Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

ISTRUZIONI PER LA CONSERVAZIONE DEI LOG DEI MESSAGGI E DEI MESSAGGI DI POSTA ELETTRONICA CERTIFICATA CON VIRUS

Versione 1.0 – 05 luglio 2016

Sommario

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

1. Introduzione e breve quadro normativo

In linea con il Decreto del Presidente della Repubblica 11 febbraio 2005 n. 68 recante le disposizioni per l'utilizzo della posta elettronica certificata ed il Decreto Ministeriale 2 novembre 2005 in materia di regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata, al fine di garantire quanto più possibile omogeneità di struttura e completezza delle informazioni necessarie per la gestione del processo di conservazione, l'Agenzia per l'Italia Digitale nell'esercizio delle sue funzioni rilascia la presente istruzione rivolte a:

- gestori di posta elettronica certificata (di seguito PEC) nel processo di conservazione dei log dei messaggi di PEC e dei messaggi contenenti virus;
- eventuali conservatori incaricati di conservare i log dei messaggi di PEC e i messaggi contenenti virus.

Il Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. (CAD), art.44, riporta i requisiti per la conservazione dei documenti informatici e stabilisce che il sistema di conservazione dei documenti informatici deve garantire:

- l'identificazione certa del soggetto che ha formato il documento (tipicamente il soggetto che ha la responsabilità del documento) e dell'amministrazione che ha prodotto il documento;
- l'integrità del documento;
- la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
- il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del Decreto Legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

Ferme restando le disposizioni recate nel Dlgs. 82/2005, i sistemi di conservazione devono rispettare i requisiti previsti dal DPCM 3 dicembre 2013 relativo alle regole tecniche in materia di sistema di conservazione. In conformità all'art. 5 del suddetto DPCM, il sistema di conservazione deve operare secondo modelli organizzativi esplicitamente definiti.

La conservazione può essere svolta all'interno della struttura organizzativa del soggetto produttore dei documenti informatici da conservare (in house) oppure affidandola in modo totale o parziale ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche (outsourcing) ai sensi dell'art. 5 comma 2, lettera a) e b) del suddetto DPCM.

Lo stesso DPCM, entrato in vigore nell'aprile del 2014, stabilisce un periodo di adeguamento di 36 mesi per i sistemi già esistenti (scadenza 11/04/2017).

Il DPCM stabilisce inoltre l'obbligo per tutti i soggetti che operano attività di conservazione di redigere il Manuale di Conservazione (art. 8); a tal proposito l'Agenzia per l'Italia Digitale ha rilasciato sul proprio sito istituzionale il documento "Schema manuale di conservazione v.2" per guidare nella corretta stesura del manuale i soggetti che intendano effettuare conservazione a norma.

Il quadro normativo di riferimento è completato dal DPCM 13 novembre 2014 recante le regole tecniche relative alla gestione dei documenti informatici, secondo cui nel caso di documento informatico formato ai sensi dell'art. 3 comma 1, lettere c) e d), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione, dall'applicazione di misure per la

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Il presente documento, oltre a fornire indicazioni sulle specifiche attività di conservazione, al fine di contestualizzare il processo di conservazione, descrive sinteticamente le fasi di generazione degli oggetti da conservare.

Torna al sommario

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

2. Log dei messaggi di PEC

2.1 Contenuto dei Log

In ottemperanza al DM del 2 novembre 2005 in materia di Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale della PEC, durante le fasi di trattamento del messaggio presso i punti di accesso, ricezione e consegna, il sistema di gestione dei messaggi PEC deve mantenere traccia delle operazioni svolte.

È compito dunque del gestore realizzare, in ogni nodo di rete del proprio sistema coinvolto nella ricezione, trasmissione e trattamento del messaggio PEC, la funzionalità di memorizzazione delle attività svolte durante le suddette fasi in un registro (log) riportante i dati significativi di ogni operazione. Il DM del 2 novembre 2005 richiede che nel log delle operazioni siano contenuti almeno i seguenti dati:

- il codice identificativo univoco assegnato al messaggio originale;
- la data e l'ora dell'evento;
- il mittente del messaggio originale;
- i destinatari del messaggio originale;
- l'oggetto del messaggio originale;
- il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
- il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);
- il gestore mittente.

Come indicato nel DM del 2 novembre 2005, gli effettivi dati registrati sui singoli log dipendono comunque dalla tipologia dell'operazione tracciata.

Sebbene non esplicitamente richiesto dalla normativa, è auspicabile che siano inviati in conservazione anche gli altri log complementari che prevedono informazioni differenti da quelle previste nella normativa (ad esempio log di sistema). Per tali log potrebbe non risultare applicabile la lista di dati richiesta dal Decreto e si rimanda per tanto alle best practices in materia di log predisposte dalla comunità scientifica.

Torna al sommario

2.2 Generazione dei log

Il log costituisce la registrazione sequenziale e cronologica di eventi generati a seguito di una operazione di una specifica entità (soggetto umano o processo automatico) con finalità di analisi, monitoraggio e verifica.

Per il gestore di PEC del mittente, il processo di generazione dei log inizia con la presa in carico del messaggio originale, mentre per il gestore di PEC del destinatario, il processo inizia con la ricezione del messaggio di PEC predisposto ed inviato dal gestore di PEC del mittente.

Al verificarsi dell'evento, il software che ha generato o rilevato l'evento stesso, provvede a collezionare la lista di dati significativi descritti in par. 2.1 e la riporta progressivamente in una area di memoria dedicata appositamente predisposta.

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

Torna al sommario

2.3 Attività di conservazione

In attuazione di quanto previsto dall'articolo 44, comma 1, del CAD, il sistema di conservazione deve assicurare la conservazione elettronica a norma di legge dei documenti tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

Ai sensi dell'art. 10, comma 1, lettera a) e b) del DM 2 novembre 2005, tutti gli eventi registrati nell'intervallo temporale stabilito dal gestore di PEC (non superiore alle ventiquattro ore), alla scadenza di tale intervallo temporale, devono essere inviati in conservazione. senza soluzione di continuità.
Il processo di generazione dei log inizia con la generazione del file di log a seguito della presa in carico del primo messaggio originale da parte del gestore di PEC del mittente ovvero a seguito della ricezione del primo messaggio di PEC da parte del gestore di PEC del destinatario, nell'intervallo temporale di riferimento. I messaggi successivi pervenuti nel medesimo intervallo temporale generano una registrazione all'interno del suddetto file di log. Al termine dell'intervallo temporale il gestore di PEC associa a tale file i metadati di riferimento e produce il pacchetto di versamento.

Metadati di riferimento
I metadati sono un insieme di dati (ergo informazioni) associati ad un documento informatico utili per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.

Nell'allegato 5 al DPCM 3 dicembre 2013, sono riportati i metadati minimi da associare ad ogni documento informatico ai quali, nel caso di specie, è opportuno aggiungerne degli ulteriori.
Di seguito si riportano i metadati da associare ai file di log comprensivi dei suddetti metadati minimi:

- identificativo univoco del file di log;
- data di chiusura del documento intesa come data della creazione dell'impronta del file di log;
- impronta del file di log;
- gestore dei messaggi di PEC che ha inviato il file in conservazione;
- oggetto, ossia la tipologia del log;
- formato del file di log;
- destinatario del file di log, rappresentato dal responsabile della sicurezza dei log dei messaggi (DM 2 novembre 2005) del gestore di PEC;
- data di inizio del periodo di riferimento per la registrazione dei log;
- data di fine del periodo di riferimento per la registrazione dei log.

Il gestore di PEC potrà individuare ulteriori metadati utili alla gestione del file di log.

Predisposizione del pacchetto di versamento (PdV)

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

Come indicato all'art.7 del DPCM del 13 novembre 2014, il trasferimento dei documenti informatici nel sistema di conservazione avviene generando un pacchetto di versamento nelle modalità e con il formato previsti dal manuale di conservazione e riportati nel manuale di conservazione: in ogni caso ai sensi dell'art.4 comma 2 del DPCM del 3 dicembre 2013 i gestori sono tenuti a memorizzare i messaggi di log utilizzando uno dei formati indicati nell'allegato 2 al suddetto DPCM o in alternativa un formato che soddisfa i requisiti definiti nello stesso allegato

Il gestore di PEC quindi predispone il pacchetto di versamento e lo invia in conservazione.

Attività del conservatore

L'esito dell'operazione di versamento deve essere puntualmente verificato dal conservatore e comunicato al gestore di PEC tramite il rapporto di versamento automaticamente generato dal sistema di conservazione. Il rapporto di versamento deve essere univocamente identificato e contenere un riferimento temporale ed una o più impronte calcolate sull'intero contenuto di ogni pacchetto di versamento a cui fa riferimento.

Il rapporto deve riportare l'accettazione o il rifiuto del pacchetto in questione. In caso di esito negativo il conservatore dovrà indicare quali anomalie si sono verificate. In caso di esito positivo il sistema di conservazione predispone un pacchetto di archiviazione (PdA) a partire dal PdV e procede con le attività di conservazione.

A differenza del PdV per cui non è definita una struttura di riferimento obbligatoria ma la stessa è concordata tra le parti e riportata nel manuale di conservazione, il PdA deve essere realizzato nel rispetto della struttura indicata nell'allegato 4 del DPCM del 3 dicembre 2013.

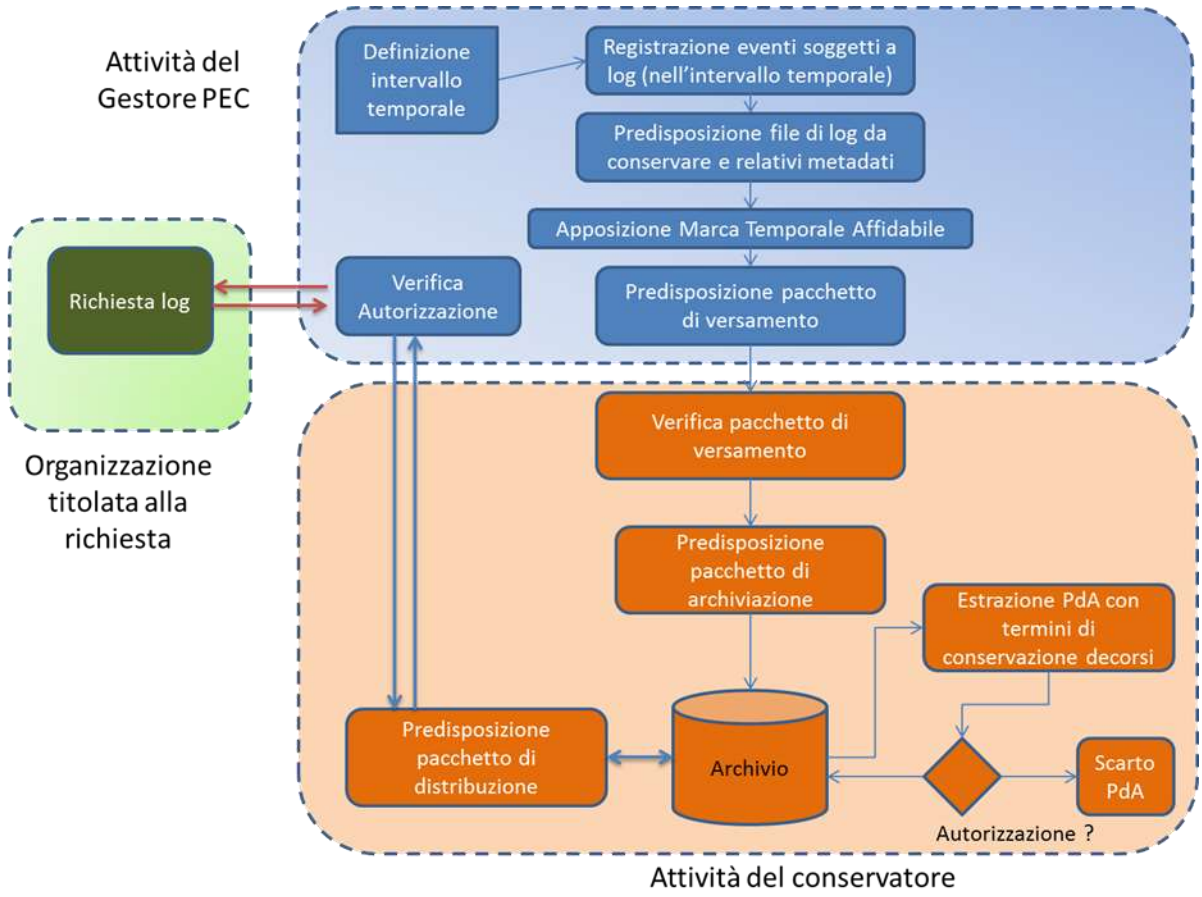
Il Responsabile della conservazione deve permettere ai soggetti autorizzati l'accesso ai log dei messaggi di PEC, attraverso la produzione di un Pacchetto di Distribuzione (PdD) nelle modalità previste nel manuale di conservazione.

I log dei messaggi inviati in conservazione devono essere conservati per almeno trenta mesi, ai sensi dell'art. 11, comma 2 del DPR 11 febbraio 2005; nel caso in cui decorrano i tempi previsti dalla normativa per lo scarto del PdA, previa autorizzazione del gestore, il sistema di conservazione rileva il PdA e dopo le opportune verifiche procede allo scarto definitivo.

Torna al sommario

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

2.4 schema flusso di lavoro conservazione log dei messaggi di PEC



Torna al sommario

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

3. Messaggi di PEC con virus

3.1 Contenuti del messaggio

In coerenza con quanto previsto dal DM 2 novembre 2005 il sistema di PEC riceve i messaggi (ricevute, avvisi e buste) in formato Multipourpouse Internet Mail Extension (MIME). I messaggi sono composti da una parte di testo descrittivo, e da una serie di allegati (messaggio originale, dati di certificazione, ecc.) variabili a seconda della tipologia del messaggio. Il messaggio, a cura del gestore di PEC è quindi inserito in una struttura S/MIME v3, firmata con la chiave privata del gestore medesimo.

Un messaggio con virus informatico (virus) ha le stesse caratteristiche di un messaggio di posta elettronica standard e trasporta, nel corpo o nell'allegato un software malevolo potenzialmente dannoso.

Torna al sommario

3.2 Individuazione dei virus

In conformità con quanto previsto dal DPR 11 febbraio 2005, n. 68, regolamento recante disposizioni per l'utilizzo della PEC, il gestore del mittente che riceva messaggi con virus informatici è tenuto a non accettarli, informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione.

Analogamente il gestore del destinatario che riceva messaggi con virus informatici è tenuto a non inoltrarli al destinatario, informando tempestivamente il gestore del mittente affinché comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione.

La rilevazione del virus avviene attraverso l'utilizzo di funzionalità di antivirus realizzate in software dedicati che intercettano il messaggio ed eseguono una verifica della presenza di virus nel messaggio riscontrandolo con le firme di virus presenti nel database delle firme del software antivirus.

Al termine di questa operazione il software antivirus restituisce il messaggio al sistema di gestione messaggi del gestore di PEC che procede accettando il messaggio o rifiutandolo e inviando una copia alla conservazione: nel caso in cui il virus venga rilevato dal gestore di PEC del mittente del messaggio originale, il gestore, produce una ricevuta di non accettazione per virus informatico, e procede con l'invio in conservazione del messaggio; nel caso in cui invece il virus venga rilevato dal gestore di PEC del destinatario del messaggio originale, questi produce una avviso di rilevazione di virus informatico e invia il messaggio di PEC in conservazione, senza inoltrarlo al destinatario.

Torna al sommario

3.3 Conservazione dei messaggi

Le attività di conservazione inerenti alla conservazione dei messaggi di PEC contenenti virus è resa obbligatoria ai sensi dell'art. 11 del DM 2 novembre 2005, secondo cui il gestore è tenuto a trattare il messaggio in conformità alle regole tecniche del suddetto Decreto Ministeriale.

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

Si evidenzia che il messaggio che trasporta un virus deve essere inviato in conservazione senza operare modifiche al messaggio originale.

Metadati di riferimento

Come già descritto in par. 2.3 relativamente ai metadati dei log dei messaggi, i metadati hanno lo scopo di descrivere il contesto, il contenuto e la struttura, nonché di permettere la gestione nel tempo dei messaggi di PEC con virus nel sistema di conservazione.

Come già introdotto in par. 2.3, nell'allegato 5 al DPCM 3 dicembre 2013, sono riportati i metadati minimi da associare ad ogni documento informatico ai quali, nel caso di specie, è opportuno aggiungerne degli ulteriori. Di seguito si riporta una lista di metadati da associare ai messaggi di PEC con virus, comprensivi dei metadati minimi consigliati per tutte le tipologie documentali

- identificativo univoco del messaggio di PEC con virus;
- data di chiusura del documento intesa come data della creazione dell'impronta del messaggio di PEC con virus;
- impronta del messaggio di PEC con virus;
- gestore dei messaggi di PEC che ha rilevato il messaggio con virus, che coincide con il gestore di PEC che ha inviato il messaggio in conservazione;
- oggetto, ossia identificativo della tipologia "messaggio con virus";
- formato del messaggio con virus;
- soggetto titolato a richiedere l'estrazione dei messaggi con virus;
- mittente del messaggio con virus;
- gestore di PEC del mittente del messaggio con virus;
- destinatario del messaggio con virus;
- gestore di PEC del destinatario del messaggio di con virus;
- data di ricezione del messaggio;
- prodotto antivirus che ha rilevato il virus nel messaggio, comprensivo della versione e della versione del database dei virus

Il gestore di PEC potrà individuare ulteriori metadati utili alla gestione del file di log.

Predisposizione del pacchetto di versamento

Come indicato all'art. 7 del DPCM del 13 novembre 2014, il trasferimento dei documenti informatici nel sistema di conservazione avviene generando un pacchetto di versamento nelle modalità e con il formato previsti dal manuale di conservazione: in ogni caso ai sensi dell'art. 4 comma 2 del DPCM del 3 dicembre 2013 i gestori sono tenuti a memorizzare messaggi con virus utilizzando uno dei formati indicati nell'allegato 2 al suddetto DPCM o in alternativa un formato che soddisfa i requisiti definiti nello stesso allegato.

La norma non riporta un vincolo temporale per l'invio in conservazione dei messaggi di posta elettronica con virus: per evitare la possibile e definitiva perdita del messaggio si suggerisce di predisporre ed inviare in conservazione il PdV quanto prima.

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

Attività del conservatore

Come già indicato in par. 2.3, il conservatore riscontra l'esito dell'operazione di versamento tramite la comunicazione del rapporto di versamento. In caso di esito positivo dell'operazione di versamento, il sistema di conservazione predispone un PdA (con struttura conforme a quanto stabilità nell'allegato 4 del DPCM del 3 dicembre 2013) e procede con le attività di conservazione.

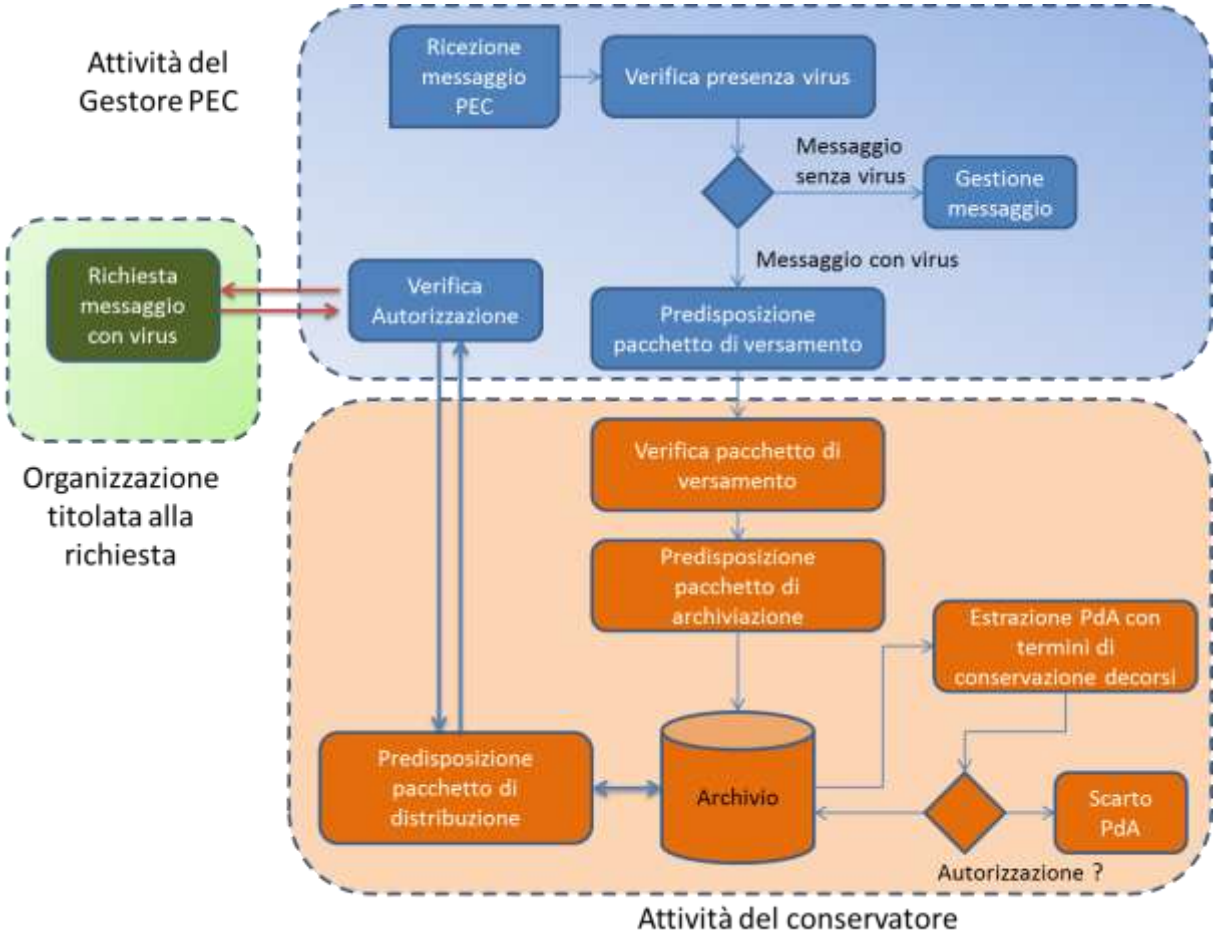
Il Responsabile della conservazione deve permettere ai soggetti autorizzati l'accesso ai messaggi con virus, attraverso la produzione di un PdD nelle modalità previste nel manuale di conservazione.

I messaggi di PEC contenenti virus inviati in conservazione devono essere conservati per almeno trenta mesi, ai sensi dell'art. 11, comma 3 del DM 2 novembre 2005; nel caso in cui decorrano i tempi previsti dalla normativa per lo scarto del PdA, previa autorizzazione del gestore, il sistema di conservazione rileva il PdA e dopo le opportune verifiche procede allo scarto definitivo.

Torna al sommario

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it

3.4 Schema flusso di lavoro conservazione messaggi di PEC contenenti virus



Torna al sommario

Agenzia per l'Italia Digitale
Viale Liszt, 21
00144 Roma, Italia
t +39 06 85264206
pec protocollo@pec.agid.gov.it direzione.generale@agid.gov.it