Croce Rossa Italiana

ALLEGATO 4

PIANO DI SICUREZZA INFORMATICA RELATIVO ALLA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Aggiornato al 03/12/2015

Nel presente allegato è riportato il piano per la sicurezza informatica di cui all'art. 4, comma 1, lettera c), del DPCM 3 dicembre 2013 – Regole tecniche per il protocollo.
Questo piano è sviluppato dal RSP d'intesa con il Responsabile dei sistemi informativi e con il responsabile del trattamento dei dati personali previste agli artt. 31/36 del decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali e del Disciplinare tecnico pubblicati nell'Allegato B dello stesso decreto.
Si fa riferimento, inoltre, all'art. 7 del citato DPCM con il quale sono definiti i requisiti minimi di sicurezza dei sistemi di protocollo informatico.
Nel piano di sicurezza, sottoposto a verifica ed aggiornamento con cadenza almeno biennale, sono state incluse le misure atte a garantire la corretta gestione e conservazione delle copie di sicurezza dell'archivio informatico.
Tale piano, inoltre, sarà integrato, con l'emanazione di ulteriori disposizioni di dettaglio, a cura del Responsabile dei Sistemi Informativi.
Il PdP di protocollo informatico e gestione documentale cui si riferisce il presente *Manuale*, pertanto, è predisposto per garantire un sistema di sicurezza per l'accesso e il trattamento dei dati personali e dei documenti articolato in vari livelli, al fine di conseguire le massime garanzie di protezione delle informazioni gestite: la visibilità di dati e documenti è consentita solo agli operatori che ne hanno prerogativa per motivi d'ufficio.
Tale sistema di sicurezza si articola infatti nei seguenti livelli:

1. accesso al sistema;
2. formazione dei documenti informatici
3. gestione dei documenti informatici
4. accessibilità ai documenti informatici
5. trasmissione e interscambio dei documenti informatici
6. conservazione dei documenti informatici

Di seguito sono illustrati in dettaglio i suddetti livelli di sicurezza.

1 - Misure di carattere generale: accesso al sistema

Il Sistema consente il controllo differenziato dell'accesso e il tracciamento di qualsiasi evento di modifica delle informazioni, individuandone l'autore.
Il Responsabile dei Sistemi informativi e/o il Responsabile del servizio per la tenuta del protocollo, ciascuno per la propria competenza, al fine di assicurare la sicurezza dell'impianto tecnologico dell'Amministrazione CRI, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, adottano le misure tecniche e organizzative di seguito specificate:

- autorizzazioni di accesso, rilasciate secondo le competenze dei singoli utenti e differenziate in base alle tipologie di operazioni stabilite da ogni Responsabile di UOR/AOO. Per abilitare un nuovo operatore il dirigente responsabile dell'UOR/AOO invia una richiesta scritta al Coordinatore della gestione documentale con la quale richiede l'abilitazione dell'operatore, mediante la compilazione del modulo appositamente predisposto (all. n. 5), specificando le funzioni alle quali l'utente deve essere abilitato.
- assegnazione ad ogni utente del sistema di un USER ID e PASSWORD , nominativi e incedibili; è cura di ogni utente – a qualunque profilo abilitato – non lasciare incustodita la postazione di lavoro connessa al sistema e/o non far utilizzare ad alcuno le proprie credenziali di accesso al sistema;
- cambio delle password con frequenza almeno trimestrale. Nello specifico il meccanismo è già in essere sulle PDL, attraverso policy active directory;

- protezione della rete dell'Amministrazione con sistemi FIREWALL. Nello specifico si tratta di un sistema firewall utm Fortinet serie 1000 in alta affidabilità ed di sistemi operativi con i criteri di protezione necessari in ambito SPC;
- backup dei dati e dei documenti con frequenza giornaliera. Nello specifico si effettua il backup (con frequenza oraria) sia dei dati che dello stato dell'infrastruttura virtuale garantendo un rapido ripristino anche dei sistemi;
- tenuta delle copie di sicurezza in locali diversi da quelli in cui è installato il sistema. Nello specifico le copie dei dati, attraverso un sistema di virtualizzazione, sono situate presso altre sedi CRI afferenti al Comitato Centrale a Roma;
- archiviazione giornaliera, in modo non modificabile, dei file di log contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e maintenance del sistema;
- facoltà per il singolo utente di effettuare specifiche funzioni/operazioni predeterminate;

Se le credenziali sono corrette, viene aperta una sessione tra il *client* dell'utente (un *browser standard*) ed il *server* applicativo comunicando a quest'ultimo solamente il codice di accesso. In questo modo le *password* non sono a conoscenza dell'applicativo. Quest'ultimo è in grado quindi di individuare in modo univoco l'utente. Infatti se da un lato un utente può avere più codici di accesso per entrare con ruoli e diritti diversi, una stessa *username* può essere attribuita ad un unico utente (è una chiave univoca nel *database* degli utenti).

Il sistema controlla inoltre che non venga utilizzato lo stesso codice di accesso (*username*) contemporaneamente da due postazioni di lavoro, impedendo un eventuale secondo accesso contemporaneo.
Pertanto la possibilità di accedere al sistema è consentita esclusivamente agli utenti abilitati, identificati da *password* personale e con facoltà operative preventivamente individuate.

1.1. Cambio password e blocco credenziali

Ogni utente può, in ogni momento, cambiare la propria password. Il sistema controlla che la password sia composta da almeno otto caratteri alfanumerici e che non contenga il nome o il cognome dell'utente. La data in cui la password viene cambiata è registrata dal sistema nel record relativo all'utente.
Il sistema, ad ogni richiesta di autenticazione, verifica la data dell'ultimo accesso e la data dell'ultimo cambio password. Nel caso in cui l'ultimo cambio password sia anteriore ai tre mesi, il sistema obbliga l'utente a cambiare la password. Nel caso in cui l'ultimo accesso al sistema sia anteriore ai sei mesi le credenziali vengono disattivate e possono essere ripristinate solo dal responsabile dell'applicativo.

2 - Formazione dei documenti informatici

2.1. Contenuti

In ogni documento informatico, al minimo, è riportata, in modo facilmente leggibile, l'indicazione del soggetto che lo forma e dell'Amministrazione (che coincide con l'AOO) di riferimento.
Al fine di tutelare la riservatezza dei dati i certificati e i documenti trasmessi ad altre amministrazioni contengono soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite.
Nel contempo se nei documenti sono presenti dati sensibili o giudiziari (vedi art. 4, comma 1, lettera d) ed e) del D. Lgs. 30 giugno 2003, n. 196) l'utente deve attivare la casella di spunta "dati sensibili/giudiziari" posta nella maschera di registrazione. Il sistema cifra sia gli elementi della registrazione di protocollo (mittente, oggetto, tipo di allegati, data, numero, etc.), sia i file allegati.

2.2. Formato del documento informatico

Ai fini del presente *Manuale* e ai sensi dell'art. 1 del D.Lgs. 82/2005, per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
In fase di registrazione dei dati di protocollo possono essere allegati documenti informatici in un qualunque formato (tipicamente prodotti da applicativi di office automation es. .DOC, .XLS, .RTF, .HTML, .XML oppure prodotti da un'acquisizione ottica es. .TIFF, .GIF, .JPEG). In ogni caso sono ammessi tutti quei formati previsti nell'allegato n. 2 del DPCM 3 dicembre 2013 sulle Regole tecniche per il protocollo informatico.
Inoltre, il sistema riporta un'impronta, a norma di legge, dell'insieme dei *file* informatici abbinati alla registrazione, sia che essi siano stati sottoscritti o meno con firma digitale.
In tal caso quindi il responsabile della registrazione constata con evidenza che non sono avvenute manipolazioni e sostituzioni di file – nemmeno da un amministratore di sistema – in quanto al richiamo della registrazione può essere effettuato il controllo dell'impronta del *file* con quello inserito all'interno del *record* della registrazione, funzione estremamente utile per i *file* non sottoscritti in modo digitale.
Il PdP è comunque predisposto alla protocollazione di documenti informatici sottoscritti con firma digitale secondo quanto previsto dalla relativa normativa.

2.3. Firma dei documenti e impronta informatica

I documenti possono essere sottoscritti con firma digitale secondo quanto previsto dalla normativa in vigore. I documenti possono essere sottoscritti sia prima della registrazione sul sistema di protocollo sia durante la fase di registrazione.
Nel secondo caso, attivabile da una casella di spunta, il sistema richiede, una volta che l'utente abbia identificato su disco locale i file da firmare, l'utilizzo di un dispositivo sicuro per la creazione della sottoscrizione (es. una smart card, un token usb, etc.).
Nel record della registrazione viene salvata l'impronta (una sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile) dei documenti informatici allegati. Questa operazione permette, in ogni momento, di evidenziare eventuali modifiche o sostituzioni dei documenti informatici allegati alle registrazioni.

3 -Gestione dei documenti informatici

Il sistema operativo dell'elaboratore, su cui è realizzato il sistema di protocollo informatico, assicura:

- l'univoca identificazione ed autenticazione degli utenti, garanzia fornita dalla gestione di credenziali assegnate esclusivamente ad ogni utilizzatore con medesimo sistema centralizzato AD;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso sono crittografate ed inalterabili.

Il sistema di protocollo informatico:

- 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.

3.1. Sulla sicurezza fisica dei documenti:

- L'accesso in lettura e scrittura alle directory di rete utilizzate come deposito dei documenti è effettuato dal processo server dell'applicativo di protocollo informatico, mai dalle stazioni di lavoro.

- Il sistema operativo che ospita la directory di rete utilizzata come deposito dei documenti è configurato in modo tale da consentire l'accesso esclusivamente al server del protocollo informatico. In questo modo qualsiasi altro utente (ad eccezione degli operatori addetti alla manutenzione del sistema e all'esecuzione delle copie di backup) non potrà mai accedere ai documenti al di fuori del sistema di gestione documentale.

In ambedue i casi, i meccanismi di registrazione ed accesso dai server dell'applicativo ARXivar verso i repository sono mediati da meccanismi ad elevato grado di complessità necessario per la sicurezza del dato e la disponibilità in ambiente prestazionale

Il Responsabile dei Sistemi informativi garantisce la puntuale esecuzione delle operazioni di backup dei dati e dei documenti registrati mettendo in atto le misure di seguito specificate:

- ogni operazione con transazioni verso la base dati ed il repository documentale (che sia di manutenzione o di backup) è sottoposta ad operazioni di monitoring e log;
- le copie di backup dei dati e dei documenti sono conservate in ambito virtuale di gestione della sicurezza del dato con diversi livelli di affidabilità e sicurezza.

4 - Accessibilità ai documenti informatici

4.1. Gestione della riservatezza

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, si può associare una Access Control List (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso ad esso. Per default il sistema segue la logica dell'organizzazione, nel senso che ciascun utente può accedere solamente ai documenti che sono stati assegnati alla sua struttura di appartenenza, o agli uffici ad esso subordinati.
Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'Amministrazione.
I documenti protetti da una Access Control List non vengono mai visualizzati agli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca full text.

4.2. Accesso da parte di utenti interni all'Amministrazione

Il livello di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti, distinto per abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni, è attribuito dal RSP.
Il controllo degli accessi è assicurato utilizzando le password e gli altri sistemi di riconoscimento ed autenticazione implementati dal Servizio Sistemi informativi.

4.3. Accesso da parte di pubbliche amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione CRI da parte di altre pubbliche amministrazioni avviene nel rispetto dei principi della cooperazione applicativa, secondo gli

standard e il modello architetturale del sistema pubblico di connettività della rete nazionale della Pubblica Amministrazione.
Il sistema presenta le funzioni minime di accesso di cui all'articolo 60, comma 2, del DPR 445/2000.
In sintesi si elencano le azioni minime indispensabili da mettere in atto preventivamente all'accesso.
L'accesso da parte di altre pubbliche amministrazioni al sistema di cui sopra avverrà, comunque, a seguito di un atto bilaterale stipulato tra la Croce Rossa Italiana e l'amministrazione che ne deve fruire, in cui vengono stabilite preventivamente le garanzie a tutela del trattamento dei dati personali e dell'utilizzo dei sistemi informativi.
In ogni caso, la Croce Rossa Italiana valuta l'eventuale introduzione di ulteriori strumenti volti a gestire i profili di autorizzazione, verificare accessi anomali, tracciare le operazioni di accesso, ovvero a individuare tassative modalità di accesso alle banche dati, dandone conto nell'atto bilaterale.

La Croce Rossa Italiana prima di stipulare ogni singolo atto bilaterale verifica:

a) la base normativa che legittima l'amministrazione fruitrice all'accesso;

b) la finalità istituzionale perseguita dall'Amministrazione fruitrice;

c) la modalità telematica di accesso più idonea rispetto alle finalità, alla natura e alla quantità dei dati, alle caratteristiche del fruitore, al volume e alla frequenza dei trasferimenti, al numero di soggetti abilitati all'accesso.

L'amministrazione disporrà poi, in ogni momento, di informazioni complete e strutturate sui fruitori autorizzati, verificando periodicamente il permanere della necessità.

La Croce Rossa Italiana, in quanto titolare del trattamento dei dati personali, deve dare attuazione a quanto previsto dagli artt. 29 e 30 del Codice della privacy, in materia di designazione degli incaricati del trattamento e eventuale designazione del responsabile del trattamento, garantendo che l'accesso sia consentito esclusivamente a tali soggetti.

4.4. Accesso da parte di utenti esterni

L'accesso per via telematica al sistema di protocollo informatico da parte di utenti esterni all'Amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente: firme elettroniche, firme digitali, CNS (Carta Nazionale dei Servizi), CIE (Carta d'Identità Elettronica), sistemi di autenticazione riconosciuti dall'amministrazione CRI. L'intero impianto sarà protetto in SSl con certificato di criptazione dei dati. Ad essi si applicheranno comunque le azioni indicate al punto 4.3.

5 - Trasmissione e interscambio dei documenti informatici

5.1. Sistema di posta elettronica

La trasmissione dei documenti informatici avviene attraverso un servizio di posta elettronica certificata.
Il server di posta certificata di cui si avvale l'amministrazione CRI, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso alle Certification Authority per la verifica dei Message Autentication Code (MAC) presenti sui messaggi ricevuti;
- tracciamento delle attività nel file di log della posta
- gestione automatica delle ricevute di ritorno.

5.2. Cifratura dei messaggi

Lo scambio di dati e documenti attraverso reti non sicure avviene attraverso l'utilizzo dei sistemi di autenticazione e cifratura basati su chiave pubblica, che consentono:

- al destinatario di verificare l'autenticità della provenienza e l'integrità del messaggio, con particolare riferimento alle parti non firmate (ad esempio la segnatura di protocollo);
- di garantire la riservatezza del messaggio per la protezione dei dati personali sensibili previsti dal D. Lgs. 196/2003 e successive modificazioni ed integrazioni.

Lo scambio di dati e documenti attraverso reti sicure, come il Sistema pubblico di connettività (SPC) o le reti interne, può avvenire anche senza adottare le misure di sicurezza di cui al precedente comma in quanto esse non sono ritenute necessarie.

6 - Conservazione dei documenti informatici

6.1. Supporti di memorizzazione

Per l'archiviazione ottica dei documenti si impiegano sistemi via network e diskbased. E' inoltre consentito l'utilizzo di qualsiasi altro supporto di memorizzazione digitale, comunque idoneo a garantire la conformità dei documenti agli originali.

6.2. Tenuta dell'archivio informatico

Il Responsabile del procedimento di conservazione digitale:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza dei supporti di memorizzazione, utilizzando gli strumenti tecnologici e le procedure descritte nelle precedenti sezioni
- definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza
- verifica periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.