Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

ACCREDITAMENTO DEI SOGGETTI PUBBLICI E PRIVATI CHE SVOLGONO ATTIVITÀ DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI

REQUISITI DI QUALITÀ E SICUREZZA PER L'ACCREDITAMENTO E LA VIGILANZA

Il presente documento è la base operativa per l'attività istruttoria svolta dall'Agenzia per l'Italia Digitale di accreditamento del soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici (di seguito "conservatore") e intende conseguire il riconoscimento dei requisiti del livello più elevato, in termini di qualità e sicurezza, ai sensi dell'art. 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale.

La tabella di seguito riportata specifica i requisiti di qualità e sicurezza atti a verificare che il sistema di conservazione del conservatore sia realizzato e gestito in conformità agli standard e specifiche tecniche contenute nel DPCM 3 dicembre 2013 in materia di sistema di conservazione.

Nello specifico si fa riferimento allo standard ISO 14721:2002 *OAIS* (Open Archival Information System), Sistema informativo aperto per l'archiviazione, e alle raccomandazioni ETSI TS 101 533-1 V1.1.1 (2011-05), Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

Per ciascun requisito sono riportati i riferimenti allo standard OAIS e alle raccomandazioni ETSI relative. Si precisa che nel caso dello standard OAIS i riferimenti riportati tra parentesi quadre sono relativi al documento "*Audit and certification of trustworthy digital repositories*" del Consultative Committee for Space Data Systems (CCSDS) mentre gli altri al documento "*Reference model for an open archival information system*" del medesimo Comitato.

Si precisa che la conformità allo standard ISO/IEC 27001:2013, richiamato anch'esso dal suddetto DPCM e che riguarda i requisiti di un ISMS (Information Security Management System), è attestata dal certificato rilasciato da un Organismo di Certificazione accreditato e trasmesso all'Agenzia per l'Italia Digitale dal conservatore.

Inoltre, si evidenzia che la struttura descrittiva dell'indice del pacchetto di archiviazione del sistema di conservazione deve essere conforme allo standard UNI 11386:2010 Standard SInCRO, Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali. L'Allegato 4 del citato DPCM 3 dicembre 2013 illustra la struttura XML dell'indice in lingua italiana per facilitare la comprensione dello standard stesso.

Il presente documento è utilizzato anche per l'attività istruttoria svolta dall'Agenzia per l'Italia Digitale per la verifica del mantenimento nel tempo dei requisiti che hanno consentito l'accreditamento del conservatore.

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
1	Organizzazione	E' definita la politica di sicurezza delle informazioni (ISPD - Information Security Policy Document) da parte dell'ente conservatore e tale documento è approvato dal management dell'ente. Il documento indirizza la protezione dei dati sulla base della loro criticità, valore e sensibilità rispetto al complessivo servizio di conservazione, definendo le politiche di alto livello, gli indirizzi da seguire e demandando alle specifiche procedure i dettagli per la loro attuazione. Il documento indirizza i ruoli e le responsabilità in merito alla sicurezza ed alla protezione delle informazioni all'interno del servizio di conservazione. Sono svolte le necessarie attività propedeutiche alle revisione periodica del documento (ad esempio il risk assessment), almeno annualmente, ed è mantenuta traccia nel tempo delle modifiche effettuate al documento (versioning). Tutte le persone coinvolte nel processo di conservazione sono a conoscenza del documento, per le parti che possono essere condivise e rese pubbliche, con evidenza dell'effettiva comunicazione. Viene data comunicazione e condivisa con le parti interessate (enti produttori, fornitori ed outsourcer) ogni cambiamento al documento ritenuto significativo (Ad esempio classificazione delle informazioni, ecc.). Sono previste apposite sessioni educative, di sensibilizzazione e formazione per il personale operante nel servizio di conservazione in merito alle politiche e procedure di sicurezza e con particolare riferimento alla riservatezza e confidenzialità delle informazioni trattate e delle relative modalità, sia durante il rapporto di lavoro che al termine, mantenendo evidenza della loro partecipazione e della consegna dei documenti.	3.1(e) [5.2.2]	A.5.1.1 A.5.1.2 A.6.2.2 A.7.2.1 A.7.2.2 A.8 A.8.1.3 A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.1 A.9.2.7 A.10.10.4
2	Organizzazione	Il manuale di conservazione contiene 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. Verificare che non vi siano gap temporali per i soggetti responsabile del servizio di conservazione. E' presente la documentazione ove viene descritta l'organizzazione dell'ente conservatore, ruoli e responsabilità. E' presente ed attuato un piano di aggiornamento professionale per il personale appartenente al servizio di conservazione.		A.6.1.1 A.6.1.3 A.6.1.6 A.6.1.7
3	Organizzazione	Le tematiche della sicurezza sono presidiate ed indirizzate, in accordo con la segregazione dei compiti all'interno del servizio di conservazione, come risulta dall'organigramma e dalle job description.	-	A.6.1.2
4	Organizzazione	Esiste una procedura per la gestione formale delle comunicazioni da e verso l'esterno del servizio di conservazione. La procedura descrive le modalità di comunicazione e le eventuali eccezioni. Ogni comunicazione formale verso l'esterno è validata da parte del management. Il personale coinvolto nel servizio è a conoscenza della procedura e la attua.	-	A.6.1.5

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
5	Organizzazione	E' attuata una verifica periodica dell'impianto documentale e della sua concreta attuazione ed applicazione, da parte del management e, ove richiesto da normative, da personale esterno.	-	A.6.1.8
6	Organizzazione	L'ente conservatore ha svolto un'attività di analisi dei rischi rispetto alla propria organizzazione, processi, infrastrutture, sistemi, processi, obiettivi, ecc. ritenuta necessaria per assicurare una piena adeguatezza delle diverse componenti del sistema di conservazione ai requisiti, vincoli ed obiettivi ed una completa conformità rispetto agli aspetti legali, normativi, standard, ecc. L'analisi dei rischi considera i rischi relativi alle parti esterne (fornitori, outsourcer, enti produttori, ecc.) Viene mantenuta la documentazione a supporto di tale analisi, inclusa quella relativa alle decisioni ed iniziative intraprese da parte del management.	3.1(e) [5.1.1] 3.1(e) [5.1.1.6] 3.1(e) [5.2.1]	A.6.2.1
7	Organizzazione	Quanto indentificato in sede di analisi dei rischi, con specifico riferimento alle terze parti, è effettivamente indirizzato da adeguate contromisure descritte nei contratti di servizio. Il management ha ricevuto ed approvato il piano della sicurezza (o documento sulla sicurezza) dei fornitori / outsourcer, per le attività rilevanti nelle quali sono coinvolte le terze parti. E' presente un piano di continuità, per le attività in outsourcing, coerente con i requisiti indicati nel BCP dell'ente conservatore. L'outsourcer ha definito un piano di ripristino, per le attività in outsourcing, periodicamente rivisto ed approvato dal management dell'ente conservatore. E' presente nei contratti di servizio, per le attività in outsourcing, la clausola di audit per assicurare all'ente conservatore la possibilità di eseguire ispezioni e verifiche. Sono mantenute le versioni del software e la relativa documentazione, nel caso in cui le attività esternalizzate riguardino lo sviluppo software.	-	A.6.2.3
8	Organizzazione	E' eseguita una verifica delle competenze e conoscenze precedentemente all'attivazione del contratto, con particolare riferimento alle persone alle quali saranno concessi privilegi di amministratore dei sistemi, in conformità con il loro ruolo ed in coerenza con l'ISPD. Le loro responsabilità sono descritte in apposito documento, con accettazione da parte delle persone interessate.	-	A.8.1.1 A.8.1.2
9	Organizzazione	E' definita ed applicata una procedura per rimuovere tempestivamente i diritti di accesso delle persone e la restituzione degli asset, in caso di interruzione del rapporto di lavoro e contratto (in caso di fornitori) e comunque per tutti coloro che non sono più coinvolti nel sistema di conservazione. La procedura prevede la comunicazione ed informazione alle persone coinvolte nel processo di conservazione.	-	A.8.3.2 A.8.3.3

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
10	Organizzazione	Il sistema di conservazione ha un processo di change management formalizzato sulla base del quale: - identificare, analizzare e valutare i cambiamenti ritenuti utili o necessari per i processi critici, che potrebbero potenzialmente impattare il sistema di conservazione. Tali cambiamenti possono essere, ad esempio, relativi ai processi di versamento, archiviazione e distribuzione dei pacchetti, ai processi, alle modalità di gestione degli accessi, alla architettura infrastrutturale ed applicativa del processo, alla sicurezza, ecc. - identificare ruoli, responsabilità ed i necessari processi autorizzativi necessari per implementare i cambiamenti nel processo e nel sistema - assegnare personale adeguato alle necessità sul processo di cambiamento (hard skill e soft skills) - definire adeguati programmi di formazione e sviluppo professionale per il personale coinvolto E' presente adeguata documentazione a supporto dei cambiamenti applicati al sistema di conservazione ed in particolare per verificare che ogni cambiamento significativo sia stato: - analizzato e valutato dal personale coinvolto - autorizzato dal responsabile del servizio, comunque almeno informato in caso di emergenza ed applicazione dei cambiamenti con modalità immediate Sono previste specifiche procedure di roll back all'interno del processo di cambiamento. Il sistema di conservazione permette la tracciabilità dei cambiamenti apportati, tramite versioning o registro del software. Il processo di cambiamento è applicato sia al personale interno, che al personale esterno, come anche nei confronti di possibili outsourcer. In caso di emergenza l'outsourcer comunica i cambiamenti eseguiti, le motivazioni sottostanti e la documentazione a supporto.	3.1(e) [3.2.1 3.2.1.1 3.2.1.2 3.2.1.3] 3.1(f) [3.3.3] 3.1(e) [5.1.1.6.1] 3.1(e) [5.2.3]	A.10.1.2 A.10.2.3
11	Organizzazione	E' descritta ed effettivamente implementata una segregazione dei compiti nello svolgimento delle attività operative, in coerenza con la separazione organizzativa dei compiti. Il personale che opera all'interno del sistema di conservazione non ha privilegi amministrativi nei sistemi, ad eccezione del ristretto personale autorizzato.	-	A.10.1.3
12	Organizzazione	I controlli di sicurezza, la definizione del servizio da assicurare ed i livelli del servizio da parte delle terze parti sono adeguatamente descritti nella documentazione.	-	A.10.2 A.10.2.1
13	Organizzazione	Esiste ed è attuato un processo (e relative attività operative) di monitoraggio e controllo dei servizi erogati da terze parti, in coerenza con quanto previsto all'interno dei contratti di servizio. Le attività sono formalmente assegnate al management aziendale ed eseguite da personale esperto sempre sotto la supervisione dei responsabili. E' presente nei contratti di servizio, per ogni attività in outsourcing, la clausola di audit per assicurare all'ente conservatore la possibilità di eseguire ispezioni e verifiche, anche non concordate.	-	A.10.2.2

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
14	Organizzazione	La documentazione in relazione all'accettazione dei sistemi (nuovi sistemi, upgrade, nuove versioni, ecc.), è mantenuta con modalità che assicurino la sua sicurezza e l'aggiornamento periodico, in particolare per la configurazione dei sistemi e per i processi di test e valutazione degli effetti di tale cambiamento sui processi critici del sistema di conservazione.	3.1(e) [5.1.1.6.2]	A.10.3.2
15	Organizzazione	Sono definite ed attuate specifiche politiche di gestione degli accessi, riviste periodicamente, che assicurano la disponibilità delle informazioni al solo personale autorizzato sulla base di specifiche procedure. Tali procedure assicurano l'accesso alle informazioni ed ai sistemi, sia al personale organizzativamente interno al processo di conservazione, che al personale esterno di supporto, in accordo con le politiche di gestione degli accessi, definendo diversi livelli di accesso sulla base delle necessità. Le procedure prevedono specifiche verifiche periodiche per assicurare la persistenza attuale di tali necessità, l'identificazione di anomalie ed eventuali problematiche, oltre all'attuazione di eventuali azioni. La documentazione ed i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.	3.1(e), 2.2 [4.6.1, 4.6.1.1]	A.11.1.1 A.11.6.1
16	Organizzazione	E' definito un processo formale, con specifica procedura, di assegnazione, revisione e cancellazione delle utenze per accedere al sistema di conservazione. Tale processo formale è applicato a chiunque abbia necessità di accedere al sistema, quali utenti dell'ente produttore, ente conservatore, fornitori, ecc. Sulla base di tale processo formale sono previste le seguenti attività minime: assegnato un solo user ID per persona, con utilizzo di utenze di gruppo solo per eccezioni strettamente controllate e preventivamente autorizzate; la richiesta di rilascio dello user ID deve pervenire da persona autorizzata ed il rilascio formalmente approvato; consegnato un documento all'utente autorizzato con i suoi diritti di accesso e con le eventuali verifiche e controllo richiesti dal processo di conservazione, con accettazione da parte dell'utente; mantenuto l'elenco storico delle credenziali di accesso assegnate. Sono periodicamente analizzate e riviste le credenziali di accesso al sistema di conservazione, sulla base della periodicità descritta nel processo e formalizzata nella procedura, per accertare che la necessità di accesso sia ancora valida. La documentazione ed i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.	-	A.11.2.1

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
17	Organizzazione	E' definito un processo formale, con specifica procedura, di assegnazione, revisione e cancellazione dei privilegi di accesso per le utenze assegnate per accedere al sistema di conservazione. Tale processo formale è applicato a chiunque abbia necessità di accedere al sistema, quali utenti dell'ente produttore, ente conservatore, fornitori, ecc. sulla base dei compiti assegnati nell'intero processo di conservazione. Sono periodicamente analizzati e rivisti i privilegi di accesso al sistema di conservazione, sulla base della periodicità descritta nel processo e formalizzata nella procedura, per accertare che tali modalità di accesso siano ancora basate su una precisa necessità. Il sistema di gestione e reportistica degli incidenti di sicurezza prevede apposite modalità di segnalazione relative all'utilizzo improprio delle credenziali di accesso e dei relativi diritti. La documentazione ed i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.	-	A.11.2.2 A.11.2.4
18	Organizzazione	E' presente un processo formale per la gestione ed assegnazione delle password di accesso al sistema di conservazione. Tale processo, basato su specifiche procedure organizzative e tecniche, prevede i controlli minimi assicurati dal sistema rispetto alla generazione ed utilizzo delle password (lunghezza minima e massima, utilizzo di caratteri, scadenza delle password, eventuali eccezioni per le utenze di sistema, ecc.) e la comunicazione ai fruitori, almeno in sede di primo accesso. Queste regole devono essere applicate per chiunque abbia accesso al sistema, sia per l'ente produttore, che per l'ente conservatore, inclusi i fornitori.	-	A.11.2.3 A.11.3.1
19	Organizzazione	Sono definite e comunicate le regole a tutto il personale coinvolto nel sistema di conservazione (interno, fornitori e terze parti), riguardo ai comportamenti da mantenere per l'utilizzo degli strumenti informatici ed alla riservatezza delle informazioni gestite, quali ad esempio: - non lasciare documenti contenenti informazioni e dati privati, sensibili, critici, ecc. sulla propria scrivania e sullo schermo del proprio computer (clear desk e clear screen policy); - utilizzo della posta elettronica come strumento lavorativo; - impiego di internet come strumento lavorativo; - linee guida per l'utilizzo di supporti fisici removibili; Tali regole sono ricomprese all'interno delle policy di sicurezza e coerentemente allineate con quanto previsto dalla normativa sulla privacy.	-	A.7.1.3 A.11.3.2 A.11.3.3

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
20	Organizzazione	E' definito ed attuato un processo formalizzato per la gestione degli eventi di sicurezza e delle debolezze associate ai sistemi utilizzati per il processo di conservazione. Tale processo descrive ruoli, responsabilità ed attività da svolgere ed è rivolto a tutte le persone, interne e fornitori, coinvolte nel sistema di conservazione, in maniera formale e con accettazione formale delle regole e dei principi. Le persone interessate sono a conoscenza ed hanno accettato i relativi ruoli e responsabilità assegnate. Sono definite specifiche procedure per la gestione, mantenimento e segnalazione degli incidenti di sicurezza e delle azioni conseguenti, del relativo livello di priorità al quale associare l'intervento, degli strumenti utilizzati, ecc. Sono descritte le modalità attraverso le quali sono riportati tali eventi, come siano mantenute tali informazioni nel sistema e come sia assicurata la loro riservatezza. Gli eventi, le azioni intraprese e le considerazioni conseguenti sono considerate nel processo di miglioramento continuo ed in particolare nel risk assessment e nell'Information Security Policy Document.	3.1(e) [5.1.1.3.1]	A.13.1.1 A.13.1.2 A.13.2.1 A.13.2.2 A.13.2.3
21	Organizzazione	Sono definiti ed attuati specifici piani per la continuità operativa del business e per la continuità tecnologica del sistema di conservazione (BCP - Business Continuity Plan e DRP - Disaster Recovery Plan). Tali piani assicurano la continuità ed il ripristino dei sistema e delle sue componenti entro le tempistiche identificate (recovery time objective e recovery point objective), in accordo con gli accordi contrattuali e le convenzioni stipulate. Sono presenti apposite procedure di emergenza (contingency) da applicare in attesa del ripristino del servizio. Sono descritti all'interno dei piani i ruoli e le responsabilità assegnate alle persone. Esiste ed è attuato il processo formalizzato per assicurare che gli eventi significativamente impattanti la normale e regolare erogazione del servizio sono segnalati, esaminati e valutati per l'eventuale dichiarazione del disastro o per l'attivazione del DRP e del BCP. Tale dichiarazione dovrebbe essere fatta da un "comitato" interno con coinvolgimento del responsabile del servizio di conservazione. I piani sono definiti sulla base del risk assessment, della business impact analysis e delle strategie di continuità, considerando tutte le componenti organizzative, operative, del business, tecnologiche, infrastrutturali che contribuiscono all'intero sistema e processo di conservazione. Sono eseguiti test, prove e verifiche periodiche con modalità che prevedano ad esempio, test degli scenari, simulazioni per le diverse componenti, verifica e ripristino delle componenti tecnologiche, ripristino parziale o totale del servizio presso un sito secondario, test e verifiche degli aspetti di facility, verifiche complessive sugli aspetti organizzativi, processi, personale, ecc.).	3.1(e) [5.2.4]	A.7.1.2 A.14.1.1 A.14.1.2 A.14.1.3 A.14.1.4 A.14.1.5

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
22	Organizzazione	Sono indicate le principali norme, regolamenti, standard, politiche, ecc. ritenuti applicabili nel sistema di conservazione e nell'impianto documentale. Il mantenimento della documentazione soddisfa i requisiti indicati nella parte 1, capitolo 5 e capitolo 7 dello standard ISO 15489.	-	A.15.1.1 A.15.1.3
23	Organizzazione	I diversi responsabili verificano, sulla base di una specifica procedura e con periodicità definite, la conformità delle proprie aree di riferimento alle politiche di sicurezza, standard ed ogni altro requisito di sicurezza. Tali verifiche di conformità dovranno essere svolte sia per le attività operative, che per gli aspetti tecnologici (per hardware e software, anche con l'utilizzo di penetration tests or vulnerability assessments). Tale procedura, oltre a definire la metodologia in base alla quale svolgere tali verifiche, assicura anche adeguata informazione nei confronti del personale complessivamente coinvolto (interno ed esterno) per le possibili problematiche derivanti dalla non conformità alle tematiche di sicurezza. In caso di coinvolgimento di personale esterno od outsourcing di parte delle attività, sono definite nei contratti gli obblighi e responsabilità reciproche, con identificazione dei rispettivi ruoli e responsabilità. E' mantenuta adeguata documentazione a supporto delle attività complessivamente svolte e dei risultati ottenuti dalle verifiche di conformità.	-	A.15.2.1 A.15.2.2
24	Organizzazione	La mission dell'ente conservatore è descritta e ben identificata, al fine di riflettere l'impegno aziendale ("commitment") per la conservazione a lungo termine, la gestione e l'accesso alle informazioni.	3.1(e) [3.1.1]	-
25	Organizzazione	E' presente un piano strategico che descrive l'approccio dell'ente conservatore alla conservazione a lungo termine, in modo coerente con la propria missione. Tale approccio, oltre che dal piano strategico, potrebbe essere desunto da verbali di riunione, documentazione amministrativa, ecc. L'ente conservatore ha definito specifici piani per assicurare la disponibilità dei dati e delle informazioni conservate all'ente produttore, in caso di cessazione delle operazioni di conservazione o modifica della propria missione (interoperabilità).	3.1(e) [3.1.2 , 3.1.2.1, 3.1.2.2]	-
26	Organizzazione	E' definita una policy per assicurare la conservazione nel tempo delle informazioni, la tipologia degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni.	3.1(e) [3.1.3]	
27	Organizzazione	Il manuale di conservazione descrive il modello organizzativo e la comunità di riferimento (ente produttore, fruitori, community informative, ecc.).	3.1(c) [3.3.1]	-

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
28	Organizzazione	Sono descritte le modalità attraverso le quali raggiungere gli obiettivi e la mission della conservazione ed i meccanismi per rivedere, aggiornare e sviluppare le proprie politiche di conservazione a lungo termine (manuale di conservazione). Sono descritte tutte le componenti 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.	3.1(e) [3.3.2 , 3.3.2.1]	-
29	Organizzazione	L'ente conservatore rende disponibile a chiunque le modalità attraverso cui assicura la trasparenza delle proprie attività e la responsabilità per le azioni operative e gestionali, rispetto al sistema di conservazione.	3.1(f) [3.3.4]	-
30	Organizzazione	L'evoluzione del sistema di conservazione (organizzazione, processi e tecnologia) è supportato dalla documentazione necessaria per attestare le motivazioni sottostanti le scelte e le misure attuate per assicurare l'integrità dei dati e delle informazioni ed in particolare, le procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche che sull'integrità degli archivi con evidenza delle soluzioni adottate in caso di anomalie.	3.1(e) [3.3.5]	-
31	Organizzazione	L'ente conservatore svolge una verifica periodica della conformità alle normative ed agli standard.	3.1(f) [3.3.6]	-
32	Organizzazione	L'ente conservatore ha definito un piano di sostenibilità finanziaria di breve, medio, lungo termine per sostenere il sistema di conservazione. Sono presenti procedure amministrative e finanziarie che assicurano la trasparenza, conformi alle normative ed ai principi contabili applicabili e revisionate da terze parti in accordo con i requisiti normativi e legali. L'ente conservatore ha attivato un processo interno per analizzare e descrivere i rischi finanziari, benefit, investimenti e costi (attività, passività e permessi).	3.1(e) [3.4.1, 3.4.2, 3.4.3]	-

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
33	Organizzazione	Il servizio di conservazione è descritto attraverso gli schemi di contratti e le convenzioni di servizio, oltre al manuale di conservazione. Sono conservati i contratti e le convenzioni di servizio con gli enti produttori che abbiano assegnato il servizio o parte di esso all'ente conservatore. Sono descritti i principali aspetti del servizio di conservazione in relazione agli oggetti della conservazione ed alle modalità di versamento, di archiviazione e di distribuzione, negli schemi di contratti e nelle convenzioni di servizio, oltre al manuale di conservazione. Sono definite e descritte, negli schemi di contratti e nelle convenzioni di servizio, le responsabilità all'interno del servizio di conservazione, tra ente produttore ed ente conservatore. L'ente conservatore ha descritto gli aspetti relativi al sistema di conservazione, per quanto riguarda diritti, licenze, permessi ottenuti dagli enti produttori (preservation policy e preservation implementation plan). L'ente conservatore gestisce correttamente i diritti di proprietà intellettuale ed eventuali restrizioni nell'utilizzo, come definito nei contratti e nelle convenzioni di servizio.	3.1(a) [3.5.1, 3.5.1.1, 3.5.1.2, 3.5.1.4, 3.5.2] 3.1(a) [3.5.1.3]	-
34	Processi	Il sistema di conservazione assicura in via generale la riservatezza dei documenti conservati, sulla base della propria architettura e dei metodi di conservazione, tramite adeguati controlli. In via eccezionale sono utilizzati algoritmi criptografici standard, qualora sia reso necessario da norme o accordi con enti produttori per proteggere i dati conservati, sempre in conformità alle norme, regolamenti e accordi; inoltre la criptografia è utilizzata per proteggere i dati trasmessi in input e output. Nel caso siano utilizzate tecniche di crittografia, sono presenti i log delle attività eseguite per verifiche, oltre a specifiche procedure di emergenza per assicurare il ripristino dei dati in caso di necessità (perdita o corruzione di dati o indisponibilità del personale critico).	-	A.12.3.1 A.12.3.2 A.15.1.6
35	Processi	I dati personali o le informazioni critiche e sensibili utilizzati nell'ambiente di test sono adeguatamente protetti e controllati, rimossi o modificati dopo il loro utilizzo (teting). La loro copia dall'ambiente di produzione è autorizzata ogni volta che ve ne sia la necessità per obiettivi di test.	-	A.12.4.2

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
36	Processi	L'accesso ai codici sorgente del programma ed agli elementi associati (quali disegni, specifiche, i programmi di verifica e piani di validazione) è strettamente controllato, al fine di evitare l'introduzione di funzionalità non autorizzate ed evitare modifiche involontarie. E' presente una specifica procedura per gestire i seguenti aspetti: le librerie dei codici sorgente non sono mantenute nelle librerie di produzione (ove possibile), il personale di supporto non ha privilegi di accesso illimitati, l'aggiornamento delle librerie e dei codici è strettamente controllato, l'elenco dei programmi è mantenuto in un ambiente sicuro, esiste un log degli accessi alle librerie dei programmi e dei codici sorgente, esiste una copia delle librerie dei programmi e dei codici sorgente. La documentazione ed i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.	-	A.12.4.3
37	Processi	Il processo di cambiamento al sistema di conservazione è attuato sulla base di un processo formale, descritto in una procedura condivisa. Sono testate tutte le modifiche al sistema prima di essere rilasciate in esercizio. Le modifiche sono testate in apposito ambiente di test. Qualunque eccezione è autorizzata ed assicura che le modifiche apportate nello stesso ambiente (sviluppo e test) non impattino l'ambiente e che questo è ripristinabile alla situazione preesistente.	-	A.12.5.1
38	Processi	Sono definite in maniera chiara (ingest: acquisition of content) la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni. Sono descritte e verificate le caratteristiche e le proprietà degli oggetti preservati, al fine di confermare l'autenticità od individuare errori rispetto a tali oggetti. E' mantenuta la documentazione delle tipologie degli oggetti sottoposti a conservazione, per rendere chiari ai fruitori le caratteristiche e le proprietà degli oggetti preservati.	3.1(b), 2.2 [4.1.1, 4.1.1.1, 4.1.1.2]	-
39	Processi	Sono definite e descritte le modalità attraverso cui sono gestiti i pacchetti di versamento e le relative informazioni e metadati.	3.1(a), 2.2 [4.1.2]	-
40	Processi	Sono definite e descritte le caratteristiche dei pacchetti di versamento, necessarie per assicurare la conservazione del pacchetto e rappresentare le informazioni ivi contenute e da conservare, ecc.	3.1(a), 2.2 [4.1.3]	-
41	Processi	E' definito il meccanismo del sistema di conservazione attraverso il quale viene verificata l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa, al fine di identificare eventuali errori di provenienza (ente produttore).	3.1(b), 2.2 [4.1.4]	-

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
42	Processi	E' definito il processo che assicura l'individuazione e correzione degli errori nel SIP al momento della creazione e di potenziali errori di trasmissione tra il produttore ed il conservatore, per ottenere un controllo sufficiente delle informazioni fornite per garantire la conservazione a lungo termine. Esistono specifici log o registri dei file ricevuti durante il processo di ingest e di trasferimento. Sono definite ed applicate le procedure che assicurano la consistenza dei record durante l'intero processo e che rendano tale processo verificabile (audit).	3.1(b), 2.2 [4.1.5]	A.12.2.1
43	Processi	E' descritto il sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate, delle procedure di gestione e di evoluzione delle medesime, 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.	3.1(b), 2.2 [4.1.6]	-
44	Processi	Il processo di acquisizione è monitorabile per assicurare all'ente produttore ed al conservatore la possibilità di analizzare lo stato durante il processo.	3.1(e), 2.2 [4.1.7]	-
45	Processi	E' presente adeguata documentazione a supporto delle attività operative ed amministrative inerenti il processo di acquisizione dei pacchetti di versamento (PDV).	3.1(f), 2.2 [4.1.8]	-
46	Processi	Il sistema di conservazione contiene la descrizione e la denominazione delle varie tipologie di pacchetti d'archiviazione gestiti (PdA) e dei loro elementi identificativi gestiti, come definito dalle Regole tecniche art.8 c.2 lettera e: la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione.	3.1(b), 2.2 [4.2.1, 4.2.1.1, 4.2.1.2]	-
47	Processi	Sono descritte le modalità attraverso le quali il pacchetto di archiviazione (PdA) sia generato a partire dal pacchetto di versamento (PdV), per assicurare una corretta e completa rappresentazione delle informazioni contenute.	3.1(b), 2.2 [4.2.2]	-
48	Processi	Sono descritte le procedure previste in caso di rifiuto di un pacchetto di versamento (PDV) o di non suo inserimento in un pacchetto di archiviazione (PDA), come previsto dalla regole tecniche art.8 c.2 lettera d, con specifico rif. art.9 c.1 lettera c Rifiuto): - 8 d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento; - 9 c) c) il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie;	3.1(b), 2.2 [4.2.3, 4.2.3.1]	-

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
49	Processi	Il sistema di conservazione ha una specifica procedura per la generazione di tutti i pacchetti di archiviazione, con modalità uniche e valide per l'intero sistema ("la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento). La procedura descrive le modalità in caso di cambiamento intervenuto nel processo. Il sistema prevede il controllo su eventuali duplicati, sia per la situazione attuale e tenendo conto anche delle situazioni future. Il sistema di conservazione ha la possibilità di identificare in modalità univoca gli oggetti, anche per diverse locazioni fisiche.	3.1(b), 2.2 [4.2.4, 4.2.4.1, 4.2.4.1.1, 4.2.4.1.2, 4.2.4.1.3, 4.2.4.1.4, 4.2.4.1.5, 4.2.4.2]	-
50	Processi	Sono descritte le modalità con cui sono verificati, identificati e gestiti i formati degli oggetti conservati per garantirne la leggibilità, in caso di applicazione di quanto previsto alle Regole tecniche art.9 c.1 lettera i-j): i) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico; j) la produzione delle copie informatiche al fi ne di adeguare il formato di cui all'art. 11, in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico. Tale modalità è assicurata da tool e metodi per identificare tutti i tipi di oggetti conservati.	3.1(b), 2.2 [4.2.5, 4.2.5.1, 4.2.5.2, 4.2.5.3, 4.2.5.4]	-
51	Processi	Sono descritte le modalità di acquisizione dei metadati (PDI, Preservation Description Information) associati agli oggetti conservati.	3.1(b), 2.2 [4.2.6.1, 4.2.6.2, 4.2.6.3]	-
52	Processi	Il sistema di conservazione descrive i criteri di mantenimento della leggibilità (per la comunità di riferimento in senso ampio) per assicurare la fruibilità e la comprensibilità delle informazioni conservate nel tempo (lungo termine).	3.1(d), 2.2 [4.2.7, 4.2.7.1, 4.2.7.2, 4.2.7.3]	-
53	Processi	Sono descritte le modalità applicate nel sistema per assicurare la conservazione nel tempo delle informazioni (long term preservation) e l'integrità, correttezza e completezza dei pacchetti di archiviazione (PdA). Il sistema di conservazione assicura la possibilità di tracciare i PdA e le eventuali azioni svolte in maniera manuale sugli stessi. Sono presenti specifici log che permettono procedure di verifica da parte delle persone autorizzate o sulla base di report specifici. Il sistema di conservazione ha uno specifico meccanismo per identificare eventuali corruzioni o perdite dei dati a seguito di specifiche azioni eseguite.	3.1(e), 2.2 [4.2.8] 3.1(e) [5.1.1.3]	A.12.2.2

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
54	Processi	Il sistema di conservazione mantiene tutta la documentazione relativa alle azioni gestionali ed ai processi amministrativi rilevanti per la creazione del PdA, per assicurare che sia creato e mantenuto in accordo con le procedure documentate. Eventuali deviazioni dal normale processo possono essere identificate ed indagate.	3.1(e), 2.2 [4.2.10]	-
55	Processi	L'ente conservatore ha descritto le proprie strategie di conservazione relative agli oggetti conservati in merito ai rischi di obsolescenza tecnologica di supporti, formati e metadati e di perdita di integrità degli oggetti stessi.	3.1(f), 2.2 [4.3.1]	-
56	Processi	Nel sistema di conservazione sono definiti adeguati processi e procedure per il monitoraggio dell'ambiente di conservazione per assicurare che gli oggetti conservati restino leggibili e usabili dagli utenti (fruibili). Tali processi e procedure assicurano adeguate notifiche nei confronti del personale del servizio.	3.1(d), 2.2 [4.3.2, 4.3.2.1]	-
57	Processi	E' definito un processo in base al quale eventuali situazioni derivanti delle attività di monitoraggio potrebbero comportare modifiche ai piani di conservazione.	3.1(e), 2.2 [4.3.3, 4.3.3.1]	-
58	Processi	E' definito ed attuato un processo di verifica del sistema di conservazione per dare evidenza dell'efficacia delle attività svolte.	3.1(f), 2.2 [4.3.4]	-
59	Processi	Sono descritte le politiche di conservazione dei pacchetti di archiviazione (PdA), in maniera dettagliata, per assicurare il contenuto dell'informazione per l'ente produttore e l'integrità nel tempo.	3.1(e), 2.2 [4.4.1, 4.4.1.1, 4.4.1.2]	-
60	Processi	Il sistema mantiene tutta la documentazione relativa alle azioni gestionali ed ai processi amministrativi rilevanti per la conservazione, mantenuta in accordo con le procedure documentate. Eventuali deviazioni sono identificate ed indagate.	3.1(e), 2.2 [4.4.2, 4.4.2.1, 4.4.2.2]	-
61	Processi	Sono descritte le informazioni dei metadati identificativi utilizzati per la ricerca degli oggetti conservati e la loro associazione al PDA nel tempo.	3.1(f), 2.2 [4.5.1, 4.5.2, 4.5.3, 4.5.3.1]	-
62	Processi	Sono definite le politiche e le procedure per rendere disponibile l'informazione ("dissemination")assicurandone l'autenticità rispetto all'originale. Tali procedure prevedono anche la registrazione e la risposta agli eventuali errori rispetto ai documenti ed in risposta agli utenti.	3.1(f), 2.2 [4.6.2, 4.6.2.1]	A.12.2.4

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
63	Infrastrutture	Esiste la separazione degli ambienti del sistema di conservazione (sviluppo, test, eventualmente qualità, produzione). I dati e le informazioni utilizzati negli ambienti diversi da quello di produzione (esercizio) sono rimossi quando non più necessari o resi anonimi. Il personale coinvolto nelle attività di sviluppo non è responsabile anche delle attività di test e della loro accettazione formale, per assicurare una separazione dei compiti.	-	A.10.1.4
64	Infrastrutture	E' definito ed attuato un processo di monitoraggio e di valutazione dell'uso delle risorse (capacity management), per analizzare e valutare le attuali prestazioni del sistema ed alla base delle proiezioni e definizione di future esigenze relative alle prestazione od a nuove ed emergenti tecnologie tali da assicurare che le prestazioni del sistema di conservazione siano adeguate e conformi alle necessità, ai livelli di servizi concordati contrattualmente e nelle convenzioni e prevengano l'obsolescenza tecnologica. Il monitoraggio e la valutazione considera tutte le diverse componenti del servizio, per assicurare una visione complessiva in ottica end to end. Il processo di monitoraggio e di valutazione dell'uso delle risorse (capacity management) è eseguito non solo tramite analisi ad hoc, ma anche con strumenti automatizzati in grado di segnalare eventuali alert e messaggi in grado di indirizzare le valutazioni e gli opportuni cambiamenti da valutare sia per l'hardware, che per il software ad esempio per minimizzare i rischi ed i costi, limitare i guasti e migliorare le performance.	3.1(e) [5.1.1.1] 3.1(e) [5.1.1.1.1] 3.1(e) [5.1.1.1.2] 3.1(e) [5.1.1.1.3] 3.1(e) [5.1.1.1.4] 3.1(e) [5.1.1.1.5] 3.1(e) [5.1.1.1.6] 3.1(e) [5.1.1.1.7] 3.1(e) [5.1.1.1.8] 3.1(e) [5.1.1.5]	A.6.1.4 A.10.3.1
65	Infrastrutture	Sono attivate specifiche contromisure contro la minaccia di virus, malware, ecc. con sistemi, processi organizzativi (ruoli, responsabilità) e procedure di controllo ed intervento. I sistemi che assicurano tali contromisure, sono periodicamente aggiornati per assicurare adeguate misure di protezione.	-	A.10.4.1 A.10.4.2

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
66	Infrastrutture	Sono definite le procedure di backup dove sono descritte le politiche attuate, i sistemi interessati, le periodicità, le prove periodiche di restore, le modalità di conservazione, ruoli e responsabilità, ecc. Tutte le persone coinvolte nel sistema di conservazione, interne ed esterne, sono a conoscenza di tali politiche e le attuino sulla base di quanto previsto. Sono periodicamente eseguite analisi e valutazioni rispetto alle necessità ed alle attuali capacità di backup, per definire un piano prospettico rispetto alle tecnologie, processi ed organizzazione tali da preservare il contenuto del sistema di conservazione e delle sue funzionalità. E' sempre tracciabile ed identificabile il numero, la locazione e la reperibilità delle copie eseguite nel processo di conservazione. E' assicurato il mantenimento del tempo delle necessarie informazioni relative all'intero sistema di conservazione, tramite backup. Sono presenti meccanismi che assicurano la sincronizzazione delle copie di un documento, al fine di mantenere unicità ed integrità del sistema di conservazione.	3.1(e) [5.1.1.2] 3.1(e) [5.1.2] 3.1(e) [5.1.2.1] 3.1(e), 2.2 [4.2.9]	A.7.1.1 A.10.1.1 A.10.5.1 A.12.2.3
67	Infrastrutture	I sistemi di rete sono adeguatamente gestiti e controllati, per assicurare la loro protezione dalle minacce e per mantenere la sicurezza dei sistemi, delle applicazioni e delle informazioni di passaggio. E' attuata una separazione dei compiti tra chi si occupa di questi aspetti e coloro che hanno compiti operativi. Sono presenti log e sistemi di monitoraggio per i sistemi di rete. Sono presenti firewall per assicurare un adeguato livello di protezione e separazione del sistema di conservazione da internet e da altre reti. Sono implementate adeguate contromisure da parte di fornitori dei servizi (security features, service levels, sistemi di intrusion detection system, ecc.). In caso di sistemi wireless relativi sempre al sistema di conservazione, sono protetti con sistemi di crittografia e meccanismi di autenticazione ed identificazione. Sono riviste periodicamente le contromisure previste per assicurare la loro coerenza con il piano della sicurezza e con l'analisi del rischio.	-	A.10.6.1 A.10.6.2

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
68	Infrastrutture	Solo per sistemi che prevedono l'utilizzo di supporti fisici rimovibili per la trasmissione dei dati, il personale incaricato (fornitori) è scelto sulla base dei requisiti definiti dal responsabile del servizio. I dati trasmessi con l'utilizzo di supporti fisici, sono protetti con sistemi crittografici. I supporti fisici non presentano riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti, della loro tipologia, ecc. L'ente conservatore, in accordo con l'ente produttore, deve aver definito ed applicato i meccanismi per rendere illegibili tali supporti fisici, dopo aver conservato i documenti in essi contenuti, ed in particolare: - aver cancellato in maniera sicura i dati contenuti, per i supporti riscrivibili - distrutto i supporti fisici in maniera da rendere non recuperabili i dati Tali modalità di gestione fanno parte delle procedure del sistema di conservazione e sono supportate da evidenze.	-	A.10.7.2 A.10.7.3 A.10.8.2 A.10.8.3
69	Infrastrutture	Solo nel caso di spedizione e consegna di documenti via email (SIP e DIP), è utilizzata posta certificata per permettere di tracciare l'intera trasmissione (invio e consegna) ed il sistema di conservazione è coerente con tale possibilità. L'ente conservatore, in accordo con l'ente produttore, deve aver definito ed applicato i meccanismi per assicurare che non siano mantenute ulteriori copie della trasmissione, dopo aver sottoposto a conservazione i dati, ad esempio assicurandosi di aver cancellato tutte le possibili copie dei messaggi di posta elettronica certificata.	-	A.10.8.4
70	Infrastrutture	Sono presenti specifiche procedure tecniche che assicurino la creazione dei log ed il loro mantenimento per le successive verifiche, per tutti i sistemi coinvolti nel sistema di conservazione. I log assicurano una copertura adeguata in termini di profondità del periodo temporale di analisi e di informazioni a disposizione per le analisi da eseguire, in conformità con i vincoli legali e normativi e con specifici accordi con l'ente produttore.	-	A.10.10.1 A.10.10.3
71	Infrastrutture	Il sistema di conservazione, in accordo con i risultati della risk analysis, applica i riferimenti temporali in maniera omogenea ed affidabile ("trusted") e questi sono mantenuti inalterati. Sono presenti sistemi di log per analizzare eventuali modifiche al sistema di apposizione dei riferimenti temporali, anche per sistemi di conservazione presenti in diverse locazioni fisiche e con fusi orari differenti (sincronizzazione ad esempio tra sito primario e sito secondario).	-	A.10.10.6
72	Infrastrutture	Le diverse componenti critiche e significative ("sensitive") del sistema di conservazione sono isolate da altri ambienti, organizzativamente, fisicamente e logicamente.	-	A.11.6.2

n.	Ambito	Requisito di controllo	Riferimento OAIS	Riferimento ETSI
73	Infrastrutture	Le specifiche tecniche, in caso di prodotti acquistati o sviluppati internamente, prevedono anche i requisiti tecnici per i controlli di sicurezza ed in particolare quelli automatici che dovrebbero essere inclusi nel sistema. Tale controlli sono adeguamenti identificati a seguito di una risk analysis e risk benefit assessment e permettono di comprendere le valutazioni svolte da parte dell'ente, in particolare per i nuovi sistemi o in occasione di aggiornamenti significativi. Sono presenti specifici documenti di accettazione dei test o, in alternativa, una valutazione indipendente od una certificazione per tali aspetti.	3.1(e) [5.1.1.4]	A.12.1.1