Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

LISTA DI RISCONTRO PER LA VISITA ISPETTIVA AGID E LA CERTIFICAZIONE DI CONFORMITÀ

v.1 del 14 aprile 2017

Descrizione della Lista di Riscontro per la visita ispettiva AgID e la certificazione di conformità dei conservatori accreditati

Premessa

In base all'articolo 44-bis del decreto legislativo 7 marzo 2005, n. 82 e s.m.i. (Codice dell'amministrazione digitale, di seguito "CAD"), che ha previsto la possibilità per i soggetti conservatori di accreditarsi presso l'Agenzia per l'Italia Digitale per erogare servizi di conservazione alle Pubbliche Amministrazioni, nonché in attuazione di quanto disposto dall'articolo 13 del DPCM 3 dicembre 2013, inerente le Regole tecniche in materia di sistema di conservazione (pubblicato in G.U. n. 59 del 12-3-2014 – Suppl. Ordinario n. 20), l'AgID ha definito, con la circolare n.65 del 10 aprile 2014 recante "Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici" e con il documento "Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza" (di seguito "documento dei Requisiti"), i requisiti che i conservatori accreditati devono possedere.

Il possesso di tali requisiti da parte del conservatore è verificato dall'AgID sia in fase di accreditamento sia durante l'attività di vigilanza mediante:

- l'esecuzione di visite ispettive a cura di AgID;
- l'esame delle relazioni della valutazione della conformità previsti dall'articolo 29 del CAD, rilasciati da un ente terzo accreditato presso "Accredia", l'organismo nazionale italiano di accreditamento.

Le verifiche per il rilascio del certificato di conformità hanno prevalentemente lo scopo di esaminare la presenza nel sistema di conservazione di tutte le procedure e le funzionalità necessarie per il soddisfacimento dei requisiti, mentre le verifiche da eseguire nel corso delle visite ispettive AgID sono rivolte prevalentemente ad approfondire aspetti specifici.

Di seguito si descrive il documento "Lista di Riscontro per le visite ispettive AgID e per la certificazione di conformità dei conservatori accreditati" (di seguito "Lista di Riscontro"), definito con l'obiettivo di supportare l'ispettore nelle sue attività di verifica del possesso dei requisiti richiesti per l'accreditamento da parte dei soggetti accreditati.
La Lista di Riscontro elenca le attività di controllo dei suddetti requisiti eliminando quelle che vengono effettuate per il rilascio della certificazione ISO 27001 e quelle eseguite da AgID nel corso dell'istruttoria di accreditamento.

Le visite ispettive sono eseguite attraverso l'esame di evidenze specifiche quali ad esempio configurazioni, log, verbali di riunioni, risultati di sessioni di test, relazioni di incidenti ed interviste al personale. Nei casi in cui si evidenzino criticità nel corso della visita ispettiva, può essere opportuno ripetere controlli già eseguiti per la certificazione di conformità.

La certificazione di conformità può evidenziare delle non conformità corredate di eventuali tempistiche per la loro risoluzione: ove indicato dal rapporto della certificazione di conformità, nella visita ispettiva successiva, è opportuno ripetere i controlli su quelle attività che hanno comportato la segnalazione delle non conformità.

Organizzazione della Lista di Riscontro

La Lista di Riscontro per le attività di vigilanza e certificazione di conformità è strutturata in campi, di seguito descritti:

1. **ID (identificativo del requisito specifico**): è riportato il codice identificativo indicato nel documento dei Requisiti a cui fanno riferimento le attività di verifica;
2. **ID - Progressivo**: individua la specifica attività di verifica nell'ambito del requisito;
3. **Componente del requisito**: identifica la porzione di requisito per la quale si dettagliano le attività di verifica in carico all'ispettore;
4. **Attività di verifica:** rappresenta sinteticamente i controlli da effettuare per il soddisfacimento del componente del requisito.
5. **Evidenze documentali**: fornisce un elenco non esaustivo dei principali documenti a supporto della attività di verifica descritta;
6. **Elementi da controllare**: fornisce un elenco non esaustivo delle principali evidenze di natura tecnica (ad esempio log, configurazioni, accessi a strumenti specifici) a supporto dell'ispettore per l'esecuzione delle attività di verifica descritte.

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
1	1	Il documento (ISPD - Information Security Policy Document) 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.	L'ispettore deve verificare che il documento ISPD descriva le modalità con cui viene valutata la criticità delle informazioni (information classification levels) rispetto al sistema di conservazione. Le misure di protezione devono essere scelte in modo proporzionato ai differenti livelli di criticità: i dettagli delle misure di protezione devono essere demandati alla politica riguardante le procedure del sistema di conservazione.	Documentazione della Politica di sicurezza delle informazioni (procedure, istruzioni) ISPD;	
	2	Sono svolte le necessarie attività propedeutiche alla revisione periodica del documento (ad esempio il risk assessment), almeno annualmente ed è mantenuta traccia nel tempo delle modifiche effettuate al documento (versioning).	L'ispettore deve verificare che eventuali modifiche all'ISP del sistema di conservazione siano registrate. In particolare deve verificare che: - la procedura di registrazione delle modifiche all'ISP sia definita nel Manuale di conservazione o nel Piano della Sicurezza, e che tale procedura sia disponibile; - esista un registro ove sono riportate le suddette modifiche; - (in caso di utilizzo di un sistema di versioning) tale sistema restituisca la versione attuale del documento ISP e che siano presenti le versioni precedenti e le modifiche che hanno portato alla versione attuale.	Manuale di Conservazione Documentazione della Politica di sicurezza delle informazioni (procedure, istruzioni) ISPD Piano della sicurezza Registro delle modifiche all'ISPD	- log di eventuali strumenti informatici per la gestione della documentazione relativa all'ISPD del sistema di conservazione
	3	Tutte le persone coinvolte nel processo di conservazione sono a conoscenza del documento, per le parti che possono essere condivise	L'ispettore deve eseguire, a campione, interviste al personale coinvolto nel processo di conservazione per verificare se il personale è a conoscenza del documento ISPD aggiornato (almeno per le parti pubbliche e per le parti di propria competenza).		

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	4	e rese pubbliche, con evidenza dell'effettiva comunicazione.	L'ispettore deve verificare, a campione, i registri di presa visione del documento. Ad esempio può: - verificare che esistano registri con le firme del personale a testimonianza che il personale ha preso visione di un aggiornamento o della disponibilità del documento; - verificare che esistano sessioni di aggiornamento dedicate al documento che descrive l'ISP, corredate di verbale e di lista delle presenze; - accedere ai log di un applicativo (ove presente) per la gestione della documentazione e verificare che l'applicativo preveda la funzionalità di distribuzione di versioni aggiornate del documento e di conferma della presa visione del documento, e verificare che esistano evidenze della presa visione della parte pubblica del documento che descrive l'ISP da parte delle persone coinvolte nel processo di conservazione.	Manuale di Conservazione Documentazione della Politica di sicurezza delle informazioni (procedure, istruzioni) ISPD; Piano della sicurezza Registro delle comunicazioni e della presa visione della disponibilità di procedure aggiornate	- eventuali registri di strumenti automatici per la gestione della documentazione
	5	Viene data comunicazione e condiviso con le parti interessate (enti produttori, fornitori ed outsourcer) ogni cambiamento al documento ritenuto significativo	L'ispettore deve verificare che esistano e siano disponibili procedure che prevedono la conferma della presa visione di modifiche e aggiornamenti del documento che descrive l'ISP da parte di enti produttori, fornitori ed outsourcer.	- procedure per la comunicazione delle modifiche del documento a enti fornitori e outsourcer.	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	6	(Ad esempio classificazione delle informazioni, ecc.).	L'ispettore deve verificare a campione, in relazione alla disponibilità del documento ISPD o ad uno specifico aggiornamento dello stesso, ove applicabile, che esistano evidenze dell'avvenuta comunicazione di tale disponibilità o di un aggiornamento ad enti terzi fornitori, produttori ed outsourcer.	- registri per testimoniare l'avvenuta comunicazione di eventuali modifiche al documento ISPD ad enti esterni, - accesso alle versioni del documento ISPD	- eventuali strumenti informatici per la gestione e approvazione della documentazione relativa alla politica di sicurezza delle informazioni del sistema di conservazione
	7	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.	L'ispettore deve verificare che siano definite e disponibili le procedure (e le pianificazioni) relative a: - un percorso di formazione e sensibilizzazione circa le procedure di sicurezza e il documento che descrive l'ISP destinato al personale impiegato nel sistema di conservazione; - sessioni di aggiornamento periodiche e/o straordinarie (ad esempio a seguito di eventuali incidenti di sicurezza). L'ispettore deve verificare che esista l'evidenza dell'avvenuta attuazione dei piani formativi e delle sessioni di aggiornamento: - accedendo ai verbali e ai registri delle sessioni (i verbali devono riportare il contenuto della sessione, la data di esecuzione della sessione di formazione e i partecipanti al corso); - verificando la disponibilità di documentazione a corredo a tali sessioni di formazione (anche nella forma di riferimenti a documentazione non disponibile); - eseguendo interviste al personale impiegato nel sistema di conservazione destinatario della formazione. L'intervista non deve rappresentare un esame delle competenze acquisite ma piuttosto una evidenza dell'avvenuta erogazione del corso.	- Pianificazione delle sessioni di formazione ed aggiornamento, approvata dal management; - registri dell'avvenuta partecipazione a sessioni di formazione/aggiornamento/sensibilizzazione con oggetto l'ISPD e le relative procedure di sicurezza.	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
2	1	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.	L'ispettore deve verificare che il Manuale di conservazione contenga i dati di tutti coloro che hanno assunto nel tempo la responsabilità del sistema di conservazione, evidenziando eventuali periodi in cui tali responsabilità non sono risultate coperte. Nota: si intende come GAP il periodo di non copertura del ruolo di responsabilità del sistema di conservazione.	- Manuale di conservazione	
	2		L'ispettore deve verificare se sono state emesse deleghe alla responsabilità del sistema di conservazione, specificando per tali deleghe soggetti funzioni ed ambiti della delega stessa.	- Manuale di conservazione - eventuali deleghe straordinarie	
	3	È presente ed attuato un piano di aggiornamento professionale per il personale appartenente al servizio di conservazione.	L'ispettore deve verificare che siano definite e disponibili le procedure (e le pianificazioni) relative a - un percorso di formazione circa le funzionalità del sistema di conservazione destinato al personale impiegato nel sistema di conservazione; - sessioni di aggiornamento periodiche e/o straordinarie (ad esempio a seguito di eventuali incidenti di sicurezza). L'ispettore deve verificare che esista l'evidenza dell'avvenuta attuazione dei piani formativi e delle sessioni di aggiornamento: - accedendo ai verbali e ai registri delle sessioni (i verbali devono riportare il contenuto della sessione, la data di esecuzione della sessione di formazione e i partecipanti al corso); - verificando la disponibilità di documentazione a corredo a tali sessioni di formazione (anche nella forma di riferimenti a documentazione non disponibile); - eseguendo interviste al personale impiegato nel sistema di conservazione destinatario della formazione. L'intervista non deve rappresentare un esame delle competenze acquisite ma piuttosto una evidenza dell'avvenuta erogazione del corso.	- Pianificazione delle sessioni di formazione ed aggiornamento, approvata dal management; - registri dell'avvenuta partecipazione a sessioni di formazione/aggiornamento/sensibilizzazione con oggetto l'ISPD e le relative procedure di sicurezza.	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	4	È presente la documentazione ove viene descritta l'organizzazione dell'ente conservatore, ruoli e responsabilità.	L'ispettore deve verificare che eventuali modifiche al Manuale di conservazione siano registrate in appositi verbali, o che siano registrate nei log del sistema di gestione della documentazione. Il Manuale di conservazione, deve riportare la versione corrente.	- Manuale di Conservazione; - verbali di aggiornamento del Manuale di Conservazione e delle relative procedure	- in caso di utilizzo di un sistema di gestione della documentazione , log del sistema ed accesso alle funzionalità del sistema.
3	**1**	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.	L'ispettore deve verificare se sono assegnati specifici compiti di presidio della sicurezza IT all'interno dell'organizzazione		
	2		L'ispettore deve verificare se è rispettata la segregazione dei compiti all'interno dell'organizzazione e se, in caso contrario, sono previsti controlli a compensazione.		
4	**1**	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	L'ispettore deve verificare che sia definita e disponibile una procedura per la gestione delle comunicazioni da e verso l'esterno.	- Procedura per la gestione delle comunicazioni da e verso l'esterno	
	2		L'ispettore deve verificare che la procedura per la gestione delle comunicazioni descriva effettivamente sia le modalità di comunicazione da e verso l'esterno sia le eventuali eccezioni. In particolare le procedure devono impedire agli impiegati del sistema di conservazione la divulgazione delle informazioni riservate (ove per riservate in questa sede di intendono le informazioni soggette a specifici accordi di riservatezza) nei contatti con soggetti od entità all'esterno del sistema di conservazione, senza prevedere l'autorizzazione di un responsabile.	- Procedura per la gestione delle comunicazioni da e verso l'esterno	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	a conoscenza della procedura e la attua.	L'ispettore deve verificare che le comunicazioni formali inerenti il sistema di conservazione e le sue attività, da e verso l'esterno, risultino autorizzate da un responsabile. Tale autorizzazione può essere verificata: - a livello di procedura (ad esempio sono autorizzate tutte le comunicazioni di un certo tipo); - tramite evidenza dell'approvazione (su carta o attraverso strumenti digitali per l'autorizzazione all'esecuzione della comunicazione).	- Procedura per la gestione delle comunicazioni da e verso l'esterno - evidenze della comunicazione e della relativa autorizzazione da parte del management	- log di eventuali strumenti automatici per l'autorizzazione delle comunicazioni
	4		L'ispettore deve verificare tramite interviste al personale che il personale è al corrente delle procedure per le comunicazioni da e verso l'esterno.		
5	**1**	L'ente conservatore ha svolto un'attività di analisi dei rischi rispetto alla propria organizzazione, processi, infrastrutture, sistemi, processi, obiettivi, ecc. 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'ispettore deve verificare che sia stata eseguita un'analisi dei rischi propedeutica all'identificazione ed implementazione delle contromisure e controlli da applicare al sistema di conservazione. Tale analisi dei rischi deve essere esplicitata nel piano della sicurezza: l'ispettore deve verificare che i risultati dell'analisi dei rischi siano stati utilizzati come input per la definizione della politica di sicurezza e delle relative procedure.	- Analisi dei rischi	
	2		L'ispettore deve verificare che l'analisi dei rischi prenda in esame tutti i componenti del sistema di conservazione (fisici e logici, e.g. locali, strumenti, funzioni).	- Analisi dei rischi - Architettura del sistema di conservazione (Manuale di conservazione)	
	3	L'analisi dei rischi considera i rischi relativi alle parti esterne (fornitori, outsourcer, enti produttori, ecc.)	L'ispettore deve verificare che l'analisi dei rischi tenga effettivamente conto delle terze parti coinvolte o che interagiscono con il sistema di conservazione (fornitori, produttori, etc.).	- Analisi dei rischi	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
7	1	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.	L'ispettore deve verificare che i contratti di servizio e le convenzioni con gli enti produttori tengano conto di quanto identificato in sede di analisi dei rischi, con specifico riferimento alle terze parti.	-Analisi dei rischi - contratti con terze parti	
	2	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.	L'ispettore deve verificare che esista evidenza della ricezione ed approvazione del piano della sicurezza di eventuali fornitori/outsourcer. Tale evidenza può essere rappresentata da una approvazione tramite firma o da una approvazione tramite uno strumento di gestione della documentazione.	- verbale di approvazione del piano della sicurezza dei fornitori ed outsourcer (relativamente alle attività di pertinenza del sistema di conservazione)	- eventuale gestore documentale
	3	È presente un piano di continuità, per le attività in outsourcing, coerente con i requisiti indicati nel BCP dell'ente conservatore.	L'ispettore deve verificare se è presente ed attivato un piano di continuità per le attività in outsourcing, coerente con i requisiti del BCP dell'ente conservatore.	- Business Continuity Plan (BCP) degli eventuali enti fornitori ed outsourcer - piano della sicurezza del sistema di conservazione	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	4	L'outsourcer ha definito un piano di ripristino, per le attività in outsourcing, periodicamente rivisto ed approvato dal management dell'ente conservatore.	L'ispettore deve verificare se è stato definito ed è disponibile un piano di ripristino per le attività in outsourcing, coerente con i requisiti dell'ente conservatore. L'ispettore deve verificare che tale piano di ripristino è soggetto a revisione periodica ed è approvato dal management, accedendo ai verbali di revisione e di approvazione del piano di ripristino delle attività in outsourcing.	- piano di ripristino delle attività in outsourcing - pianificazione delle revisioni del piano di ripristino delle attività in outsourcing - verbali di revisione del piano di ripristino delle attività in outsourcing	
	5	È 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.	L'ispettore deve verificare che sia presente la clausola di audit nei contratti di servizio con fornitori ed outsourcer.	- contratti di servizio con fornitori ed outsourcer	
	6	Sono mantenute le versioni del software e la relativa documentazione, nel caso in cui le attività esternalizzate riguardino lo sviluppo software.	L'ispettore deve verificare se , in caso di sviluppo software esternalizzato, viene adottato uno strumento di configuration management (CM). L'ispettore deve verificare la corretta configurazione dello strumento di CM (ad esempio accedendo, a campione e con il supporto dell'ente conservatore, ad una versione del software prodotto da un outsourcer e verificando che è indicato lo stato della versione del software, e.g. corrente o obsoleta, le modifiche apportate rispetto alla versione precedente, la data di applicazione e di ritiro dal sistema di quella specifica versione di software). Nota: sebbene sia preferibile l'utilizzo di un CM, potrebbe non essere l'unico modo per gestire le versioni del software.	- procedure per la gestione del software esternalizzato	- accesso ad eventuali strumenti di configuration management

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
9	1	È 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.	L'ispettore deve verificare se esiste una procedura relativa alla gestione degli asset affidati ai soggetti per i quali si verifica - una interruzione del rapporto di lavoro; - uno spostamento di mansione nel sistema. L'ispettore deve verificare se la procedura contiene la richiesta di registrazione delle seguenti informazioni - l'evento che genera le attività da svolgere; - i vari soggetti coinvolti; - le attività da svolgere (segnalazione dell'evento, gestione degli asset e cancellazione diritti di accesso al sistema).	- procedura restituzione degli asset in caso di interruzione del rapporto di lavoro o di spostamento di mansione - procedura rimozione diritti di accesso al sistema, in caso di interruzione del rapporto di lavoro o di spostamento di mansione	
	2		L'ispettore deve verificare se la procedura è applicata incrociando le informazioni: - dei registri relativi a precedenti interruzioni del rapporto di lavoro o modifiche alle mansioni di soggetti coinvolti nel sistema di conservazione; - dei registri relativi all'assegnazione degli asset a tali soggetti; - della configurazione dei permessi sul sistema di accesso relativi a tali soggetti. L'ispettore deve verificare tramite interviste agli amministratori di sistema se sono al corrente della procedura per la rimozione tempestiva di tutti o di parte dei diritti di accesso al sistema di conservazione ai soggetti non più coinvolti nel sistema o non più coinvolti in una specifica attività.	- procedura restituzione degli asset in caso di interruzione del rapporto di lavoro o di spostamento di mansione - procedura rimozione diritti di accesso al sistema, in caso di interruzione del rapporto di lavoro o di spostamento di mansione	- log accessi al sistema e log accessi al sw di configurazione dei permessi - configurazione permessi del sistema di accesso

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	La procedura prevede la comunicazione ed informazione alle persone coinvolte nel processo di conservazione.	L'ispettore deve verificare anche se la procedura descrive modalità per comunicare ai ruoli interessati eventuali interruzioni di rapporti di lavoro e modifiche alle mansioni di un soggetto che opera nel sistema di conservazione.	- procedura restituzione degli asset in caso di interruzione del rapporto di lavoro o di spostamento di mansione - procedura rimozione diritti di accesso al sistema, in caso di interruzione del rapporto di lavoro o di spostamento di mansione	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
10	**1**	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 Sono previste specifiche procedure di roll back all'interno del processo di cambiamento.	L'ispettore deve verificare che il sistema di conservazione preveda un processo di revisione dei processi critici per il sistema di conservazione, che descriva le attività per l'individuazione e l'analisi di realizzabilità di eventuali migliorie e modifiche al sistema di conservazione. L'ispettore deve verificare che tale processo contenga indicazioni per - identificare ruoli, responsabilità e permessi necessari per attuare le modifiche; - selezionare il personale con le competenze adeguate (ad esempio verificando che il personale è selezionato sulla base delle competenze registrate dall'organizzazione , sul cv o su una matrice ad uso interno); - definire piani di formazione ed eventualmente sviluppo professionale, specifici per il personale coinvolto nell'attuazione delle modifiche. Nel merito del processo, si chiede all'ispettore di verificare inoltre che il processo preveda anche misure di ripristino (rollback) del sistema alla condizione precedente l'applicazione della modifica. Le misure di ripristino devono includere una descrizione delle motivazioni e valutazioni eseguite (ad esempio a seguito di test funzionali sul sistema in campo) per giungere alla conclusione di operare il ripristino allo stato di partenza.	- processo per la gestione delle modifiche al sistema di conservazione (e.g. nel Manuale di Conservazione e/o nel piano della conservazione)	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	È 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	L'ispettore deve verificare - che esistano verbali o presentazioni/descrizioni dei risultati delle analisi svolte relativamente a modifiche e cambiamenti attuati a processi critici del sistema di conservazione; - che esistano evidenze dell'approvazione esplicita ad eseguire tali cambiamenti da parte del responsabile dei sistema di conservazione; - eventualmente che esistano evidenze dell'avvenuta comunicazione dell'esigenza di eseguire tali cambiamenti senza approvazione (in tal caso sarebbe utile capire perché non si è proceduto con l'approvazione).	- verbali o risultati delle analisi e valutazioni eseguite circa l'efficacia dei processi critici del sistema di conservazione che sono stati modificati - documento di approvazione delle modifiche eseguite da parte del responsabile del sistema di conservazione (firma) o eventualmente evidenze di presa visione dell'esigenza di eseguire tali modifiche	- se presenti, log di strumenti per la gestione della documentazione (e.g. approvazione tramite firma digitale o altro del documento che descrive le modifiche e/o presa visione di una specifica comunicazione relativa alle modifiche da attuare)
	3	Il sistema di conservazione permette la tracciabilità dei cambiamenti apportati, tramite versioning o registro del software.	L'ispettore deve verificare che esistano tracce di modifiche attuate ai processi critici del sistema di conservazione: tali evidenze sono reperibili tramite accesso al software di versioning (o di configuration management, CM) verificando che - sia possibile risalire alla versione attuale del software in esercizio; - una modifica a campione attuata ad un processo critico del sistema di conservazione sia identificata in modo univoco in tale SW, specificando la data in cui tale modifica è stata eseguita e il/i soggetti che hanno applicato la modifica; - sia riferita e disponibile sia la versione di SW precedente a quella attualmente in esercizio, sia la versione in campo del codice relativo al SW che recepisce la modifica attuata.		- log del sistema di versioning o registro del software adottato

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	4	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.	L'ispettore deve verificare che il processo preveda - procedure di comunicazione, ad eventuali outsourcer, delle modifiche di eventuali processi critici (tali modifiche devono essere comunicate per tempo a meno di dover fronteggiare emergenze che risultano dimostrabili); - procedure di comunicazione, all'organizzazione del conservatore, di eventuali modifiche ai processi critici del sistema di conservazione operate da outsourcer del sistema (tali modifiche devono essere comunicate per tempo a meno di dover fronteggiare emergenze che risultano dimostrabili). Possibilmente la controparte dovrebbe poter confermare di aver ricevuto notizia delle modifiche comunicate. L'ispettore a campione può verificare se esistono evidenze di tali comunicazioni	- processo per la gestione delle modifiche al sistema di conservazione (e.g. nel Manuale di conservazione e/o nel piano della conservazione); - evidenze di comunicazioni tra conservatore e rispettivi outsourcer (se presenti) relative ad eventuali modifiche operate su processi critici del sistema di conservazione	
11	**1**	È descritta ed effettivamente implementata una segregazione dei compiti nello svolgimento delle attività operative, in coerenza con la separazione organizzativa dei compiti.	L'ispettore deve verificare che: - esista una definizione di ruoli e mansioni nell'ambito delle funzionalità del sistema di conservazione. La definizione di ruoli e mansioni deve evidenziare come sono segregati i compiti; - tale segregazione sia correttamente declinata nei ruoli e nei relativi permessi di accesso configurati per l'accesso alle funzionalità del sistema di conservazione. L'amministratore deve verificare che almeno i compiti di amministratore di sistema, operatore e auditor siano definiti e correttamente segregati.	- definizione di ruoli e mansioni (Manuale di Conservazione, piano della sicurezza); - mansionario (Manuale di Conservazione, piano della sicurezza)	- configurazione del software deputato ad implementare le funzionalità del controllo di accesso al sistema di conservazione; - log del sistema di controllo di accesso

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	Il personale che opera all'interno del sistema di conservazione non ha privilegi amministrativi nei sistemi, ad eccezione del ristretto personale autorizzato.	L'ispettore, tramite l'interazione con le funzionalità di controllo di accesso, e i log del sistema deve verificare che nessun utente con ruolo operatore del sistema di conservazione acceda al sistema con privilegi amministrativi. Nota:i log di accesso al sistema possono essere generati: - dalle applicazioni specifiche del sistema di conservazione; - dal sistema operativo (log di sistema); - da strumenti dedicati alla generazione e gestione dei log.		- configurazione del SW deputato ad implementare le funzionalità del controllo di accesso al sistema di conservazione; - log del sistema di controllo di accesso
12	**1**	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.	L'ispettore deve verificare che - esista un piano della sicurezza e una certificazione ISO 27001 per il sistema di conservazione (e il relativo Statement of Applicability che includa i controlli di sicurezza); - esista una definizione del servizio da assicurare; - i livelli del servizio da parte delle terze parti siano descritti nei documenti del sistema di conservazione.	- Manuale di Conservazione: indicazioni per la predisposizione dei contratti con terze parti - statement of applicability (della certificazione ISO 27001)	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
13	1	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 dai contratti di servizio.	L'ispettore deve verificare che i contratti con terze parti contengano degli accordi sulla qualità del servizio (SLA) adeguati alle esigenze del sistema di conservazione. I contratti devono prevedere la possibilità di una verifica ed ispezione da parte dell'ente conservatore sui sistemi in outsourcing impegnati nelle attività di conservazione oggetto del contratto. (Nota per l'ispettore: non si riporta la possibilità di predisporre strumenti di monitoraggio automatici, L'ETSI fa solo riferimento ad Audit periodici. Comunque sarebbe buona norma poter valutare sempre l'operato dell'outsourcer ad esempio tramite strumenti di monitoraggio basati su parametri misurabili automaticamente)	- contratti di servizio e SLA - eventuale report di audit; - procedure per le ispezioni e l'audit	- eventuali strumenti di monitoraggio dei parametri individuati come riferimento per la fornitura del servizio
	2	Le attività sono formalmente assegnate al management aziendale ed eseguite da personale esperto sempre la supervisione dei responsabili.	L'ispettore deve verificare che in fase di definizione dei contratti verso terze parti sia previsto l'impiego da parte di queste di personale esperto e competente, sotto la responsabilità del management di riferimento per l'ente conservatore.	- contratto di servizio e SLA	
	3	È 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.	L'ispettore deve verificare - l'esistenza di un piano di verifiche ed ispezioni da eseguire presso la sede dell'attività in outsourcing da eseguire; - a campione uno o più verbali relativi alle verifiche ed ispezioni eseguite, presso le sedi delle attività in outsourcing, incrociandoli con il piano di verifiche previsto, e le comunicazioni scambiate con l'ente oggetto dell'ispezione relative all'ispezione sotto verifica.	- pianificazioni delle ispezioni verso terze parti (outsourcer e fornitori) - comunicazioni scambiante con l'ente terzo; - verbali di audit periodici presso le sedi dell'ente terzo	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
14	1	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.	L'ispettore deve verificare che esista una documentazione (anche nella forma di verbali di riunioni) che evidenzi come il management abbia approvato eventuali richieste di modifica al sistema di conservazione, ad esempio di acquisizione di nuovi sistemi, esecuzione di aggiornamenti o installazione di nuove versioni del software impiegato per la conservazione. A titolo di esempio, l'ispettore può chiedere di visionare le evidenze delle motivazioni che hanno consentito al management di approvare un aggiornamento di sicurezza (ad esempio, analisi dell'applicabilità al sistema di conservazione di una vulnerabilità specifica di un COTS, oppure obsolescenza dell'Hardware impiegato nel sistema di conservazione etc.). La documentazione deve essere sotto controllo di configurazione e di accesso, ossia deve risultare periodicamente aggiornata e protetta da accessi non autorizzati.	- evidenze di accettazione della di software specifici da parte del management	- eventuali strumenti per la gestione della documentazione
	2		L'ispettore deve verificare che esiste una documentazione di test utilizzata per l'accettazione di aggiornamenti, modifiche, integrazioni di nuovi componenti o aggiornamenti dei componenti già presenti nel sistema. Tale documentazione di test deve contenere un piano dei test, una descrizione dei test da eseguire, una analisi della completezza dei test rispetto alle caratteristiche del sistema di conservazione e alle funzionalità dell'elemento introdotto, e un risultato positivo o negativo del test.	- documentazione di test di elementi o componenti aggiuntivi al sistema di conservazione	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3		L'ispettore deve verificare che l'acquisizione e configurazione di nodi di rete al sistema di conservazione, sia avvenuta a seguito di una specifica approvazione da parte del responsabile per la sicurezza del sistema di conservazione.	- documentazione di approvazione ufficiale da parte del responsabile per la sicurezza, dell'acquisizione e autorizzazione della connessione al sistema di qualunque nodo di rete.	
	4		L'ispettore deve verificare che esista e sia aggiornata la documentazione di installazione, configurazione e messa in sicurezza di ogni elemento o componente del sistema di conservazione.	- documentazione di configurazione e messa in sicurezza per ogni elemento o componente del sistema di conservazione (ad esempio elaboratori con più funzioni, server, host firewall)	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
15	1	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.	L'ispettore deve verificare che sia definita una politica di controllo di accesso alle informazioni gestite dal sistema di conservazione. La politica deve - tenere in considerazioni tutte le sedi coinvolte nel sistema di conservazione; - definire almeno i seguenti ruoli: operatore, amministratore di sistema, proprietario delle informazioni, auditor, terze parti (ad esempio le autorità preposte alla vigilanza, ove applicabile). La politica deve prevedere almeno i seguenti aspetti: - gli operatori non devono accedere alle configurazioni del sistema su cui operano; - gli amministratori di sistema non devono poter operare come operatori a bassi privilegi sui sistemi che essi stessi amministrano; - gli auditor del sistema di conservazione e i proprietari dell'informazione devono avere solo permessi di lettura; - le terze parti devono avere permessi congruenti alle necessità di accesso.	- politiche di accesso alle informazioni ed al sistema; - eventuali procedure per l'attuazione di tali politiche.	
	2	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.	L'ispettore deve verificare che siano definite procedure di revisione periodica della politica di accesso. Tale processo di revisione deve - rilevare eventuali anomalie; - rilevare se la definizione delle necessità di accesso risultano corrette (o ancora valide a seguito di specifici eventi quali modifiche al sistema); - prevedere eventuali azioni correttive alle politiche.	- piano di revisione periodica della politica di controllo di accesso; - verbali di revisione; - evidenze di azioni correttive apportate alle politiche.	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	La documentazione ed i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.	L'ispettore deve verificare se la politica prevede la definizione di permessi di sola lettura al solo personale autorizzato per - i log degli accessi; - la documentazione relativa agli accessi. L'ispettore deve verificare tramite i file di configurazione che la politica di accesso sia effettivamente implementata nel sistema (ad esempio ispezionando i permessi per l'accesso ad uno specifico SW per la gestione dei log, Sistema operativo o file specifico).	- politiche di accesso alle informazioni ed al sistema e relative procedure	- sistemi di gestione dei log e log degli elementi del sistema di elaborazione; - configurazione dei permessi di accesso ai file di log - configurazione dei permessi del sistema
16	**1**	È definito un processo formale, con specifica procedura, di assegnazione, revisione e cancellazione delle utenze per accedere al sistema di conservazione.	L'ispettore deve verificare che esista una procedura formale attraverso cui assegnare e revocare utenze di accesso al sistema di conservazione a chiunque abbia necessità di accedere al sistema: - utenti dell'ente produttore; - soggetti autorizzati dell'ente conservatore; - fornitori di servizi esterni.	- procedura per la gestione delle credenziali di accesso al sistema;	
	2	Tale processo formale è applicato a chiunque abbia necessità di accedere al sistema, quali utenti dell'ente produttore, ente conservatore, fornitori, ecc.	L'ispettore deve verificare che la procedura formale per l'assegnazione e la revoca delle utenze di accesso al sistema di conservazione a chiunque abbia necessità di accedere al sistema sia effettivamente applicata, ad esempio verificando eventuali verbali di assegnazione delle utenze (a campione, selezionando sia utenti dell'ente produttore, sia soggetti autorizzati dall'ente conservatore sia fornitori di servizi esterni) e riscontrando tali informazioni con i log degli strumenti di gestione delle utenze.		- strumenti per la configurazione delle utenze per l'accesso alle funzionalità del sistema di conservazione.

	3	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.	L'ispettore deve verificare che, a livello di procedura per l'assegnazione delle utenze di accesso: - la richiesta di rilascio di nuove credenziali per l'accesso al sistema provenga da un soggetto autorizzato (e.g. responsabile della conservazione, responsabile della sicurezza del sistema di conservazione); - sia assegnato un solo Identificativo ad ogni utente. Eventuali richieste di accesso di gruppo, devono essere motivate e autorizzate per situazioni eccezionali; - sia prevista l'accettazione delle politiche del sistema di conservazione da parte dell'utente che riceve le credenziali; - sia prevista la registrazione delle credenziali in un registro che mantiene lo storico delle credenziali assegnate; - sia prevista una procedura di revisione delle credenziali per verificare se esiste ancora la necessità di accedere al sistema. Tale procedura dovrebbe utilizzare anche strumenti di ispezione dei log per verificare eventuali utenze inattive. Per verificare l'applicazione effettiva della procedura l'ispettore, con il supporto del sistema di conservazione, sia tramite l'accesso alle funzionalità di configurazione delle utenze per l'accesso al sistema sia attraverso l'ispezione di evidenze documentali, deve - estrarre alcune utenze a campione e verificare che abbiano un solo identificativo, che la sua generazione sia stata approvata, verificare che esista il documento firmato di consegna delle credenziali e di accettazione delle politiche per quell'utente specifico. Il documento deve specificare le autorizzazioni dell'utente (i diritti di accesso); - verificare, tramite le configurazioni delle funzionalità di accesso al sistema di conservazione, se esistono utenze di gruppo e, in caso affermativo, verificare la relativa documentazione a corredo che conferma la situazione straordinaria. Per verificare che gli utenti abbiano consapevolezza delle politiche di accesso l'ispettore può eseguire delle interviste a campione al personale (integrando il controllo eseguito precedentemente).	- procedura per la gestione degli accessi al sistema	- configurazione della funzionalità di accesso al sistema (lista utenti registrati, elenco storico delle credenziali di accesso)

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	4	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.	L'ispettore deve esaminare a campione i verbali relativi alle revisioni eseguite per la valutazione delle necessità di esistenza delle utenze e verificare che le utenze che non hanno più necessità di accedere siano state effettivamente rimosse. L'ispettore deve verificare che esistano e siano utilizzati strumenti per verificare tramite i log degli accessi al sistema, che non risultino accessi al sistema da parte di utenze "inattive"	- procedura per la gestione degli accessi al sistema	- configurazione della funzionalità di accesso al sistema (lista utenti registrati, elenco storico delle credenziali di accesso) - log degli accessi
	5	La documentazione ed i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.	(attività di verifica già descritta per il Requisito #15) L'ispettore deve verificare se la politica prevede la definizione di permessi di sola lettura al solo personale autorizzato per - i log degli accessi; - la documentazione relativa agli accessi. L'ispettore deve verificare tramite i file di configurazione che la politica di accesso sia effettivamente implementata nel sistema (ad esempio ispezionando ai permessi per l'accesso ad uno specifico SW per la gestione dei log, Sistema operativo o file specifico).	- politiche di accesso alle informazioni ed al sistema e relative procedure	- sistemi di gestione dei log e log degli elementi del sistema di elaborazione; - configurazione dei permessi di accesso ai file di log - configurazione dei permessi del sistema
17	**1**	È 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.	L'ispettore deve verificare che esiste una procedura formale attraverso cui assegnare e revocare i permessi di accesso alle funzionalità del sistema di conservazione alle utenze già identificate.	- politiche di accesso alle informazioni ed al sistema e relative procedure	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	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.	L'ispettore deve verificare che sia prevista una procedura di revisione dei permessi accesso alle funzionalità del sistema per ogni utenza: la procedura di revisione ha la finalità di confermare che esista ancora la necessità di accedere a tali funzionalità da parte dell'utenza in esame. La procedura deve prevedere la possibilità di eseguire tale revisione anche a seguito di incidenti di sicurezza relativi ad utilizzi impropri dei permessi di accesso da parte di un utente del sistema di conservazione. Tale procedura dovrebbe inoltre utilizzare anche strumenti di ispezione dei log per verificare la presenza di situazioni in cui utenze hanno determinati permessi ma non ne hanno usufruito in un determinato periodo temporale: tali strumenti sono finalizzati ad individuare eventuali errori di configurazione. Per verificare l'applicazione effettiva della procedura l'ispettore deve - selezionare, con il supporto dell'ente di conservazione, alcune utenze a campione e verificare sia tramite verbali di assegnazione sia attraverso l'accesso alle funzionalità di controllo di accesso, che abbiano permessi di accesso congruenti con le proprie mansioni e che l'assegnazione dei permessi di accesso sia stata approvata da un responsabile; - verificare la funzionalità di controllo di accesso ad esempio eseguendo tentativi di accesso con un utente specifico e verificando che può accedere alle funzionalità per le quali ha i permessi di accesso e che non può accedere alle funzionalità per le quali non dispone dei relativi permessi di accesso. Per verificare che gli utenti abbiano consapevolezza dei propri permessi di accesso l'ispettore può eseguire delle interviste a campione al personale (integrando il controllo eseguito precedentemente).	- politiche di accesso alle informazioni ed al sistema e relative procedure - eventuali verbali di assegnazione di permessi di accesso a specifiche funzionalità del sistema	- configurazione della funzionalità di accesso al sistema; - log degli accessi alle funzionalità del sistema; - accesso alle funzionalità del sistema

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	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.	L'ispettore deve esaminare i verbali relativi alle revisioni eseguite per la valutazione delle necessità di esistenza di specifici permessi di accesso e verificare che i permessi relativi ad utenze che non hanno più necessità di utilizzare una specifica funzione del sistema siano stati effettivamente revocati. Ove possibile l'ispettore deve individuare una segnalazione di utilizzo improprio dei permessi di accesso (o un malfunzionamento del sistema per il controllo degli accessi) e verificare che ha attivato una revisione dei permessi assegnati. L'ispettore deve verificare che esistano e siano utilizzati strumenti per verificare tramite i log degli accessi al sistema, che non esistano utenze che non eseguono più gli accessi alle funzionalità del sistema per le quali dispongono dei relativi permessi di accesso.	- verbali delle revisioni dei diritti di accesso degli utenti;	- log del sistema di controllo degli accessi e delle relative configurazioni - eventuali log degli applicativi che hanno generato la segnalazione di incidenti
	4	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.	L'ispettore deve verificare che le procedure relative alla gestione degli incidenti prevedano - strumenti e configurazioni idonee a rilevare eventuali utilizzi impropri delle credenziali di accesso (ad esempio tentativi di eseguire, da parte di utenti operatori, operazioni che richiedono privilegi di amministrazione); - modalità per segnalare eventuali utilizzi impropri delle credenziali di accesso ed integrare la segnalazione nel sistema di gestione reportistica degli incidenti. L'ispettore deve verificare, attraverso il sistema di gestione della reportistica degli eventi e con il supporto dell'ente conservatore, che siano segnalati gli eventi relativi a utilizzi impropri dei diritti di accesso; L'ispettore deve verificare che tali segnalazioni siano analizzate in un verbale di revisione periodica dei diritti di accesso. L'ispettore può eseguire interviste per verificare l'applicazione delle procedure di revisione dei diritti di accesso.	- verbali delle revisioni dei diritti di accesso degli utenti; - report degli incidenti di sicurezza	- log del sistema di controllo degli accessi e delle relative configurazioni - eventuali log degli applicativi che hanno generato la segnalazione di incidenti

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	5	La documentazione ed i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.	(attività di verifica già descritta per il Requisito #15) L'ispettore deve verificare se la politica prevede la definizione di permessi di sola lettura al solo personale autorizzato per - i log degli accessi; - la documentazione relativa agli accessi. L'ispettore deve verificare tramite i file di configurazione che la politica di accesso sia effettivamente implementata nel sistema (ad esempio ispezionando ai permessi per l'accesso ad uno specifico SW per la gestione dei log, Sistema operativo o file specifico).	- politiche di accesso alle informazioni ed al sistema e relative procedure	- sistemi di gestione dei log e log degli elementi del sistema di elaborazione; - configurazione dei permessi di accesso ai file di log - configurazione dei permessi del sistema
18	**1**	È presente un processo formale per la gestione ed assegnazione delle password di accesso al sistema di conservazione.	L'ispettore deve verificare che esista una procedura formale di assegnazione delle password. La procedura deve prevedere misure procedurali (richieste da inoltrare per l'assegnazione di una nuova password, gestione di blocchi dell'utente ed eventuali segnalazioni) e tecniche (azioni da eseguire per impostare la password, impostazioni di scadenza etc.).	- procedure per l'assegnazione, generazione e gestione delle password	

	2	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.	L'ispettore deve verificare che la procedura l'assegnazione e la gestione delle password: - preveda i controlli minimi (vedi anche allegato B al Codice in materia di protezione dei dati personali) per la generazione della password (lunghezza minima, utilizzo di caratteri alfanumerici e caratteri speciali, etc.) - preveda limitazioni nell'uso della password (scadenza ed eventuali eccezioni per alcune utenze di sistema come ad esempio gli amministratori, etc.) - preveda la comunicazione ai fruitori delle password di tale regole (almeno in sede di primo accesso). In caso di malfunzionamento della funzione di autenticazione devono essere bloccati automaticamente i privilegi di accesso al sistema per gli utenti finali: in tali evenienze l'amministratore di sistema deve essere incaricato di risolvere il problema e ripristinare la normale operatività della funzionalità di autenticazione. La procedura deve prevedere che dopo un certo numero di tentativi errati il sistema blocchi l'utente, registrando l'evento. La procedura deve prevedere che, in caso di autenticazione eseguita senza successo, non sia comunicata alcuna informazione relativamente al tipo di errore accaduto (e.g. non deve essere comunicato all'utente se ha sbagliato user ID o password). La procedura deve prevedere che la password di default per l'accesso alle applicazioni sia modificata al primo accesso. La procedura deve prevedere che le password generate dal sistema risultino uniche (ossia deve prevedere l'implementazione di un controllo per impedire il riuso delle password) ed essere basata sull'utilizzo di valori casuali (ad esempio facendo uso di generatori di sequenze casuali o pseudocasuali). Le aree di memoria utilizzate perla generazione e gestione delle password devono essere cancellate in modo sicuro preferibilmente utilizzando algoritmi standard (possono essere previste eccezioni e misure più lasche laddove si preveda l'utilizzo di One Time Password). La procedura deve prevedere che l'utente accetti	- procedure per l'assegnazione, generazione e gestione delle password	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
			formalmente di cambiare immediatamente la sua password se ha il dubbio ragionevole che la password sia stata compromessa: l'utente in tale evenienza deve anche segnalare l'evento come un incidente di sicurezza. Nei casi in cui si utilizzi un contact center che assiste un utente del sistema, il contact center non deve avere l'opportunità di modificare la password dell'utente di sistema cui fornisce assistenza.		
	3	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.	L'ispettore deve verificare che sia stata condotta una analisi da parte dell'ente conservatore, sia accedendo ai verbali sia verificando che l'analisi è "ragionevole", ossia l'ente conservatore, sulla base della classificazione operata circa la criticità delle informazioni e di eventuali ulteriori normative (e.g. codice in materia di protezione dei dati personali) ha predisposto dei controlli relativi al rispetto di requisiti minimi per le password, ad esempio circa la dimensione (lunghezza minima e/o massima) la composizione (caratteri alfanumerici, caratteri speciali, etc.) o la scadenza.	- procedure per l'assegnazione, generazione e gestione delle password	

	4	Queste regole devono essere applicate per chiunque abbia accesso al sistema, sia per l'ente produttore, che per l'ente conservatore, inclusi i fornitori.	L'ispettore deve verificare a campione, la documentazione utilizzata per la consegna delle password; Inoltre, l'ispettore deve verificare l'effettiva implementazione della procedura accedendo al sistema. Per le verifiche che seguono è opportuno concordare una utenza di test con l'ente conservatore al fine di non creare disservizi sul sistema in esercizio. Ogni verifica sul sistema deve essere concordata con l'ente (ad esempio se è sul sistema in esercizio, l'ente deve attuare le procedure necessarie per non creare disservizi). In particolare l'ispettore deve verificare: - accedendo al sistema (con il supporto dell'ente conservatore) che al primo accesso siano comunicate le modalità di gestione delle password e le responsabilità dell'utente cui è assegnata una specifica password. Inoltre accedendo al sistema l'ispettore deve verificare che il sistema richieda la modifica della password al primo utilizzo (questo controllo può essere anche verificato tramite accesso ai log delle comunicazioni eseguite e dei cambi di password); -accedendo al sistema, che il sistema effettivamente rigetti la generazione di una password (sia periodicamente lato utente sia alla prima generazione) se non rispetta i criteri definiti (e.g. lunghezza, utilizzo di numeri e caratteri) (questo controllo può essere anche verificato tramite accesso ai log delle comunicazioni eseguite e dei cambi di password); - attraverso i log di sistema, che sia stato effettivamente richiesto ad esempio il cambio della password alla scadenza della validità della stessa (questo controllo può essere anche verificato tramite accesso ai log delle comunicazioni eseguite e dei cambi di password); - accedendo al sistema, che il sistema effettivamente blocchi l'accesso dopo un numero predefinito di tentativi di autenticazione falliti e che il sistema non comunichi informazioni relative al tipo di errore verificatosi in fase di autenticazione (questo controllo può essere anche verificato tramite accesso ai log delle comunicazioni eseguite e dei cambi di password); - se il sistema genera password, che le password generate dal sistema risultino uniche e siano generate utilizzando algoritmi standard effettivi o de facto; - che le aree di memoria coinvolte nella gestione, assegnazione ed eventuale generazione delle password siano cancellate in modo sicuro utilizzando	- procedure per l'assegnazione, generazione e gestione delle password; - evidenze della comunicazione delle password	- log dei sistemi di configurazione degli accessi; - accesso al sistema di configurazione degli accessi; - accesso al sistema di conservazione; - log di sistema relativi alle autenticazioni, generate dalle applicazioni del sistema di conservazione

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
			metodologie standard effettive o de facto. L'ispettore deve verificare il log relativi al cambio della password dell'utente in caso di incidente di sicurezza eventuale relativo al sospetto concreto o alla certezza di compromissione della password. Attraverso interviste l'ispettore può verificare se gli utenti del sistema sono al corrente delle procedure aggiornate per la gestione delle proprie password.		
	5	Sono definite e comunicate le regole a tutto il personale coinvolto nel sistema di conservazione (interno, fornitori e terze parti),	L'ispettore deve verificare se l'ente conservatore ha definito politiche per l'utilizzo di strumenti informatici. La politica deve prevedere funzionalità di logoff automatico dal sistema dopo un periodo di inattività.	- politiche per l'utilizzo degli strumenti informatici	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
19	1	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	L'ispettore deve esaminare verbali di comunicazione e verificare che le politiche per l'utilizzo degli strumenti informatici siano state comunicate a tutto il personale coinvolto nel sistema di conservazione (interno, fornitori, terze parti). L'ispettore può verificare che il personale coinvolto nel sistema di conservazione sia al corrente delle politiche per l'utilizzo degli strumenti informatici tramite interviste a campione.	- politiche per l'utilizzo degli strumenti informatici - verbali della comunicazione delle politiche dell'ente conservatore a personale interno, fornitori e terze parti	
	2	Tali regole sono ricomprese all'interno delle policy di sicurezza e coerentemente allineate con quanto previsto dalla normativa sulla privacy.	L'ispettore deve verificare che le politiche di sicurezza dell'organizzazione includano le politiche per l'utilizzo degli strumenti informatici. L'ispettore deve verificare che siano state esplicitamente prese in esame le misure previste dalla normativa sulla privacy (allegato B).	- politiche di sicurezza dell'organizzazione (piano della sicurezza) - politiche circa l'utilizzo degli strumenti informatici	

20	**1**	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.	L'ispettore deve verificare che il piano della sicurezza contenga una procedura di gestione degli incidenti che descriva ruoli, responsabilità e attività da svolgere che preveda la presa visione (e l'accettazione del le regole in esso contenute) da parte dei soggetti i cui ruoli risultano coinvolti nella procedura. In questo caso la conferma di aver ricevuto correttamente le istruzioni per la gestioni degli incidenti risulta di particolare rilevanza. l'ispettore deve verificare che tale procedura preveda: [REPORT INCIDENTI DI SICUREZZA/VULNERABILITA'] - le istruzioni circa come riportare qualunque incidente di sicurezza e vulnerabilità non appena questo/a viene rilevato/a. L'accesso a tali rapporti deve essere consentito solo a persone autorizzate a meno di autorizzazioni esplicite da parte di un responsabile dell'ente conservatore; - le istruzioni su come assegnare un livello di classifica agli incidenti di sicurezza e alle vulnerabilità del sistema; - le modalità per comunicare formalmente le istruzioni per eventuali sub-contraenti coinvolti nel processo di comunicazione (e gli obblighi lato subcontraenti, tra i quali la richiesta di divulgare le istruzioni ai propri operatori); la procedura deve prevedere l'accettazione da parte dei sub-contraenti della ricezione delle istruzioni fornite. [GESTIONE DELL'INCIDENTE E INTEGRAZIONE NELL'ANALISI DEI RISCHI] - il coinvolgimento di un team e la definizione di tempistiche per la risoluzione dell'incidente o per l'analisi della vulnerabilità ed eventualmente le correzioni definite in base alla classificazione assegnata all'evento; - la definizione di un soggetto incaricato responsabile per la gestione delle segnalazioni; - le istruzioni su come gestire incidenti e vulnerabilità del sistema. Sia l'esistenza di un team sia di questo responsabile deve essere comunicato a subcontraenti e terze parti; - la registrazione di ogni azione correlata alla segnalazione dell'incidente o della vulnerabilità rilevata sul sistema: il report deve contenere la causa scatenante lo stato di emergenza, tutte le azioni intraprese, le condizioni che hanno consentito al responsabile di considerare chiusa la situazione di emergenza, il riferimento temporale del ripristino del sistema alle condizioni precedenti la segnalazione.	- procedure per la gestione degli incidenti di sicurezza e del rilevamento di vulnerabilità del sistema. - eventuali rapporti relativi alla gestione di segnalazioni di eventi quali incidenti di sicurezza e vulnerabilità del sistema.	- eventuali strumenti per la gestione degli incidenti (ad esempio workflow per la gestione della segnalazione) - registri degli incidenti di sicurezza e dei relativi report - configurazioni per l'accesso ai report degli incidenti di sicurezza - log di accesso al sistema di gestione degli incident

			L'ispettore deve verificare - che esista e sia disponibile documentazione di approvazione, da parte di ogni operatore impegnato nel sistema di conservazione, di aver preso visione della politica dell'ente relativa alla segnalazione di incidenti e vulnerabilità e delle conseguenze per il non rispetto della politica; - che esistano rapporti di eventuali incidenti di sicurezza o del rilevamento di vulnerabilità di sicurezza del sistema. Tali rapporti devono contenere una descrizione dell'evento, la data di occorrenza, la data di segnalazione, le azioni eseguite, gli elementi che hanno consentito di considerare l'evento risolto e la data di chiusura della segnalazione; nel caso di una nuova vulnerabilità rilevata l'ispettore deve verificare che il rapporto contenga come è stata rilevata tale vulnerabilità, le analisi eseguite circa la sfruttabilità nell'ambiente di utilizzo del sistema, l'analisi di impatto e la conseguente decisione da parte del management in termini di gestione del rischio. - attraverso il sistema di gestione degli incidenti di sicurezza e delle segnalazioni di vulnerabilità che tali eventi siano stati a. classificati in modo corretto; b. gestiti secondo le istruzioni previste dalla procedura. L'ispettore deve verificare inoltre che - non sia possibile accedere alle informazioni relative ai report tramite una utenza non autorizzata, utilizzando le funzionalità messe a disposizione dal sistema; - solo utenze autorizzate abbiano acceduto alle informazioni contenute nei report. Questo controllo può essere verificato tramite eventuali log di accesso allo strumento per la gestione degli incidenti o direttamente tramite log di accesso al report (se lo strumento prevede la generazione di tali report).		

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	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.	L'ispettore deve verificare che la procedura di gestione degli incidenti e di gestione della vulnerabilità tenga in considerazione tutti i soggetti impegnati nel sistema di conservazione (inclusi i soggetti esterni); la procedura deve definire, tra gli altri: - i sistemi sotto monitoraggio; - la tipologia di monitoraggio svolta; - la modalità con cui viene predisposta la reportistica (formato, contenuti, presentazione, permessi di accesso a specifici ruoli etc.). L'ispettore deve accedere a campione: - agli strumenti utilizzati per il monitoraggio e alle relative configurazioni per confermare che la procedura di gestione degli incidenti di sicurezza e di segnalazione delle vulnerabilità è effettivamente applicata; - ad uno o più report di monitoraggio per verificare che contiene le informazioni dichiarate nella procedura.	- report degli strumenti utilizzati per il monitoraggio del sistema di conservazione	- strumenti per il monitoraggio delle vulnerabilità del sistema e relativi log e configurazioni
	3		L'ispettore deve verificare che la procedura sia applicata a tutte le persone coinvolte nel sistema di conservazione (interne ed esterne).	- procedure per la gestione degli incidenti di sicurezza e delle vulnerabilità del sistema di conservazione	
	4	Le persone interessate sono a conoscenza ed hanno accettato i relativi ruoli e responsabilità assegnate.	L'ispettore deve verificare che esista evidenza della presa visione delle procedure relative alla gestione degli incidenti e delle vulnerabilità da parte dei soggetti i cui ruoli risultano coinvolti nella procedura. L'ispettore può verificare se tali soggetti sono al corrente delle procedure relative alla gestione degli incidenti e delle vulnerabilità tramite interviste a campione.	- verbali di presa visione delle procedure per la gestione degli incidenti di sicurezza e delle vulnerabilità del sistema di conservazione	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	5	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.	L'ispettore deve verificare che, a fronte di un evento (incidente di sicurezza/vulnerabilità rilevata) sia stata eseguita una attività di aggiornamento dell'analisi dei rischi e una revisione della politica di sicurezza del sistema di conservazione.	- verbali e rapporti revisione dell'analisi dei rischi e della politica di sicurezza del sistema di conservazione	
21	**1**	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).	L'ispettore deve verificare che esista un piano per la continuità operativa e un piano di disaster recovery. L'ispettore deve verificare: - evidenze dell'attuazione delle procedure ordinarie di supporto al BCP e DRP; - eventuali evidenze dell'attuazione di BCP e DR (nei casi in cui è stato necessario attivare il piano di BCP o in caso di incidente o disastro).	- business continuity plan e disaster recovery - evidenze dell'applicazione del BCP e DR	
	2	Tali piani assicurano la continuità ed il ripristino del 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.	I piani BCP e DRP devono prevedere ruoli e responsabilità assegnate alle persone: tra questi deve essere individuato il responsabile da contattare in caso di disastro e il team di operatori con competenze adeguate da contattare in caso di disastro. Le procedure previste nel BCP devono prevedere che tale team operativo sia disponibile in tempi compatibili con il massimo tempo di disservizio accettabile per il sistema. Il BCP può prevedere che tale team sia interno all'organizzazione o esterno: nel secondo caso devono essere previste sanzioni nel caso in cui il team non reagisca nei tempi stabiliti da contratto. I piani devono considerare tutte le componenti organizzative, operative, del business, tecnologiche, infrastrutturali del sistema di conservazione.	- documentazione risk assessment, business impact analisys - BCP e DRP	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3		L'ispettore deve verificare che il BCP e il piano di DR tengano conto, per ogni tipologia di documento in conservazione, delle tempistiche identificate per il disservizio nei piani BCP, almeno per i seguenti servizi critici del sistema di conservazione: acquisizione di documenti, processo di conservazione dei documenti, presentazione dei documenti.	- documentazione risk assessment, business impact analisys - BCP e DRP	
	4		L'ispettore deve verificare che il BCP e il piano di DR tengano conto, per ogni tipologia di documento in conservazione, delle tempistiche identificate negli accordi contrattuali con gli utenti del servizio di conservazione (produttori, fruitori).	- BCP e DRP - accordi contrattuali con utenti del servizio - accordi contrattuali con terze parti	
	5	Sono presenti apposite procedure di emergenza (contingency) da applicare in attesa del ripristino del servizio.	L'ispettore deve verificare che esistano procedure di emergenza previste da applicare per il ripristino del servizio. Nota: sembra irragionevole prevedere che l'ispettore sia in grado di verificare se le procedure sono adeguate nel merito tecnico di ogni sistema di conservazione: le verifiche che si ipotizzano riguardano unicamente ispezioni di natura procedurale. L'ispettore deve verificare: - se esistono evidenze di almeno una applicazione di procedura di emergenza; - se il sistema ha mantenuto i parametri di qualità del servizio previsti dal BCP e DRP e dagli accordi contrattuali in situazioni di emergenza (e.g. durata del disservizio, funzionalità minime concordate, etc.).	- procedure di emergenza da applicare per il ripristino del servizio; - verbali e rapporti di eventuali situazioni che hanno richiesto l'applicazione della procedura di emergenza	
	6	Sono descritti all'interno dei piani i ruoli e le responsabilità assegnate alle persone.	L'ispettore deve verificare che all'interno dei BCP e del piano di DR siano previsti ruoli e responsabilità. L'ispettore deve verificare se le evidenze di applicazione del BCP e DR mostrano l'effettivo coinvolgimento dei ruoli nelle modalità previste nei piani stessi.	- BCP e DRP - evidenze di applicazione del BCP e del DRP	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	7	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.	L'ispettore deve verificare : - eventuali evidenze (verbali e rapporti) dell'attivazione di un piano di DRP, sulla base dell'analisi delle segnalazioni ricevute; - se la dichiarazione di attivazione di una procedura di DRP risulta (dai verbali) eseguita da un comitato composto almeno anche dal responsabile del servizio di conservazione (in caso negativo dovrebbero essere presenti motivazioni per la scelta del comitato). L'ispettore può verificare l'attuazione dei piani BCP e DRP tramite interviste al personale coinvolto per verificare se sono a conoscenza di tali piani.	- procedure di segnalazione degli incidenti - verbali di attivazione del DRP	- log di eventuali strumenti informatici per la gestione degli incidenti informatici
	8	Tale dichiarazione dovrebbe essere fatta da un "comitato" interno con coinvolgimento del responsabile del servizio di conservazione.	L'ispettore deve accedere a campione ad una dichiarazione di attivazione di una procedura DRP per verificare se è avvenuta ad opera di un comitato che coinvolge il responsabile della conservazione.	- dichiarazione disattivazione di un DRP	
	9	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.	L'ispettore deve verificare se i piani BCP e DRP tengono conto di tutte le componenti organizzative, operative, del business, tecnologiche, infrastrutturali che contribuiscono all'intero sistema e processo di conservazione.	- BCP e DRP - evidenze di applicazione del BCP e del DRP	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	10	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.).	L'ispettore deve verificare che esista una pianificazione delle seguenti sessioni di test periodici: 1) technical recovery testing (per assicurare che il sistema può essere effettivamente ripristinato) Il test deve essere finalizzato a verificare se le funzionalità sono completamente ripristinate nei tempi definiti dal BCP; 2) testing recovery da un sito alternativo (i processi di business risultano operativi in parallelo con le operazioni di recupero e lontano dal sito principale); 3) test dei servizi dei fornitori (finalizzati a confermare che i servizi forniti da fornitori esterni nel tempo soddisfano i parametri di servizio definiti a livello contrattuale). Una ispezione completa deve essere eseguita dal sistema di conservazione con cadenza almeno annuale. 4) test completo di ogni funzione e procedura La pianificazione deve contenere almeno: - un identificativo univoco di ogni test eseguito; - una descrizione della procedura di test; - l'obiettivo del test (ossia la tipologia di verifica e la funzione che si intende verificare); - i risultati attesi; Il report prodotto a seguito di ogni sessione di test deve descrivere il risultato attuale, segnalando eventuali anomalie e difformità rispetto al risultato atteso. L'ispettore deve esaminare, oltre al piano di test, i report relativi ad una sessione di test per verificare se è stato eseguito nelle modalità pianificate, se sono correttamente riportati i risultati attesi e se eventuali anomalie sono state segnalate e gestite (ad esempio attraverso la segnalazione di un incidente)	- piani di test; - rapporti delle sessioni di test; - architettura del sistema di conservazione; - le relazioni di ispezioni da parte del sistema di conservazione verso soggetti esterni	- log delle applicazioni impegnate nelle sessioni di test

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
22	1	Sono indicate le principali norme, regolamenti, standard, politiche, ecc. ritenuti applicabili nel sistema di conservazione e nell'impianto documentale.	L'ispettore deve verificare se sono indicate nel Manuale di conservazione e nel Piano della Sicurezza le principali norme, regolamenti, standard, politiche, ecc. ritenuti applicabili per il sistema di conservazione ed il relativo impianto documentale a supporto (politiche, processi e procedure).	- Manuale di conservazione - piano della sicurezza	
	2	I mantenimento della documentazione soddisfa i requisiti indicati nella parte 1, capitolo 5 e capitolo 7 dello standard ISO 15489.	l'ispettore deve verificare se le regole applicate dall'ente conservatore per il mantenimento della documentazione soddisfano i requisiti indicati nella parte 1, capitolo 5 e capitolo 7 dello standard ISO 15489 (rispettivamente Regulatory Environment e Records Management Requirements)	- Manuale di conservazione	
23	1	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).	L'ispettore deve verificare che siano previste sessioni, preferibilmente non pianificate, di revisione dell'effettiva attuazione delle politiche di sicurezza applicabili ad ogni dipartimento da parte del responsabile del rispettivo dipartimento. L'ispettore deve verificare che tali sessioni prevedano anche l'esame di rapporti di esecuzione di prove di intrusione e rapporti di vulnerability assessment, ed eventuali log di strumenti automatici utilizzati per l'esecuzione delle attività previste.	- procedure per la verifica delle politiche di sicurezza	
	2		L'ispettore deve verificare che esistano evidenze che il personale coinvolto nelle sessioni di revisione dell'applicazione delle politiche di sicurezza sia al corrente delle conseguenze per il sistema di conservazione della non osservazione di tali politiche.	- fogli di presa visione delle procedure	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	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.	L'ispettore deve verificare che negli accordi contrattuali con personale esterno siano definiti ruoli, responsabilità ed obblighi congruenti con quanto definito nelle procedure per la verifica della conformità del sistema di conservazione alle politiche di sicurezza e agli standard di riferimento applicabili.	- procedure per la verifica delle politiche di sicurezza - accordi contrattuali	
24	**1**	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.	L'ispettore deve verificare che sia presente adeguata descrizione della mission dell'ente conservatore nei documenti amministrativi, tecnici e organizzativi generali. Ad esempio la missione dell'ente potrebbe riguardare un target specifico per la conservazione, quale ad esempio la conservazione in ambito pubblica amministrazione.	Documento descrittivo della missione dell'ente (Manuale della qualità)	
	2		L'ispettore deve verificare che la documentazione rifletta l'impegno aziendale per la conservazione a lungo termine, la gestione e l'accesso alle informazioni. La strategia potrebbe essere una declinazione della mission: nel caso dell'esempio di conservazione di documenti della pubblica amministrazione, una strategia potrebbe essere quella relativa all'allineamento nel tempo dell'ente conservatore ai requisiti espressi dalle PA per la conservazione.	Documento descrittivo della missione dell'ente	
25	**1**	È 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'ispettore deve verificare che siano presenti ulteriori documenti descrittivi dell'approccio dell'ente conservatore (ad esempio evidenze oggettive relative all'esecuzione del piano operativo strategico, quali verbali di riunione, documentazione amministrativa, ecc.).	- verbali di riunione, documentazione amministrativa, - piani per assicurare la disponibilità dei dati delle informazioni conservate presso l'ente produttore, in caso di cessazione delle operazioni di conservazione o modifica della propria operabilità	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	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).	L'ispettore deve verificare che l'ente conservatore abbia 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. (nota: l'interoperabilità è anche ottenuta se sono rispettati i requisiti tecnici per la gestione dei pacchetti di archiviazione e dei relativi indici. Questo controllo risulta dunque supportato anche da altri controlli).	- verbali di riunione, documentazione amministrativa, - piani per assicurare la disponibilità dei dati delle informazioni conservate presso l'ente produttore, in caso di cessazione delle operazioni di conservazione o modifica della propria operabilità	
26	**1**	È 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.	L'ispettore deve verificare se l'ente conservatore ha definito 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.	- policy per assicurare la conservazione nel tempo delle informazioni	
27	**1**	Il Manuale di Conservazione descrive il modello organizzativo e la comunità di riferimento (ente produttore, fruitori, community informative, ecc.).	L'ispettore deve verificare se il Manuale di Conservazione descrive il modello organizzativo applicato al servizio e la comunità di riferimento (ente produttore, fruitori, community informative, ecc.).	- Manuale di Conservazione	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
28	1	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.	L'ispettore deve verificare se nel Manuale di conservazione sono descritte tutte le componenti del sistema di conservazione, comprensivo di tutte le componenti organizzative, procedurali, tecnologiche ed infrastrutturali, fisiche e logiche, opportunamente documentate.	- documentazione di progetto: architettura logica e fisica del sistema di conservazione	
	2		L'ispettore deve verificare se nel Manuale di Conservazione sono presenti le procedure di gestione e di evoluzione per le componenti del sistema di conservazione.	- manuali operativi del sistema di conservazione; - manuali di installazione del sistema di configurazione	
29	1	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.	L'ispettore deve verificare se sono descritte ed applicate le modalità attraverso le quali assicurare trasparenza per le proprie attività e la responsabilità per le azioni operative e gestionali, rispetto al sistema di conservazione.	- procedure per la comunicazione a chi ne fa richiesta delle modalità attraverso cui assicura la trasparenza	
	2		L'ispettore deve verificare se è mantenuta adeguata documentazione per assicurare anche a posteriori tale trasparenza.	- procedure per la comunicazione a chi ne fa richiesta delle modalità attraverso cui assicura la trasparenza	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
31	1	L'ente conservatore svolge una verifica periodica della conformità alle normative ed agli standard.	L'ispettore deve verificare che sia definita nel Manuale di Conservazione una procedura per eseguire audit periodici finalizzati a verificare che sia mantenuta conformità agli standard di riferimento e alle normative applicabili.	processo formalizzato di revisione periodica della conformità alle normative ed agli standard	
	2		In base alla lista di normative e standard dichiarati, l'ispettore deve ispezionare a campione i report di tali audit, verificando la periodicità con la quale sono condotti, le modalità di esecuzione e i controlli eseguiti per confermare la conformità a standard e normative.	- verbali degli audit di revisione della conformità agli standard e normative	

33	**1**	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.	L'ispettore deve verificare che gli schemi di contratti e le convenzioni di servizio, oltre al Manuale di conservazione, descrivano le modalità attraverso le quali è svolto il servizio di conservazione. Tale controllo è relativo principalmente alle attività del conservatore nei confronti di privati: nel caso di conservazione per la P.A. gli schemi di contratto sono stabiliti dalla PA.	- schemi di contratti e convenzioni di servizio - Manuale di conservazione	art. 6 c7 (regole tecniche) Manuale di Conservazione e schemi di contratti e convenzioni di servizio: processi di trasformazione in riferimento al registro dei formati oppure giustificazione della mancata trasformazione in rapporto alla Comunità di Riferimento le modalità relative ad acquisizione, manutenzione, fruibilità e scarto degli oggetti conservati condizioni particolari in riferimento ai diversi produttori/clienti quando avviene la presa in custodia e di

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
					conseguenza quando si diventa responsabili degli oggetti conservati esplicitare il Quadro Normativo di Riferimento

	2	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.	L'ispettore deve verificare che gli schemi di contratti e nelle convenzioni di servizio, oltre al Manuale di conservazione, descrivano i principali aspetti del servizio di conservazione per i documenti conservati e le modalità di versamento, di archiviazione e di distribuzione. Tale controllo è relativo principalmente alle attività del conservatore nei confronti di privati: nel caso di conservazione per la P.A. gli schemi di contratto sono stabiliti dalla PA.	- schemi di contratti e convenzioni di servizio - Manuale di conservazione	art. 6 c7 (regole tecniche) Manuale di Conservazione e schemi di contratti e convenzioni di servizio: processi di trasformazione in riferimento al registro dei formati oppure giustificazione della mancata trasformazione in rapporto alla Comunità di Riferimento le modalità relative ad acquisizione, manutenzione, fruibilità e scarto degli oggetti conservati condizioni particolari in riferimento ai diversi produttori/clienti quando avviene la presa in custodia e di

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
					conseguenza quando si diventa responsabili degli oggetti conservati esplicitare il Quadro Normativo di Riferimento
	3	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'ispettore deve verificare che le responsabilità all'interno del servizio di conservazione, tra ente produttore ed ente conservatore siano definite e descritte negli schemi di contratti e nelle convenzioni di servizio. Tale controllo è relativo principalmente alle attività del conservatore nei confronti di privati: nel caso di conservazione per la P.A. gli schemi di contratto sono stabiliti dalla PA.	- schemi di contratti e convenzioni di servizio - Manuale di conservazione	
	4	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'ispettore deve verificare che siano descritti gli aspetti relativi al sistema di conservazione, per diritti, licenze, permessi ottenuti dagli enti produttori (preservation policy e preservation implementation plan). Tale controllo è relativo principalmente alle attività del conservatore nei confronti di privati: nel caso di conservazione per la P.A. gli schemi di contratto sono stabiliti dalla PA.	- preservation policy - implementation plan	
	5	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.	L'ispettore deve verificare che siano conservati i contratti e le convenzioni di servizio con gli enti produttori che abbiano assegnato il servizio o parte di esso all'ente conservatore.	- contratti - convezioni di servizio	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	6	L'ente conservatore gestisce correttamente i diritti di proprietà intellettuale ed eventuali restrizioni nell'utilizzo, come definito nei contratti e nelle convenzioni di servizio.	L'ispettore deve verificare se sono gestiti i diritti di proprietà intellettuale ed eventuali restrizioni nell'utilizzo, come definito nei contratti e nelle convenzioni di servizio.	- contratti - convenzioni di servizio - Manuale di conservazione e procedure per la gestione di diritti si proprietà intellettuale	
34	**1**	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.	Qualora siano utilizzati nel sistema strumenti crittografici per la protezione dei documenti in conservazione, l'ispettore deve verificare che: - le implementazioni di tali strumenti realizzino algoritmi crittografici standard (o standard di fatto) con robustezza dichiarata sufficiente a resistere ad attacchi che richiedono per la riuscita un tempo superiore alla vita dei documenti da conservare. - esistano procedure in grado di garantire che non circolino dati in chiaro relativi ai documenti conservati, fatta eccezione per metadati concordati con il produttore; - esistano procedure per fornire dati in chiaro su richiesta delle autorità competenti. La politica di sicurezza del sistema di conservazione deve monitorare le novità in ambito crittografico e se necessario eseguire aggiornamenti degli algoritmi di sicurezza e/o delle implementazioni che ne fanno uso. - l'ispettore deve verificare a campione se uno specifico documento in conservazione estratto al momento della visita ispettiva e per il quale si è concordato (o risulta obbligatorio dalle normative vigenti) applicare la cifratura, risulta effettivamente cifrato con l'algoritmo di cifratura specificato nella documentazione. - l'ispettore deve eseguire la procedura che definisce le modalità per decifrare le informazioni su richiesta di una entità autorizzata.	- procedure per la gestione della protezione delle informazioni in conservazione - procedure per l'accesso alle informazioni in conservazione da parte dell'autorità che ne fa richiesta (ove previsto)	- accesso ai sistemi di generazione della chiave crittografica, - accesso alle informazioni protette da crittografia, - log delle applicazioni che realizzano le funzionalità crittografiche

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	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).	L'ispettore deve confermare l'effettivo utilizzo delle funzionalità di cifratura verificando i log degli applicativi preposti alla realizzazione degli algoritmi crittografici.		- log delle applicazioni che realizzano le funzionalità crittografiche
	3		L'ispettore deve verificare l'efficacia delle procedure per il recupero delle chiavi crittografiche in caso di corruzione della chiave principale o indisponibilità delle persone incaricate di eseguire le procedure ordinarie. In caso di utilizzo di tecniche crittografiche l'ispettore deve verificare se esistono procedure di gestione dell'incidenti di sicurezza relativo alla compromissione delle chiavi di cifratura o se ci sono evidenze di una violazione dello strumento che utilizza il meccanismo di crittografia.	- procedure specifiche per la gestione degli incidenti di sicurezza in caso di compromissione di una chiave crittografica - procedure per il recupero delle chiavi crittografiche in situazioni straordinarie	
35	**1**	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 (testing).	L'esecuzione di attività di verifica può richiedere l'utilizzo di dati personali o informazioni classificate come "critiche" o sensibili. L'ispettore deve verificare se nell'ambiente di test siano presenti dati personali o informazioni classificate dal sistema di conservazione come critiche o sensibili: questa verifica può risultare soddisfatta sia accedendo direttamente alle informazioni memorizzate nell'ambiente di test sia attraverso la visione di procedure specifiche per la gestione di dati personali o informazioni critiche.	- piano di test - procedure di test	- accesso ai dati conservati nell'ambiente di test

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2		L'ispettore deve verificare se il piano dei test e le relative procedure, in caso di utilizzo di dati personali o informazioni classificate come critiche o sensibili per il sistema di conservazione, prevede misure di protezione per tali informazioni. Le procedure devono descrivere le modalità attraverso cui al termine del test sono rimosse o modificate le informazioni utilizzate per il test (soprattutto nel caso in cui tali informazioni ricadono nella categoria di cui sopra) In particolare, nel caso di - dati personali: il sistema di test deve rispettare le indicazioni dell'allegato B del D.LGS. 30/6/2013 n. 196 Codice in materia di protezione dei dati personali; - informazioni sensibili o critiche : il sistema di test in questo caso deve realizzare la stessa politica del sistema in esercizio (a meno che il sistema di conservazione non abbia fatto la scelta, motivata, di utilizzare in ambiente di test una tipologia di dati più critica di quelli utilizzati in esercizio).	- piano di test - procedure di test	- log dei sistemi impiegati nell'ambiente di test; - configurazione degli strumenti impiegati negli ambienti di test;
	3	La loro copia dall'ambiente di produzione è autorizzata ogni volta che ve ne sia la necessità per obiettivi di test.	Qualora per l'esecuzione di test si utilizzino dati personali o informazioni critiche o sensibili per il sistema di conservazione, l'ispettore deve verificare se le procedure di test prevedono l'approvazione dell'utilizzo di tali dati. L'ispettore deve verificare se sui verbali o rapporti delle sessioni di test eseguite, sono presenti le eventuali approvazioni da parte del responsabile del sistema di conservazione per l'utilizzo di dati personali o delle informazioni in oggetto.	- piano di test - procedure di test - verbali delle sessioni di test	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
36	**1**	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.	L'ispettore deve verificare se - è presente ed è configurato correttamente un sistema di gestione della configurazione; - sono previsti ruoli per l'accesso a tali strumenti e se tali ruoli risultano correttamente configurati sul sistema (nello specifico solo gli sviluppatori autorizzati e i relativi responsabili devono poter accedere al codice sorgente); - le modifiche alla configurazione e al software sono eseguite a seguito di una approvazione formale. L'ispettore deve esaminare a campione una registrazione di attività di modifica al software, confermando che - esiste una approvazione della modifica da eseguire (firma, presa visione etc.); - la modifica è eseguita da personale autorizzato. L'ispettore deve verificare tramite interviste al personale che il personale sia al corrente delle politiche per l'accesso al codice del software del sistema di conservazione e alla relativa documentazione di sviluppo.	- procedure per la gestione del codice sorgente dei SW del sistema di conservazione e alla relativa documentazione di progetto - rapporti di modifiche e aggiornamenti eseguiti al SW.	- configurazione del sistema di gestione della configurazione e documentazione (CVS - CM) - log degli accessi al sistema di gestione della configurazione e documentazione

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	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.	L'ispettore deve verificare che esistano procedure per fare si che - le librerie del codice sorgente risultino memorizzate in un ambiente separato dall'ambiente in esercizio (ad esempio su macchine differenti separate logicamente e/o fisicamente. Un esempio potrebbe essere il seguente: l'ambiente di sviluppo è fisicamente isolato dall'ambiente in esercizio, oppure l'ambiente di sviluppo è su una sottorete isolata tramite funzionalità di firewall); - il personale di supporto non abbia privilegi di accesso illimitati alle librerie del codice sorgente; - l'elenco dei programmi sia mantenuto in un ambiente sicuro (accesso logico controllato, ad esempio tramite funzionalità di autenticazione di un software di configuration management; accesso fisico controllato ad esempio tramite misure di controllo degli accessi fisici come badge e porte blindate) e siano registrati in un registro specifico tutti gli accessi alle librerie dei programmi e dei codici sorgente; - esista almeno una copia di backup delle librerie dei programmi e dei codici sorgente. L'ispettore deve verificare tramite log dello strumento per la gestione del codice sorgente se, a campione, l'accesso al codice sorgente e alla relativa documentazione, programmi di verifica e piani di validazione è registrato e genera log. L'ispettore deve verificare se i log generati dall'accesso al codice sorgente e alla relativa documentazione risultano coerenti con le politiche impostate per l'accesso a tali dati.		

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	La documentazione ed i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.	(attività di verifica già descritta per il Requisito #15) L'ispettore deve verificare se la politica prevede la definizione di permessi di sola lettura al solo personale autorizzato per - i log degli accessi ; - la documentazione relativa agli accessi. L'ispettore deve verificare tramite i file di configurazione che la politica di accesso sia effettivamente implementata nel sistema (ad esempio ispezionando ai permessi per l'accesso ad uno specifico SW per la gestione dei log, Sistema operativo o file specifico.	- politiche di accesso alle informazioni ed al sistema e relative procedure	- sistemi di gestione dei log e log degli elementi del sistema di elaborazione; - configurazione dei permessi di accesso ai file di log - configurazione dei permessi del sistema
37	**1**	Il processo di cambiamento al sistema di conservazione è attuato sulla base di un processo formale, descritto in una procedura condivisa.	Nota per l'ispettore: alcuni controlli possono risultare parzialmente soddisfatti dalle attività previste per il soddisfacimento del requisito 10. L'ispettore deve verificare che esista una procedura condivisa per la gestione delle modifiche al sistema di conservazione: - la procedura deve prevedere anche le istruzioni per ripristinare la situazione preesistente all'applicazione della modifica; - la procedura, ove preveda eccezioni all'applicazione in campo di una modifica (ad esempio in caso di emergenza), deve presentare motivazioni convincenti circa la necessità di non eseguire parte o tutti i test previsti dalle procedure standard. L'ispettore deve verificare tramite intervista al personale che il personale addetto allo sviluppo sia al corrente delle procedure per l'applicazione di modifiche al sistema in campo (ivi incluse le verifiche circa l'esecuzione di test sulle modifiche da applicare). L'ispettore deve verificare tramite i verbali relativi alle modifiche operate al sistema che esista evidenza dell'esecuzione di verifiche della corretta implementazione (test) di tutte le modifiche da applicare al sistema.	- verbali dell'applicazione delle modifiche al sistema e relative approvazioni - relazioni circa l'esito dei test eseguiti sulle modifiche applicate al sistema	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2		Controllo già soddisfatto dalla procedura di change management (requisito 10)		
	3	Le modifiche sono testate in apposito ambiente di test. (integrazione: Sono testate tutte le modifiche al sistema prima di essere rilasciate in esercizio)	La procedura per l'attuazione delle modifiche al sistema di conservazione deve prevedere che tutte le modifiche e le componenti soggette a modifica siano interessate da apposite sessioni di test, eseguite nell'apposito ambiente di test predisposto dall'ente conservatore.	- procedura per l'attuazione delle modifiche al sistema di conservazione - piani di test	
	4	Qualunque eccezione è autorizzata ed assicurar che le modifiche apportate nello stesso ambiente (sviluppo e test) non impattino l'ambiente e che questo è ripristinabile alla situazione preesistente.	L'ispettore deve verificare che, ove la procedura preveda situazioni di emergenza (attuazione di modifiche senza l'esecuzione di test specifici), le soluzioni adottate in emergenza risultino approvate da un responsabile del sistema di conservazione.	- procedura per l'attuazione delle modifiche al sistema di conservazione - piani di test	
	5		L'ispettore deve verificare se esistono evidenze di eccezioni nell'applicazione delle modifiche al sistema di conservazione (nella forma di modifiche attuate senza che fossero eseguiti tutti o parte dei test previsti) e se tali evidenze sono accompagnate da una approvazione specifica di un responsabile del sistema di conservazione.	- verbali dell'attuazione di una modifica - approvazione dell'attuazione di una o più modifiche in via eccezionale senza aver eseguito sessioni di test	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	6	Le modifiche sono testate in apposito ambiente di test.	L'ispettore deve verificare che il piano dei test contenga almeno: - un identificativo univoco di ogni test eseguito; - una descrizione della procedura di test; - l'obiettivo del test (ossia la tipologia di verifica e la funzione che si intende verificare); - i risultati attesi. Il report prodotto a seguito di ogni sessione di test deve descrivere il risultato attuale, segnalando eventuali anomalie e difformità rispetto al risultato atteso. L'ispettore deve esaminare, oltre al piano di test, i report relativi ad una sessione di test per verificare se i test risultano eseguiti nelle modalità pianificate, se sono correttamente riportati i risultati attesi e se eventuali anomalie sono state segnalate e gestite (ad esempio attraverso la segnalazione di un incidente)	- documentazione di test: verbali e risultati ottenuti	
38	**1**	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.	L'ispettore deve verificare che, nel Manuale di conservazione, sia identificato il contenuto informativo e le proprietà di ogni oggetto da conservare. L'ispettore deve verificare che le procedure relative alla conservazione contengano il registro dei formati conservati e la relativa tipologia di metadati ad essi associati. L'ispettore deve verificare a campione se quanto dichiarato nel Manuale di conservazione è coerente con quanto dichiarato negli allegati tecnici ai contratti e se eventuali eccezioni sono riportate nei contrati.	- Manuale di conservazione: descrizione delle tipologie di oggetti sottoposti a conservazione - allegati tecnici ai contratti	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	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.	L'ispettore deve verificare se le procedure di acquisizione dell'oggetto da conservare descrivono: - in che modo viene accertato il formato dell'oggetto da conservare; - quali formati sono accettati; - quali formati sono verificati; - quali formati sono conservati a lungo termine; - quali tipologie di verifiche sono previste dal sistema relativamente agli oggetti da acquisire nel sistema di conservazione per confermare l'integrità dal dato ricevuto e in caso la validità della firma apposta all'oggetto (firma corretta, certificato di firma valido, autorità di certificazione valida). - il comportamento del sistema di conservazione in caso di ricezione di oggetti non conformi a quanto descritto nel Manuale di conservazione o negli accordi con l'ente produttore. L'ispettore deve verificare il comportamento del sistema accedendo ai log della funzione di verifica della validità degli oggetti sottoposti a conservazione e dei relativi metadati: - a campione deve accedere ad uno o più oggetti, con il supporto di un operatore dell'ente di conservazione e tramite gli strumenti messi a disposizione dal sistema di conservazione, e verificare se il formato effettivo è conforme ai formati descritti nel Manuale o nei contratti; - a campione deve accedere ai log del sistema di conservazione e verificare gli eventi di acquisizione di uno specifico oggetto e le relative registrazione (ivi incluso un controllo non andato a buon fine e il relativo rigetto dell'oggetto da parte del sistema di conservazione).	- procedure per l'acquisizione degli oggetti e la verifica della corrispondenza ad un formato specifico previsto dal Manuale di conservazione e/o da accordi contrattuali con gli enti produttori.	- funzionalità del software di acquisizione degli oggetti da conservare - log relativi alle acquisizioni degli oggetti da conservare e alle relative verifiche di correttezza e completezza degli oggetti consegnati dal produttore al sistema di conservazione

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	È mantenuta la documentazione delle tipologie degli oggetti sottoposti a conservazione, per rendere chiari ai fruitori le caratteristiche e le proprietà degli oggetti preservati.	L'ispettore deve verificare che sia a disposizione dei fruitori del servizio di conservazione un documento che descrive le caratteristiche e le proprietà degli oggetti preservati.	- Manuale di conservazione: descrizione delle tipologie di oggetti sottoposti a conservazione; - eventuale documentazione dedicata ai fruitori delle informazioni	
39	**1**	Sono definite e descritte le modalità attraverso cui sono gestiti i pacchetti di versamento e le relative informazioni e metadati.	L'ispettore deve verificare che il Manuale di conservazione preveda una descrizione delle modalità di gestione dei pacchetti di versamento e delle relative informazioni e metadati (acquisizione, presa in carico, generazione pacchetti di archiviazione). In particolare deve essere descritto - le modalità per l'invio del pacchetto di versamento; - quali metadati vengono utilizzati e come sono classificati.	- Manuale di conservazione: descrizione delle tipologie degli oggetti sottoposti a conservazione; - allegati tecnici: formato del pacchetto di versamento; - allegati tecnici: procedure per l'acquisizione del pacchetto di versamento (invio lato produttore del documento e acquisizione lato ente conservatore)	- pacchetto di versamento; - log del sistema: ricezione di un pacchetto di versamento e log delle verifiche eseguite su un pacchetto di versamento)

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
40	**1**	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.	L'ispettore deve verificare che il Manuale di conservazione ed eventualmente gli accordi contrattuali con il produttore descrivano il formato del pacchetto di versamento e dei relativi metadati.	- allegati tecnici: formato del pacchetto di versamento e dei relativi metadati	- pacchetto di versamento
41	**1**	È 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).	Il sistema di conservazione deve acquisire i documenti attraverso un canale sicuro che protegge le informazioni scambiate per diversi aspetti: cifratura, non ripudio, integrità. Il canale sicuro è generato a seguito della definizione del contratto con l'ente produttore; in tal senso si ritiene il soggetto "identificato in modo certo". L'ispettore deve verificare che le procedure di acquisizione dei pacchetti di versamento prevedano l'istaurazione di un canale protetto con caratteristiche di verifica dei mittenti del messaggio e di firma di ogni messaggio scambiato. L'ispettore deve accedere ai log di sistema e verificare che tale canale è effettivamente istaurato.	- allegati tecnici: procedure per l'acquisizione del pacchetto di versamento (invio lato produttore del documento e acquisizione lato ente conservatore)	- applicazione per la generazione di un canale fidato verso l'ente produttore - log dell'applicazione di generazione di un canale fidato
42	**1**	È 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.	L'ispettore deve verificare che esista una procedura per l'acquisizione, la verifica e l'eventuale rifiuto del pacchetto di versamento. L'ispettore deve verificare che sia applicata una procedura per l'acquisizione, la verifica e l'eventuale rifiuto del pacchetto di versamento, accedendo con il supporto del sistema di conservazione ai log del sistema.	- procedura di acquisizione del pacchetto di versamento, verifiche del pacchetto di versamento, rifiuto del pacchetto di versamento; - allegati tecnici ai contratti	- log degli applicativi utilizzati per la trasmissione dei messaggi

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2		L'ispettore deve verificare che siano previsti ed implementati meccanismi di individuazione e correzione degli errori durante la trasmissione del pacchetto di versamento (specificando l'algoritmo utilizzato e il numero e la tipologia di errori che il sistema deve essere in grado di rilevare e/o correggere). Questo requisito può risultare soddisfatto realizzando un canale dotato di funzionalità di controllo dell'integrità. In tal caso l'ispettore deve verificare che l'applicativo che realizza il canale con controllo dell'integrità dei messaggi scambiati sia configurato correttamente accedendo alle configurazioni dell'applicativo stesso. Eventuali anomalie (errori nella trasmissione e in generale verifiche fallite dell'integrità del messaggio) devono generare una segnalazione gestita come previsto nel piano della sicurezza e nel Manuale di conservazione.	- procedura di acquisizione del pacchetto di versamento, verifiche del pacchetto di versamento, rifiuto del pacchetto di versamento;	- accesso alla funzionalità di verifica dell'integrità - accesso alle configurazioni del canale sicuro
	3	Esistono specifici log o registri dei file ricevuti durante il processo di ingest e di trasferimento.	L'ispettore deve verificare che esistano log del trasferimento dei messaggi relativi ai pacchetti di versamento. Il controllo può essere eseguito ad esempio tramite accesso ai log dell'applicativo che realizza, lato sistema di conservazione, il canale sicuro oppure tramite accesso ad un sistema di gestione e visualizzazione dei log.	- procedura di acquisizione del pacchetto di versamento, verifiche del pacchetto di versamento, rifiuto del pacchetto di versamento;	- log degli applicativi utilizzati per la trasmissione dei messaggi

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	4	Sono definite ed applicate le procedure che assicurano la consistenza dei record durante l'intero processo e che rendano tale processo verificabile (audit).	Nota per l'ispettore: la consistenza dell'intero processo è garantita da: - la presenza di una canale che garantisce l'integrità dei dati trasmessi sul canale da produttore a conservatore; - la natura automatica del processo di trasformazione del PDV in PDA; - la firma del PDA da parte del responsabile. L'ispettore deve verificare che la funzione di produzione del PDA a partire dal PDV ricevuto correttamente sia automatica e non preveda interazioni umane che possano modificare il contenuto informativo del PDA. L'ispettore deve esaminare a campione i log prodotti dallo strumento utilizzato al fine di confermare l'effettiva applicazione della funzione di produzione automatica del PDA.	- documentazione di sviluppo delle funzionalità del sistema di conservazione	- evidenze e log dello strumento di produzione del PDA a partire da un PDV
	5		L'ispettore deve confermare che il processo di acquisizione è complessivamente verificabile, (ossia predisposto per subire un audit).		

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
43	**1**	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.	L'ispettore deve verificare che esista adeguata documentazione e descrizione per tutte le componenti del sistema di conservazione (la documentazione di riferimento riguarda tutte le componenti tecnologiche, fisiche e logiche, le procedure di gestione e di evoluzione delle medesime, le procedure di monitoraggio della funzionalità del sistema di conservazione e le verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie) Ad esempio, l'ispettore deve verificare che esista: - una descrizione dell'architettura fisica del sistema; - una descrizione dell'architettura logica (funzionalità di ogni nodo di rete (suddivisione in reti differenti etc.); - procedure per gli aggiornamenti software e del firmware(di sicurezza e funzionali); - procedure per l'aggiornamento delle componenti HW; - funzionalità e procedure di monitoraggio della funzionalità del sistema di conservazione; - una descrizione delle funzionalità per la verifica dell'integrità degli archivi. La descrizione deve riportare l'algoritmo utilizzato e l'azione da intraprendere a fronte del rilevamento di una anomalia/errore nell'integrità dell'archivio stesso.	- Manuale di conservazione; - documenti di progetto: specifiche funzionali, progetto ad alto livello del sistema, descrizioni della topologia del sistema, lista di HW, SW e FW impiegato nel sistema,	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
44	1	Il processo di acquisizione è monitorabile per assicurare all'ente produttore ed al conservatore la possibilità di analizzare lo stato durante il processo.	L'ispettore deve verificare che siano definiti, realizzati ed applicati strumenti per verificare lo stato dell'acquisizione e archiviazione di uno specifico pacchetto di versamento. L'ispettore deve accedere a tali strumenti e verificare a campione la funzionalità a fronte di operazioni di versamento nel sistema di conservazione. L'ispettore può anche verificare il corretto funzionamento di tali strumenti in ambiente di test, avendo ricevuto sufficienti garanzie che l'ambiente è una istanziazione corretta e fedele dell'ambiente di test. L'ispettore a campione può scegliere di verificare il corretto funzionamento dello strumento di monitoraggio: - in caso di pacchetto di versamento ricevuto correttamente; - in caso di pacchetto di versamento con controllo di integrità fallito; - in caso di pacchetto di versamento con metadati incongruenti con quelli concordati con il produttore; - in caso di ulteriori "tipologie" di anomalie.		- funzionalità di monitoraggio della qualità del servizio di conservazione
45	1	E' presente adeguata documentazione a supporto delle attività operative ed amministrative inerenti il processo di acquisizione dei pacchetti di versamento (PDV).	L'ispettore può verificare tramite interviste a campione al personale coinvolto nel processo di versamento che il personale è al corrente delle procedure relative al processo di acquisizione dei pacchetti di versamento.	- procedure per l'acquisizione dei pacchetti di versamento - eventuali guide e manuali per l'acquisizione dei pacchetti	
	2		L'ispettore deve: - verificare se risultano disponibili i verbali o rapporti che descrivono l'esito dell'acquisizione del pacchetto di versamento; - esaminare i log degli strumenti di acquisizione (al fine di confermare che siano state eseguite le istruzioni come descritto nella documentazione); - procedere ad interviste al personale coinvolto nel processo di acquisizioni, verificando se è al corrente dell'esistenza della documentazione.	- eventuali verbali / rapporti del processo di acquisizione	- log di strumenti di acquisizione

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
47	**1**	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.	L'ispettore deve verificare che la presenza di procedure che riportano la descrizione di come il PDA sia generato a partire dal PDV, dettagliando eventuali trasformazioni sia ai contenuti sia ai metadati. L'ispettore deve verificare a campione alcuni contratti a conferma di eventuali accordi speciali sul pacchetto di archiviazione concordate con l'ente produttore e/o con il fruitore del servizio di conservazione.	Manuale di conservazione: procedure per la generazione del PDA a partire dal PDV. - allegati tecnici ai contratti per l'accesso ai servizi di conservazione	
48	**1**	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 dalle 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;	L'ispettore deve verificare che le procedure per l'accettazione e gestione di un PDV prevedano - la descrizione delle condizioni sotto le quali il PDV viene rifiutato; - la descrizione delle azioni conseguenti al rifiuto di un PDV o di non suo inserimento in un PDA (ad esempio comunicazione al produttore, predisposizione di un rapporto, modalità di eliminazione del PDV, etc.). Le procedure relative al rifiuto di un PDV devono prevedere la produzione della motivazione per il rifiuto (l'ente produttore deve essere messo in condizioni di correggere il PDV sulla base delle indicazioni ricevute dall'ente conservatore ed inviarlo nuovamente in conservazione). L'ispettore può esaminare i log del sistema per verificare che la gestione di un pacchetti di versamento rifiutato sia conforme a quanto dichiarato nelle relative procedure.	Manuale di conservazione: procedure per la generazione del PDA a partire dal PDV. - allegati tecnici ai contratti per l'accesso ai servizi di conservazione - eventuali verbali di rifiuto di un PDV	- log del sistema di conservazione: applicativo deputato all'accettazione del PDV nel sistema e alla trasformazione in PDA
	2		L'ispettore deve verificare a campione la documentazione prodotta per il rifiuto di un PDV e le azioni intraprese a seguito di tale evento (in tale attività di verifica è inclusa la verifica che sia disponibile l'evidenza, realisticamente generata da uno strumento automatico, di una comunicazione prodotta dall'ente conservatore per segnalare le motivazioni del rifiuto di una parte o di tutto il PDV).		

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
49	**1**	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 procedura descrive le modalità in caso di cambiamento intervenuto nel processo.	L'ispettore deve verificare se esiste traccia delle modifiche operate al sistema di generazione dei PDA. Qualora la modifica sia scaturita da un malfunzionamento del SW o da un aggiornamento di sicurezza, nel verbale della modifica del sistema di generazione dei PDA deve essere riportato anche l'incidente di sicurezza che ha scatenato l'applicazione della modifica.	- verbali di modifiche apportate al sistema di generazione dei PDA	- log del dello strumento di gestione della configurazione (CM, Configuration Management); -log dello strumento di gestione della documentazione

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
50	**1**	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 fine 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. Tale modalità è assicurata da tool e metodi per identificare tutti i tipi di oggetti conservati.	L'ispettore deve confermare che le verifiche e la gestione dei formati degli oggetti conservati sono eseguite tramite strumenti informatici.		- strumenti per la verifica e la gestione del formato degli oggetti in conservazione e relativi log.

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
51	1	Sono descritte le modalità di acquisizione dei metadati (PDI, Preservation Description Information) associati agli oggetti conservati.	L'ispettore deve verificare che la procedura di acquisizione degli oggetti descriva le modalità per acquisire i metadati associati agli oggetti conservati. La procedura deve descrivere le verifiche da eseguire sui metadati che devono contenere almeno i seguenti campi: - identificativo univoco nella forma di stringa alfanumerica di 20 caratteri (e.g. URI); - data di chiusura, in formato gg/mm/aaa (ossia da quando il documento informatico è immodificabile); - oggetto (nella forma di testo libero max 100 caratteri). Potrebbe essere una descrizione analitica, un indice, etc.; - soggetto produttore (nome 40 caratteri, cognome 40 caratteri, codice fiscale).; - destinatario: chi ha l'autorità e la competenza per ricevere il documento informatico. (nome 40 caratteri, cognome 40 caratteri, codice fiscale). L'ispettore deve verificare che la procedura sia effettivamente applicata accedendo, con il supporto del sistema di conservazione, ai log del sistema o ai metadati di uno specifico oggetto conservato.	- procedura di acquisizione dei metadati associati agli oggetti - allegati tecnici ai contratti	
	2		L'ispettore deve verificare che le modalità per acquisire i metadati associati agli oggetti conservati siano soggette a revisione a fronte di specifici eventi quali ad esempio modifiche di normativa o gestione di nuove tipologie di documenti.	- procedure e pianificazioni relative la revisione delle modalità di acquisizione dei metadati associati agli oggetti conservati; - verbali di aggiornamento e modifica delle modalità di acquisizione dei metadati associati agli oggetti conservati.	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
52	**1**	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).	L'ispettore deve verificare che risultino descritti i "criteri di mantenimento della leggibilità" finalizzati ad assicurare la fruibilità (da parte delle comunità destinatarie delle informazioni) e la comprensibilità delle informazioni conservate nel tempo (lungo termine). Devono essere definiti in modo chiaro i casi in cui vengono effettuati controlli di intellegibilità dei contenuti (ad esempio XML controllabili con xsd).	- descrizione dei criteri di mantenimento della leggibilità	
53	**1**	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).	L'ispettore deve verificare se sono definite procedure e strumenti (anche automatici): - per la conservazione nel tempo delle informazioni; - per la verifica dell'integrità dei PDA.	- procedure e documentazione di sistema per la conservazione nel tempo delle informazioni. - procedure e documentazioni di sistema che descrive le funzionalità di verifica di controllo di integrità dei PDA	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	Il sistema di conservazione assicura la possibilità di tracciare i PdA e le eventuali azioni svolte in maniera Manuale sugli stessi.	L'ispettore deve verificare che esistano procedure e strumenti per il monitoraggio e il tracciamento dei PDA: per tracciamento di un PDA si intende la registrazione di tutte le azioni svolte sul PDA ad esempio: - produzione di eventuali copie e duplicati; - eventuali modifiche e cancellazioni autorizzate operate su richiesta specifica del produttore o a seguito di altra richiesta valida. L'ispettore deve accedere allo strumento di tracciamento del PDA e verificarne il funzionamento attraverso: - verifiche dei log dello strumento; - simulazioni di intervento (ad esempio produzione di copie e/o duplicati; eventuali modifiche e cancellazioni) su PDA e relative evidenze prodotte dallo strumento.	- procedure di monitoraggio e tracciamento del PDA; - procedure di verifica del controllo di integrità	- strumenti per il monitoraggio dei PDA e per la verifica dell'integrità dei PDA nel sistema di conservazione - log degli strumenti per il monitoraggio e la gestione manuale dei PDA e per la verifica dell'integrità degli stessi
	3	Il sistema di conservazione ha uno specifico meccanismo per identificare eventuali corruzioni o perdite dei dati a seguito di specifiche azioni eseguite.	L'ispettore deve verificare che esistano procedure e/o strumenti automatici per l'analisi dei log finalizzati a verificare gli accessi ai PDA e le operazioni compiute su di essi dai vari soggetti del sistema di conservazione.	- procedure di verifica degli accessi ad uno specifico PDA	- strumenti per il monitoraggio dei PDA e per la verifica dell'integrità dei PDA nel sistema di conservazione - log degli strumenti per il monitoraggio e la gestione manuale dei PDA e per la verifica dell'integrità degli stessi

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
54	1	Sono presenti specifici log che permettono procedure di verifica da parte delle persone autorizzate o sulla base di report specifici.	(attività di verifica già descritta per il Requisito #15) L'ispettore deve verificare se la politica prevede la definizione di permessi di sola lettura al solo personale autorizzato per - i log degli accessi; - la documentazione relativa agli accessi. L'ispettore deve verificare tramite i file di configurazione che la politica di accesso SIA effettivamente implementata nel sistema (ad esempio ispezionando ai permessi per l'accesso ad uno specifico SW per la gestione dei log, Sistema operativo o file specifico).	- politiche di accesso alle informazioni ed al sistema e relative procedure	- sistemi di gestione dei log e log degli elementi del sistema di elaborazione; - configurazione dei permessi di accesso ai file di log - configurazione dei permessi del sistema
	2	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.	L'ispettore deve verificare se è presente la documentazione relativa alle azioni gestionali ed ai processi amministrativi rilevanti per la creazione del PdA, al fine di verificare che il PdA sia creato e mantenuto in accordo con le procedure documentate.	- registro dei rapporti di versamento - descrizione delle verifiche effettuate in fase di generazione dei PDA	
	3	Eventuali deviazioni dal normale processo possono essere identificate ed indagate.	L'ispettore deve verificare se le eventuali deviazioni dal normale processo sono identificate e possono essere indagate.	- registro dei rapporti di versamento - descrizione delle verifiche effettuate in fase di generazione dei PDA	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
55	1	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.	L'ispettore deve verificare se risultano descritte le strategie di conservazione relative agli oggetti conservati, con preciso riferimento ai rischi di obsolescenza tecnologica di supporti, formati e metadati e di perdita di integrità degli oggetti stessi.	descrizione delle 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 - processi di analisi dei requisiti, monitoraggio tecnologico (obsolescenza) e di mercato, evoluzione e progettazione del servizio	
	2		L'ispettore deve verificare se esistono relazioni e verbali che attestano l'attuazione della strategia di conservazione (ad esempio revisioni periodiche, analisi aggiornata e periodica dell'obsolescenza tecnologica dei supporti etc.).	verbali di revisioni periodiche e di analisi aggiornate e periodica dell'obsolescenza tecnologica dei supporti etc.	
56	1	Nel sistema di conservazione sono definiti ed attuati adeguati processi	L'ispettore deve verificare le procedure di monitoraggio previste dal Manuale di conservazione prevedono notifiche al personale di servizio.	Procedure di monitoraggio	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	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.	L'ispettore deve verificare a campione l'evidenza della produzione delle notifiche al personale di servizio relative alle funzioni di monitoraggio dell'ambiente di conservazione.	Evidenze delle procedure di monitoraggio	Evidenze delle procedure di monitoraggio
57	**1**	E' definito un processo in base al quale eventuali situazioni derivanti delle attività di monitoraggio potrebbero comportare modifiche ai piani di conservazione.	L'ispettore deve verificare se risulta definito un processo di monitoraggio finalizzato ad individuare che possono comportare modifiche ai piani di conservazione (ad esempio per mitigare o annullare gli effetti dell'obsolescenza).	- procedure di monitoraggio e aggiornamento del sistema	
	2		L'ispettore deve esaminare a campione i verbali del monitoraggio finalizzato ad individuare situazioni che possono comportare modifiche ai piani di conservazione.	- rapporti di monitoraggio	
58	**1**	E' definito ed attuato un processo di verifica del sistema di	L'ispettore deve confermare che esistono procedure finalizzate alla verifica del corretto funzionamento del sistema di conservazione nel suo insieme attraverso l'esecuzione di test sistema.	- procedure di verifica interna	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	conservazione per dare evidenza dell'efficacia delle attività svolte.	L'ispettore deve verificare che esistano evidenze delle verifiche interne eseguite ispezionando report a campione e confermando che le funzioni principali di un sistema di conservazione sono sollecitate in modo completo dai test eseguiti.		- strumenti automatici eventuali per l'esecuzione di self test; - procedure di monitoraggio dello stato dei processi informatici che realizzano il sistema di conservazione
59	**1**	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.	In questa sede si focalizza l'attività dell'ispettore sulla verifica che eventuali modifiche ai pacchetti di conservazione sono tracciate: L'ispettore deve verificare che eventuali modifiche ai pacchetti di conservazione siano registrate. Il log di tali azioni deve contenere le informazioni circa la modifica eseguita, il soggetto che ha eseguito la modifica, la data e l'ora in cui sono state eseguite le modifiche.	- specifiche tecniche della memorizzazione delle componenti del PDA nel sistema;	
	2		L'ispettore deve verificare se viene tenuta traccia delle eventuali modifiche delle politiche di conservazione dei pacchetti di archiviazione	- politiche di conservazione; - verbali di modifica delle politiche di conservazione	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
60	1	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.	L'ispettore deve verificare che sia mantenuta tutta la documentazione relativa alle azioni gestionali ed ai processi amministrativi rilevanti per la conservazione, in accordo con le relative procedure.	- procedure per la gestione della documentazione - evidenze della gestione della documentazione	- strumenti per la gestione della documentazione e relativi log
	2	Eventuali deviazioni sono identificate ed indagate.	L'ispettore deve verificare che eventuali deviazioni dalle procedure del sistema per quanto riguarda la documentazione relativa alle azioni gestionali ed ai processi amministrativi siano identificate ed indagate.	- eventuali verbali e rapporti dell'indagine eseguita	
61	1	Sono descritte le informazioni dei metadati identificativi utilizzati per la ricerca degli oggetti conservati e la loro associazione al PDA nel tempo.	L'ispettore deve verificare che - siano definite procedure interne ed eventuali procedure specifiche tramite accordi con il produttore o l'utente finale per l'indicizzazione e la ricerca dei PDA e delle informazioni in esso contenute tramite l'utilizzo di specifici metadati associati al PDA; - tali procedure siano applicate (tale verifica può avvenire ad esempio accedendo ad uno specifico PDA e verificando che la struttura dell'indice è conforme allo schema definito nella norma UNI 11386 e contiene i metadati utilizzati per eseguire le ricerche conformi a quanto descritto nelle procedure, oppure accedendo allo strumento di ricerca e verificando che la ricerca di una informazione a campione e del relativo PDA in conservazione va a buon fine, oppure ancora verificando i log dello strumento di ricerca e confermando che ad una ricerca specifica sono forniti i risultati corretti).	- procedure per la rappresentazione e conservazione dei metadati - procedure per l'indicizzazione e la ricerca dei PDA tramite specifici metadati - allegati tecnici ai contratti e procedure specifiche	- accesso agli strumenti automatici per la ricerca di specifiche informazioni conservate e dei relativi PDA tramite specifici metadati - log degli strumenti di cui sopra; - log degli strumenti di accesso in modifica ai metadati

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2		L'ispettore deve verificare che eventuali modifiche ai metadati dei PDA siano correttamente registrate.		- log degli strumenti di accesso in modifica ai metadati
62	**1**	Sono definite le politiche e le procedure per rendere disponibile l'informazione ("dissemination") assicurandone l'autenticità rispetto all'originale.	L'ispettore deve verificare che siano definite procedure per l'esibizione dell'informazione e del pacchetto di distribuzione PDD che la contiene. Tali procedure devono prevedere meccanismi di verifica dell'integrità rispetto all'originale fornito in conservazione. Ove previsto dal Manuale della sicurezza, l'ispettore deve verificare che esista una procedura per cui ogni pacchetto di distribuzione sia sottoscritto tramite firma digitale dal responsabile della conversazione.	- procedure per l'edizione dei PDD; - procedure per il recepimento e la gestione di eventuali errori segnalati - eventuali segnalazioni di errore e corrispettivi rapporti di gestione della segnalazione	- log degli strumenti per l'esibizione dei PDD; - sistema di accesso al sistema di conservazione
	2	Tali procedure prevedono anche la registrazione e la risposta agli eventuali errori rispetto ai documenti ed in risposta agli utenti.	L'ispettore deve verificare che le procedure per l'esibizione dell'informazione e del pacchetto di distribuzione PDD che la contiene prevedano - meccanismi di verifica della conformità dell'informazione contenuta nel PDD rispetto all'informazione originale, consegnata in conservazione; - meccanismi di recepimento degli errori e procedure per attivare una modifica (se necessaria) del PDA; - meccanismi per la registrazione di ogni evento di distribuzione; L'ispettore deve verificare l'applicazione delle procedure previste per l'esibizione dell'informazione e del pacchetto di distribuzione che la contiene accedendo, con il supporto del sistema di conservazione, ai log degli strumenti utilizzati per la predisposizione dei PDD ed eventualmente ai PDD stessi.	- procedure per l'edizione dei PDD; - procedure per il recepimento e la gestione di eventuali errori segnalati - eventuali segnalazioni di errore e corrispettivi rapporti di gestione della segnalazione	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
63	1	Esiste la separazione degli ambienti del sistema di conservazione (sviluppo, test, eventualmente qualità, produzione).	L'ispettore deve verificare che il sistema di conservazione preveda ambienti separati per lo sviluppo, l'ambiente di test e l'ambiente in produzione. Tale separazione dovrebbe essere fisica (locali separati non direttamente connessi tra loro) o logica (ad esempio ambiente di test e ambiente di sviluppo ospitati negli stessi locali ma separati proceduralmente e logicamente, ossia le reti sono separate da funzionalità di filtraggio e le procedure garantiscono la separazione tra ruoli autorizzati ad accedere ad uno specifico ambiente e controlli da eseguire sull'ambiente operativo in cui è ospitato il sistema sotto test o in sviluppo). In caso di separazione logica l'ispettore deve verificare le configurazioni degli strumenti utilizzati per attuare tale separazione.	- procedure per la separazione degli ambienti di test, sviluppo e produzione; - registri di accesso agli specifici ambienti	- sistemi di controllo di accesso all'ambiente di test e relativi log; - sistemi di controllo di accesso agli strumenti di sviluppo e relativi log; - configurazioni degli elementi utilizzati per la separazione logica degli ambienti di test, di sviluppo e di produzione
	2	I dati e le informazioni utilizzati negli ambienti diversi da quello di produzione (esercizio) sono rimossi quando non più necessari o resi anonimi.	L'ispettore deve verificare se, qualora siano utilizzate informazioni specifiche per l'esecuzione dei test, eventuali dati "sensibili" sono rimossi dalle informazioni utilizzate per i test o comunque resi anonimi.		

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	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.	L'ispettore deve verificare che le procedure prevedano una separazione chiara tra personale coinvolto nelle attività di sviluppo e personale coinvolto nelle attività di test. Tale separazione deve essere controllata a campione anche verificando il personale autorizzato ad accedere agli ambienti di sviluppo e all'ambiente di test. L'ispettore può intervistare a campione il personale autorizzato ad accedere agli ambienti di sviluppo, test e produzione e verificare se sono al corrente delle procedure in campo per la separazione.	- procedure per la separazione degli ambienti di test, sviluppo e produzione; - registri di accesso agli specifici ambienti	
64	**1**	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.	L'ispettore deve verificare se esiste un processo di monitoraggio e di valutazione dell'uso delle risorse (capacity management), che abbia come obiettivi l'analisi e la valutazione delle attuali prestazioni del sistema. Per la definizione del monitoraggio devono essere individuati specifici parametri chiave per la valutazione delle prestazioni del sistema. Esempi di parametri da considerare sono: contatori dei PDV ricevuti e dei PDA generati, contatori degli errori, contatori delle segnalazioni, contatori degli incidenti di sicurezza registrati (separati per incidente di sicurezza), contatori di eventuali modifiche, contatori dei PDD consegnati etc..	- eventuali studi di fattibilità per aggiornamenti del sistema - documentazione e procedure a supporto delle attività di monitoraggio	- strumento di monitoraggio delle prestazioni;
	2		L'ispettore deve verificare che il processo di monitoraggio e di valutazione dell'uso delle risorse (capacity management) sia utilizzato per le successive proiezioni di impegno e per la definizione delle future esigenze relative alle prestazioni 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 che prevengano l'obsolescenza tecnologica.	- eventuali studi di fattibilità per aggiornamenti del sistema - documentazione e procedure a supporto delle attività di monitoraggio	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3	Il monitoraggio e la valutazione considera tutte le diverse componenti del servizio, per assicurare una visione complessiva in ottica end to end.	L'ispettore deve verificare che il processo di monitoraggio e di valutazione dell'uso delle risorse (capacity management) coinvolga tutte le componenti del servizio di conservazione	- documentazione e procedure a supporto delle attività di monitoraggio	
	4	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.	Tale monitoraggio deve essere realizzato tramite strumenti automatici: l'ispettore dovrebbe verificare che tali strumenti automatici siano realizzati ed utilizzati (ad es. verificando i log degli accessi) e che i parametri dichiarati come di interesse per la valutazione delle prestazioni sono effettivamente rappresentati dallo strumento in modo comprensibile.	- documentazione e procedure a supporto delle attività di monitoraggio	- strumento di monitoraggio delle prestazioni;
	5		Gli strumenti automatici devono prevedere funzionalità di segnalazione di eventuali alert e messaggi di anomalia al pari di report e segnalazioni periodiche, il tutto finalizzato a stimolare l'analisi di eventuali modifiche al sistema di conservazione (o a costituire la base per analisi analoghe ma eseguite su base periodica). L'ispettore deve verificare i report prodotti dagli strumenti di monitoraggio al fine di confermarne l'effettiva applicazione.		- strumento di monitoraggio delle prestazioni;

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
65	**1**	Sono attivate specifiche contromisure contro la minaccia di virus, malware, ecc. con sistemi, processi organizzativi (ruoli, responsabilità) e procedure di controllo ed intervento.	L'ispettore deve verificare che il sistema preveda procedure per il rilevamento di virus e malware nel sistema di conservazione e nelle rappresentazioni digitali dei dati in esso conservati. Deve essere realizzata nel sistema una funzionalità di antivirus deputata alla scansione del software impiegato e dei file utilizzati nel sistema di conservazione (ivi inclusi i file dei PDV e PDD) e una funzionalità di prevenzione delle intrusioni deputata al rilevamento di malware specifici. Tale procedura deve prevedere scansioni periodiche e ad hoc sulla base di specifici eventi (ad esempio la ricezione di un PDV). In caso di rilevamento di un malware nel sistema, il sottosistema coinvolto (un elaboratore specifico o ad esempio la sottorete apparentemente compromessa) deve essere disconnesso dal sistema di conservazione e l'evento deve essere gestito come un incidente di sicurezza. Le procedure devono impedire che personale non autorizzato tenti di rimuovere il malware: ogni tentativo deve essere memorizzato in appositi log di sicurezza del sottosistema. Le procedure devono prevedere la decifratura di qualunque file proveniente da un soggetto esterno ricevuto in forma cifrata: a seguito della decifratura deve essere applicata la procedura di verifica del malware. Prima del ripristino di qualunque file da un supporto di backup, deve essere eseguita una scansione per rilevare la presenza di eventuali virus e malware. Accedendo alle funzionalità del sistema con il supporto dell'ente conservatore l'ispettore deve - verificare la configurazione del software (attivato e configurato per eseguire scansioni su eseguibili e file previsti dalle procedure); - verificare che le firme di virus e malware risultino aggiornate (compatibilmente con i piani di aggiornamento delle stesse); - esaminare i piani di test e i relativi rapporti eseguiti per verificare la funzionalità di verifica della presenza di virus e malware nel sistema di conservazione. Se possibile deve replicare un test nell'ambiente di test; - esaminare i log del sw di rilevamento di virus e malware e confermare che eventuali scansioni sono eseguite con cadenza periodica e in occasione degli eventi indicati nella procedura.	- pianificazioni di scansioni periodiche alla ricerca di virus e malware - report di scansioni periodiche alla ricerca di virus e malware	- strumenti per la scansione automatica e il rilevamento di virus e malware nel software impiegato nel sistema e relativi report

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
66	1	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.	L'ispettore deve verificare che esistano procedure di backup che facciano riferimento alle rispettive politiche attuate, e che tali procedure che descrivano: - i sistemi interessati (anche le applicazioni SW e la documentazione operativa come manuali, al fine di assicurare la continuità operativa); - la periodicità per l'esecuzione dei backup (verificando che tale periodicità risulti coerente con quanto definito nelle procedure di business continuity); - la pianificazione di prove periodiche per verificare il corretto funzionamento di procedure di ripristino; - i ruoli interessati nel processo e le relative responsabilità; - le modalità di conservazione dei backup (e i relativi check periodici di consistenza delle copie di backup); - come viene mantenuta l'interoperabilità dei backup.	- procedure di backup	
	2	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.	L'ispettore deve verificare, attraverso i verbali di presa visione, che tutti i soggetti coinvolti nel backup abbiano preso visione delle procedure e politiche di backup. L'ispettore può intervistare a campione il personale impegnato nell'esecuzione dei backup e nel ripristino eventuale di file da copie di backup, al fine di verificare che siano a conoscenza e attuino le procedure di backup. L'ispettore può valutare l'opportunità di chiedere evidenza di una copia di backup eseguita.	- procedure di backup	- accesso alle funzionalità di backup e relativi log
	3	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.	L'ispettore deve verificare, accedendo a campione al sistema di produzione e ripristino dei dati di backup, che sia tracciabile il numero, la posizione e la reperibilità delle copie di backup prodotte durante il processo di conservazione.	- documentazione di progetto del sistema di backup	- accesso al sistema di backup e relativi log

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	4	Sono presenti meccanismi che assicurano la sincronizzazione delle copie di un documento, al fine di mantenere unicità ed integrità del sistema di conservazione.	L'ispettore deve verificare che siano previste da procedura e siano attivi in campo strumenti per assicurare la sincronizzazione delle copie di un documento. L'ispettore può valutare l'opportunità di integrare le verifiche (con il supporto dell'ente di conservazione) tramite accesso a log di eventuali registrazioni di sincronizzazione di copie di un documento e tramite verifica diretta di documenti sincronizzati e verificare che risultino identici. Ove possibile l'ispettore può valutare l'opportunità di integrare le verifiche accedendo a documentazione di test della funzionalità di sincronizzazione.	- documentazione di progetto del sistema di backup	- accesso al sistema di backup e relativi log
	5	E' sempre tracciabile ed identificabile il numero, la locazione e la reperibilità delle copie eseguite nel processo di conservazione.	L'ispettore deve verificare che il processo di conservazione descriva le modalità attraverso cui è sempre possibile rintracciare in modo univoco ogni copia eseguita, almeno tramite identificativo (univoco) e posizione della copia. Tramite accesso ai log e alle evidenze del sistema, ovvero tramite accesso alle funzionalità del sistema, l'ispettore deve verificare che tali modalità siano effettivamente attuate.		- accesso alle funzioni del sistema e ai relativi log
	6	E' assicurato il mantenimento del tempo delle necessarie informazioni relative all'intero sistema di conservazione, tramite backup.	L'ispettore deve verificare se esistono procedure per garantire che tutte le necessarie informazioni relative all'intero sistema di conservazione, tramite backup, siano mantenute del tempo.		
67	**1**	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.	L'ispettore deve verificare che siano assegnate responsabilità per garantire che i sistemi di rete siano 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. L'ispettore deve verificare che siano presenti processi e strumenti e identificati ruoli per garantire che i sistemi di rete siano 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.	- procedure per la gestione dei sistemi di rete	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	E' attuata una separazione dei compiti tra chi si occupa di questi aspetti e coloro che hanno compiti operativi.	L'ispettore deve verificare che la procedura preveda una separazione nell'assegnazione dei ruoli incaricati di gestire i sistemi di rete e i ruoli operativi del sistema di conservazione.	- procedure per la gestione dei sistemi di rete	
	3	Sono presenti log e sistemi di monitoraggio per i sistemi di rete.	L'ispettore deve verificare che nel sistema i "sistemi di rete" (intesi come i nodi che realizzano l'infrastruttura e i servizi di rete, quali switch, router, firewall, server, etc.). - generino log circa le proprie attività; -siano soggetti a strumenti di monitoraggio dello stato e delle prestazioni (carico della CPU, carico di rete, etc.).		
	4	Sono presenti firewall per assicurare un adeguato livello di protezione e separazione del sistema di conservazione da internet e da altre reti.	L'ispettore deve verificare che l'architettura del sistema di conservazione preveda l'utilizzo per la realizzazione di funzionalità di filtraggio dei pacchetti scambiati sulla rete e protezione della rete del sistema di conservazione dalla rete internet (firewall). L'ispettore deve verificare che tali firewall siano effettivamente implementati nel sistema (ad esempio verificando accedendo ai log di tali funzionalità di filtraggio) e deve verificare che i firewall siano correttamente configurati (ad esempio accedendo al file di configurazione del firewall stesso).		
	5	Sono implementate adeguate contromisure da parte di fornitori dei servizi (security features, service levels, sistemi di intrusion detection system, ecc.).	L'ispettore deve confermare che l'ente conservatore abbia operato una verifica circa l'adeguatezza delle misure di protezione adottate dai fornitori; l'ispettore deve verificare inoltre che nei contratti siano definite le misure minime che deve realizzare il fornitore per contrastare specifiche minacce per l'ente conservatore).		

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	6	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 dei rischi. (controllo già coperto)	L'ispettore deve verificare che, in presenza di reti locali wireless, la connessione al punto di accesso utilizzi algoritmi crittografici. L'ispettore deve accedere agli strumenti deputati alla configurazione e realizzazione di tali reti locali e confermare che l'accesso sia effettivamente protetto tramite funzionalità di autenticazione e le informazioni in transito siano protette da algoritmi di cifratura robusti. La connessione wireless espone il sistema a diverse minacce, rendendo accessibile il sistema di accesso da un soggetto malintenzionato penetrato in un perimetro geografico non facilmente identificabile: è preferibile non utilizzare tali strumenti nel sistema di conservazione. Qualora l'utilizzo di funzionalità di accesso alla rete tramite mezzo wireless risulti indispensabile, è raccomandabile la separazione della sottorete wireless dalle sottoreti dove sono presenti i nodi principali del sistema di conservazione (archivi, funzionalità di accesso, etc.) attraverso la definizione di aree DMZ ed MZ.	- procedure per l'accesso tramite canale wireless al sistema di conservazione	- configurazione dei punti di accesso wireless
68	**1**	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.	L'ispettore deve verificare che le procedure per la selezione del personale incaricato (fornitori) per la trasmissione dei dati attraverso l'utilizzo di supporti fisici rimovibili prevedano requisiti definiti dal responsabile del servizio.	- procedure per la selezione del personale incaricato per il trasferimento di supporti fisici rimovibili	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	I dati trasmessi con l'utilizzo di supporti fisici, sono protetti con sistemi crittografici.	L'ispettore deve verificare che, in caso di trasferimento di dati utilizzando un supporto rimovibile, tali dati risultino protetti tramite strumenti crittografici. La verifica può avvenire: - verificando le procedure per la predisposizione dei supporti fisici rimovibili e il caricamento dei dati su di essi; - accedendo ad un supporto rimovibile e verificando che i dati non siano leggibili; - accedendo al sistema nelle funzionalità di predisposizione dei supporti fisici rimovibili e verificando, anche tramite i log, che sia effettivamente utilizzata una funzionalità di cifratura che realizza un algoritmo standard.		supporti rimovibili; - funzionalità di predisposizione dei supporti rimovibili
	3	I supporti fisici non presentano riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti, della loro tipologia, ecc.	L'ispettore deve verificare - che le procedure per la predisposizione dei supporti fisici rimovibili prevedano che non sia apposto su di essi alcun riferimento all'ente produttore, ai dati in esso contenuti e alla loro tipologia, ad alcun metadato correlato ai dati in esso contenuti. - che tali procedure siano effettivamente applicate, accedendo ad esempio ad un supporto rimovibile predisposto per il trasferimento (ove possibile) o richiedendo la generazione di un supporto fisico rimovibile nel rispetto della procedura e/o tramite interviste al personale preposto alla predisposizione dei supporti fisici rimovibili. - che il personale coinvolto nelle procedure di predisposizione dei supporti fisici rimovibili sia al corrente delle relative procedure tramite interviste.	- procedure per la predisposizione dei supporti rimovibili	- accesso ai supporti rimovibili

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	4	L'ente conservatore, in accordo con l'ente produttore, deve aver definito ed applicato i meccanismi per rendere illeggibili 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	L'ispettore deve verificare che siano definite procedure per rendere illeggibili i supporti fisici una volta che siano stati utilizzati per trasportare informazioni del sistema di conservazione. Tali procedure possono prevedere: - wipe (cancellazione sicura) a più livelli del supporto rimovibile; - distruzione fisica del supporto rimovibile (tramite incenerimento o distruzione in pezzi multipli a partire dai quali non è possibile ricostruire il supporto originario).	- procedure per la cancellazione sicura dei supporti rimovibili utilizzati per il trasporto dei dati da sottoporre a conservazione - eventuali rapporti di cancellazione sicura o di distruzione di supporti rimovibili -	- log degli strumenti per la cancellazione sicura delle informazioni dai supporti rimovibili
	5	Tali modalità di gestione fanno parte delle procedure del sistema di conservazione e sono supportate da evidenze.	L'ispettore deve prendere visione di verbali e rapporti e verificare che siano state rispettate le procedure previste per la cancellazione sicura o distruzione dei supporti rimovibili in esame. Per i supporti rimovibili per i quali sia stata prevista la cancellazione sicura l'ispettore potrebbe prevedere attività di verifica dell'effettiva cancellazione (ad esempio semplice analisi dei supporti connessi a strumenti di verifica fino ad analisi approfondite eseguite con strumenti specifici).	- procedure per la cancellazione sicura dei supporti rimovibili utilizzati per il trasporto dei dati da sottoporre a conservazione - eventuali rapporti di cancellazione sicura o di distruzione di supporti rimovibili -	- log degli strumenti per la cancellazione sicura delle informazioni dai supporti rimovibili

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
69	1	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'ispettore deve verificare che, in caso di consegna e spedizione di documenti tramite posta elettronica, le procedure prevedano l'utilizzo unicamente di posta elettronica certificata. Le procedure devono inoltre prevedere la verifica che al termine della trasmissione non siano mantenute ulteriori copie dei documenti in conservazione (ad esempio da procedura devono essere cancellate le copie inviate). L'ispettore deve esaminare i rapporti di consegna tramite posta elettronica e confermare l'utilizzo di posta elettronica certificata valida	- procedure per il trasferimento delle informazioni tramite messaggi di posta elettronica certificati	- - strumenti per la predisposizione e l'invio della posta elettronica certificata; cartelle relative alla posta inviata in locale e in remoto.
	2	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.	L'ispettore deve verificare che non siano mantenute copie dei messaggi inviati (ad esempio accedendo, con il supporto dell'ente conservatore, agli account per l'invio della posta certificata nell'ambito del sistema di conservazione e navigando le cartelle per confermare che non siano tenute copie non autorizzate dei messaggi di posta relativi al sistema stesso).	- procedure per il trasferimento delle informazioni tramite messaggi di posta elettronica certificati	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
70	1	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.	Il sistema deve prevedere la generazione dei log per ogni evento rilevante per il sistema stesso. L'ispettore deve verificare che - è definita una lista di eventi da sottoporre ad audit; - la procedura preveda che i log abbiano avere caratteristiche di completezza, (data, sistema che ha scatenato l'evento e la relativa generazione dei log, descrizione dell'evento) , inalterabilità e possibilità della verifica della loro integrità (cod. privacy), che i log siano conservati per un periodo non inferiore a sei mesi (cod. privacy), che i log siano accessibili solo da personale autorizzato - i log devono essere soggetti a backup con cadenza almeno quotidiana -L'ispettore deve verificare a campione che i log siano generati e che contengano le informazioni previste dalla procedura e da eventuali ulteriori accordi con il produttore dell'informazione accedendo ai log dei sottosistemi e , ove presente (ed auspicabile) ad un sistema centralizzato per la gestione dei log,	- documentazione di progetto - procedure per la generazione dei log - eventuali allegati tecnici ai contratti	- log degli applicativi utilizzati dall'intero sistema di conservazione
	2	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.	L'ispettore deve verificare che le procedure prevedano che i log siano conservati per un periodo di tempo sufficiente a - condurre analisi nelle modalità indicate dalle procedure del sistema di conservazione; - soddisfare i requisiti espressi in eventuali vincoli normativi (e.g. codice in materia di protezione dei dati personali), legali e contrattuali. L'ispettore accedendo ai log degli applicativi o tramite il sistema di gestione centralizzato dei log, deve verificare che siano mantenuti log per un periodo temporale congruente con quanto definito nelle relative procedure.	- documentazione di progetto; - procedure per la generazione dei log - eventuali allegati tecnici ai contratti	- log degli applicativi utilizzati dall'intero sistema di conservazione

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	3		(attività di verifica già descritta per il Requisito #15) L'ispettore deve verificare se la politica prevede la definizione di permessi di sola lettura al solo personale autorizzato per - i log degli accessi ; - la documentazione relativa agli accessi. L'ispettore deve verificare tramite i file di configurazione che la politica di accesso sia effettivamente implementata nel sistema (ad esempio ispezionando ai permessi per l'accesso ad uno specifico SW per la gestione dei log, Sistema operativo o file specifico).	- politiche di accesso alle informazioni ed al sistema e relative procedure	- sistemi di gestione dei log e log degli elementi del sistema di elaborazione; - configurazione dei permessi di accesso ai file di log - configurazione dei permessi del sistema
71	**1**	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.	L'ispettore deve verificare che sia prevista la generazione di riferimenti temporali affidabili. Devono essere previste procedure di aggiornamento automatico della data di sistema di tutti i componenti del sistema di elaborazione. L'ispettore deve verificare che il sistema sia dotato di funzionalità di generazione di riferimenti temporali affidabili, che ogni componente del sistema sia dotato di meccanismi per l'allineamento automatico della data e ora, che tale meccanismo è configurato correttamente (ad esempio accedendo alle funzionalità del sistema operativo relative all'applicazione di protocolli NTP) e che i log riportino correttamente tale data ed ora. Le procedure e le configurazioni devono riguardare anche componenti del sistema dislocate in posizioni fisiche differenti: l'allineamento temporale deve essere mantenuto anche tra componenti del sistema posizionate in fusi orari differenti. Ove possibile, l'ispettore deve anche accedere all'ora di sistema di componenti differenti dell'sistema di conservazione e verificarne per quanto possibile l'allineamento effettivo. Ove possibile l'ispettore, sempre con il supporto dell'ente certificatore, può eseguire un tentativo di disallineamento temporale (ad esempio su macchine di test che replicano l'ambiente in esercizio) e verificare che la funzionalità di allineamento temporale ripristina il corretto riferimento temporale	- documentazione di progetto - procedure automatiche per l'allineamento temporale degli orologi dei diversi elementi del sistema	- accesso alle funzionalità di allineamento di data ed ora del sistema di conservazione

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	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).	Eventuali modifiche ai riferimenti temporali di sistema devono essere registrate: l'ispettore deve verificare se esiste evidenza nel sistema di tale evento.	- documentazione di progetto - procedure automatiche per l'allineamento temporale degli orologi dei diversi elementi del sistema - eventuali verbali di modifiche ai riferimenti temporali	- accesso alle funzionalità di allineamento di data ed ora del sistema di conservazione ed ai relativi log
72	**1**	Le diverse componenti critiche e significative ("sensitive") del sistema di conservazione sono isolate da altri ambienti, organizzativamente, fisicamente e logicamente.	L'ispettore deve verificare se le diverse componenti critiche e significative ("sensitive") del sistema di conservazione sono isolate da altri ambienti, organizzativamente, fisicamente e logicamente.	- Manuale di conservazione	
73	**1**	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.	L'ispettore deve verificare che le specifiche tecniche, in caso di prodotti acquistati o sviluppati internamente, prevedano anche i requisiti tecnici per i controlli di sicurezza ed in particolare quelli automatici che dovrebbero essere inclusi nel sistema.	- specifiche tecniche dei componenti acquisitati (COTS) per il sistema di conservazione	

ID	ID – PROG.	COMPONENTE DEL REQUISITO	ATTIVITA' DI VERIFICA	EVIDENZE DOCUMENTALI	ELEMENTI DA CONTROLLARE
	2	Tale controlli sono adeguatamente 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.	L'ispettore deve verificare che - i requisiti tecnici per i controlli di sicurezza siano in linea con quanto definito nel risk assessment (prendendo visione dell'analisi condotta); - siano comunque presenti specifici documenti di accettazione dei test (o una valutazione indipendente o una certificazione che copre gli aspetti relativi ai controlli di sicurezza per i prodotti acquistati o sviluppati internamente).	- specifiche tecniche dei componenti acquisitati (COTS) per il sistema di conservazione - risultati di test di accettazione	