La tecnologia "Change Management" ed i costi di Information Technology in un'organizzazione sanitaria

Franco G., Donner D., Chierichetti F., Guarrera G.*

Azienda Provinciale per i Servizi Sanitari - APSS Trento
apss@pec.apss.tn.it

Sommario

Questo studio vuole essere la fotografia di un caso reale da cui trarre utili considerazioni operative, sia per ridurre i costi di Information Technology, che per abbattere il rischio tecnologico dovuto a frequenti aggiornamenti del software: parte più costosa del sistema informativo sanitario. L'elaborato illustra come introdurre in Azienda sanitaria dei processi organizzativi standardizzati atti a governare le frequenti attività di modifica del software in uso ed offrire maggior beneficio a tutti i livelli gestionali, diminuendo il rischio clinico/operativo ed ottimizzando i processi di governance. Partendo da un'analisi dello scenario esistente, si propone al manager una soluzione dal rapporto costo/efficacia conveniente - ovvero il processo di IT Change Management - al fine di governare in sicurezza il sistema informativo sanitario e proteggere il raggiungimento degli obiettivi aziendali.

I. Introduzione

Se paragonassimo l'Azienda sanitaria ad un corpo umano, il software ne rappresenterebbe il sistema nervoso centrale. Piccoli cambiamenti su tale componente avrebbero enorme impatto sugli organi dell'intero sistema causando rallentamenti, blocchi delle funzionalità, mancanza di coordinamento e potenziali danni irreversibili. Una progettazione ed una gestione errata del software potrebbero produrre problematiche di varia entità che, sia valutate singolarmente che in maniera olistica, andrebbero a costituire una seria minaccia al funzionamento generale del sistema [1]. Di conseguenza risulta fondamentale proteggere questo asset core adottando specifiche attenzioni, evitando così incidenti e possibili situazioni di crisi.
Negli ultimi anni la centralizzazione dei servizi e dei sistemi informatici della Pubblica Amministrazione ha comportato da un lato una diminuzione generale degli incidenti, dall'altro un aumento della criticità dei sistemi stessi e della superficie di impatto intesa come entità degli eventuali danni [2]. Il potenziamento e la ridondanza delle infrastrutture elettriche, con l'evoluzione e l'aumento di velocità e resilienza delle reti di comunicazione, ha eliminato sensibilmente gli incidenti relativi a blackout elettrico ed indisponibilità del collegamento di rete. Di conseguenza il focus delle problematiche si è spostato ad un livello più alto: il software [3].
Il software è una componente molto costosa che frequentemente va aggiornata (vide infra), risulta sempre più complessa, interdipendente ed indispensabile. Necessita di protezione e monitoraggio in quanto presente in tutti i livelli e processi aziendali e in quanto parte più onerosa dei servizi informatici. Grazie ad esso le strutture interne ed esterne delle Aziende sanitarie hanno raggiunto un livello di controllo ed automazione mai visto prima. Le

*I dati preliminari di questo studio sono stati presentati all'8°Congresso SIHTA "HTA tra decisione e consenso " svolto a Roma presso il Centro Congressi Palazzo Rospigliosi in data 3 Ottobre 2015, in forma di presentazione orale, nella sessione "Percorsi, processi e modelli organizzativi".

nuove tecnologie di diagnostica strumentale, la condivisione delle informazioni sanitarie tra professionisti di strutture diverse, la dematerializzazione dei certificati di malattia e delle prescrizioni farmacologiche, la telemedicina, nonché i sofisticati sistemi automatici di monitoraggio ed allarme continuano ad apportare notevole beneficio all'utenza Aziendale [4].
Può sembrare strano, ma l'utilizzo del software presenta delle problematiche intrinseche ed in prima battuta di difficile risoluzione. Semplici aggiornamenti, ad esempio, possono creare blocchi parziali o totali di funzionamento ed anche perdite di dati. E' per questo motivo che un processo coordinato di supervisione e gestione dei cambiamenti software risulta indispensabile. Sebbene già da tempo sia stata posta attenzione ad alcuni aspetti di sicurezza, quali la tutela della privacy ed il rischio clinico, in quanto previsti dalla legge e quindi obbligatori, manca una corretta gestione del cambiamento del software: non esistono infatti nelle Aziende sanitarie dei processi e delle figure ad hoc [5]. Un miglioramento in tal senso renderebbe l'Azienda più in grado di interpretare il contesto di cambiamento tecnologico, ottimizzando i costi gestionali e disponendo più correttamente le risorse. In tal modo, gli incidenti sugli asset core dovrebbero mostrare una significativa diminuzione. Non agendo su questo asset i potenziali danni, sia relativamente al settore umano (pazienti, operatori) che tecnologico (dati d'archivio), possono risultare non più circoscrivibili ad un livello accettabile.
L'esternalizzazione della gestione hardware e software spesso comporta una gestione incompleta del risk assessment periodico, un'adozione di procedure di comunicazione insufficienti ed un carente monitoraggio e controllo preventivo e detettivo [6]. Una banale minaccia informatica potrebbe sfruttare queste vulnerabilità e generare anche un security incident. Dal momento che le informazioni trattate dai sistemi informativi sanitari possono essere catalogate come 'supersensibili', in quanto riferite direttamente alla salute della persona, risulta ancor più necessario adottare e mantenere alti livelli di sicurezza e qualità nella gestione dei dati e dei processi, istituendo specifiche misure di protezione che tengano conto delle tecnologie, delle interdipendenze tra servizi e delle finalità [7]. La perdita di qualità dei dati ha un'inevitabile ricaduta trasversale nell'organizzazione, creando un effetto domino di forte impatto negativo dal punto di vista dell'erogazione dei processi e della salute dei pazienti [8]. Tale propagazione di errore andrebbe evitata adottando contromisure organizzative aziendali, coinvolgendo maggiormente il reparto IT, obbligando le terze parti a misure di controllo ed audit tramite strumenti giuridico/contrattuali ed implementando processi organizzativi e framework tecnologici orientati alla sicurezza.
La gestione del cambiamento del software andrebbe monitorata centralmente e configurata come attività on-going e non one-time, dedicando personale qualificato a definire obiettivi di sicurezza, politiche del cambiamento tecnologico, standard e linee guida aziendali. Il referente tecnologico delle Unità Operative dovrebbe acquisire le competenze del Change Manager per interfacciarsi con il Risk Manager e l'Information Security Manager. La politica aziendale dovrebbe inoltre essere orientata verso la gestione del post-cambiamento per raccogliere e gestire i feedback degli utenti ai fini del miglioramento continuo. Le problematiche riscontrate in tal modo verrebbero indirizzate dai professionisti ai rispettivi stakeholders misurando il grado culturale degli stessi [9].
La cultura del personale interno e dei fornitori risulta una componente essenziale intrinseca ad ogni processo, a cui va posta particolare attenzione. La logica di business, utilizzata da controparti esterne, normalmente differisce da quella dell'Azienda sanitaria; ciò comporta dei rischi, dovuti al gap culturale, che possono precludere la creazione di partnership professionali inclini alle buone pratiche di sicurezza. Per evitare ciò è necessario un team dedicato altamente competente che predisponga opportuni processi di gestione del rischio delle terze parti [10].
La consapevolezza di queste tematiche potrebbe crescere ed espandersi in maniera capillare, per improntare un livello culturale ed un clima

aziendale incline alle buone pratiche di gestione del cambiamento tecnologico. La sicurezza non verrebbe più vista come costo e pesante responsabilità, ma verrebbe rivalutata come obiettivo e valore aggiunto [11].

II. Materiali e metodi

A. Gli incidenti di sicurezza

Ogni servizio erogato dall'Azienda sanitaria è costituito, oltre che dal software, anche da ulteriori asset molto onerosi quali i professionisti utilizzatori, l'hardware, le infrastrutture di rete. Dal punto di vista dell'analisi dei rischi, ognuna di queste componenti presenta tre caratteristiche fondamentali:

- CONFIDENTIALITY. Confidenzialità è l'equivalente di riservatezza o più semplicemente privacy. Le misure adottate per assicurare la confidenzialità servono a prevenire che informazioni riservate e sensibili vengano consultate da persone non autorizzate.
- INTEGRITY. Integrità significa mantenere la consistenza, la precisione e l'attendibilità dei dati nel loro intero ciclo di vita. I dati non possono essere cambiati da nessuna componente del servizio senza una specifica autorizzazione né alterati a causa di errori.
- AVAILABILITY. Disponibilità significa garantire rigorosamente la continuità ed il corretto funzionamento dei processi che gestiscono le informazioni. I dati devono essere disponibili agli utenti secondo i Service Level Agreement - SLA garantiti dal fornitore o dall'Azienda.

Il livello di sicurezza di ogni asset dipende quindi dalla somma di questi tre parametri [12]. Qualsiasi atto di violazione di un'esplicita od implicita politica di sicurezza aziendale basata su queste tre componenti si definisce incidente di sicurezza. Le casistiche principali in cui si verifica un incidente di sicurezza possono essere così riassunte:

- Tentativi non autorizzati per guadagnare accesso ai dati ed ai sistemi;
- interruzioni di servizio inattese a causa di guasti od errori;
- interruzioni deliberate della indisponibilità dei servizi;
- uso non autorizzato di un sistema per processare o memorizzare dati;
- cambiamenti alle caratteristiche di un sistema hardware, firmware o software senza che il proprietario ne sia a conoscenza, o che non abbia fornito istruzioni in tal senso ed opportuno consenso.

Gli aggiornamenti software rientrano tra le cause principali di incidente di sicurezza [13]. Nel momento in cui si bloccano parzialmente o interamente le operazioni routinarie di erogazione del servizio, le problematiche che ne scaturiscono possono venire rilevate sia immediatamente che con tempi differiti. In base all'esperienza e secondo un'ottica user centered, tenendo conto dei parametri di usabilità del software ed interazione uomo/macchina, durante un incidente di sicurezza sul software si possono verificare i seguenti diversi contesti cognitivi:

- **Mancanza di riferimenti a livello grafico**. Gli spostamenti o le rimozioni di componenti grafiche senza aver preventivamente informato gli utilizzatori del software possono creare disorientamento. Gli utenti, infatti, abituati a percorrere degli iter grafici famigliari e ricorrenti si disorientano e, perdendo i riferimenti, non riescono più a procedere nell'attività. A questo punto devono intraprendere dei task autonomi di workaround o chiedere del supporto. Tale evento ha un costo stimato direttamente proporzionale al tempo impiegato per riprendere il normale decorso del processo. Gli spostamenti delle componenti grafiche che gestiscono l'input dei dati da parte dell'utente possono anche generare l'immissione errata delle informazioni.
- **Errata funzionalità di calcolo**. A causa di errori il software, non eseguendo più le operazioni correttamente e/o non completando le fasi del processo in manie-

ra idonea, fornisce un dato errato. Gli utenti percepiscono l'errore di calcolo che espone i dati a rischio confidenzialità, integrità e disponibilità. In questo caso gli utilizzatori sono costretti a sospendere l'attività e segnalare nell'immediato la problematica al fornitore, in attesa di ricevere chiarimenti ed opportune autorizzazioni a procedere e comunque, se possibile, proseguire l'attività in modo alternativo. Il costo di tale incidente potrebbe anche essere maggiore del tempo impiegato alla ripresa della normale attività andando ad incidere sulla gravosità degli oneri.

- **Fase di stress lavoro correlato**. Nel momento in cui l'utente non riesce più a governare le fasi di processo del proprio lavoro, emergono degli aspetti psicologici difficilmente gestibili che possono causare all'Azienda ulteriori danni indiretti. L'utilizzatore del programma è in balia degli eventi: "E' stato predisposto un processo di test da parte del fornitore prima di rilasciare il software? O sto facendo da cavia?". Il subire si trasforma in colpevolizzare: la qualità e l'efficienza del lavoro rischiano di decadere e l'utente si sente inappropriato.

In caso di blocco informatico gli operatori si possono avvalere di procedure alternative per proseguire manualmente le attività di erogazione del servizio con il supporto cartaceo o tramite altri strumenti informatici sostitutivi. Tale modalità di lavoro comporta ovviamente maggiori rischi inerenti alla privacy ed un degrado progressivo delle attività.

B. La quantificazione del danno

In seguito ad un incidente di sicurezza sul software ci si limita, nella maggioranza dei casi, alla fase di risoluzione del problema tralasciando l'analisi conclusiva di post incidente: fondamentale per la quantificazione del danno e la definizione di idonee misure di contenimento e prevenzione [14].

Nell'Unità Operativa di Medicina Nucleare dell'Azienda Provinciale per i Servizi Sanitari di Trento è stato possibile analizzare in maniera approfondita tale tipo di evento.
Una delle attività core dell'Unità Operativa di Medicina Nucleare è la misurazione della differenza nei pazienti tra stabilità/progressione di malattia e risposta alle terapie (parziale/completa/assente), ottenuta attraverso strumenti software di diagnostica per immagini. Si trattano dati relativi ad esami mediamente composti da 1.200 a 4.000 immagini digitalizzate ed il lavoro medio su queste sofisticate applicazioni software è 1.800 ore annuali di operatore tecnico. Il software gestionale che governa questo processo rappresenta un asset critico senza il quale la refertazione non è possibile non esistendo alternative ad esso. A seguito di un aggiornamento software il processo di rielaborazione degli esami è rimasto bloccato ed un cospicuo numero di dati ha perso di integrità. L'unico modo per eseguire la rielaborazione è stato richiamare una ad una ogni registrazione, correggendola manualmente da consolle. Per sistemare gli errori sui dati, ad un ritmo di 10 esami al giorno per 60 giorni lavorativi, si sono rese necessarie 600 ore lavorative di operatore tecnico. Si è stimato l'impatto tramite un metodo di quantificazione del danno che ha tenuto conto del numero di ore operatore impiegate per la correzione degli errori ed il suo costo orario. Poiché il costo orario dell'operatore è di 25,46 €, si è stimato un danno di 600 h x 25,46 € = 15.276 €. Sono stati aggiunti nel costo complessivo ulteriori elementi intangibili:

- stress lavoro correlato,
- disagio dell'operatore,
- presenza di maggiori rischi, in particolare quello legato alla privacy.

L'Unità Operativa ha dichiarato che simili accadimenti possono verificarsi in seguito ad attività di aggiornamento del software.
Dal 10 settembre 2004 sono state rilevate direttamente dal reparto IT dell'Azienda sanitaria problematiche simili anche in altri servizi [15]:

- Servizio di backup e restore (4)
- Rete di dominio aziendale (86)

- Rete banda larga (2)
- Anatomia Patologica (1)
- File sharing (2)
- CUP - Centro Unico di Prenotazione (4)
- Prescrizione elettronica (3)
- Servizio di repository dei referti (63)
- LIS - Laboratory Information System (17)
- Catena informatizzata laboratorio (4)
- Accettazione laboratorio (6)
- RIS - Radiology Information System (23)
- SIO - Sistema Informativo Ospedaliero (45)
- Sistema Informativo Territoriale (17)
- Posta elettronica (12)
- Sistemi di accettazione (12)
- Anagrafe assistiti (16)
- Ser.T - Servizio per le Tossicodipendenze (2)
- Trasfusionale (2)
- Terapia intensiva e rianimazione (2)
- Screening mammografico (1)
- Accesso internet (2)
- Sistema del Protocollo Informatico Provinciale (2)
- Gestione contabilità (1)
- Gestione magazzino (1)
- Gestione richieste (1)
- Gestione logistica (1)
- Gestione cespiti (1)
- Gestione Servizi Tecnici (1)

Anche in questi casi le statistiche hanno confermato che gli incidenti si sono verificati a seguito di una carente gestione dello IT Change Management.
La mancanza all'interno dell'Azienda di una struttura di riferimento al monitoraggio degli incidenti, indipendente dal reparto IT, rende sottostimato il conteggio di tali accadimenti purtroppo non segnalati e registrati.

C. Lo scenario di rischio attuale

L'azienda eroga centinaia di servizi con una tecnologia informatica e clinica sempre più complessa ed interconnessa che, certamente, offre dei benefici significativi ma, contemporaneamente, può causare criticità ed incidenti a catena. In tale contesto, caratterizzato dall'introduzione delle nuove tecnologie e dalle minacce informatiche sempre più sofisticate, anche gli operatori vengono esposti a nuovi rischi [16, 17, 18]. Le logiche di business dei produttori di software, totalmente diverse da quelle delle Aziende sanitarie, non sempre si curano degli aspetti di sicurezza del cliente. Inoltre, all'interno dell'Azienda sanitaria, non esistono dei processi coordinati che controllino l'operato e lo stato di sicurezza dei terzi. A causa di questa situazione è nato un gap culturale a svantaggio dell'Azienda sanitaria.
Ulteriore vulnerabilità è legata ad una sola parziale presenza di un approccio agile e sistematico verso gli aspetti legati alla sicurezza del software. Mancano figure trasversali ed operative certificate e competenti in materia di rischio e sicurezza informatica, che siano in grado di interfacciarsi con il reparto IT e le Business Units per implementare politiche e processi organizzativi interni utili al cambiamento.
Le carenti politiche di Change Management per i sistemi sanitari interconnessi sono tra le maggiori cause di rischio [19, 20].
La procedura sostitutiva od alternativa non sempre è attuabile, sia per il suo costo di implementazione, sia per la ormai totale informatizzazione che, purtroppo, non permette un efficace processo parallelo.
Un'ulteriore componente dello scenario di rischio attuale è la problematica relativa alla privacy. In tale contesto la criticità si presenta in forma più elevata in quanto correlata a dati sensibili e supersensibili. Operazioni non autorizzate o alterazioni che intacchino non solo la confidenzialità, ma anche l'integrità e la disponibilità di tali informazioni personali, possono dare adito a procedimenti legali, in particolare:

- sanzioni amministrative da parte dell'Autorità Garante [21],
- risarcimento del danno da parte dell'interessato,
- illecito penale nei confronti del Titolare del Trattamento dei dati,
- sospensione del Trattamento dei dati [22].

Dal 2015 la normativa privacy obbliga le Aziende sanitarie a segnalare all'Autorità Garante l'accadimento di violazioni sui dati (data breach) ed incidenti informatici avvenuti sui trattamenti gestori di dossier e fascicolo sanitario elettronico [23]. Risulta sempre più faticoso comprendere ed applicare le normative e le regolamentazioni in ambito privacy e sicurezza in quanto implementate tramite standard internazionali e tecnologici molto complessi. Tale difficoltà rende il costo di adeguamento sempre più elevato.

D. I costi del cambiamento del software

Analizzando negli anni i costi IT, notiamo come il parametro relativo alla diminuzione del costo dell'hardware risulti inversamente proporzionale a quello del software [24]. Ad oggi, in un singolo sistema informatico, il costo del software incide maggiormente rispetto a quello dell'hardware sul Total Cost of Ownership (TCO) [25] . Per fare un esempio, la componente software di un sistema di diagnostica per immagini può incidere anche per il 70% sul prezzo d'acquisto della fornitura totale (hardware, software e strumentazione elettromedicale). Il software rientra in assoluto tra gli asset più importanti del sistema informativo aziendale e come tutti i beni più preziosi va opportunamente tutelato. Risultano quindi fondamentali il controllo e la supervisione atti a garantirne continuità e sicurezza, nell'ottica del miglioramento della qualità dei processi. Si tratta di una componente che necessita di aggiornamenti continui per motivi legati ai seguenti contesti di sviluppo operativo:

- MANUTENZIONE CORRETTIVA. Attività gestionale eseguibile in maniera ordinaria e straordinaria che serve ad eliminare gli errori del software rilevati dagli utenti durante l'operatività in ambiente di test e produzione.
- MANUTENZIONE EVOLUTIVA. Normalmente dovrebbe essere pianificata in accordo con il cliente e consiste nell'introdurre nel software nuove automazioni o migliorie di attività del processo gestionale ordinario.
- COMPLIANCE TECNOLOGICA. In questo caso le modifiche al software sono richieste dal cliente al fine di permettere nel processo gestionale il rispetto delle politiche e degli standard aziendali.
- ADEGUAMENTO NORMATIVO. Le modifiche sono svolte per adeguare il software a nuove regolamentazioni provinciali, regionali, nazionali e comunitarie.
- ADEGUAMENTO DI SICUREZZA. Le patch di sicurezza vengono applicate per risolvere vulnerabilità che un utente malevolo o il cybercrime possono sfruttare per accedere ad informazioni riservate, per alterare e cancellare dati oppure bloccare le funzionalità del software e dei sistemi ad esso collegati senza autorizzazione.

Ogni modifica dovrebbe essere sempre gestita dalla software house tramite un rigoroso processo di Release Management che prevede la gestione e la pianificazione controllata dello sviluppo e messa in produzione del software attraverso differenti fasi, in opportuni ambienti di test. Non sempre ciò si verifica a causa degli elevati costi che comporta lo svolgimento di questi task ed a politiche aziendali del fornitore. Tale processo dovrebbe contenere i danni in caso di errori e garantire un eventuale ritorno alla situazione precedente (backout). L'ingegneria del software, negli anni, ha sviluppato dei framework in grado di garantire elevati livelli di sicurezza per soddisfare le esigenze del cliente, bilanciando vantaggi e svantaggi. Queste sono le tipologie principali di Release Management:

- WATERFALL MODEL. Il modello a cascata richiama la tipica sequenza di fasi della produzione manifatturiera. E' il primo modello di ciclo di vita del software. Il processo è statico e prevede delle fasi sequenziali che producono un output per la fase successiva (Requirements-Design-Implementation-Verification-Maintenance). E' un modello

obsoleto che presenta molti difetti dovuti alla difficoltà di coordinamento ed agli elevati costi di sviluppo e test.
- PLAN DRIVEN METHODS. Il rilascio delle release tramite metodi pianificati prevede una schedulazione delle modifiche applicate in maniera cumulativa e consistente. Ciò causa maggiori rischi dovuti all'alta probabilità di errore ed alla difficoltà di backout.
- AGILE SOFTWARE DEVELOPEMENT. E' un insieme di metodi di sviluppo che prevede una maggiore interazione con l'utente finale con rilascio frequente di piccole modifiche. In tal modo gli impatti, in caso di errore, risultano limitati ed è più facile eseguire il backout.
- CONTINUOS DELIVERY. L'aggiornamento del software segue gli stessi canoni dell'Agile Developement ma a cicli più brevi. I rilasci del software sono effettuati continuamente.
- DevOps - DEVELOPEMENT OPERATIONS. E' un modello integrato di controllo e miglioramento che mira alla continua comunicazione e collaborazione tra developers, referenti di Information Technology ed utenti utilizzatori, che prevede l'applicazione di rilasci in maniera flessibile e molto frequente. Il software aumenta di affidabilità e sicurezza tramite più veloci cicli di sviluppo e rilascio.

I costi relativi alla manutenzione del software in un anno possono incidere dal 10% al 15% sul prezzo di acquisto. Al termine del ciclo di vita di un software, che può durare anche più di 10 anni, i costi indiretti relativi alla soluzione di tali problematiche possono ammontare al 400% - 500% del costo di acquisto iniziale. Nella pratica la ripartizione di questi oneri viene quantificata in costi diretti ed intangibili quali:

- MINORE SICUREZZA DEL PAZIENTE
- DISAGIO E STRESS LAVORO CORRELATO
- PERDITA DI INTEGRITA' DEL DATO
- TEMPO DEDICATO ALLA SUA CORREZIONE
- PERDITA DI DISPONIBILITA' DEL DATO
- TEMPO DEDICATO AL SUO REPERIMENTO

Nell'ottica di contenimento dei costi ed eliminazione degli sprechi, la presa in considerazione di questi aspetti rappresenterebbe un ottimo punto d'inizio per elaborare una strategia di sicurezza e risparmio.

E. Il giusto approccio per diminuire la superficie di rischio

Le problematiche legate al cambiamento del software, come abbiamo visto, sono innumerevoli. I costi accennati nel paragrafo precedente rappresentano solo la punta dell'iceberg. Poiché la mancanza di supervisione dei cambiamenti è tra i veicoli di rischio principali dell'Azienda sanitaria [26], l'obiettivo innanzitutto è proteggere il core business con una barriera di controllo che coinvolga le seguenti aree:

- RISORSE UMANE
- PROCESSI ORGANIZZATIVI
- GESTIONE DELLE TERZE PARTI

Come consigliato dallo standard di sicurezza ISO 27001, l'attività di supervisione del cambiamento andrebbe incorporata in un processo ongoing rivolto al miglioramento continuo nel medio e lungo periodo, anche al fine di garantire un Information Security Management System - ISMS [27]. Per poter contrastare la problematica del cambiamento occorre infatti fare riferimento al Ciclo di Deming - Plan Do Check Act - così da migliorare nel tempo la sicurezza, la capacità operativa e il grado di maturità.
Potremmo classificare i possibili approcci alle problematiche di sicurezza in tre categorie:

- MATURITY LEVEL 1: Approccio reattivo. Tale forma mentis caratterizza la "mentalità alla vecchia maniera". Si risolvono le problematiche ma non si fa in modo di prevenirle né di impedirne la reiterazione. I costi di risposta all'incidente risultano complessivamente alti.
- MATURITY LEVEL 2: Approccio proattivo. Oltre a possedere una buona capacità di risoluzione del problema, si evi-

ta che quest'ultimo si reiteri grazie ad un'analisi accurata delle cause scatenanti. Ne deriva una possibile diminuzione dei costi.
- MATURITY LEVEL 3: Approccio predittivo. Si cerca di prevenire il danno analizzando periodicamente i processi di sistema e l'ambiente circostante per identificare correttamente il rischio inerente e nuove potenziali minacce. E' in assoluto il migliore approccio: permette di contenere i rischi ed i costi.

Ad oggi il maturity level della maggior parte delle Aziende sanitarie si colloca tra il primo ed il secondo livello.
Una corretta strategia implementativa del processo di monitoraggio dei cambiamenti sul software deve tenere conto di questo grado di partenza e considerare i seguenti passaggi operativi:

- definire gli obiettivi di sicurezza e la strategia con Risk Manager e Security Manager;
- diffondere delle metodologie standard di analisi del rischio alle quali fare riferimento;
- agevolare la comunicazione all'interno dell'Azienda, cercando di non considerare le Business Units come dei silos;
- monitorare, eseguire controlli preventivi e detettivi;
- coinvolgere le terze parti con strumenti giuridico/contrattuali ed attività di controllo/audit;
- contenere gli impatti sulla corretta diagnosi del paziente;
- evitare alterazioni e propagazione di errori sui dati;

Tra le possibili soluzioni attuabili nel contesto sanitario, quella che risulta avere un miglior rapporto costi/benefici è il processo di IT Change Management.

F. Il processo di IT Change Management

Fonti e standard internazionali autorevoli come Gartner, ITIL, ISACA COBIT, ISO 20000, ISO 27001 identificano tale processo come componente fondamentale per governare i processi e le risorse IT all'interno dell'Azienda. Questo framework, ormai consolidato, si interessa dei cambiamenti dell'infrastruttura IT utilizzando metodi e procedure standard con l'obiettivo di:

- analizzare i rischi,
- comprendere i cambiamenti in corso,
- verificare preventivamente le modifiche software,
- ridurre l'impatto umano e tecnologico dovuto ad incidenti,
- offrire un'efficiente gestione dei cambiamenti,
- contenere i costi legati ai cambiamenti.

Il processo si colloca all'interno del quadro di governo dei servizi di IT Service Management. Le componenti principali di questo framework si possono identificare nelle seguenti risorse:

- RFC (REQUEST FOR CHANGE). Per richiedere un cambiamento è obbligatorio redigere una richiesta formale con le informazioni necessarie alla successiva valutazione, approvazione ed implementazione. Le motivazioni principali di una RFC possono riguardare le modifiche delle componenti software dei servizi, ma anche le contromisure intraprese a seguito di un incidente, l'insoddisfazione di un utente di un servizio, la modifica di una configurazione hardware e di rete, gli spostamenti logistici ed i cambiamenti richiesti a seguito di richieste organizzative ed adeguamenti normativi.
- CHANGE INITIATOR. Gli utenti aziendali e le terze parti autorizzate possono innescare il processo di Change Management inoltrando una RFC. Nel caso in cui tutti fossero Change Initiators, un service desk dovrebbe raccogliere le RCF per garantire un inoltro appropriato delle stesse.

- CHANGE ADVISORY BOARD (CAB). E' un team decisionale di esperti, formato dal Change Manager, che comprende figure IT e Business Unit Managers. Il compito principale di questo gruppo è analizzare le RFC di una certa entità, determinando gli impatti e le risorse necessarie per la loro implementazione, nonché garantire che i cambiamenti siano svolti in maniera pronta ed efficace. Il CAB partecipa in meeting programmati esprimendo il proprio parere sui Change in agenda al fine di autorizzarne l'esecuzione.
- CHANGE ADVISORY BOARD / EMERGENCY CHANGE (CAB/EC). E' un team decisionale, simile al CAB, ma costitutito per svolgere l'autorizzazione delle richieste in regime di Emergency Change - EC. Le situazioni di emergenza possono imporre che i membri del gruppo siano reperibili e, per questo motivo, gli incontri del gruppo vengono normalmente svolti virtualmente per autorizzare le richieste o declassarle ad una categoria inferiore.
- CHANGE EXECUTOR / CHANGE IMPLEMENTER / CHANGE BUILDER. Questa figura, rappresentata dall'esperto tecnologico referente di servizio o amministratore di sistema, viene coinvolta nell'applicazione e nell'implementazione delle RFC per assicurare che tutte le risorse hardware, software, licenze, ecc.. siano disponibili. Una volta implementato il Change, il Change Executor indica nella RFC la tipogia di test più appropriata per verificare l'implementazione. Se tale attività richiedesse il coinvolgimento di una terza parte, l'attività dovrebbe essere documentata direttamente nella RFC. Il Change Executor dovrebbe essere sempre identificato nella RFC, in modo tale che tutti gli attori coinvolti nel processo sappiano a chi sia stata indirizzata la richiesta.
- CHANGE MANAGER. E' il ruolo più importante del processo normalmente ricoperto da un esperto di IT e Security. Il Change Manager riceve, traccia e determina insieme al Change Initiator la priorità di tutte le RFC e respinge eventuali richieste non praticabili. Decide quali sono i componenti del CAB e pianifica gli incontri del gruppo, fornendo preventivamente a tutti i membri la lista delle richieste da esaminare in modo che si possa effettuare una valutazione preliminare. In caso di emergenza convoca un CAB/EC. Presiede tutti i meetings fornendo informazioni su eventuali rischi ed offrendo supporto decisionale. Collabora con tutte le strutture coinvolte per coordinare le fasi di implementazione e test previste dalla pianificazione e controlla con il Change Tester ed il Change Executor l'esito delle verifiche. In caso di errori supervisiona le RFC e comunica le decisioni intraprese documentando eventuali fasi di backout. Esegue le attività di controllo e verifica in modo che tutti i Change siano gestiti correttamente, assicurando il raggiungimento degli obiettivi. Chiude le RFC e presenta al management dei report regolari ed accurati supervisionando l'intero processo, segnalando specifici trend in atto e problematiche emergenti.
- FORWARD SCHEDULE OF CHANGES (FSC). Le RFC approvate e di imminente applicazione si inseriscono in un elenco che viene condiviso con tutte le altre figure coinvolte per pianificare i rilasci. Lo FSC deve avere una schedulazione dettagliata per il breve periodo ed una pianificazione di massima per il lungo periodo. Deve contenere eventuali periodi di downtime da comunicare agli utilizzatori dei servizi.
- PROJECTED SERVICE AVAILABILITY (PSA). Il PSA rappresenta un documento dove vengono evidenziati gli effetti del cambiamento sui Service Level Agreement - SLA. Questa componente viene distribuita congiuntamente allo FSC per condividere con il Service Desk, l'Availability Management e gli utilizzatori le

informazioni dei rilasci.

- CHANGE MODEL. Un Change Model è una tipologia di RFC per la quale è stato preventivamente stabilito uno specifico percorso predefinito. L'iter del modello normalmente si basa sul tipo di richiesta, sulla gravità e sull'impatto. I Change con impatto marginale seguono un loro percorso e possono essere approvati direttamente dal responsabile diretto del Change Initiator senza essere necessariamente autorizzati dal Change Manager o dal CAB.
- MANAGEMENT SOFTWARE. Per gestire il processo nella sua interezza è necessario un software enterprise di IT Service Management - ITSM che, tramite un Configuration Management Data Base - CMDB, interfaccia i moduli software di governo IT dell'Azienda e dei fornitori.

Una volta definite le componenti principali, le fasi del processo di IT Change Management possono essere così riassunte:

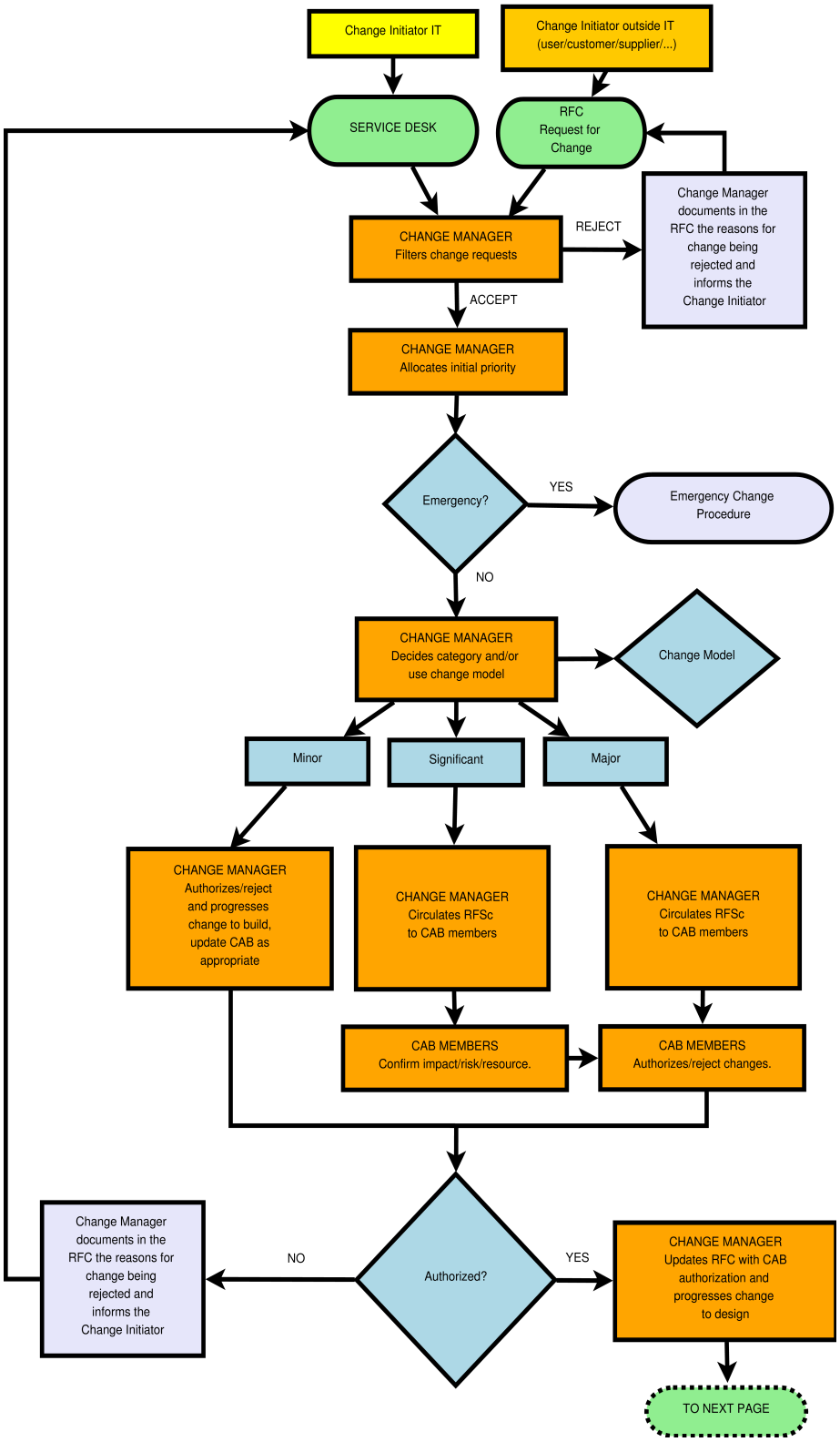
- **FASE DI PROPOSTA**. Ogni membro dell'organizzazione, utente del servizio e fornitore esterno autorizzato può essere un Change Initiator e richiedere un cambiamento di un servizio tramite l'inoltro di una RFC (Request For Change). Una volta inoltrata la richiesta il Change Manager può procedere con l'accettazione od il rifiuto della stessa. In caso di rifiuto il Change Manager documenta nella RFC la motivazione del recesso della richiesta ed informa il Change Initiator. In caso di accettazione, il Change Manager assegna alla richiesta una priorità iniziale decidendo il grado di urgenza, eventualmente innescando un Emergency Change [28].
- **FASE DI APPROVAZIONE**. Se la la RFC viene considerata urgente, viene invocata l'Emergency Change Procedure. In tutti gli altri casi il Change Manager assegna una tipologia secondo una scala di gravità:
  - STANDARD CHANGE. Richiesta preautorizzata che utilizza una procedura validata preventivamente.
  - IT CHANGE MODEL. Richiesta riferita ad un IT Change Model. Può richiedere ulteriore livello di autorizzazione.
  - MINOR. Il Change Manager decide sul rifiuto od eventualmente sul proseguimento della richiesta informando opportunamente il CAB.
  - SIGNIFICANT. Il Change Manager non decide ed invia preventivamente l'elenco delle RFC ai membri del CAB. Il CAB prende visione e conferma il grado di rischio, l'impatto e le risorse da utilizzare proposte dal Change Manager e procede all'eventuale autorizzazione o rifiuto della RFC.
  - MAJOR. Il Change Manager non decide ed invia preventivamente l'elenco delle RFC ai membri del CAB, il quale procede all'eventuale immediata autorizzazione o rifiuto della RFC.

  L'approvazione delle richieste può quindi essere effettuata direttamente dal Change Manager nel caso di richieste con priorità minore. Per tutti gli altri casi l'elenco delle RFC viene inviato preventivamente al CAB. L'autorizzazione o l'eventuale recesso vengono effettuati durante i meeting programmati direttamente dai membri del CAB. Se la richiesta non viene accolta, il Change Manager documenta le motivazioni informando il Change Initiator. In caso di accoglimento della richiesta, il Change Manager aggiorna lo stato della RFC e procede con la fase di esecuzione [29].
- **FASE DI PIANIFICAZIONE E TEST**. In questa fase il Change Executor pianifica, implementa e verifica il Change con la supervisione ed il coordinamento del Change Manager. L'attività può essere espletata da in due funzioni specifiche di Change Executor:
  - CHANGE DESIGNER. Questa figu-

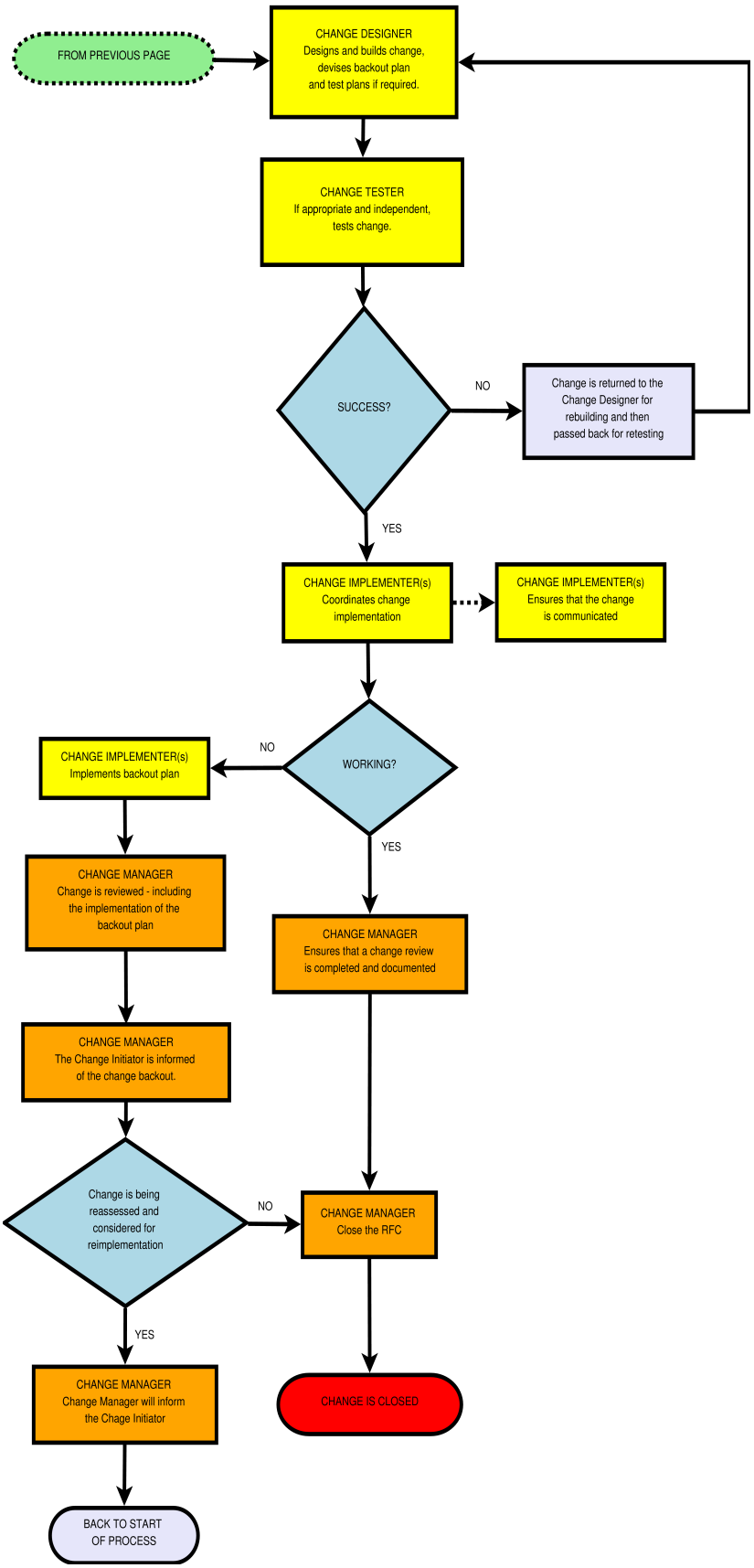
ra analizza la RFC disegnando e pianificando la costruzione del cambiamento escogitando le tecniche di applicazione. Successivamente implementa e verifica il backout plan, il piano di rientro pensato per ritornare alla situazione precedente, il caso in cui l'applicazione del cambiamento creasse problematiche di sicurezza.
  - CHANGE TESTER. Se ritenuto appropriato dal Change Manager, possono essere impiegate più risorse per verificare la corretta applicazione dei cambiamenti. La figura del Change Tester dovrebbe garantire imparzialità, correttezza e qualità del test. Per questo motivo si preferisce che tale fase sia completata da una terza parte indipendente e non dal Change Executor. In caso di test fallito, la RFC torna al Change Designer per essere revisionata e successivamente reiterata al Change Tester per la sua verifica [30].
- **FASE DI ESECUZIONE**. Il Change Executor coordina l'implementazione del Change e si assicura che tale attività sia comunicata alle parti interessate. Se il Change nell'ambiente di produzione non ha successo, viene implementato il backout plan. Il Change Manager rivede tutte le parti della RFC, inclusa l'implementazione del backout plan, ed informa il Change Initiator. Se il Change non viene rivalutato e riconsiderato per la reimplementazione, il Change Manager chiude la RFC. Se il Change viene riconsiderato per la reimplementazione, il processo riparte dall'inizio. Nel caso in cui il Change abbia invece successo, il Change Manager verifica che la RFC sia completa in tutte le sue parti, eventualmente le integra con le informazioni mancanti e la chiude per terminare il processo [31].

Il ciclo di vita di questo processo permetterebbe nel tempo di monitorare parametri molto importanti relativamente all'organizzazione. Per esempio, esaminare il trend di abuso delle RFC svolte in Emergency Change rappresenterebbe una delle metriche più importanti per misurare lo stato di sicurezza aziendale. Allo stato dell'arte vi sono validi riferimenti per introdurre questo framework in azienda. Il modello di IT Change Management proposto da UCISA - Università di Oxford, basato su ITIL, risulta idoneo e propedeutico all'introduzione del processo in Azienda [32]. Per questo motivo è stato preso come riferimento.

IT CHANGE MANAGEMENT PROCESS: FASE DI PROPOSTA ED APPROVAZIONE



IT CHANGE MANAGEMENT PROCESS: FASE DI PIANIFICAZIONE, TEST ED ESECUZIONE



III. Risultati

A. Analisi costo/efficacia

Abbiamo potuto osservare come l'infrastruttura IT sia sempre più complessa e sia costituita da centinaia di software tra loro fortemente interdipendenti; come tali strumenti siano utilizzati costantemente da migliaia di persone e in essi la frequenza di security incidents sia molto elevata a causa di continue modifiche effettuate senza un'efficace processo di supervisione.
Se un unico piccolo incidente in una singola Unità Operativa ha comportato un danno di circa 15.000 €, calcolato solo sulle ore di lavoro straordinario dell'operatore, senza contare il disagio, lo stress lavoro correlato e la possibilità di eventuali contenziosi legali che ne sarebbero potuti scaturire, quanto sono venuti a costare all'Azienda tutti gli incidenti che si sono già verificati?
L'impiego di un Change Manager, in grado di supervisionare il processo di IT Change Management, all'interno di un'Azienda sanitaria di grandi dimensioni, potrebbe essere stimato in circa 80.000 € / anno.
Il costo dei software dedicati potrebbe essere ammortizzato utilizzando strumenti open source e risorse interne.
Molti casi al mondo dimostrano come il processo di IT Change Management sia una tematica di interesse e costituisca un grande patrimonio aziendale in grado di ridurre efficacemente i rischi e migliorare l'erogazione dei servizi, soddisfacendo le esigenze reali delle Business Units [33, 34]. Tra i numerosi benefici ottenibili evidenziamo [35]:

- RISPARMIO TEMPO OPERATORE
- RISPARMIO COSTI DI MANUTENZIONE SOFTWARE
- RIDUZIONE IMPATTO UMANO E TECNOLOGICO
- RIDUZIONE GAP CULTURALE CON I FORNITORI
- MINORE RISCHIO
- MINORE STRESS E DISAGIO OPERATORE
- MAGGIORE QUALITA' ED EFFICIENZA
- MAGGIORE CONTROLLO DELLE TERZE PARTI
- MAGGIORE CONSAPEVOLEZZA
- ALTA COMPETENZA
- APPROCCIO PROATTIVO/PREDITTIVO
- MIGLIORAMENTO CONTINUO

IV. Discussione - Conclusioni

Sono state investite negli anni molte risorse per aggiornare le infrastrutture, le reti di comunicazione ed i software utilizzati dai professionisti sanitari. Il patrimonio informativo delle Aziende sanitarie oggi risulta oggetto di mantenimento ma soprattutto di protezione, poiché in esso convergono i dati sanitari di tutti i cittadini. I fornitori garantiscono che i loro software sono esenti da errori e che gli aggiornamenti vengono rilasciati in seguito a processi di controllo e test, ma la realtà dimostra che il grado di sensibilità verso queste tematiche non è sempre quello desiderato. Fortunatamente le problematiche analizzate possono essere risolte facendo riferimento a strumenti quali il processo di IT Change Management. La riallocazione interna delle risorse porterebbe sensibili benefici nelle aree problematiche, consentendo un miglioramento continuo anche nel medio-lungo periodo.
Il processo di Change Management è un framework molto versatile ed universale che può essere, inizialmente, applicato solo al software e, successivamente, impiegato anche al monitoraggio della gestione di altre infrastrutture di base, quali le configurazioni dei sistemi, delle reti, degli elettromedicali e di tutto ciò che riguarda la tecnologia e per quanto di competenza nella definizione e preparazione delle gare di acquisizione e manutenzione del software. Come tutti i modelli di riferimento, va introdotto in Azienda ed adattato in maniera opportuna per poterlo valorizzare, rendere efficace, agile e fruibile.

Riferimenti bibliografici

[1] Application security assurance prediction: *Information technology - Security techniques - Application security ISO/IEC 27034:2011*. International Organization for Standardization (ISO) - International Electrotechnical Commission (IEC)

[2] Agenzia per l'Italia Digitale: *Linee Guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione - 6/8/2013* . Presidenza del Consiglio dei Ministri

[3] Agenzia per l'Italia Digitale: *Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni - 2013* . Presidenza del Consiglio dei Ministri

[4] European Commission - DG CONNECT: *eHealth projects Research and Innovation in the field of ICT for Health and Wellbeing: an overview - June 2015*. Digital Agenda for Europe.

[5] Osservatorio delle Competenze Digitali 2015: *L'investimento per un futuro che è già presente - Dati, scenari e proposte per l'Italia digitale*. ASSINFORM - Associazione italiana per l'Information Technology

[6] Government of the HKSAR: *IT OUTSOURCING SECURITY - February 2008*. Government of the Hong Kong Special Administrative Region

[7] Garante per la protezione dei dati personali: *Parere su uno schema di linee-guida in materia di Disaster Recovery delle pubbliche amministrazioni - 20 ottobre 2011 [1851672].*

[8] David Loshin: *Evaluating the Business Impacts of Poor Data Quality - January 2011*. Knowledge Integrity, Inc

[9] The Lewin Group, Inc. : *Indicators of Cultural Competence in Health Care Delivery Organizations: An Organizational Cultural Competence Assessment Profile - April 2002*. Health Resources and Services Administration - U.S. Department of Health and Human Services

[10] PA Consulting Group: *Security for industrial control systems - Manage third party risks - A good practice guide 12/5/2015*. CNPI - Centre for the Protection of National Infrastructure; CESG - Communications-Electronics Security Group UK

[11] Antonello Soro: *La protezione dei dati bussola nel futuro digitale - Intervento di Antonello Soro, Presidente dell'Autorità Garante per la protezione dei dati personali*. Privacy Day Forum - 21 ottobre 2015 – Roma

[12] C-I-A triad: *Information Security Standard ISO/IEC 27002:2013*. International Organization for Standardization (ISO); International Electrotechnical Commission (IEC)

[13] Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone (2012): *Computer Security Incident Handling Guide*. National Institute of Standards and Technology - NIST

[14] Kannamani R. : *A Study of Retrospective change in ITIL Service Management*. IOSR Journal of Business and Management (IOSRJBM), Oct. 2012 PP 45-47

[15] Dott. Giampaolo Franco: *Documento interno: CRASH - Continuity Reporter and Alerter for Security Helper (2008): Sistema di monitoraggio degli incidenti informatici*. Azienda Provinciale per i Servizi Sanitari

[16] Frederick G. Mackaden: *Seven SoftwarerelaDNA:HealthITted Incidents and How to Avoid or Remediate them*. ISACA Journal - January/February 2016

[17] TOP 10 HEALTH TECHNOLOGY HAZARDS FOR 2015 - November 2014: *Risk 2 - Data Integrity: Incorrect or Missing Data in EHRs and Other Health IT Systems*. *Risk 9 - Cybersecurity: Insufficient Protections for Medical Devices and Systems*. Emergency Care Research Institute - ECRI Institute

[18] Advisory Services Security: *Changing the game - Key findings from The Global State of Information Security Survey 2013*. PricewaterhouseCoopers (PwC)

[19] TOP 10 HEALTH TECHNOLOGY HAZARDS FOR 2014 - November 2013: *Risk 7 - Neglecting change management for networked devices and systems*. Emergency Care Research Institute - ECRI Institute

[20] Glenn O'Donnel: *The State And Direction Of IT Service Management: 2012 to 2013 - March 17, 2014*. Forrester Research

[21] Garante per la protezione dei dati personali: *Diffusione dei dati personali degli utenti registrati sul portale di una ASL - 17 dicembre 2015 [4630534]*. Prescrizioni e divieto del Garante

[22] Garante per la protezione dei dati personali: *Trattamento di dati tramite il dossier sanitario aziendale - 3 luglio 2014 [3325808]*. Prescrizioni e divieto del Garante

[23] Garante per la protezione dei dati personali: *Linee guida in materia di Dossier Sanitario - 4 giugno 2015*. Deliberazione

[24] Jorgenson, Dale W. and Kevin Stiroh: *Source Hardware Cost Index, Raising the Speed Limit: US Economic Growth in the Information Age. Measuring and Sustaining The New Economy - 31 Oct 2000*. National Academy Press 2001.

[25] Dean S. Petracca: *Software Pricing Trends How Vendors Can Capitalize on the Shift to New Revenue Models - January 2007*. PricewaterhouseCoopers (PwC)

[26] Pacific Northwest National Laboratory - IT Services Division: *Risk-Based IT Change Management - 2007*. Joanne R. Hugi Excellence Award - Application for the Norwest Academic Computing Consortium

[27] ISMS - Information Security Management System: *Information Security Standard ISO/IEC 27001:2013*. International Organization for Standardization (ISO) - International Electrotechnical Commission (IEC)

[28] NUIT - Northwestern University Information Technology: *Change Management Process - June 2011*.

[29] Evergreen Systems, Inc. : *Sample IT Change Management Policies and Procedures Guide - 2007*. SANS Institute - SysAdmin, Audit, Networking, and Security

[30] Peter Doherty, Peter Waterhouse: *White Papaer: Change Management: A CA IT Service Management Process Map - 2006*. CA Technologies - USA

[31] Peter Doherty: *TECHNOLOGY brief: Change Management: A CA Service Management Process Map - 2009*. CA Technologies - USA

[32] UCISA Project and Change Management Group: *ITIL - Example of a Change Management Procedure / Change Process Diagram - 2014*. UCISA University of Oxford - Universities and Colleges Information Systems Association

[33] John Forsythe, Siobhan Carrol, Chris Norton, Elizabeth Mackenroth, Rebecca Norton, Rowan Strain: *The DNA of Health IT change Management - November 2012*. PricewaterhouseCoopers

[34] Alexander Hoerbst, Werner O Hackl, Roland Blomer and Elske Ammenwerth: *The status of IT service management in health care - ITIL in selected European countries - 21 December 2011*. BMC Medical Informatics and Decision Making

[35] Doug Tyre: *Calculating ITIL ROI - Issues and Case Study Results January, 20 2012*. Executive Information and Technology Institute - University of Miami