

Manuale di Conservazione

di ARCHIVIUM SRL

EMISSIONE DEL DOCUMENTO

Titolo Documento	Manuale della Conservazione Archivium Srl
Responsabile di Processo	Elena Lauritano
Autore	Carlotta Landi
Verificato da	Elena Lauritano
Approvato da	Mariarosa Carucci
Stato del Documento	In vigore
Data Ultima Versione	20/09/2015
Numero Versione	3.6

REGISTRO DELLE VERSIONI

N. Versione	Data Versione	Autore	Verificato/Approvato	Descrizione delle Modifiche
0.1	01/06/2007	Elena Lauritano		Prima Stesura del documento
1.0	15/06/2007	Elena Lauritano	Mariarosa Carucci	Modifiche per nuovi modelli documentali
2.0	31/08/2008	Elena Lauritano	Mariarosa Carucci	Modifiche per adeguamento ArchiCons 2.0
3.0	01/02/2010	Elena Lauritano	Mariarosa Carucci	Modifiche per adeguamento modalità di firma digitale
3.1	31/03/2014	Elena Lauritano	Mariarosa Carucci	Modifiche per Adeguamento Normativo Regole Tecniche
3.2	30/06/2014	Elena Lauritano	Mariarosa Carucci	Modifiche per Adeguamento Fatturazione Elettronica vs PA
3.3	10/01/2015	Elena Lauritano	Mariarosa Carucci	Adeguamento per nuove modalità di firma automatica
3.4	31/03/2015	Elena Lauritano	Mariarosa Carucci	Adeguamento traccia Agid
3.5	16/06/2015	Elena Lauritano	Mariarosa Carucci	Adeguamento AGID e ISO 27001:2013
3.6	20/09/2015	Carlotta Landi	Elena Lauritano	Adeguamento contenuti ad indice Agid

Indice generale

1. SCOPO E AMBITO DEL DOCUMENTO.....	3
1.1 Scopo del Manuale.....	3
1.2 Contesto di riferimento.....	4
2. TERMINOLOGIA (GLOSSARIO, ACRONIMI).....	5
3. NORMATIVA E STANDARD DI RIFERIMENTO.....	13
3.1 Normativa di riferimento.....	13
3.2 Standard di riferimento.....	14
4. RUOLI E RESPONSABILITÀ.....	15
4.1 Responsabili del sistema di Conservazione.....	15
4.2 Altri Ruoli.....	18
5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE.....	20
5.1 Organigramma.....	20
5.2 Strutture Organizzative.....	21
6. OGGETTI SOTTOPOSTI A CONSERVAZIONE.....	25
6.1 Oggetti conservati.....	25
6.2 Pacchetto di versamento.....	28
6.3 Pacchetto di archiviazione.....	30
6.4 Pacchetto di distribuzione.....	34
7. IL PROCESSO DI CONSERVAZIONE.....	34
7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico.....	38
7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	39
7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico.....	41
7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	42
7.5 Preparazione e gestione del pacchetto di archiviazione.....	43
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 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori.....	49
8. IL SISTEMA DI CONSERVAZIONE.....	50
8.1 Componenti Logiche e Tecnologiche.....	50
8.2 Componenti Fisiche.....	52
8.3 Procedure di gestione e di evoluzione.....	54
8.4 Change management.....	55
9. MONITORAGGIO E CONTROLLI.....	56
9.1 Procedure di monitoraggio.....	56
9.2 Verifica dell'integrità degli archivi.....	57
9.3 Soluzioni adottate in caso di anomalie.....	58
9.4 Incident Management.....	58
9.5 Release Management.....	59
9.6 Event Management.....	59

1. SCOPO E AMBITO DEL DOCUMENTO

1.1 Scopo del Manuale

Il Manuale di Conservazione è lo strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 8 del DPCM 3 Dicembre 2013.

Il presente Manuale è prodotto in formato digitale da parte di Archivium in collaborazione con il Cliente, pubblicato in apposito repository del Servizio ad uso interno Archivium e fornito al Cliente ed è reso pubblico nel formato .Pdf sul quale viene apposta la firma digitale del legale rappresentante ed è conservato secondo le disposizioni della normativa vigente

Il Manuale descrive l'organizzazione, i soggetti coinvolti e i relativi ruoli, il processo, le architetture e le infrastrutture utilizzate per erogare il Servizio di Conservazione Digitale a Norma. Inoltre vengono descritte anche le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento del sistema di conservazione. In particolare sono descritte le procedure operative adottate da Archivium per il procedimento di conservazione elettronica a norma di legge.

Il manuale della Conservazione è correlato ad altri documenti che descrivono in maniera puntuale il contesto dell'erogazione del Servizio di Conservazione Digitale a Norma per ciascun singolo cliente.

Tipo Documento	Descrizione
Allegato Tecnico alle Condizioni Generali di Servizio	Questo documento è frutto dell'analisi "as is " e "dlivery to be" e riguarda specifiche condizioni tecnico funzionali e procedurali del processo di conservazione. Questo documento è parte integrante delle Condizioni Generali di Servizio sottoscritte dal Cliente prima dell'attivazione del servizio.
Allegato A al Manuale della Conservazione – Specificità del Contratto	Questo documento esplicita, per ciascun singolo cliente, eventuali specificità in merito all'organizzazione, ai soggetti coinvolti e ai ruoli svolti dagli stessi, al modello di funzionamento, alla descrizione del processo, alla descrizione delle architetture e delle infrastrutture utilizzate, alle misure di sicurezza adottate.
Piano di Sicurezza	Il Piano della Sicurezza (PdS) descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI) dell'organizzazione esclusivamente per quanto attiene le attività di conservazione documentale ex DPCM 3 dicembre 2013 e, quindi, inerenti quanto definito nell'ambito del Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni).

1.2 Contesto di riferimento

Conformemente a quanto previsto dalle Regole Tecniche in materia di sistema di conservazione (DPCM 3 dicembre 2013, di seguito “Regole Tecniche”) all’art. 5 comma 2, lett. B, il servizio viene proposto da Archivium in qualità di “Terza parte fidata” e consente la conservazione elettronica a norma di legge di documenti elettronici e/o analogici, in outsourcing. Il manuale riassume i compiti che sono descritti dalle *Regole Tecniche* e dal *Codice dell’Amministrazione Digitale*, si seguito anche “CAD” (Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche/integrazioni).

Archivium srl eroga servizi di gestione documentale che possono comprendere tutte le fasi di vita del documento, dalla sua formazione, alla sua gestione, per procedere con l’archiviazione ed infine la conservazione. Si possono logicamente distinguere i processi di:

Processi di Gestione Documentale, all’interno dei quali si svolgono attività di:

- Acquisizione della copia digitale di documenti analogici cartacei e/o elettronici;
- Estrazione dei metadati identificativi dei documenti da archiviare;
- Pubblicazione su applicativi Web di consultazione e ricerca dei documenti archiviati.

Processi di Conservazione Documentale a Norma che invece vengono analizzati all’interno del Manuale della Conservazione.

Archivium propone il Servizio di Conservazione Digitale a Norma (CDN) erogandolo in modalità di Full Outsourcing. Tale modalità è supportata dall’articolo 44 del CAD in base al quale la conservazione può essere svolta affidandola, in modo totale o parziale, ad altri soggetti che offrono idonee garanzie organizzative e tecnologiche, nonché accreditati come conservatori presso l’Agenzia per l’Italia digitale.

Il Cliente sceglie di delegare il ruolo di Responsabile della Conservazione ad una figura esterna, incaricando Archivium ed accettando la soluzione proposta in sede di sottoscrizione del Condizioni Generali di Servizio e suoi allegati. Inoltre Archivium assumerà il Ruolo di Responsabile Esterno del Trattamento dei dati personali (D.Lgs 196/03)

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Convenzioni di lettura e acronimi

Di seguito i principali acronimi utilizzati nel documento e relative definizioni:

TERMINE	DEFINIZIONE
AgID	Agenzia per l'Italia Digitale
Archivium	Società Archivium Srl. (anche Archivium)
CA	Certification Authority, cioè ente accreditato per l'emissione e la gestione di certificati di firma qualificata
CAD	Codice dell'Amministrazione Digitale, Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche/integrazioni
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate Revocation List, liste di certificati digitali revocati
FTPS	FTPS (anche conosciuto come FTP-ES, FTP-SSL e FTP Secure) è un'estensione del comunemente usato File Transfer Protocol (FTP) che aggiunge supporto per il Transport Layer Security (TLS) e il Secure Sockets Layer (SSL), protocollo crittografico.
HASH	Impronta informatica di un documento ottenuta applicando una "funzione di hash" e costituita da una sequenza di simboli binari.
HTTP	Hyper Text Transfer Protocol (identificativo convenzionale per un sito)
HTTPS	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client.
IPdA	<i>Indice del Pacchetto di Archiviazione</i> – evidenza informatica associata ad ogni pacchetto di archiviazione contenente un insieme di informazioni articolate secondo lo standard SInCRO
NAS	Network Attached Storage, dispositivi ad alta capacità, sicurezza ed affidabilità per la memorizzazione dei dati

PADES-T	PDF Advanced Electronic Signature, formato standard di firma su PDF, con informazioni aggiuntive rispetto al formato base (PADES-BES) per includere la marca temporale
PdA	Pacchetto di archiviazione

TERMINE	DEFINIZIONE
PKCS#7	Standard della sintassi dei messaggi crittografici, usato per firmare o criptare messaggi in una infrastruttura a chiave pubblica (PKI).
Piano della Sicurezza	Piano della sicurezza del sistema di conservazione
PO	Process Owner
RDC	Responsabile della Conservazione
RSIS	Responsabile dei Sistemi e della Sicurezza
SinCRO	Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI11386:2010) - Standard nazionale in linguaggio xml, riguardante la struttura dell'insieme di dati a supporto del processo di conservazione
TSA	Time Stamping Authority, infrastruttura necessaria a realizzare e svolgere la funzione di timbratura temporale.
UTC	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee –CCIR)

Definizioni

Di seguito si riporta il glossario dei termini contenuti nelle regole tecniche di cui all'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni in materia di documento informatico e sistema di conservazione dei documenti informatici che si aggiungono alle definizioni del citato decreto ed a quelle del decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445 e successive modificazioni e integrazioni.

TERMINE	DEFINIZIONE
accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
attestazione di conformità di copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da Notaio o altro Pubblico Ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
autenticazione del documento Informatico	La validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore, o alle circostanze, anche temporali, della redazione.

TERMINE	DEFINIZIONE
autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	Collezione di dati registrati e correlati tra loro
certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
codice o CAD	Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione

TERMINE	DEFINIZIONE
destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	Produzione di duplicati informatici
esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione
firma elettronica avanzata	L'insieme dei dati in forma elettronica, allegati oppure connessi ad un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi sono stati successivamente modificati.
firma elettronica qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica ed una privata, correlate tra loro, che consente al titolare, tramite la chiave privata e al destinatario tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti

TERMINE	DEFINIZIONE
generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
insieme minimo di metadati del documento informatico integrità	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
marca temporale	evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale; la marca temporale prova l'esistenza in un certo momento di una determinata informazione, sotto forma di struttura dati firmata da una Time Stamping Authority;

TERMINE	DEFINIZIONE
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3/12/2013
pacchetto di archiviazione	Detto anche PdA, pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3/12/2013 e secondo le modalità riportate nel manuale di conservazione
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato e descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione

TERMINE	DEFINIZIONE
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
referimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.
staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

Per ogni altra definizione è possibile far riferimento all'allegato 1 alle Regole Tecniche di cui all'art. 71 del CAD in materia di documento informatico e sistema di conservazione dei documenti informatici

3. NORMATIVA E STANDARD DI RIFERIMENTO

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, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65- Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- Decreto del Presidente del Consiglio 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005

3.2 Standard di riferimento

- 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.

4. RUOLI E RESPONSABILITÀ

4.1 Responsabili del sistema di Conservazione

Di seguito sono indicate le attività svolte e i nominativi delle persone che ricoprono i ruoli elencati nella tabella seguente, così come individuati nel documento “Profili professionali” pubblicato da Agid.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe	Periodo nel ruolo
Responsabile del servizio di conservazione	Elena Lauritano	- Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione - Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente - Corretta erogazione del servizio di Conservazione all'ente produttore - Gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione. - Gestione dell'esercizio delle componenti software del sistema di conservazione	Dal 2007 ad oggi	Mariarosa Carucci	Dal 2007 ad oggi
Responsabile Sicurezza dei sistemi per la conservazione	Elena Lauritano	- Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza. - Segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Dal 2007 ad oggi	Fabio Volpe	Dal 2015 ad oggi

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe	Periodo nel ruolo
Responsabile funzione archivistica di conservazione	Daniele Codebò	<i>Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato.</i> - Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici. - Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione. - Collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Dal 2013 ad oggi		
Responsabile trattamento dati personali	Mariarosa Carucci	- Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. - Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Dal 2007 ad oggi		

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe	Periodo nel ruolo
Responsabile sistemi informativi per la conservazione	Fabio Volpe	- Gestione dell'esercizio delle componenti hardware del sistema di conservazione. - Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore. - Segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di Conservazione e individuazione e pianificazione delle necessarie azioni correttive. - Pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione - Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione.	Dal 2015 d oggi		
Responsabile sviluppo e manutenzione del sistema di conservazione	Umberto Casotto	- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione. - Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione. - Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione. - Interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche. - Gestione dello sviluppo di siti web e portali connessi al servizio di Conservazione.	Dal 2014 ad oggi	Rosa Gambarota	Dal 2014 ad oggi

Le responsabilità attinenti ad Archivium in qualità di delegato dal RCN sono definite nella Lettera di Delega fornita dal Cliente in conformità a quanto previsto dalla normativa.

Il nominativo del Responsabile della Conservazione Del Cliente e del Responsabile del Trattamento dei Dati sono indicati nell'Allegato A – Specificità del Contratto nel quale sono anche riportate le attività affidate al Responsabile del Servizio di Conservazione. Come richiesto dalla normativa, Archivium svolge la propria funzione con la massima cura e presidio attraverso un gruppo di risorse specialistiche dedicate all'erogazione, gestione, supporto, presidio del Servizio, in base ad una stabile organizzazione interna aziendale. In tal modo garantisce la presenza di personale qualificato e diversificato in base alle specifiche esigenze, munito di preparazione professionale e di conoscenze tecniche adeguate, disponibile all'interazione con il responsabile della conservazione del Cliente nelle varie fasi del Servizio.

4.2 Altri Ruoli

Responsabili del Cliente: Titolare, “Process Owner” e “Referente IT”

Archivium srl prevede all'interno del processo di conservazione digitale a norma l'individuazione di figure supplementari a quelle individuate dai profili professionali sopra riportati nella tabella – coinvolgendo di fatto il cliente con dei propri referenti all'interno del servizio. Queste figure professionali vengono individuate all'interno della struttura organizzativa del cliente e presidiano il dominio del servizio all'interno della propria struttura con competenze e responsabilità specifiche. Le figure coinvolte sono: il Titolare, il Process owner e il Referente IT.

Il Titolare è il soggetto titolare della documentazione, ovvero il Cliente che invia al Sistema di Gestione/ Archiviazione Documentale la documentazione da archiviare e conservare.

Il Titolare può inviare due tipologie di flussi documentali:

- quello cartaceo che viene digitalizzato attraverso il service di scansione
- quello elettronico (servizio di mail farm, ftp, omogeneizzazione documentale, arricchimento/epurazione flussi)

Il Titolare interviene nel Sistema di Conservazione come “Titolare dei contenuti” oggetto del processo

Il Process Owner ed il Referente IT:

- sono responsabili di quanto accade nel proprio perimetro di sicurezza per quanto riguarda la costruzione ed il trasferimento dei pacchetti informativi, nonché del rispetto delle modalità e delle tempistiche di invio.
- definiscono la lista della gestione degli accessi e le relative permission degli utenti, che potranno accedere in modalità profilata ai singoli archivi.
- Se contrattualizzato, questi referenti hanno la possibilità di indicare il responsabile o l'utente che può fare richiesta dei pacchetti di distribuzione su supporti fisici autoconsistenti con esplicita indicazione per il loro recapito, in aggiunta alla modalità di richiesta standard tramite portale web (per i soli utenti abilitati)
- qualora si rendesse necessario in caso di richiesta di esibizione, il Process Owner è autorizzato a richiedere l'intervento del Responsabile del Servizio di Conservazione.

Il Processo Owner è di fatto un profondo conoscitore dei processi di formazione e gestione delle tipologie documentali da sottoporre a conservazione – è dotato altresì di conoscenze tecniche così da supportare il Responsabile del Servizio di Conservazione nella definizione degli standard di processo. Tramite gli strumenti del portale web messi a disposizione e la reportistica, il Processo Owner monitora l'andamento e la completezza di quanto sottoposto a conservazione.

Il process owner ha completa conoscenza e visibilità su quanto deve essere conservato ed è responsabile del controllo sull'effettiva completezza di quanto è stato ricevuto dall'outsourcer.

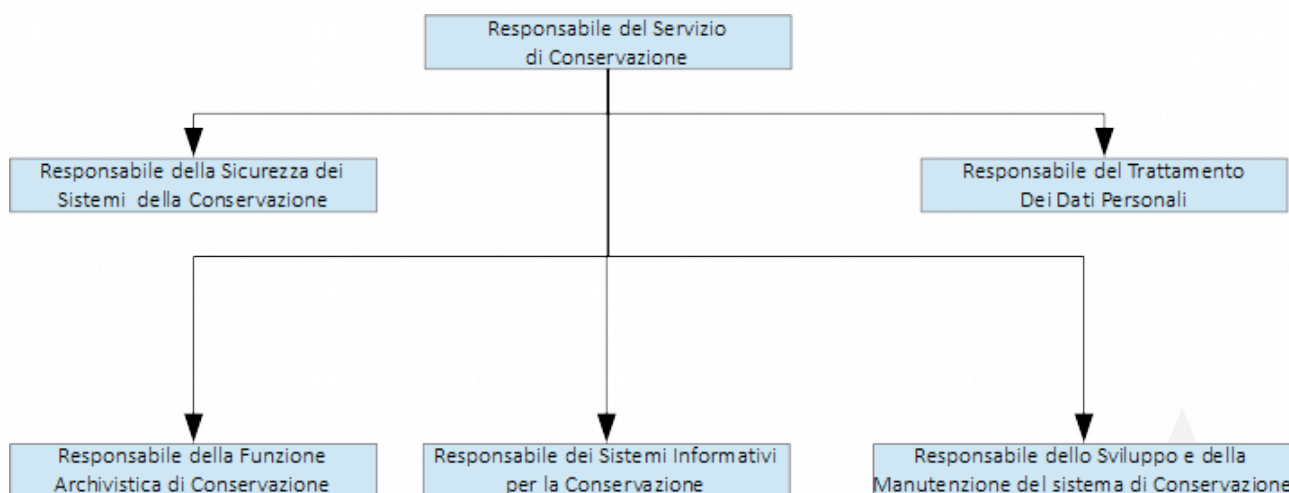
Il Referente IT esegue di fatto operativamente il controllo sui singoli flussi trasferiti all'outsourcer. Il sistema di conservazione provvede alla produzione di rapporti di log ogniqualvolta un documento venga trasferito dal perimetro del cliente a quello dell'outsourcer. Il referente IT monitora i rapporti e verifica la coincidenza in termini di quantità e qualità dei documenti trasferiti e ricevuti dall'outsourcer, analizzando le eventuali anomalie ricevute dal sistema di presa in carico dei documenti. La gestione delle anomalie prevede qualora venisse individuato un pattern reiterato eventuali change requests che possono essere richieste direttamente al supporto tecnico dell'outsourcer.

Il Referente IT è la figura di intermediazione tecnica tra il Process Owner del cliente e l'outsourcer.

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Viene riportato di seguito l'organigramma presente in Archivium Srl per la gestione del processo di conservazione digitale a norma. 5.2 Strutture organizzative



Archivium offre servizi di gestione documentale in full outsourcing e distingue i suoi servizi in processi di:

- Gestione e Archiviazione Documentale ai fini della ricerca e consultazione il cui fine è quello di normalizzare, organizzare, e rendere consultabili via web i documenti elettronici
- Conservazione Digitale a Norma

Le due tipologie di servizio sono logicamente distinte e solo le seconde sono oggetto del presente Manuale. Allo scopo di garantire un adeguato e soddisfacente livello di qualità dei servizi offerti, la struttura aziendale di Archivium è organizzata per processi; a livello aziendale è quindi definito il quadro generale di riferimento delle procedure e delle relative competenze e responsabilità. Ogni collaboratore, individualmente o come partecipante ad un team, per competenza, si attiene alle indicazioni delle procedure e delle istruzioni aziendali definite dal Sistema Integrato Qualità e Sicurezza. Le attività sono assegnate in base ai ruoli aziendali definiti. Anche il processo di Conservazione è posto in essere sulla base di questo quadro organizzativo sia per gli aspetti di erogazione che di monitoraggio. Il processo di conservazione impone alle aziende l'istituzione di una struttura ed una organizzazione, coerente con le proprie politiche di efficienza gestionale, che garantisca la piena osservanza di tale normativa. A tal scopo, in base alle specifiche necessità aziendali, il Conservatore, sia dal punto di vista della impostazione operativa delle attività di conservazione, sia dal punto di vista della scelta delle risorse coinvolte nel processo, organizza il lavoro affinché esso venga svolto secondo i principi stabiliti dalla legislazione.

5.2 Strutture Organizzative

Attività proprie di ciascun contratto di servizio di conservazione

<i>Id</i>	<i>Tipo Attività</i>	<i>Descrizione</i>
1	Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	Il processo si avvia con la sottoscrizione da parte del Cliente del contratto che sancisce le modalità e le caratteristiche del servizio da erogare.
2	Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	Archivium, se necessario, implementa per conto del Cliente un Sistema di Gestione Documentale che precede il Processo di Conservazione Digitale a Norma che si conclude con la formazione del PdV. Sui PdV vengono effettuati controlli sulla conformità dei formati e dei metadati. I documenti e i metadati sono pronti per entrare nel sistema di versamento, la catena di custodia viene garantita a partire dall'entrata dei documenti nel sistema di versamento. Una volta entrati nel sistema di versamento, per ciascun flusso documentale viene generato un rapporto di versamento ed un relativo eventuale rapporto di scarto in mancanza di congruità con il modello documentale di conservazione o di integrità dei documenti. Il rapporto di versamento, se previsto contrattualmente, può essere sottoscritto con firma elettronica avanzata dal Conservatore attraverso una procedura di firma massiva.
3	Preparazione e gestione del pacchetto di archiviazione	Vengono definite le tempistiche e le cadenze con le quali i documenti appartenenti ad un modello documentale debbono essere processati. Vengono definite le regole di costruzione del pacchetto di archiviazione, si tratta di una divisione o di un raggruppamento dei documenti sulla base di uno più metadati. Sulla base delle regole di group/ungroup e di schedulazione per ciascun modello documentale associato all'azienda cliente vengono creati i pacchetti di archiviazione. L'attività della creazione del pacchetto di conservazione prevede la creazione dell'evidenza informatica in formato UniSincro, che viene firmata e marcata temporalmente dal Conservatore. I pacchetti di archiviazione vengono salvati nel repository e diventano consultabili da apposito portale web. Le azioni propedeutiche alla preparazione del Pacchetto di Archiviazione consistono nel verificare l'adeguatezza dei file ai requisiti per la pacchettizzazione. Nel caso in cui il pacchetto di archiviazione sottoposto alla procedura non risulti idoneo, il sistema restituisce un errore, evidenziandone anche la causa. La segnalazione di errore rimane tracciata all'interno dell'applicazione. L'evidenza informatica, firmata e marcata temporalmente dal Responsabile del Servizio di Conservazione, unitamente ai documenti con relativi metadati di conservazione formano il pacchetto di archiviazione che viene inserito sul portale di esibizione ArchiCons. L'accesso al portale ArchiCons è consentito ai soli utenti accreditati (ovvero che possiedono il certificato X509 emesso durante la profilazione dell'utente dal responsabile del servizio di conservazione).

Id	Tipo Attività	Descrizione
4	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	L'utente abilitato, previa strong authentication, accede al pannello delle richieste del pacchetto di distribuzione scegliendo quali documenti desidera che vengano inseriti nel pacchetto di distribuzione. La richiesta viene inviata tramite notifica al Conservatore. Il Conservatore provvede alla creazione del pacchetto di distribuzione, sottoscrivendo il nuovo Indice di Conservazione con firma digitale (o elettronica qualificata) e apponendo una marca temporale. Una procedura automatica crea un supporto (file) compresso contenente i documenti e le evidenze dell'avvenuto processo di conservazione. Il pacchetto di distribuzione viene messo a disposizione dell'utente sul portale e notificato via mail.
5	Scarto dei pacchetti di archiviazione	Nel caso in cui il pacchetto di archiviazione sottoposto alla procedura non risulti idoneo, il sistema restituisce un errore, evidenziandone anche la causa. La segnalazione di errore rimane tracciata all'interno dell'applicazione.
6	Chiusura del servizio di conservazione (al termine di un contratto).	Il Cliente viene informato della eventuale dismissione delle utenze entro 30 giorni dalla data di recesso/scadenza del Contratto. Allo scadere del 30esimo giorno dalla data di recesso/scadenza del Contratto, Archivium: • Disattiva il Cliente all'interno dell'Anagrafica; • Disattiva le utenze associate al Cliente; • Revoca il Certificato; • Cancella i documenti e i dati relativi ai singoli record dei documenti. Al termine delle operazioni di chiusura degli account, Archivium invia al Cliente una mail nella quale conferma l'avvenuta cancellazione di tutti i documenti e dei dati relativi.

Ruolo- Attività	Titolare	Produttore	Responsabile Servizio della Conservazione	Utente
Produzione del documento	R, A			
Invio dei documenti al sistema di gestione documentale	R	R, C	A	
Ricezione dei flussi documentali		R	A	
Normalizzazione e Omogeneizzazione dei flussi documentali		R, C	A	
Creazione del Pacchetto di Versamento		R	A	
Invio ed eventuale sottoscrizione del Rapporto di Versamento			A, R	
Creazione e sottoscrizione del Pacchetto di Archiviazione			A, R	
Ricerca e consultazione dei documenti conservati			A	R
Richiesta Pacchetto di Distribuzione			A	R
Creazione ed invio del Pacchetto di Distribuzione			A, R	

Qui sopra viene proposta la matrice delle responsabilità degli attori coinvolti nel Processo di Conservazione Digitale a Norma (RACI – Responsible, Accountable, Consulted, Informed)

Attività proprie di gestione dei sistemi informativi:

Conduzione e manutenzione del sistema di conservazione

Attività	Ruoli coinvolti	Descrizione
Gestione dei malfunzionamenti	Supporto Tecnico	In caso di anomalie relative al corretto funzionamento del sistema di conservazione, intervengono una serie di processi a supporto: - <i>Incident Management</i> : è il processo deputato a raccogliere segnalazioni di malfunzionamento da parte dei Clienti, verificare l'effettiva anomalia ed intervenire per consentire al Cliente di effettuare le attività necessarie. - <i>Event Management</i> : è il processo deputato a raccogliere le segnalazioni provenienti dai sistemi di monitoraggio, interpretarle ed attivare i processi specifici a supporto (in caso di malfunzionamento attiva il processo di Incident, in caso di cambio di stato verificare il processo di Change management per assicurarsi che il cambiamento sia stato autorizzato, ecc).
Gestione dei cambiamenti	RSIS / Supporto tecnico	Per apportare modifiche applicative e/o infrastrutturali è necessario che queste vengano autorizzate: il processo di <i>Change Management</i> è finalizzato ad assicurare che ciascun cambiamento sia autorizzato dal ruolo avente i diritti autorizzativi. Questo processo è finalizzato anche ad effettuare l'analisi dei rischi legati ai cambiamenti.
Evoluzione del sistema di conservazione	RSIS / Supporto tecnico	Per quanto concerne la verifica del corretto dimensionamento interviene il processo di <i>Capacity Management</i> , il quale, grazie al supporto dell'Event Management, è in grado di identificare potenziali cali di performance, indicando quali attività intraprendere per evitare degradi nell'erogazione del servizio (svuotamento dei dischi, compressione dei file, aggiunta di risorse, ecc).

L'infrastruttura è così composta:

Sito primario c/o Datacenter COLT Telecom di Torino - Via Livorno 60, 10144 Torino (TO)

Sito primario presso il quale viene esercitato il servizio di conservazione documentale (società esterna)

Sito secondario c/o Datacenter Seeweb di Frosinone - Corso Lazio 9a, 03100 Frosinone (FR)

Sito secondario presso il quale viene esercitato il servizio di Disaster Recovery (società esterna) – sito a 600 Km dal sito primario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il sistema di conservazione di Archivium, denominato Archicons, in attuazione di quanto previsto dall'articolo 44, comma 1, del CAD, assicura la conservazione elettronica a norma di legge, tramite l'adozione di regole, procedure e tecnologie, dei documenti dei clienti, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità nel tempo..

Il sistema di conservazione Archicons provvede a gestire l'intero ciclo dell'oggetto conservato nell'ambito del processo di conservazione, dalla sua presa in carico, alla conservazione, fino allo scarto.

Si intende per oggetto di conservazione sia il singolo documento, che eventualmente il fascicolo documentale all'interno del quale il documento è inserito.

Il sistema Archicons, aderendo al modello di gestione degli oggetti sottoposti a conservazione OAIS - Open Archival Information System, e conseguentemente anche delle Regole Tecniche, prevede il trattamento degli stessi all'interno di pacchetti informativi distinguibili in Pacchetti di Versamento, Pacchetti di Archiviazione e Pacchetti di Distribuzione.

6.1 Oggetti conservati

Il sistema di conservazione deve assicurare l'identificazione univoca e la reperibilità dei documenti conservati e dei fascicoli informatici nei quali essi sono eventualmente inseriti. Per poter raggiungere tale obiettivo è necessario procedere all'identificazione delle tipologie documentali da sottoporre a conservazione. Per ciascuna tipologia documentale viene prevista l'associazione di specifici metadati (chiavi di ricerca) che guidano la ricerca e l'individuazione del documento da parte del cliente, oltre a quelli previsti eventualmente per legge.

La scelta delle chiavi di ricerca viene effettuata in fase di analisi as is con i referenti di progetto del cliente – ogni cliente può dotarsi di un modello documentale che comprende, oltre ad un set standard, altre chiavi di ricerca personalizzate a seconda delle esigenze specifiche. Viene riportato qui di seguito in una tabella esemplificativa quanto presente nell'Allegato A al Manuale della Conservazione, questa tabella viene compilata per ciascuna singola tipologia documentale sottoposta a conservazione:

<i>Informazioni generali</i>	<i>Descrizione</i>
Tipo Archivio	Amministrativo
Tipo Documento	Ad . es. Fatture Attive, Note credito, Note Debito, Libro Magazzino
Durata di Conservazione Richiesta	10 anni
Applicativo di partenza	
Tipo Flusso Dati Atteso	
Formato Documento Atteso	
Naming Convention Flusso Dati	
Naming Convention Immagini	

Per ciascuna tipologia di documento (Amministrativo e Non) viene compilata la seguente tabella: (la compilazione qui di seguito è a mero titolo esemplificativo)

<i>Indice</i>	<i>Descrizione</i>	<i>Tipo Campo</i>	<i>Obbligatorio</i>
Numero Documento	Identificativo del numero relativo al documento	INT – Max 5	Y
Data Documento	Data di emissione del documento	Date – yyyy-mm-gg	Y
Oggetto	Oggetto del documento	Varchar 100	Y
...			

Per quanto riguarda la conservazione dei documenti rilevanti ai fini fiscali la normativa richiede che siano consentite le funzioni di ricerca e di estrazione dagli archivi dei documenti o delle informazioni in relazione ad un set minimo di metadati individuati più precisamente in:

- Ragione Sociale
 - Codice Fiscale – Partita Iva
 - Numero Documento
 - Data Documento
- e loro associazioni logiche.

Il sistema conservazione è predisposto per gestire i formati che possono maggiormente garantire i principi di interoperabilità tra i sistemi di conservazione. La scelta dei formati viene effettuata in accordo con il cliente, utilizzando uno o più formati previsti nell'Allegato 2 al DPCM 3/12/2013, che viene sintetizzato nella tabella seguente. I formati individuati dalla normativa sono stati scelti in modo che possano consentire la più diffusa leggibilità nel tempo.

Formati Gestiti

Formato File	Proprietario	Estensione	Standard	Tipo MIME	Viewer	Produttore Viewer
PDF	Adobe Systems	.pdf	ISO32000-1	application/pdf	Adobe Reader	Adobe Systems
PDF/A	Adobe Systems	.pdf	ISO19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)	application/pdf	Adobe Reader	Adobe Systems
TIFF	Adobe	.tif	N.A.	Image/tif	Vari (ad. es. IrfanView, AlternTiff)	Vari
XML	W3C	.xml	N.A.	application/xml text/xml	Mozilla, Chrome, I.E.	Firefox, Google, Microsoft
TXT	Ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere (Character Encoding) adottata	.txt	N.A.	N.A.	Mozilla, Chrome, I.E.	Firefox, Google, Microsoft
ODF	Consorzio OASIS OpenOffice.org	.ods- .odp- .odg- .odb	ISO/IEC 26300:2006	application/vnd.oasis.opendocument. text		www.oasis-open.org
EML	Vari	.eml	RFC2822		Client Posta Elettronica	
JPG	Joint Photographics Experts Group	.jpg- .jpeg	ISO/IEC 10918:1	image/jpeg	Vari	Vari

6.2 Pacchetto di versamento

E' il pacchetto informativo con cui il soggetto produttore trasferisce gli oggetti da conservare al Sistema di Conservazione. Il versamento di un Pacchetto di Versamento genera, da parte del Sistema di Conservazione, un rapporto di versamento che attesta l'avvenuta presa in carico da parte del Sistema di Conservazione dei Pacchetti di Versamento inviati dal Produttore. Il rapporto di versamento, univocamente identificato e conservato dal Sistema di Conservazione, certifica che i documenti inviati dal Produttore coincidano con quelli acquisiti dal Sistema di Conservazione. Il rapporto, è rilasciato dal Sistema di Conservazione in modalità automatica successivamente alla presa in carico e alla verifica del Pacchetto di Versamento. Il rapporto contiene un riferimento temporale e può essere sottoscritto con firma digitale o elettronica qualificata sulla base degli accordi contrattuali; Il rapporto di versamento differisce dal rapporto di presa in carico solo in quanto a operatori coinvolti. Il rapporto di presa in carico coinvolge il titolare ed il sistema di gestione documentale, mentre il rapporto di versamento coinvolge il produttore ed il sistema di conservazione – hanno entrambi l'obiettivo di garantire al mittente del flusso informativo la ricezione di un adeguato feedback in merito alle operazioni effettuate.

Il Servizio CDN di Archivium è basato su un'architettura fisica ed applicativa. La divisione tra il sistema di versamento e sistema di conservazione corrisponde ad una separazione di natura logica, i documenti non sono quindi soggetti a trasferimenti tra ambienti che non siano attestati sulla medesima infrastruttura. I documenti inseriti nel sistema di versamento vengono sottoposti ad opportune verifiche durante il caricamento, In tal modo non sono esposti a rischi di alterazioni né modifiche in fase di trasferimento alle procedure di conservazione, che comunque verificano, con procedure automatiche, in ogni fase del processo l'integrità del documento attraverso il calcolo e la comparazione dell'impronta del documento.

Le verifiche e l'identificazione delle anomalie sono quindi effettuate a monte del processo, nell'ambito del sistema di versamento, dove vengono eventualmente rilevati gli scarti. Le fasi successive avvengono sotto il monitoraggio del sistema di gestione, che controlla il corretto svolgimento del processo di conservazione e produce la relativa reportistica sia in relazione alle eventuali anomalie rilevate sia in riferimento a quanto correttamente conservato.

Gli oggetti destinati al Sistema di Conservazione vengono identificati sulla base del risultato dell'analisi svolta in fase di attivazione del servizio. L'analisi ha il compito di associare a ciascuna tipologia documentale un template (modello documentale) compliant alle esigenze normative e di ricerca del cliente.

Ogni documento viene inviato al sistema di conservazione all'interno di un pacchetto di versamento contenente l'oggetto da conservare ed è corredato di un set specifico di metadati oltre che alla sua impronta, che viene calcolata e verificata ad ogni step del processo di conservazione.

Il PdV contiene i documenti digitali da conservare ed un file indice che ne descrive il contenuto in termini di:

- **Descrizione dei documenti secondo i metadati definiti nell'allegato 5 del D.P.C.M. 3 dicembre 2013 (con riferimento ai metadati minimi del documento informatico)**
- **Evidenza informatica ottenuta dall'applicazione della funzione di Hash SHA 256 per ogni singolo Documento Informatico;**
- **Percorso URI di ogni singolo Documento Informatico.**

Le specifiche delle modalità di composizione ed invio del pacchetto di versamento vengono definite in fase di setup del servizio in accordo con il cliente. I singoli documenti vengono identificati in maniera univoca all'interno del Sistema di Conservazione nell'ambito della singola azienda e della singola tipologia documentale; inoltre i documenti (a seconda del modello documentale prestabilito) sono arricchiti dalle informazioni contenute nei metadati preconcordati.

Il processo di conservazione digitale a norma viene effettuato da Archivium sulla base delle tempistiche prestabilite con il cliente per ciascuna singola tipologia documentale e comunque entro e non oltre i termini previsti dalla normativa.

A fronte dell'analisi iniziale congiunta del processo di formazione e gestione dei documenti, svolta per ciascun modello documentale, vengono stabilite le modalità di configurazione della suite ArchiCons, la quale consente per ciascun cliente e modello documentale, l'implementazione di un workflow dedicato e parametrico rispetto alle singole tipologie documentali.

6.3 Pacchetto di archiviazione

Il pacchetto di archiviazione (PdA) è l'insieme di documenti conservati a norma con annesso l'indice di conservazione, al quale viene apposta firma elettronica qualificata del conservatore Archivium e marca temporale. E' un pacchetto informativo con cui il Sistema di Conservazione a Norma conserva i dati con garanzia di integrità e reperibilità nel tempo. Il PdA viene formato a seguito della aggregazione o suddivisione di uno o più PdV. Il lotto di documenti sottoposti a conservazione viene riepilogato nell'IdC (formato SinCRO) che contiene oltre ai metadati minimi previsti dalla normativa, anche specifici indici di conservazione per la ricerca dei documenti (IPdA).

Il sistema di conservazione di Archivium prevede la gestione del pacchetto di archiviazione in base alle specifiche della struttura dati riportate da Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali (SinCRO) UNI 11386:2010 e declinate nel DPCM 03/12/2013.

Ciascun Pacchetto di Archiviazione contiene quindi:

- I documenti elettronici confluiti nello stesso a partire da uno o più pacchetti di versamento
- L'Indice di Conservazione sul quale sono state apposte firma digitale e marca temporale dal responsabile del servizio di conservazione
- Lo schema formale con cui vengono formati ed incapsulati i metadati di Archiviazione dei documenti.

L'IdC viene formato in conformità allo schema xsd "Schema dell'Indice del Pacchetto di Conservazione" che ne descrive la struttura.

Il sistema di conservazione di Archivium prevede la gestione del pacchetto di archiviazione in base alle specifiche della struttura dati riportate dal DPCM 03/12/2013.

Ciascun documento conservato trova riferimento all'interno dell'Indice del pacchetto di archiviazione (IPdA) generato dalla suite ArchiCons. La struttura dell'IPdA è definita in modo univoco per ciascuna tipologia documentale sulla base di template predefinite ed eventualmente customizzate per la parte Moreinfo, per la quale si entra nel merito poco più avanti. Tale struttura è conforme allo standard nazionale SinCRO - Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), lo standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

La struttura dell'indice del pacchetto di archiviazione prevede una sezione apposita denominata Moreinfo. In questa sezione vengono inseriti i metadati specifici afferenti alle diverse classi documentali scelti in accordo con il cliente sulla base delle esigenze di ricerca e reperibilità dei documenti conservati, oltre che i metadati minimi richiesti dalla normativa, indicati nell'Allegato 4 (Specifiche tecniche del Pacchetto di Archiviazione) delle Regole Tecniche in materia di conservazione. .

Qui di seguito la schematizzazione della struttura dati del Pacchetto di Archiviazione:

<sincro:SelfDescription>

Informazioni relative all'indice di conservazione stesso, associato al volume di conservazione

<sincro:ID sincro:scheme="local">IdC_687_NotificaFatturaPA_2_20150915154124

Identificativo univoco dell'entità descritta – Pacchetto di Archiviazione

<sincro:CreatingApplication>

Informazioni sull'applicazione che ha generato l'indice del pacchetto di Archiviazione

<sincro:Name>ArchiCons

Nome dell'applicazione che ha generato l'indice del pacchetto di Archiviazione

<sincro:Version>3.0

Versione dell'applicazione che ha generato l'indice del pacchetto di Archiviazione

<sincro:Producer>Archivium Srl

Nome del produttore dell'applicazione che ha generato l'IdC

<sincro:SourceIdC>

Informazioni relative ad uno o più IdPA da cui è originato quello in oggetto

<sincro:ID>

Identificativo univo del pacchetto di derivazione

<sincro:Path>

Percorso relativo alla localizzazione del file cui l'elemento si riferisce

<sincro:VdC>

Informazioni relative al volume di conservazione

<sincro:ID sincro:scheme="local">

Identificativo univoco del volume di conservazione

<sincro:VdCGroup>

Informazioni relative alla tipologia/aggregazione di natura logica o fisica cui il VdC appartiene

<sincro:Label>

Nome della tipologia/aggregazione cui appartiene il VdC (ad es. Notifiche fatture PA, Libro Giornale,...)

<sincro:Description>Anno YYYY – Periodo Fiscale di Riferimento

Informazioni descrittive relative ad un'eventuale tipologia o aggregazione di natura logica o fisica cui il VdC appartiene. Esplicitazione delle regole di grouping

<sincro:MoreInfo sincro:XMLScheme="file://VdCScheme">

Informazioni ulteriori specifiche dell'azienda Titolare dei documenti posti in conservazione, compreso il numero totale di documenti presenti nel pacchetto informativo

<sincro:EmbeddedMetadata>

Informazioni dell'elemento Moreinfo integrate nell'IdC e strutturate nel formato xml

<CustomMetadata>

Elenco dei metadati relativi all'azienda

<CodiceFiscale> Codice Fiscale Azienda

<PartitaIva> Partita Iva Azienda

<Azienda> Ragione Sociale Azienda

<Indirizzo> Indirizzo Sede Legale Azienda

<Cap> Codice Postale

<Localita> Città

<Provincia> Provincia

<NumeroDocumenti> Numero Documenti Presenti nel pacchetto

<sincro:FileGroup>

Elemento di aggregazione di più file oggetto di conservazione digitale a norma

<sincro:Label>

Nome del file compreso di estensione es.

<sincro:File sincro:encoding="us-ascii" sincro:extension="xml" sincro:format="application/xml">

Informazioni relative al file oggetto di conservazione digitale a norma

<sincro:ID>

Identificativo univoco del file

<sincro:Path>

Informazione relativa alla localizzazione del file espressa come indirizzo URL

<sincro:Hash sincro:function="sha256">

Informazione dell'impronta del file cui l'elemento si riferisce, viene indicato anche l'algoritmo con il quale è stata calcolata l'impronta

<sincro:MoreInfo sincro: XMLScheme= "file://ModDoc"

Informazioni aggiuntive relative al singolo documento

<sincro:EmbeddedMetadata>

Informazioni dell'elemento Moreinfo integrate nell'IdC e strutturate nel formato xml

<CustomMetadata>

Elenco dei metadati relativi al singolo documento appartenente alla singola tipologia documentale

<NomeIndice> Valore

<NomeIndice> Valore

<NomeIndice> Valore

<DataOraFirma> Valore obbligatorio

<File_Size> Valore obbligatorio

<sincro:Process>

Informazioni relative allo svolgimento del processo di conservazione digitale a norma

<sincro:Agent sincro:type="organization" sincro:role="PreservationManager">

Informazioni relative ai soggetti che intervengono nel processo di conservazione digitale a norma

<sincro:AgentName>

Denominazione dell'agente che interviene nel processo di conservazione digitale a norma

<sincro:FormalName>Archivium srl

<sincro:Agent_ID sincro:scheme="TaxCode">IT:09468600011

Identificativo univoco dell'agente che interviene nel processo di conservazione digitale a norma,
in particolare codice fiscale compreso di codice paese individuato da ISO3166

<sincro:TimeReference>

Informazioni relative a data-ora di realizzazione dell'indice di conservazione

<sincro:TimeInfo>YYYY-MM-DDTHH:MM:SS+01:00

Informazioni relative a data-ora realizzazione dell'Indice di Conservazione nel formato UNI ISO
8601:2010

6.4 Pacchetto di distribuzione

Si possono ricondurre ai pacchetti di distribuzione i documenti conservati a norma, disponibili per l'esibizione, via portale web oppure da supporto auto consistente o altre modalità concordate con il Cliente e descritte nel presente documento. Il Pacchetto di Distribuzione viene creato sulla base di una richiesta dell'utente autorizzato. Il Pacchetto di Distribuzione può non coincidere con il pacchetto di archiviazione. La generazione del Pacchetto di Distribuzione prevede un processo che ha come output l'insieme dei documenti di cui viene richiesta l'esibizione, dei loro rispettivi Indici di Conservazione firmati e marcati e di un nuovo indice conservazione, chiamato in questo caso "Indice del Pacchetto di Distribuzione" - quest'ultimo avrà le medesime caratteristiche tecniche dell'indice di conservazione ma avrà quale contenuto i dati relativi al pacchetto di distribuzione ed i dati relativi ai documenti di cui è richiesta l'esibizione e l'opponibilità a terzi. Anche in questo caso verrà applicato al file indice il processo di firma elettronica qualificata e quello di applicazione della marca temporale. Il pacchetto di distribuzione sarà disponibile in un'apposita area del portale web.

7. IL PROCESSO DI CONSERVAZIONE

Archivium definisce Processo di Conservazione Digitale a Norma come l'insieme delle attività che vengono svolte da Archivium stessa per la conservazione documentale; si intende per Servizio di Conservazione Digitale a Norma l'espletamento del processo verso il cliente.

La suite ArchiCons, definibile come lo strumento in grado di espletare il servizio di conservazione esternalizzato da parte del cliente all'outsourcer, è stata pensata per essere ampiamente configurabile in relazione a ciascuna azienda. E' una piattaforma multiazienda; ogni azienda dispone di un ambiente logicamente distinto da quello delle altre aziende e univocamente identificabile all'interno dell'intera suite. Archicons gestisce, se necessario, il concetto di gruppo aziendale e di aggregatore (professionista che gestisce più aziende).

La suite permette di gestire con un unico approccio omogeneo tutte le aziende e tutti i modelli documentali. E' comunque imprescindibile la separazione logica tra i vari ambienti, e nei casi di necessità anche dei modelli documentali. La suite Archicons permette la completa parametrizzazione per ciascuna azienda- modello documentale di di configurazioni, processi di workflow (autorizzazioni e firme), modalità di formazione e consistenza dei pacchetti informativi e delle modalità di inserimento ed estrazione dei flussi dati dalla suite stessa.

Il Responsabile del Servizio di Conservazione ed i suoi delegati, nonché altri operatori interni eventualmente autorizzati, possono accedere all'ambiente di monitoraggio dei processi di conservazione, dove è possibile attraverso una visione aggregata, monitorare l'andamento dei servizi di conservazione a tutti gli stages per tutte le aziende.

Il processo di conservazione digitale a norma di Archivium prevede, come definito dall'articolo 9 del DPCM del 3 dicembre 2013, quanto segue:

- a) l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
- b) la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione
- c) l'eventuale rifiuto del pacchetto di versamento, nel caso in cui i controlli di cui sopra abbiano evidenziato delle anomalie;
- d) la generazione in modo automatico del rapporto di versamento relativo ad un pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e tutte le impronte, calcolate sui documenti del pacchetto di versamento, secondo le modalità descritte nel presente manuale di conservazione;
- e) la sottoscrizione del rapporto di versamento con firma elettronica qualificata apposta dal responsabile della conservazione o da un suo delegato in modalità automatica- massiva,
- f) la preparazione, la sottoscrizione con firma digitale del responsabile della conservazione o di un suo delegato e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 del dpcm del 3 dicembre 2013 e secondo le modalità riportate nel presente manuale della conservazione;
- g) la preparazione e la sottoscrizione con firma digitale e con l'apposizione della marca temporale sull'Indice del pacchetto di distribuzione ai fini di ottemperare alla richiesta di esibizione dell'utente;
- h) ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti, o in parte anche per estratto, con i pacchetti di archiviazione;

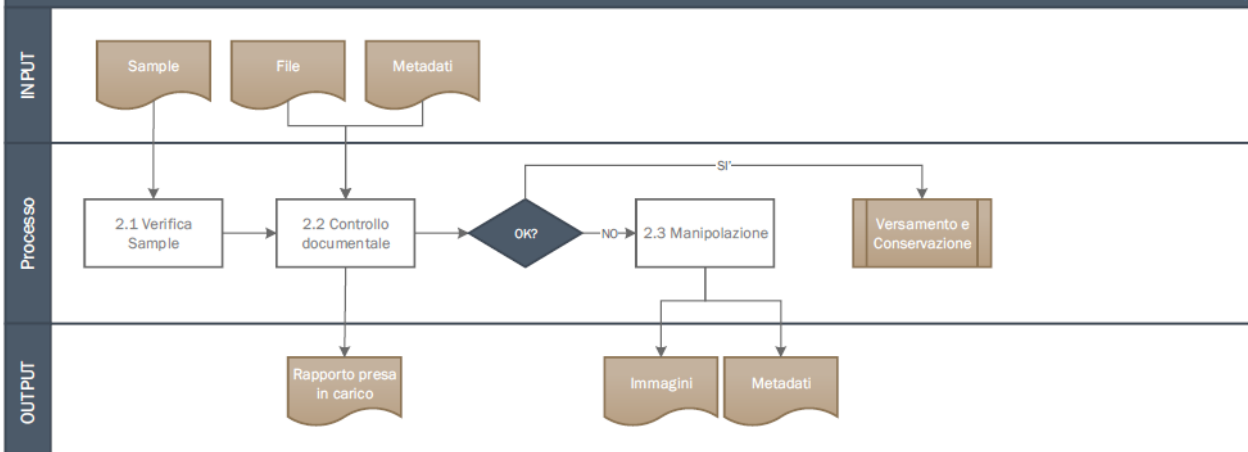
Il processo di conservazione digitale a norma si avvia con la sottoscrizione da parte del Cliente del contratto che sancisce le modalità e le caratteristiche del servizio da erogare. Archivium, se necessario, implementa per conto del Cliente un Sistema di Gestione Documentale che precede il Processo di Conservazione Digitale a Norma e che si conclude con la formazione del PdV. Il Ruolo di Produttore è svolto quindi da Archivium.

Il Sistema di Gestione Documentale è fornito da Archivium in full outsourcing ed ha lo scopo di omogenizzare i flussi documentali e di renderli idonei al processo di conservazione. L'output del Sistema di Gestione Documentale è il pacchetto di versamento formato da una serie di file immagine (i documenti veri e propri) ed un file indice contenente per ciascun documento un set di metadati compliant alle richieste normative e alle esigenze di consultazione del cliente. Il sistema Archicons attribuisce un identificativo univoco di piattaforma a ciascun singolo oggetto presente nel sistema, così da consentirne l'individuazione in modo diretto e persistente; inoltre garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

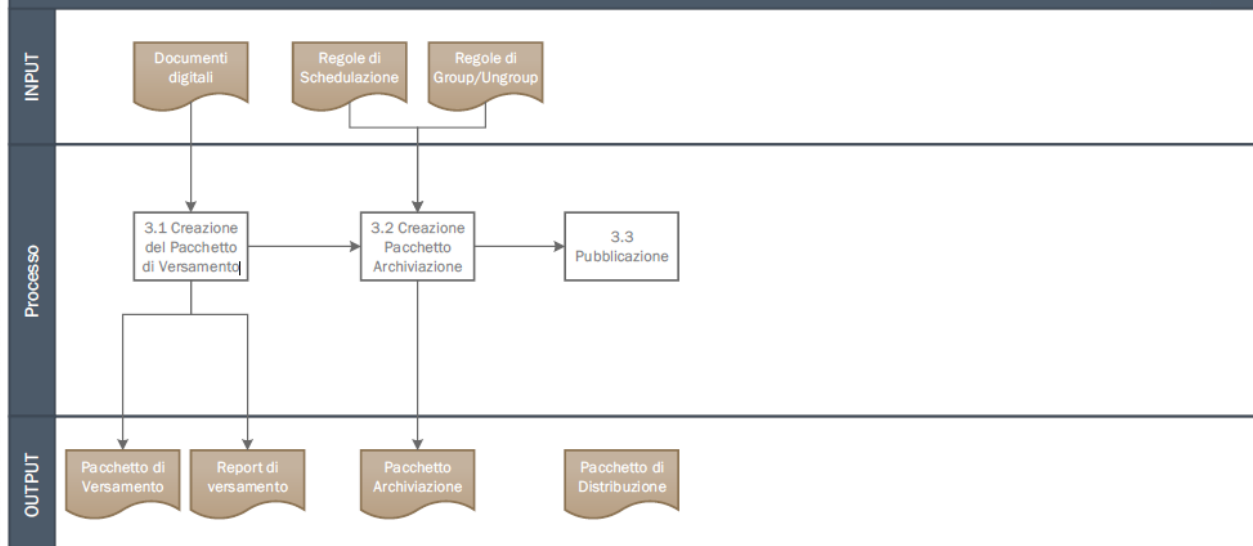
Il processo di Conservazione Digitale a Norma è suddiviso in tre sotto-processi (a monte può esistere un processo di pre-versamento custom per ciascun singolo cliente che sceglie i servizi di gestione documentale a monte di quelli di conservazione):

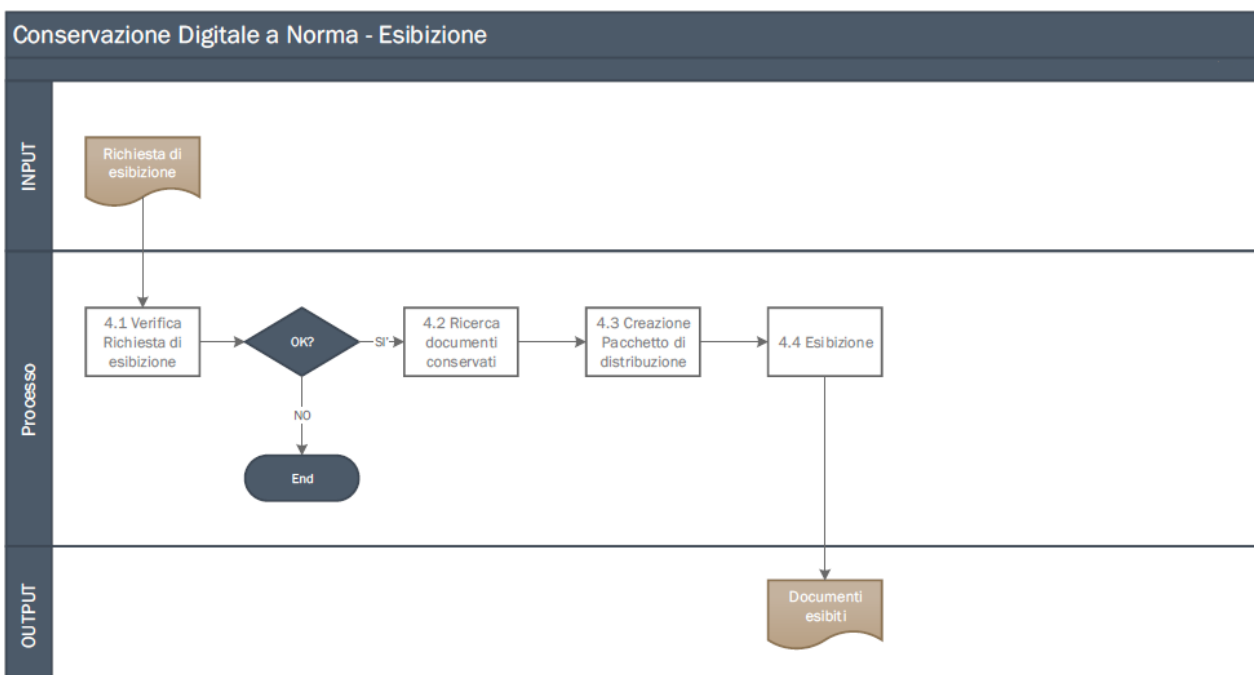
- Versamento;
- Conservazione;
- Esibizione.

Conservazione Digitale a Norma – Pre-versamento



Conservazione Digitale a Norma – Versamento e Conservazione





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

Archivium prevede che il Cliente possa fornire i documenti da conservare a norma attraverso altri Servizi messi a disposizione del Cliente stesso:

- **Servizio Paper Service:** il Cliente fornisce ad Archivium la documentazione in formato cartaceo; Archivium si occupa della scansione dei documenti, della generazione degli indici e dei metadati finalizzati alla futura consultazione ed esibizione.

I Clienti hanno a disposizione piattaforme (anche verticalizzate, come ad es. per la gestione delle fatture elettroniche PA), e Servizi Web che consentono loro di generare e/o caricare i documenti oggetto di Conservazione Digitale a Norma. Il servizio “Versamento e Conservazione” emette un Report per confermare l’avvenuta presa in carico dei documenti.

Servizi Web ed integrazioni applicative da altri gestionali:

- **Servizio Mio Archivio:** il Cliente può decidere di effettuare l'upload di documenti ed eventualmente dei relativi metadati tramite portale web, dove potrà consultare, firmare ed approvare i documenti prima del processo di conservazione digitale a norma.
- **Servizio di Upload FTPS:** il Cliente ha facoltà di caricare in autonomia su un’area riservata e soggetta alle regole di sicurezza informatica adottate da Archivium le immagini dei documenti da sottoporre a conservazione digitale a norma ed eventualmente dei relativi metadati. Sarà cura di Archivium normalizzare i documenti ai fini della conservazione.

A valle dei Servizi a supporto della Conservazione Digitale a Norma, il processo continua come descritto nel Manuale di conservazione. E' possibile che il Cliente invii alla piattaforma Archivium i documenti da conservare corredati dalle strutture di indici da abbinare. L'indicizzazione dei documenti può eventualmente anche essere effettuata in service direttamente da operatori qualificati di Archivium in base a quanto specificatamente concordato con il Cliente all'interno del sistema di gestione documentale. Il produttore, persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.

Si tratta di Archivium se intervengono dei processi di preventiva gestione documentale (digitalizzazione, classificazione ed estrazione dei metadati) – Archivium diventa soggetto incaricato alla produzione e/o gestione dei documenti e/o relativi metadati da inviare al sistema di conservazione. Se il cliente fornisce pacchetti informativi nativamente elettronici via ftps, il cliente riceve un rapporto di presa in carico contenente l'elenco di ciascun file ricevuto con annessa ciascuna relativa impronta. Il file di presa in carico può essere sottoscritto con firma digitale del responsabile del servizio di conservazione e marcato temporalmente, sulla base delle intese contrattuali. Il flusso elettronico viene controllato ed inserito nel sistema di gestione documentale che predisporrà il pacchetto di versamento senza ulteriori operazioni. Il cliente ha l'onere di verificare l'impronta del documento presente sia nel rapporto di presa in carico che nel rapporto di versamento, se non ci sono state ulteriori elaborazioni. I dati sono trasferiti dalla postazione utente al Servizio centralizzato attraverso il protocollo HTTPS (o FTPS) che garantisce un trasferimento sicuro delle informazioni.

Ogni volta che il sistema di versamento riceve un nuovo pacchetto informativo, l'evento viene appositamente tracciato all'interno del log system.

Ciascun log relativo alla ricezione di un nuovo pacchetto di versamento registra le seguenti informazioni:

IdLog: identificativo univoco dell'attività
IdPacchetto: identificativo del pacchetto informativo
Data-ora: data ora dell'evento occorso in formato UTC
ServerName: identificativo del server chiamante
Script: identificativo del metodo utilizzato per il trasferimento
IdSessione: (token) identificativo della sessione di versamento
IdUtente: identificativo del soggetto che ha eseguito il versamento
Utente: nome cognome utente
IPUtente: indirizzo IP dal quale è stato effettuato il versamento
Operazione: tipo di operazione eseguita, in questo caso versamento
EsitoOperazione: esito dell'operazione
CodificaErrore: identificativo della tipologia di errore
DescrizioneErrore: spiegazione che descrive l'errore occorso.

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

Nel momento in cui i documenti vengono versanti all'interno del sistema di versamento, i documenti subiscono una fase di controllo più o meno articolato a seconda della tipologia, ma che comunque garantisce la verifica sulla conformità e sulla correttezza dei documenti da inviare in conservazione. In particolare la serie dei controlli minimi prevede:

- Controlli di conformità
- Verifica di coerenza tra contenuto del PdV e file indice
- Formato dei documenti (stabiliti in primis dalla normativa ed eventualmente in secundis da accordi contrattuali)
- Presenza dei metadati previsti
- Presenza di tutte le informazioni definite per le specifiche categorie documentali obbligatorie
- Integrità del Pacchetto di Versamento

Sulla base delle modalità di invio (canale di trasmissione dei documenti e dei metadati) alcuni controlli vengono effettuati a monte del sistema di versamento, a fronte della presa in carico dei documenti da parte di Archivium, altri invece hanno ragione di essere eseguiti solo a fronte del versamento.

Controlli effettuati durante la presa in carico:

- identificazione del mittente sulla base del canale di presa in carico (APK, stato utenza attivo, ...)
- controllo dell'identità del firmatario sulla firma digitale, se il cliente fornisce una white list di firmatari
- controlli di integrità sui singoli documenti
- controlli sulle firme digitali
- controlli sui formati accettati da normativa e accordi contrattuali
- controlli sulla presenza dei metadati obbligatori previsti dalla normativa e dagli accordi contrattuali

Controlli effettuati durante il versamento:

- dell'integrità del documento memorizzato sul supporto rispetto all'impronta associata allo stesso
- di univocità degli identificativi degli oggetti contenuti nel PdV
- di univocità degli oggetti contenuti nel PdV rispetto a quanto già sottoposto in conservazione (non bloccante)
- di formato del documento previsto tra quelli conservabili per normativa
- di presenza dei metadati obbligatori previsti dalla normativa e dagli accordi contrattuali
- di validità del certificato di firma e di attendibilità della CA che lo ha rilasciato
- di validità dell'algoritmo di firma utilizzato per la firma dei documenti all'interno del PdV
- di corrispondenza del numero di documenti versati con il numero di documenti presi in carico nell'indice del pacchetto di versamento

In fase di analisi sono concordate le regole puntuali per l'esecuzione di eventuali controlli di univocità, duplicazione, coerenza e completezza dei documenti conservati, con segnalazione di eventuali documenti mancanti in relazione alle regole definite in accordo con il cliente.

I controlli possono dare un esito positivo o negativo – in questo secondo caso vengono presi in considerazione due tipologie di errori: bloccanti e non.

Se si è in presenza di un errore bloccante, il sistema produce una segnalazione e la invia al cliente in modo che possa definire la gestione dell'anomalia e giungere al completamento del processo. Se l'errore non è bloccante, sarà l'operatore interno a verificare eventuali regole predefinite con il cliente, agendo dunque di conseguenza secondo istruzioni, oppure, in mancanza di esse provvederà a contattare il referente del cliente.

Ogni volta che il sistema di versamento effettua le operazioni di controllo sui pacchetti di versamento, l'evento viene appositamente tracciato all'interno del log system.

Ciascun log relativo al controllo di un pacchetto di versamento registra le seguenti informazioni:

IdLog: identificativo univoco dell'attività
IdPacchetto: identificativo del pacchetto informativo
Data-ora: data ora dell'evento occorso in formato UTC
ServerName: identificativo del server chiamante
Script: identificativo del metodo utilizzato per il controllo
IdSessione: (token) identificativo della sessione di controllo
IdUtente: identificativo dell'agent che ha eseguito il controllo
Utente: descrizione agent
Operazione: tipo di operazione eseguita, in questo caso controllo
EsitoOperazione: esito dell'operazione
CodificaErrore: identificativo della tipologia di errore
DescrizioneErrore: spiegazione che descrive l'errore occorso

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

Una volta terminata la fase di acquisizione dei documenti attraverso la gestione ed i controlli sui pacchetti di versamento, il sistema di conservazione genera un rapporto di versamento univocamente identificato attraverso un identificativo complesso. Il rapporto di versamento contiene i riferimenti di ciascun documento compresa l'impronta (SHA256) ed il riferimento temporale (UTC), poco più avanti verrà effettuata una descrizione dettagliata del suo contenuto.

Il log system registra l'operazione di accettazione del pacchetto di versamento aggiornando lo stato del pacchetto in accettato (o scartato in caso contrario con indicazione della motivazione dell'errore) e producendo il rapporto di versamento o scarto.

Per ciascun flusso inviato al sistema di versamento da qualunque canale di trasmissione previsto, il sistema prevede la generazione del rapporto di versamento. Questo documento è sottoscritto con firma elettronica qualificata del responsabile del servizio di conservazione di Archivium.

Struttura del Rapporto di Versamento:

[2015-07-30T17:18:09+02:00] Rapporto di Versamento dell'Azienda 0639
[2015-07-30T17:18:09+02:00] Utente XYZ
[2015-07-30T17:18:09+02:00] Firmatario Autorizzato XXX
[2015-07-30T17:18:09+02:00] Nome Modello modFatturaElettronica
[2015-07-30T17:18:09+02:00] Analisi cartella di versamento numero 9
[2015-07-30T17:18:09+02:00]
[2015-07-30T17:18:09+02:00]
[2015-07-30T17:18:09+02:00] Trovato File:
[2015-07-30T17:18:09+02:00] Nome File: IT09468600011_14020.xml.p7m
[2015-07-30T17:18:09+02:00] Dimensione File: 5502 Byte
[2015-07-30T17:18:09+02:00] Hash File (SHA256):
5b27632e28d6f47ce590461b8c0420d802d4a3a581cda43b724f6961ef149b40
[2015-07-30T17:18:09+02:00] Tipo File: application/pkcs7-mime
[2015-07-30T17:18:09+02:00] Estensione File: p7m
[2015-07-30T17:18:09+02:00] Data File: 2015-07-30 17:18:09
[2015-07-30T17:18:09+02:00] ...
[2015-07-30T17:18:13+02:00] Fine Rapporto di Versamento

Ogni Rapporto di Versamento si riferisce ad un gruppo di documenti omogenei per tipologia o associazione logica.

In ciascun Rapporto di Versamento sono presenti:

- i riferimenti dell'utente che ha inviato i dati e dell'azienda cui appartengono i documenti.
- un riferimento temporale della generazione e chiusura del rapporto di versamento, in testa ed in coda al documento
- il riferimento del firmatario autorizzato alla sottoscrizione del Rapporto di Versamento
- il riferimento all'identificativo del pacchetto di versamento
- il riferimento all'aggregazione/tipologia documentale
- il numero totale dei file analizzati nel pacchetto di versamento

Per ciascun file analizzato viene riportato:

- il nome file
- la dimensione in byte
- hash del file
- algoritmo con il quale è stato calcolato l'algoritmo di hash
- formato del file
- estensione file
- riferimento temporale del file

I Rapporti di Versamento sottoscritti con firma elettronica qualificata vengono sottoposti a processo di conservazione digitale a norma con cadenza non superiore all'anno.

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

La mancata coerenza con i controlli sopra citati al paragrafo 7.2 di anche solo uno dei documenti presenti all'interno del Pacchetto di Versamento produce il mancato versamento dell'intero pacchetto e la generazione di un rapporto di scarto con l'indicazione del controllo non superato.

Il PdV contenente almeno un documento informatico che non passa almeno uno dei controlli indicati nel paragrafo 7.2, viene rifiutato in toto e i documenti relativi messi in stato "rifiutato". Il processo continua con la gestione delle anomalie segnalate o l'eliminazione dal pacchetto di versamento scartato di uno o più documenti che non hanno superato i controlli. Questi documenti vengono salvati in un'apposita share di discard insieme al rapporto di scarto.

Il rapporto di scarto ha la medesima struttura del rapporto di versamento, anch'esso viene identificato univocamente, ed include l'elenco dei documenti scartati dalla piattaforma, nonché il riferimento temporale (UTC).

Anche i Rapporti di scarto vengono sottoscritti con firma elettronica qualificata e vengono sottoposti a processo di conservazione digitale a norma con cadenza non superiore all'anno

L'elenco di tutti i pacchetti di versamento accettati e rifiutati vengono segnalati via mail dal Sistema di Conservazione al Responsabile del Servizio di Conservazione e al Produttore con due distinte segnalazioni.

Gli utenti interessati possono verificare e controllare quanto contenuto nell'apposita area di memorizzazione dei PdV rifiutati oppure direttamente dalla piattaforma web.

7.5 Preparazione e gestione del pacchetto di archiviazione

Il sistema di conservazione di Archivium prevede la gestione del pacchetto di archiviazione in base alle specifiche della struttura dati riportate dal DPCM 03/12/2013.

Ogni documento conservato è quindi corredato dell'Indice del pacchetto di archiviazione (IPdA) generato da Archivium. La struttura dell'IPdA è definita in modo univoco per ciascuna tipologia documentale. Tale struttura è conforme allo standard nazionale SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), lo standard riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione che prevede una specifica articolazione per mezzo del linguaggio formale XML.

La struttura prevede inoltre la sezione MoreInfo, la quale dà l'opportunità di entrare nel merito di metadati specifici ed afferenti alle singole tipologie documentali. La sezione dei metadati aggiuntivi viene inizialmente proposta da Archivium e discussa con il cliente.

L'Indice del Pacchetto di Archiviazione viene firmato digitalmente attraverso lo standard CadES.

Il sistema di versamento e conservazione sono in costante comunicazione tra loro (flusso di comunicazione bidirezionale – il secondo viene attivato dal primo al termine della fase di controllo indicata nei paragrafi precedenti, il primo riceve adeguati feedback di quanto accaduto durante il processo).

In fase di setup è possibile prestabilire in base alla tipologia documentale le tempistiche di invio in conservazione dei documenti ricevuti all'interno dei pacchetti di versamento, tenendo chiaramente conto di eventuali prescrizioni normative.

Una volta completata la fase di verifica ed accettazione del Pacchetto di Versamento e di formazione del Rapporto di Versamento, il processo si conclude con la formazione di un Pacchetto di Archiviazione costruito sulla base di regole di raggruppamento/sezionamento e sulla base di regole di schedulazione. Quindi in un pacchetto di Archiviazione possono confluire più pacchetti di versamento oppure solo una sezione di esso.

Il Pacchetto di Archiviazione è identificato attraverso un identificativo numerico complesso. A ciascun record presente nella base dati relativo a ciascun singolo documento è associato sia l'identificativo del pacchetto di versamento che quello del pacchetto di Archiviazione, in modo da poter seguire l'iter di ciascun singolo documento.

Il processo di trasformazione dei pacchetti di versamento in pacchetti di conservazione, avviene sostanzialmente attraverso due passaggi:

- Schedulazione dei pacchetti di archiviazione;
- Conservazione dei pacchetti di archiviazione.

Sulla base delle regole di group/ungroup e di schedulazione per ciascun modello documentale associato all'azienda cliente vengono creati i pacchetti di archiviazione. L'attività della creazione del pacchetto di Archiviazione prevede la creazione dell'evidenza informatica in formato UniSincro, che viene firmata e marcata temporalmente dal Conservatore. I pacchetti di archiviazione vengono salvati nel repository e diventano consultabili da apposito portale web.

L'evidenza informatica, firmata e marcata temporalmente dal Responsabile del Servizio di Conservazione, unitamente ai documenti con relativi metadati di conservazione formano il pacchetto di archiviazione che viene inserito sul portale di esibizione ArchiCons.

L'accesso al portale ArchiCons è consentito ai soli utenti accreditati (ovvero che possiedono il certificato X509 emesso durante la profilazione dell'utente dal responsabile del servizio di conservazione o di un suo delegato).

Il Pacchetto di Archiviazione può definirsi pronto all'elaborazione dopo la presa in carico dei pacchetti di versamento che hanno superato i controlli e tenuto conto delle sopracitate regole di scheduling e di raggruppamento. Il Pacchetto di Archiviazione è composto dai documenti e dall'Indice del Pacchetto di Archiviazione, prodotto sulla base delle specifiche UniSincro già descritte.

La suite ArchiCons prevede un'apposita area ad accesso riservato agli utenti che ne hanno titolo, dove vengono attivati i processi di firma digitale e di marca temporale delle evidenze informatiche. Queste operazioni possono essere svolte singolarmente o in modalità massiva a discrezione dell'operatore.

La suite Archicons prevede l'attivazione da parte dell'utente autorizzato dei processi di firma e di marca temporale. Le fasi di apposizione della firma del responsabile all'interno del procedimento di conservazione di Archivium e della marca temporale seguono l'iter di seguito descritto :

- per ciascun indice di conservazione correttamente compilato viene calcolata l'impronta mediante algoritmo di Hashing SHA-256
- viene apposta la firma all'impronta del documento mediante uso del certificato elettronico qualificato del responsabile del servizio di conservazione
- viene apposta la marca temporale alla firma, richiedendo il servizio al Time Stamping Server di una CA
- viene creato un'envelope (file .p7m) in formato PKCS#7 che contiene il documento, la firma e di un file tsd contenente la marca temporale

Le operazioni di apposizione di firma e marcatura temporale vengono effettuate nel rispetto delle normative specifiche in materia di firme e validazione temporale.

Il PdA prevede l'utilizzo di Firma Digitale secondo lo Standard ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI)- CMS Advanced Electronic Signatures (CadES). I Certificati crittografici utilizzati nel processo di firma sono certificati rilasciati da Certification Authority.

Il Processo di Conservazione Elettronica prevede l'utilizzo di riferimento temporale opponibile a terzi quale la Marca Temporale rilasciata da Certification Authority secondo lo standard RFC 3161 basata su infrastruttura a chiave asimmetrica X.509. Le TSA (Time Stamping Authority) utilizzate nel processo di apposizione del riferimento temporale sono apposte da Certification Authority accreditate AgID (<http://www.agid.gov.it/identitadigitali/firme-elettroniche/certificatori-attivi>).

Il certificato di firma del responsabile del servizio di conservazione è rilasciato dalla CA Namirial e memorizzato nei dispositivi HSM, in grado di garantire elevati livelli di sicurezza, affidabilità e performance in termini di velocità di esecuzione delle operazioni di firma. Tale processo permette di rispondere ai requisiti di autenticità, non modificabilità, integrità, staticità.

A fronte del completamento del processo di firma e marca del pacchetto di archiviazione, termina di fatto il core del processo di conservazione. La suite Archicons provvede ad aggiornare per ciascun singolo pacchetto di archiviazione e per ciascun singolo record lo stato dell'operazione. Sulla base della profilazione dell'utente, potrà essere verificato dallo stesso lo stato di conservazione del singolo documento, del singolo pacchetto di archiviazione e/o di entrambi a seconda delle viste consultate.

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

La suite di conservazione prevede l'accesso ai documenti conservati principalmente dal portale ArchiCons (portale web ad accesso profilato). Gli utenti che possono accedere al sistema di consultazione devono essere opportunamente registrati e profilati. La profilazione è definita sulla base delle specifiche fornite dal Cliente, consentendo la definizione dei profili degli utenti e delle relazioni tra di essi e il controllo degli accessi. Il protocollo di accesso ai documenti utilizzato è di norma il protocollo https. E' inoltre prevista su richiesta la produzione di supporti autoconsistenti consegnati al cliente periodicamente. Il portale web ha due modalità di accesso ai documenti: in sola consultazione ed in richiesta esibizione.

La modalità di sola consultazione prevede la possibilità di ricercare attraverso l'associazione logica dei metadati i singoli documenti o un loro aggregato all'interno delle classi documentali predefinite. A ciascun record è associata la possibilità di visualizzazione e download del singolo documento e dell'indice del pacchetto di archiviazione all'interno del quale è stato conservato. E' inoltre possibile la ricerca per pacchetti di archiviazione, per la quale sono garantite le funzionalità di download dell'intero pacchetto comprensivo di immagini e indice del pacchetto di archiviazione opportunamente firmato digitalmente e marcato temporalmente.

La modalità "richiesta di esibizione" ha un accesso riservato ad un gruppo di utenti di alto profilo, che ha a disposizione la possibilità di richiedere la creazione e la consegna del pacchetto di distribuzione.

Ai fini della interoperabilità tra sistemi di conservazione, il sistema di Archivium prevede la produzione di pacchetti di distribuzione generati a fronte della richiesta dell'utente. I pacchetti di distribuzione sono dunque completi di tutti gli elementi in grado di verificare gli elementi di firma e marca temporale (Art. 9, comma 1 lett. h DPCM 3/12/2013). La ricerca dei documenti ai fini della richiesta della creazione del pacchetto di distribuzione avviene tramite l'utilizzo delle chiavi di ricerca corrispondenti ai metadati specifici per ogni tipologia documentale.

Sempre all'interno della suite ArchiCons, esistono apposite funzionalità atte a garantire all'utente la possibilità di effettuare le opportune verifiche di integrità dei documenti presenti all'interno del pacchetto di distribuzione, nonché lo scaricamento in locale degli stessi da apposita area e/o l'eventuale invio tramite mail.

Ulteriori modalità di esibizione sono possibili sulla base di accordi specifici tra il cliente ed Archivium e sono declinate nel documento di specificità del servizio presente per ciascun cliente.

In caso di ispezioni dalle autorità competenti è possibile creare utenze apposite con ruolo di auditor, che hanno permessi di lettura e download su quanto viene dichiarato oggetto di auditing.

Il Pacchetto di Distribuzione viene creato sulla base di una richiesta dell'utente autorizzato.

Il Pacchetto di Distribuzione può non coincidere con il pacchetto di archiviazione e consiste nella possibilità per l'utente autorizzato di effettuare il download del supporto compresso (zip) direttamente da portale web e contiene i documenti richiesti, l'indice del pacchetto di conservazione relativo al pacchetto di archiviazione all'interno del quale i pacchetti sono stati conservati e l'indice del pacchetto di distribuzione sottoscritto con firma digitale del RCN e marcato temporalmente.

A fronte della richiesta di generazione di uno o più pacchetti di distribuzione, il sistema di conservazione esegue le verifiche di e correttezza e coerenza dei pacchetti di distribuzione generati e dei documenti contenuti, andando a confrontare le impronte con quelle dei documenti originariamente conservati nel pacchetto di archiviazione. Ogni attività di richiesta, controllo, visualizzazione e download dei pacchetti di distribuzione è loggata all'interno del log system. In caso di errore, dovuto a titolo esemplificativo a problemi di trasmissione o perdita di dati, l'utente ha la facoltà di richiedere nuovamente il pacchetto di distribuzione tramite la piattaforma web.

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

Il Servizio di conservazione digitale a norma di Archivium si attiene a quanto previsto dalle Regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 per quanto riguarda la produzione di duplicati.

La procedura che provvede alla generazione delle copie informatiche e delle copie per immagine su supporto informatico di documenti e scritture analogici rilevanti ai fini tributari, viene eseguita in conformità a quanto previsto dal DMEF 17/06/2014 art. 4 comma 1.

Dietro apposita richiesta del Cliente, i pacchetti di distribuzione possono essere prodotti e resi disponibili ai clienti anche attraverso l'utilizzo di supporti di memorizzazione auto consistenti, che non contengono riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti e della loro tipologia. La procedura di generazione del supporto autoconsistente prevede l'estrazione di pacchetti di archiviazione/distribuzione ai fini dell'esibizione dei documenti conservati dal repository di conservazione. I documenti vengono memorizzati sul supporto – la scelta del supporto è eseguita sulla base dei volumi occupati dai documenti richiesti.

All'interno di ciascun supporto sono presenti i pacchetti informativi richiesti organizzati per le singole tipologie documentali. I documenti sono ricercabili attraverso i metadati prestabiliti in fase di analisi con il cliente (sono i medesimi presenti nel portale web)..

Archivium mette a disposizione per la ricerca e la consultazione dei documenti un software atto alla visualizzazione (viewer) dei documenti e presente sul supporto stesso, che comprende le funzionalità di ricerca, visualizzazione e download. Il software presente a bordo del supporto è un eseguibile basato su tecnologie open source, libero dunque da costi di licenze.

I supporti fisici, prima di essere consegnati, vengono protetti tramite un sistema di cifratura. Il certificato di decifratura viene comunicato tramite canale differente (generalmente via pec). La consegna dei supporti ottici è affidata esclusivamente a personale selezionato, espressamente incaricato del loro trasporto.

Nei casi previsti dalla normativa in cui si renda necessaria la presenza del Pubblico Ufficiale, è nelle facoltà del cliente richiedere la produzione del duplicato informatico del documento conservato corredato dell'attestazione di conformità prevista dall'articolo 23, comma 2 del Codice dell'Amministrazione Digitale.

Le necessità di produzione di copie informatiche dei documenti sottoposti a conservazione possono essere ricondotte principalmente a due tipologie:

- esigenze di esibizione verso terzi
 - esigenze di riversamento sostitutivo (per contrastare in via preventiva i rischi legati all'obsolescenza tecnologica)
- In merito a questa seconda tipologia di necessità di adeguamento al contesto tecnologico e normativo e per assicurarsi di essere in grado di garantire la leggibilità nel tempo dei documenti informatici conservati, sarà cura del Responsabile dello sviluppo e della manutenzione del sistema di conservazione l'attività di valutazione continua nel tempo di adeguamento dei formati documentali in riferimento ai nuovi scenari tecnologici e/o giuridici.

7.8 Scarto dei pacchetti di archiviazione

Lo scarto dei pacchetti informativi sottoposti a conservazione digitale a norma è previsto principalmente per le seguenti fattispecie:

- Scadenza naturale dell'obbligo di conservazione su una partizione di un determinato archivio
- Scadenza del contratto di conservazione e mancato rinnovo
- Recesso anticipato dal contratto di conservazione

A fronte della necessità di provvedere allo scarto di pacchetti informativi, il processo prevede che ne venga data comunicazione al cliente con un congruo preavviso – individuato di default in 30 giorni. Tempistiche differenti possono essere stabilite in accordo con il cliente e inserite nel documento di specificità.

Il sistema genera apposito report che individua la tipologia documentale da sottoporre a scarto con l'elenco dei documenti coinvolti dalla procedura e la relativa data della cancellazione. Per cancellazione si intende l'eliminazione dei documenti inseriti nei pacchetti informativi, dei relativi metadati presenti nella base dati ed il blocco delle utenze che ne avevano accesso.

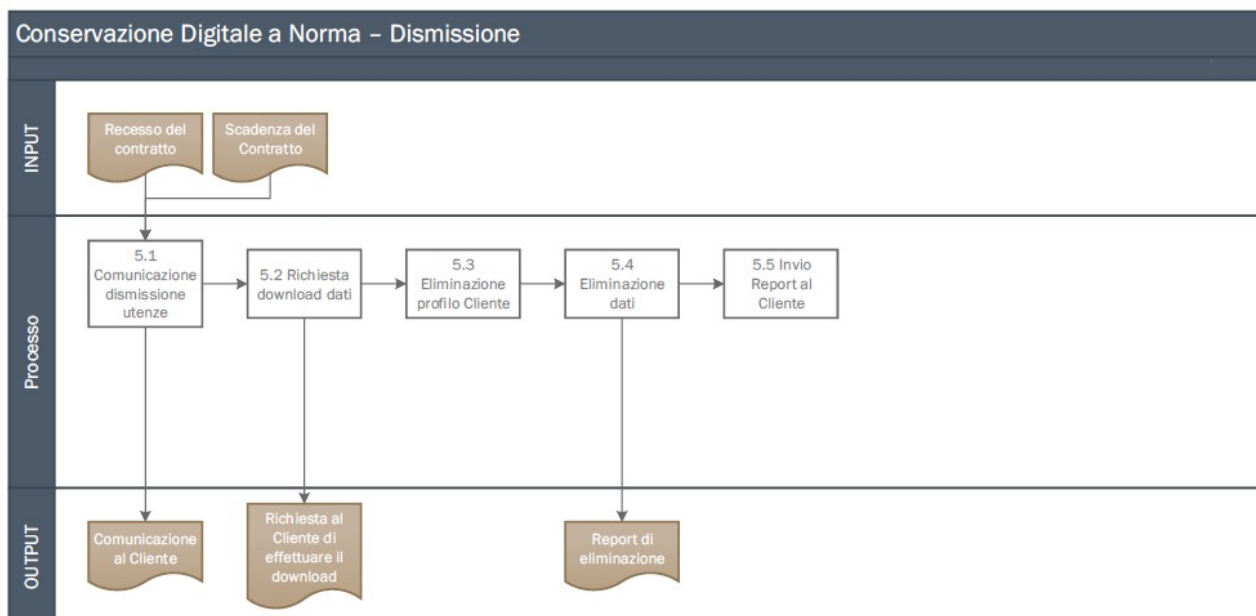
In particolare il processo di scarto si articola nelle fasi riportate nell'immagine sottostante. A fronte della comunicazione della prossimità della procedura di scarto, viene inviata la comunicazione al cliente di provvedere al download dei pacchetti informativi che stanno per subire lo scarto. A scadenza del preavviso, vengono bloccate le utenze cliente che avevano accesso ai documenti e successivamente il sistema procede all'eliminazione dei dati e dei documenti provvedendo a creare un'apposita reportistica di avvenuto scarto. Il sistema logga queste operazioni di cancellazione in un'apposita tabella. Il log di scarto registra tutte le operazioni di scarto dei documenti dei pacchetti informativi.

Nella tabella principale vengono registrati l'azienda, il modello documentale e il numero di documenti scartati. Nella tabella di dettaglio, per ogni documento, viene registrato l'id univoco che identifica il documento all'interno della tabella di versamento relativa al modello documentale in oggetto. Il contenuto del log di scarto è consultabile tramite specifica voce di menu dell'applicazione a disposizione dell'operatore interno.

Al termine del periodo di conservazione, se previsto contrattualmente, vengono consegnati al cliente tutti i pacchetti informativi sottoposti a conservazione su supporti di memorizzazione autoconsistenti. I pacchetti informativi sono organizzati come descritto nel paragrafo 7.7

A fronte dell'eliminazione dei documenti e dei metadati, come descritto nei paragrafi precedenti, viene effettuata la chiusura degli account, nonché viene predisposto l'invio di una comunicazione di conferma dell'avvenuta cancellazione di tutti i documenti e dei dati relativi.

Il processo di scarto si può sintetizzare come segue:



Nel caso di scarto di documenti e metadati la cui titolarità sia riconducibile ad una pubblica amministrazione è necessario provvedere alla richiesta preventiva di un'autorizzazione della Soprintendenza archivistica o della Commissione di sorveglianza di riferimento (come previsto dal Codice dei Beni Culturali Dlgs 42/2004) che il Titolare dovrà ottenere in tempo utile per procedere allo scarto materiale della documentazione.

Nel caso in cui lo scarto faccia riferimento ad archivi pubblici o privati di particolare interesse culturale, è necessario richiedere una preventiva autorizzazione del Ministero dei Beni e della Attività Culturali e del Turismo.

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

La suite Archicons prevede la potenziale interoperabilità ed integrazione:

- a monte, con piattaforme di gestione documentale o altri sistemi informativi aziendali, grazie all'esposizione di servizi web richiamabili da qualunque applicativo e,
- a valle, con altri sistemi di conservazione in caso di cambio conservatore (bidirezionale).

Inoltre, anche di fronte ad eventuali evoluzioni normative e tecnologiche prevedibili nel tempo, Archivium è in grado di adeguarsi tempestivamente disponendo di risorse tecnico – organizzative adeguate all'avvicinarsi delle novità tecnologiche.

L'interoperabilità è garantita in primis dall'utilizzo della struttura dell'indice del pacchetto di archiviazione, generato secondo le regole tecniche in materia di sistema di conservazione e secondo lo standard nazionale UNI SINCRO 11386:2010. La medesima struttura è utilizzata anche per la costruzione dell'indice del pacchetto di distribuzione.

Nel caso di riconsegna di tutti i PdA conservati (ad esempio per la chiusura del servizio o per la cessazione anticipata del servizio secondo quanto concordato contrattualmente) il titolare dei documenti (utente) potrà richiedere la loro distribuzione con una modalità massiva.

Il sistema ArchiCons è in grado di acquisire pacchetti di versamento/pacchetti di archiviazione conformi con la struttura UNI SINCRO 11386:2010 nel caso di subentro su archivi gestiti da altro conservatore che abbia adottato tale standard per la generazione dell'IPdA. Anche l'accettazione e l'utilizzo esclusivo dei formati previsti dall'allegato 2 delle Regole Tecniche promuovono la garanzia di interoperabilità tra i sistemi e la trasferibilità ad altri conservatori.

8. IL SISTEMA DI CONSERVAZIONE

Nei successivi paragrafi vengono descritte in dettaglio le componenti logiche, tecnologiche e fisiche esistenti e le loro principali funzionalità, che vanno a comporre l'intero Sistema di Conservazione. Gli aspetti relativi alla sicurezza informatica del Sistema sono riportati dettagliatamente all'interno del Piano della Sicurezza, secondo quanto previsto dall'art. 12 del DPCM 3 dicembre 2013 a cui si fa rinvio.

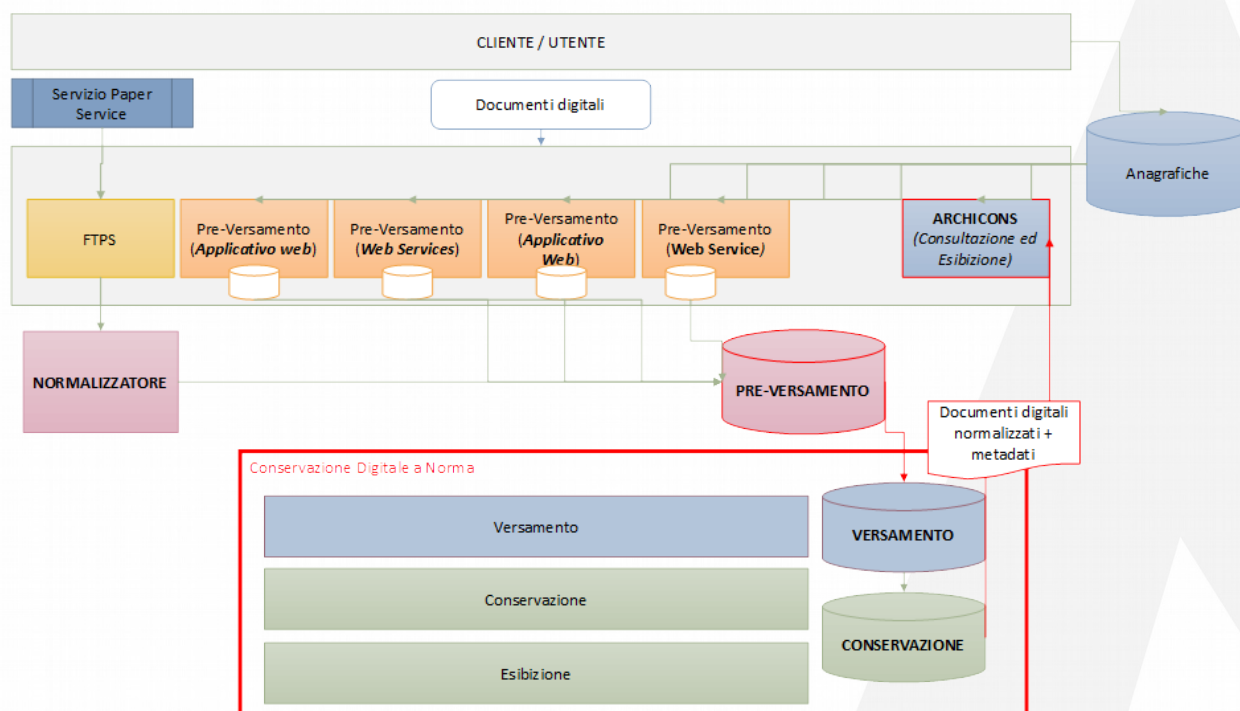
All'interno del Piano della Sicurezza vengono descritte le modalità con cui Archivium assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, entrando nel dettaglio dei controlli di sicurezza delle diverse componenti del sistema e delle procedure adottate per garantire la ridondanza degli archivi medesimi (Backup), la dislocazione geografica (Disaster Recovery) e la Continuità Operativa (Business Continuity).

8.1 Componenti Logiche e Tecnologiche

L'applicazione Archicons, denominato nel presente documento anche come più genericamente il Sistema di Conservazione, consiste essenzialmente in tre moduli applicativi:

- Versamento
- Conservazione
- Esibizione

I moduli Versamento e Conservazione sono finalizzati alla Conservazione Digitale a Norma, pertanto prevedono l'acquisizione dei documenti, la relativa indicizzazione per la ricerca e l'archiviazione documentale secondo le normative di riferimento. L'Esibizione è il modulo che permette invece la generazione dei documenti preventivamente conservati per un loro utilizzo secondo i termini di legge.



Ogni modulo risponde ad una logica di struttura multi tier:

- Livello di Presentazione Front End e Componenti Logico Applicative atte allo svolgimento di tutte le fasi del processo di conservazione: insieme delle interfacce attraverso le quali gli utenti interagiscono con il sistema nelle diverse fasi del processo di conservazione utilizzando le componenti logiche sottostanti.
- Livello di Gestione Dati: rappresentato dai differenti DB di gestione-omogenizzazione dati, versamento, conservazione e gestione anagrafiche-modelli documentali (la gestione database è esplicitata poco più avanti)
- Livello Repository per lo storage dei documenti e dei pacchetti informativi gestiti, versati e conservati

L'infrastruttura relativa ad Archicons ha una componente centrale, per l'elaborazione e presentazione delle informazioni, ospitata nel Datacenter COLT Telecom di Torino. In particolare, i Clienti finali Archicons hanno a disposizione diversi Servizi Web che consentono loro di generare e/o caricare i documenti oggetto di Conservazione Digitale a Norma. Il primo modulo "*Versamento e Conservazione*" emette un Report di versamento per confermare l'avvenuta presa in carico dei documenti.

I dati sono trasferiti dalla postazione utente al Servizio centralizzato attraverso il protocollo HTTPS (o FTPS) che garantisce un trasferimento sicuro delle informazioni.

Infine gli utenti, mediante la propria postazione di lavoro e attraverso lo stesso canale di comunicazione per l'acquisizione dei dati, possono accedere alla componente centrale di Archicons per la visualizzazione ed elaborazione dei dati (Esibizione).

Il Servizio è erogato su un'infrastruttura situata presso Data Center Colt – certificato ISO27001. La soluzione prevede adeguati presidi tecnologici e infrastrutturali volti a garantire misure di alta affidabilità e disaster recovery in linea con le indicazioni della normativa in materia e con le prassi adottate sul mercato.

Attraverso l'implementazione dei Processi di "Business Continuity e Disaster Recovery" è stata predisposta una infrastruttura aggiuntiva rispetto a quella ubicata nel sito primario di Torino, attraverso cui poter erogare i servizi relativi all'ambiente di esercizio dell'applicazione Archicons. Questa infrastruttura, ubicata a Frosinone presso il datacenter Seeweb, diventa operativa in caso di eventi di interruzione non pianificati dei servizi sul sito primario.

L'infrastruttura relativa all'ambiente di esercizio dell'applicazione Archicons presente nel sito secondario è speculare a quella nel sito primario, in modo da garantire l'assenza di degradi prestazionali.

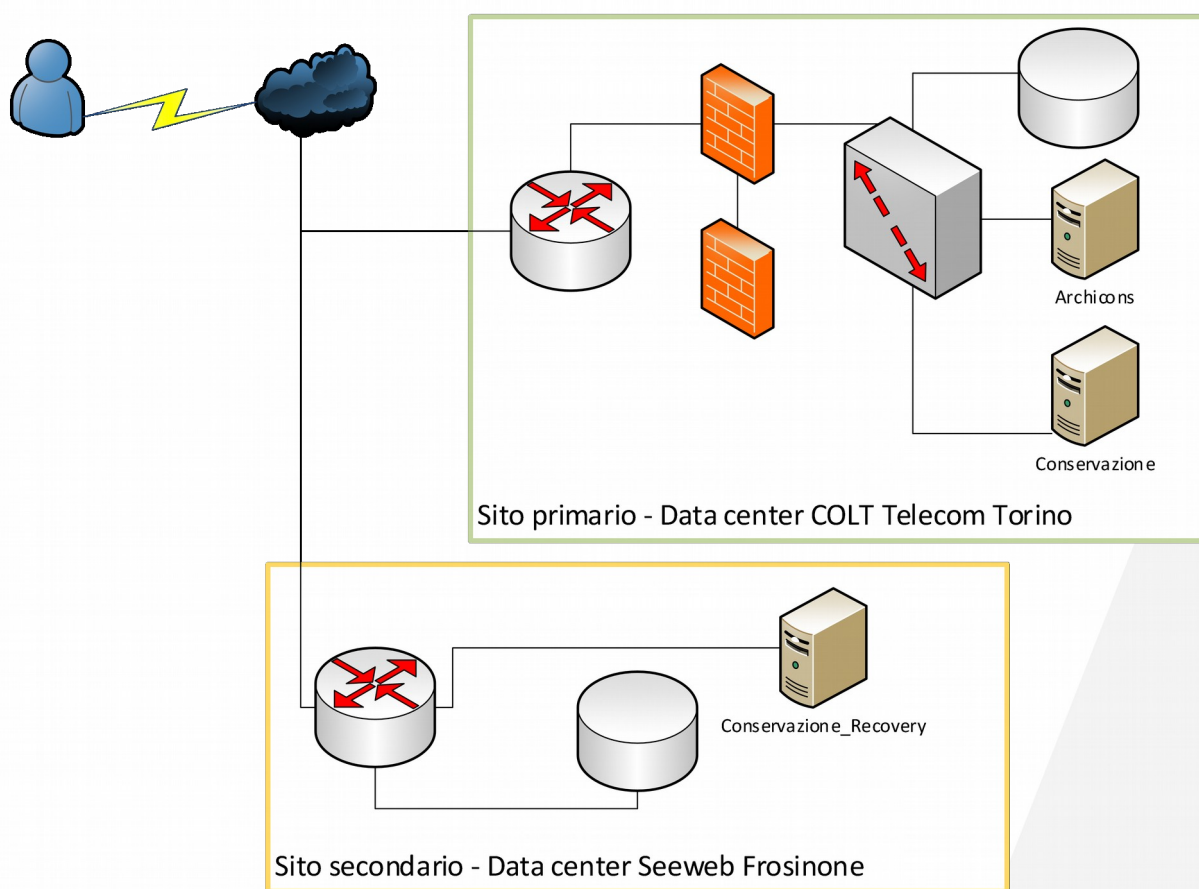
Nell'architettura è prevista una separazione fisica e logica degli ambienti di sviluppo e produzione.

Nell'erogazione del Servizio di conservazione Archicons di Archivium, gli aspetti della sicurezza rispettano i principi espressi dalle policies aziendali di Archivium e dei Datacenter presso i quali risiedono la farm principale e secondaria di Archivium. Entrambi i datacenter detengono la certificazione ISO 27001 a garanzia del rispetto delle misure e dei principi di sicurezza richiesti.

8.2 Componenti Fisiche

Schema e descrizione dei siti di conservazione e delle connessioni tra i diversi siti e tra i diversi attori del sistema, con riferimento alle componenti tecnologiche del paragrafo precedente.

Schema e descrizione delle componenti fisiche presenti in ciascuno dei siti di conservazione.



Nel Datacenter primario sono presenti i seguenti elementi:

- Un server virtuale di sviluppo e test con ambiente controllato ed omogeneo rispetto all'ambiente di produzione;
- Un server virtuale "Archicons" che acquisisce i dati e li invia, attraverso i Web Services, al DB "AZI_GE"
- Un server virtuale "Conservazione" che riceve i dati dal server "Archicons" attraverso un Controller che apre la connessione sul DB AZI_VE da un'utenza dedicata con password criptata, l'utenza lancia la procedura di trasferimento FTP tra i due server e c'è il controllo dell'hash
- DB AZI_GE: è il data base che memorizza le informazioni gestite ed elaborate dal Web Service
- DB AZI_VE: è il data base che memorizza le informazioni gestite ed elaborate dal Web Service
- DB AZI_CO: è il data base che memorizza le informazioni gestite ed elaborate dal Web Service
- DB ANAGRAFICHE: è il database che contiene i dati relativi ai Clienti e agli utenti e Modelli Documentali, inoltre gestisce i token per gli accessi – nonché le relazioni tra di essi.

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

8.3 Procedure di gestione e di evoluzione

Il Sistema di Conservazione ha come principale scopo quello di garantire che per tutti i documenti in esso conservati siano verificate le condizioni previste dall'art. 44 del Codice dell'Amministrazione Digitale.

Sono dunque state poste in essere adeguate politiche di governance e gestione per poter ottemperare agli obblighi richiesti di garantire integrità, leggibilità e reperibilità nel tempo dei documenti, nonché il rispetto delle misure di sicurezza previste dal decreto legislativo 30 giugno 2003, n. 196.

Le procedure di gestione del sistema di conservazione prevedono un costante monitoraggio del sistema stesso, così da poter intercettare in modo tempestivo eventuali necessità di ripristini, modifiche e/o evoluzioni del sistema stesso.

Il sistema di conservazione ha uno specifico meccanismo per identificare eventuali corruzioni o perdite dei dati a seguito di specifiche azioni eseguite. Il sistema di conservazione mantiene tutta la documentazione relativa alle azioni gestionali ed ai processi amministrativi rilevanti per la creazione del PdA. Eventuali deviazioni dal normale processo possono essere identificate ed indagate. Sono descritte le politiche di conservazione dei pacchetti di archiviazione (PdA), in maniera dettagliata, per assicurare il contenuto dell'informazione per l'ente produttore e l'integrità nel tempo.

Il sistema mantiene tutta la documentazione relativa alle azioni gestionali ed ai processi amministrativi rilevanti per la conservazione, mantenuta in accordo con le procedure documentate all'interno del Sistema di Gestione Integrato. Tali procedure prevedono anche la registrazione e la risposta agli eventuali errori rispetto ai documenti ed in risposta agli utenti.

I requisiti di sicurezza (sicurezza fisica, sicurezza logica e sicurezza organizzativa) adottati nella conduzione e manutenzione del sistema di conservazione, nelle politiche di gestione dell'incident management e della continuità operativa del servizio di conservazione sono specificati e riportati nel piano della sicurezza e nella documentazione del sistema di gestione della sicurezza.

Il conservatore mantiene la cronologia delle releases utilizzando un apposita naming convention di cartelle e storicizzando le vecchie releases.

La procedura dei rilasci del software è una procedura che segue i requisiti imposti dalla certificazione ISO/IEC 27001:2013.

Archivium mette a disposizione sia un servizio di assistenza attraverso un portale di web ticketing che permette la segnalazione di anomalie, bug, richieste di assistenza tecnica – normativa – organizzativa agli utenti preventivamente autorizzati all'utilizzo.

Il sistema prevede due livelli di help desk:

- Help Desk di primo livello: è composto da addetti in grado di risolvere dubbi relativi all'utilizzo del servizio, del portale web o di procedura. E' il primo livello di contatto tra utente ed azienda – se l'intervento non è risolutivo, l'operatore di help desk di primo livello è in grado di identificare la natura del problema e di assegnare tramite la piattaforma di assistenza la segnalazione ad un operatore di help desk di secondo livello.
- Help Desk di Secondo Livello: è suddiviso in più aree tematiche Assistenza Tecnica – Sviluppo e Maintenance – Amministrativo&Legale. Gli operatori di secondo livello prendono in carico le segnalazioni pervenute dagli operatori di help desk di primo livello, provvedono alla risoluzione di dubbi ed anomalie, chiudendo i ticket a loro assegnati direttamente tramite la piattaforma.

8.4 Change management

La gestione dei Change è finalizzata a verificare che i cambiamenti all'infrastruttura e/o alle applicazioni non abbiano impatto sulla gestione della sicurezza dei dati.

Il RSIS (Responsabile dei Sistemi e della Sicurezza), è responsabile – direttamente o tramite riferimenti da lui indicati – dell'identificazione, analisi e valutazione degli impatti sui controlli di sicurezza, scaturiti eventualmente da uno o più cambiamenti al Servizio CDN. Questa valutazione, qualora si ritenga necessario, potrà essere supportata da metodologie e strumenti di Risk Analysis, aventi il fine di agevolare proprio la valutazione di impatto. Nel momento in cui sorge necessità di aggiungere / modificare / rimuovere asset hardware o software, è necessario che chi manifesta tale necessità invii una mail al responsabile dei sistemi informativi / responsabile della sicurezza, al fine di valutare i rischi di tali Change. Il Responsabile dei sistemi informativi / responsabile della sicurezza, valuterà le richieste e deciderà se approvarle o rifiutarle, mediante comunicazione scritta (e-mail).

Il Report relativo agli Asset dovrà essere modificato di conseguenza. Nel caso in cui il cambiamento comporti un disservizio o un degrado, devono essere disponibili specifiche procedure di roll back. Il processo di cambiamento è applicato sia al personale interno, che al personale esterno, come anche nei confronti di possibili outsourcer.

In caso di emergenza l'outsourcer comunica i cambiamenti eseguiti, le motivazioni sottostanti e la documentazione a supporto via e-mail al RSIS. La documentazione in relazione all'accettazione dei sistemi (nuovi sistemi, upgrade, nuove versioni, ecc.), è mantenuta con modalità che assicurino la sua sicurezza e l'aggiornamento periodico, in particolare per la configurazione dei sistemi e per i processi di test e valutazione degli effetti di tale cambiamento sui processi critici del sistema di conservazione

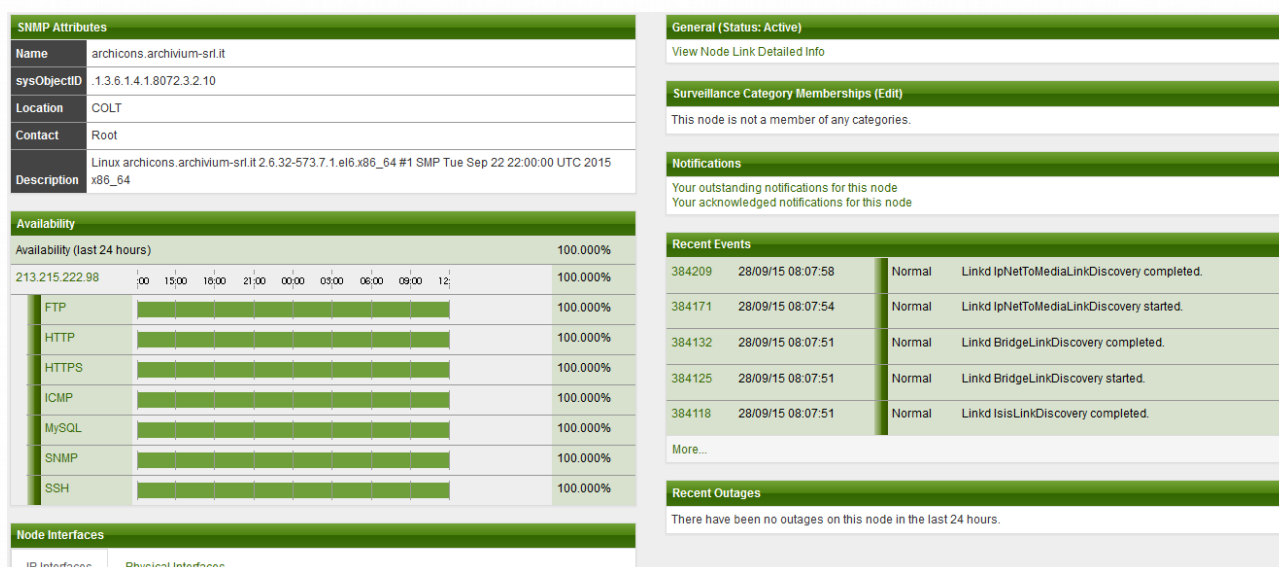
9. MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

Il sistema di conservazione di Archivium è sottoposto a costante monitoraggio, attraverso l'adozione di specifici strumenti in grado di rilevare eventuali malfunzionamenti ed è dotato di adeguate politiche ed istruzioni al fine di garantire il ripristino dei livelli standard di erogazione del servizio.

Il monitoraggio è effettuato a livello sistemistico ed applicativo su tutti i moduli che costituiscono il sistema, dal pre-versamento, al versamento, al modulo di conservazione ed infine quello di esibizione. A livello sistemistico viene monitorato l'uptime delle macchine, nonché l'utilizzo delle loro risorse e le disponibilità residue.

Il software utilizzato è OpenNMS:



Per quanto riguarda la parte applicativa, è disponibile inoltre un servizio di help desk che garantisce assistenza per anomalie riguardanti gli accessi al sistema di conservazione ed in merito alle trasmissioni dei pacchetti informativi. Il sistema di monitoraggio sistemistico e applicativo di Archivium è in grado di rilevare le anomalie specifiche del sistema di conservazione e provvede a generare apposite segnalazioni agli utenti preposti.

Sia le segnalazioni di anomalia che le relative azioni intraprese al fine della risoluzione delle stesse sono documentate nei log di sistema specifici del sistema di conservazione ed anch'essi conservati nel tempo.

9.2 Verifica dell'integrità degli archivi

L'attività di verifica dell'integrità dei documenti viene svolta dalla Suite ArchiCons attraverso il monitoraggio continuo della disponibilità dei servizi. L'integrità degli archivi consiste in una verifica di congruità calcolata confrontando il numero di files presenti nel pacchetto di archiviazione, il numero di record presenti nel database ed il numero totale dei documenti riportati all'interno dell'indice del Pacchetto di Archiviazione.

Per quanto riguarda la verifica di integrità, è presente all'interno della suite ArchiCons una procedura che effettua il calcolo automatico dell'hash del documento e provvede alla sua comparazione con l'hash presente all'interno dell'indice del pacchetto di conservazione.

Per quanto riguarda le verifiche sulla leggibilità dei documenti viene effettuata a campione su una percentuale congrua dei documenti conservati (1% se non diversamente previsto dalle clausole contrattuali) l'apertura dei files da parte di un operatore che ne attesterà la leggibilità ad occhio umano.

In caso di non conformità viene prodotto un report di anomalie inviato al Responsabile del Servizio di Conservazione. In caso di esito di controllo negativo sulla leggibilità o sull'integrità dei documenti conservati, è necessario mettere in atto la procedura di riversamento diretto, come previsto dalle Regole Tecniche art.7 dalle altre copie ancora consistenti.

L'allerta preventiva è implementata a livello di infrastruttura fisica e logica. Il sistema di monitoraggio controlla in tempo reale se tutti i componenti del sistema di conservazione sono disponibili e se le relative performance sono soddisfacenti. In caso di malfunzionamento e/o degrado, il sistema di monitoraggio effettua la segnalazione via e-mail. La mail consente al gruppo tecnico di verificare e di intervenire secondo l'apposito processo da instradare (rimozione del malfunzionamento, apertura di una richiesta di cambiamento per migliorare le performance, ecc).

Poiché l'allerta preventiva è in tempo reale, la schedulazione delle verifiche riguarda la leggibilità dei documenti. Ciascun contratto prevede delle verifiche periodiche (mensili, trimestrali, etc) in funzione del volume di documenti previsti.

Sistemi di analisi dei risultati e di archiviazione dei medesimi: per quanto concerne l'analisi e l'archiviazione dei risultati:

- **il sistema di monitoraggio archivia tutti i dati rilevati in tempo reale e li storicizza per un mese;**
- **il report relativo alle eventuali anomalie emerse dal controllo visivo dei documenti viene salvato e mantenuto per la durata prevista dal contratto.**

9.3 Soluzioni adottate in caso di anomalie

Il supporto tecnico comunicherà i riferimenti tramite i quali contattare il supporto di primo livello che svolgerà il ruolo di prima interfaccia per la ricezione delle richieste. Il supporto di I livello sarà disponibile per essere contattato telefonicamente e/o per email negli orari indicati nel contratto.

Il supporto di I livello è incaricato di ricevere gli Alert dal sistema di monitoraggio e le Richieste da parte del Cliente, attivando i diversi processi in funzione della tipologia di segnalazione/richiesta:

- **Incident Management** a fronte di malfunzionamenti e/o guasti;
- **Service Request** a fronte di richieste di informazioni e/o richieste di cambiamenti e/o richieste di accesso. Le Richieste inerenti la necessità di apportare cambiamenti saranno identificate come **Change** a fronte della necessità di migliorare delle prestazioni e/o delle funzionalità.

Per ogni richiesta, Il supporto tecnico comunicherà via e-mail la ***presa in carico dell'attività***.

9.4 Incident Management

Tutte le attività a fronte di malfunzionamenti segnalati dal Cliente o in seguito alla segnalazione di Exception (attraverso i sistemi di Alert) emerse in relazione a guasti e/o malfunzionamenti, sono da considerarsi attività gestite attraverso il processo di **Incident Management**.

- Le attività inerenti la gestione degli incident causati da malfunzionamenti/degradi relativi al sistema operativo e/o al corretto funzionamento e le corrette configurazioni del server (servizi centralizzati) sono incluse nel canone.
- Le attività inerenti la gestione degli incident causati dalle postazioni di lavoro o terze parti non sono comprese nel canone (extra-manutenzione).

A fronte del verificarsi di un Incident, Il supporto tecnico si impegna ad intervenire autonomamente per il ripristino delle funzionalità. Qualora la natura dell'intervento pregiudichi l'erogazione di altri servizi o richieda azioni da parte del Cliente, sarà cura del supporto tecnico avvisare il Cliente, con cui si concorderà eventualmente la linea di azione da intraprendere (escalation). Durante l'orario di reperibilità, Il supporto tecnico è autorizzata preventivamente dal Cliente ad applicare le procedure che ritiene più opportune per l'applicazione dei workaround.

In caso di Incident di Sicurezza "bloccante" il supporto tecnico interviene senza necessariamente l'approvazione scritta da parte del Cliente. Per le altre tipologie di incident invece, in caso di necessità di down dei sistemi, verrà opportunamente segnalata al Cliente la necessità di operare in tale modalità e verranno concordate le tempistiche per effettuare l'eventuale spegnimento dell'infrastruttura.

9.5 Release Management

Il supporto tecnico garantisce un costante aggiornamento dei sistemi a fronte di rilasci da parte dei produttori software, di versioni che correggano errori o vulnerabilità dei sistemi e dei servizi.

In particolare Il supporto tecnico si occuperà di evadere tutte le attività relative alle *Minor Release* necessarie; le attività relative all'installazione e configurazione di Major release non sono incluse nel canone e potranno essere oggetto di valutazione del rischio ed emissione di Offerta ad hoc.

9.6 Event Management

Il supporto tecnico si occuperà dell'implementazione di sistemi di alert basati su logwatch, software OpenNMS.

Destinatari delle segnalazioni saranno i contatti del supporto tecnico incaricato del primo livello di assistenza.

A fronte dell'Alert (Warning ed Exception), sarà compito del supporto tecnico intraprendere le operazioni necessarie al ripristino nei tempi e nelle modalità previste per la tipologia di servizio. In caso di segnalazione relativa ad eventi di sicurezza e/o di debolezze associate ai sistemi utilizzati, il supporto tecnico comunicherà tempestivamente al Cliente la segnalazione, ed in caso di effettivo Incident di Sicurezza, questo verrà trattato come specificato nell'apposita sezione.