MANUALE DI CONSERVAZIONE

DI BBBELL S.p.A.

Redatto	M. Bazzi		**BBBELL S.p.A.**
Validato	E. Boccardo	18/03/2016	**BBBELL S.P.A.** **Presidente**
	M. Bazzi		**BBBELL S.P.A.** **Responsabile servizio di conservazione**
	N. Savino		**Responsabile funzione archivistica**
	N. Savino		**Responsabile dello sviluppo e della Manutenzione del sistema di conservazione**
Verificato	S.Salvati		**BBBELL S.P.A.** **Responsabile Servizi Informativi**

Ed. 03	Rev. 02	Data edizione: 14/11/2019 Data revisione: 26/02/2021

DISTRIBUZIONE		
DA	**A**	**Firma**
RGQS e Sicurezza Dati (RGQSS)	**DIREZIONE GENERALE**	
	ENTE DI CERTIFICAZIONE	

COPIA NON CONTROLLATA	

INDICE DELLE REVISIONI

N°	DATA	DESCRIZIONE	Paragrafi variati	Pagine variate
Ed. 01	21/09/2016	Redazione iniziale	Tutti	Tutte
Ed. 02	16/08/2017	Riedizione totale	Tutti	Tutte
Rev 01	31/10/2017	Correzioni a seguito verifica Rina	3 4.2 4.3 5.1 5.2 7.2 7.3 9	12 14 15 17 e 18 19 31 31 e 33 39
Rev 02	01/02/2018	Correzioni a seguito osservazioni AgID (inserimento “Torna al sommario” - inserimento didascalie e indice figure – precisazioni varie)	Tutti	Tutte
Rev 03	10/09/2018	Aggiornato ragione sociale Savino Solution	4.3 6 7.4.4	16 24 37
Ed. 03	19/11/2019	Aggiornamento totale con allineamento S.S.	Tutti	Tutte
Rev 02	26/02/2021	Correzioni a seguito di verifica Rina e controllo generale	Tutti	Tutte

RESPONSABILITA'

FUNZIONE	EMISSIONE E DISTRIBUZIONE	VERIFICA E APPROVAZIONE
	RGQSS	Direzione Generale
NOME	Maurizio Bazzi	Enrico Boccardo
FIRMA		

SOMMARIO

INDICE DELLE FIGURE

SCOPO E AMBITO DEL DOCUMENTO

Il presente documento, redatto in conformità dell'art. 8 del D.P.C.M. del 3 dicembre del 2013, costituisce il Manuale del sistema di conservazione di BBBELL, nel quale sono descritti:
Il modello organizzativo;
i ruoli e le responsabilità;
i processi e le procedure;
l'architettura logica e fisica del suo sistema di conservazione.

Lo scopo del documento è quello di fornire ai soggetti pubblici e privati, le informazioni adeguate a conoscere i requisiti organizzativi, di processo, architetturali, funzionali e di sicurezza, in conformità ai quali BBBELL eroga il servizio di conservazione al livello più elevato in termini di qualità e sicurezza.

Si evidenzia che il servizio è erogato nel DC BBBELL, nel rispetto dei requisiti di continuità, sicurezza fisica e logica, back-up, monitoraggio, presidio operativo, sistemistico, infrastrutture logistiche e gestione reti dati che il Data Center garantisce e descrive negli specifici documenti.

Il DC è certificato ISO 27001 con estensione ai controlli ISO 27017 e 27018.

Torna al sommario

1. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

1.1 Glossario

Termini	Definizioni
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
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
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
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
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, **dall'Agenzia per l'Italia digitale,** il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, **dall'Agenzia per l'Italia digitale**
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Copia di sicurezza	Copia di *backup* degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione

Termini	Definizioni
Documento informatico	il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (Regolamento 910/2014)
Firma elettronica avanzata	Una firma elettronica che soddisfi i requisiti di cui all'articolo 26, ovvero a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati. (Regolamento 910/2014)
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (Regolamento 910/2014)
Firma digitale	Un particolare tipo di firma elettronica qualificata basata 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
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Immodificabilità	caratteristica che rende il contenuto del 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
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

Termini	Definizioni
	documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Marca temporale	è il risultato di una procedura informatica – detta servizio di marcatura temporale – grazie alla quale si attribuisce a un documento informatico un riferimento temporale opponibile a terzi.
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
Pacchetto di archiviazione (PdA)	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le modalità riportate nel manuale di conservazione
Pacchetto di distribuzione (PdD)	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento (PdV)	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
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
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 7, comma 1 delle regole tecniche del sistema di conservazione. (definizione dell'allegato I – glossario del DPCM 3 dicembre in materia di sistemi di conservazione.) Nelle pubbliche amministrazioni è la persona fisica presente all'interno dell'amministrazione.
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	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza

Termini	Definizioni
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
Unità di archiviazione	L'unità atomica inviata dal produttore per la conservazione, cioè un documento o un fascicolo
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

Torna al sommario

1.2 Acronimi

Acronimi	Definizioni
AgID	Agenzia per l'Italia Digitale
CA	Certification Authority
FTP server	Programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
IdP	strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utente all'interno di un ambito di sicurezza.
PdV	Pacchetto di Versamento
PdA	Pacchetto di Acquisizione
PdD	Pacchetto di Distribuzione
OAIS	ISO 14721:2012; Space Data information transfer system
ETSI	European Telecommunications Standards Institute

Torna al sommario

2. NORMATIVA E STANDARD DI RIFERIMENTO

2.1 Normativa di riferimento

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- Decreto del Presidente del Consiglio dei Ministri 13 novembre del 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 ammirazioni ai sensi degli art. 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. 82/2005.
- Codice dell'Amministrazione digitale D.lgs. 217/2017 s.m.i.
- Regolamento (UE) n. 910/2014 (eIDAS: electronic IDentification Authentication and Signature) del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
- Regolamento UE 679/2016 (GDPR)

Torna al sommario

2.2 Standard di riferimento

Nella definizione del contesto normativo tramite il quale regolamentare l'operato dei conservatori, il legislatore ha provveduto ad identificare un set di standard tecnologici di valenza internazionale a cui riferirsi, sia al fine di recepire le ricerche e gli studi effettuati a livello internazionale sull'argomento, sia al fine di definire un percorso che permetta agli operatori Italiani di rispondere in maniera proattiva alla nascente normativa europea. Segue, quindi, l'attuale scenario tecnologico a cui BBBELL si attiene, nell'ambito del servizio di conservazione:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management

systems – Requirements, Requisiti di un ISMS (Information Security Management System);

- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- ISO 15489 -1:2004 Information and documentation – Records Management – part 1: General

Torna al sommario

3. RUOLI E RESPONSABILITÀ

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali deleghe
Responsabile del servizio di conservazione	Maurizio Bazzi	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; - monitoraggio della 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	Da agosto 2012	nessuna
Responsabile Sicurezza dei sistemi per la conservazione	Maurizio Bazzi	Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Da agosto 2012	nessuna
Responsabile funzione archivistica di conservazione	Nicola Savino	- Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del	Per BBBELL dal 18/03/2016 Per altri clienti dal 2009	nessuna

		trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.		
Responsabile trattamento dati personali	Salvatore Salvati	- 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 giugno 2002	nessuna
Responsabile sistemi informativi per la conservazione	Salvatore Salvati	. Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; . monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; - 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 giugno 2002	nessuna
Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Savino	- 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.	Per BBBELL dal 18/03/2016 Per altri clienti dal 2009	nessuna

Torna al sommario

4. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

4.1 Premessa

Nata nel 2003 a Torino, BBBell è un operatore di telecomunicazioni (principalmente wireless) specializzato nei servizi avanzati di telefonia e connettività Internet a banda ultra larga realizzati con tecnologia radio, alternative e indipendenti rispetto alle tradizionali reti in rame e alla fibra. Attualmente il sistema di infrastrutture radio di proprietà di BBBell copre capillarmente il nord ovest d'Italia.

Nel 2015 ha ottenuto la certificazione ISO27001 relativamente ai servizi erogati tramite il proprio Data Center.

Tra la fine del 2016 e l'inizio del 2017 BBBELL ha implementato il proprio sistema di Conservazione a norma.

Torna al sommario

4.2 Organigramma

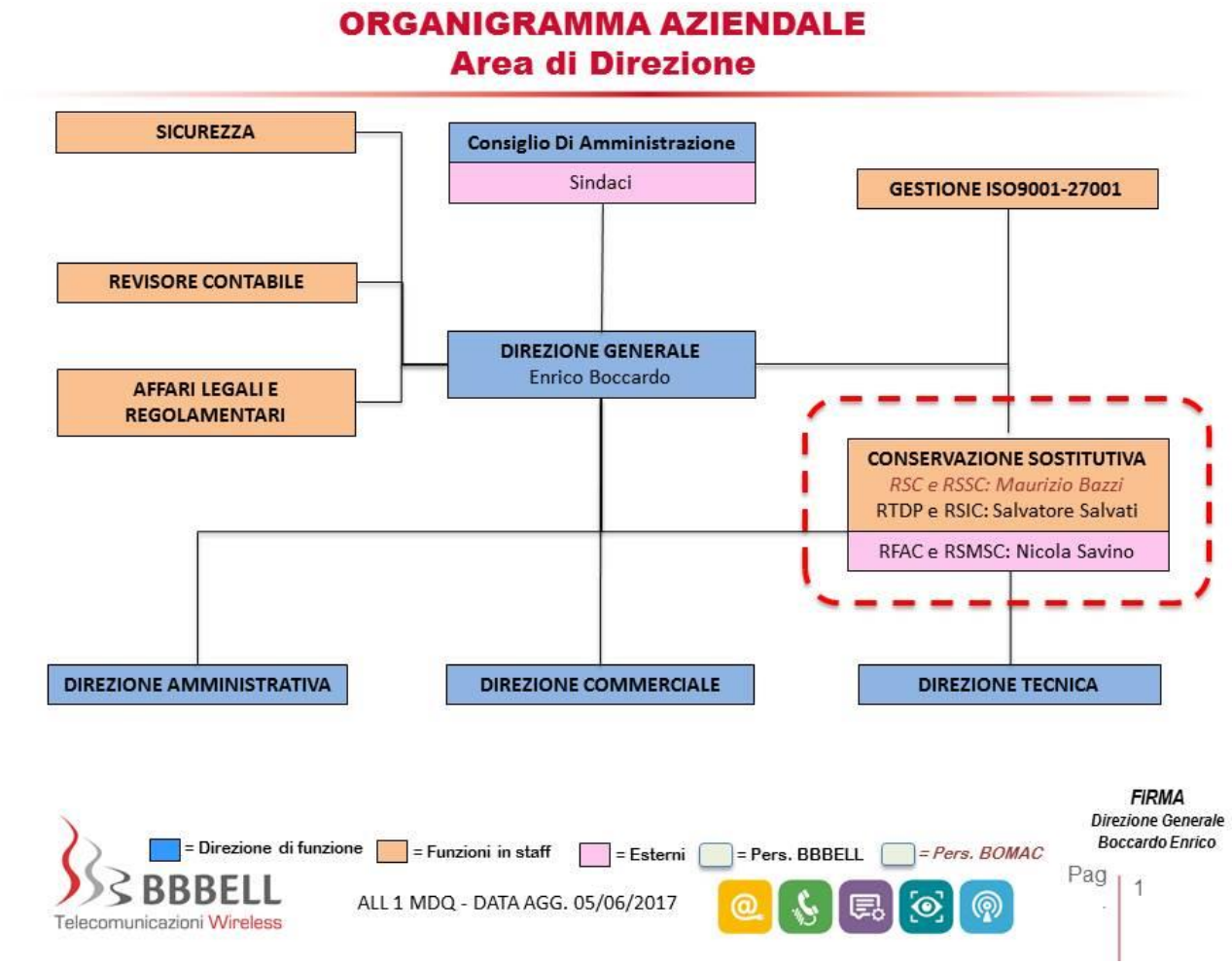


Figura 1- Organigramma Area di Direzione

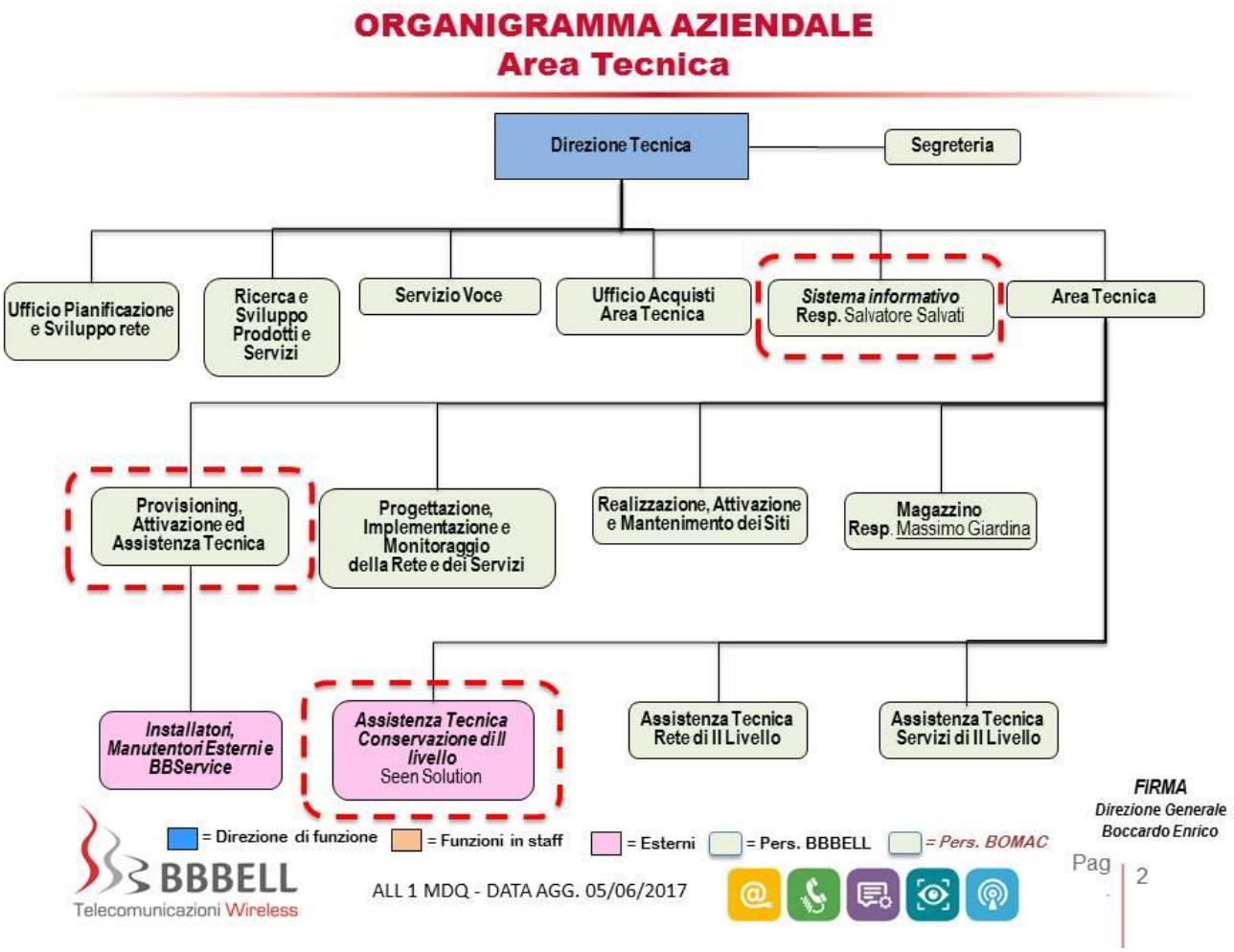


Figura 2 - Organigramma Area Tecnica

Torna al sommario

4.3 Strutture organizzative

Tutte le attività e le operatività inerenti il processo di conservazione, rispondente alle norme vigenti come indicate in premessa, vengono elencate nel presente manuale dal Responsabile del servizio di conservazione, all'interno del quale vengono riportate tutte le figure professionali richieste da AGID:

RSC Responsabile del servizio di conservazione **Maurizio Bazzi**				
RSSC Responsabile Sicurezza dei sistemi per la conservazione **Maurizio Bazzi**	**RFA** Responsabile funzione archivistica di conservazione **Nicola Savino**	**RTDP** Responsabile trattamento dati personali **Salvatore Salvati**	**RSIC** Responsabile sistemi informativi per la conservazione **Salvatore Salvati**	**RSMSC** Resp. sviluppo e manutenzione del sistema di conservazione **Nicola Savino**

Vengono descritte nel seguito le strutture organizzative, comprese le responsabilità, che intervengono nelle principali funzioni che riguardano il servizio di conservazione, quali:

Attività proprie di ciascun contratto di servizio di conservazione:

Queste attività, sotto il coordinamento del RSC, vengono condotte dal personale di vendita di BBBell attraverso il Contratto con il Cliente/Produttore.

Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto);

Questa attività, sotto il coordinamento del RSC, viene eseguita dal Provisioning che opera direttamente sui sistemi, predisponendo le attività per avviare il Contratto.

Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento;

Il Cliente/Produttore invia il Pacchetto di Versamento, contenente i documenti oggetti di conservazione ed il sistema produce il rapporto di versamento. Tale attività è eseguita sotto la responsabilità del RSC e del RSIC, che verificano l'eventuale presenza di alert bloccanti da parte del sistema di conservazione e provvedono alla corretta gestione/produzione del PDV.

Preparazione e gestione del pacchetto di archiviazione;

Questa attività viene svolta dal RSC, che verifica l'eventuale presenza di alert bloccanti da parte del sistema di conservazione e provvede alla risoluzione per la corretta gestione/produzione del PDA.

Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta;

Questa attività viene svolta dal Cliente/Produttore attraverso la funzionalità garantita ed offerta dal sistema di conservazione. Eventuali errori nella produzione del PDD, vengono immediatamente notificati al RSC e al RSIC, che provvedono alla risoluzione per la corretta gestione/produzione del PDD.

Scarto dei pacchetti di archiviazione;

Questa attività è sotto la responsabilità del RSC secondo quanto indicato nel paragrafo 6.8.

Chiusura del servizio di conservazione (al termine di un contratto).

Questa attività, sotto il coordinamento del RSC, viene eseguita dal Provisioning che opera direttamente sui sistemi, predisponendo le attività per chiudere il Contratto compresa la fornitura al Cliente/Produttore del PDD e il supporto informatico per il riversamento presso altro Conservatore(Interoperabilità).

Attività proprie di gestione dei sistemi informativi:

Questa attività viene svolta dalle risorse dei Sistemi Informativi sotto il coordinamento e responsabilità del RSIC.

Conduzione e manutenzione del sistema di conservazione;

Questa attività viene svolta dalle risorse di secondo livello di Savino Solution sotto il coordinamento e responsabilità del RSMSC.

Monitoraggio del sistema di conservazione;

Questa attività viene svolta dalle risorse dei Sistemi Informativi sotto il coordinamento e responsabilità del RSIC.

Change Management;

Questa attività viene svolta dalle risorse dei sistemi informativi e dalle risorse di secondo livello di Savino Solution sotto il coordinamento e responsabilità del RSIC e del RSMSC.

Verifica periodica di conformità a normativa e standard di riferimento.

Questa attività, sotto la responsabilità del RSC, viene svolta di concerto dal RSC stesso e dal RFA.

Torna al sommario

4.4 Aggiornamento professionale

Il personale coinvolto nel servizio viene istruito su:
le specificità tecniche e di sicurezza (vulnerabilità e minacce e relative contromisure adottate) dei sistemi/impianti da prendere in carico, anche attraverso opportuni manuali di gestione-amministrazione;
il corretto utilizzo dei sistemi IT impiegati a supporto dell'attività quotidiana (e-mail, software ecc..);
la generazione e la gestione delle password;
la responsabilità ed il ruolo;
il tracciamento delle attività.
Regole tecniche in materia di sistema di conservazione (dpcm 3 dicembre 2013 e successivi) e aspetti di sicurezza tipici di un progetto di conservazione digitale ovvero le contromisure che garantiscono autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici, come previsto dal CAD (art.44).

Sono inoltre previsti periodici piani di training e sessioni dedicate agli aspetti della sicurezza delle informazioni con particolare riguardo agli aspetti della conservazione.

La direzione Risorse Umane gestisce operativamente la formazione al termine del processo di rilevazione dei fabbisogni riportati nel Piano dei fabbisogni formativi.

Per il personale appartenente al servizio di conservazione sono previste:
sessioni di formazione ove si tratti di personale in nuovo ingresso
aggiornamento professionale, per tutto il personale interessato, a seguito di modifiche a norme e/o funzionalità e/o processi gestionali, e/o requisiti di sicurezza

Torna al sommario

5. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Gli oggetti oggetto di conservazione possono essere distinti:
Documenti informatici e documenti amministrativi informatici prodotti dal cliente con metadati associati a seconda delle tipologie documentali oggetto di conservazione;
Fascicoli informatici: aggregazione di più documenti informatici con metadati associati a seconda sia della tipologia del fascicolo sia dei documenti

Torna al sommario

5.1 Oggetti conservati

I formati più comuni gestiti sono riassunti nella tabella sottostante:

Tipo File	Visualizzatore
XML	Mozilla - Chrome - Internet Explorer Altri Browser.
TIFF	Image/tiff
P7M	Software specifico per la verifica delle firme digitali e per la visualizzazione dei relativi file (p.e Dike)
PDF	Adobe Reader
PDF(PADES)	Adobe Reader
XML(XADES)	Mozilla - Chrome - Internet Explorer Altri Browser

Tutti i documenti portati in conservazione sono trattati dal sistema in forma di pacchetti informativi, come di seguito definiti:
Pacchetto di versamento (PdV)
Pacchetto di archiviazione (PdA)
Pacchetto di distribuzione (PdD)

Per ogni singolo cliente, “nella specificità del contratto” vengono definiti:
L’elenco dei documenti conservati, i formati e la loro natura;
Il formato del PdV e le modalità di versamento nel SdC da parte del Produttore;
l’elenco e la descrizioni di eventuali metadati specifici associati ai documenti;
il periodo di conservazione e le modalità di scarto dei PdA;
qualsiasi altra informazione ritenuta utile a definire e regolamentare lo specifico processo di conservazione.

I formati dei documenti gestiti per il sistema di conservazione sono quelli all’Allegato 2 delle Regole tecniche di

cui al punto 5.

In particolare i principali formati sono:
XML: SDI 1.0, SDI 1.1
PDF
PDF/A

I formati per gli indici del Versamento (IdV) sono:
XML
TXT

I formati di firma ammessi per la chiusura del pacchetto di versamento sono:
PAdES: ETSI TS 102 778
CAdES: ETSI TS 101 733
XAdES: ETSI TS 101 903

Il sistema di conservazione di BBBELL gestisce la conservazione di qualunque tipologia documentale secondo quanto definito dal contratto di servizio verso il cliente, purché la tipologia documentale sia effettivamente dematerializzabile o conservabile nativamente in digitale, secondo le norme attuali. Il sistema di conservazione può prendersi carico di gestire i documenti secondo i processi di conservazione qui definiti. A titolo di esempio, vengono indiate alcune tipologie documentali di maggiore interesse:

Documenti soggetti a conservazione	Processo di conservazione	Formato del documento	Tempo di conservazione	Campi di ricerca utilizzati
Fatture PA	Conservazione digitale dei documenti	XML firmato o in CAdES o XAdES	Entro il 31 dicembre dell'anno successivo	-Cognome-Nome-Denominazione-Codice fiscale - Partita Iva -Dat-Associazioni logiche dei campi
Fatture Attive	Conservazione digitale dei documenti	PDF con firma PAdES o CAdES	Entro il 31 dicembre dell'anno successivo	-Cognome-Nome-Denominazione-Codice fiscale - Partita Iva -Data-Associazioni logiche dei campi
Fatture Passive	Conservazione digitale dei documenti	PDF con firma PAdES o CAdES	Entro il 31 dicembre dell'anno successivo	Cognome-Nome-Denominazione-Codice fiscale - Partita Iva -Data-Associazioni logiche dei campi
Libri e Registri Contabili	Conservazione digitale dei documenti	PDF con firma PAdES o CAdES	Annuale	Partita Iva – Anno- Mese-Sezionale
LUL	Conservazione digitale dei documenti	PDF con firma PAdES o CAdES	Mensile	Numero Documento Data Documento - C.F. - Cognome – Nome - Centro di costo - IdEmploy

Il sistema consente la parametrizzazione del piano di classificazione in essere presso il singolo soggetto produttore

Il piano di classificazione deve essere articolato in livelli gerarchici

Torna al sommario

5.2 Pacchetto di versamento

Il versamento dei documenti viene effettuato in modalità asincrona e prevede che il sistema versante possa inviare una singola unità di archiviazione o più di esse.

In particolare viene verificata la validità della firma apposta sul documento.

Per tale ragione, al fine di verificare la validità della firma e quindi l'integrità del documento ci si avvale del software fornito dalla Commissione Europea "DSS WebApp" .

Ciò significa che il pacchetto di versamento viene analizzato e se accettato viene prodotto un rapporto di versamento al produttore che attesta che il sistema del conservatore ha preso in carico il pacchetto di versamento stesso e procederà alla produzione del pacchetto di archiviazione.

Il pacchetto di versamento (PdV) è costituito da:
un indice di versamento contenente le informazioni generali del PdV, i metadati associati a ciascun documento oggetto di conservazione;
le unità di archiviazione oggetto dell'operazione di versamento dichiarate nell'indice di versamento.

Il sistema di conservazione, garantendo l'integrità del versamento, riceve i documenti anche in diversi formati tramite canali concordati con il cliente.

A titolo di esempio ma non esaustivo si ricorda che il cliente potrebbe inviare i documenti per la generazione del pacchetto di versamento in questo modo (viene anche descritta la metodologia per garantire integrità):
Canale di Invio: Connessione SFTP in una struttura a cartelle predefinita oppure tramite webservice direttamente al sistema documentale, attraverso un canale protetto tramite il protocollo HTTPS.
Integrità garantita da: Firma digitale o controllo di un hash del file (eventualmente presente nell'indice).

A caricamento avvenuto il sistema effettua i seguenti controlli:
che i files del PdV siano tutti firmati digitalmente; in caso contrario il sistema si comporta in modo diverso in base agli accordi contrattuali:
qualora il Cliente dovesse inviare documenti esclusivamente firmati digitalmente il sistema avvisa il Cliente che ci sono dei files non firmati e li individua, affinché possano essere firmati digitalmente.
se il contratto di servizio con il Cliente, prevede la conservazione di fatture analogiche e quindi non firmate digitalmente al momento dell'emissione, il sistema sarà in grado di ricevere i files non firmati e di procedere con la firma automatica massiva tramite HSM sicuro, per rendere le fatture analogiche, documenti informatici e provvedere successivamente alla conservazione come dettato dal Art. 4 recante gli *Obblighi da osservare per la dematerializzazione di documenti e scritture analogici rilevanti ai fini tributari* , del DMEF del 17 Giugno 2014
che il file sia integro e non corrotto, diversamente il sistema avvisa di rieffettuare il caricamento.

All'interno delle configurazioni dell'archiviazione e nel processo di versamento, sulla gestione degli utenti adibiti al versamento, sono gestite le informazioni degli utenti produttori.

Un utente produttore deve essere censito sul sistema con alcune informazioni obbligatorie:
Tipo documento (Carta Identità, Codice fiscale)
Numero documento
Codice Fiscale
Ente
Indirizzo email

L'utente produttore viene in questo modo collegato ad un Ente.

Il sistema gestisce un'anagrafica degli Enti centralizzata indipendentemente dai tenant facendo visualizzare su

ogni tenant solo gli enti associati a quel tenant.

Un Ente possiede le seguenti informazioni:
Ragione Sociale
P Iva/Codice Fiscale
Indirizzo
Città
Telefono
Contratto

Un utente produttore deve essere collegato ad un ente (anagrafica centralizzata).

Ogni ente è collegato a un contratto. L'anagrafica dei contratti è strutturata come segue:
Id contratto
Data inizio
Data scadenza
Descrizione
Tipologia

Nel caso in cui l'ente produttore, nella "specificità del contratto", richieda una fornitura di servizio per il processo di conservazione di documenti che contengano dati sensibili, il pacchetto di versamento conterrà esclusivamente dati cifrati, ovvero verrà rifiutato il PdV che eventualmente contenga dati trasmessi in chiaro dall'ente produttore.

Torna al sommario

5.3 Pacchetto di archiviazione

Il Pacchetto di Archiviazione – PdA - è il pacchetto informativo con cui il SdC conserva i documenti informatici e il loro indice di conservazione con garanzia di integrità e reperibilità nel tempo. Esso viene formato in seguito alla trasformazione di uno o più Pacchetti di Versamento.

L'indice di conservazione definito come IdC è un file in formato XML SinCRO UNI 11386 : 2010, che riporta per ogni documento archiviato alcune informazioni del file stesso tra cui una stringa URN e un'impronta HASH.

L'URN è una stringa che rappresenta in maniera univoca il file stesso senza determinarne l'ubicazione mentre la stringa di HASH rappresenta un'impronta del documento ricavata dalla sequenza di bit del file stesso che garantisce nel tempo il controllo della corrispondenza esatta del contenuto originale.

Ad un singolo pacchetto di versamento possono corrispondere più pacchetti di archiviazione e viceversa.

La figura seguente riporta la struttura del file xml in accordo allo standard Sincro UNI 11386:2010

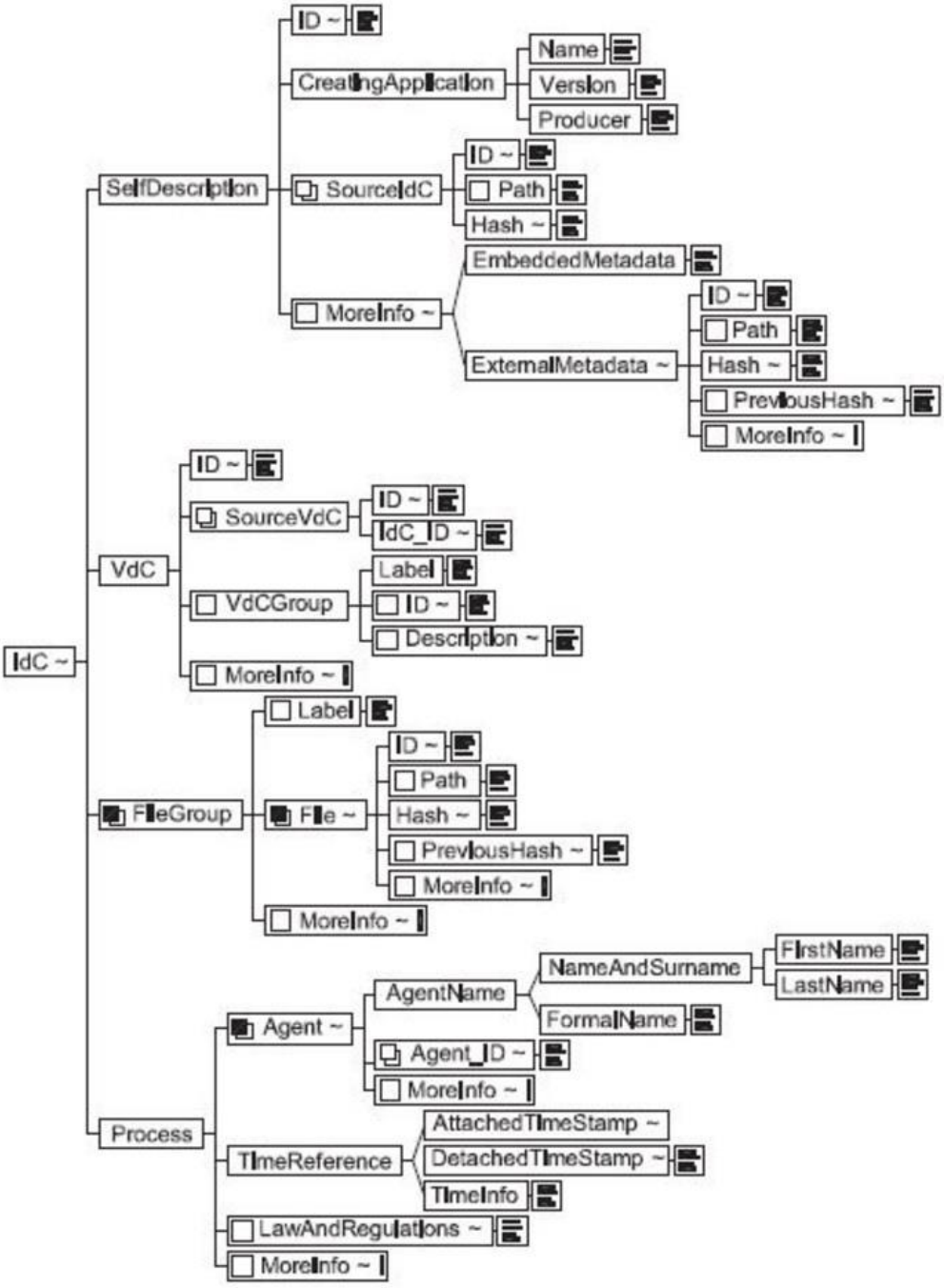


Figura 3 - Struttura del file xml

Un pacchetto di archiviazione è firmato digitalmente e marcato temporalmente.

La ricezione di un rapporto di versamento da parte del cliente non implica che il pacchetto di archiviazione sia stato prodotto, ma solo l'accettazione del pacchetto di versamento.

Torna al sommario

5.4 Pacchetto di distribuzione

Il sistema permette la ricerca nel tempo di tutti i pacchetti di archiviazione precedentemente creati, mettendo a disposizione un oggetto detto pacchetto di distribuzione.

Il pacchetto di distribuzione (PdD) è formato da un archivio compresso in formato .zip contenente:
l'indice del pacchetto di archiviazione aggregato all'operazione di conservazione, firmato in PADES o in XADES dal Responsabile della conservazione;
la marca temporale operata sull'indice del pacchetto di archiviazione sottoscritto che attesta data e ora in cui è avvenuta la conservazione;
le unità di archiviazione aggregate all'operazione di conservazione.

All'interno del file zip è presente una pagina web aprendo la quale è possibile navigare tra i documenti del pacchetto.

Il pacchetto di distribuzione, pertanto, è un pacchetto software generato dinamicamente da una eventuale ricerca, che contiene indice xml e copia dei documenti estratti, con un mini webserver integrato che permette di consultare istantaneamente, con interfaccia avanzata, documenti versati e/o conservati su sistemi Windows.

Nel Pacchetto di distribuzione non vengono inseriti i tool di installazione necessari a visualizzare i file presenti nello stesso, in quanto la leggibilità del documento nel tempo è di responsabilità dell'ente produttore.

Con l'ente produttore verrà stabilito nella "specificità del contratto" che in caso di risoluzione del contratto l'ente conservatore fornisce tutti i documenti conservati tramite vari PDD. Alla consegna del PDD, verrà concordato con il cliente che i dati verranno automaticamente cancellati dopo 15 giorni dalla consegna effettiva tramite file zip.

Torna al sommario

6. IL PROCESSO DI CONSERVAZIONE

Il sistema qui presentato e le figure riportate di seguito, sono riferite al software di Savino Solution acquistato da BBBell al fine di avere un sistema di conservazione digitale a norma.

Il processo di conservazione digitale si svolge sugli aggregati logici definiti unità di archiviazione, ovvero formate da uno o più documenti che compongono l'archivio dell'ente produttore.

La figura seguente illustra le modalità di interazione tra gli attori coinvolti e gli output prodotti

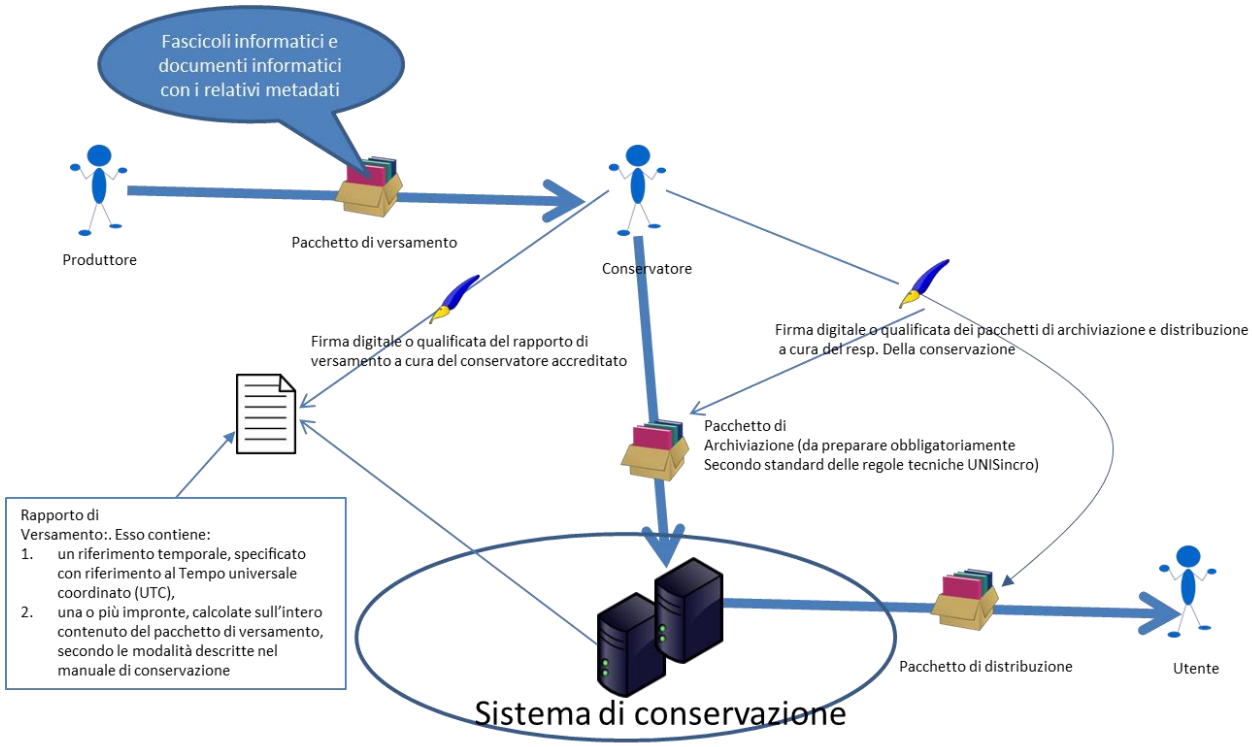


Figura 4 - Modalità di interazione tra gli attori coinvolti e gli output prodotti

Il processo di conservazione è illustrato, per ciò che concerne le attività che partono dalla presa in carico dei documenti, e che perdurano per tutto il ciclo di vita degli stessi nelle due figure successive.

Nella descrizione si possono osservare dei (sotto)processi sincroni (il loro inizio è consequenziale al termine di un precedente sottoprocesso), asincroni e periodici (il loro inizio è schedulato ad intervalli di tempo definiti).

La prima figura illustra il processo dalla presa in carico del pacchetto di versamento fino alle creazione ed alla conservazione del pacchetto di conservazione, per talune attività le stesse vengono ulteriormente dettagliate in sottoattività:

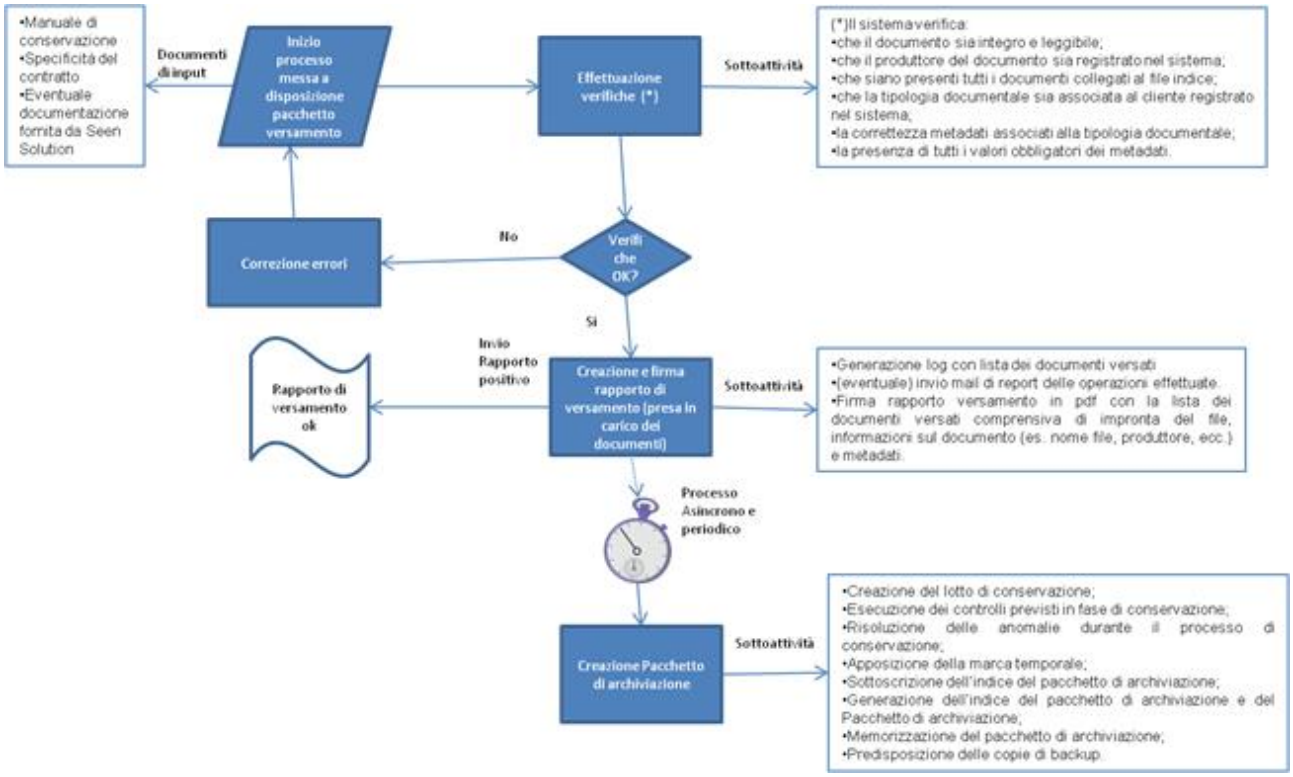


Figura 5 - Processo di presa in carico del pacchetto di versamento

Successivamente alla creazione e conservazione del pacchetto di archiviazione vengono eseguite tutte le attività asincrone e periodiche sui documenti come illustrato nella figura seguente:

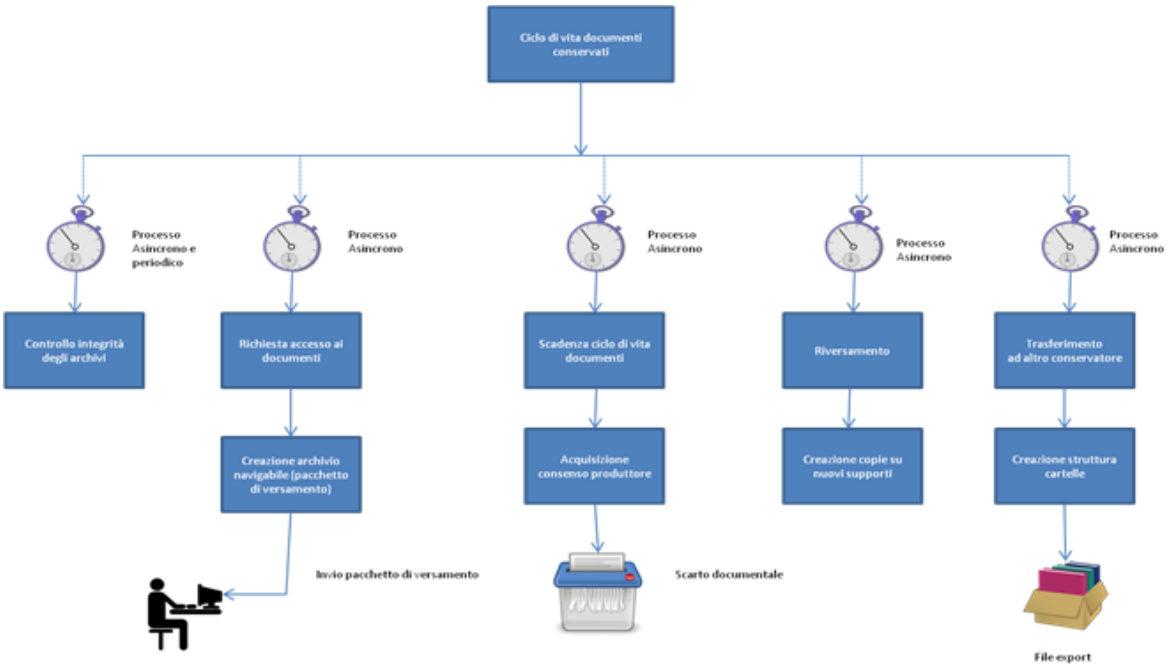


Figura 6 - Attività asincrone e periodiche sui documenti

Il processo di conservazione digitale avviene secondo le modalità indicate di seguito:
l'Ente Produttore invia in conservazione le unità di archiviazione indirizzate nel Pacchetto di Versamento ed il sistema esegue in automatico i controlli;
il sistema genera automaticamente il Rapporto di Versamento che viene messo a disposizione dell'Utente all'interno della piattaforma "BBCONS";
versati i documenti, il Responsabile del servizio di conservazione crea il Pacchetto di archiviazione attraverso un job periodico o forzando la creazione manuale;
con la creazione del PdA la procedura si conclude generando un Indice del Pacchetto di archiviazione (UNISINCRO 11386:2010), l'apposizione della firma digitale da parte del Responsabile del servizio di conservazione che attesta il regolare svolgimento del processo di conservazione e la marca temporale sul pacchetto di archiviazione stesso.

Con la creazione del Pacchetto di archiviazione:
viene generata una copia del pacchetto sul sistema di backup remoto;
viene generato, per ogni operazione di conservazione, un Pacchetto di distribuzione, per consentire l'esibizione e la fruizione dei documenti conservati.

Alla decorrenza dei termini di conservazione, previsti dalla legge e indicati dal Produttore, viene effettuato lo scarto dei PdA.

Torna al sommario

6.1 Modalità di acquisizione dei pacchetti di versamento

È presente una modalità di acquisizione del pacchetto di versamento che viene generato dal sistema di conservazione, come da passaggi successivi:

1) l'ente produttore invia i file da conservare a norma;

2) all'atto della conservazione vengono ricercati nel sistema i documenti effettivamente da conservare;

3)da questa lista di documenti viene generato un indice di versamento in formato XML contenente l'elenco dei file con tutti i metadati associati;

4) l'indice di versamento viene inviato al produttore via mail;

5) viene in seguito generato il pacchetto di conservazione/archiviazione , a seguito del quale verrà creato un rapporto di versamento in formato pdf, anch'esso conservato nello stesso pacchetto.

Il software che si occupa del caricamento dei documenti nel sistema documentale genera automaticamente log per ciascuna operazione effettuata: dall'upload effettivo del file, dall'aggiornamento dei metadati alle transizioni dei work flow del documento stesso.

Il versamento dei documenti viene effettuato in modalità asincrona e prevede che il sistema versante possa inviare una o più unità di archiviazione.

Più specificatamente:
il produttore produce il PdV così come definito nel documento "Allegato B- Configurazione del sistema di conservazione" del contratto" e lo trasferisce al SdC tramite canali ftp o web service
il sistema acquisisce i metadati forniti nei file indice ove ciascun file è riferito ad un documento da versare.

Torna al sommario

6.2 Verifiche effettuate sui pacchetti di versamento

All'atto dell'acquisizione dei documenti versati il processo automatico effettua i seguenti controlli:
identifica il produttore in virtù delle credenziali già rilasciate per versare i documenti nella cartella di riferimento

verifica che i metadati inseriti rispettino la tipologia documentale scelta e che siano presenti tutti i valori obbligatori.
verifica la consistenza dei documenti versati

Il sistema controlla la coerenza dei metadati forniti nei file indice rispetto all'obbligatorietà degli elementi concordati anche in fase di contratto.

All'atto del caricamento del file sul documentale ne viene verificata la presenza dei metadati minimi e dei formati standard previsti dalla normativa. In caso di esito positivo si procede al caricamento nel documento, nel caso contrario viene notificata tramite una mail all'ente produttore l'errore riscontro e ne viene richiesta una nuova trasmissione dello stesso documento.

Torna al sommario

6.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento

Eseguiti i controlli di cui al paragrafo precedente sul pacchetto di versamento, se quest'ultimo viene accettato, il sistema genera un log che include, tra l'altro, la lista dei documenti versati e, su richiesta del cliente, il sistema può inviare una mail di report delle operazioni effettuate.

Il Log viene firmato e marcato temporalmente e inviato in conservazione.

Il rapporto di versamento viene generato dopo l'accettazione del pacchetto di versamento e contestualmente firmato.

Il rapporto di versamento è un file PDF contenente la lista dei documenti versati comprensiva di impronta del file, informazioni sul documento (es. nome file, produttore, ecc.) e metadati.

Il rapporto di versamento viene conservato sul sistema unitamente ai documenti versati di riferimento.

Torna al sommario

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

I pacchetti di versamento vengono rifiutati se:
Il documento è illeggibile o corrotto
Il produttore del documento non è registrato nel sistema
Il documento collegato al file indice non è presente
La tipologia documentale del documento non è associata al cliente registrato nel sistema
I metadati relativi alla tipologia documentale non sono corretti
Non sono stati specificati tutti i valori obbligatori dei metadati

Si precisa che tutte le operazioni di processo effettuate sul sistema di conservazione, vengono comunicate tramite Email e PEC al Produttore e allo stesso Responsabile del servizio di conservazione.

Torna al sommario

6.5 Preparazione e gestione del pacchetto di archiviazione

La preparazione e la gestione del Pacchetto di archiviazione viene effettuata attraverso un processo ad hoc, avente le seguenti specifiche fasi:
Creazione del pacchetto di conservazione contenente i documenti versati dal Produttore;
Esecuzione dei controlli previsti in fase di conservazione come indicato nei Paragrafi 5.2 e 6.2;
Generazione dell'indice del pacchetto di archiviazione e del Pacchetto di archiviazione.

Il PdA viene memorizzato all'interno del file system con la seguente strutturazione a cartelle:
ROOT_CONSERVAZIONE\NOME_PRODUTTORE\NOME_PACCHETTO\

Il file indice del pacchetto di archiviazione (XML), la marca temporale (TSR) e il Rapporto di Versamento (PDF) sono memorizzati all'interno della cartella principale del pacchetto.

I nomi dei tre file sopra indicati seguono la seguente regola per la nomenclatura:
IDPACCHETTO_NOMEPACCHETTO_AAAA_MM_GG_HH_II (dove AAAA, MM, GG, HH, II rappresentano la data in cui è stato generato il pacchetto).

I documenti facenti parte del PdA sono memorizzati in cartelle organizzati per tipologia documentale.
Apposizione della firma digitale tramite HSM del Responsabile del Servizio di Conservazione sul Pacchetto;
Apposizione della marca temporale tramite HSM;
Memorizzazione sicura su server dedicato separato fisicamente e logicamente e organizzativamente dagli altri sistemi, del pacchetto di archiviazione;
Predisposizione delle copie di backup.

Torna al sommario

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

In accordo alla normativa il sistema di conservazione deve permettere la creazione di un pacchetto di distribuzione per permettere la consultazione dei documenti conservati da parte degli aventi diritto secondo la normativa vigente.

Connettendosi al sistema tramite interfaccia web, previa autenticazione, è possibile ottenere, per i documenti ricercati, i documenti stessi archiviati in un file .zip insieme ad una pagina web per la navigazione all'interno dei file una volta decompresso il pacchetto.

Torna al sommario

6.7 Produzione di duplicati e descrizione dell'eventuale intervento del pubblico ufficiale

Esistono casi in cui è necessaria la produzione di una copia informatica con attestazione di conformità da parte di un Pubblico Ufficiale, ovvero:

- Quando il formato del documento deve adeguarsi all'evoluzione tecnologica;
- Quando deve far fronte a specifiche esigenze dell'utente.

In tal caso, il processo richiede la gestione di una migrazione(riversamento) di documenti informatici, ovvero il processo che avviene attraverso una conservazione con differenti regole tecniche, terminando così con l'apposizione di una marca temporale e della firma digitale da parte del Responsabile di Conservazione che ne attesta lo svolgimento del processo sull'insieme dei documenti e sul Pacchetto di Archiviazione contenente una o più impronte modificate rispetto alla conservazione precedente.
Nel caso di duplicati e copie informatiche dei documenti conservati, qualora risultasse necessaria l'attestazione di conformità il Responsabile del Servizio di Conservazione si potrà avvalere di un pubblico ufficiale nominato di volta in volta dal Cliente/Produttore o Ente Titolare dei Documenti Informatici da conservare.

Tali operazione di "Migrazione(Riversamento)" vengono registrate nel sistema di conservazione BBCons, evidenziando che la sorgente del nuovo pacchetto di archiviazione proviene da un altro pacchetto e se ne dà evidenza sia nei log sia nei file UNISINCRO, valorizzando il campo SourceVDC e il campo iPDA_IDPRE.

Torna al sommario

6.8 Scarto dei pacchetti di archiviazione

Lo scarto dei pacchetti di archiviazione dal sistema di conservazione a norma avviene alla scadenza dei termini di conservazione e comunque definiti in sede contrattuale con il Cliente.

In tal caso sei mesi prima della scadenza viene inviata una comunicazione al Titolare dell'archivio, con la

descrizione dei documenti prossimi al termine di conservazione; il Titolare dovrà o confermare la cancellazione o richiedere il prolungamento del periodo di conservazione.

Lo scambio di informazione deve avvenire in forma scritta e firmata digitalmente sia dal Responsabile di conservazione che dal titolare dell'archivio.

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo.

Torna al sommario

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

La principale struttura-dati a garanzia dell'interoperabilità per SAVINO SOLUTION è il Pacchetto di Archiviazione generato secondo le regole tecniche in materia di sistema di conservazione e secondo lo standard nazionale UNI SINCRO 11386:2010. La sua distribuzione avviene attraverso la richiesta di uno o più Pacchetti di Distribuzione (PdD) tramite diverse funzionalità e modalità (interfaccia web, web service, sFTP, ecc.) messe a disposizione dal servizio BBCons che garantisce la corretta trasferibilità da parte del produttore ad altro conservatore. Nel caso di riconsegna di tutti i PdA conservati (ad esempio per la chiusura del servizio o per la cessazione anticipata del servizio secondo quanto concordato contrattualmente) il produttore dei documenti (utente) potrà richiedere la loro distribuzione al sistema BBCons, inviando richiesta via mail direttamente al Responsabile del Servizio di Conservazione.

Tale archivio presenta la seguente struttura in singole cartelle:
NOME PRODUTTORE
TIPOLOGIA DOCUMENTALE1
LISTA DOCUMENTI
TIPOLOGIA DOCUMENTALE2
LISTA DOCUMENTI
RAPPORTO DI VERSAMENTO (PDF)
INDICE DEL RAPPORTO DI VERSAMENTO (XML)
MARCA TEMPORALE

Torna al sommario

7. IL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione ha internamente diverse e numerose funzionalità che sono in grado di gestire la riservatezza dei dati in esso registrati:
Profilazione dell'utenza includendo i livelli di amministratore del sistema e creando profili differenziati per le differenti utenze dei clienti in modo da permettere talune operazioni solo a determinati profili.
Tracciamento delle attività eseguite sul sistema inclusivo della tipologia di attività (esempio: creazione pacchetti di distribuzione o esportazione Log) e dell'utenza che l'ha eseguita.
Esportazione dei log firmati digitalmente
Revisione periodica dei diritti d'accesso con possibilità di conferma, modifica o revoca degli stessi

Torna al sommario

7.1 Componenti Logiche

Le componenti logiche del sistema di conservazione sono identificate dalla figura seguente:

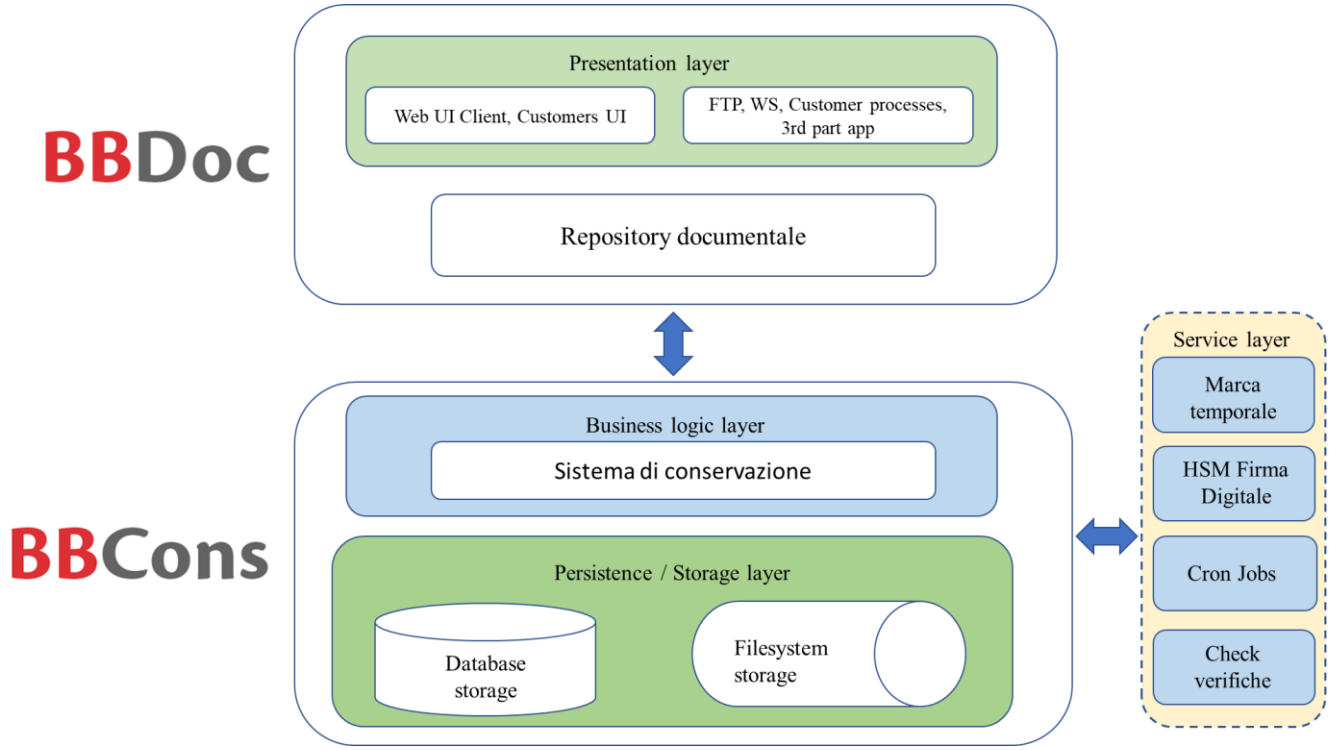


Figura 7 - Componenti logiche del sistema di conservazione

BBDoc: è il software di repository documentale che permette di caricare e/o versare i tipi di documenti che poi saranno sottoposti a conservazione.

BBCons: è il software di conservazione che a partire da un pacchetto di versamento genera automaticamente un pacchetto di conservazione che è firmato digitalmente e marcato temporalmente dal Responsabile della conservazione. Tale piattaforma permette al produttore di consultare e/o generare i pacchetti di distribuzione ovvero i pacchetti di conservazione creati a norma di legge.

Presentation Layer. È il layer che rappresenta l'interfaccia utente nativa del sistema o prodotta dal cliente tramite cui accedere al sistema e/o degli endpoint FTP, processi automatici o applicazioni di terzi che effettuano le operazioni utilizzando i web service

Business Logic Layer. Rappresenta le parti logiche del sistema, ovvero la logica di conservazione e quella di memorizzazione dei documenti Repository documentale / DMS. In questo blocco vengono definiti e decisi le modalità di memorizzazione e smistamento dei documenti.

Persistence/Storage Layer. E formato dal motore database per la persistenza dei dati e metadati dei documenti e dal sistema di memorizzazione su File System.

Services Layer. Rappresenta un set di servizi esterni al sistema che svolgono operazioni verticalizzate quali ad esempio la firma elettronica HSM dei documenti non firmati e l'apposizione della marca temporale (TSR) , la verifica di integrità dei file oppure operazioni schedulate e/o customizzate per i clienti.

Torna al sommario

7.2 Componenti Tecnologiche

Il sistema è accessibile dall'esterno tramite (s)ftp e web services per il versamento dei pacchetti e tramite i principali web browser (Internet Explorer, Firefox, Chrome) per le operazioni di consultazione e di operation & maintenance.

In particolare web il sistema separa la logica di presentazione dei dati da quella di business implementando il paradigma model-view-controller (MVC) in cui:
Il controller intercetta tutte le richieste remote, mantenendo coerente e consistente lo stato del dialogo con l'utente remoto
La view si occupa della presentazione dei risultati delle operazioni (consultazione, ricerca, operation & maintenance)
Il model interloquisce con le basi di dati (filesystem, tabelle) alle quali accede direttamente, con il controller per le richieste di ricerca e manipolazione dei dati e con la view;

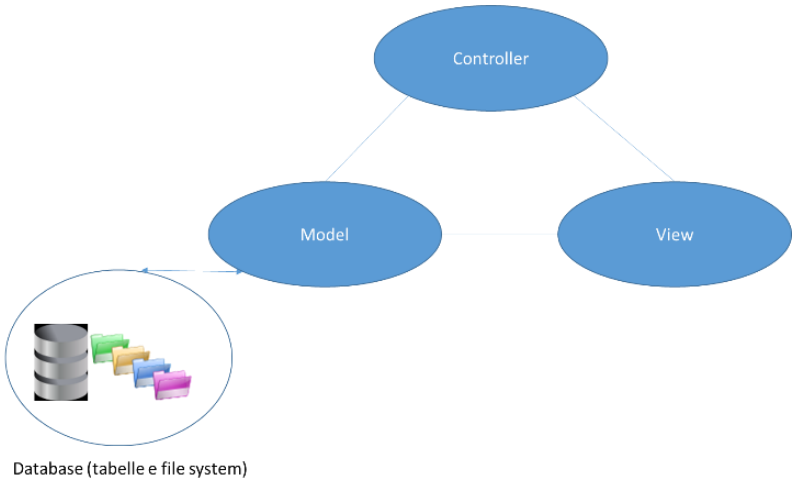


Figura 8 - Il modello MVC e le basi di dati

Il software applicativo del controller e della view è scritto in PHP per il tramite di librerie standard su web server Apache, mentre le tabelle del database sono implementate mediante database di uso standard.

I dati identificativi della Certification Autorithy (CA) sono:
Per la Firma Digitale: ARUBA PEC S.p.A. Via Sergio Ramelli 8 – 52100 Arezzo (AR) P. IVA: 01879020517 Gestore Certificato ed Autorità di Certificazione iscritta all'Elenco Pubblico dei Certificatori accreditati dal Digit PA.
ARUBA PEC S.p.A. Via Sergio Ramelli 8 – 52100 Arezzo (AR) P. IVA: 01879020517 Gestore Certificato ed Autorità di Certificazione iscritta all'Elenco Pubblico dei Certificatori accreditati dal AGID.

Torna al sommario

7.3 Componenti Fisiche

L'architettura del sistema è realizzata considerando i datacenter implementati come macchine virtuali di cui si elencano alcune caratteristiche:
Ubuntu Server 10.04
Disco 200gb
Web Server: Apache 2.2.14, con php 5.2.17 e DB PostgreSql o MySQL.
Software:
Turnkey che offre un menù per la configurazione della scheda di rete,
Webmin (interfaccia web per le configurazioni di sistema)
Webshell (una shell utilizzabile tramite interfaccia web)

E' possibile implementare su uno stesso host virtuale sia l'application server che il database server, duplicandolo per garantire la continuità operativa e fornendo il filtraggio degli accessi come descritto nella figura seguente:

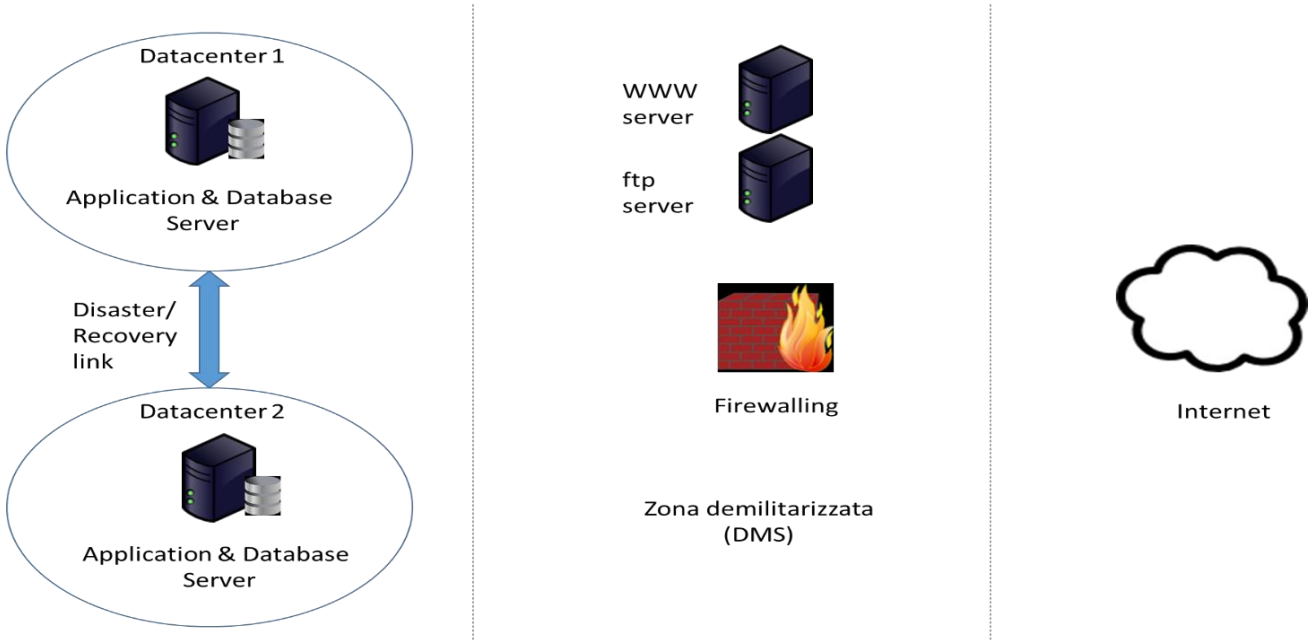


Figura 9 - Application e database server collocati su uno stesso host virtuale

In alternativa è possibile implementare l'application server ed il database server su due host virtuali separati duplicandoli per garantire la continuità operativa e fornendo il filtraggio degli accessi come descritto nella figura

seguente:

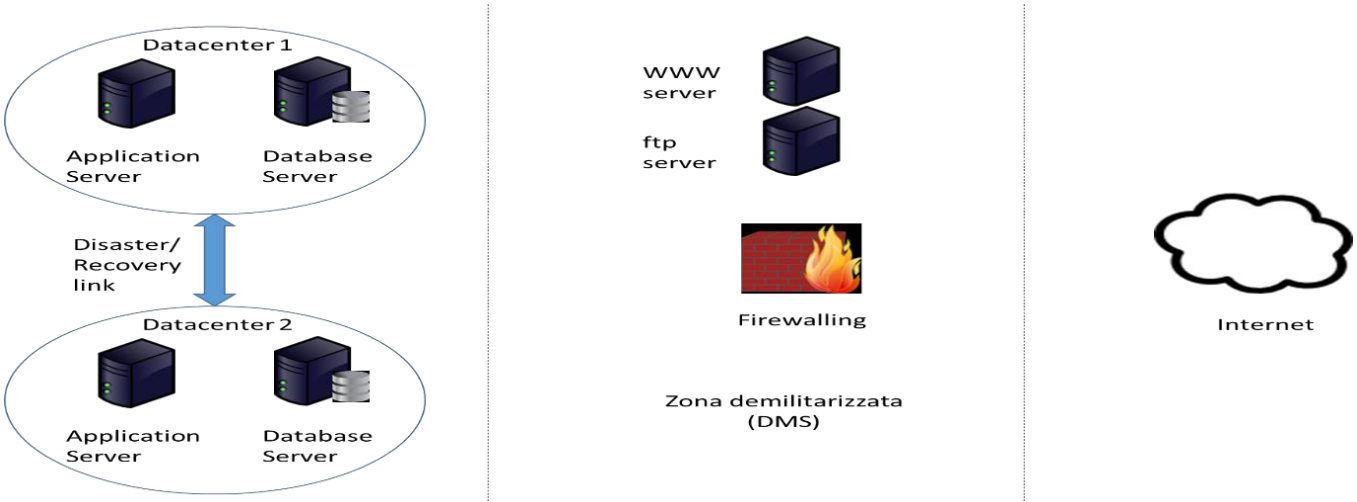


Figura 10 - Application e database server collocati su due host virtuali

La duplicazione dei data center di cui uno situato a Torino e l'altro a Bergamo presso Aruba permettono di implementare le politiche di disaster e recovery per garantire la continuità operativa, mentre le strategie di firewalling permettono il filtraggio degli accessi esterni allo scopo di proteggere i server e le basi di dati.

La soluzione di virtualizzazione dei datacenter 1 e 2 è implementata tramite VMware 5.5 enterprise.

Il cluster situato presso il DC-BBBELL è formato da 3 host atti a contenere i nodi logici, completamente indipendenti, che compongono il sistema di conservazione e l'archivio di conservazione basato sull'impiego di uno storage con dischi configurati in RAID 5.

Al sistema principale è collegato un ulteriore sistema di backup su uno storage indipendente dal primario con dischi configurati in RAID10.

In caso di fault dei sistemi, la ripartenza viene effettuata operando tramite l'interfaccia di Zerto presso il DC-ARUBA, che si occuperà di riavviare automaticamente la macchina.

È pienamente rispettata la raccomandazione di AGID relative alle distanze fra CED ed è da sottolineare la completa indipendenza sia fisica sia logica dei due CED che in nessun caso fanno ricorso a strutture condivise e a nessun livello (elettrico, rete, etc).

Sul Data Center di Bergamo (DC-ARUBA) sono state acquistate risorse in modalità Server Dedicato per gestire la totale ridondanza dei dati e quindi per il Backup, attraverso una segregazione fisica e logica rispetto ad altri sistemi. In più in tali infrastrutture di proprietà di BBBell , presenti nei locali di Aruba in modalità Server Dedicato, sono accessibili e gestite da personale BBBELL e dal personale di Aruba specificatamente e all'uopo autorizzato ed incaricato.

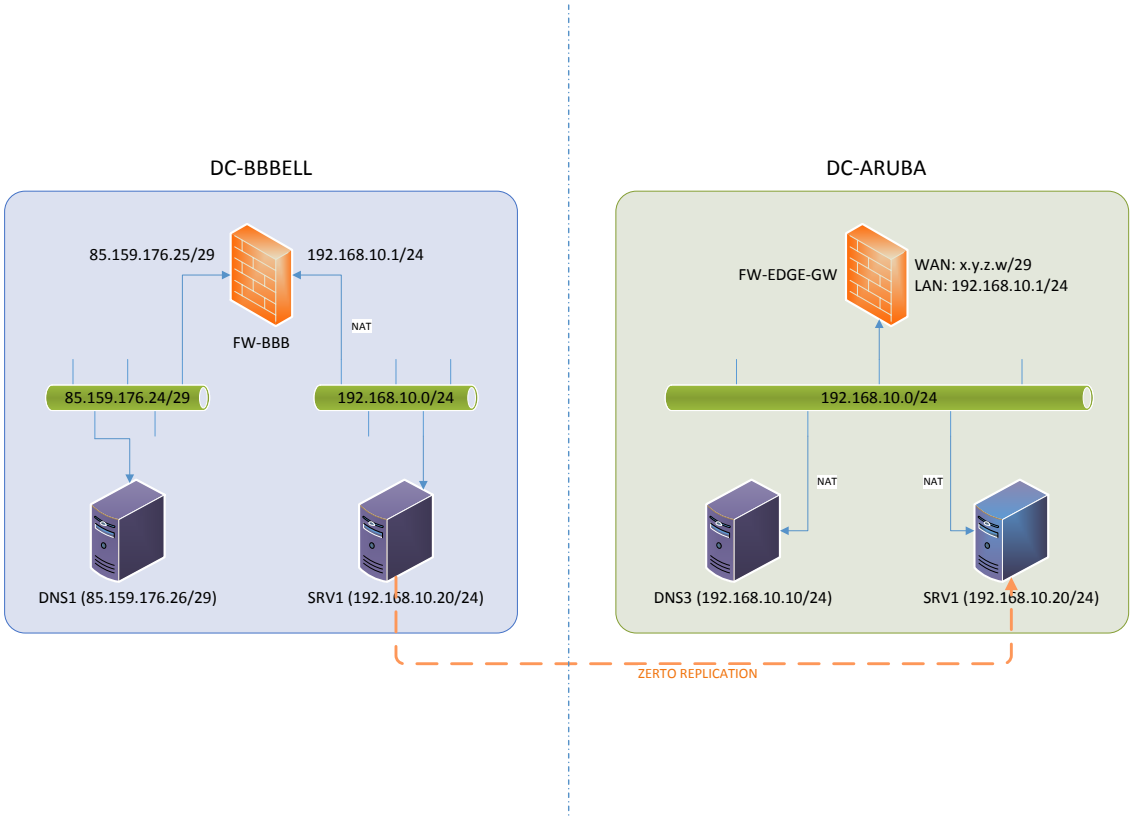


Figura 11 - Replicazione tramite Zerto

I nodi fisici sono costituiti dalle seguenti apparecchiature:

Ruolo	Datacenter	Modello	Qty
Nodo 1	DC-BBBELL	Server Lenovo x3650 M5, 2 CPU Intel Xeon 12 core E5-2690 v3 2.5GHz, 128GB RAM, 2 dischi da 300GB SAS RAID1, 4 porte di rete 1GB, 2 schede FC single port 8GB	3
Storage 1	DC-BBBELL	Storage EMC^2 VNX5200, 25 dischi SAS 900GB, 3 dischi SAS Flash 200GB per cache, 8 porte FC 8GB	1
Storage 2	DC-BBBELL	Storage IBM DS3512, 12 dischi NL-SATA 2TB	1
Nodo 2	DC-ARUBA	Resource pool da 4GHz, 8GB RAM, 250GB storage	1

DC-BBBELL è localizzato presso la Sede Legale di BBBELL: Corso Svizzera 185, 10149 Torino TO.
DC-ARUBA è localizzato presso la Sede di Aruba SpA: Via San Clemente 53, 24036 – Ponte San Pietro (BG).
La distanza tra i due siti è di circa 500 Km.

Torna al sommario

7.4 Procedure di gestione e di evoluzione

7.4.1 Conduzione e manutenzione del sistema di conservazione

BBBELL applica le proprie politiche di conduzione e manutenzione dei Sistemi Informativi in ambito aziendale, sulla base delle prescrizioni di legge, degli impegni contrattuali e delle indicazioni AGID, al fine di proteggere il proprio patrimonio informativo e quello dei suoi Clienti.

La conduzione e la manutenzione del sistema informativo hanno i seguenti obiettivi principali:
garantire la corretta e sicura operatività delle infrastrutture di elaborazione delle informazioni;
proteggere l'integrità del software e delle informazioni;
garantire la salvaguardia dei dati in transito sulle reti e la protezione delle infrastrutture di supporto;
prevenire errori, perdite, modifiche non autorizzate o abuso delle informazioni nelle applicazioni;
mantenere la sicurezza del software dei sistemi applicativi e delle informazioni

Le richieste di cambiamento su sistemi già in esercizio sono essenzialmente originate da:
malfunzionamenti riguardanti il software di base, hardware, software applicativo;
esigenze di miglioramento delle prestazioni, manutenibilità ed usabilità del sistema;
esigenze di adeguamento ai mutamenti intervenuti nell'ambiente tecnico/operativo. L'innovazione tecnologica può essere a sua volta indotta (causa/effetto) da esigenze di miglioramento del software applicativo (capacity management);
introduzione di nuove funzionalità esplicitamente richieste dall'utente.

I cambi da operare su sistemi in Esercizio sono classificabili in base a diversi parametri, quali ad esempio:
l'entità dell'impatto sia sull'operatività del servizio erogato, sia sui componenti HW e SW implicati;
la tipologia dell'intervento, espresso in termini di manutenzione correttiva, evolutiva, adeguativa;
l'urgenza degli interventi, pianificabili o meno (es. interventi per i quali è necessario un fermo del sistema che può essere programmato o accidentale, a seconda delle cause che lo determinano).

Nell'ambito delle attività che insistono sui sistemi di produzione è possibile definire una classificazione tra attività che per loro natura sono *pianificabili* ed attività *non pianificabili*.

Per le prime dovranno essere individuati dei criteri di allocazione temporale in modo da evitare, il più possibile, impatti negativi sui livelli di servizio concordati.

Per le seconde saranno individuate delle finestre temporali nelle quali si cercherà di svolgerle comunque, fermo restando che eventuali attività ritenute critiche o di assoluta necessità, potranno essere effettuate in qualsiasi momento, all'occorrenza anche durante il normale orario di esercizio e quindi al di fuori delle finestre temporali individuate, potendo comportare, in questo caso, una riduzione dei livelli di disponibilità concordati.

Nella conduzione e manutenzione del servizio, BBBELL adotta una politica di gestione delle utenze, dei ruoli e privilegi d'accesso, delle credenziali, conforme a quanto definito nella gestione dei DC e nella progettazione e gestione dei propri servizi.

Nella conduzione del servizio vengono altresì applicate le policy di sicurezza BBBELL inerenti la gestione degli asset, dei supporti di memorizzazione, delle "scrivanie e schermi puliti".

Torna al sommario

7.4.2 Gestione e conservazione dei log

BBBELL considera i log di sistema facenti parte del proprio patrimonio informativo meritevole di protezione da

tutto ciò che è in grado di minacciarlo; per tale motivo ha definito le politiche relative alla gestione dei log, che applica nei suoi DC, sulla base delle prescrizioni di legge, degli impegni contrattuali con il cliente e delle indicazioni AGID, al fine di proteggere il proprio patrimonio informativo e quello dei propri Clienti.

I log raccolti riguardano eventi inerenti:

A) Il processo di conservazione (di cui vengono memorizzati i seguenti eventi rilevanti):

a. Login

b. Creazione/modifica/cancellazione di un produttore

c. Creazione/modifica/cancellazione del Responsabile di conservazione

d. L'avvio e il termine del processo di conservazione

e. L'avvio della verifica di integrità del pacchetto di archiviazione

f. Logout

B) Gli accessi interni ed esterni al sistema;

C) Gli eventi generati dall'hardware o dalla piattaforma.

Ogni log prodotto dai processi sopra indicati, viene firmato digitalmente per il principio di integrità e portato in conservazione digitale mensilmente.

Ogni operazione(evento) rilevante eseguita sul sistema viene salvata sul database di conservazione che è sottoposto al backup con cadenza quotidiana congiuntamente all'intero server nel cloud di Aruba, come da piano di Disaster recovery descritto dalla Savino Solution.

Al fine di consentire la tracciabilità delle operazioni loggate nel data base, quest'ultime non vengono mai cancellate dal sistema.

Inoltre è possibile esportare il pacchetto di conservazione dei Log delle operazioni effettuate sul modulo e sul sistema di versamento e archiviazione utilizzando l'apposita sezione "esportazione log", per sottoporti ad eventuale richiesta da parte del Produttore o di Organi Istituzionali.

Specificando un intervallo di date, un responsabile per la firma e le cartelle/fascicoli (solo per il log delle operazioni sul sistema di versamento) sarà possibile scaricare il documento PDF firmato e marcato

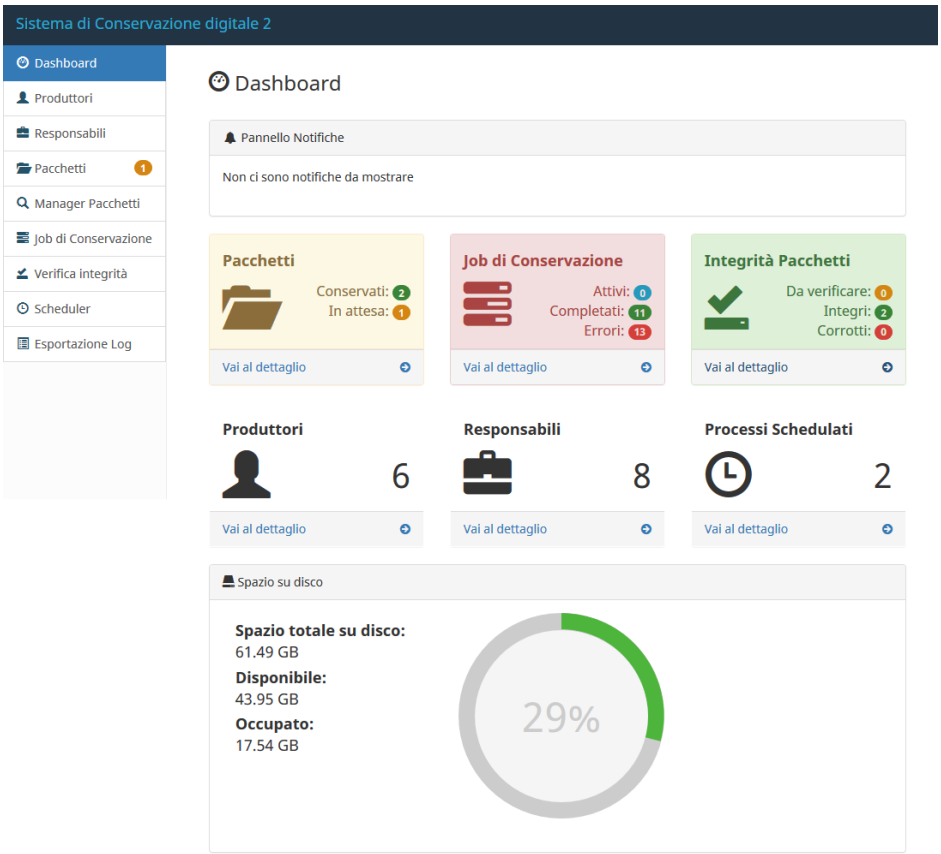
temporalmente contenente la lista delle operazioni effettuate nel periodo prescelto.

Torna al sommario

7.4.3 Monitoraggio del sistema di conservazione

Il monitoraggio dei sistemi di conservazione viene effettuato con il seguente schema:
monitoraggio istantaneo va riferito ad eventi che accadono nel sistema e per i quali vengono utilizzati degli strumenti per una rapida comunicazione via mail ai responsabili; la classificazione dell'evento viene ripartita:
- per ambito (hardware, software, rete);
- per gravità (impatto totale, parziale o nullo sul servizio).

In particolare il monitoraggio del sistema di conservazione BBCons viene previsto tramite una dashboard all'accesso utente al modulo di conservazione, attraverso cui viene data evidenza dello stato del sistema. Il monitoraggio del sistema di conservazione BBCons viene effettuato tramite controlli automatici interrogando il database di conservazione riguardante le informazioni sui pacchetti (da conservare, conservati e processi di conservazione in esecuzione), le informazioni sull'integrità dei pacchetti conservati e dei pacchetti di distribuzione generati, le informazioni sui produttori e sui responsabili del servizio di conservazione. Inoltre viene monitorato automaticamente lo spazio su disco e tramite segnalazioni grafiche vengono segnalate eventuali situazioni di errore e avvisi con notifiche testuali.



Il sistema di conservazione prevede diverse procedure per il monitoraggio delle attività di sistema e dell'integrità delle informazioni.

In particolare la dashboard è composta da:

- una lista di notifiche (avvisi, messaggi di errore o operazioni da effettuare),
- dei box contenenti informazioni sulle singole sezioni del modulo e conteggio dei totali
- riquadro per il monitoraggio dello spazio disponibile su disco.

I box e le notifiche hanno colorazioni differenti a seconda delle situazioni: giallo per avvisi, rosso per situazioni di errore e verde o azzurro per messaggi informativi.

Lo stesso sistema di avvisi viene replicato sulle singole voci del menu oppure nelle pagine e nelle form di sistema.

Per quanto riguarda procedure altamente delicate come il processo di conservazione e la verifica di integrità dei pacchetti, le notifiche web, vengono corredate da notifiche via mail che informano l'utente sull'inizio e la fine delle procedure segnalandone la corretta esecuzione o eventualmente le situazioni di errore.

Tramite lo scheduler è inoltre possibile monitorare l'integrità dei PdV conservati tramite procedure periodiche stabilite dall'utente.

Inoltre il sistema tiene traccia con un sistema di contatori dei totali dei PdV e dei PdA generati, dei processi di conservazione avviati, di quelli terminati correttamente e in generale di tutte le procedure effettuate sul sistema di conservazione.

Un riepilogo settimanale di tutte le segnalazioni relative al monitoraggio del sistema di conservazione BBCons viene inviato automaticamente via mail ai responsabili del servizio di conservazione.

Il monitoraggio comporta l'attività di supporto tecnico, on demand, nelle fasi di manutenzione o deployment delle applicazioni.

Torna al sommario

7.4.4 Change management

Il software che realizza il sistema di conservazione, acquistato da BBBELL, è di proprietà della Società SAVINO SOLUTION, in persona del legale rappresentate p.t. Ing. Nicola Savino, con sede legale in Piazza Flavio Gioia 3, 84122 Salerno (SA).

Per tale ragione il processo di change management è gestito da SAVINO SOLUTION con la massima attenzione e professionalità ed è di interesse sia per il cliente che per l'azienda.

Le change request, infatti, possono essere sia autogenerate dalla stessa SAVINO SOLUTION per adeguamenti normativi o tecnologici, organizzativi e di processo imposti dagli standard di qualità che generate da BBBELL per gestire ad esempio nuovi requisiti sopraggiunti durante la fase di esercizio.

È previsto un meccanismo di gestione delle priorità delle change request e di pianificazione delle deadline delle stesse con meccanismi di tracciabilità delle stesse e la presenza di una board interna che ne controlla l'avanzamento con tutti gli stakeholder.

Per maggiori dettagli si rimanda alla procedura di Change Management del fornitore SAVINO SOLUTION.

Torna al sommario

7.4.5 Verifica periodica di conformità a normativa e standard di riferimento

Ai fini della verifica di conformità sono periodicamente effettuati degli audit interni applicando procedure appositamente definite che stabiliscono il processo di verifica, attività, ruoli e responsabilità.

Le verifiche ispettive sono eseguite sui documenti e/o prodotti delle attività esaminate e sulle registrazioni risultanti dallo svolgimento delle attività.

Qualora contrattualmente richiesto, la procedura si estende al personale e alle attività di eventuali sub-fornitori.

Il processo di audit si compone dei seguenti passi :
Pianificazione : è predisposto il Piano delle verifiche ispettive (sulla base di una serie di elementi tra cui le non conformità riscontrate, gli obiettivi ed i piani di miglioramento) in modo che venga verificata l'efficacia del Sistema di Gestione Integrato e che tutti i processi di rilievo siano visti di norma una volta l'anno.
Assegnazione : a partire da una lista a disposizione del responsabile della qualità sono scelti gli ispettori, sulla base di specifici criteri di formazione e qualificazione, per tipologia di norma da verificare
Accordo di visita : l'ispettore concorda la data di visita con il responsabile da esaminare richiedendo l'eventuale documentazione necessaria
Esecuzione visita ispettiva : l'ispettore esegue la verifica dei requisiti del Sistema che fanno capo al responsabile esaminato, confrontando le evidenze delle attività svolte con le procedure previste per quelle attività.
Verifica chiusura non conformità : l'ispettore verifica e valuta le correzioni effettuate e ne dichiara la (eventuale) risoluzione
Riepilogo delle non conformità : viene redatto il riepilogo delle non conformità (indirizzato, nei momenti pianificati, al riesame della Direzione).

Infine, viene consultata periodicamente la sezione NEWS sul portale www.assistenzasavino.com dove sono pubblicate notizie riguardo novità normative, specifiche tecniche ed eventuali disservizi da parte di SDI.

Savino Solution, infine, invia una newsletter tutte le volte che viene aggiunta una notizia sul suddetto portale, che viene inoltrata ai Clienti BBBell.

Torna al sommario

8. MONITORAGGIO E CONTROLLI

Al fine di garantire ed assicurare la continuità operativa del sistema di conservazione BBCons, in accordo anche ai requisiti di qualità minimi previsti contrattualmente con il soggetto produttore nella specificità del contratto, BBBELL adotta e implementa un processo e una procedura di monitoraggio e di relativo controllo.

Torna al sommario

8.1 Procedure di monitoraggio

Vengono qui descritte le procedure di monitoraggio del sistema di conservazione (comprensive dei relativi report e log) effettuate sul funzionamento del software applicativo e di sistema, nonché sulle componenti hardware, anche con l'obiettivo di valutare l'efficacia del sistema di conservazione.

Ulteriori procedure aggiuntive richieste dal soggetto Produttore descritte nel documento di specificità del contratto.

Le grandezze monitorate per tutte le macchine virtuali e fisiche sono:

- Sistema
- Memoria (RAM e disco)
- Cpu usage e rilevamento dei picchi
- Stato dei processi di sistema
- Esito e durata dei processi di backup
- Rete (solo per le macchine fisiche)
- raggiungibilità dei sistemi fisici e virtuali
- traffico di rete giornaliero e mensile (volume dati scambiati)
- max traffico picco banda su su base 15 min
- RDBMS
- spazio occupato dal DB
- query wait on lock
- idle in transaction status
- Stato ed esito dei processi di conservazione

Vengono stabiliti dei valori di soglia raggiunti i quali il sistema invia una richiesta di ticket all'helpdesk di supporto.

La piattaforma di virtualizzazione del DC-BBBELL è monitorata attraverso l'uso del VCenter del VMWare

Il sistema genera dei log a livello di:

- operazioni di amministratore
- operazioni utente
- operazioni del sistema (e.g. esito monitoraggi periodici)
- eventi

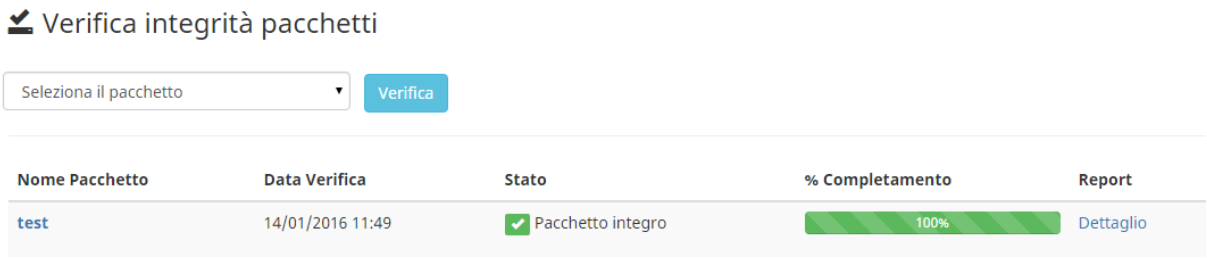
ciò significa che sia la piattaforma sia l'applicazione di conservazione generano dei log, molti dei quali descritti già a proposito della descrizione del processo di conservazione nei paragrafi precedenti.

È possibile l'esportazione dei log di conservazione al cliente su sua richiesta.

Torna al sommario

8.2 Verifica dell'integrità degli archivi

Per assicurare la verifica dell'integrità dei documenti conservati nella loro omogeneità rispetto agli indici, in accordo con il cliente e pari a quanto previsto dalla normativa in atto, il sistema ne applica procedure automatizzate. Difatti, dallo scheduler il Responsabile del servizio di conservazione verifica l'integrità del pacchetto stesso.



In particolare vengono verificate le seguenti integrità:

- Che il totale dei file conservati corrisponda al totale dei file presenti sul file system e versati.
- Che i documenti conservati non siano corrotti e che l'HASH del file non differisca da quello memorizzato all'atto della conservazione per garantire che non sia stato modificato
- Che siano presenti i file indice e che non siano stati modificati (controllo HASH)

Nel caso in cui in uno o più dei precedenti punti vengano riscontrate anomalie viene segnalato al responsabile il quale attuerà le procedure di ripristino.

Le procedure di ripristino, oltre a quanto indicato nel Paragrafo 6.7, riguardano anche il ripristino dei dati, dei flussi informativi e dei documenti precedentemente memorizzati sia nel Piano di Backup sia nel Piano di Disaster Recovery, come specificato nel Piano di Sicurezza e nel Paragrafo 8.3.

Nel caso contrario il pacchetto viene considerato consistente ed integro.

La procedura di verifica integrità può essere avviata in qualsiasi momento da pannello web, oppure può essere schedulata dalla apposita sezione "Scheduler", selezionando la frequenza di esecuzione."

In entrambi i casi il sistema invierà una mail contenente il risultato dell'operazione.

Torna al sommario

8.3 Soluzioni adottate in caso di anomalie

Vengono descritte le soluzioni adottate a fronte di anomalie riscontrate a seguito del monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi.

Accordi specifici concordati con il soggetto Produttore possono essere descritti nell'allegato "Specificità del contratto".

Le anomalie possono essere suddivise come anomalie:

- software
- hardware
- integrità dei pacchetti o del database

Il reparto di helpdesk è notificato dal sistema in seguito ai monitoraggi prima descritti e provvede a gestire:
Le anomalie hardware con le operazioni di riparazione/sostituzione delle componenti danneggiate garantendo nel transitorio la continuità operativa del sistema
Le anomalie software con le procedure di ripristino, reinstallazione software, riavvio dei servizi, trasferimento

del software su altra macchina fisica o virtuale, apertura di ticket specifici verso i fornitori di servizi software applicativi e/o di piattaforma e monitoraggio degli stessi.
Le anomalie di database tramite ripristino delle copie di backup o creazione di una nuova istanza del DB su un'altra macchina con successivo ripristino i dati.
Le anomalie dei pacchetti conservati tramite l'intervento del responsabile del servizio di conservazione, di concerto anche con il responsabile della sicurezza dei sistemi il quale individuerà le cause della anomalia, e provvederà, qualora necessario, a ripristinare copie di backup, avendo cura di verificare l'integrità dei pacchetti e dandone evidenza al Produttore. Le modalità di gestione degli incidenti di sicurezza sono riportate nel Piano della Sicurezza del Servizio di Conservazione.

Torna al sommario

9. PIANO DI TERMINAZIONE DEL SERVIZIO

Ai fini di garantire l'interoperabilità tra sistemi di conservazione, BBCons è in grado di produrre dei PDD coincidenti con i PdA.

In particolare i PdD generati dal Sistema di Conservazione sono conformi allo standard UNI SInCRO.

Se il servizio di conservazione nei confronti di un Cliente/Produttore dovesse interrompersi per qualsiasi motivazione, prevista dal contratto o meno, BBBELL provvede all'esportazione dei PdA conservati in identici PdD su supporti fisici rimovibili che saranno consegnati entro 30 giorni alla richiesta ai Titolari stessi previa loro sottoscrizione dei relativi verbali di consegna; i supporti fisici verranno consegnati secondo le modalità richieste dal cliente.

Il Sistema di Conservazione è inoltre in grado di accettare il versamento di PdD provenienti da altri sistemi di conservazione strutturati secondo lo standard UNI SinCRO.

BBBELL, in caso di cessazione delle operazioni di conservazione o modifica della propria missione (interoperabilità), provvederà ad avvisare i propri Clienti/Produttori, con un anticipo di almeno 60 giorni, producendo su supporti fisici rimovibili l'intero contenuto dei supporti logici conservati (tramite vari PDD)e li riconsegnerà ai titolari, previa loro sottoscrizione dei relativi verbali di consegna e secondo le modalità richiesta dal cliente.

I dati verranno automaticamente cancellati dopo 15 giorni dalla consegna.

Per maggiori dettagli si rimanda allo specifico Piano di Cessazione del Servizio di Conservazione BBBELL.

Torna al sommario