Sistema Socio Sanitario
Regione Lombardia
ATS Montagna

ALLEGATO N. 5

Piano di sicurezza informatica relativo alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici

In questo allegato è riportato il piano per la sicurezza informatica di cui all'art. 4, comma 1, lettera c), del DPCM 31 ottobre 2000, questo piano è sviluppato dal Responsabile dei flussi documentali, d'intesa con il Direttore dei sistemi informativi. Esso è sottoposto a verifica ed aggiornamento con cadenza annuale e deve considerare almeno i seguenti aspetti: analisi dei rischi, politiche di sicurezza ed interventi operativi. Nel piano di sicurezza informatica sono state incluse le misure atte a garantire la corretta gestione e conservazione delle copie di sicurezza dell'archivio informatico.

I - Misure di carattere generale

Il Direttore dei Sistemi informativi, al fine di assicurare la sicurezza dell'impianto tecnologico dell'ATS, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, adotta le misure tecniche e organizzative di seguito specificate:

- assegnazione ad ogni utente del sistema di un USER ID e PASSWORD;
- cambio delle password con frequenza almeno trimestrale;
- protezione della rete dell'Amministrazione con sistemi FIREWALL;
- backup dei dati e dei documenti con frequenza giornaliera;
- tenuta delle copie di sicurezza in locali diversi da quelli in cui è installato il sistema;
- backup giornaliero 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.

II - Formazione dei documenti informatici

Formati

Per la ricezione, produzione e conservazione dei documenti informatici si adottano formati che al minimo possiedono i requisiti di: leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Nello specifico:

a) PDF - PDF/A

Sviluppato da	Adobe Systems http://www.adobe.com/
Estensione	.pdf
Tipo MIME	application/pdf
Formato aperto	Sì
Specifiche tecniche	Pubbliche
Standard	ISO 32000-1 (PDF) ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
Ultima versione	1.7
Collegamento utile	http://www.pdfa.org/doku.php

b) TIFF

Sviluppato da	Aldus Corporation in seguito acquistata da Adobe
Estensioni	.tif
Tipo MIME	image/tiff
Formato aperto	No
Specifiche tecniche	Pubbliche
Ultime versioni	TIFF 6.0 del 1992 TIFF Supplement 2 del 2002
Collegamenti utili	http://partners.adobe.com/public/developer/tiff/index.html

c) JPEG

Sviluppato da	Joint Photographic Experts Group
Estensioni	.jpg, .jpeg
Tipo MIME	image/jpeg
Formato aperto	Sì
Specifiche tecniche	Pubbliche
Standard	ISO/IEC 10918:1
Ultima versione	2009
Collegamenti utili	http://www.jpeg.org/ www.iso.org

d) OFFICE OPEN XML (OOXML)

Sviluppato da	Microsoft http://www.microsoft.com http://www.microsoft.it
Estensioni principali	.docx, .xlsx, .pptx
Tipo MIME	
Formato aperto	Sì
Derivato da	XML
Specifiche tecniche	pubblicate da Microsoft dal 2007
Standard	ISO/IEC DIS 29500:2008
Ultima versione	1.1
Possibile presenza codice maligno	Sì
Collegamenti utili	http://msdn.microsoft.com/en-us/library/aa338205.aspx http://standards.iso.org/ittf/PubliclyAvailableStandards www.iso.org

e) OPEN DOCUMENT FORMAT

Sviluppato da	OASIS http://www.oasis-open.org/ Oracle America (già Sun Microsystems) http://www.oracle.com/it/index.html
Estensioni	.ods, .odp, .odg, .odb
Tipo MIME	application/vnd.oasis.opendocument.text
Formato aperto	Sì
Derivato da	XML
Specifiche tecniche	pubblicate da OASIS dal 2005
Standard	ISO/IEC 26300:2006 UNI CEI ISO/IEC 26300
Ultima versione	1.0
Collegamenti utili	http://books.evc-cit.info/ http://www.oasis-open.org www.iso.org

f) XML

Sviluppato da	W3C
Estensioni	.xml
Tipo MIME	application/xml text/xml
Formato aperto	Sì
Specifiche tecniche	pubblicate da W3C http://www.w3.org/XML/
Collegamenti utili	http://www.w3.org/

g) TXT

Sottoscrizione

La sottoscrizione dei documenti informatici è eseguita con una firma elettronica/digitale, basata su un certificato rilasciato da un certificatore accreditato e generata con un dispositivo sicuro.

Per i documenti informatici che non necessitano di sottoscrizione, l'identificazione dei soggetti che li producono è assicurata dal sistema informatico di gestione dei documenti oppure dal sistema di posta elettronica certificata.

Datazione
Per attribuire una data certa al documento informatico ci si avvale del servizio di marcatura temporale (time stamping) fornito dal certificatore accreditato.

III- II Gestione dei documenti informatici

Sistema di gestione informatica del protocollo e dei documenti
Il sistema operativo dell'elaboratore, su cui è realizzato il sistema di gestione informatica del protocollo e dei documenti, è conforme alle specifiche previste dalla normativa vigente. Esso assicura:

a) l'univoca identificazione ed autenticazione degli utenti;

b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;

c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;

d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette da modifiche non autorizzate e il sistema assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

La conformità del sistema operativo alle specifiche di cui sopra sono attestate dal fornitore.

Per la generazione delle impronte dei documenti informatici il sistema utilizza la funzione di HASH 256.

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 Direttore del Servizio informatico garantisce la puntuale esecuzione delle operazioni di backup dei dati e dei documenti registrati, da parte di personale appositamente autorizzato.

Ogni operazione di manutenzione o di backup effettuata sul sistema che ospita la base documentale e sul sistema di protocollo informatico è registrata su un file di log periodicamente controllato.

Le copie di backup dei dati e dei documenti sono conservate a cura del Direttore dei servizi informativi in un luogo diverso dalla sede dell'amministrazione a cura di un soggetto terzo con il quale si è stabilita la convenzione per la conservazione.

Per il piano di Continuità operativa e per le previsioni di "Disaster Recovery" si rimanda alle indicazioni regionali inerenti SFT – studio di fattibilità tecnica di disaster recovery per le aziende santarie pubbliche della regione lombardia.

IV - Accessibilità ai documenti informatici

Gestione della riservatezza

A ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è associata 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; l'amministrazione adotta regole per l'accesso ai documenti sulla base della normativa vigente in materia di privacy. L'elenco dei dipendenti abilitati è estratto dal sistema informatico.

V - Trasmissione e interscambio dei documenti informatici

Sistema di posta elettronica

La trasmissione dei documenti informatici avviene attraverso un servizio di posta elettronica certificata conforme agli standard della rete nazionale delle pubbliche amministrazioni. L'ATS
si avvale di un servizio di "posta elettronica certificata" offerto da un soggetto in grado di assicurare la riservatezza e la sicurezza del canale di comunicazione; di dare certezza sulla data di spedizione e di consegna dei documenti e al rilascio di ricevute di ritorno elettroniche.
Il server di posta certificata di cui si avvale l'ATS, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

a) accesso alla Certification Authority per la verifica dei Message Autentication Code (MAC) presenti sui messaggi ricevuti;

b) tracciamento delle attività nel file di log della posta;
c) gestione automatica delle ricevute di ritorno.

Interoperabilità e cooperazione applicativa

Lo scambio di documenti informatici soggetti a registrazione di protocollo, in modalità interoperabilità e cooperazione applicativa, potrà avvenire mediante messaggi conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.

Cifratura dei messaggi

a) Lo scambio di dati e documenti attraverso reti non sicure avviene con l'utilizzo dei sistemi di autenticazione e cifratura.

b) Lo scambio di dati e documenti attraverso reti sicure, come la Rete nazionale delle pubbliche amministrazioni 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.

VI - Conservazione dei documenti informatici

Supporti di memorizzazione
Per l'archiviazione ottica dei documenti si utilizzano i supporti di memorizzazione digitale che consentono la registrazione mediante la tecnologia laser (WORM, CD-R, DVD-R).

Procedure di conservazione

Il riferimento temporale, inteso come l'informazione, contenente la data e l'ora in cui viene ultimato il processo di conservazione digitale, associata ad uno o più documenti digitali, è generato secondo i canoni di sicurezza.

Tenuta dell'archivio informatico
Il Responsabile del procedimento di conservazione digitale (Conservatore) sulla base di quanto specificato nel manuale di gestione e nel piano di conservazione:

a) adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza;

b) definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;

c) 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.

VIII – Specifiche tecniche di scansione dei documenti cartacei

I documenti cartacei acquisiti tramite scansione saranno di tipo PDF/A con risoluzione 200DPI di base e modalità bianco/nero