARCHIVIO (ndr – modulo hyperSIC.Archivio, hyperSIC.PortalArchivio).
Il recupero del documento informatico conservato avviene come per l'esibizione con la differenza che è possibile selezionare la funzionalità di "produzione copia"; questa predispone una copia del documento nel formato richiesto (digitale o cartaceo) apponendo le corrette indicazioni di conformità al documento in conservazione come previsto dal CAD.

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Lo scarto dei documenti avviene al termine del periodo di conservazione indicato dal RC nella creazione del pacchetto di versamento ed avviene mediante la cancellazione dei documenti informatici e dei file degli attributi dal sistema di storage.
Preventivamente alla cancellazione è compito del RC chiedere la relativa autorizzazione allo scarto alla competente Soprintendenza archivistica e far pervenire detta autorizzazione a RSC di APSer.ARCHIVIO; in assenza di tale autorizzazione, ed in concomitanza con la scadenza del contratto per il servizio di conservazione stipulato tra le parti (ndr- Cliente e a.p.systems), RSC applica il procedimento della restituzione a RC degli archivi di competenza.

Torna al sommario

7.9 Annullamento dei pacchetti di versamento

Nel caso in cui il RC ravvisi versamenti fatti per errore e ne faccia precisa richiesta nelle modalità descritte nel documento SdC o nel caso in cui il PdV sia rifiutato da oltre 12 mesi ed il RC non abbia provveduto alla sua bonifica, APSer.Archivio effettua l'annullamento del PdV (e del rispettivo PdA se esistente): i pacchetti vengono marcati come "annullati" e non vengono considerati nelle ricerche. I pacchetti non vengono però cancellati fisicamente dallo storage.

Torna al sommario

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

In caso di recesso o scadenza del contratto di servizio della conservazione, a.p.systems riversa tutti i documenti informatici del Cliente, affidatigli in conservazione completi dei files a corredo per la loro corretta tenuta in archivio, nel sistema di conservazione indicato dal RC con funzione conforme allo standard UNI SinCRo su canali sicuri concordati con RC, secondo modalità e tempi indicati nel documento SdC. Tale archivio verrà mantenuto da APSer.Archivio fino a conclusione del riversamento e a valle di verifiche svolte insieme dal RC e RSC e che abbiano raggiunto esito

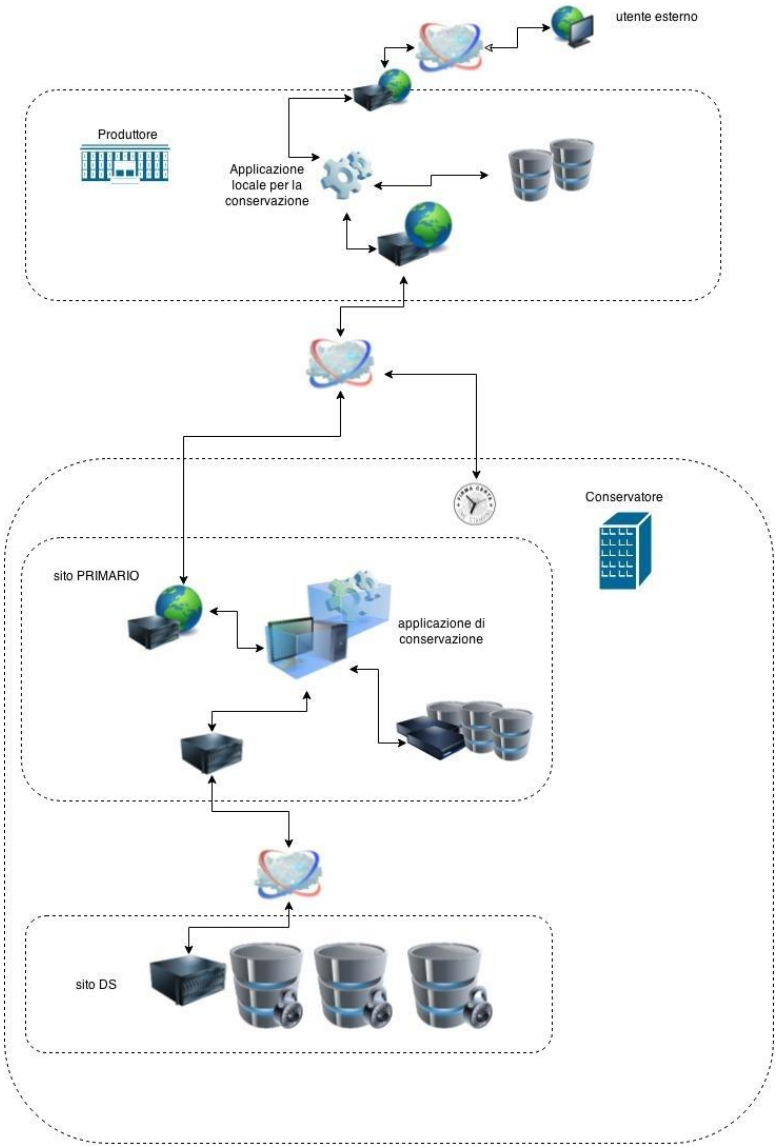
positivo; solo al termine di tale risultato, e comunque solo in presenza dell'autorizzazione del MIBACT, RSC darà luogo alla cancellazione dell'archivio del Cliente e garantirà la non leggibilità dei dati ad esso associati.

Anche nel caso in cui il Cliente voglia confluire un suo archivio da un conservatore terzo in APSer.Archivio, APSer.Archivio è in grado di riceverlo in formato Uni SinCRo nel canale di comunicazione protetto e concordato con il Cliente.
Qualora il conservatore terzo non sia in grado di operare nel rispetto dello standard UNI SinCRo, a.p.systems può supportare il Cliente per consentire il trasferimento in base ad accordi specifici al di fuori del servizio di conservazione stesso.

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE

L'architettura del sistema di conservazione APSer.ARCHIVIO è rappresentata dal seguente schema



8.1 Componenti logiche, tecnologiche, fisiche

Tutte le risorse critiche a livello interstrutturale sono state ridondate con meccanismi di duplicazione delle risorse e di attivazione di meccanismi di alta disponibilità. Inoltre al fine di raggiungere la più alta disponibilità di servizi e di consentire disponibilità anche in caso di aggiornamenti o errore

umano, si sono ridondati i servizi applicativi più critici, seguendo uno schema di distribuzione sulle risorse ad ogni livello seguendo schemi di distribuzione che massimizza la disponibilità anche in caso di fallimenti multipli che colpiscono i vari livelli dell'infrastruttura.

Le risorse critiche ridondate sono:

- Database in cluster con tecnologia in alte disponibilità e senza storage condivisi.
- Bilanciatori di carico e Firewall configurati in alta disponibilità. Per ridurre i rischi di interruzione della connettività, di indisponibilità dei servizi e di abbassamento dei controlli di sicurezza perimetrali.
- Server web applicativi multipli e in bilanciamento, per massimizzare la disponibilità dei servizi SaaS.

Per quanto riguarda l'alimentazione elettrica sono presenti apparati magneto-termici autoriarmanti in modo da evitare cadute di tensione in caso di problemi transitori (es.: sovratensioni temporanee) ed è stata effettuata la suddivisione delle fasi e ribilanciamento sulla base degli effettivi carichi.
Sono installati UPS performanti e dotati di management e la configurazione di questi UPS avviene in modo ridondato sugli alimentatori dei server, inoltre è installato un gruppo elettrogeno con potenza minima sufficiente a garantire alimentazione elettrica in caso di indisponibilità della fornitura di rete, per il Datacenter e gli armadi di rete di piano.

Server

I server dedicati alla conservazione sostitutiva sono basati su host fisici su cui vengono eseguite le macchine virtuali su sistema di virtualizzazione VMWare vSphere 5.5:

Host fisici: gli host fisici su cui vengono eseguite le macchine virtuali indicate sono più server fisici HP Proliant DL380p G8 su cui è stato installato e configurato hypervisor vSphere in modalità cluster HA

Host Virtuali: negli host virtuali la parte Application/Web è installata su macchine virtuali server Microsoft Windows 2012 R2 con IIS in bilanciamento di carico e ridondanza (webhost2, webhost3, …) disposti a gruppi su host di virtualizzazione separati Il bilanciamento è generato da 2 bilanciatori Linux con servizi in HA (LVS) mentre la parte di DBMS è installata su macchine virtuali con sistemi operativi Microsoft Windows 2012 R2 su 2 macchine virtuali dbnode1 e dbnode2, disposte

su 2 host di virtualizzazione separati.

Database

Il DBMS usato su sistemi operativi Microsoft Windows 2012 R2 è SQL Server 2012 in configurazione ridondata (AlwasyOn).

Storage

Il sottosistema storage, su cui risiedono i dischi delle macchine virtuali indicate, è costituito da 4 storage HP Lefthand (StoreVirtual) in tecnologia SAS, configurati in NetRaid-10.
L'accesso agli storage avviene tramite interfacce di rete configurate in numero di 4 per ogni storage con tecnologia Multi-pathing. In questo modo il guasto fino a 3 switch, cavi, schede di rete degli storage non impatta sull'accesso ai dati. Inoltre i protocolli di aggregazione dei flussi utilizzati, consentono un canale di comunicazione verso gli storage più elevato rispetto alla connessione singola.

Connettività

il sottosistema di rete su cu insiste il sistema di conservazione è costituito da 4 switch in cluster con connessioni ridondanti e in bilanciamento di ogni componente (host virtualizzazione, storage, ecc.). Gli switch sono HP5120 in configurazione IRF.
La configurazione della connessione tra i due router Fastweb e la sezione Internet dei 4 switch IRF è realizzata in modo tale da consentire failover automatico e trasparente sia in caso di fallimento di uno dei due router Fastweb che di uno degli switch IRF.

Sistemi di backup

Il backup viene eseguito salvando le immagini complete delle macchine virtuali in modo consistente, secondo le politiche descritte nel documento di sicurezza della attività operative aziendali – procedura 12.
Anche il Backup delle configurazioni dei sistemi operativi di virtualizzazione (hypervisor), vengono effettuati con periodicità indicata nel predetto documento.
Le aree di recovery sono rappresentate dai nastri di backup. Alcuni files contenenti dati di recovery sono le directory in cui sono contenuti i backup di SQL Server a cui ha accesso solo il Responsabile dei Sistemi Informativi.
Di seguito i dati salienti delle politiche di backup, dettagliatamente descritte nei documenti ISO27001
Politiche di Backup dei dati
Le politiche di backup si fondano principalmente sull'utilizzo di tre

strumenti di backup:

- Veeam Backup & Recovery (backup e recovery intere macchine virtuali "Restore Entire Backup" o "Instant VM Recovery")
- Veeam Backup & Recovery (backup e recovery singoli file mediante "File Level Recovery")
- SQL Server Backup (FULL + LOG)

Per quanto riguarda Veeam i valori di RPO e RTO vengono specificati nella policy di backup e si riferiscono alla disponibilità dell'intera macchina virtuale e dei dati in essa contenuti
I backup delle VM e dei database sono riversati inoltre su dispositivi rimovibili (RDX). I dispositivi rimuovibili così costituiti e contenenti tutti i backup della settimana precedente, sotto la responsabilità del Direttore Assistenza e Customer Care vengono trasportati presso una sede esterna dotata di cassaforte e impianto anti-intrusione.
Per consentire il ripristino di dati a lunga scadenza si utilizzano dispositivi rimovibili mensili e annuali.
Per ogni tipologia di backup viene inviata una notifica mail al Responsabile dei Sistemi Informativi e agli Amministratori di Sistema.
Le copie di backup su cassetta vengono portate all'esterno con cadenza settimanale.
È in essere una procedure per garantire l'integrità e la consistenza dei dati contenuti nei supporti magnetici utilizzati per le copie di backup (verifica di ogni backup eseguita dal sistema per ogni supporto al termine del backup stesso più verifiche periodiche di restore a campione).
In caso di danneggiamento dei dati o degli strumenti di elaborazione esistono specifiche procedure interne di ripristino.
In caso di perdita di dati, il responsabile del settore richiede via mail al Responsabile del Sistema Informativo la necessità di restore. Il Responsabile del Sistema Informativo in collaborazione con il richiedente esegue restore da NAS, in posizione originale o in altra posizione al fine di verificare la presenza dei dati richiesti e consegnarli al richiedente.
Tutto il sistema di backup e sotto diretto controllo del Responsabile dei Sistemi Informativi (RSI).

Disaster Recovery Plan

IL DRP è allegato al Business Continuity Plan del Sistema di Gestione della Sicurezza (SGSI) di a.p.systems e disciplina procedure e attività atte a garantire, nel caso di un evento distruttivo, il ripristino delle applicazioni informatiche critiche per l'azienda entro un tempo limitato, rispondente alle esigenze del business aziendale e tendente a limitare il più possibile le perdite causate dall'interruzione dell'attività.

Il piano prevede soluzioni tecnologiche ed organizzative tali da permettere all'azienda di continuare ad operare nelle sue attività critiche durante l'emergenza e fino al ritorno ad una situazione di normalità. La designazione dei processi che devono essere coperti da Disaster Recovery è definita dal CdS sulla base dell'analisi dei rischi e della valutazione degli investimenti strutturali da stanziare per la continuità di ogni processo in base alla sua criticità per l'azienda.
La parte iniziale del Piano contiene:

- Indicazione dei livelli di servizio
- Localizzazione delle sedi fisiche di recovery
- Struttura del team responsabile dell'attuazione del Piano stesso ed escalation
- Struttura e compiti del personale del gruppo operativo di emergenza
- Condizioni di attivazione del Piano
- Periodo di validità e sua ultima data di revisione
- Indicazione della durata massima dell'utilizzo delle sedi fisiche di recovery

Lo sviluppo del Piano si articola nei seguenti argomenti:

- Protezione dei dati nelle sedi fisiche di recovery
- Soluzioni di recovery per le attività principali
- Procedure di back- up (interne od esterne)
- Dettagli relativi per la notifica dell'emergenza ai clienti, fornitori e approvvigionamenti
- Procedure di reperibilità del personale e servizi trasferiti
- Localizzazione delle utilities nelle sedi fisiche di recovery
- Modalità di trasferimento dei dipendenti e della documentazione alle sedi fisiche di recovery
- Predisposizione e distribuzione dei posti di lavoro nella sede di recovery
- Localizzazione degli enti o istituzioni rilevanti nella zona delle sedi fisiche di recovery
- Modalità di contatto di manodopera straordinaria per supporto operativo
- Procedure di sicurezza delle sedi fisiche di recovery
- Modalità e procedure di rientro sul sito principale

Gli allegati riguardano:

- Gestione delle comunicazioni interne all'azienda
- Gestione delle comunicazioni esterne all'azienda
- Modalità di reperimento del personale necessario

- Moduli di reporting e monitoring
- struttura organizzativa per l'applicazione del Piano in caso di emergenza, il suo aggiornamento e le esercitazioni periodiche per valutarne l'efficacia. La struttura comprende i componenti del CdS e i responsabili d'area coinvolti nei processi che rientrano nel piano.

applicazione di conservazione

Per la parte gestionale, APSer.ARCHIVIO si basa sulla suite applicativa web-nativa hyperSIC® di a.p.systems; in particolare si sfrutta il modulo hyperSIC.Archivio a cui si accede attraverso una connessione internet e con il quale vengono gestite tutte le fasi del processo di conservazione sia da parte dell'Ente che di a.p.systems.
Infatti con hyperSIC.Archivio sono costruiti gli iter procedurali grazie ai quali il Produttore da una parte ed il Conservatore dall'altra collaborano e lavorano ai fini della conservazione.

E' definito un processo formale, con specifica procedura, di assegnazione, revisione e cancellazione delle utenze per accedere al sistema di conservazione. Tale processo formale è applicato a chiunque abbia necessità di accedere al sistema.
Sulla base di tale processo formale sono previste le seguenti attività minime:

- assegnazione di un solo user ID per persona, con utilizzo di utenze di gruppo solo per eccezioni strettamente controllate e preventivamente autorizzate;
- la richiesta di rilascio dello user ID deve pervenire da persona autorizzata ed il il rilascio formalmente approvato;
- consegna di un documento all'utente autorizzato con i suoi diritti di accesso e con le eventuali verifiche e controlli previsti dal processo di conservazione, con accettazione da parte dell'utente;
- manutenzione dell'elenco storico delle credenziali di accesso assegnate.

Sono periodicamente analizzate e riviste le credenziali di accesso al sistema di conservazione, sulla base della periodicità descritta nel processo e formalizzata nella procedura, per accertare che la necessità di accesso sia ancora valida.

Torna al sommario

8.2 Conduzione e manutenzione del sistema di conservazione

L'avviamento di nuovi Clienti e la gestione operativa vengono effettuate in conformità a quanto previsto dalla procedura PQ3CSiC del Sistema di Gestione Integrato della Qualità e Sicurezza di a.p.systems.

La gestione del sistema di conservazione è affidata al RSM che, in collaborazione con RSI, ne pianifica gli eventuali aggiornamenti, gli Upgrade e le eventuali sostituzioni previa approvazione del RSC.
La metodologia adottata per la messa in produzione dei nuovi sistemi è quella di pianificare un progetto specifico che preveda le seguenti fasi:

1. Predisposizione sistema di test
2. Replica di tutte le funzionalità del sistema
3. Collaudo
4. Predisposizione delle procedure di ripristino situazione iniziale
5. Predisposizione delle procedure di controllo e verifica nuovo sistema
6. Parallelismo (ove possibile) vecchio nuovo sistema
7. Rilascio del nuovo sistema
8. Periodo di controllo e verifica

La metodologia adottata per la gestione degli aggiornamenti (Patch Management) prevede invece la seguente procedura:

1. Acquisizione delle informazioni sugli aggiornamenti
2. Valutazione dell'effettiva necessità d'aggiornamento
3. Eventuale installazione sui sistemi
4. Breve verifica/collaudo delle principali funzioni e applicazioni aziendali (applicazione delle patch a sistemi di test)
5. Rilascio autorizzazione all'aggiornamento sui sistemi interni (applicazione delle patch ai sistemi di produzione)

Torna al sommario

8.3 Change Management

Le procedure di controllo dei cambiamenti nel sistema di conservazione prevedono l'applicazione della seguente prassi:

1. Ogni richiesta di cambiamento viene valutata e concordata dal RSC, dal RSI e da RSM.
2. RSC e RSI, in collaborazione con RSM, effettuano l'analisi delle modifiche e rilascia un Work Order con tutte le specifiche
3. RSI effettuano le modifiche del caso garantendo la possibilità di

ripristino e il mantenimento delle funzioni standard

4. RSM procede al test in ambiente di sviluppo e in ambiente di produzione limitando, in un primo momento, le funzionalità di sistema (per esempio: bloccando le code di invio mail) per poi procedere all'effettiva validazione.

Nel caso in cui il cambiamento richieda la modifica di codice comune o di funzionalità generiche al sistema di conservazione, RSM deve concordare la variazione con il RSI; eventuali test aggiuntivi vengono eseguiti per garantire la stabilità del sistema.
Al termine della modifica vengono rilasciati gli strumenti necessari al RSC per testare e validare la modifica stessa in fase di test e in fase di produzione/validazione.
Infatti, in caso di modifica, alle applicazioni viene modificato lo stato dell'applicazione da stato di produzione a stato di validazione che obbliga il RSC e lo staff tecnico ad un monitoraggio approfondito della produzione della nuova applicazione.
La documentazione di supporto completa l'analisi precedentemente redatta dal RSC e viene divulgata al personale interessato. Ove fattibile, si integrano le procedure per il controllo dei cambiamenti e per l'applicazione. Le procedure per i cambiamenti comprendono:

1. Mantenere una registrazione dei livelli di autorizzazione concordati
2. Assicurare che i cambiamenti siano sottoposti da utenti autorizzati
3. Riesaminare i controlli e le procedure per l'integrità così da assicurare che non saranno compromessi dai cambiamenti
4. Identificare tutti i software, le informazioni, le registrazioni nel database e gli hardware che necessitano modifiche
5. Ottenere approvazione formale per le proposte dettagliate prima che il lavoro cominci
6. Assicurarsi che l'attuazione sia svolta in modo da minimizzare stravolgimenti aziendali
7. Mantenere un controllo sulla versione per tutti gli aggiornamenti di software
8. Mantenere una traccia di audit di tutte le richieste di cambiamento
9. Assicurare che l'attuazione dei cambiamenti abbia luogo al momento giusto e non disturbi i processi aziendali coinvolti

Torna al sommario

8.4 Verifica periodica di conformità normativa e standard di riferimento

a.p.systems tiene sotto controllo la conformità ai requisiti cogenti, normativi e contrattuali alimentando un elenco gestito da RSC, RSGI, e RSSC.
L'elenco viene mantenuto aggiornato selezionando i riferimenti normativi di interesse per il sistema di conservazione.

Torna al sommario

9 MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

APSer.Archivio consente di monitorare le fasi di versamento e archiviazione nonché lo stato di vita dell'archivio attraverso un sistema software web-based (ndr –hyperSIC.Archivio, hyperSIC.PortalArchivio) accessibile, con opportune credenziali rilasciate in base a quanto definito nel documento SdC, sia dal RC che dal RSC. Sempre da tale ambiente, APSer.Archivio offre l'opportunità di ottenere statistiche e reports sul servizio di conservazione reso al Cliente.

Al RSC vengono inoltre sottoposti gli esiti dei test di funzionamento dell'ambiente sistemistico (hardware, software e networking) dei siti che costituiscono il data-center di APSer.Archivio, a cura del RSSC e del RSI.
Se presenti esiti negativi, RSC apre la procedura di "incidente della sicurezza". Nel caso siano evidenziate criticità o eventuali punti di miglioramento, queste sono oggetto di esame e proposta di intervento, da concordare con RC del Cliente solo se impattante verso i suoi archivi.

Sotto il profilo sistemistico si rimanda la Piano della Sicurezza del Sistema di Conservazione APSer.Archivi, paragrafo "monitoraggio e controlli".

Torna al sommario

9.2 Verifica dell'integrità degli archivi

L'integrità degli archivi è assicurata da quanto previsto nel piano della sicurezza per il sistema di conservazione e dalle tecnologie in uso da APSer.Archivio; per le verifiche e misure adottate ad assicurare l'integrità si demanda a quanto previsto nel suddetto piano.

Tuttavia, i documenti informatici affidati in conservazione ad APSer.Archivio vengono sottoposti a verifica per ulteriori due livelli: sull'integrità e consistenza dei PdA e sull'effettività leggibilità dei documenti informatici conservati.

Torna al sommario

9.2.1 Verifica dell'integrità e della consistenza dei pacchetti di archiviazione e degli indici dei documenti generati dal Processo di Conservazione, in carico al RC;

La verifica dell'impianto documentale e la sua concreta attuazione ed applicazione viene eseguita annualmente all'interno del piano degli auditing interni previsti dalle norme ISO 27001 e ISO 9001. Inoltre su base annuale un ente terzo accreditato effettua le verifiche sull'erogazione del servizio.

Torna al sommario

9.2.2 Verifica dell'effettiva leggibilità dei documenti informatici inseriti all'interno dei lotti, in carico al RSC.

RC con cadenza biennale supervisiona il processo di controllo della consistenza e l'integrità dei pacchetti di documenti informatici, dei relativi files attributi e dei files di indice delegandone l'esecuzione ai tecnici specializzati della struttura a.p.systems: per questo, con cadenza biennale RSC verifica anche che, per i formati dei file utilizzati per la conservazione dei documenti, sia disponibile sul mercato un visualizzatore aggiornato e conforme alle specifiche del singolo formato di file. Il monitoraggio è supportato anche dall'esito di test di validità sempre in esercizio ed eseguiti automaticamente da APSer.Archivio.
La procedura viene effettuata sui dati presenti all'interno del sistema di storage e sulle copie di sicurezza custodite dal RSC.
RC può controllare il monitoraggio e gli esiti dei test specifici attraverso l'interfaccia applicativa di APSer.ARCHIVIO (hyperSIC.Archivio) in qualsiasi momento.

Torna al sommario

9.2.3 registro delle verifiche periodiche

Tutte le procedure di verifica, gli eventuali interventi sul software applicativo, le modifiche delle configurazioni, l'assegnazione delle deleghe a svolgere opportune operazioni, nonché tutti gli avvenimenti importanti o ritenuti tali dai RC e RSC, ai fini del corretto svolgimento del processo di conservazione, sono opportunamente tracciati su un apposito registro custodito presso APSer.ARCHIVIO.

Torna al sommario

9.3 Soluzioni adottate in caso di incidenti della sicurezza

Le segnalazioni di incidenti inerenti la sicurezza, sono una responsabilità di tutti i dipendenti e collaboratori di a.p.systems e sono fondamentali per un miglioramento della sicurezza del sistema di conservazione APSer.Archivio. Gli incidenti della sicurezza comprendono oltre agli atti volontari, anche gli atti involontari (Es.: l'apparecchiatura è posizionata in maniera tale da provocare urti o rischi di malfunzionamento). Tutte queste segnalazioni sono classificabili come incidenti della sicurezza, intendendo per incidente l'indisponibilità, la non integrità o la non riservatezza del documento informatico in conservazione.
Per segnalare un incidente inerente la sicurezza del sistema di conservazione ci sono diversi strumenti: la posta elettronica aziendale e il SIA. Il destinatario della segnalazione è il RSSC (RSSC).

La segnalazione di un incidente deve contenere le seguenti informazioni:

- Tipologia di incidente
    - Sicurezza fisica - alcuni esempi di violazione della sicurezza fisica sono: accessi o tentativi di accesso alla sede aziendale di personale non autorizzato esterno, accessi volontari o involontari di personale interno ad aree riservate, violazione delle norme di accesso alle aree riservate, etc.
    - Sicurezza operativa - alcuni esempi di violazione della sicurezza operativa sono: comunicazione di informazioni confidenziali o riservate a personale non autorizzato, violazioni del regolamento aziendale, violazioni delle policy "Clear desktop policy" o "Apparecchiature fuori sito e Telelavoro", etc.
    - Sicurezza logica - alcuni esempi di violazione della sicurezza logica sono: anomalie software, hardware e netware del sistema di

conservazione, l'utilizzo di apparecchiature non autorizzate all'interno della sede APS, danneggiamento volontario o involontario di apparecchiature di proprietà di APS, violazione delle norme di utilizzo dei beni personali (Computer, palmare, etc.), utilizzo improprio delle credenziali di accesso e dei relativi diritti.

- Informazioni temporali/geografiche
    - Data e ora dell'incidente;
    - Luogo dell'incidente.
    - Personale coinvolto
- Indicazioni relative al personale dipendente, ai collaboratori o personale esterno coinvolto nell'incidente inerente la sicurezza.
- Descrizione dell'incidente
    - Descrizione dell'incidente come percepito.

RSSC definisce con il RSC il trattamento da effettuare quale risposta all'incidente verificatosi.

Sulla base della analisi condotta e registrata RSSC, in collaborazione con RSGI, valuta l'opportunità di aprire una NC sul SGI al fine di raccogliere le prove, individuare le cause e definire Azioni Correttive da implementare a livello procedurale, tecnico o di risorse umane. Analogamente nel caso di incidenti mancati o potenziali RSSC e RSGI valutano l'apertura di NC potenziali che a fronte dell'analisi delle cause potrebbero dar luogo ad Azioni Preventive. La gestione delle NC e delle AC/AP viene effettuata in conformità a quanto previsto rispettivamente dalle procedure PQ 0.7 e PQ 5.2. del Sistema di Gestione Integrato Qualità e Sicurezza di a.p.systems.
RSSC ove necessario storicizza le prove raccolte in merito all'incidente verificatosi e segnala a RSGI la necessità di aprire una NC.

Torna al sommario