Piano di sicurezza dei documenti informatici

Documento n. 13

Premessa

I documenti informatici ricevuti o prodotti dall'Amministrazione sono soggetti a registrazione obbligatoria, ad eccezione di quelli soggetti a registrazione particolare il cui elenco è allegato al manuale di gestione - ai sensi dell'art. 53, comma 5 DPR 445/2000 - e di quelli esclusi dal predetto manuale.

Il presente piano di sicurezza fa riferimento all'applicativo per il protocollo informatico e per la gestione dei flussi documentali di PA Digitale SpA, erogato in modalità ASP. Per servizio ASP ("Application Service Providing" ossia "Fornitore di Servizi Applicativi") si intende la modalità con cui PA Digitale S.p.A fornisce i servizi applicativi inerenti alle funzionalità gestite dal proprio software da remoto (attraverso un Datacenter) in favore dei Clienti che vi accedono attraverso browser. Per Datacenter si intende il centro servizi che ospita e gestisce l'insieme delle risorse hardware, il software di base, l'applicativo necessario a consentire l'utilizzo dei prodotti, dei software e delle procedure informatiche di proprietà di PA Digitale S.p.A, nonché i dati del Cliente.

Il presente piano riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, che saranno conservati da PA Digitale S.p.A nei sistemi allocati presso il Datacenter Zucchetti S.p.A, situato in via Polenghi Lombardo, Lodi (LO). Il Datacenter Zucchetti è certificato in base agli standard internazionali ISO/IEC 27001:2013.

Il centro di ripristino, sede dove sono ubicati i sistemi atti a sostenere la ripresa dei servizi IT, è collocato presso Aruba S.p.A. Via Gobetti 96, Arezzo.

All'Ente fruitore del servizio in modalità ASP (Application Service Providing) è poi demandata la componente "locale" della sicurezza, relativa alle postazioni di lavoro degli utenti, della rete locale e delle componenti annesse.

L'organizzazione della componente locale, le sue misure e politiche di sicurezza, contribuisce a stabilire adeguati livelli di salvaguardia dei documenti trattati.

1 Obiettivi del piano di sicurezza

Il Piano di sicurezza garantisce che:

1. i documenti e le informazioni trattati dall'Amministrazione che usufruisce del protocollo siano disponibili, integri e riservati;
2. i dati personali, sensibili e/o giudiziari vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2 Generalità

L'Ente ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni. Le misure adottate per la sicurezza sono le seguenti:

1. protezione dei sistemi di accesso e conservazione delle informazioni;
2. assegnazione a ciascun utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione personale (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
3. cambio delle password con frequenza almeno semestrale durante la fase di esercizio (tale scadenza è parametrizzabile);
4. piano di continuità del servizio, con riferimento sia all'esecuzione e alla gestione delle copie di riserva dei dati e dei documenti (da effettuarsi con frequenza giornaliera), sia alla capacità di ripristino del sistema informativo entro 4 ore in caso di disastro;
5. conservazione delle copie di riserva dei dati e dei documenti affidata al fornitore del Datacenter;
6. impiego e manutenzione di adeguati sistemi di sicurezza (antivirus, firewall, packaging di patch e service pack correttivi dei sistemi operativi);
7. impiego di un sistema di abilitazioni alle funzionalità, che dia l'abilitazione alla trattazione delle registrazioni dei documenti e delle registrazioni a esse associate esclusivamente a chi ne sia responsabile, in termini di:
    - visibilità delle registrazioni e dei dati
    - gestione delle registrazioni
    - visibilità e gestione dei documenti elettronici allegati alle registrazioni
8. archiviazione giornaliera immodificabile delle estrazioni in PDF/A del registro di protocollo

Il piano in argomento è soggetto a revisione formale con cadenza almeno biennale.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati, solo in caso di necessità, dal Responsabile del protocollo designato dall'Ente (di cui all'art. 61 del DPR 445/2000) e dal titolare dei dati e, ove previsto, da tutti gli aventi diritto in base alla Legge.

3 Formazione dei documenti: aspetti attinenti alla sicurezza

Nell'ambito di gestione del sistema che governa il protocollo informatico e i flussi documentali, le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

1. l'identificabilità del soggetto che ha formato il documento per i documenti soggetti a protocollazione, l'AOO di riferimento;
2. quando prescritta, la sottoscrizione dei documenti informatici con firma digitale, ai sensi delle vigenti norme tecniche;
3. l'idoneità dei documenti a essere gestiti mediante strumenti informatici e a essere registrati mediante il protocollo informatico;
4. l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
5. la leggibilità dei documenti nel tempo;
6. l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che adottano i formati standard previsti dalla normativa vigente in materia di documenti informatici e che posseggano requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

I documenti informatici redatti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro eventuale sottoscrizione con firma digitale, nei formati standard (preferibilmente PDF e PDF/A), come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al DPCM 13 novembre 2014 (Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).

4 Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative destinate a erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente. Come citato in premessa, PA Digitale produce e dispone di prodotti software e applicazioni per le pubbliche amministrazioni idonei per essere utilizzati da collegamento remoto in modalità ASP e di un Centro di servizio denominato Datacenter collegato alla rete Internet e destinato a ospitare e gestire le risorse hardware e software necessarie a offrire ai propri Clienti i Servizi ASP.
Il sistema di gestione informatica dei documenti:

1. garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
2. assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
3. consente il reperimento delle informazioni riguardanti i documenti registrati;
4. consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di privacy, con particolare riferimento al trattamento dei dati sensibili e giudiziari;
5. garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Per la gestione dei documenti informatici all'interno dell'AOO, il responsabile del Servizio archivistico fa riferimento alle norme stabilite dal responsabile dei sistemi informativi dell'Ente.

4.1. Componente organizzativa della sicurezza

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo, gran parte delle funzioni/responsabilità di sicurezza sono demandate all'erogatore del servizio di protocollo. La componente organizzativa della sicurezza connessa con la gestione del protocollo e della documentazione è relativa principalmente alle attività svolte presso il Datacenter Zucchetti, nelle vesti di erogatore del servizio di protocollo in modalità ASP.
Nella gestione del Datacenter sono state individuate tutte le figure preposte all'adozione di tutte le procedure di sicurezza previste nell'ambito dell'organigramma gestito per la certificazione ISO/IEC 27001:2013.

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

1. *sicurezza informatica* - principalmente inerente alla definizione dei piani di sicurezza e della progettazione dei sistemi di sicurezza;
2. *sicurezza operativa* - realizza, gestisce e mantiene in efficienza le misure di sicurezza così da soddisfare le linee strategiche di indirizzo definite dalla funzione *sicurezza informatica;*
3. *revisione* - controlla le misure di sicurezza adottate, verificandone l'efficacia e la coerenza con le politiche di sicurezza.

Relativamente alla componente fisica della sicurezza sono stati definiti i ruoli previsti dalla certificazione ISO/IEC 27001:2013 per il Datacenter Zucchetti.

La componente organizzativa della sicurezza afferente l'AOO è articolata e gestita secondo quanto stabilito dalla struttura competente dalla politica di sicurezza messa in atto dall'Ente.

4.2. Componente fisica della sicurezza

Relativamente alla **sicurezza fisica**, il sistema si avvale del Datacenter Zucchetti, realizzato in un ex caveau bancario blindato, dotato di sistemi di protezione contro ogni minaccia, per garantire la massima sicurezza a dati e servizi. Il servizio di erogazione del Data Center è certificato ISO/IEC 27001:2013, e nello specifico:

1. per quanto riguarda la **rete elettrica e refrigerazione**: si avvale di un impianto di distribuzione elettrica ridondato; di gruppi di continuità statici (UPS); di un impianto di condizionamento dotato di 2 centrali frigorifere; di un sistema di controllo automatico;
2. per quanto riguarda la **prevenzione incendi**: si avvale di rilevamento fumi con sensori ottici analogici, doppie porte antincendio; spegnimento automatico incendi a gas inerte;
3. per quanto riguarda il **controllo accessi**: si avvale di sorveglianza armata; videocontrollo; sistema antintrusione; controllo accessi con lettore card e finger print.

4.3. Componente logica della sicurezza

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del sistema di protocollo, è stata realizzata attraverso:

1. l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto dannoso delle minacce sulle vulnerabilità del sistema informatico:
    - identificazione, autenticazione ed autorizzazione degli utenti;

- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- non ripudio dell'origine (da parte del mittente);
- non ripudio della ricezione (da parte del destinatario);

2. la ridondanza dei sistemi di esercizio.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità del sistema di protocollo informatico, è stata implementata una soluzione centralizzata per la gestione degli utenti del protocollo medesimo. Tale soluzione consente l'identificazione, l'autenticazione e l'autorizzazione degli utenti con le seguenti caratteristiche:

1. unico *login* per la gestione dei diritti di accesso ai servizi applicativi;
2. unico sistema di *repository* delle credenziali di accesso degli utenti;
3. unico database delle anagrafiche contenente tutti i profili di utenza.

4.4 Componente infrastrutturale della sicurezza

Come già citato nel precedente paragrafo 4.2, nel Datacenter sono disponibili i seguenti impianti, atti a garantire la sicurezza fisica dei dati:

1. antincendio
2. rilevazione dell'allagamento
3. luci di emergenza
4. continuità elettrica
5. controllo degli accessi e dei varchi fisici
6. gruppo di continuità (UPS) dimensionato
7. gruppo elettrogeno centralizzato

Gli impianti e le considerazioni precedenti valgono anche per la componente infrastrutturale della sicurezza per l'Ente. In particolare:

1. antincendio;
2. luci di emergenza;
3. continuità elettrica;

4.5. Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite dalle informazioni di qualsiasi tipo (dati, transazioni, registrazioni, ecc.) presenti o transitate sul sistema di protocollo e che occorre mantenere dal punto di vista regolamentare, oppure necessarie in caso di dispute legali che abbiano come oggetto di contesa le operazioni effettuate sul sistema stesso o indispensabili per poter analizzare compiutamente lo svolgersi di eventuali incidenti di sicurezza.
Le registrazioni di sicurezza sono costituite da:

1. i log di sistema, generati dal sistema operativo
2. i log dei dispositivi di protezione periferica del sistema informatico (intrusion detection system IDS, sensori di rete e firewall)
3. le registrazioni del sistema

Le registrazioni di sicurezza sono soggette alle misure di sicurezza previste dalla certificazione ISO/IEC 27001:2013.

5 Trasmissione e interscambio dei documenti informatici

Gli addetti dell'AOO alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati e i documenti trasmessi all'interno della AOO o ad altre AOO, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'AOO, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

1. accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare l'integrità del messaggio e del suo contenuto;
2. tracciamento delle attività nel file di log della posta;
3. gestione automatica delle ricevute di ritorno

Lo scambio per via telematica di messaggi protocollati tra AOO diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

5.1 All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività e i processi amministrativi conseguenti (articolo 55, comma 4, DPR 445/2000).
Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.
Il mezzo di comunicazione telematica di base è la posta elettronica certificata con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.
La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal Codice dell'Amministrazione Digitale.

5.2 All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica (e quindi esterni al sistema di protocollo informatico) non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.
Gli uffici organizzativi di riferimento dell'AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica in attuazione di quanto previsto dalla Direttiva del Ministro per l'innovazione e le tecnologie del 18 novembre 2005 concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

6 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, personale *(userID)* e privata *(password)* e un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.
La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate a un utente del servizio di protocollo e gestione documentale. In sintesi:

1. *consultazione,* per visualizzare in modo selettivo le registrazioni di protocollo;
2. *inserimento,* per inserire gli estremi di protocollo e effettuare una registrazione di protocollo e associare i documenti;

La profilazione preventiva include anche abilitazioni non destinate a tutti gli utenti, quali:

1. *modifica,* per modificare i dati opzionali di una registrazione di protocollo;
2. *annullamento,* per annullare una registrazione di protocollo autorizzata dal Responsabile del Servizio archivistico.

Le regole per la composizione delle *password* e il blocco delle utenze valgono sia per gli amministratori dell'AOO che per gli utenti dell'AOO.
Le relative politiche di composizione, aggiornamento e, in generale di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.
Il sistema di protocollo fruito dall'AOO:

1. consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
2. assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una *Access Control List* (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso a esso (sistema di autorizzazione o profilazione utenza).
Considerato che il sistema di protocollo segue la logica dell'organizzazione, ciascun utente può accedere

solamente ai documenti che sono stati assegnati alla struttura di appartenenza .
Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO.
I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso.

6.1. Utenti interni alla AOO
I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal responsabile del Servizio archivistico dell'AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.
La gestione delle utenze rispetta i seguenti principi operativi:

1. gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati
2. la credenziale privata degli utenti e dell'amministratore AOO non transita in chiaro sulla rete, né al momento della prima generazione, né successivamente al momento del login.

6.2. Accesso al registro di protocollo per utenti interni alla AOO
L'autorizzazione all'accesso al registro di protocollo è regolata tramite i seguenti strumenti:

1. assegnazione del documento alla struttura di competenza;
2. definizione delle ACL del documento
3. ruoli degli utenti, gestiti dall'amministratore di ente (amministrazione),
4. protocollazione "particolare o riservata"

La visibilità completa sul registro di protocollo è consentita agli utenti abilitati alla funzionalità di gestione del registro di protocollo. Più in generale, gli utenti abilitati a vedere tutte le registrazioni di protocollo sono quegli utenti per i quali, tra le abilitazioni di struttura organizzativa, sia stata definita la possibilità di visibilità su documenti e fascicoli a prescindere dalla loro ACL.
L'utente assegnatario dei documenti protocollati è invece abilitato a una vista parziale sul registro di protocollo. Tale vista è definita da assegnazione e ACL del documento.
L'utente che gestisce lo smistamento dei documenti può inoltrare i documenti di cui esso e/o la struttura per conto della quale opera risultano assegnatari al destinatario finale di competenza.

6.3. Utenti esterni alla AOO - Altre AOO/Amministrazioni
L'accesso al sistema di gestione informatica dei documenti dell'Amministrazione da parte di altre AOO avviene nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui agli art. 72 e ss del DLgs 82/2005.

6.4. Utenti esterni alla AOO - Privati
Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

7. Conservazione dei documenti informatici
La conservazione dei documenti informatici avviene sulla base delle disposizioni riportate nel:

1. DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell'archivio corrente dell'Ente
2. DPCM 3 dicembre 2013 per i documenti inviati in conservazione

7.1 Conservazione del registro giornaliero di protocollo
Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.
Al riguardo di seguito si descrivono le modalità di produzione di invio in conservazione delle registrazioni di protocollo informatico; il dettaglio delle modalità di invio in conservazione sono riportate nel dettaglio all'interno del manuale di conservazione.
Il sistema di protocollo provvede all'esecuzione automatica della stampa su file in formato PDF/A del registro giornaliero di protocollo e del registro delle modifiche. Il sistema di protocollo ogni giorno crea automaticamente due file con estensione PDF/A, contenenti:

1. il riepilogo di tutte le registrazioni di protocollo eseguite nell'ambito della medesima giornata
2. le modifiche e gli eventuali annullamenti occorsi ai protocolli precedentemente acquisiti

Il registro delle modifiche viene creato solo se nella giornata sono stati effettuati annullamenti-modifiche.
I metadati da inviare in conservazione unitamente alla copia dei registri di cui sopra sono:

1. metadati di identificazione, contengono le informazioni relative all'Ente che sta inviando il documento al conservatore e quelle del protocollo che identificano univocamente il documento.

2. metadati di profilo generali, contengono le informazioni generali sul documento, come oggetto e data.
3. metadati di profilo specifici, contengono le informazioni specifiche del tipo di documento, come numero di protocolli effettuati nella giornata, numero iniziale e numero finale.

La produzione del registro giornaliero e del registro delle modifiche avviene dopo lo scattare della mezzanotte della giornata di riferimento.

All'avvio del processo di creazione del pacchetto di versamento vengono elaborati i dati presenti nel registro di protocollo al fine di:
1. ottenere i metadati di profilo specifici da inviare al sistema di conservazione
2. effettuare la registrazione del file PDF/A nel registro stabilito e memorizzare tra gli attributi estesi del documento quelli calcolati precedentemente
3. predisporre il documento all'invio in conservazione

Il trasferimento del pacchetto di versamento al sistema di conservazione è nativamente integrato con l'applicativo del protocollo informatico. Al riguardo è previsto un processo automatico che si occupi di creare il pacchetto di versamento, inviarlo al sistema di conservazione e registrare lo stato del versamento stesso. Il processo provvede a:
1. estrarre dal sistema di protocollo i documenti registro giornaliero e registro delle modifiche da inviare in conservazione.
2. predisporre il pacchetto di versamento estraendo le informazioni necessarie dal documento e dal sistema
3. inviare il pacchetto - con possibilità di invio manuale o automatica
4. indicare nel documento lo stato "conservato"

7.2 Registro di emergenza
In condizioni di emergenza si applicano le modalità di registrazione e di recupero dei dati descritte all'articolo 63 del DPR 445/2000, in materia di gestione del Registro di emergenza.

In generale sono previste tre cause di emergenza:
Emergenza dovuta a cause dipendenti dal Datacenter, pertanto:
a) PA Digitale avvisa l'Ente che, per cause dipendenti da una interruzione locale (si intende per locale l'interruzione che dipende dal Datacenter), non è possibile utilizzare nell'arco della giornata lavorativa la procedura informatica di protocollo;
b) PA Digitale avvisa l'Ente che, per cause dipendenti da una interruzione locale (si intende per locale l'interruzione che dipende dal Datacenter), non è possibile utilizzare la procedura informatica di protocollo per un periodo superiore alla giornata lavorativa;
c) terminata l'emergenza, PA Digitale comunica tempestivamente all'Ente il ripristino della procedura informatica di protocollo.

Emergenza dovuta da cause dipendenti dall'Ente, pertanto:
a) l'Ente avvisa PA Digitale che per cause dipendenti da una interruzione locale (si intende per locale l'interruzione che dipende dall'Ente per cause connesse al luogo in cui ha sede) non è possibile utilizzare nell'arco della giornata lavorativa la procedura informatica di protocollo;
b) l'Ente avvisa PA Digitale che per cause dipendenti da una interruzione locale (si intende per locale l'interruzione che dipende dall'Ente per cause connesse al luogo in cui ha sede) non è possibile utilizzare la procedura informatica di protocollo per un periodo superiore alla giornata lavorativa;
c) terminata l'emergenza, l'Ente comunica tempestivamente a PA Digitale il ripristino della procedura informatica di protocollo.

Emergenza dovuta da cause di forza maggiore o calamità:
a) PA Digitale / l'Ente avvisa che per cause di forza maggiore o calamità non è possibile utilizzare la procedura informatica di protocollo ed è / deve essere istituito il registro di emergenza;
b) terminata l'emergenza, PA Digitale / l'Ente comunica tempestivamente il ripristino della procedura informatica di protocollo.

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare la procedura informatica di protocollo per effettuare le registrazioni, le operazioni di registrazioni di protocollo devono essere effettuate sul registro di emergenza, come previsto dal Manuale di gestione documentale.

7.3 Conservazione delle registrazioni di sicurezza / Supporti rimovibili / Politica dei salvataggi

Tutti i dati relativi alle registrazioni di protocollo sono conservati sui server dedicati presso il Datacenter. Per la natura dell'applicativo di gestione del protocollo informatico, basato su tecnologia web, i dati non vengono in alcun momento salvati localmente sui pc degli operatori di protocollo. All'interno del Datacenter non è previsto l'uso di supporti rimovibili. La politica dei salvataggi segue quanto stabilito nell'allegato 12 - Piano di continuità operativa.