Azienda OspedalieraBrotzu

Deliberazione n. 642

Adottata dal Commissario Straordinario in data - 7 APR. 2016

OGGETTO: adozione manuale di conservazione sostitutiva.

Pubblicata all'Albo Pretorio dell'Azienda a partire dal - 8 APR. 2016 per 15 giorni consecutivi e posta a disposizione per la consultazione.

IL Commissario Straordinario Dr.ssa Graziella Pintus
Coadiuvato dal
DIRETTORE AMMINISTRATIVO Dr.ssa Laura Balata
DIRETTORE SANITARIO Dr.ssa Maria Gabriella Nardi

Su Proposta del Responsabile della Conservazione Sostitutiva.

Premesso che con il D.Lgs 82/2005, noto come Codice della Amministrazione Digitale, prevede all'art. 43 la validità di qualunque atto, dato, documento di cui sia prescritta la conservazione digitale, purché questa sia effettuata nel rispetto della normativa.

Considerato che all'art. 44 comma 1 bis del D.Lgs, di cui sopra prevede che la gestione di una simile conservazione sia carico di un Responsabile della conservazione documentale.

Considerato che nell'ottica del completamento regolamentare di tale normativa è stato emanato il DPCM 3 dicembre 2013 recante 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".

Dato atto che con delibera n 1808 del 21.10.2015 è stato nominato quale Responsabile della conservazione documentale il funzionario degli AA.GG. Dott. Giuliano Marras e suo delegato per le questione tecnico informatiche l'Ing. Andrea Alimonda, Dirigente Analista della Struttura dei Servizi Informatici.

Visto che l'art. 8 DPCM del 3 dicembre 2013 (recante Regole tecniche in materia di sistema conservazione), richiede l'adozione di un manuale di conservazione che illustri dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Visto la proposta di manuale di conservazione proposto dal Responsabile della Conservazione, allegato alla presente.

Visto il parere favorevole del delegato del Responsabile della Conservazione, Ing. Andrea Alimonda.

Visto il parere favorevole del Direttore Sanitario nonché del Direttore Amministrativo.

DELIBERA

Di adottare il manuale di conservazione di cui all'art. 8 DPCM del 3 dicembre 2013, allegato alla presente per farne parte integrante e sostanziale.

Il Direttore Amministrativo
Dr.ssa Laura Balata

Il Direttore Sanitario
Dr.ssa Maria Gabriella Nardi

Il Commissario Straordinario
Dr.ssa Graziella Pintus

Res.Cons.Doc.Dr.G.Marras

Manuale di Conservazione

Azienda Ospedaliera Brotzu
Cagliari

Storia del documento

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	31/03/2016	Giuliano Marras	*Resp.Conserv.Sost.*
Verifica			
Approvazione			

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Paragrafo	Modifiche apportate	Osservazioni
1	31/03/2016	/	Prima versione del documento	0

INDICE DEL DOCUMENTO

Manuale di Conservazione
2016

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale del sistema di conservazione (di seguito per brevità chiamato anche "Manuale") e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione dei processi, in particolare le modalità di versamento, archiviazione e distribuzione, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione digitale di documenti informatici.
Con il presente Manuale si fa riferimento alla versione corrente del presente documento.
In particolare, nel presente Manuale sono riportati:
a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
c) la descrizione delle tipologie dei documenti informatici sottoposti a conservazione,
d) comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
e) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento e della descrizione dei controlli effettuati su ciascuno specifico formato adottato;
f) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
g) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
h) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logi-che, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
i) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
j) la descrizione delle procedure per la produzione di duplicati o copie;
k) i tempi entro i quali le diverse tipologie di documenti informatici devono essere oggetto di scarto/cancellazione;
l) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
m) le normative in vigore nei luoghi dove sono conservati i documenti;

Il Manuale recepisce le disposizioni di cui al D.Lgs. 7 marzo 2005, n. 82, e s.m.i. (Codice dell'amministrazione digitale), di seguito per brevità chiamato anche "Codice" o "CAD", oltre alle indicazioni riportate nei provvedimenti di legge o di prassi richiamati nel capitolo "Riferimenti normativi e di prassi" nonché i provvedimenti di natura tecnica richiamati nel capitolo "Riferimenti tecnici".
Questo documento è pubblicato sul sito Web dell'AOB.
Il documento è pubblicato in formato PDF sottoscritto con firma digitale del Responsabile del servizio di Conservazione in modo tale da assicurarne l'integrità e l'autenticità.
Come versione corrente del Manuale si intenderà esclusivamente la versione in formato elettronico disponibile sul sito Web di cui sopra.

TERMINOLOGIA (GLOSSARIO, ACRONIMI, DEFINIZIONI)

Agenzia per L'Italia Digitale (già DigitPA): Ente pubblico non economico, con competenza nel settore delle tec-nologie dell'informazione e della comunicazione nell'ambito della pubblica amministrazione. L'Ente, che ha ereditato le funzioni di DigitPA che, a sua volta, ha ereditato le funzioni del CNIPA, opera secondo le direttive per l'attuazione delle politiche e sotto la vigilanza del Ministro per la pubblica amministrazione e l'innovazione, con autonomia tecnica e funzionale, amministrativa, contabile, finanziaria e patrimoniale;
-**AOB**, Azienda Ospedaliera "G.Brotzu" Cagliari;

ASP - Application Service Provider: Fornitore di Servizi Applicativi;
CAD: Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni - "Codice dell'amministrazione digitale";
CA - Certificatore Accreditato: soggetto autorizzato dall'Agenzia per l'Italia Digitale che garantisce l'identità dei soggetti che utilizzano la firma digitale;
CC - Common Criteria: Criteri per la valutazione della sicurezza nei sistemi informatici, con riconoscimento internazionale in quanto evoluzione dei criteri europei (ITSEC), statunitensi (Federal Criteria), e canadesi (Canadian Criteria);
C.M. - Circolare Ministeriale;
CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione: creato con l'articolo 176 del DL 196/03, il CNIPA ha incorporato le strutture e le funzioni dell'AIPA e del Centro Tecnico della RUPA ed è stato quindi sostituito da DigitPA e quindi dall'AgID - Agenzia per l'Italia Digitale;
CSCD - contratto di servizio di conservazione dei documenti: Contratto di servizio di conservazione dei documenti, ove sono esplicitate chiaramente: l'ambito della delega conferita, le specifiche funzioni, le attività e le responsabilità affidate al Conservatore Esterno.
D.LGS. - Decreto Legislativo;
D.M. - Decreto Ministeriale;
DNS – Domain Name System: Sistema di gestione dei nomi simbolici associati ad indirizzi di siti e domini Internet: Quando un messaggio di posta elettronica (e-mail), o un applicativo di consultazione di siti internet (browser) punta ad un dominio, il DNS traduce il nome inserito sotto forma di URL (es. http://www.....it)/ in un indirizzo costituito da una sequenza numerica convenzionale (es. 123.123.23.3).
D.P.C.M.: Decreto del Presidente del Consiglio dei Ministri;
D.P.R.: Decreto Presidente della Repubblica;
DPS: Documento Programmatico per la Sicurezza;
ETSI: European Telecommunications Standards Institute;
-**FTP Server**, programma che permette di accettare connessioni in entrata e di comunicare con un client attraverso il protocollo FTP.

Internet Data Center o IDC: il centro servizi che ospita e gestisce l'insieme delle risorse hardware, il software di base, l'applicativo necessario a consentire l'utilizzo dei prodotti, dei software e delle procedure informatiche del Gestore Esterno, nonché i documenti informatici del cliente del Gestore;
-**IdP,** Strumento per rilasciare le informazioni di identificazione e di tutti i soggetti che cercano di interagire con un sistema.

HSM - Hardware Security Module: dispositivi hardware dedicati per la sicurezza crittografica e la gestione delle chiavi in grado di garantire un elevato livello di protezione;

HTTP (Hypertext Transfer Protocol): Protocollo di trasmissione, che permette lo scambio di file (testi, immagini grafiche, suoni, video e altri documenti multimediali) su World Wide Web;
HTTPS (Secure Hypertext Transfer Protocol): Protocollo di trasmissione, sviluppato da Netscape Communications Corporation, per la cifratura e decifratura dei dati trasmessi durante la consultazione di siti e pagine In-

ternet. Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL;
ICT - Information and Communication Technology: Tecnologia dell'Informazione e delle Telecomunicazioni. Il dipartimento che gestisce i sistemi informatici e telematici;
INTERNET: Un sistema globale di reti informatiche nel quale gli utenti di singoli computer possono ottenere in-formazioni da luoghi diversi. Lo sua grande diffusione è stata determinata principalmente dall'introduzione dei protocolli di trasmissione di documenti con riferimenti ipertestuali (HTTP) e dallo sviluppo del World Wide Web (WWW);
ISO – International Organization for Standardization: Organizzazione internazionale per la standardizzazione, costituita da organismi nazionali provenienti da più di 75 paesi. Ha stabilito numerosi standard nell'area dei si-stemi informativi. L'ANSI (American National Standards Institute) è uno dei principali organismi appartenenti all'ISO;
ITSEC – Information Technology Security Evaluation Criteria: Criteri europei per la valutazione della sicurezza nei sistemi informatici;
MEF: Ministero dell'Economia e delle Finanze;
NTP – Network Time Protocol: Protocollo per la sincronizzazione del tempo;
OID – Object IDentifier: Sequenza numerica univoca che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO;
PdV: Pacchetto di Versamento
PdA: Pacchetto di Archiviazione
PdD: Pacchetto di Distribuzione
PU: Pubblico Ufficiale
PIN – Personal Identification Number: Codice di sicurezza riservato che permette l'identificazione del soggetto abbinato ad un dispositivo fisico. Permette ad esempio l'attivazione delle funzioni del dispositivo di firma;
POP – Point of Presence: Punto di accesso alla rete internet;
PSCD - Prestatore di Servizi di Conservazione dei Dati: nella fattispecie, ARUBA;
SSL – Secure Socket Layer: Protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica;
SLA - Service Level Agreement: strumenti contrattuali che definiscono le metriche di servizio (es. qualità di servizio) che devono essere rispettate da un fornitore di servizi nei confronti dei propri clienti;
TSA - Time Stamping Authority;
TSS - Time Stamping Service;
TUDA - DPR 28 dicembre 2000, n. 445, e successive modificazioni - "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
URL – Uniform Resource Locator: Sistema standard di nomenclatura specificante un sito, dominio o altro oggetto (file, gruppo di discussione, ecc.) su Internet. La prima parte dell'URL (http:, ftp:, file:, telnet:, news:) spe-cifica il protocollo di accesso all'oggetto;
XML - Extensible Markup Language;
WWW – World Wide Web: insieme di risorse interconnesse da hyperlink accessibili tramite Internet

DEFINIZIONI

Secondo la normativa vigente e ai fini dell'interpretazione del presente Manuale, i termini e le espressioni sotto elencate avranno il significato descritto nelle definizioni in esso riportate. Qualora le definizioni adottate dalla normativa di riferimento non fossero riportate nell'elenco che segue, si rimanda ai testi in vigore per la loro consultazione.
I termini e le espressioni non definiti avranno il significato loro attribuito all'interno del paragrafo o sezione che li contiene.

Accesso: operazione che consente a chi ne ha diritto di prendere visione dei documenti informatici conservati;
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 conserva-zione o di certificazione del processo di conservazione;
Agente di Alterazione: sono agenti di alterazione le macro, i codici eseguibili nascosti, le formule di foglio di lavoro nascoste o difficili da individuare, sequenze di caratteri nascoste all'interno dei dati le quali sono ignora-te dall'applicazione originalmente prevista per la presentazione, che però possono essere riconosciute quando i dati vengano elaborati con altre applicazioni;
Aggregazione documentale informatica: raccolta di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente;
Archivio: complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività;
Archivio informatico: archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico;
Area organizzativa omogenea: un insieme di funzioni e di strutture, individuate dall'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico: dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico;
Autenticità: caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico;
Base di dati: collezione di dati registrati e correlati tra loro;
Certificatore accreditato: soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dell'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 eliminazio-ne o conservazione nel tempo;
Chiusura del pacchetto di archiviazione: operazione consistente nella sottoscrizione del pacchetto di archiviazione con firma digitale apposta da un Firmatario Delegato del Conservatore esterno e apposizione di una validazione temporale con marca temporale alla relativa impronta;
Classificazione: attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci indi-viduate attraverso specifici metadati;
Cliente: è l'AOB in veste di controparte contrattuale di un contratto di Conservazione, rispetto al Conservatore stesso. Il Cliente è l'unico e legittimo titolare degli oggetti/dati/documenti depositati in conservazione;
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 o da un certificatore accreditato, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza;
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;

Contrassegno a stampa: contrassegno generato elettronicamente, apposto a stampa sulla copia analogica di un documento amministrativo informatico per verificarne provenienza e conformità all'originale;
Contratto: è il Contratto per l'affidamento del servizio di conservazione digitale di documenti informatici perfezionato AOB (Cliente) e conservatore esterno, che regola gli aspetti generali dell'erogazione del Servizio di conservazione digitale dei documenti informatici del Cliente;
Coordinatore della Gestione Documentale: responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 e s.m.i. nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee;
Copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;
Copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;
Copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;
Copia di sicurezza: copia di backup degli archivi del sistema di conservazione;
Descrittore evidenze: vedi pacchetto informativo;
Destinatario: identifica il soggetto/sistema al quale il documento informatico è indirizzato;
DIRT: documenti informatici rilevanti ai fini delle disposizioni tributarie;
Documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;
Documento analogico originale: documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
Documento originale unico: è quel documento analogico il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta, anche presso terzi e che non soddisfa, dunque, alcuna delle condizioni elencate nella definizione di "Documento analogico originale";
Documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
Duplicato Informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso supporto o su supporti diversi, della medesima sequenza di valori binari del documento originario;
Duplicazione dei documenti informatici: produzione di duplicati informatici;
Esibizione: operazione che consente di visualizzare un documento conservato e di ottenerne copia;
Estratto per riassunto: documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici;
Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informa-tica;
Fascicolo informatico: raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell'ambito della pubblica amministrazione. Per i soggetti privati è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all'erogazione di uno specifico servizio o prestazione;
File di chiusura: insieme di metadati, su cui è apposta la firma digitale e marca temporale, in grado di fornire prova dell'integrità di un insieme di documenti informatici, ad esso associati, la cui conservazione decorre dal momento di apposizione della marca temporale;
Firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
Fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

Formato: modalità di rappresentazione del documento informatico mediante codifica binaria; comunemente è identificato attraverso l'estensione del file e/o il tipo MIME;
Funzionalità aggiuntive: le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni;
Funzionalità interoperative: le componenti del sistema di protocollo informatico finalizzate a rispondere alme-no ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;
Funzionalità minima: la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;
Funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una sequenza di bit (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;
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 documen-to informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione;
idPdV: Indice del Pacchetto di Versamento
Immodificabilità: caratteristica che rende la rappresentazione 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 pri-ma di una opportuna funzione di hash;
Insieme minimo di metadati del documento informatico: complesso dei metadati da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta;
Integrità: insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato;
Interoperabilità: capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi;
Leggibilità: insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti;
Log di sistema: registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introduco-no in una base di dati;
Manuale di gestione: strumento che descrive il sistema di gestione informatica dei documenti;
Memorizzazione: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elabora-zione, di documenti analogici o informatici;
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*;
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;
Normativa regolante la conservazione digitale di documenti informatici: si intende: il D.lgs. 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione Digitale "CAD") e i relativi decreti attuativi, le regole tecniche e aggiungendo, per il documento informatico a rilevanza tributaria, le disposizioni di cui al DMEF 17 giugno 2014 e s.m.i., il DPR 26 ottobre 1972 n. 633 e s.m.i., il DPR 29 settembre 1973 n. 600 e s.m.i., i provvedimenti interpre-tativi emessi dagli organi competenti;
Originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o do-cumenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

Pacchetto di archiviazione: pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e 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 invio documenti: pacchetto informativo utilizzato per inviare i documenti fisici al sistema di conservazione a seguito dell'avvenuta accettazione di un pacchetto di versamento;
Pacchetto di versamento: pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel *Manuale* di conservazione;
Pacchetto informativo: contenitore che racchiude uno o più oggetti da conservare (documenti informatici, do-cumenti amministrativi informatici, documenti informatici rilevanti ai fini tributari, fascicoli informatici, aggre-gazioni 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;
Piano della sicurezza del sistema di gestione informatica dei documenti: documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza;
Piano di conservazione: strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;
Piano generale della sicurezza: documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza;
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;
Processo/servizio di marcatura temporale: è il processo/servizio che associa in modo affidabile un'informazione e un particolare momento, al fine di stabilire prove attendibili che indicano il momento in cui l'informazione esisteva;
Produttore: persona fisica o giuridica responsabile del contenuto del pacchetto di versamento identificato, nel caso di pubblica amministrazione, nella figura del 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;
Registrazione informatica: insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente;
Registro particolare: registro informatico specializzato per tipologia o per oggetto; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.;
Registro di protocollo: registro informatico della corrispondenza in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti;
Repertorio informatico: registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche che trattano il procedimento, ordinati secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica;
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi: dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;

Responsabile della conservazione: è l'AOB, nella persona fisica dallo stesso formalmente incaricata quale responsabile dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici depositati in conservazione nell'ambito della fornitura del servizio di conservazione in esterno;
Responsabile del Servizio di conservazione: è il soggetto contrattuale che opererà attraverso uno o più persone fisiche formalmente incaricate all'esecuzione dell'insieme delle attività finalizzate alla conservazione a norma dei documenti informatici nell'ambito della fornitura del servizio di conservazione all'AOB;
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;
Riferimento temporale: informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento;
Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse culturale;
Servizio di conservazione dei documenti: è il Servizio di conservazione dei documenti informatici fornito conservatore esterno che risponde all'esigenza di avere i documenti informatici dell'AOB (e più in generale delle amministrazioni pubbliche o soggetti privati che necessitino di tale servizio) conservati nel rispetto della normativa vigente; è il Servizio a cui sono affidati i documenti informatici del Cliente (AOB) per essere conservati in modo elettronico per un periodo di tempo specificato nel Contratto;
Sistema di classificazione: strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata;
Sistema di conservazione: insieme di hardware, software, politiche, procedure, linee guida, regolamenti interni, infrastrutture fisiche e organizzative, volto ad assicurare la conservazione elettronica dei documenti del Cliente almeno per il periodo di tempo specificato nel contratto di servizio di conservazione dei documenti in vigore. Detto sistema tratta i documenti informatici in conservazione in pacchetti informativi che si distinguono in: pacchetti di versamento, pacchetti di archiviazione e pacchetti di distribuzione;
Sistema di gestione informatica dei documenti: nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445 e s.m.i.; per i privati è il sistema che consente la tenuta di un documento informatico;
Staticità: caratteristica che indica 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;
Transazione informatica: particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati;
Testo unico: decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni;
Titolare del trattamento[1]: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della si-curezza;
Ufficio utente: riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico;
Utente: persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse;
Validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.
Versamento agli archivi di stato: operazione con cui il responsabile della conservazione di un'amministrazione statale effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della

documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali;

NORMATIVA E STANDARD DI RIFERIMENTO

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;
- DPR 11 febbraio 2005, n. 68 - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Circolare dell'Agenzia delle Entrate n. 36/E del 6 dicembre 2006 - Decreto ministeriale 23 gennaio 2004; Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui

al decreto legislativo n. 82 del 2005;

- Circolare MEF del 31 marzo 2014 n. 1/DF – circolare interpretativa del DECRETO 3 aprile 2013, n. 55 - Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244.
- 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.

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.

RUOLI E RESPONSABILITÀ

ruoli	nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile della Conservazione AOB	Giuliano Marras	Conservazione Sostitutiva	21/10/2015	Andrea Alimonda Ex delibera 1808/2015
Responsabile del servizio di conservazione	ARUBA PEC spa	1. Fatturazione Attiva 2. Fatturazione Passiva 3. Registro Protocollo informatico	12/01/2016 (firma digitale del contratto da parte del Commissario AOB)	
Responsabile Sicurezza dei sistemi per la conservazione	ARUBA PEC spa	1. Fatturazione Attiva 2. Fatturazione Passiva 3. Registro Protocollo informatico	12/01/2016 (firma digitale del contratto da parte del Commissario AOB)	
Responsabile funzione archivistica di conservazione	ARUBA PEC spa	1. Fatturazione Attiva 2. Fatturazione Passiva 3. Registro Protocollo informatico	12/01/2016 (firma digitale del contratto da parte del Commissario AOB)	
Responsabile trattamento dati personali	ARUBA PEC spa	1. Fatturazione Attiva 2. Fatturazione Passiva 3. Registro Protocollo informatico	12/01/2016 (firma digitale del contratto da parte del Commissario AOB)	
Responsabile sistemi informativi per la conservazione	ARUBA PEC Spa	1. Fatturazione Attiva 2. Fatturazione Passiva 3. Registro Protocollo informatico	12/01/2016 (firma digitale del contratto da parte del Commissario AOB)	
Responsabile sviluppo e manutenzione del sistema di conservazione	ARUBA PEC spa	1. Fatturazione Attiva 2. Fatturazione Passiva 3. Registro Protocollo informatico	12/01/2016 (firma digitale del contratto da parte del Commissario AOB)	

STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

Organigramma

Indicazione delle strutture organizzative coinvolte nel servizio di conservazione.

Affari Generali: AOB (Responsabile Conservazione)

Sistemi Informatici: AOB (Delegato Responsabile Conservazione)

Engineering Spa (affidatario fornitura progetto SiSar): elaborazione e trasmissione dei file in conservazione sostitutiva.

Aruba Pec Spa: (Responsabile Servizio Conservazione, Fatturazione e registro informatico Protocollo)

Strutture organizzative

Servizio di conservazione delle attività di fatturazione attiva e passiva e registro del protocollo mediante sottoscrizione contratto con data 12/01/2016 con ARUBA PEC SPA

- acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento: ARUBA PEC spa.
- Rapporti di versamento generati da Aruba Spa e notificati all'indirizzo PEC AOB: notifiche.conservazione@pec.aobrotzu.it.
- preparazione e trasmissione del pacchetto di archiviazione: Engineering Spa.
- Gestione del pacchetto di archiviazione trasmesso: Aruba Spa
- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta; ARUBA PEC
- scarto dei pacchetti di archiviazione; ARUBA PEC
- chiusura del servizio di conservazione (al termine di un contratto). Responsabile Conservazione, Delegato Responsabile.

- attività proprie di gestione dei sistemi informativi:
  - conduzione e manutenzione del sistema di conservazione; Aruba Pec
  - monitoraggio del sistema di conservazione; Aruba Pec
  - change management: Responsabile Conservazione e delegato.
  - verifica periodica di conformità a normativa e standard di riferimento: Responsabile

conservazione e Engineering

OGGETTI SOTTOPOSTI A CONSERVAZIONE

Tipo doc.	produttore	visualizzatore	formato del file	versione del formato	sistema operativo	riferimenti e licenza relativa scadenza
Fattura Attiva	AOB	Areas AMC	XML	1.1	/	/
Fattura Passiva	AOB	Areas AMC	XML	1.1	/	/
Registro Protocollo	AOB	Sistema Protocollo informatico SISAR	PDF - PDF/A, TIFF, JPG, Office Open XML (OOXML), Open Document Format, XML, TXT, Formati Messaggi di posta elettronica	/	/	/

Oggetti Conservati:

Pacchetto di versamento

AOB è Responsabile della produzione del pacchetto informativo (pacchetto di versamento) inviato poi dal produttore al sistema di conservazione secondo un formato predefinito

Pacchetto di archiviazione

E' un processo gestito dal Responsabile del Servizio di Conservazione. Al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'indice del pacchetto di archiviazione viene realizzata dal Responsabile del Servizio di Conservazione in conformità con quanto previsto dallo standard "Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali", (c.d. SInCRO), ossia

dalla norma UNI 11386 dell'ottobre 2010.

Pacchetto di distribuzione

L'AOB può richiedere la creazione di un pacchetto di distribuzione contenente il documento digitale o l'insieme dei documenti digitali, corredati da tutti o parte dei metadati previsti nel pacchetto di archiviazione. Nel modello OAIS e in linea con la normativa vigente, il pacchetto di distribuzione è strutturato nel modello dati come il pacchetto di archiviazione . Nel contenuto può anche non coincidere col pacchetto di archiviazione, se le circostanze lo richiedano.

IL PROCESSO DI CONSERVAZIONE

Descrizione generale delle diverse funzioni relative al processo di conservazione.

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

La ricezione e presa in carico di un pacchetto di versamento segue uno schema logico di funzionamento che si articola in due fasi distinte: ricezione dell'Indice del Pacchetto di Versamento (IPdV) e ricezione dei documenti che fanno parte del Pacchetto di Versamento (PdV).
L'uno e gli altri possono essere trasmessi al sistema di conservazione attraverso canali diversi.
Alternativamen-te essi possono essere:

- interfaccia web
- invocazione di metodi tramite web service REST
- invio in allegato a una mail PEC
- trasferimento via protocollo FTP

Ogni canale messo a disposizione è provvisto di opportuni accorgimenti per la trasmissione dei dati in modalità sicura:
l'interfaccia web viaggia su protocollo HTTPS

il web service REST è contattabile tramite protocollo HTTPS

la PEC nativamente garantisce autenticità della provenienza e notifica di consegna in modalità sicura

il server FTP è raggiungibile via SFTP

Per il completamento delle operazioni di conservazione di un PdV non è necessario scegliere esclusivamente uno dei canali sopra citati. La ricezione, anche in maniera asincrona, dei singoli componenti di un PdV possono arrivare anche da canali diversi.
Il sistema di conservazione si assume la responsabilità della presa in carico di un PdV solo dopo che tutte le sue parti (IPdV e relativi documenti) vengono correttamente ricevuti e superano con esito positivo i relativi control-li.
Tale operazione viene ufficialmente sancita dalla produzione del cosiddetto Rapporto di Versamento (RdV) che viene consegnato al cliente all'indirizzo PEC fornito nella fase contrattuale.

- Poichè la produzione del RdV rappresenta formalmente la presa in carico del PdV da parte del sistema di con-servazione, il RdV viene marcato temporalmente e firmato digitalmente direttamente o via delega dal Respon-sabile del Sistema di Conservazione.

controlli effettuati sui pacchetti di versamento e sugli oggetti in essi contenuti

Le funzionalità attivate nel processo di versamento/acquisizione del pacchetto di versamento prevedono dei controlli sia nella fase di ricezione dell'indice del PdV che sui singoli documenti inviati e corrispondenti a quanto previsto nell'indice stesso. La tabella riportata in basso elenca le diverse tipologie di controlli effettuati e per ognuna di esse indica l'azione prevista da sistema. Quest'ultima può tradursi in una operazione di scarto o noti-fica di un warning.
Controlli dell'indice del Pacchetto di versamento

Il deposito di un pacchetto di versamento e' distinto per ciascun lotto di documenti informatici omogenei (documenti omogenei, ossia aventi la stessa classe documentale). Pertanto, a classi documentali diverse corrispondono diversi PdV e versamenti, uno per ogni classe.

ID	Oggetto del controllo	Azione in caso di check negativo
Verifica Autorizzazioni		
1.01	viene verificato che l'utente che effettua il versamento sia abilitato all'invio dei Pdv	Il sistema scarta l'intero pacchetto
Verifica formale indice del PdV		
2.01	viene verificato che l'oggetto ricevuto sia formalmente un indice xml in linea con lo standard DocFly	Il sistema scarta l'intero pacchetto
2.02	viene verificato che il PdV è versato nei termini contrattuali e di servizio stabiliti col produttore	WARNING: Il sistema accetta il PdV ma non garantisce la conservazione nei termini concordati
Verifica presenza dati-documenti nell'indice del PdV		
3.01	viene verificato che l'indicazione del sistema di conservazione sia corretta	Il sistema scarta il PdV poiché il metadato contenuto nell'indice indica un sistema di conservazione diverso da DocFly
3.02	viene verificato che l'identificativo specificato nel Pdv non sia già presente nel sistema di conservazione	Il sistema verifica se il PdV (che contiene lo stesso ID) non sia già stato conservato. In questo caso il sistema considera il nuove indice in sostituzione del

		precedente. Viene invece scartato qualora il PdV risulta essere in stato 'conser-vato'.
3.04	viene effettuato un controllo semantico sui metadati presenti nell'indice del PdV	Il sistema scarta il PdV poiché uno o piu' metadati non rispettano il formato condivi-so nel contratti di servizio
3.05	viene controllato che per ciascun documento dichiarato e descritto all'interno dell'indice del Pdv: a. tutti i metadati minimi obbligatori siano presenti e nel formato corretto; b. il formato del documento è un formato ammesso c. l'estensione del documento sia tra quelle ammesse per il tipo documento; d. il formato dichiarato sia corrispondente all'estensio-ne del nome file	Il sistema scarta il PdV perché le verifiche formali sui documenti dichiarati nell'indice del PdV han-no avuto esito negativo
Verifiche Paternità		
4.01	viene verificato che il Pdv, nel caso abbia estensione P7M, sia firmato con certificato valido	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo
4.02	viene verificato che tutte le firme apposte al Pdv siano valide	Il sistema scarta il PdV perché le verifiche formali sui certificati di firma hanno avuto esito negativo

Controlli nella fase di ricezione dei documenti (files)

Controllo ricezione documenti

1.01	viene verificato che l'hash del documento informatico in-viato sia corrispondente all'hash dichiarato all'interno del medesimo indice del pacchetto al fine di avere garanzia che la trasmissione del pacchetto sia avvenuta corretta-mente e che l'integrità del documento informatico ricevu-to sia assicurata	Il sistema scarta il documento poi-ché non atteso
1.02	in caso di file P7M viene verificata la validità della firma apposta su ogni singolo documento: o Controllo di conformità. o Controllo Crittografico. o Controllo Catena Trusted. o Controllo Certificato. o Controllo CRL	Il sistema scarta il documento qua-lora il certificato di firma non sia valido WARNING: in caso di documenti firmati e il certificato di firma uti-lizzato e' prossimo alla scadenza, il sistema evidenzia un warning.
1.03	viene verificato che il documento sia leggibile	Il sistema scarta il documento nel caso questo non sia leggibile
1.02	viene verificato che il formato del documento informatico sia effettivamente valido e corrispondente a quanto di-chiarato nel pacchetto di versamento. In tal caso i control-li eseguiti variano in funzione del formato atteso per cia-scuno specifico documento.	Il sistema scarta il documento poi-ché il formato non e' quello atteso
1.03	viene verificato che i documenti ricevuti non siano già presenti nel sistema di conservazione;	WARNING: il documento viene ac-cettato e il sistema invia una noti-fica
1.04	viene verificato che la ricezione dei documenti si sia cor-rettamente conclusa entro la data limite di ricezione sta-bilita col produttore nel contratto di servizio	WARNING: il documento viene ac-cettato ma il sistema non garanti-sce la conservazione nei termini concordati

accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico:

Il sistema di conservazione predispone, per ciascun pacchetto di versamento, un **rapporto di versamento** che viene firmato dal Responsabile del Sistema di Conservazione.
In particolare il rapporto di versamento contiene, tra l'altro, le seguenti informazioni:

– identificativo unico del PdV, come indicato nel relativo IPdV
– identificativo unico del PdV fornito dal sistema di conservazione
– data di ricezione dell'IPdV
– per ogni documento accettato viene indicato:
- id univoco, come indicato nell'IPdV
- id univoco fornito dal sistema di conservazione
- hash
- data di ricezione
- esito della ricezione (accettato o warning)
- descrizione warning, ove necessario

rifiuto dei pacchetti di versamento e generazione del rapporto di versamento con evidenziazione delle anomalie

Il pacchetto può essere restituito al sistema versante con l'indicazione di eventuali anomalie. In tale caso il versamento viene considerato rifiutato e generato un rapporto contenente le indicazioni specifiche, come da paragrafo precedente.

preparazione e gestione del pacchetto di archiviazione

Il File di Chiusura è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualifica-ta, corroborata da una marca temporale.
La struttura del file di chiusura è costruita sulla base delle specifiche della struttura dati (UNI 11386:2010)

preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

L'AOB può richiedere la creazione di un pacchetto di distribuzione contenente il documento digitale o l'insieme dei documenti digitali, corredati da tutti o parte dei metadati previsti nel pacchetto di archiviazione. Nel modello OAIS e in linea con la normativa vigente, il pacchetto di distribuzione è strutturato nel modello dati come il pacchetto di archiviazione . La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione).
In questo caso, un PdD può anche non coincidere con il pacchetto di archiviazione originale conservato: anzi, molto spesso, ragioni di opportunità inducono a distribuire pacchetti informativi che sono un'estrazione del contenuto informativo di un PdA. Può anche verificarsi il caso di pacchetto di distribuzione che sono il frutto di più PdA che vengono "spacchettati" e reimpacchettati per un più fruibile utilizzo da parte dell'utente.
L'AOB, quindi, è in grado di interrogare il sistema per ricevere in uscita uno specifico pacchetto di distribuzione. L'AOB utilizzerà le funzionalità di richiesta di esibizione di un documento o di un insieme di documenti, per ottenerne una replica esatta secondo i fini previsti dalla norma.
In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema di conservazione risponderà resti-tuendo un PdD che nel caso più completo conterrà:
- Nome (ID) dei files/ documenti richiesti nel formato previsto per la loro visualizzazione e conetnuti nel pacchetto.
- Un'estrazione dei metadati associati ai documenti.
- L'indice di conservazione firmato e marcato dal Responsabile del Servizio di Conservazione o delegato.
- Indice del Pacchetto di Archiviazione di appartenenza (qualora richiesto)
- I viewer necessaria alla visualizzazione dei documenti del pacchetto

A fronte di una richiesta di produzione del pacchetto di distribuzione, il sistema effettua delle verifiche di coe-

renza e correttezza del pacchetto e dei documenti in esso contenuti. A tal proposito, il sistema di conservazione verifica che le impronte dei documenti restituiti nel PdD corrispondano a quelle presenti nel relativo indice del pacchetto di archiviazione; in modo da garantire che i documenti stessi non abbiano subito alterazioni o modi-fiche nei contenuti.

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

L'AOB può depositare in conservazione copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico, a propria cura e spese, e predisporrà quanto necessario per ottemperare a quanto previsto dalle richiamate disposizioni.
In particolare, sarà cura e carico dell'AOB:
a) produrre la copia per immagine su supporto informatico del documento analogico mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto;

successivamente:
b) (ai fini di quanto stabilito dall'articolo 22, co. 3, del CAD), dovrà sottoscrivere con firma digitale la copia per immagine del documento analogico;

oppure
c) laddove richiesto dalla natura dell'attività, (art. 22, comma 2, del CAD), dovrà inserire nel documento informatico contenente la copia per immagine, l'attestazione di conformità all'originale analogico. Il documento informatico così formato dovrà poi essere sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata di pubblico ufficiale a ciò autorizzato.

Se richiesta la presenza del PU, le spese saranno a carico dell'AOB. In ogni caso il Responsabile del Servizio di conservazione darà tutto il supporto tecnico necessario.

scarto dei pacchetti di archiviazione:

Alla scadenza dei termini di conservazione, l'AOB riceverà una notifica via PEC dal sistema di conservazione e in autonomia potrà decidere di eliminare i documenti conservati attraverso le funzionalità previste dal sistema di conservazione.

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

al fine di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, la struttura dell'indice del pacchetto di archiviazione viene realizzata dal Responsabile del Servizio di Conservazoine in conformità con quanto previsto dallo standard *"Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali"*, (c.d. SInCRO), ossia dalla norma UNI 11386 dell'ottobre 2010.
I pacchetti di archiviazione generati dal sistema di conservazione vengono trattati al solo scopo di soddisfare i requisiti della conservazione digitale dei documenti ed al soddisfacimento delle richieste di produzione di pachetti di distribuzione e di esibizione.
Il soddisfacimento dei requisiti della conservazione digitale implica che i pacchetti di archiviazione vengano firmati digitalmente dal responsabile del sistema di conservazione o da un suo delegato e marcati temporalmente per assicurarne la validità nel corso del tempo.
La produzione di pacchetti di distribuzione o l'esibizione di pacchetti di archiviazione comporta invece la

produzione di duplicati degli stessi che sono successivamente utilizzati nei processi. Il pacchetto di archiviazione memorizzato all'interno del sistema non subisce più alcuna modifica successiva alla firma digitale e all'apposizione della marca temporale.

IL SISTEMA DI CONSERVAZIONE

Il processo di conservazione si articola nelle seguenti fasi: **FASE 1**	**Acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico**
Descrizione sintetica	Consiste nella ricezione dell'IPdV
FASE 2	Verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previ-ste nel presente Manuale di conservazione e con i formati di conservazione
Descrizione sintetica	In questa fase vengono condotti i controlli sull'IPdV
FASE 3	Preparazione del rapporto di conferma
Descrizione sintetica	A seconda dell'esito del controllo sull'IPdV viene prodotto un rapporto di conferma che viene restituito al sistema versante. NOTA BENE: il rapporto di conferma non implica la presa in carico del versamento da parte del sistema
FASE 4	Eventuale rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla FASE 2 abbiano evidenziato anomalie e/o non conformità
Descrizione sintetica	Alternativamente alla fase 3 viene restituito al sistema versante l'indicazione di eventuali anomalie. In tale caso il versamento viene rifiutato
FASE 5	Ricezione dei documenti
Descrizione sintetica	Il sistema si mette in attesa dei documenti del PdV
FASE 6	Verifica dei documenti
Descrizione sintetica	In questa fase vengono condotti i controlli specifici del documento ricevuto
FASE 7	Generazione automatica del rapporto di versamento relativo a ciascun pacchetto di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità di seguito descritte
Descrizione sintetica	Una volta ricevuti correttamente, o con warning, tutti i documenti del PdV viene pro-dotto il PdV
FASE 8	Sottoscrizione del rapporto di versamento con firma digitale apposta da ARUBA

Descrizione sintetica	Il RdV viene firmato digitalmente dal Responsabile del Sistema di Conservazione o da un suo delegato. Infine il RdV viene inviato all'AoB via email PEC. In questa fase Aruba Pec prende in carico il versamento ufficialmente
FASE 9	Preparazione e gestione del pacchetto di archiviazione (c.d. File di chiusura)
Descrizione sintetica	Il File di Chiusura è un insieme di metadati in grado di fornire prova dell'integrità dell'insieme dei documenti, ad esso correlati la cui conservazione decorre da una data determinata, la cui prova di integrità è fornita tramite una firma elettronica qualifica-ta, corroborata da una marca temporale. La struttura del file di chiusura è costruita sulla base delle specifiche della struttura dati (UNI 11386:2010) contenute nell'allegato 4 alle regole tecniche e secondo le mo-dalità riportate nel manuale della conservazione
FASE 10	Sottoscrizione del pacchetto di archiviazione con firma digitale apposta da ARUBA e apposizione di una validazione temporale con marca temporale alla relativa impronta. Tale operazione viene in breve chiamata anche "Chiusura del pacchetto di archiviazione"
Descrizione sintetica	Il Pacchetto di Archiviazione (PdA), che viene costruito dal versamento di uno o più PdV, viene "chiuso" nel momento in cui tutti i PdV sono stati presi in carico dal siste-ma. La chiusura viene sancita dall'apposizione di opportuna marca temporale, per stabilirne l'istante di creazione, e firma digitale del Responsabile del Sistema di Con-servazione o di un suo delegato, per garantirne l'immodificabilità. Con la suddetta firma apposta in calce al file di chiusura e la suddetta dichiarazione il conservatore NON SOTTOSCRIVE il contenuto e la semantica dei documenti conservati ma asserisce solamente che il processo di conservazione è stato eseguito correttamente, nel ri-spetto delle norme giuridiche e delle indicazioni contrattuali di servizio.
FASE 11	Preparazione e sottoscrizione con firma digitale di ARUBA del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente
Descrizione sintetica	Il pacchetto di distribuzione (PdD) è definito in base alle esigenze del richiedente e può contenere anche un set parziale di metadati. È generato a partire dai pacchetti di archiviazione. Nel caso più semplice il PdD contiene dei duplicati del PdA. In alternativa esso può essere costituito da una scelta di documenti conservati selezionati attraverso una o più interrogazioni. I risultati di tali ricerche possono essere raccolti in un'area di lavoro e da qui può essere prodotto il PdD voluto.
FASE 12	Produzione di duplicati informatici effettuati su

	richiesta del Cliente in conformità a quanto previ-sto dalle regole tecniche in materia di formazione del documento informatico
Descrizione sintetica	Per duplicato informatico si intende il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima se-quenza di valori binari del documento originario. I duplicati informatici hanno il me-desimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche in materia di formazione del documento informatico, ovvero se contiene la stessa sequenza di bit del documento informatico di origine.
FASE 13	Eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei ter-mini di conservazione previsti dal Contratto di servizio, dandone preventiva informativa al Cliente al fine di raccoglierne il consenso
Descrizione sintetica	Alla scadenza dei termini di conservazione, il cliente in autonomia puo' decidere di cancellar ei documenti in conservazione.

Componenti logiche

Sicurezza Logica dei sistemi e degli apparati

I protocolli ed i servizi utilizzati per la gestione degli apparati (SNMP, RADIUS, NTP, Log, LDAP) vengono erogati solo verso le reti di management mediante l'utilizzo di ACL (Access Control List). All'interno delle reti dedicate, se il protocollo/servizio lo supporta, è in ogni caso necessario autenticarsi.
Tutti i protocolli previsti per l'accesso ed il controllo dei sistemi sono di tipo sicuro cifrato, prevedendo ssh, https o rdp.
All'interno dei singoli apparati i servizi non necessari vengono disattivati e quelli necessari vengono erogati solo verso le interfacce che richiedono che tali servizi vengano resi disponibili.
Le politiche e le conseguenti architetture e configurazioni di rete adottate garantiscono fra l'altro:

- L'impossibilità di effettuare IP spoofing da un qualsiasi utente connesso direttamente alla rete
- L'impossibilità di effettuare attacchi smurf, fraggle, land tramite limitazione nell'accesso agli indirizzi di broadcast e filtraggio dei pacchetti che riportano un indirizzo sorgente palesemente scorretto
- La capacità di reagire tempestivamente a qualsiasi tipo di attacco alle proprie infrastrutture anche tramite la possibilità di configurare in qualsiasi punto della rete qualsiasi regola di filtraggio atta a mitigare il fenomeno evidenziato

L'autorizzazione all'accesso alla configurazione di un apparato è nominale, non di gruppo. L'accesso ad una specifica classe d'apparati dipende dall'appartenenza dell'utente ad uno specifico gruppo. L'associazione dell'utenza al Gruppo permette di confinare l'accesso degli utenti ai soli apparati la cui gestione è in carico al Gruppo. Sulla base di tale appartenenza, L'AOB potrà autenticarsi sull'apparato utilizzando una login ed una password personali nel caso di apparati con tecnologia IP mentre per quanto riguarda apparati di trasporto (SDH e DWDM) l'autenticazione si esegue a livello dei sistemi di gestione. Sono stati inoltre introdotti dei meccanismi di gestione delle password (lunghezza minima, presenza di caratteri numerici, ecc.) di enable e

delle password locali in modo da ottenere un bilanciamento tra l'esigenza di avere un adegua-to livello di sicurezza e le esigenze di implementazione/gestione delle linee guida.
L'inserimento di un nuovo utente in un gruppo deve essere richiesto dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di Trasporto. Successivamente alla configurazione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al respon-sabile del gruppo. La rimozione di un utente da un gruppo deve essere richiesta dal responsabile del gruppo stesso. La richiesta deve pervenire via e-mail all'apposita casella di posta nel caso della rete IP o all'amministratore di rete nel caso di accesso agli apparati di rete di trasporto.
Successivamente alla rimozione dell'utente, sarà inviata e-mail di conferma all'utente stesso ed al responsabile del gruppo. Le password utilizzate dagli utenti dovranno seguire le seguenti regole:

- Non inferiori agli 8 caratteri (in accordo con la legge delega 127/2001 Allegato B comma 7)
- Non devono essere facilmente indovinabili. Nomi propri, nomi di prodotti, nomi di Clienti ecc.. sono da evitare
- Devono contenere caratteri misti: minuscole, maiuscole, numeri, spazi, caratteri speciali (@, %, $ ecc.)
- Non devono coincidere con le password utilizzate per altri servizi di rete.

L'utente viene invitato a cambiare con regolarità la sua password utente. Nel caso l'utente decidesse di non cambiare la propria password vengono adottate le seguenti misure:

- Trascorsi due mesi, dall'ultimo cambio di password effettuato, l'utente riceverà dei solleciti settimanali per cambiare.

Architettura Logica

Articolata su tre livelli

- **Presentation layer**: L'applicazione è pensata per essere scalabile, aumentando il numero dei Web container attraverso una logica di server clustering, gestita automaticamente dal sistema, che, a seconda del livello di carico di ciascun server, distribuirà al meglio le richieste dei client

- **Business logic (o application) layer**: La Business Logic implementa l'intelligenza necessaria per gestire le varie istanze di Alfresco sia in scrittura, duplicando l'informazione su almeno due di esse, sia in fase di ricerca, distribuendo le query sulle varie istanze disponibili. Tutte le istanze Alfresco sono sempre disponibili almeno in lettura

- **Store (& Database) layer**: la parte di back end è composta da diverse coppie di istanze di Alfresco. Ogni istanza è costituita dal DB e dal relativo file system. Il DB è duplicato in modalità Master-Master su due nodi predisposti sull'ambiente virtuale e contiene i metadati conservati; il FS contiene l'archivio (dati conservati) e non necessita di replica in quanto il dato viene scritto sempre su almeno due istanze (replica applicativa). Ognuna delle istanze è quindi replicata a livello applicativo e tale replica garantisce sia la salvaguardia delle informazioni trattate sia la continuità operativa in consultazione, qualora uno dei due nodi "gemelli" non dovesse essere disponibile.

Componenti fisiche: architettura

La soluzione è composta da due infrastrutture fra loro interconnesse:

- un sito di Produzione completamente autosufficiente e con tutte le componenti ridondate in HA e collegato tramite fibre ottiche dedicate e di proprietà, con doppia via, al sito secondario,
- un sito Secondario di DR predisposto alla replica dei dati e con le componenti necessarie ad una ripartenza del servizio.

Tutte le componenti utilizzate sono di tipologia enterprise e, come tutte le soluzioni implementate dal responsabile del servizio, utilizzano prodotti di marche ampliamente riconosciute e leader del meracto di riferimento.

Il sito di produzione ospita una infrastruttura virtuale basata su soluzione VMware sul quale vengono istallati:
- i nodi di Front-End (almeno due) per le interfacce di caricamento, esibizione e gestione,
- gli Application o Business Logic server (almeno due),
- le istanze della soluzione documentale Alfresco, un singolo nodo per ogni istanza,
- un nodo virtuale dedicato al DB server MSQL di ogni istanza Alfresco, la seconda copia in Master-Master è installata sul sito secondario,
- un nodo virtuale per la gestione delle code del sistema di caricamento,
- un nodo virtuale che implementa il DB MySQl che contiene tutte le informazioni per la gestione dell'infrastruttura (configurazione, accounting, etc.), la seconda copia in Master-Master è installata sul sito secondario,
- Storage di livello enterprise per l'archiviazione dei documenti;
- Link ed interfacce verso i sistemi di Firma e Marcatura presenti nel medesimo data Center

La figura sottostante schematizza quanto implementato sul sito principale senza entrare nelle specifiche moda-lità di replica.
Al fine di garantire i ridondanza e bilanciamento del traffico vengono utilizzati dispositivi di load balancing in grado di distribuire il carico di lavoro su un numero di macchine virtualmente illimitato. Questo meccanismo permette di risolvere oltre a problemi prestazionali con la semplice aggiunta a caldo di nuove macchine, anche problemi relativi ad eventuali guasti delle componenti bilanciate, nonché la manutenzione programmata dei singoli nodi.

MONITORAGGIO E CONTROLLI

- Funzioni di monitoraggio complessivo sulle operazioni pianificate
- Sistema di log ed errori
- Invio di email
- Sistema di tracciamento con revisioni
- Controllo dei server

Procedure di monitoraggio della funzionalità del sistema di conservazione

Il Responsabile del Servizio di Conservazione assicura la verifica periodica del funzionamento, nel tempo, del sistema di conservazione.
Il controllo della buona funzionalità del sistema di conservazione avviene tramite apposite funzionalità di monitoraggio del software. Esse mostrano l'esito delle operazioni automatiche eseguite sul sistema di conservazione come la generazione dei pacchetti di archiviazione, la chiusura dei pacchetti di archiviazione e la verifica dell'integrità degli archivi.
Unitamente all'esito delle predette operazioni vengono controllati anche i log delle operazioni medesime al fine di avere maggiore certezza di quanto effettivamente eseguito dal sistema di conservazione. Tutte queste informazioni sono controllate per ciascun singolo cliente.
Il monitoraggio avviene inoltre anche a livello di processi di elaborazione sul sistema di conservazione. Questo permette di individuare eventuali casi di processi bloccati che potrebbero inficiare il funzionamento del sistema stesso.
Un ultimo controllo del buon funzionamento del sistema può avvenire tramite il monitoraggio delle tracciature che vengono effettuate a livello di database. Tutte le operazioni eseguite determinano infatti la creazione di apposite revisioni che registrano tutte le modifiche intervenute sul sistema permettendo eventualmente di ri-pristinare i dati a seguito di situazioni anomale.

Verifiche sull'integrità degli archivi

Il Responsabile del Servizio di Conservazione assicura la verifica periodica, **con cadenza non superiore all'anno**, dell'integrità degli archivi e della leg-gibilità degli stessi; assicura, inoltre, agli organismi competenti previsti dalle norme vigenti l'assistenza e le ri-sorse necessarie per l'espletamento delle attività di verifica e di vigilanza.
Il sistema di conservazione esegue periodicamente ed automaticamente le operazioni di controllo dell'integrità degli archivi. Tali operazioni vengono eseguite solo su una certa percentuale dell'archivio che viene definita nella configurazione del sistema di conservazione.
Il controllo eseguito è di due tipologie:
- **controllo di leggibilità:** consiste nel verificare che i singoli bit degli oggetti siano tutti correttamente leggibili. Questo fornisce garanzia del buono stato del supporto di memorizzazione.

- **controllo di integrità:** consiste nel ricalcolare l'hash di ciascun oggetto e verificare che corrisponda all'hash memorizzato nel sistema. Questo fornisce una ragionevole certezza dell'integrità degli oggetti dato che la funzione di hash restituisce un valore differente anche a seguito della modifica di un solo bit dell'oggetto.

La combinazione dei due tipi di controllo descritti non fornisce però garanzia di poter visualizzare correttamen-te il documento e che lo stesso sia effettivamente intellegibile dall'uomo.
Infatti questa garanzia non può essere fornita senza entrare nel merito del documento stesso. La garanzia della corretta visualizzazione del documento è d'altro canto garantita dalla scelta del formato PDF/A per i documenti conservati. Questo formato possiede infatti la caratteristica intrinseca di fornire leggibilità a lungo termine oltre all'ulteriore garanzia di essere basato su specifiche pubbliche (ISO 19005-2005).

Pianificazione delle verifiche periodiche da effettuare

Il controllo periodico dell'integrità degli archivi avviene con una frequenza di una volta al mese.

Mantenimento della firma per il periodo di conservazione

Il sistema di conservazione si avvale di un fornitore terzo (Certificatore accreditato) per le attività di firma digitale e di marcatura temporale. Questo fornitore garantisce che gli elaboratori che offrono il servizio di marcatu-ra temporale e di firma digitale sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema garantisce gli elaboratori dalla possibilità di compromissioni fisiche

grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali. Non è infatti consentito l'accesso e la permanenza di una sola persona. I locali ove si svolgono le procedure di firma e marca sono dotati di sofisticati impianti di allarme, telecamere, microfoni, rilevatori di movimento (che si attivano soltanto quando nessuna persona vi è presente), al fine di controllare ogni movimento all'interno degli stessi.