



Agenzia per la Formazione, l'Orientamento e il Lavoro di Monza e Brianza

Piano per la sicurezza dei documenti informatici

Rev 1 del 30/05/2019

SOMMARIO

2. **PREMESSA..... 3**

3. **IL PIANO DI SICUREZZA DOCUMENTALE..... 4**

 FORMAZIONE DEI DOCUMENTI: ASPETTI ATTINENTI ALLA SICUREZZA..... 4

 GESTIONE DEI DOCUMENTI INFORMATICI..... 5

 COMPONENTE ORGANIZZATIVA DELLA SICUREZZA..... 5

 SICUREZZA DI ACCESSO..... 6

 SICUREZZA DEL DATACENTER..... 6

 COMPONENTE LOGICA DELLA SICUREZZA..... 7

 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO E DI SICUREZZA..... 7

 TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI..... 7

 ALL'ESTERNO DI AFOL(INTEROPERABILITÀ DEI SISTEMI DI PROTOCOLLO INFORMATICO)..... 8

 ALL'INTERNO DI AFOL..... 8

 ACCESSO AI DOCUMENTI INFORMATICI..... 9

 UTENTI INTERNI..... 9

 ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI AD AFOL..... 10

 CONSERVAZIONE DEI DOCUMENTI INFORMATICI..... 10

Conservazione del registro di protocollo..... 10

 REGISTRO DI EMERGENZA..... 11

 CONSERVAZIONE DELLE REGISTRAZIONI DI SICUREZZA / SUPPORTI RIMOVIBILI / POLITICA DEI SALVATAGGI..... 12

1. PREMESSA

Il presente piano di sicurezza fa riferimento all'applicativo per la gestione documentale e il protocollo informatico e per la gestione dei flussi documentali del fornitore dell'applicativo (Dgroove), erogato in modalità ASP. Per servizio ASP ("Application Service Providing" ossia "Fornitore di Servizi Applicativi") si intende la modalità con cui Dgroove 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 sviluppate da Dgroove.

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 Dgroove nei sistemi allocati presso i Datacenter descritti nel manuale di conservazione documentale.

Ad Afol 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.

Il Piano di sicurezza garantisce che:

- i documenti e le informazioni trattati da Afol siano disponibili, integri e riservati;
- 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. IL PIANO DI SICUREZZA DOCUMENTALE

Afol MB 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. conservazione delle copie di riserva dei dati e dei documenti affidata al fornitore del Datacenter;
5. impiego e manutenzione di adeguati sistemi di sicurezza (antivirus, firewall, packaging di patch e service pack correttivi dei sistemi operativi);
6. 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:
 - a. visibilità delle registrazioni e dei dati
 - b. gestione delle registrazioni
 - c. visibilità e gestione dei documenti elettronici allegati alle registrazioni

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 e della gestione documentale designato da Afol (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.

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:

- l'identificabilità del soggetto che ha formato il documento per i documenti soggetti a protocollazione;
- quando prescritta, la sottoscrizione dei documenti informatici con firma digitale, ai sensi delle vigenti norme tecniche;

- l'idoneità dei documenti a essere gestiti mediante strumenti informatici e a essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti.

I documenti di Afol 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 da Afol 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, 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).

GESTIONE DEI DOCUMENTI INFORMATICI

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 di Afol, il responsabile del Servizio archivistico fa riferimento alle norme stabilite dal responsabile dei sistemi informativi di Afol.

COMPONENTE ORGANIZZATIVA DELLA SICUREZZA

Considerata la particolare modalità di fruizione del servizio di gestione della documentazione e 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 fornito in modalità ASP.

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;

SICUREZZA DI ACCESSO

L'autentica utente della soluzione di gestione documentale (Docsuite) utilizzata in Afol è di tipo Windows Integrated, quindi collegata al "dominio AD" Aziendale. Lo scambio di sicurezza avviene per mezzo di token (Kerberos, NTLM) di autentica e quindi le credenziali non viaggiano mai in chiaro tra il client e il server.

La gestione dei gruppi utente può essere integrata con il "dominio AD" oppure essere gestita in modo autonomo sul database DocSuite.

I contenitori della DocSuite definiscono la suddivisione dei documenti in «armadi logici» ciascuno con una propria sicurezza di base attribuita ai documenti contenuti.

I settori della DocSuite definiscono la struttura del funzioni-gramma aziendale.

Settori e Contenitori e gruppi sono poi posti in relazione con l'organigramma aziendale e collegati a diversi livelli di privilegi o policy di sicurezza.

SICUREZZA DEL DATACENTER

La soluzione è installata nel cloud Azure di Microsoft in una sottoscrizione CSP dedicata ad AFOL Monza Brianza gestita dalla funzione Assistenza di Dgroove. Le procedure di gestione dei sistemi informativi e dell'ambiente cloud da parte della funzione Assistenza di Dgroove, le procedure di progettazione ed evoluzione applicativa della BU GED di Dgroove, sono certificate UNI EN ISO 9001.

L'ambiente cloud di Microsoft Azure offre ampie certificazioni reperibili, sia per quanto riguarda la riservatezza dei dati e sia per ciò che concerne le politiche di disaster recovery e continuità operativa.

Azure soddisfa un'ampia gamma di standard di conformità internazionali e specifici del settore, come GDPR (General Data Protection Regulation), ISO 27001, HIPAA, FedRAMP, SOC 1 e SOC 2. Controlli rigorosi di terzi, come quelli eseguiti dal British Standards Institute, verificano la conformità di Azure con le rigide normative di sicurezza definite da questi standard.

Al seguente url o altri dedicati da Microsoft si possono trovare le certificazioni:

- <https://azure.microsoft.com/it-it/overview/trusted-cloud/>
- <https://azure.microsoft.com/it-it/support/trust-center/>

In particolare le certificazioni ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud e ISO 27001.

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:
 - a. identificazione, autenticazione ed autorizzazione degli utenti;
 - b. riservatezza dei dati;
 - c. integrità dei dati;
 - d. integrità del flusso dei messaggi;
 - e. non ripudio dell'origine (da parte del mittente);
 - f. 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.

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 (firewall)
3. le registrazioni del sistema

TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Gli addetti (collaboratori e dipendenti) 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 di Afol MB, 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 Afol, oltre alle funzioni di un server SMTP o IMAP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;

Lo scambio per via telematica di documenti protocollati da AFOL, in generale, esige specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, particolari e/o giudiziari come previsto dal Regolamento UE 2016/679 e dal D.Lgs. 196/2003 e sue modificazioni.

ALL'ESTERNO DI AFOL (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.

ALL'INTERNO DI AFOL

Per i messaggi scambiati all'interno di Afol 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 di Afol si scambiano documenti informatici attraverso l'utilizzo del sistema di gestione documentale, di un sistema di cartelle condivise e con diversi livelli di protezione e 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.

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:

- consultazione, per visualizzare in modo selettivo le registrazioni di protocollo e dei documenti;
- inserimento, per inserire gli estremi di protocollo e i documenti, effettuare una registrazione di protocollo e associare i documenti;

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

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

Le regole per la composizione delle password e il blocco delle utenze valgono sia per gli amministratori di sistema di Afol che per gli utenti.

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 da Afol:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- 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.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso.

UTENTI INTERNI

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal responsabile del sistema documentale e del servizio di gestione. 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:

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

ACCESSO AL REGISTRO DI PROTOCOLLO PER UTENTI INTERNI AD AFOL

L'autorizzazione all'accesso al registro di protocollo è regolata tramite i seguenti strumenti:

- assegnazione del documento alla struttura di competenza;
- definizione delle ACL del documento
- ruoli degli utenti, gestiti dall'amministratore di sistema (amministrazione),

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.

CONSERVAZIONE DEI DOCUMENTI INFORMATICI

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

- DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell'archivio corrente di Afol
- DPCM 3 dicembre 2013 per i documenti inviati in conservazione

CONSERVAZIONE DEL REGISTRO DI PROTOCOLLO

Per la conservazione del registro di protocollo, 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 un modulo specifico in formato PDF/A del registro giornaliero di protocollo e del registro delle modifiche. Il sistema di protocollo ogni giorno crea automaticamente due file, 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"

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:

- 1) Dgroove avvisa Afol 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;
- 2) Dgroove avvisa Afol 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;

- 3) terminata l'emergenza, Dgroove comunica tempestivamente ad Afol il ripristino della procedura informatica di protocollo.

Emergenza dovuta da cause dipendenti da Afol, pertanto:

- 1) Afol avvisa Dgroove che per cause dipendenti da una interruzione locale (si intende per locale l'interruzione che dipende da Afol per cause connesse al luogo in cui ha sede) non è possibile utilizzare nell'arco della giornata lavorativa la procedura informatica di protocollo;
- 2) Afol avvisa Dgroove 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;
- 3) terminata l'emergenza, Afol comunica tempestivamente a Dgroove il ripristino della procedura informatica di protocollo.

Emergenza dovuta da cause di forza maggiore o calamità:

- 1) Dgroove / Afol 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;
- 2) terminata l'emergenza, Dgroove / Afol 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.

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 nel Piano di continuità operativa.

**La presente copia e' conforme all'originale depositato
presso gli archivi dell'Azienda**

EA-31-58-CC-1D-A7-84-C9-19-27-78-3D-DC-53-ED-2A-FF-22-0E-37

CAdES 1 di 1 del 06/06/2019 13:41:43

Soggetto: BARBARA RIVA

S.N. Certificato: 3432 29

Validità certificato dal 31/01/2017 13:14:19 al 31/01/2020 02:00:00

Rilasciato da InfoCert Firma Qualificata 2, INFOCERT SPA, IT
