BANCA D'ITALIA
EUROSISTEMA

Gestione dell'Informazione

MANUALE TECNICO DI CONSERVAZIONE DEI DOCUMENTI DIGITALI

Adottato ai sensi degli artt. 20, co. 3 e 5-bis, 23-ter co. 4, 43, co. 1 e 3, 44, e 71 del Decreto legislativo 7 marzo 2005, n. 82, *Codice dell'amministrazione digitale*, delle *Linee guida* AgID sulla formazione, gestione e conservazione dei documenti informatici e dei seguenti articoli del DPCM 3 dicembre 2013 contenenti "Regole tecniche per il protocollo informatico":

- art. 2 comma 1, *Oggetto e ambito di applicazione*;
- art. 6, *Funzionalità*;
- art. 9, *Formato della segnatura di protocollo*;
- art. 18, commi 1 e 5, *Modalità di registrazione dei documenti informatici*;
- art. 20, *Segnatura di protocollo dei documenti trasmessi*;
- art. 21, *Informazioni da includere nella segnatura*.

SOMMARIO

ELENCO DEGLI ACRONIMI

AgID	Agenzia per l'Italia digitale
ASBI	Archivio Storico della Banca d'Italia
CD	*Compact disc*
D.Lgs	Decreto legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
DVD	*Digital versatile disc*
FTP	*File transfer protocol*
GEDOC	Divisione Gestione dei documenti del Servizio Gestione dell'Informazione
ID	Identificativo univoco
IPdA	Indice Pacchetto di Archiviazione
IPA	Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi
ISO	*International standard organization*
OAIS	*Open archival information system*.
PdA	Pacchetto di archiviazione
PdD	Pacchetto di distribuzione
PdV	Pacchetto di versamento
PDF	*Portable document format*
PDI	Informazioni descrittive per la conservazione *(Preservation description information)*
RdV	Rapporto di versamento
SinCRO	Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali
SCDI	Sistema di conservazione dei documenti informatici
SGDD	Sistema di gestione documentale digitale
TSA	*Time Stamping Authority*
UNI	Ente nazionale italiano di unificazione
XML	*Extensible markup language*

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente *Manuale tecnico di conservazione dei documenti digitali* (di seguito, anche *Manuale*) illustra il modello organizzativo e il processo di conservazione dei documenti informatici prodotti o ricevuti, adottato dalla Banca d'Italia sia dal punto di vista organizzativo sia dal punto di vista tecnico ed operativo.

In particolare, il presente *Manuale*, a norma del paragrafo 4.6 delle *Linee Guida* AgID sulla formazione, gestione e conservazione dei documenti informatici, indica:

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 degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
h) 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;
i) la descrizione delle procedure per la produzione di duplicati o copie;
j) i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione e i tempi di scarto, così come indicati nel *Piano di conservazione*;
k) 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;
l) le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

La Banca d'Italia (di seguito, anche Banca) utilizza, un Sistema di gestione documentale digitale (di seguito, anche SGDD) [1] per la tenuta del protocollo informatico, la gestione dei flussi documentali e la conservazione degli archivi[2].

I principi, le regole e le modalità di gestione dei documenti formati e acquisiti dalla Banca sono descritti e disciplinati nel *Manuale di gestione documentale*, pubblicato sul sito dell'Istituto (www.bancaditalia.it), cui si fa interamente riferimento.

Nell'ambito del SGDD, attraverso l'applicativo Virgilio prodotto da SIAV SpA, è realizzato il Sistema di conservazione dei documenti informatici (di seguito, anche SCDI), disciplinato dal presente *Manuale*.

[1] Il SGDD è operativo dal 22 giugno 2009.
[2] Ai sensi dell'art. 61 del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* (di seguito, *Testo unico*)

2. NORMATIVA E STANDARD DI RIFERIMENTO

2.1. NORMATIVA DI RIFERIMENTO

Il presente *Manuale* è adottato ai sensi del paragrafo 4.3 delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* (nel seguito del documento referenziate come "*Linee Guida AgID*"), nel rispetto della seguente 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 - 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 - Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (anche noto come TUDA);
- Decreto Legislativo 22 gennaio 2004, n. 42 - Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 - Codice dell'amministrazione digitale (CAD), modificato e integrato con il Decreto legislativo n. 179 del 26 agosto 2016;
- Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, aggiornato con Decreto Legislativo 10 agosto 2018 n. 101;
- Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Regolamento (UE) n. 910/2014 eIDAS (electronic IDentification Authentication and Signature), base normativa comune per i Paesi membri dell'U.E. per quanto riguarda i servizi fiduciari, i mezzi di identificazione elettronica e le modalità di interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni;
- Art. 25 (Anticipazione obbligo fattura elettronica) del Decreto Legge 24 aprile 2014, n. 66 (Misure urgenti per la competitività e la giustizia sociale), convertito, con modificazioni, dalla Legge 23 giugno 2014, n. 89;
- Decreto del Ministero dell'Economia e delle Finanze 3 aprile 2013, n. 55 (Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'art. 1, commi da 209 a 213, L. 24 dicembre 2007, n. 244);
- Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto- articolo 21, comma 5, del decreto legislativo n. 82/2005;
- Circolare Agenzia delle entrate n. 36 del 06 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");
- Circolare Agenzia delle entrate n. 18/E del 24 giugno 2014 ("IVA – Ulteriori istruzioni in tema di fatturazione");
- Risoluzione n. 46/E Agenzia delle Entrate 10 aprile 2017 - Termini per la conservazione dei documenti rilevanti ai fini tributari; l'Agenzia precisa che il termine per la conservazione di tutti i documenti informatici, anche quelli rilevanti a fini IVA, deve essere eseguita entro il terzo mese successivo al termine di presentazione delle dichiarazioni annuali, da intendersi, in un'ottica di semplificazione e uniformità del sistema, con il termine di presentazione delle dichiarazioni dei redditi;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali

ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;

- Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013, Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico, oppure in caso di conservazione digitale, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- Decreto Presidente del Consiglio dei Ministri 13 novembre 2014, Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23 -bis, 23 -ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82.
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
- Artt. 19-22 del Decreto Legge 22 giugno 2012, n. 83 ("Misure urgenti per la crescita del Paese"), convertito, con modificazioni, dalla Legge 7 agosto 2012, n. 134, con cui è stata istituita la "Agenzia per l'Italia Digitale" (AgID);
- Deliberazione CNIPA 21 maggio 2009, n. 45 – Regole per il riconoscimento e la verifica del documento informatico;
- Misure minime di sicurezza ICT emanate dall'AgID con Circolare del 18 aprile 2017, n. 2/2017;
- Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate (emanate da AgID con determinazioni n. 121 e 147 del 2019);
- Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, (emanate da AgID con determinazioni n. 407/2020 e n. 371/2021 e s.m.i.)
- Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici pubblicato il 25 giugno 2021 con determinazione AgID n. 455/2021. Tale Regolamento definisce i nuovi criteri per la fornitura del servizio di conservazione dei documenti informatici, fissando in un apposito allegato i requisiti generali nonché i requisiti di qualità, di sicurezza e organizzazione necessari per la fornitura del servizio. Composto di due allegati tecnici, il Regolamento è emanato secondo quanto previsto dall'articolo 34, comma 1-bis del Decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020 ed entrerà in vigore il 1° gennaio 2022, data a partire dalla quale è abrogata la Circolare n. 65/2014 "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".

2.2. STANDARD DI RIFERIMENTO

Nel rispetto degli standard e delle specifiche tecniche di cui all'allegato 4 delle *Linee guida* l'attività di conservazione si basa sui seguenti standard:

- EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
- EAD (3)/ISAD (G);
- 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;
- ISO 14721:2012 - OAIS *(Open Archivai Information System),* Sistema informativo aperto per l'archiviazione;
- ISO 15836:2009 - *Information and documentation - The Dublin Core metadata element set*, Sistema di metadati del Dublin Core;
- ISO/IEC 27001:2013 - *Information technology - Security techniques - Information security management systems - Requirements,* Requisiti di un ISMS *(Information Security Management System*);
- PREMIS - *PREservation Metadata: Implementation Strategies*;
- SCONS2/EAG/ISDIAH;
- SIARD - *Software Independent Archiving of Relational Databases*;
- UNI 11386:2010 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

Per l'elaborazione del presente documento, sono stati presi in considerazione anche gli standard di seguito elencati:

- ISAAR (cpf) - International Standard archival authority record for corporate bodies, persons and families;
- ISAD (G) - General international standard archival description;
- ISO 16363:2011 - Audit and certification of trustworthy digital repositories;
- ISO 23081 - 1:2006 - Information and documentation - records management processes - metadata for records;
- ISO 20104 - Space data and information transfer systems - Producer-Archive Interface Specification (PAIS)
- ISO 20652 - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard;
- ISO/CD TR 26102 - Requirements for long-term preservation of electronic records;
- ISO/TR 18492 - Long-term preservation of electronic document-based information;
- Iso/Iec 17021:2006 - Conformity assessment - Requirements for bodies providing audit and certification of management system;
- Mag - Metadati amministrativi e gestionali;
- METS - Metadata Encoding and Transmission Standard;
- Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018
- Moreq - Model Requirements for Electronic Records Management;
- Pronom - registro internazionale sui formati idonei alla conservazione a lungo termine;
- Rlg - Nara Task force on digital repository certification: Audit checklist for certifying digital repositories.

3. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE, RUOLI E RESPONSABILITÀ

ruoli	attività di competenza	struttura	soggetto	eventuali deleghe
Responsabile del servizio di conservazione	• Gestione amministrativa del sistema di conservazione dei documenti informatici (SCDI). • Autenticazione per lotti dei dati da parte del Responsabile del SCDI o di uno dei suoi delegati, mediante apposizione della propria firma digitale. • Scarto dei pacchetti di archiviazione, previa autorizzazione delle Autorità archivistiche, sulla base del Massimario di conservazione e di scarto Di concerto con il Servizio Sviluppo informatico: • Governo della gestione del Sistema di Conservazione • Verifica periodica di conformità a normativa e standard di riferimento. Di concerto con il Servizio Sviluppo informatico: • definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;	**Servizio Gestione dell'informazione**	**Capo Servizio**	Personale dell'Area Manageriale e Alte professionalità formalmente delegato dal Capo del Servizio Gestione dell'informazione
Responsabile Sicurezza dei sistemi per la conservazione	• rispetto e monitoraggio dei requisiti di sicurezza del Sistema di Conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	**Gestione sistemi informatici**		
Titolare del trattamento dei dati personali	• Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali	**Banca d'Italia nel suo complesso**	**Direttore generale**	Servizio Organizzazione

Responsabile sistemi informativi per la conservazione	• Gestione tecnica del SCDI (applicazione informatica, piattaforma tecnologica e archivi di dati). • acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento; • preparazione e gestione del pacchetto di archiviazione; • su richiesta, preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche Di concerto con il Servizio Gestione dei sistemi informatici: • monitoraggio del sistema di conservazione	**Servizio Sviluppo Informatico**	**Capo Servizio**	
Responsabile sviluppo e manutenzione del sistema di conservazione	• conduzione e manutenzione del sistema di conservazione; • *change management;*	**Servizio Sviluppo Informatico**	**Capo Servizio**	

4. OGGETTI SOTTOPOSTI A CONSERVAZIONE

4.1. CLASSI DOCUMENTALI OGGETTO DI CONSERVAZIONE

Sono sottoposti a conservazione tutti i documenti gestiti nel SGDD completi dei relativi metadati.

Le classi documentali oggetto di conservazione sono:

- "Esterni" (Ambito: Protocollo - in arrivo)
- "Interni" (Ambito: Protocollo - in uscita e interni)
- Notifica in uscita (Ambito: Registro Documenti fiscalmente rilevanti)
- Notifica in entrata (Ambito: Registro Documenti fiscalmente rilevanti)
- Fattura nazionale (Ambito: Registro Documenti fiscalmente rilevanti)
- Fattura estera (Ambito: Registro documenti fiscalmente rilevanti)
- Autofattura - Intra (Ambito: Registro documenti fiscalmente rilevanti)
- Fattura (Ambito: Fatture attive)
- Notifica (Ambito: Fatture attive)
- Esterni eProc (Ambito: Protocollo *e-procurement* - in arrivo)
- Report protocolli giornalieri - (Ambito: Registro mensile /Registro giornaliero di protocollo)

Per ciascun oggetto sottoposto a conservazione, sono conservati il *file* digitale e i metadati.

Per quanto riguarda il file digitale, i documenti sono conservati nel formato descritto e disciplinato nel *Manuale di gestione documentale*.

Di seguito l'elenco dei formati accettati dal sistema di conservazione Virgilio.

Formato	Proprietario/Gestore del formato	Estensione	Tipo Mime	Aperto	Visualizzatore
PDF, PDF/A	Adobe Systems	.pdf	Application/pdf	Sì	Adobe Reader
TIFF	Aldus Corporation	.tif	Image/tiff	No	Visualizzatori di immagini
JPEG	Joint photographic experts group	.jpeg .jpg	Image/jpeg	Sì	Visualizzatori di immagini
Office, Open XML	Microsoft	.docx, .xlxs, .pptx	MIME	Sì	Visualizzatori compatibili
XML	W3C	.xml	Application/xml text/xml	Sì	Web browser
TXT	txt/plain	.txt	ASCII, UTF-8, UNICODE	Sì	Visualizzatori di testo
PEC, EMAIL	Vari	.eml	RCF 2822/MIME	No	Client di posta elettronica che supportano la visualizzazione di file .eml
ODF	Consorzio OASIS OpenOffice.org	.ods, .odp, .odg, .odb	Application/vnd.oasis opendocument.text	Sì	Visualizzatori di immagini

Nei paragrafi seguenti vengono specificati i metadati oggetto di conservazione digitale per ciascuna classe documentale.

4.1.1. Esterni (Ambito: Protocollo - in arrivo)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto Conservatore
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Mittente	SÌ	Mittente o destinatario
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Assegnato a	SÌ	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Archivio	SÌ	Registro Ufficiale
Titolo	SÌ	Codice di classificazione
Classe	SÌ	Codice di classificazione
Sottoclasse	SÌ	Codice di classificazione
Data Ricezione	NO	
Protocollo Mittente	NO	
Data - Protocollo Mittente	NO	
Formato	NO	Cartaceo/Elettronico
Procedimento Amministrativo	NO	

4.1.2. Interni (Ambito: Protocollo - in Uscita e Interni)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Destinatario	SÌ	Destinatario
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Mittente	SÌ	Soggetto/ufficio titolare del procedimento - Struttura/Filiale
Impronta	SÌ	Impronta
Archivio		Registro Ufficiale
Titolo	SÌ (Classificazione)	Codice di classificazione
Classe	SÌ (Classificazione)	Codice di classificazione
Sottoclasse	SÌ (Classificazione)	Codice di classificazione
Protocollo Mittente	NO	
Data Protocollo Mittente	NO	
Unità	NO	
Formato	NO	
Tipo di Spedizione	NO	
Tipo Comunicazione	NO	
Copie Cartacee	NO	SÌ/NO
Procedimento Amministrativo	NO	

4.1.3. Notifica in uscita (Ambito: Registro Documenti fiscalmente rilevanti)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Oggetto (Esito e descrizione- tipo ricevuta)	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Mittente (o Codice struttura, se presente)	SÌ	Soggetto/ufficio titolare del procedimento
Unità (o Codice ufficio, se presente)	NO	
Impronta	SÌ	Impronta
Identificativo SDI	NO	
Formato	NO	
Stato	NO	
Fornitore	NO	
Partita IVA - Codice fiscale	NO	
Riferimento Fattura	NO	
Data Fattura	NO	
Nome *File*	NO	

4.1.4. Notifica in entrata (Ambito: Registro Documenti fiscalmente rilevanti)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Mittente	SÌ	Mittente del documento (es. SDI)
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Oggetto (esito e descrizione - tipo ricevuta)	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Struttura -(o Codice Struttura, se presente)	SÌ	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Formato	NO	
Data Ricezione	NO	
Stato	NO	
Nome *File*	NO	
Identificativo SDI	NO	

4.1.5. Fattura nazionale (Ambito: Registro Documenti fiscalmente rilevanti)

Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Mittente	SÌ	Mittente del documento (es. SDI)
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Struttura - (o Codice Struttura, se presente)	SÌ	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Data Ricezione	NO	
Archivio	NO	
Fornitore	NO	
Partita Iva	NO	
Codice Fiscale	NO	
Riferimento Fattura	NO	
Data Fattura	NO	
Formato	NO	
Stato Documento	NO	
Progressivo univoco	NO	

4.1.6. Fattura estera (Ambito: Registro documenti fiscalmente rilevanti)

Metadati inviati in conservazione digitale	**Obbligatorietà**	**Riferimento normativa**
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Fornitore	SÌ	Mittente
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Struttura - (o Codice struttura, se presente)	NO	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Partita Iva	NO	
Riferimento Fattura	NO	
Data Fattura	NO	
Formato	NO	
Stato Documento	NO	

4.1.7. Autofattura - Intra (Ambito: Registro documenti fiscalmente rilevanti)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Fornitore	SÌ	Mittente
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Struttura - (o Codice ufficio, se presente)	NO	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Partita Iva	NO	
Codice Fiscale	NO	
Riferimento Fattura	NO	
Data Fattura	NO	
Rif. N. Protocollo	NO	
Rif. Data Protocollo	NO	
Stato Documento	NO	

4.1.8. Fattura (Ambito: Fatture attive)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Mittente	SÌ	Soggetto/ufficio titolare del procedimento
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Destinatario	SÌ	Destinatario
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Impronta	SÌ	Impronta
Tipo Spedizione	NO	
Denominazione	NO	
Data Registrazione	NO	
Numero Documento	NO	
Partita IVA	NO	
Codice Fiscale	NO	
Archivio	NO	
Tipologia documentale	NO	

4.1.9. Notifica (Ambito: Fatture attive)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Mittente	SÌ	Mittente del documento (es. SDI)
Protocollo	SÌ	Numero di protocollo
Data Protocollo	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Assegnato a	NO	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Archivio	NO	
Tipologia documentale	NO	
Formato	NO	
Data Ricezione	NO	
Stato	NO	

4.1.10. Esterni eProc (Ambito: Protocollo *e-procurement* - in arrivo)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Protocollo *e- procurement*	SÌ	Numero di protocollo
Data Protocollo *e- procurement*	SÌ	Data di protocollo
Mittente	SÌ	Mittente o destinatario
Oggetto	SÌ	Oggetto
Allegati	NO	Identificazione degli allegati
Assegnato a	SÌ	Soggetto/ufficio titolare del procedimento
Impronta	SÌ	Impronta
Archivio	SÌ	Registro Ufficiale
Titolo	SÌ	Codice di classificazione
Classe	SÌ	Codice di classificazione
Sottoclasse	SÌ	Codice di classificazione
Tipo esterno	NO	
Formato	NO	Cartaceo/Elettronico
Procedimento amministrativo	NO	

4.1.11.Report protocolli giornalieri (Ambito: Registro mensile/Registro giornaliero di protocollo)

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa[3]
Id Documento	SÌ	Identificativo
Denominazione Amministrazione	SÌ	Amministrazione titolare
Soggetto produttore	SÌ	Codice IPA
Soggetto conservatore	SÌ	Soggetto conservatore
Numero Progressivo del registro	SÌ	Numero di protocollo
Data di creazione del registro	SÌ	Data di protocollo
Oggetto	SÌ	Oggetto
Codice identificativo del Registro	NO	Identificazione degli allegati
Responsabile gestione documentale	NO	Soggetto/ufficio titolare del procedimento
Classificazione	NO	Codice di classificazione
Impronta	SÌ	Impronta
Protocollo iniziale (numero prima registrazione)	SÌ	
Protocollo finale (numero ultima registrazione)	SÌ	
Data prima registrazione e data ultima registrazione	NO	

[3] Per il registro giornaliero di protocollo si fa riferimento al set di metadati fornito dall'AgID nel documento "Istruzioni per la produzione del registro giornaliero di protocollo".

4.2. FASCICOLI

Un documento viene immesso nel sistema di conservazione solo dopo il suo inserimento in un fascicolo. Per fascicolo si fa riferimento all'aggregazione documentale di cui all'all.5 delle *Linee Guida AgID*. L'inserimento di ciascun documento oggetto di conservazione nel relativo fascicolo di appartenenza viene effettuata dal soggetto/ufficio titolare del procedimento, attraverso apposite funzioni sul SGDD.

In tabella sono riportati i metadati dell'aggregazione documentale "Fascicoli".

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
IdAgg	SÌ	ID Aggregazione
Tipologia fascicolo	SÌ	Tipologia Fascicolo
Soggetti	SÌ	Soggetti
Assegnazione	SÌ	Assegnazione
DataApertura	SÌ	Data apertura
Classificazione	SÌ	Classificazione
Progressivo	SÌ	Progressivo
Chiave descrittiva	SÌ	Chiave descrittiva - Oggetto
Data chiusura	NO	DataChiusura
Procedimento amministrativo	SÌ	Procedimento amministrativo
Indice documenti	SÌ	Indice documenti
Posizione fisica aggregazione documentale	Obbligatoria solo per i fascicoli ibridi	Posizione fisica aggregazione documentale
IdAggPrimario	NO	Identificativo dell'Aggregazione Primaria
Tempo di conservazione	SI	Tempo di conservazione
Note	NO	Note

Solo per la tipologia fascicolo = "Procedimento amministrativo" sono inoltre presenti i seguenti ulteriori metadati.

Metadati inviati in conservazione digitale	Obbligatorietà	Riferimento normativa
Preparatoria – Data inizio fase	NO	Procedimento Amministrativo
Preparatoria – Data fine fase	NO	Procedimento Amministrativo
Istruttoria – Data inizio fase	NO	Procedimento Amministrativo
Istruttoria – Data fine fase	NO	Procedimento Amministrativo
Consultiva – Data inizio fase	NO	Procedimento Amministrativo
Consultiva – Data fine fase	NO	Procedimento Amministrativo
Decisoria o deliberativa – Data inizio fase	NO	Procedimento Amministrativo
Decisoria o deliberativa – Data fine fase	NO	Procedimento Amministrativo
Integrazione dell'efficacia – Data inizio fase	NO	Procedimento Amministrativo
Integrazione dell'efficacia – Data fine fase	NO	Procedimento Amministrativo

5. IL PROCESSO DI CONSERVAZIONE

5.1. ASPETTI GENERALI

Il processo di conservazione avviene con cadenza periodica secondo le regole tecniche stabilite dalla normativa ed è articolato nelle seguenti fasi:

- memorizzazione dei documenti informatici;
- verifica del corretto svolgimento del processo di memorizzazione;
- autenticazione per lotti dei dati da parte del Responsabile del SCDI[4] mediante firma digitale;
- attribuzione automatica del riferimento temporale che attesta la conclusione del processo.

I documenti informatici sono conservati in ordine cronologico e identificati per numero di protocollo. Alla fine del riversamento il SCDI produce il Registro di protocollo. I dati e le informazioni vengono memorizzati su supporti informatici realizzati in due copie autentiche, conservate in luoghi diversi[5].

L'accesso ai dati, in formato consultabile, è consentito al Responsabile del SCDI e alle persone da lui autorizzate. L'esibizione a soggetti esterni alla Banca che ne abbiano titolo di documenti presenti nel SCDI può essere effettuata mediante copia cartacea autenticata o in formato elettronico non modificabile, previa richiesta al Servizio GIN[6] che li renderà disponibili nella modalità richiesta.

5.2. MODELLO ORGANIZZATIVO INTERNO

Il modello organizzativo adottato dalla Banca per la conservazione digitale è coerente con lo standard internazionale OAIS per la conservazione di oggetti digitali a lungo termine[7].

Nel sistema di conservazione operano tre soggetti con diversi ruoli e competenze:

- il produttore è identificato negli addetti o nei sistemi informativi che forniscono i documenti da conservare;
- il responsabile è identificato nel Capo del Servizio Gestione dell'Informazione, che definisce e attua le politiche complessive del processo e del sistema e ne governa la gestione con piena responsabilità. Può delegare parte delle proprie funzioni ad addetti che abbiano maturato competenze ed esperienza nelle attività di gestione documentale;
- l'utente è identificato negli addetti o sistemi che interagiscono con il sistema di conservazione al fine di ricercare le informazioni di interesse.

L'Istituto, ai sensi dell'art. 44 del CAD e dell'art. 4.3 delle *Linee Guida AgID*, gestisce al proprio interno la conservazione dei documenti informatici dallo stesso prodotti e acquisiti attraverso il sistema di conservazione denominato Virgilio, fornito da Siav S.p.A..

Il mantenimento nel tempo del valore legale dei documenti e i processi di verifica/integrità dei supporti virtualizzati (*LifeCycle*) sono assicurati da una serie di servizi automatici di gestione e manutenzione dell'archivio digitale tra cui:

- gestione multi-azienda/multi-ente, che permette di suddividere l'archivio digitale per azienda o ente; per ciascuno di essi è possibile attribuire diversi profili e ruoli per l'accesso ai dati e l'esecuzione delle attività di conservazione;
- gestione per ambiti, che consente di organizzare logicamente l'archivio definendo ambiti documentali distinti (relativi ad esempio alle diverse tipologie documentali);
- gestione per classi o tipologie documentali, che permette di rintracciare un documento

[4] Le azioni consentite al Responsabile possono sempre essere compiute dal soggetto delegato.
[5] I documenti analogici dai quali è stata tratta la copia digitalizzata sono conservati dalla Struttura che ne ha curato la digitalizzazione.
[6] La richiesta deve essere inviata alla casella funzionale GIN.Archivio@bancaditalia.it.
[7] Conformemente alla previsione di cui all'allegato 4 delle *linee guida AgID*.

tramite una serie di dati allo stesso associati.

Il sistema di conservazione Virgilio gestisce il *workflow* relativo a tutte le fasi del processo conservativo che vengono controllate e monitorate.

Il processo di conservazione descritto nel presente *Manuale* viene costantemente aggiornato (con contestuale aggiornamento del *Manuale* stesso) a seguito di interventi normativi, introduzione di nuove tipologie sottoposte a conservazione o modifiche al modello organizzativo e/o al processo di conservazione.

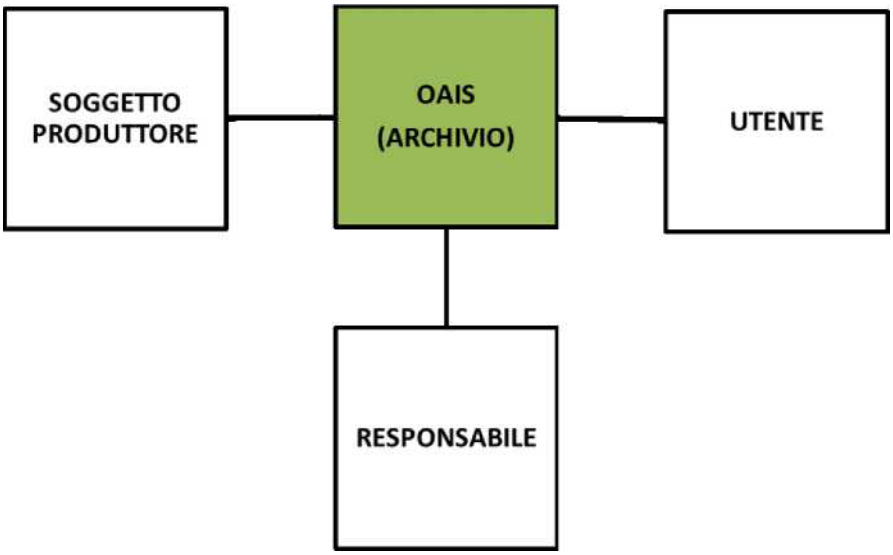

Figura 9- Virgilio - modello OAIS

5.3. IL PROCESSO DI CONSERVAZIONE

Gli oggetti digitali sottoposti al processo di conservazione sono organizzati in pacchetti informativi, intesi come contenitori che racchiudono uno o più oggetti da trattare (documenti informatici, aggregazioni informatiche) comprensivi delle informazioni per la loro interpretazione e rappresentazione.

I pacchetti informativi contengono non solo il documento e/o l'aggregazione informatica ma anche i metadati necessari a garantirne la conservazione e l'accesso nel lungo periodo.

Secondo il modello OAIS, il SCDI adotta procedure in grado di garantire la conservazione nel lungo periodo monitorando tutte le attività inglobate nelle tre fasi principali di:

- immissione nel sistema di conservazione;
- certificazione e conservazione;
- distribuzione ed esibizione all'utenza.

La trasmissione delle informazioni tra il produttore e il Sistema di conservazione e tra questo e l'utente avviene attraverso pacchetti informativi che a seconda della loro funzione si distinguono in tre tipologie:

- Pacchetto di versamento (PdV);
- Pacchetto di archiviazione (PdA);
- Pacchetto di distribuzione (PdD).

Nei successivi paragrafi sono illustrate le principali fasi del processo di gestione e conservazione[8] (schematizzato nella Figura 10) dal momento della trasmissione del PdV da parte del soggetto produttore fino alla creazione del PdD.

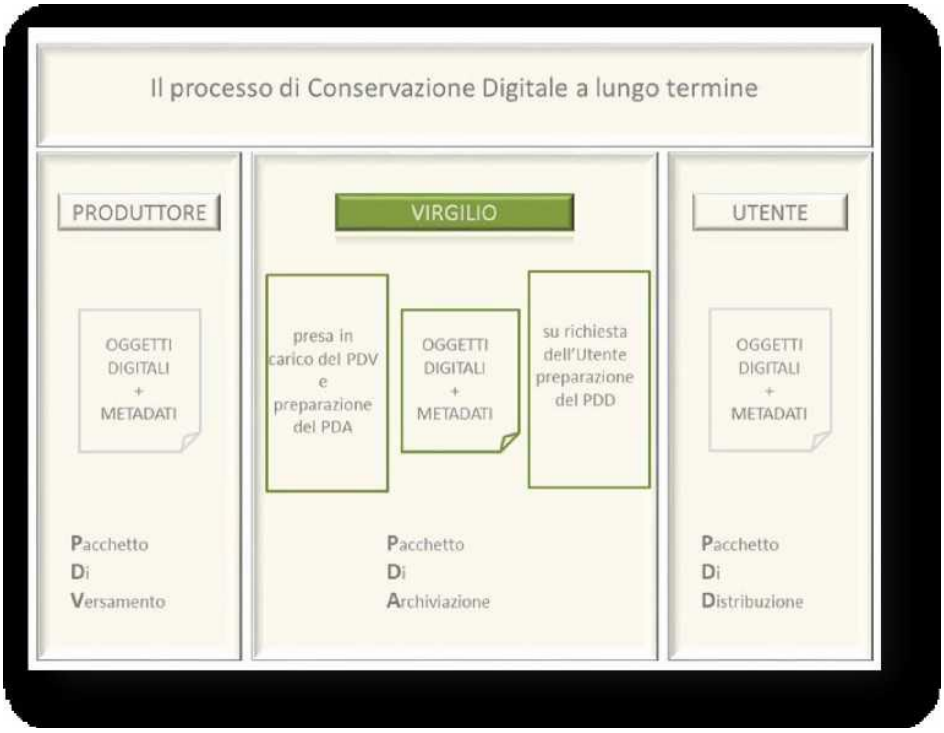

Figura 10- Schema del processo di conservazione

5.4. CREAZIONE DEL PACCHETTO DI VERSAMENTO (PDV)

Il PdV è l'insieme di oggetti digitali e metadati (risorse digitali) provenienti dal soggetto produttore e versati nel sistema di conservazione. Il processo di acquisizione individua le attività finalizzate all'accettazione delle risorse digitali versate dal soggetto produttore e alla loro preparazione per l'inserimento nell'archivio[9].

Viene verificata in modo automatico la presenza dei metadati obbligatori e aggiuntivi associati alle tipologie/aggregazioni documentali informatiche da versare nel sistema e, se presenti, si procede alla lavorazione del PdV; altrimenti è effettuata una pre-lavorazione per attribuire i metadati al documento.

I metadati che devono essere presenti in un documento informatico sono:

- Identificativo
- Modalità di formazione
- Tipologia documentale
- Dati di registrazione
- Chiave descrittiva
- Soggetti
- Allegati
- Classificazione

[8] Qualora intervengano modifiche/integrazioni/correzioni inerenti il processo di conservazione è compito del Responsabile del servizio di conservazione riportarle nel presente *Manuale*.
[9] Il Responsabile del servizio di conservazione è responsabile del coordinamento dell'intero processo e del monitoraggio delle attività.

- Riservato
- Identificativo del formato
- Verifica
- IdAgg
- Identificativo Documento Primario
- Nome Del Documento
- Versione del documento
- Tracciature modifiche documento
- Tempo di conservazione
- Note
- data di chiusura;
- oggetto (sintesi del contenuto di un documento);
- soggetto produttore;
- destinatario.

I metadati per il documento amministrativo informatico sono:

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

I documenti digitali vengono trasferiti sul *filesystem* di Virgilio tramite connettore "nativo" al SGDD. I documenti sono trasferiti nell'area dedicata di presa in carico; i *file* da elaborare vengono suddivisi per tipologia documentale e scaricati in cartelle appositamente predisposte. Viene verificata la presenza di ulteriori metadati inerenti il contesto e l'integrità degli oggetti/aggregazioni documentali versati nel sistema ovvero delle informazioni descrittive per la conservazione a lungo termine dei PdA.

A ogni documento versato in conservazione il sistema associa automaticamente una serie di metadati di processo; tra questi assume particolare importanza il codice alfanumerico identificativo univoco (d'ora in poi ID univoco[10]) del soggetto produttore assegnato ad ogni oggetto/aggregazione documentale informatica.

L'ID univoco ha una duplice funzione:

- segna la tracciabilità del documento durante l'intero processo di conservazione;
- identifica in modo univoco il soggetto produttore.

Il soggetto produttore, dopo aver trasferito il PdV nell'area di presa in carico, invia l'impronta (contenente l'*hash*) dei documenti inserendola tra i metadati. Al momento della presa in carico del PdV il sistema ricalcola automaticamente l'impronta di ogni documento e la confronta con quella indicata nei metadati. In questo modo viene garantita l'integrità dei documenti in quanto si ha la sicurezza che non siano intervenute perdite di dati durante le fasi di lavorazione.

[10] L'ID univoco è un codice di 20 caratteri alfanumerici: i primi 6 caratteri identificano il soggetto produttore e sono comuni a tutti gli oggetti documentali versati nel sistema da parte del medesimo produttore. I restanti 14 caratteri sono univoci per ogni documento versato nel sistema. L'identificativo del soggetto produttore coincide con il codice IPA della Banca.

5.5. FASE DI VERSAMENTO

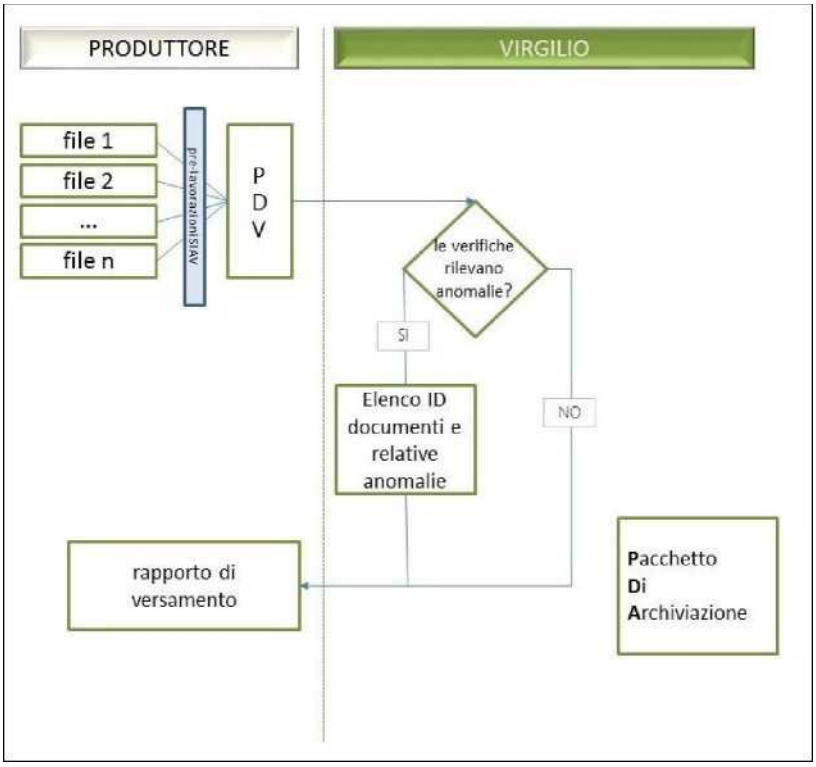

Figura 11- Fase di versamento

La Figura 11 illustra il flusso di lavoro dell'intera fase di versamento, dal trasferimento dei documenti/aggregazioni informatiche da parte del soggetto produttore fino alla formazione del PdA.

5.6. VERIFICHE, ECCEZIONI E RAPPORTO DI VERSAMENTO

L'acquisizione dei PdV nel sistema di conservazione avviene a cadenza programmata. Per ogni pacchetto ricevuto, Virgilio verifica automaticamente che il contenuto sia rispondente a quanto previsto e confronta l'impronta ricalcolata del documento con quella inviata dal soggetto produttore, per verificare l'integrità della documentazione trasmessa.

Qualora venissero rilevate eventuali anomalie il sistema provvede a notificarle al produttore.

Il Responsabile del servizio di conservazione dispone lo svolgimento di periodici controlli sui documenti e sulle aggregazioni documentali presenti nel sistema tramite i rapporti di versamento prodotti dal SCDI, in modo da identificare eventuali anomalie rispetto ai formati destinati alla conservazione. È comunque possibile modificare/integrare l'elenco dei formati ammessi, stabilendo eventuali eccezioni[11].

I controlli effettuati da Virgilio sui documenti e sulle aggregazioni informatiche versate dal soggetto produttore comprendono anche le verifiche volte ad identificare il formato dei *file*[12].

[11] Le eccezioni fanno riferimento alla necessità, da parte del soggetto produttore, di conservare i documenti in formati non compatibili con la conservazione a lungo termine e sui quali non sia possibile effettuare una conversione di formato senza alterarne la leggibilità e la forma. In questo caso il Responsabile del servizio di conservazione ammette tali documenti nel sistema di conservazione specificando che non è possibile assicurarne l'integrità e la leggibilità per la conservazione a lungo termine.

[12] Comunemente il formato di un file è riconosciuto attraverso la sua estensione; ai fini di una corretta identificazione questo non è però sufficiente in quanto l'estensione di un file può essere modificata, volontariamente o involontariamente, ad esempio a causa di una ridenominazione accidentale o per l'intervento di un virus. In ogni caso, anche se eseguita correttamente, l'identificazione del file tramite l'estensione permette di riconoscere solo la famiglia di formati cui

Per la verifica dei formati[13] all'interno di Virgilio si utilizzano dei *tool* di riconoscimento basati sull'identificazione di particolari sequenze composte in modo variabile da 2 a 10 *byte* che si trovano in specifiche posizioni del *file* (comunemente all'inizio).

Effettuata la verifica del formato, il sistema genera automaticamente il rapporto di versamento, che contiene un riferimento temporale.

Il rapporto di versamento è un *file* in formato .xml che attesta l'esito di versamento del PdV trasferito dal Titolare al SDC.

In sostanza il RdV, per ciascun *file* incluso nel PdV, riporta le seguenti informazioni:

- URN, stringa univoca che identifica il documento;
- metadati del singolo *file*;
- impronta del *file*.

Il Sistema di conservazione genera in automatico il RdV che viene reso disponibile al Titolare; contestualmente alla generazione del RdV, viene segnalato anche l'esito del conferimento che può essere positivo, nel caso in cui non siano state evidenziate anomalie, oppure negativo se al contrario il sistema identifichi un errore o un'anomalia del PdV.

I rapporti di versamento vengono salvati dal sistema e versati in conservazione; Virgilio raggruppa la tipologia documentale "rapporto" che, per ogni soggetto produttore, include tutti i rapporti di versamento.

5.7. RIFIUTO DEL PACCHETTO DI VERSAMENTO

Nel caso in cui le verifiche diano esito negativo il sistema segnala la presenza di un'anomalia[14] e rifiuta i documenti. Virgilio segnala i documenti anomali contenuti nel PdV all'interno del rapporto di versamento per il successivo intervento di risoluzione dell'anomalia, rielaborazione e reinvio del PdV.

5.8. PACCHETTO DI ARCHIVIAZIONE

Il pacchetto di archiviazione (PdA) è il pacchetto di informazioni destinato alla conservazione a lungo termine ed è un'aggregazione di quattro tipi di oggetti informativi:

- il contenuto informativo *(content information* - CI), che include i dati di interesse primario, ossia le informazioni destinate alla conservazione e le informazioni di rappresentazione associate, ad es. uno specifico documento XML e lo schema XML relativo;
- le informazioni descrittive per la conservazione (PDI), che includono le informazioni di identificazione dell'oggetto digitale, di contesto, provenienza e integrità;
- le informazioni sull'impacchettamento (*packaging information* - PI), cioè le informazioni sulla composizione del pacchetto informativo (al fine di collegare l'oggetto digitale e i metadati associati);
- le informazioni descrittive, finalizzate a sostenere l'accesso alle risorse/contenuto informativo mediante strumenti di ricerca o di recupero.

Il PdA si ottiene dalla trasformazione di uno o più PdV attraverso le operazioni di conservazione a lungo termine (*archival storage*) delle risorse digitali affidate a Virgilio.

La componente *archival storage* conserva i documenti garantendo l'integrità e la fruibilità a lungo termine delle sequenze di bit (*bit stream*) e ne permette il recupero per eventuali consultazioni.

---

appartiene e non la specifica versione, utile ai fini di una corretta rappresentazione del file.

[13] Per la lista dei formati accettati fare riferimento al *Manuale di gestione documentale*

[14] Si hanno documenti anomali in presenza di corruzione o perdita di dati (ad esempio i dati sono memorizzati su formati non compatibili, metadati mancanti, documenti con firma scaduta).

Il Responsabile della conservazione della Banca dispone il periodico aggiornamento dei PdA per la migrazione dei formati. Inoltre, d'accordo con i responsabili della sicurezza e dei sistemi informativi della Banca, aggiorna le politiche di recupero in caso di incidente (*disaster recovery*).

Il PdA (Figura 12) prevede una specifica strutturazione in formato XML secondo quanto definito dallo standard UNI SinCRO[15].

Le informazioni PDI costituiscono metadati fondamentali per la conservazione a lungo termine dei documenti; tali informazioni sono articolate in cinque aree:

- Provenienza: informazioni relative alla provenienza del contenuto informativo ovvero dati sulla natura giuridica, organigramma e funzionigramma del soggetto produttore e tracciabilità dei cambiamenti avvenuti;
- Identificazione: informazioni che identificano in maniera univoca gli oggetti digitali (ad es. data e numero di protocollo);
- Integrità: informazioni sulla verifica della firma e impronta dell'autore del documento/aggregazione informatica;
- Contesto: informazioni che mostrano le relazioni esistenti tra il contenuto informativo e il contesto in cui è stato prodotto (es. l'ID del documento, il Piano di classificazione);
- Diritti: informazioni sui diritti di accesso al contenuto informativo.

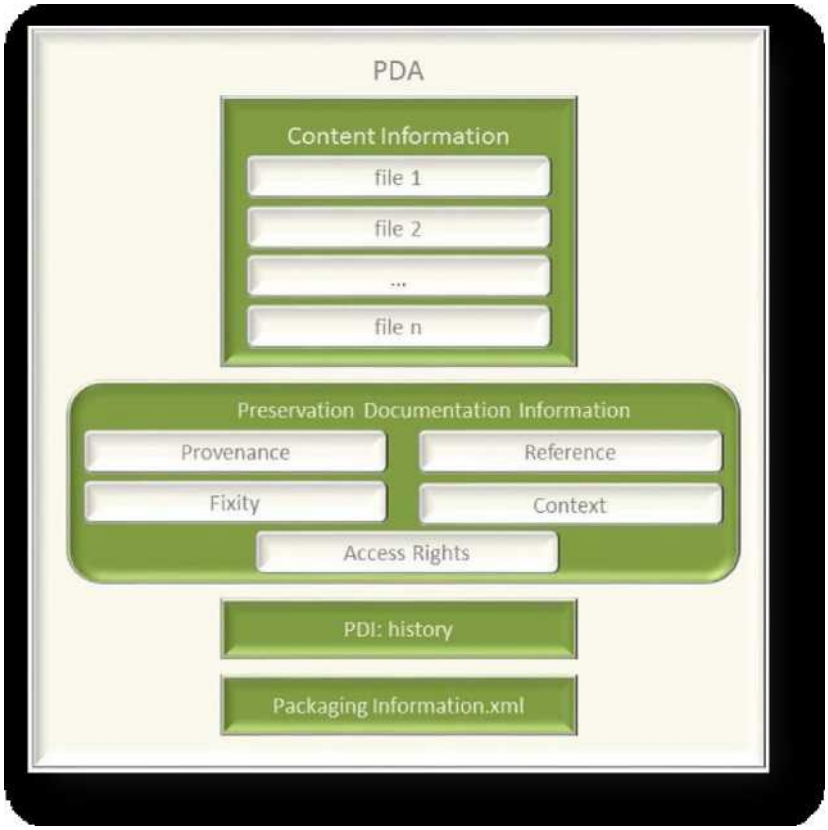

Figura 12- Schema del PdA

[15] Tale standard definisce, nel rispetto del modello OAIS, una struttura di dati XML che consente di predisporre sia le informazioni identificative minime (previste dal legislatore) sia un'infrastruttura generale in grado di gestire tutte le informazioni archivistiche necessarie al processo di formazione e tenuta dei documenti informatici in modo da assicurare l'interoperabilità tra sistemi e la conservazione a lungo termine.

5.9. CREAZIONE E STRUTTURA

Il sistema di conservazione gestisce esclusivamente PdA omogenei, che sono formati accorpando documenti informatici della stessa tipologia.

Virgilio scompatta i PdV suddividendo i documenti in base alla tipologia documentale cui appartengono; per ogni tipologia documentale viene formato un PdA (Figura 13).

Se nel PdV sono presenti documenti fiscali su cui vanno effettuati i controlli di continuità (ad esempio fatture), il sistema procede ad accorpare i documenti appartenenti alla stessa tipologia documentale e a ordinarli, effettuando successivamente i controlli sulla numerazione dei documenti. Se vengono riscontrate anomalie, il sistema provvede automaticamente a bloccare la formazione del PdA, a segnalare il problema e a richiedere un nuovo invio. Il sistema sospende il processo per quello specifico PdA fino all'invio del documento rettificato. Dopo il nuovo invio vengono effettuati di nuovo i controlli di continuità e, in caso di esito positivo, il sistema procede alla formazione del PdA.

Una volta formato, il PdA viene firmato digitalmente dal Responsabile del servizio di conservazione.

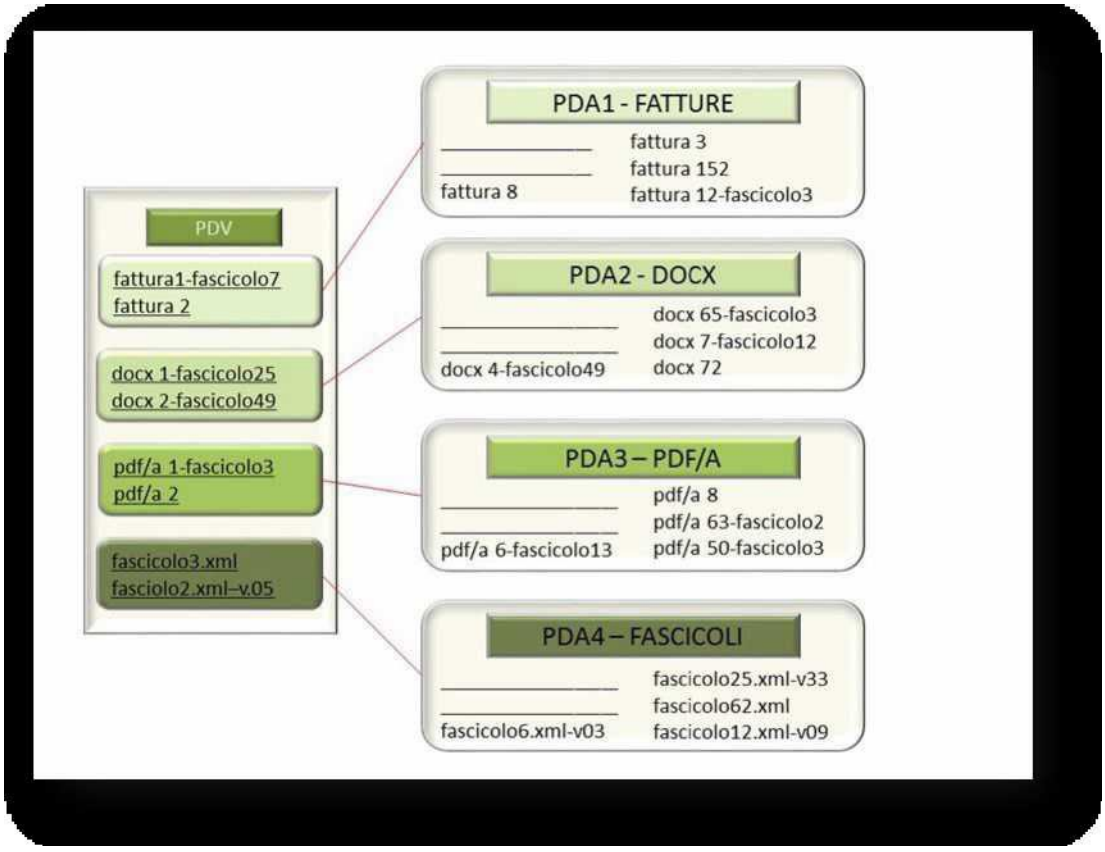

Figura 13- Formazione del PdA

5.10. L'INDICE DEL PACCHETTO DI ARCHIVIAZIONE

Il lotto di documenti sottoposti a conservazione viene riepilogato in un *file* di chiusura, detto Indice del Pacchetto di archiviazione (IPdA), il quale costituisce l'evidenza informatica associata ad ogni PdA.

Attraverso l'IPdA si può procedere alla verifica delle informazioni archivistiche necessarie al processo di tenuta dei documenti/aggregazioni informatiche e obbligatorie per assicurare le garanzie di affidabilità, integrità e autenticità nel lungo periodo.

Le informazioni archivistiche obbligatorie racchiuse in un IPdA sono:

- descrizione generale, che comprende l'identificativo univoco dell'IPdA e le informazioni relative all'applicazione che lo ha generato (nome e versione dell'applicativo e produttore del *software*). Nel caso di modifica del contenuto di un PdA già presente all'interno del sistema di conservazione, si includeranno nell'IPdA i riferimenti relativi ad esso;
- attributi del relativo PdA, che comprendono l'identificativo univoco del PdA e, eventualmente, i riferimenti che permettono di collegare tale PdA ad altri PdA presenti all'interno del sistema di conservazione come descritto al punto precedente;
- *file* gruppo, che permette di aggregare più oggetti documentali presenti all'interno del PdA indicandone l'identificativo univoco e l'impronta. Tale attributo consente di formare degli insiemi di oggetti sulla base di criteri funzionali;
- processo, attraverso il quale vengono inserite le informazioni riguardanti il processo di conservazione dello specifico PdA cui l'IPdA fa riferimento. Sono riportati i dati dei soggetti intervenuti durante il processo di formazione del PdA, le informazioni relative a data e ora di produzione dell'IPdA sotto forma di riferimento temporale; è previsto un campo *Extrainfo* in cui il sistema riporta le informazioni utili a richiamare i *log* di sistema salvati e conservati nel *database* Oracle.

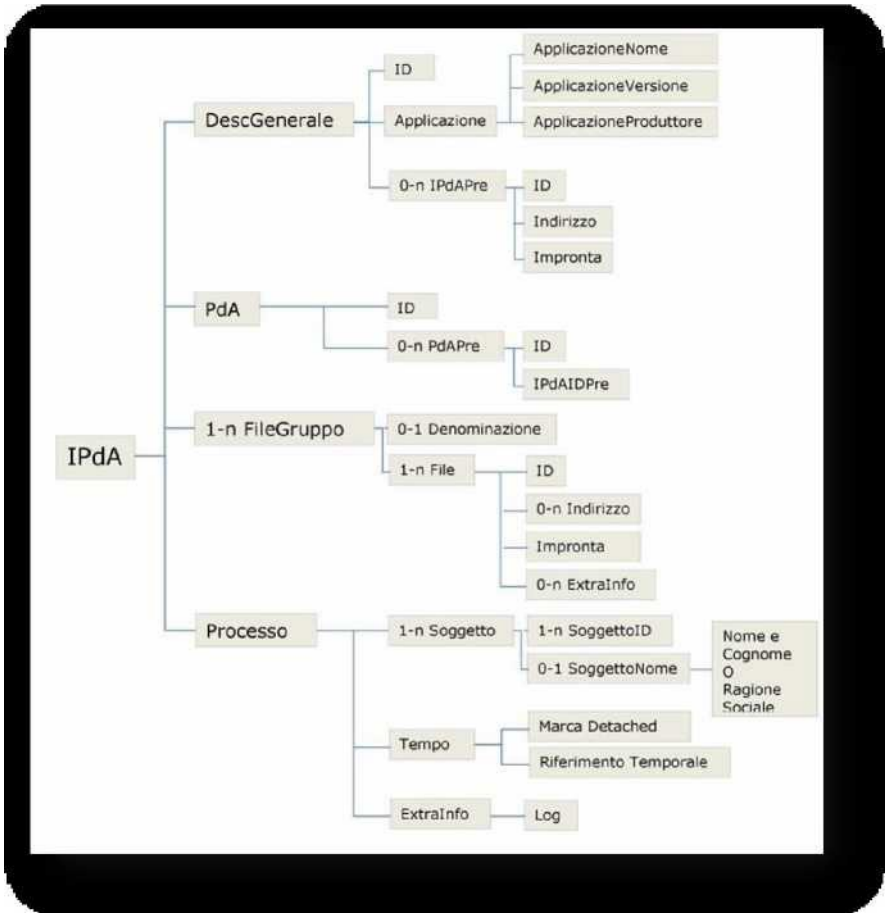

Figura 14-Struttura dell'IPdA

5.11. RICHIESTA DI ESIBIZIONE E DIRITTI D'ACCESSO

L'utente è la persona o il sistema che interagisce con il sistema di conservazione al fine di ricercare le informazioni di interesse.

Il documento conservato deve essere leggibile in qualunque momento e disponibile su richiesta anche su supporto ottico e/o analogico. La richiesta di esibizione deve essere inoltrata al Servizio GIN.

I soggetti produttori possono essere autorizzati ad accedere direttamente, tramite *username* e *password* forniti dal conservatore, alla *console web* di esibizione di Virgilio e a ricercare i documenti di interesse.

5.12. CREAZIONE ED ESIBIZIONE DEL PACCHETTO DI DISTRIBUZIONE

In base agli ID univoci forniti dal soggetto produttore al momento della richiesta, il sistema localizza i documenti conservati nei diversi PdA ed effettua un duplicato. I duplicati sono inseriti all'interno di un unico PdD, che viene firmato digitalmente dal Responsabile del servizio di conservazione e salvato nel formato di *file* immagine ISO; a questo punto il sistema produce il PdD. Virgilio restituisce un messaggio di avvenuta presa in carico in cui viene indicato il *link* del canale FTP o FTPS dal quale si può procedere a scaricare il *file* immagine ISO del PdD.

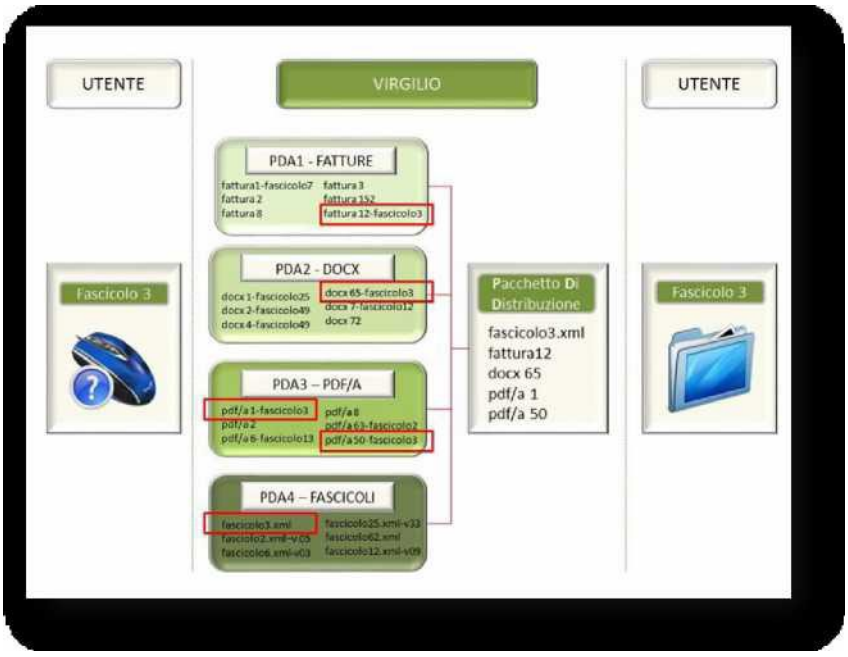

Figura 15- Schema del processo di esibizione

5.13. STRUTTURA DATI PER GLI OGGETTI DIGITALI E PER I METADATI

Le informazioni necessarie alla conservazione degli oggetti digitali, e relativi metadati, vengono organizzate in file XML conforme allo standard UNI SInCRO e salvate all'interno della base dati del SdC.

Per ogni tipologia di oggetti digitali sottoposti alla conservazione viene definito uno specifico set di metadati suddiviso, al suo interno, in due subset: metadati obbligatori[16] e facoltativi.

La memorizzazione dei metadati collegati al documento digitale avviene all'interno di un *file* XML conservato all'interno della base dati del SdC.

Parallelamente il documento digitale a cui fanno riferimento i predetti metadati e la sua impronta sono conservati in un *repository* dedicato all'interno della base dati del SCDI[17] e indicizzato per successive interrogazioni.

Nel caso del PdD il salvataggio avviene su *file system* e non all'interno della base dati. Il reperimento dell'oggetto digitale avviene in maniera trasparente se si utilizza il visualizzatore proprio del SCDI; in

[16] Con le *linee guida* entrate in vigore nel 2022 non si parla più di metadati minimi

[17] Il salvataggio è organizzato secondo una struttura di cartelle organizzata in base a soggetto produttore, data e ora del versamento.

alternativa è sempre possibile risalire al documento attraverso i suoi metadati per il tramite dell'IPdA[18] UNI SInCRO.

[18] Gli oggetti digitali saranno raggiungibili consultando direttamente l'IPdA ed il file, specificato nella sezione "*documentspath*" inserita in "mediainfo". L'accesso agli oggetti digitali avviene utilizzando come chiave di accesso l'indice del documento, specificato per ogni *file*, e la posizione nel *repository* del PdD, che viene estratta dal file indicato in "*documentspath*".

6. IL PROCESSO DI SELEZIONE E SCARTO DEI DOCUMENTI DIGITALI

Il processo di selezione e scarto include gli interventi finalizzati:

- alla conservazione senza limiti di tempo (SLT) della documentazione di interesse storico;
- allo scarto della restante documentazione dopo che questa ha maturato i tempi di conservazione previsti dal *Massimario di selezione e di scarto*[15], previa autorizzazione della Soprintendenza archivistica del Lazio.

Per i documenti a conservazione SLT è previsto il trasferimento della competenza all'ASBI.

Il Responsabile del sistema di conservazione verifica periodicamente la documentazione scartabile in base al piano di conservazione e, una volta ottenuta l'autorizzazione dalla Soprintendenza del Lazio, avvia il processo di scarto localizzando i documenti in base al proprio codice identificativo univoco (ID univoco).

I documenti digitali scartati sono censiti in un registro (Rapporto di scarto) che contiene gli ID univoci dei documenti sottoposti alla procedura e le informazioni utili a richiamare i *log* di sistema relativi all'intero processo[19].

Il Rapporto di scarto costituisce una specifica tipologia documentale e pertanto è anch'esso sottoposto al processo di conservazione.

Nel caso in cui il processo di scarto coinvolga tutti i documenti contenuti in un unico PdA, il sistema provvede a cancellare fisicamente l'intero PdA dall'archivio. In questa eventualità nel rapporto di scarto viene riportato anche l'ID del PdA oltre a quello dei documenti ivi contenuti.

[19] Virgilio applica un filtro che impedisce la visualizzazione e la modifica dei documenti scartati

7. SICUREZZA LOGICA E FISICA DEI DOCUMENTI CONSERVATI

7.1. CONTROLLI SULLA LEGGIBILITÀ

Conservare un contenuto informativo digitale significa mantenere nel tempo la capacità di riprodurlo con il contenuto e la forma originaria. In altre parole, significa mantenere, attraverso il sistema di conservazione, la capacità di leggere la relativa sequenza binaria nella sua interezza, di interpretarla con le regole del formato elettronico, di visualizzare, a video, a stampa o su un altro dispositivo di output, il documento risultante.

Per mantenere nel lungo periodo l'autenticità, l'integrità e la leggibilità di tutti i documenti conservati nel sistema, è stato predisposto un piano della sicurezza volto ad individuare e correggere tempestivamente eventuali processi di corruzione dei documenti e dei supporti.

Il Responsabile del servizio di conservazione pianifica la tempistica e le attività per la verifica dei documenti conservati. Alcune verifiche vengono effettuate automaticamente dal sistema, che seleziona un campione casuale di documenti dall'intero archivio di ogni soggetto produttore, calcola l'impronta di ogni documento e la confronta con quella rilevata al momento dell'acquisizione del documento stesso da parte del sistema di conservazione e che si trova memorizzata tra i metadati[20].

La leggibilità dei documenti conservati è assicurata attraverso:

- il confronto dell'impronta, in quanto la corruzione della stringa di *bit* che compone il documento provocherebbe la visualizzazione a schermo in maniera distorta[21].
- la possibilità di reperire strumenti *software* e *hardware* in grado di visualizzare il documento[22].

Il Responsabile del servizio di conservazione garantisce l'aggiornamento dei formati e dei supporti utilizzati all'interno del sistema di conservazione e, nel caso individui un caso di obsolescenza tecnologica, attua tempestivamente il piano di riversamento.

7.2. PRODUZIONE DI COPIE E DUPLICATI

Il salvataggio dei dati avviene con frequenza almeno settimanale. Inoltre sono gestite periodicamente le procedure per la produzione di copie e duplicati dei PdA e PdD. Le copie informatiche dei documenti contenuti in un PdA sono identiche ai documenti originali[23] .

La copia conforme al documento informatico originale viene prodotta su richiesta del soggetto produttore. Nel caso in cui un documento debba essere esibito in giudizio o in altra sede ufficiale, il Responsabile della conservazione attesta la conformità della copia prodotta all'originale.

Due copie di sicurezza dei PdA vengono prodotte nel momento in cui il PdA viene generato e sono memorizzate automaticamente sui server, conservate in luoghi diversi.

È possibile, in situazioni particolari, generare copie anche su supporti fisici (CD, DVD, *pendrive*); ogni copia ISO è corredata di un numero progressivo del PdA e dalla tipologia di documenti che contiene. Le etichette poste sul singolo supporto devono contenere:

---

[20] Se l'impronta risulta valida significa che la stringa di bit che forma il documento informatico è rimasta invariata, e non sono occorse nel tempo delle corruzioni, volontarie o involontarie, che possano aver cambiato la forma e/o il contenuto del documento. Attraverso il confronto delle impronte è possibile verificare, oltre all'integrità, anche l'autenticità del documento. Infatti la modifica o la rimozione delle firme digitali e delle marche/riferimenti temporali apposte al documento andrebbe a modificare la stringa di *byte* che lo compone causando la generazione di un'impronta differente.

[21] Il grado di perdita di leggibilità dipende dal livello di corruzione intervenuto e dalla solidità del formato in cui il documento è salvato

[22] In questo caso si parla di porre rimedio all'obsolescenza tecnologica, ovvero degli effetti del progresso tecnologico e dell'introduzione sul mercato di tecnologie sempre più avanzate, che causa il disuso di formati e supporti.

[23] Il duplicato informatico è il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della stessa sequenza di valori binari del documento originario.

- identificativo/nome/ragione sociale del soggetto produttore;
- data di masterizzazione e numero della copia;
- informazioni sul PdA conservato (oggetti e tipologia dei documenti archiviati nel supporto);
- la data di prima certificazione della copia ISO che contiene;
- gli estremi cronologici di ogni copia ISO ivi contenuta.

7.3. VERIFICHE, RIVERSAMENTO E MONITORAGGIO

L'integrità, la leggibilità dei dati e la robustezza dei supporti sono soggette a verifica periodica; in caso di obsolescenza, si procede alla generazione di copie e al riversamento[24].

Nel corso di un periodo di conservazione dei documenti, può essere necessario trasferire il contenuto da un supporto di memorizzazione a un altro. Tale esigenza può presentarsi, ad esempio, nel caso in cui sia necessario creare copie di *backup* o in caso di obsolescenza tecnologica dei supporti.

L'operazione deve essere effettuata dal Responsabile del servizio di conservazione, e assume il nome tecnico di "processo di riversamento diretto". Il riversamento diretto prevede che le informazioni riportate sul nuovo supporto non subiscano alcuna modifica[25].

Periodicamente viene garantita la conformità degli archivi digitali conservati attraverso i seguenti interventi:

- controlli di processo, per lo più automatizzati dal sistema, sulle fasi operative del processo di conservazione e sulla gestione delle anomalie;
- controlli periodici pianificati preventivamente dai responsabili della conservazione e dei sistemi informativi;
- controlli e manutenzione delle strutture *hardware* e *software*.

Il Servizio Gestione sistemi informatici quale responsabile dei sistemi e della sicurezza informatica, effettua e monitora le procedure di *backup*; d'intesa con il Responsabile del servizio di conservazione, coordina anche le attività previste per il piano di gestione di continuità operativa e del *risk assessment* indicate nel Piano per la sicurezza.

Il sistema effettua diversi controlli:

- tracciamento e monitoraggio di tutte le attività del processo di conservazione e di gestione dei supporti, notificando gli esiti delle diverse attività svolte, così come eventuali problemi, anomalie e criticità;
- verifica, per ogni documento conservato, di leggibilità, integrità, valore legale e livello di obsolescenza del formato;
- rinnovo automatico del periodo di validità dei certificati dei documenti, tracciando e segnalando gli esiti.

Tutti gli esiti delle operazioni svolte, incluse le anomalie e le situazioni critiche o potenzialmente rischiose evidenziate dal sistema di conservazione, sono visualizzabili sui *report* disponibili *online* attraverso la console di gestione.

[24] Il riversamento è il processo attraverso il quale si riproducono i documenti affidati a dispositivi di memorizzazione digitali. Le tipologie di riversamento sono due: diretto e sostitutivo e si differenziano per il tipo di risultato che producono.
[25] Per certificare che questo accada, il sistema calcola automaticamente un'impronta dei documenti registrati sul supporto prima del trasferimento e la confronta con l'impronta calcolata dopo il riversamento diretto.

8. COMPONENTI

8.1. COMPONENTI LOGICHE

I servizi Windows sono utilizzati per effettuare le operazioni di conservazione (creazione del PdA, ecc.) e per l'esecuzione delle attività di Virgilio (monitoraggio, ecc.). I servizi gestiti attraverso la *console* di configurazione del sistema sono i seguenti:

1) *Accettazione* - Servizio usato per inserire nuovi documenti in Virgilio: come sistemi di *input* può utilizzare file di testo (stile CSV con separatore o a lunghezza fissa) e/o può interfacciarsi direttamente con Archiflow (oppure con un altro Sistema documentale) attraverso l'utilizzo di un modulo specifico;
2) *Creazione PdA* - Servizio per la creazione del PdA in base a modelli predefiniti;
3) *Certificazione* - Servizio per la certificazione automatica del PdA con apposizione di firma digitale e marca temporale;
4) *Materializzazione* - Creazione delle copie fisiche in base alle regole impostate;
5) *Monitoraggio* - Servizio di monitoraggio dell'archivio digitale; viene pianificato periodicamente dal responsabile della manutenzione del SdC e prevede la verifica della consistenza e coerenza dei documenti;
6) *Operazioni generiche* - Servizio per la gestione delle operazioni generiche quali ad esempio la cancellazione, le richieste effettuate dal *web*, ecc;
7) *WCF per il Web* -Servizi WCF per il web; può essere definito una volta sola per tutto l'impianto;
8) *WCF di amministrazione* - I servizi WCF di amministrazione dispongono di una serie di funzionalità per la creazione di Aziende, tipologie documentali, ecc.; può essere definito una volta sola per tutto l'impianto;
9) *WCF per i Gadget*- Espone i servizi per l'utilizzo dei Gadget di Virgilio; può essere definito una volta sola per tutto l'impianto;
10) *FTP HTTPS*- Non è un servizio Windows; viene utilizzato dal SdC per identificare la modalità di trasporto delle copie ISO sul server web tramite il protocollo HTTPS;
11) *Gestione PdA* - Questo servizio gestisce la storicizzazione del PdA corrente delle immagini.

Tali servizi, in ambienti che utilizzano più server, possono essere definiti più volte in modo da parallelizzare le operazioni su entità differenti.

Le funzionalità che caratterizzano il SDC e rese disponibili sono di seguito sintetizzate:

- verifica dei documenti in termini di leggibilità, integrità, ecc.;
- gestione del PdA di documenti;
- certificazione del PdA;
- materializzazione del PdA certificato;
- ricerca ed esibizione dei documenti;
- monitoraggio sullo stato logico e fisico del sistema;
- amministrazione e configurazione del sistema.

8.2. COMPONENTI TECNOLOGICHE

Nell'architettura di Virgilio, i servizi caratterizzanti sono interoperabili secondo una definizione formale indipendente dalla piattaforma e dalle tecnologie di sviluppo (come Java, .NET, etc.) dato che viene applicata una logica comunemente conosciuta come *Service-Oriented Architecture* (SOA). Ciò significa che ogni servizio può essere richiamato per eseguire i propri compiti senza avere conoscenza dell'applicazione chiamante e senza che l'applicazione, a sua volta, abbia conoscenza del servizio che effettivamente esegue l'operazione.

Il SOA funziona attraverso l'uso di un componente di orchestrazione, secondo il modello dell'Enterprise Service Bus, che opera nel rispetto dei principi di cooperazione applicativa basati sullo standard xml.

L'implicazione principale di un tale approccio, grazie alla possibilità di modificare in maniera semplice le modalità di interazione tra i servizi e in generale la loro combinazione (per soddisfare le esigenze dei processi che implementano), prevede che la logica di business sia svincolata dalla tecnologia utilizzata, per cui è possibile realizzare la separazione tra "cosa un'applicazione fa" da "come lo fa".

Un ulteriore vantaggio di un'architettura a servizi è l'integrazione immediata con altri applicativi via web services; in sintesi altri applicativi, indipendentemente dal linguaggio di programmazione in cui sono stati scritti e dalla piattaforma su cui sono implementati, possono utilizzare i servizi messi a disposizione attraverso l'invio tramite HTTPS di messaggi in formato xml.

L'organizzazione in servizi, interagenti tra loro e attivabili in funzione delle esigenze, permette di massimizzare anche la modularità e l'estensibilità della soluzione, ottimizzando da una parte il carico di lavoro e soddisfacendo dall'altra tutte le esigenze di amministrazione delle attività di conservazione a norma degli archivi digitali.

In particolare in Virgilio sono attivi i seguenti moduli:

- Accettazione PdV;
- Generazione PdA;
- Certificazione PdA;
- Materializzazione PdA;
- Monitoraggio;
- Gestione PdA.

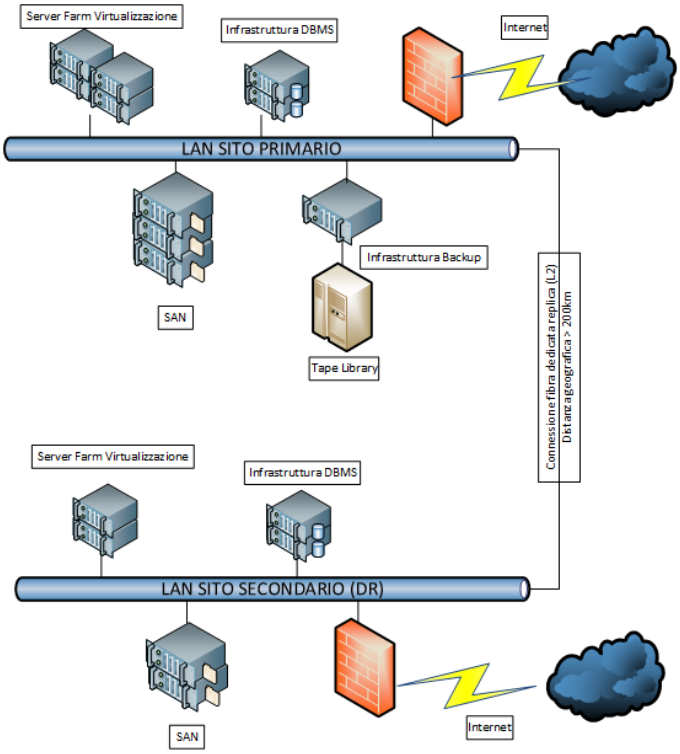

Figura 16 – Infrastruttura *Disaster Recovery*

8.3. COMPONENTI FISICHE

L'architettura del SDC è stata progettata per gestire in modo ottimale la performance del processo di conservazione e di esibizione applicando un approccio multi-server e tecniche di bilanciamento intelligente del carico di lavoro.

In particolare essa garantisce:

- l'estensibilità della soluzione, grazie alla possibilità di attivare solo i moduli necessari per la specifica implementazione;
- l'alta affidabilità, grazie alla possibilità di distribuire i moduli su server indipendenti e di clusterizzare tutti i suoi componenti;
- la scalabilità, grazie alla possibilità di distribuire i vari moduli su più server al crescere del carico di lavoro e di sfruttare la piena compatibilità con i più diffusi e affidabili sistemi NAS e SAN per la gestione dello *storage*.

Si precisa che le diverse componenti critiche e significative ("sensitive") del sistema di conservazione sono isolate da altri ambienti, organizzativamente, fisicamente e logicamente, in quanto organizzativamente il DSO è un settore specifico con personale dedicato; dal punto di vista logico il SDC risulta configurato su macchine dedicate, gli schemi database e le reti sono separate, la SAN è frazionata, ecc.

Per quanto riguarda l'isolamento fisico:

- gli apparati del SDC sono collocati in un'area sorvegliata, accessibile soltanto al personale autorizzato;
- il sito di *Disaster Recovery* è ospitato nei locali di un Data Center certificato, posizionato ad una distanza in linea d'aria superiore a 200 km dal sito primario.

Per ulteriori dettagli si rimanda al Piano della sicurezza (in Appendice).

APPENDICE – CENNI SUL PIANO PER LA SICUREZZA

Nel Piano di Sicurezza del SDCI sono definiti i controlli di sicurezza delle diverse componenti del sistema e le procedure adottate per garantire la conservazione a lungo termine degli archivi, le procedure di recupero da incidenti (*Disaster Recovery*) e la Continuità Operativa (*Business Continuity*).

In questa sede se ne dà una descrizione sintetica con la finalità di esporre i principi fondanti[26].

I. LA SICUREZZA INFORMATICA IN BANCA D'ITALIA

La sicurezza informatica degli archivi dell'Istituto rientra nella strategia per garantire un'efficace ed efficiente gestione della sicurezza informatica, basata su un *framework* volto a definire:

- il sistema dei ruoli e delle responsabilità per assicurare un insieme di misure e azioni coordinate per la resilienza cibernetica della banca;
- le attività volte a prevenire, mitigare e gestire attacchi *cyber* di origine interna o esterna ed eventi accidentali, suscettibili di determinare impatti negativi sul patrimonio, sulla reputazione o sullo svolgimento dei compiti della Banca.

Il *framework* si inserisce nel vigente quadro normativo e organizzativo che disciplina la materia, di seguito riepilogato:

Circolare	Finalità
Norme in materia di sicurezza informatica	La circolare definisce e disciplina il sistema costituito dall'insieme di norme di comportamento, assetti organizzativi, misure tecniche, metodologie e processi volti alla tutela delle risorse informatiche dell'Istituto. Si definiscono gli obiettivi, i princìpi generali, le responsabilità dei ruoli organizzativi interessati e i processi fondamentali del sistema aziendale di sicurezza informatica.
Sviluppo e gestione dei servizi ICT	La circolare disciplina gli obiettivi, gli assetti organizzativi e le regole procedurali posti alla base dei principali processi correlati allo sviluppo e alla gestione della risorsa informatica nell'Istituto. In particolare, vengono definiti: i) le competenze dei diversi ruoli organizzativi interessati; ii) i processi trasversali di programmazione operativa e di coordinamento.
Disposizioni in materia di trattamento dei dati personali	La circolare disciplina l'attuazione delle norme in materia di trattamento dei dati personali in Banca. Le disposizioni sulla *privacy* si applicano anche ai trattamenti di dati personali effettuati dalla Banca, che soggiace alle regole di carattere generale valide per tutti i trattamenti effettuati da soggetti pubblici e privati nonché ai principi ulteriori applicabili ai trattamenti svolti dai soli soggetti pubblici. La normativa, in particolare, stabilisce i ruoli e le connesse responsabilità nel trattamento dei dati personali, altamente personali, rientranti in categorie particolari (es. salute, orientamento sessuale) e relativi a condanne penali e reati.
La tutela della riservatezza delle informazioni	L'obiettivo della circolare è quello di favorire la consapevolezza da parte di tutto il personale del livello di riservatezza delle informazioni trattate; queste ultime riguardano non solo le informazioni elaborate con strumenti informatici, ma anche quelle gestite con supporti cartacei, apparati telefonici o altre modalità. La circolare prende in considerazione i due profili rilevanti, e strettamente interconnessi, relativi alla classificazione delle informazioni e ai presidi di sicurezza che ne discendono; questi ultimi vengono declinati anche con riferimento al livello di circolazione delle informazioni e ai comportamenti da assumere nel trattamento dei documenti riservati.
Sistema aziendale di gestione del rischio operativo	La circolare disciplina il sistema adottato in Banca per la gestione del rischio operativo (Operational Risk Management, ORM), individuando i soggetti coinvolti e le attività da svolgere. I rischi operativi scaturiscono dai processi attraverso i quali la Banca quotidianamente svolge i suoi compiti, sia di natura istituzionale sia strumentale.

[26] Per i dettagli si rimanda al documento *Piano di sicurezza del Sistema di Conservazione digitale*, a visibilità ristretta.

Governance Framework per la *Cyber resilience*	Il *fremwork* mira a definire, conseguire e mantenere un livello d *cyber resilience* appropriato e coerente con i livelli di criticità dei servizi offerti, in attuazione della Strategia di *cyber resilience* della Banca.

Accanto alla Governance, implementata per mezzo di tale *framework*, si individuano altre quattro funzioni primarie (Identificazione, Protezione, Rilevazione, Risposta e Ripristino) oltre a tre capacità trasversali (Verifica, *Awareness*, Apprendimento e Crescita). L'assetto complessivo per la gestione della sicurezza è rappresentato nella Figura 17.

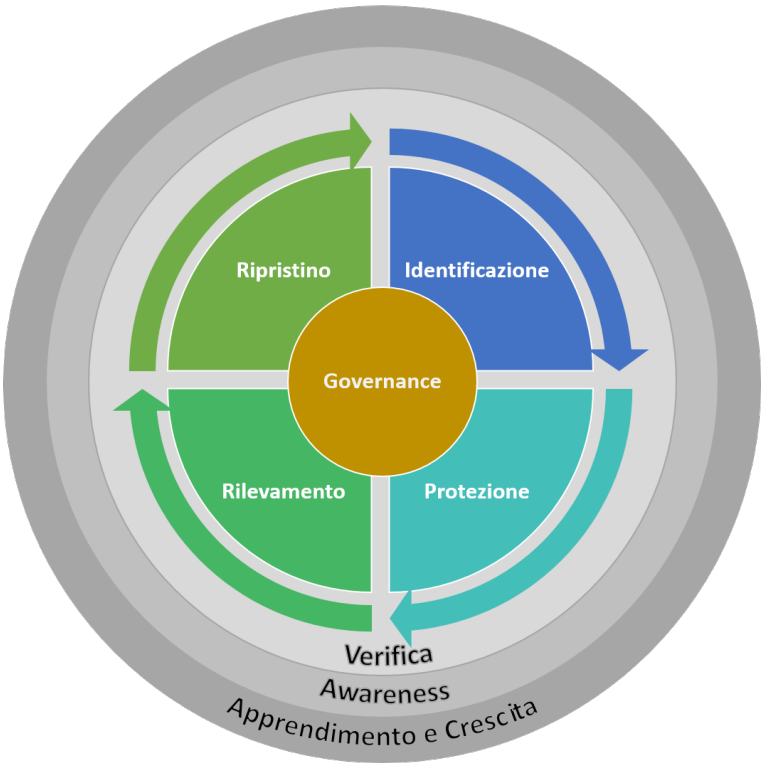

Figura 17 - Assetto complessivo per la gestione della sicurezza

II. IDENTIFICAZIONE

Primo passo per il raggiungimento di un adeguato livello di sicurezza è l'identificazione degli *asset* informatici[27] critici (*criticality assessment*) e delle minacce a cui sono soggetti (analisi del rischio informatico). Dal punto di vista della *business continuity* si individuano, inoltre, gli *asset* critici per la continuità del processo operativo supportato. È prevista, inoltre, l'attività di *cyber threat intelligence* con l'obiettivo di acquisire le informazioni da fonti eterogenee e trasmettere la conoscenza sviluppata agli opportuni attori della *constituency*[28]. Nel caso degli archivi le strutture che intervengono, per propria competenza, sono il *System owner*[29], la funzione informatica e l'Organizzazione, oltre ad altre Strutture che a vario titolo prestano il loro contributo su aspetti peculiari quali la riservatezza (valutazione d'impatto DPIA).

[27] Si definisce *asset* informatico un'informazione in formato digitale, sia in corso di elaborazione sia archiviata, nonché le infrastrutture e i sistemi a supporto (es. piattaforme elaborative).
[28] Comunità di utenti ed entità interni o esterni all'organizzazione verso cui vengono condivise le informazioni. Questa potrà essere illimitata (es. chiunque ne faccia richiesta), oppure può essere limitata da alcune restrizioni, quali ad esempio vincoli di natura geografica o politica (*constituency* nazionale o governativa).
[29] Il *System owner* è responsabile delle procedure informatiche di propria competenza lungo l'intero ciclo di vita e ne garantisce l'aderenza alla normativa e la conformità al livello di sicurezza stabilito.

III. PROTEZIONE

Questa funzione è volta ad assicurare che gli *asset* informatici della Banca ricevano l'adeguato livello di protezione per la disponibilità, l'integrità e la riservatezza. Le misure messe in campo garantiscono da una parte i controlli preventivi focalizzati sulla rilevazione e dall'altra la risposta e il ripristino a seguito di incidenti. Nel caso degli archivi le strutture che intervengono, per propria competenza, sono il *System owner*, la funzione informatica e l'Organizzazione.

IV. RILEVAMENTO

I controlli focalizzati sulla rilevazione sono progettati, implementati e gestiti con l'obiettivo di riconoscere rapidamente i segni di eventi *cyber* indesiderati in modo da rendere tempestiva la fase successiva di risposta, contenendo l'impatto. Nel caso degli archivi interviene la funzione informatica con le Unità Organizzative coinvolte nel processo di *security incident handling*

V. RISPOSTA E RIPRISTINO

Tale funzione si connota nelle attività necessarie per rispondere tempestivamente all'evento avverso e per ripristinare i livelli di servizio alla condizione di normale operatività. Nel caso degli archivi interviene principalmente la funzione informatica oltre alle Strutture competenti per l'esecuzione delle misure individuate nei piani di continuità settoriale. In accordo con tali piani può essere dichiarato lo stato di emergenza generale.

VI. VERIFICA

La verifica per mezzo di test è una componente fondamentale per garantire l'efficacia di ogni misura di sicurezza e prevedere l'esecuzione periodica di un ampio spettro di attività, dal livello tecnico-organizzativo a quello strategico; tra queste rilevano: i *vulnerability assessment*, gli *scenario-based* test, i *penetration* test e i *red team* test. Nel caso degli archivi concorrono il *System owner*, la funzione informatica e le Strutture competenti, queste ultime per le simulazioni di incidenti di sicurezza.

VII. *AWARENESS*

Fattore abilitante alla corretta osservazione e comprensione di minacce e vulnerabilità in termini di loro evoluzione e correlate azioni difensive da porre in essere per la prevenzione o la mitigazione di un incidente di sicurezza. Determinante per questa capacità è disporre di un processo di *cyber threat intelligence* in grado di produrre e trasferire in modo accurato e tempestivo le informazioni rilevanti per prevenire e rispondere rapidamente a eventi avversi. La funzione informatica svolge il ruolo chiave per attività di *information sharing* e specifiche campagne di sensibilizzazione rivolte alla totalità o a specifici gruppi di dipendenti per accrescere la loro consapevolezza in relazione ai rischi individuali a cui sono esposti e ai possibili conseguenti impatti per l'Istituto.

VIII. APPRENDIMENTO E CRESCITA

Data la dinamicità della minaccia *cyber* e degli *asset* da proteggere assume fondamentale importanza che i processi di sicurezza informatica siano in grado di evolvere adattandosi. A tal fine rileva la conoscenza prodotta dalle attività di *cyber threat intelligence* e dalla valorizzazione delle lezioni apprese conseguentemente alla gestione di eventi avversi reali o simulati attraverso la capacità di test. Come per l'*awareness* anche in questo ambito la funzione informatica gioca un ruolo chiave.