UNIVERSITÀ CATTOLICA del Sacro Cuore
ALTEMS
ALTA SCUOLA DI ECONOMIA E MANAGEMENT DEI SISTEMI SANITARI

hisSA health information system Security Assessment MD

La cyber-security nella sanità

Metodologia di analisi e modello di maturità per la valutazione della sicurezza nei sistemi informativi collegati con i dispositivi medici secondo un approccio di Health Technology Assessment

Fabrizio Massimo Ferrara
Coordinatore scientifico "Laboratorio sui sistemi informativi sanitari" ALTEMS

Con il contributo di:

- Massimo Capponi, IoT
- Massimo Casciello, Ministero della Salute - Direzione generale della vigilanza sugli enti e della sicurezza delle cure
- Tiziana Catarci, Dipartimento di Ingegneria Informatica, Automatica e Gestionale, Università Sapienza
- Quirino Davoli, Dipartimento Tecnologie Informatiche ASL Roma 3
- Mario Fregonara Medici, APSS Trento e Associazione Italiana Ingegneri Clinici
- Paolo Romolo Locatelli, Politecnico di Milano, Osservatorio Innovazione Digitale in Sanità
- Sergio Pillon, Commissione Paritetica Nazionale per la governance delle linee di indirizzo della Telemedicina
- Elena Sini, HIMSS Italian Community
- Mariachiara Violante, Laboratorio sui sistemi informativi sanitari ALTEMS

Premessa

E' ormai ampiamente riconosciuto che in una azienda sanitaria moderna il sistema informativo non può essere un semplice insieme di tecnologie e programmi software più o meno correlati fra loro, ma deve rappresentare uno strumento completo ed integrato per il governo della struttura, sia dal punto di vista della gestione corrente che sotto il profilo della strategia evolutiva, assicurando la continuità dei processi aziendali attraverso i diversi settori e l'integrazione e la disponibilità del patrimonio informativo sotto il profilo sia clinico che amministrativo. E questo sia all'interno dell'azienda che nel contesto della rete territoriale per la continuità del percorso assistenziale del paziente.

In una tale visione, una valenza particolare assume ovviamente la gestione della "sicurezza" (includendo in questo termine anche gli aspetti di protezione dei dati personali, secondo quanto prescritto dal recente Regolamento UE 2016/679), che va intesa non solo dal punto di vista prettamente tecnologico, ma in quadro più ampio, tale da garantire l'esecuzione sicura e corretta dei processi aziendali, minimizzando e prevenendo –per quanto possibile– tutti i rischi ai quali l'azienda può essere esposta. Rischi che –nel settore sanitario– assumono una rilevanza particolare in quanto possono avere implicazioni anche sulla stessa salute del paziente.

Anche per quanto riguarda il profilo normativo, vale la pena di sottolineare come il Regolamento UE sulla protezione dei dati personali definisca principi e regole di ampio respiro, non circoscrivibili a singole attività o procedure ma di rilevanza per tutte le attività dell'organizzazione. Il loro rispetto nell'ambito del sistema informativo, pertanto, richiede un approccio organico ed integrato che tenga conto di tutti gli aspetti in tutti i settori: dall'organizzazione dei dati, alle funzionalità, alle tecnologie.

In questa visione maggiormente strategica, anche le modalità organizzative secondo cui viene valutato, monitorato ed evoluto il sistema e le caratteristiche funzionali ed informative del sistema informativo costituiscono quindi elementi fondamentali e qualificanti ai fini della sicurezza e della gestione del rischio nell'azienda sanitaria.

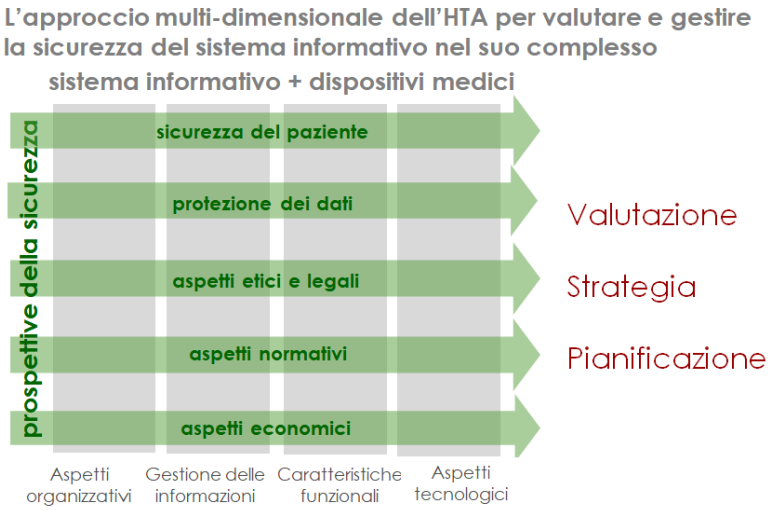
In estrema sintesi l'obiettivo finale di un "sistema informativo sicuro" può essere individuato nella capacità

a) di seguire e supportare senza soluzione di continuità i processi dell'organizzazione (sia quelli che si esauriscono all'interno di un singolo settore che –soprattutto– quelli che si articolano attraverso settori diversi e sul territorio),
b) di integrare e proteggere i dati raccolti attraverso applicazioni, contesti e dispositivi anche eterogenei rendendoli disponibili quando e come necessario alle persone autorizzate,
c) di fornire un contributo attivo nell'identificazione di rischi e situazioni di allarme, anche correlando autonomamente informazioni diverse, anche nel caso di co-morbilità e dimenticanze da parte dell'utente.

Il tutto supportato da una infrastruttura tecnologica robusta ed affidabile, e gestito secondo una organizzazione e criteri formalizzati e misurabili, secondo principi di monitoraggio e miglioramento progressivo.

In un tale scenario, **la gestione della sicurezza** nei sistemi informativi e la definizione di strategie evolutive che tengano conto sia delle possibilità connesse a nuovi modelli organizzativi e a nuove tecnologie, sia delle normative sempre più precise e stringenti **si devono necessariamente basare su un approccio multi-dimensionale che tenga conto di tutte le caratteristiche e di tutti gli aspetti che incidono di fattori di rischio**.

Nel 2016, in collaborazione con la Direzione Generale dei sistemi informativi del Ministero della Salute, l'ALTEMS (Alta Scuola di Economia e Management dei Sistemi Sanitari) ha condotto una indagine a livello nazionale[1] -cui hanno partecipato 113 ospedali- sulla sicurezza dei sistemi informativi sanitari coniugando la tradizionale analisi degli aspetti - organizzativi, informativi, funzionali e tecnologici- del sistema informativo con le prospettive proprie dell'approccio dall' Health Technology Assessment[2,3], quali il rischio clinico[4], l'impatto sul paziente, la protezione dei dati, l'aspetto economico, le implicazioni etiche, la rispondenza alle normative, etc. come schematizzato in figura.



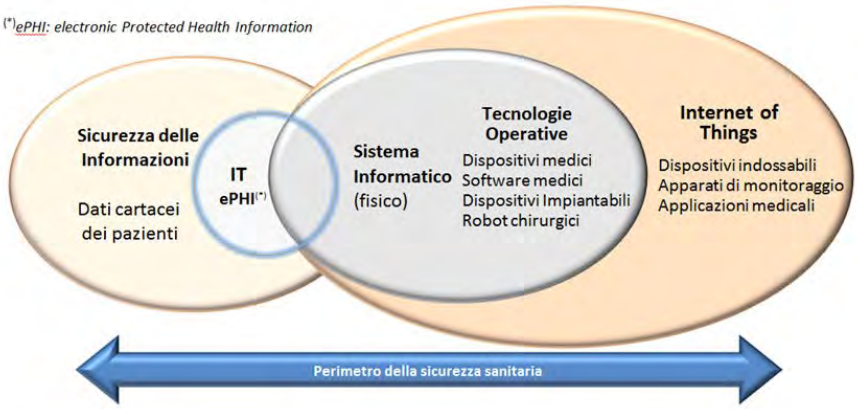
Lo studio ha prodotto una fotografia dello scenario degli aspetti complessivi di sicurezza nei sistemi informativi sanitari secondo un insieme di indicatori -organizzativi, funzionali, informativi e tecnologici- di validità generale ed indipendenti da specifici prodotti ed implementazioni, ed ha proposto una metodologia ed un "modello di maturità" secondo cui rappresentare le modalità di gestione ed il livello di sicurezza complessiva nei sistemi informativi sanitari.

Secondo questo approccio e partendo da questo quadro di validità generale per qualsiasi sistema informativo sanitario, questo nuovo studio definisce una metodologia di analisi ed un modello di riferimento per gli aspetti di sicurezza specifici dei contesti -sempre più rilevanti- in cui i dispositivi medici elettronici rivestono un ruolo significativo nel processo

1 https://altems.unicatt.it/altems-i-sistemi-informativi-sanitari-per-il-governo-dell-organizzazione-analisi-della-sicurezza
2 Ferrara, "ICT e HTA: il ruolo dell'HTA nella valutazione dei sistemi informativi sanitari"; IX congresso SIHTA, Ottobre 2016
3 Ferrara F.M., Cicchetti A., "I sistemi informativi e l'Health Technology Assessment", Progettare per la Sanità, Nov. 2016
4 Ferrara F.M., Pillon S. "Medicina Digitale – Sicurezza per il medico e per il paziente", Progettare per la Sanità, Sett. 2016

assistenziale e di cura. Sempre di più, infatti, le prestazioni erogate in ambito ospedaliero sono basate su un impiego intensivo di apparecchiature e dispositivi medici connessi con il sistema (IDC stima che entro il 2020 il 16% dei dati sanitari sarà proveniente da dispositivi medici, inclusi gli scenari di IoT).

Il contesto del sistema informativo si amplia quindi fino ad includere dispositivi medici, e **la sicurezza complessiva dipende sempre di più dalla sicurezza del binomio "sistema informativo + dispositivi connessi"**, come schematizzato nella seguente figura.



Per raccogliere informazioni oggettive e misurabili della realtà attuale su cui basare il modello, è stata condotta una indagine sul contesto dei sistemi informativi collegati con i dispositivi medici nelle aziende sanitarie italiane a cui hanno partecipato 112 ospedali.

Lo studio è collegato e sinergico alla parallela iniziativa (www.gdpr-sanita.it), promossa da ALTEMS e HIMSS Italian Community con la partecipazione di tutte le associazioni sanitarie, per la definizione di un codice di condotta per la protezione dei dati personali in sanità, secondo quanto previsto dall'Articolo 40 del GDPR.

Indice

1. L'esigenza di un approccio multi-dimensionale alla sicurezza nei sistemi informativi sanitari

E' ormai ampiamente riconosciuto che in una azienda sanitaria moderna il sistema informativo non può essere un semplice insieme di tecnologie e programmi software più o meno correlati fra loro, ma deve rappresentare uno strumento completo ed integrato per il governo della struttura, sia dal punto di vista della gestione corrente che sotto il profilo della strategia evolutiva, assicurando la continuità dei processi aziendali attraverso i diversi settori e l'integrazione e la disponibilità del patrimonio informativo sotto il profilo sia clinico che amministrativo. E questo sia all'interno dell'azienda che nel contesto della rete territoriale per la continuità del percorso assistenziale del paziente.

In una tale visione, una valenza particolare assume ovviamente la gestione della "sicurezza" (includendo in questo termine anche gli aspetti di protezione dei dati personali, secondo quanto prescritto dal recente Regolamento UE 2016/679), che va intesa non solo dal punto di vista prettamente tecnologico, ma in quadro più ampio, tale da garantire l'esecuzione sicura e corretta dei processi aziendali, minimizzando e prevenendo –per quanto possibile– tutti i rischi ai quali l'azienda può essere esposta. Rischi che –nel settore sanitario– assumono una rilevanza particolare in quanto possono avere implicazioni anche sulla stessa salute del paziente.

Il Regolamento europeo per la protezione dei dati personali

Nel rispetto dei principi generali definiti nel regolamento **le singole organizzazioni devono definire, implementare e gestire un proprio sistema organico di**

- strutture organizzative
- procedure operative
- soluzioni tecniche
- documentazione

per la gestione, la sicurezza e la protezione dei dati personali

Obblighi del titolare

- **Organicità** dell'approccio (organizzazione, progettazione, tecnologia)
- **Riesami periodici ed aggiornamento**
- **Sicurezza** dell'utilizzo effettuato
- **Responsabilizzazione**
- **Evidenza** delle azioni effettuate per il rispetto del regolamento

La stessa norma ISO/IEC 27001 –inizialmente nata con un focus principalmente tecnologico– nelle sue più recenti versioni si è ampliata verso un approccio olistico di "sicurezza totale", che abbracci l'analisi e per quanto possibile la prevenzione di tutti i rischi aziendali. Sul sito ISO la norma viene infatti testualmente definita come "*requirements for an Information Security Management System (ISMS): a systematic*

approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process".

Anche per quanto riguarda il profilo normativo, vale la pena di sottolineare come il Regolamento UE sulla protezione dei dati personali definisca principi e regole di ampio respiro, non circoscrivibili a singole attività o procedure ma di rilevanza per tutte le attività dell'organizzazione. Il loro rispetto nell'ambito del sistema informativo, pertanto, richiede un approccio organico ed integrato che tenga conto di tutti gli aspetti in tutti i settori: dall'organizzazione dei dati, alle funzionalità, alle tecnologie.

In questa visione maggiormente strategica, anche le caratteristiche funzionali ed informative del sistema informativo costituiscono quindi elementi fondamentali e qualificanti ai fini della sicurezza e della gestione del rischio nell'azienda sanitaria.

In estrema sintesi l'obiettivo finale di un "sistema informativo sicuro" può essere individuato nella capacità di seguire e supportare senza soluzione di continuità i processi dell'organizzazione (sia quelli che si esauriscono all'interno di un singolo settore che – soprattutto– quelli che si articolano attraverso settori diversi) e di rendere disponibili tutte le informazioni di potenziale rilevanza nei tempi e nei modi appropriati per le diverse esigenze. Includendo in questo scenario di completezza informativa non solo il rendere disponibili "passivamente" tutte le informazioni sul paziente, indipendentemente dal momento e dal settore in cui tali informazioni sono state raccolte, ma anche la capacità di svolgere un ruolo proattivo nei confronti dell'utente, evidenziando autonomamente situazioni di potenziale rischio grazie alla correlazione delle informazioni stesse, sia sulla base di regole e criteri già in uso nella pratica clinica (es- co-morbilità) che in base a più complessi algoritmi di knowledge discovery e business intelligence applicati alla medicina.

Il tutto secondo i ruoli e le abilitazioni dei vari utenti nel rispetto delle normative legate alla particolare natura dei dati trattati, coniugate con la necessità di poter gestire tempestivamente situazioni critiche e di emergenza.

In un tale scenario, la gestione della sicurezza nei sistemi informativi e la definizione di strategie evolutive che tengano conto sia delle possibilità connesse a nuovi modelli organizzativi, a nuovi protocolli clinici e a nuove tecnologie (e dei rischi connessi), sia delle normative sempre più precise e stringenti si deve necessariamente basare su un approccio multi-dimensionale.

A questo scopo, la "tradizionale" analisi degli aspetti del sistema informativo in termini organizzativi, informativi, funzionali e tecnologici[5] può essere coniugata ed integrata con le prospettive proprie dell'approccio dall' Health Technology Assessment[6,7], quali il rischio

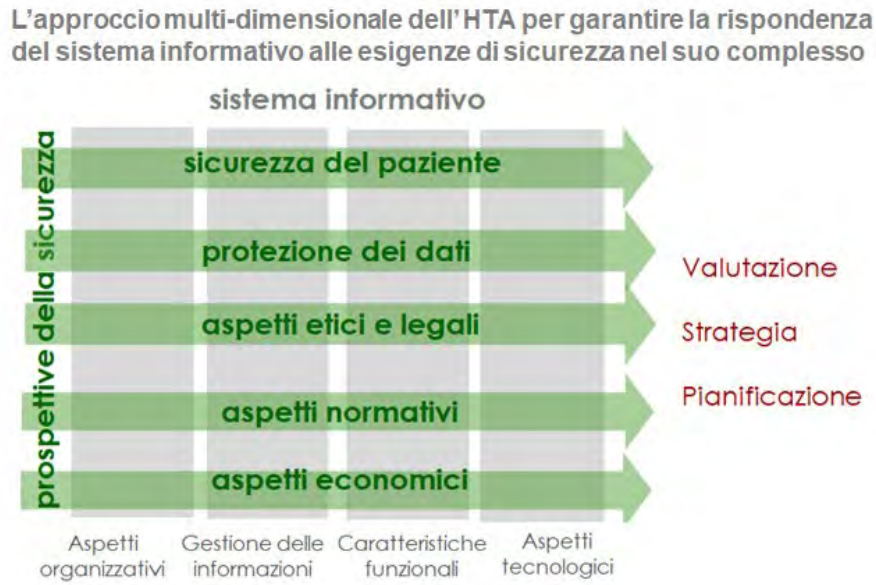
[5] ISO/IEC 10746 "Information Technology - Open distributed processing – Reference model"
[6] Ferrara, "ICT e HTA: il ruolo dell'HTA nella valutazione dei sistemi informativi sanitari"; IX congresso SIHTA, Ottobre 2016
[7] Ferrara F.M., Cicchetti A., "I sistemi informativi e l'Health Technology Assessment", Progettare per la Sanità, Novembre 2016

clinico[8], l'impatto sul paziente, l'aspetto economico, le implicazioni etiche, la rispondenza alle normative, etc.

Seguendo questo approccio, per disporre di termini di riferimento di validità generale, tali da rendere possibile anche la classificazione ed il confronto secondo criteri omogenei, ci si può basare su due prospettive:

- le caratteristiche dei sistemi, descritte - secondo metodologie e standard propri dell'ICT - in modo da evidenziarne i vari aspetti in termini di organizzazione, struttura ed operatività, indipendentemente dagli specifici prodotti adottati nei diversi contesti;

- i requisiti di sicurezza nella sua accezione complessiva, articolati secondo le diverse prospettive suggerite dall'HTA, in modo da classificare le varie tipologie di rischio in funzione delle tipologie di conseguenze, dal punto di vista clinico, legale ed economico.



Con questi criteri, fra il 2016 e l'inizio del 2017, il "Laboratorio ALTEMS sui sistemi informatici Sanitari" ha condotto uno studio ed una indagine a livello nazionale - cui hanno contribuito 46 aziende sanitarie e 113 presidi ospedalieri - ("***his*SA**: health information systems Security Assessment"[9]) mediante il quale:

[8] Ferrara F.M., Pillon S. "Medicina Digitale – Sicurezza per il medico e per il paziente", Progettare per la Sanità, Settembre 2016

[9] http://altems.unicatt.it/altems-i-sistemi-informativi-sanitari-per-il-governo-dell-organizzazione-analisi-della-sicurezza

- È stata ottenuta una "fotografia" omogenea delle caratteristiche dei sistemi informativi delle aziende sanitarie italiane, rilevanti ai fini della sicurezza, intesa in questa sua accezione "totale" del termine;

- È stata individuare una metodologia per l'analisi ed un modello di classificazione dei sistemi informativi secondo "livelli di sicurezza", basati su un approccio olistico e su indicatori misurabili, indipendenti dalle specifiche soluzioni tecnologiche adottate.

La metodologia ***his*SA** fornisce un modello di validità generale, basato su un insieme di indicatori essenziali sulla struttura del sistema informativo sanitario.

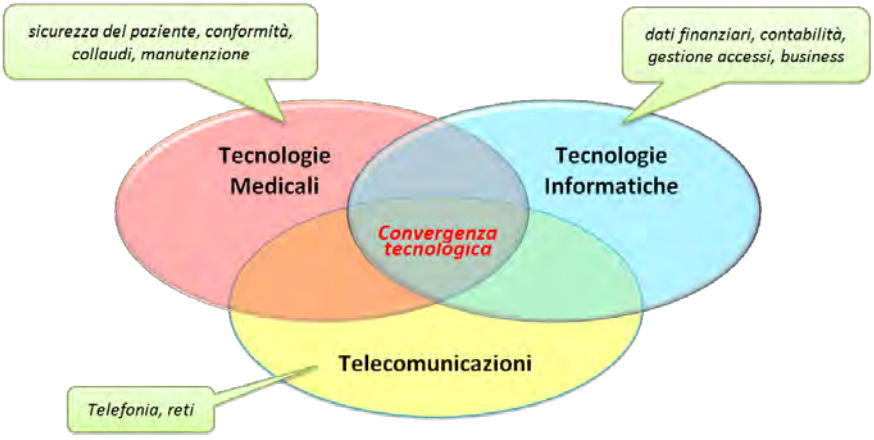
Partendo da tale quadro di riferimento generale, questo studio approfondisce e dettaglia l'analisi ed il modello complessivo della sicurezza, prendendo in considerazione gli aspetti inerenti all'integrazione e l'interazione dei dispositivi medici, come evidenziato nella seguente figura.

2. I dispositivi medici nel contesto del sistema informativo sanitario

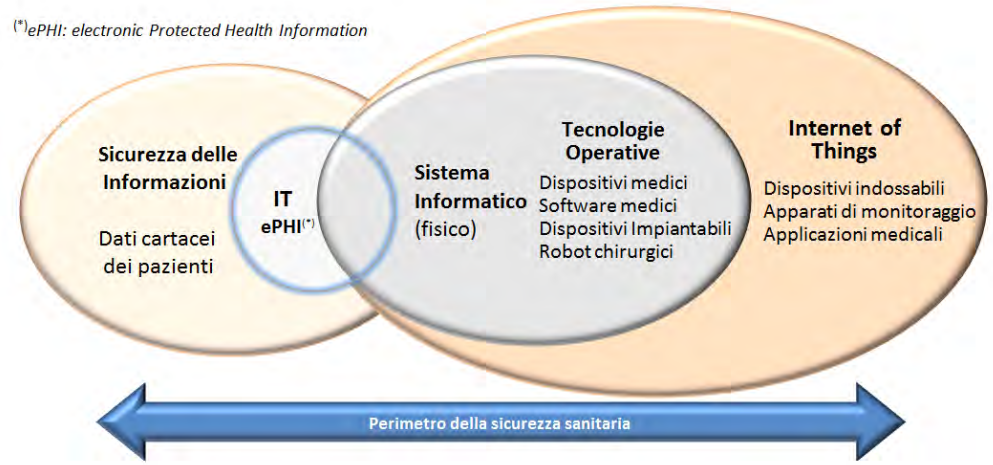
2.1 La sicurezza dei dispositivi medici nelle organizzazioni sanitarie

La sicurezza delle cure è uno degli obiettivi prioritari che il nostro Servizio Sanitario Nazionale si pone. Lo sviluppo di interventi efficaci è strettamente correlato all'individuazione e alla comprensione delle criticità dell'organizzazione e richiede una cultura radicata che consenta di superare le barriere per l'attuazione di misure organizzative e di comportamento volti a preservare il profilo di sicurezza delle tecnologie utilizzate nei processi di diagnosi e cura. La sicurezza dei pazienti, quindi, si colloca nella prospettiva di un complessivo miglioramento della qualità e, poiché dipende dall'interazione delle molteplici componenti che agiscono nel sistema, deve essere affrontata attraverso l'adozione di pratiche di governo clinico. Tali procedure hanno lo scopo di porre al centro della programmazione e gestione dei servizi sanitari i bisogni dei cittadini, valorizzando nel contempo il ruolo e la responsabilità di tutte le figure professionali che operano in sanità. Conseguentemente, il profilo di sicurezza di un dispositivo medico non dipende esclusivamente dalla sicurezza intrinseca del dispositivo, garantita dal rilascio del marchio CE, ma è assicurato anche da un utilizzo clinico appropriato e dall'impiego in un contesto organizzativo capace di garantirne la sicurezza.

Nella realtà operativa del settore sanitario, i tradizionali perimetri dell'Information Technology (*IT*) e della Ingegneria Clinica (*CE*) sono fortemente collegati tramite reti condivise; questo espone entrambi domini a interazioni con le conseguenti problematiche di sicurezza informatica in un contesto reso ancor più complesso dalla scarsa comunicazione tra ciascuno dei soggetti, direttamente o indirettamente coinvolti nelle attività. Le cause sono da ricercare nelle vulnerabilità della sicurezza, nella frequente obsolescenza tecnologica ma soprattutto nella gestione inadeguata dei dispositivi.



I dispositivi medici una volta erano apparecchiature isolate e non collegate in rete, al limite dotate di monitoraggio diagnostico unidirezionale con accesso locale e riservato al solo fornitore; oggi le apparecchiature sono completamente connesse in rete con comunicazioni bidirezionali, accesso da remoto, connettività wireless e software di gestione complesso, analogo a quello di un qualsiasi sistema di elaborazione. In pratica, si è realizzata la transizione al *Software come Dispositivo Medico (SaMD)*



In questo contesto strettamente integrato ed interconnesso, la quasi totalità delle prestazioni assistenziali che sono garantite in ambito ospedaliero sono basate su un impiego intensivo di apparecchiature e dispositivi medici, il cui grado di efficienza e di efficacia può quindi influenzare, direttamente ed indirettamente sia la qualità del servizio erogato che la sicurezza del paziente e degli operatori.

Al fine di garantire standard di sicurezza uniformi ed adeguati, occorre applicare rigorosamente una metodologia di "valutazione del rischio" (introdotta per la prima volta dal D. Lgs. 626/94) e quindi stimare, per ogni singola tecnologia, il reale scostamento dai "requisiti essenziali" di sicurezza indicati nella normativa vigente. Tale procedura permette di stabilire la corretta priorità degli interventi finalizzati alla riduzione ed al contenimento del rischio entro la soglia di accettabilità.

Nel suo complesso, la sicurezza connessa con l'uso del dispositivo medico deve - innanzi tutto- essere **correlata al controllo del rischio per il paziente**, classificabile in cinque livelli:

Trascurabile: disagio o disagio temporaneo

Minore:	lesioni o menomazioni temporanee che non richiedono un intervento medico
Grave:	risultati in lesioni o menomazioni che richiedono un intervento medico professionale
Critico:	risultati in menomazione permanente o lesioni mortali
Catastrofico:	risultati nella morte del paziente

Questi livelli di rischio rappresentano il termine di riferimento ultimo ai quali relazionare i vari aspetti della sicurezza, considerati nel loro insieme e tenendo conto che l'affidabilità di un sistema complesso è determinata dall'affidabilità del componente più debole.

2.2 L'avvento dell'ICT e l'importanza di garantire la sicurezza dei dati clinici

L'attuale evoluzione tecnologica ha permesso di collegare tra loro due mondi che fino a qualche anno fa risultavano essere sconnessi tra loro e poco comunicanti, quello relativo ai dispositivi medici e quello dell'ICT relativo alla sicurezza informatica. Un dispositivo medico potrebbe essere considerato come un "insieme di apparecchiature componenti", che possono essere integrati in un "sistema a rete" con altri dispositivi, sistemi di calcolo, di archiviazione e di recupero dell'informazione. Questa evoluzione ha portato le organizzazioni sanitarie a un miglioramento nel processo e nel trattamento dei dati in termini di tempo (es. archiviare un referto), spazio (es. ottimizzazione degli spazi di archiviazione delle cartelle cliniche) e, almeno in parte, anche in termini economici. Conseguentemente, non è più possibile non considerare come fondamentale, viste le enormi quantità di dati clinici e sanitari che gestiscono i sistemi sanitari, il punto di vista della sicurezza informatica.

L'utilizzo dell'ICT influisce in modo significativo sugli obiettivi e sulle relative sfide e opportunità di un'organizzazione sanitaria. In particolare l'utilizzo dei dispositivi in rete potrebbe comportare:

- *un miglioramento della diagnostica e delle procedure chirurgiche*: l'ICT non consente solo nuovi metodi di trattamento ma potrebbero anche migliorare le procedure esistenti

- *una migliore la gestione del percorso del paziente*: un'assistenza sanitaria e un percorso del paziente efficiente possono diminuire i tempi di attesa e la durata delle degenze ospedaliere, ridurre gli errori, aumentare i ricavi e la soddisfazione del paziente. In particolare, la disponibilità di informazioni relative al paziente in tutte le fasi del percorso diagnostico terapeutico potrebbero ottimizzare l'ammissione, la programmazione delle singole procedure e la dimissione definendo un percorso senza soluzione di continuità.

- *uno sviluppo dell'assistenza medica remota*: uno degli obiettivi principali dell'introduzione di dispositivi IoT nel contesto dell'assistenza sanitaria è la capacità di estendere il monitoraggio dei pazienti oltre i confini dell'ospedale e fornire assistenza medica remota. Diversi dispositivi medici, ad es. dispositivi impiantabili, dispositivi indossabili e altri dispositivi mobili introducono la capacità di eseguire in tempo reale un monitoraggio del paziente attraverso la misurazione dei parametri vitali e rendono queste misurazioni facilmente disponibili al personale ospedaliero tramite una connessione di rete. Quindi, l'ammissione del paziente in ospedale può essere limitata a quei casi ritenuti necessari, con conseguente riduzione dei costi dell'assistenza.

- *maggiore sicurezza dei pazienti*: se utilizzati correttamente, i dispositivi medici che raccolgono dati relativi ai parametri vitali del paziente, all'assunzione di farmaci o al monitoraggio del funzionamento delle tecnologie salvavita possono portare ad aumentare la sicurezza del paziente se sono collegati e in grado di fornire alert tempestivi.

D'altra parte, la mancanza di idonei strumenti di protezione della rete dei dati ospedalieri può portare non solo al danneggiamento della tecnologia e di conseguenza dei pazienti, ma anche rendere la rete stessa facile preda di hackers malintenzionati che, ad esempio con malware come Crypto-locker e affini, nel peggiore dei casi potrebbero recuperare illegalmente dati personali e sensibili.

Tale necessità è ulteriormente enfatizzata dal diffondersi della telemedicina, quindi i "nuovi pericoli" sono sostanzialmente legati all'introduzione progressiva di sistemi di elaborazione automatizzata di grandi quantità di informazioni connesse a parametri biomedici. La componente informatica è divenuta uno degli elementi dominanti, a discapito delle "classiche" componenti meccaniche, elettromeccaniche ed elettroniche. È, quindi, in fortissima crescita il numero di tecnologie la cui affidabilità dipende principalmente dal corretto funzionamento dei relativi software sia che sovrintendano al funzionamento dell'apparecchiatura o che siano deputati alla presentazione e controllo dei parametri biologici/biofisici. Le situazioni di pericolo che si vengono così a creare sono rese ancor più "subdole" dal fatto che, in molti casi, trattasi di rischio di tipo "indiretto": si provoca un errore diagnostico-terapeutico sul paziente non dovuto direttamente ad imprecisione medico-assistenziale ma al malfunzionamento della tecnologia oppure a causa di un suo utilizzo scorretto. È quindi fondamentale e auspicabile che gli enti si tutelino con misure di sicurezza adeguate per proteggere capitale, tecnologia e conoscenza, in particolar modo i sistemi e i servizi che trattano dati sensibili, attraverso investimenti sulla messa in sicurezza della rete informatica e dei dispositivi medici che producono questi dati ed informazioni. Lo scopo è quello di ottenere un elevato grado di protezione da attacchi esterni e garantire così la continuità operativa della struttura. È necessario, inoltre, che questo grado di protezione sia periodicamente verificato attraverso un'analisi del rischio che produca parametri oggettivi per la valutazione di tutti i sistemi, servizi e le apparecchiature collegate alla rete IT-medicale. Esistono, infine, diversi problemi di riservatezza delle informazioni trasmesse e di definizione dei profili di responsabilità dei vari attori coinvolti nel processo.

2.3 I rischi per il paziente in caso di vulnerabilità di cybersecurity

Come precedentemente argomentato, le strutture sanitarie sono delle strutture complesse che erogano prestazioni strettamente correlate ad una vasta gamma di dispositivi medici e per i quali deve essere garantito un livello di sicurezza molto elevato.

L'evoluzione tecnologica dei dispositivi medici cresce ad un tasso molto elevato, per tale motivo non è possibile mitigare completamente i rischi informatici (Cybersecurity) attraverso dei soli controlli pre-marketing. In ambito ospedaliero, i programmi di gestione del rischio legati alla sicurezza informatica dovrebbero enfatizzare le vulnerabilità che potrebbero consentire l'accesso non autorizzato, la modifica, l'uso improprio di informazioni archiviate, consultate o trasferite da un dispositivo medico a un altro in rete con il primo, minacciando la sicurezza del paziente. Il mantenimento del profilo di sicurezza può essere attuato tramite un monitoraggio che permetta l'identificazione e il rilevamento delle vulnerabilità e dei rischi della cybersicurezza sia intrinsechi del dispositivo che provenienti dall'esterno.

Dal punto di vista del paziente il rischio associato all'utilizzo di dispositivi medici in rete è correlato

- all'esportabilità delle vulnerabilità di cybersecurity
- alla gravità del danno del paziente se la vulnerabilità dovesse essere sfruttata.

Per condurre una valutazione del rischio di cyber-vulnerabilità è necessario comprendere se il rischio di danno al paziente è controllato (accettabile) o incontrollato (inaccettabile). Un metodo di valutare l'accettabilità del rischio comporta l'uso di una matrice con combinazioni di "sfruttabilità" e "gravità del danno provocato al paziente" in modo da determinare se il rischio di danno al paziente è controllato o incontrollato. Il problema è legato ai rischi che rimangono incontrollati, poiché in questi casi è necessario implementare ulteriori interventi correttivi.

Valutazione del rischio per i pazienti

2.4 I dispositivi medici in rete nelle organizzazioni sanitarie

Ci sono molteplici problematiche legate all'impiego di tecnologie trasmissive e alla gestione ed utilizzo della telemedicina con riferimento al corretto impiego delle strumentazioni, alla loro installazione ed ai requisiti impiantistici dell'ambiente in cui vengono collocate, al fine di garantire disponibilità, continuità e qualità del servizio nonché la correttezza delle informazioni trasmesse e la tempestività delle stesse in caso di emergenza sanitaria. Dall'analisi di tali problematiche si evince la necessità di poter definire dei criteri per la classificazione delle tecnologie che ICT che sono utilizzate nei contesti sanitari al fine di rendere più semplice e standardizzata la loro individuazione. In letteratura, l'unica classificazione dei dispositivi medici in rete è stata strutturata dell'ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione), che li ha classificati in base all'impatto causato dall'interruzione del servizio.

Tale criterio permette di classificare i dispositivi medici come segue.

Remote care system asset

comprendono tutte quelle tecnologie che possono fornire servizi sanitari ai pazienti in località remote (ad esempio a casa) come (i) le apparecchiature mediche impiantabili o indossabili per il tele-monitoraggio e la telediagnosi (es misuratore della pressione sanguigna, della frequenza cardiaca, sistemi per la misurazione del glucosio, elettrocardiografo e altri sistemi per la misurazione dei parametri fisiologici a distanza); (ii) attrezzature mediche per la distribuzione di farmaci (apparecchiature automatiche di dosaggio); (iii) apparecchiature per la telemedicina.

Networked medical device

includono (i) i dispositivi mobili (ad esempio dispositivi di misurazione del glucosio); (ii) dispositivi esterni indossabili (ad esempio pompe per insulina portatili, contatori di temperatura wireless); (iii) dispositivi impiantabili (ad esempio pacemaker cardiaci); (iv) dispositivi fissi (ad esempio scanner per tomografia computerizzata (CT), macchine di supporto vitale, stazioni di distribuzione di farmaci chemioterapici); (v) dispositivi di supporto (ad esempio robot assistiti).

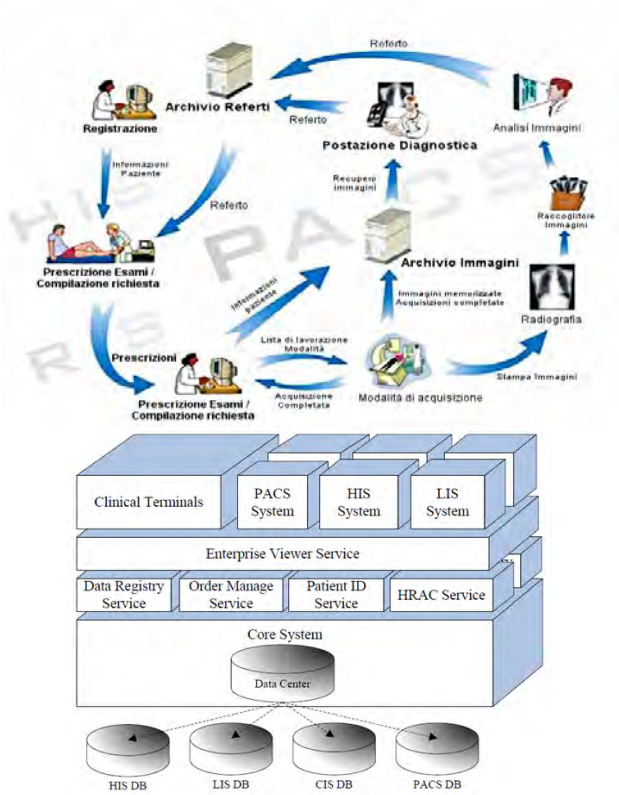
Identification systems

sono utilizzati per tracciare e autenticare pazienti, personale o attrezzature ospedaliere come ad esempio (i) i sistemi di identificazione come tag, braccialetti, etichette e badge intelligenti e (ii) scanner biometrici.

Interconnected clinical information systems

includono tutti i sistemi di informazione degli ospedali come (i) i sistemi di informazione ospedaliera (HIS); (ii) i sistemi di informazione di laboratorio (LIS); (iii) i sistemi di informazione radiologica (RIS); (iv) il sistema di informazioni sulla farmacia (PIS); (v) sistema di informazione sulla patologia;

(vi) il sistema della banca del sangue; (vii) il sistema di archiviazione e comunicazione di immagini (PACS); e (viii) il sistema informativo di ricerca.



La problematica legata alla definizione di criteri oggettivi e riproducibili atti a classificare i dispositivi medici in rete sulla base dei rischi informatici, risiede soprattutto nella molteplicità di tecnologie che ricadono in tale definizione. Inoltre, l'individuazione di tali tecnologie è contesto dipendente dal grado di informatizzazione della struttura sanitaria considerata.

La necessità di definire dei criteri di conseguenza risulta essere una sfida per il livello centrale in modo da poter definire degli interventi correttivi a seconda della tecnologia.

2.5 Classificazione dei dispositivi

Ai fini di questo studio sono prese in considerazione le **apparecchiature elettroniche digitali e connesse (Dispositivi Medici Attivi)**, dotate di elettronica interna di memorizzazione e di elaborazione, interfacce di acquisizione e/o di attuazione nonché canali di comunicazione verso l'esterno che consentono loro di interagire fisicamente e/o trasferire informazioni con l'ambiente (informatico) in cui essi operano, con il paziente e con gli operatori sanitari.

Dal punto di vista del loro posizionamento nell'ambito della struttura e del loro ruolo nel corso dei processi clinico-assistenziali, i dispositivi medici sono stati classificati secondo tre gruppi, in relazione alle modalità di uso e di gestione nel contesto del sistema informativo:

- "**individuale**", si intendono quelle apparecchiature di basso costo, utilizzabili individualmente da parte del paziente (all'esterno o all'interno del centro) e/o da personale sanitario nell'ambito dell'attività clinica e/o assistenziale per la rilevazione di parametri (es. strumenti commerciali, ECG ed altra strumentazione portatile, misuratori portatili di valori ematici, etc.).

- "**condiviso**", si intendono quelle apparecchiature di costo contenuto, in dotazione all'interno di una specifica UO della struttura per la misurazione di parametri vitali e/o l'effettuazione di esami diagnostici complementari alle attività cliniche della struttura stessa (es. ecografi, flussimetri, ecc.). Operano autonomamente (collegate o meno con il sistema sanitario centrale dell'organizzazione) e non necessitano di sistemi informatici articolati e complessi per il loro controllo.

- "**centralizzato**", si intendono le apparecchiature di alto costo e complessità, collegate con e controllate da sistemi informatici complessi e dedicati (cosiddetta diagnostica "pesante", apparecchiature di laboratorio, robot chirurgici, ecc.) stabilmente installate all'interno di UO della struttura, e costituenti strumenti essenziali e critici per l'effettuazione delle attività della UO stessa. Oltre che per il loro numero relativamente ridotto, per motivi di costo, complessità e rilevanza clinico/organizzativa, queste apparecchiature "centralizzate" sono usualmente acquisite, installate e gestite nell'ambito di processi e procedure formalizzate, valide per tutta la struttura.

3. Survey sulla gestione degli aspetti di sicurezza nelle aziende sanitarie

3.1 Obiettivi dell'indagine

Secondo questo approccio, è stata compiuta una indagine sui contesti dei sistemi informativi e dei dispositivi medici nelle aziende sanitarie italiane, con tre obiettivi;

a) ottenere una fotografia delle caratteristiche qualificanti dei vari contesti sotto il profilo organizzativo, informativo, funzionale e tecnologico, secondo criteri omogenei, indipendenti soluzioni di mercato adottate e tali quindi da poter essere condivisi quali termini di riferimento comuni;

b) dettagliare, anche sulla base dei contributi ricevuti mediante i questionari compilati, un insieme di indicatori -puntuali e misurabili- circa alcune caratteristiche del binomio "sistema informativo + dispositivo medico" di particolare rilevanza ai fini della sicurezza e, più in generale, della qualità del supporto informatico disponibile alle attività cliniche ed assistenziali.

b) proporre, sulla base degli indicatori, un "modello di maturità" mediante il quale descrivere e classificare il livello di sicurezza complessivo per gli aspetti inerenti ai dispositivi medici integrati con il sistema informativo.

Lo studio è stato condotto mediante un questionario sulla organizzazione delle aziende e sulle caratteristiche dei sistemi informativi sanitari che è stato diffuso fra le strutture sanitarie -pubbliche e private- di tutte le regioni italiane.

Per ogni argomento, il questionario prevedeva sia risposte chiuse che la possibilità di commenti e descrizioni aggiuntive, considerate dall'interlocutore utili per circostanziare meglio i singoli argomenti.

Grazie a tali contributi aggiuntivi, le caratteristiche inizialmente individuate sono state migliorate e dettagliate, consentendo la definizione degli indicatori e della struttura metodologica descritti nel seguito.

Vale sottolineare come le caratteristiche, correlate con le normative e con i fattori di rischio, **siano state espresse mediante indicatori indipendenti da specifiche soluzioni tecnologiche e/o di mercato**, in modo fornire un riferimento omogeneo e di validità generale.

Il questionario è stato implementato via web[10] per essere compilabile on-line, ed è stato è stato diffuso nel periodo agosto-ottobre 2018 ad ospedali ed aziende sanitarie in tutto il territorio nazionale, -sensibilizzate all'iniziativa anche mediante contatti diretti ed iniziative di promozione e informazione condotte in collaborazione con associazioni professionali e scientifiche- in modo da raccogliere

[10] sul sito https://www.surveygizmo.com/s3/4454990/indagine-sugli-aspetti-della-sicurezza-nel-contesto-di-un-sistema-informativo-sanitario-integrato-con-dispositivi-medici

un significativo campione di scenari sulla base del quale costruire il modello di riferimento e di maturità della sicurezza.

3.2 Struttura del questionario

Per individuare dei termini di riferimento di validità generale indipendentemente da specifiche soluzioni tecnologiche ed in grado quindi descrivere in modo omogeneo le diverse realtà sono stati individuati alcuni indicatori in grado di parte l'individuazione di termini di riferimento omogenei è indispensabile per disporre di criteri di validità generale secondo i quali descrivere e confrontare i diversi scenari ad un livello concettuale indipendente da specifiche soluzioni implementative, ma al tempo stesso completo e non ambiguo in termini di requisiti e caratteristiche.

Per far ciò l'approccio seguito si è basato su alcune linee-guida di riferimento largamente diffuse:

a) ISO-ODP "Open distributed processing" che suggerisce l'adozione di quattro prospettive complementari, ma individualmente autonome ed auto-consistenti, per la descrizione del sistema: gli aspetti organizzativi, informativi, funzionali e tecnologici

b) ISO 12967 "Health Informatics System Architecture", che -in accordo con questo riferimento metodologico-, propone un approccio incrementale di specifica ed un modello di riferimento, per quanto riguarda l'integrazione delle informazioni e la formalizzazione dei processi.

c) ISO-27001, la norma di riferimento per la sicurezza informatica, che nelle più recenti versioni si è ampliata verso un approccio di "sicurezza totale", per fornire un quadro metodologico complessivo, tale da abbracciare l'analisi la gestione e, per quanto possibile la prevenzione, di tutti i fattori di rischio.

d) Il Regolamento Europeo sulla protezione dei dati personali.

Traendo spunto da queste linee guida, sono state individuate alcune caratteristiche del sistema informativo di possibile rilevanza ai fini della sicurezza, articolate secondo tre prospettive:

a) prospettiva organizzativa
Analizza le caratteristiche secondo cui è organizzata l'azienda in relazione alla gestione della sicurezza collegata con le funzionalità la gestione e l'evoluzione del sistema informativo.

c) prospettiva implementativa, sotto i profili informativo e funzionale

Analizza le caratteristiche del sistema informativo in termini di struttura ed operatività in termini di gestione delle informazioni e di funzionalità attualmente implementate nel supporto ai principali processi organizzativi ed assistenziali.

c) prospettiva tecnologica
Analizza le caratteristiche del sistema informativo in termini di caratteristiche dell'infrastruttura tecnologica.

Nell'ambito di ognuna di queste prospettive sono individuate alcune caratteristiche di particolare rilevanza ai fini della prevenzione e gestione dei rischi e della sicurezza, come schematizzato nella seguente figura.

3.3 Composizione e significatività del campione

Hanno risposto al questionario **36 aziende sanitarie** corrispondenti ad un totale di **112 presidi ospedalieri** (ed altrettanti sistemi informativi).

Per ogni ospedale partecipante all'indagine sono state raccolte 156 informazioni sui vari aspetti della organizzazione e delle caratteristiche del sistema informativo, ripartiti come segue:

- Caratteristiche di contesto 36

- Aspetti organizzativi 49
- Aspetti informativi 21
- Aspetti funzionali 20
- Aspetti tecnologici 30

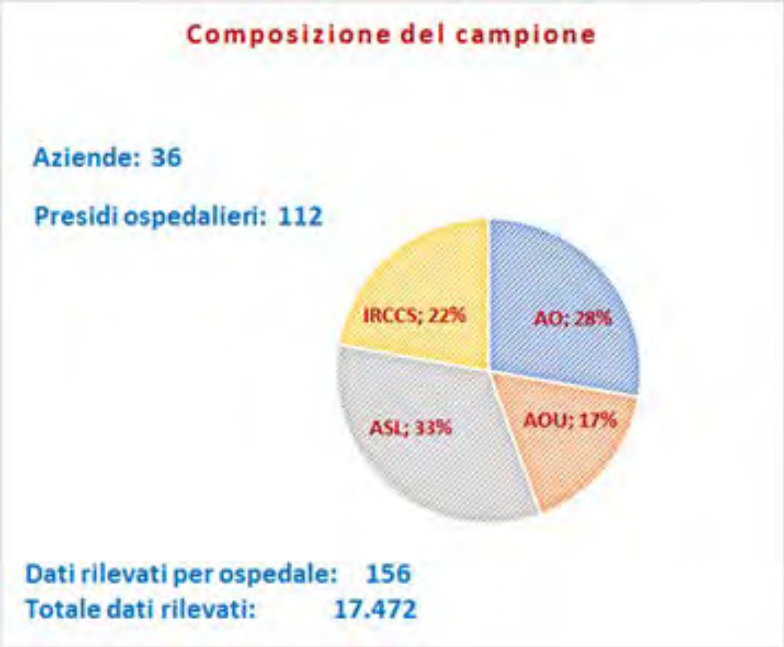
Considerati i 112 presidi ospedalieri che hanno partecipato all'indagine, **il volume totale delle informazioni raccolte** e sulle quali si è basato lo studio e la definizione del modello **è pari a 17.462** dati.

I seguenti grafici riportano la composizione del campione rilevato, in termini di tipologia di aziende, di distribuzione geografica e di volumi di attività.

Sulla base del volume di dati raccolti e della articolazione delle tipologie di aziende partecipanti, il campione rappresenta uno scenario significativo ai fini della validità degli indicatori definiti e del modello di maturità della sicurezza dei dispositivi medici nel contesto dei sistemi informativi delle aziende sanitarie italiane.

Composizione del campione

Come evidenziato nel grafico, il campione censito comprende tutte le tipologie di aziende sanitarie.

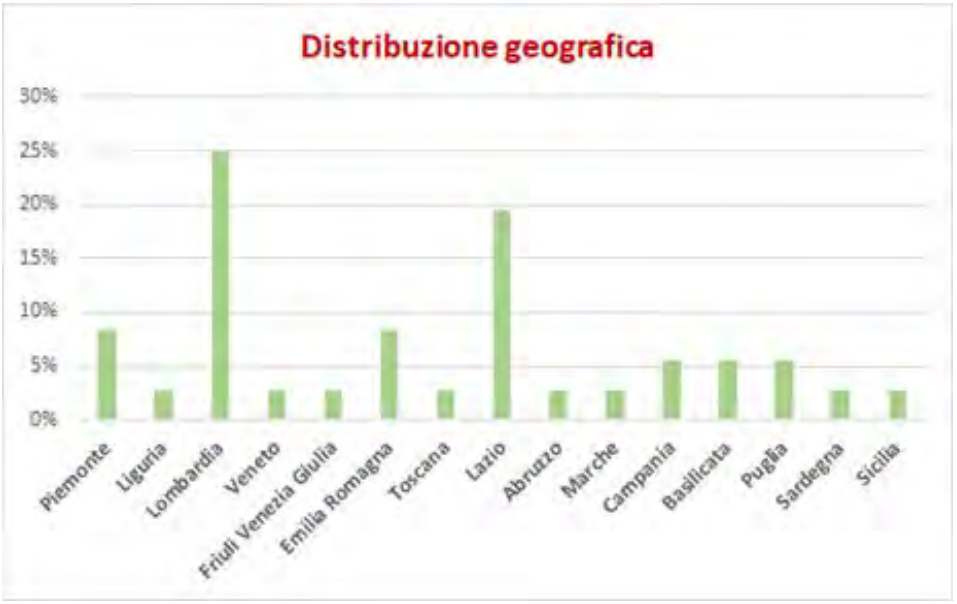


Volume di attività

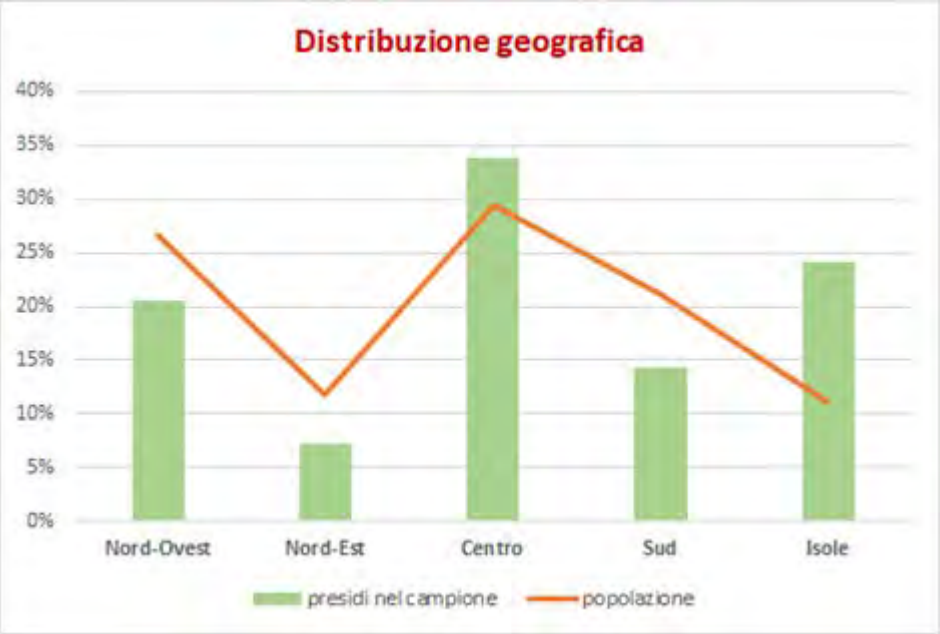
I volumi di attività delle aziende censite dimostrano la significatività del campione dal punto di vista delle diverse dimensioni delle strutture.

Distribuzione geografica

La distribuzione geografica del campione copre le diverse realtà regionali.



Nel seguente grafico viene evidenziata la correlazione fra il campione e la popolazione di riferimento rispetto al totale nazionale nelle diverse aree geografiche.

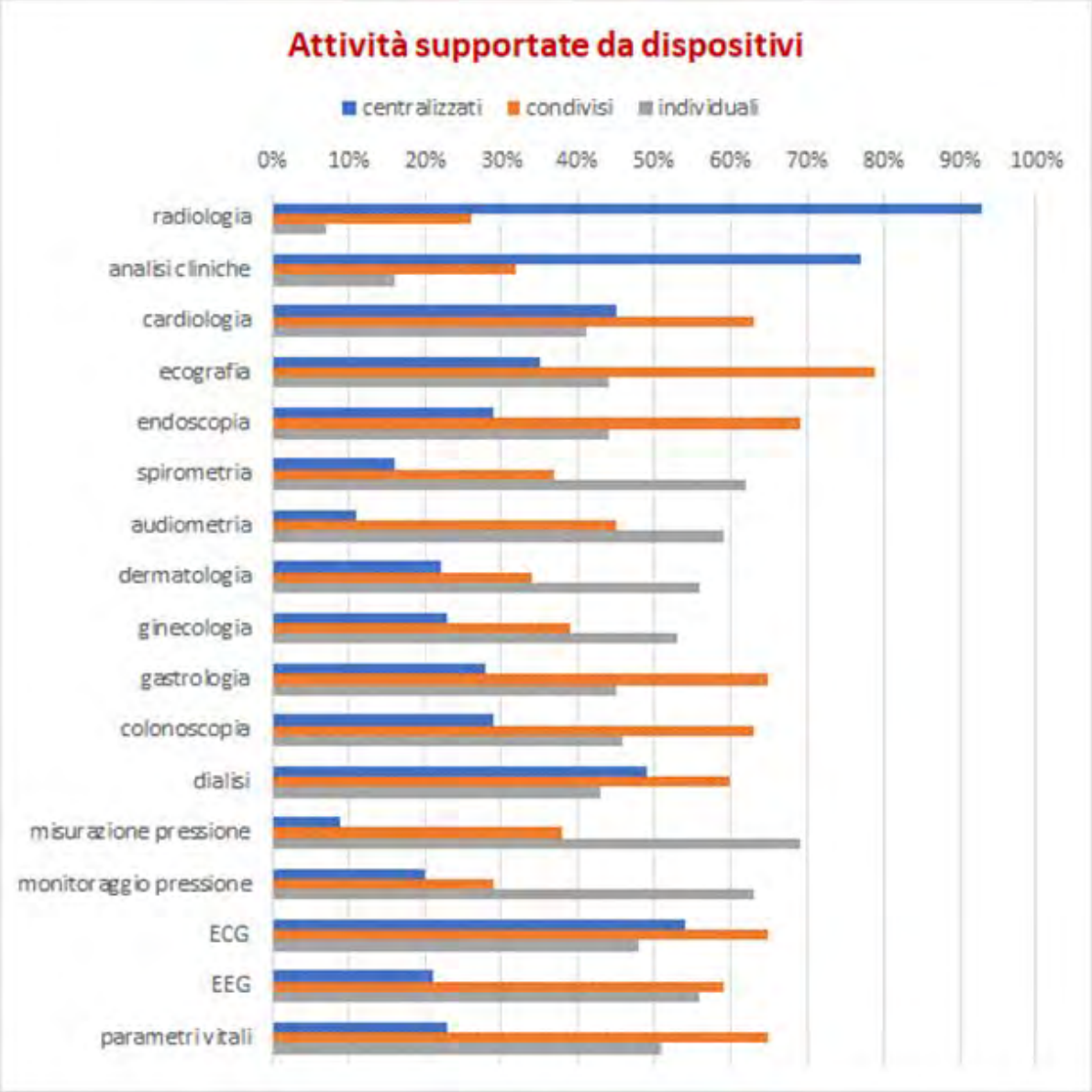


3.4 Contesti operativi

In questa sezione sono analizzati i contesti operativi delle varie strutture, in termini di tipologia di attività clinico-assistenziali che sono eseguite con il supporto di dispositivi medici.

3.4.1 Principali attività eseguite con l'uso di dispositivi

Il seguente prospetto elenca le principali attività clinico-assistenziali effettuate con il supporto di dispositivi, classificati secondo le tre categorie definite.



3.4.2 Livello di diffusione dei dispositivi condivisi ed individuali

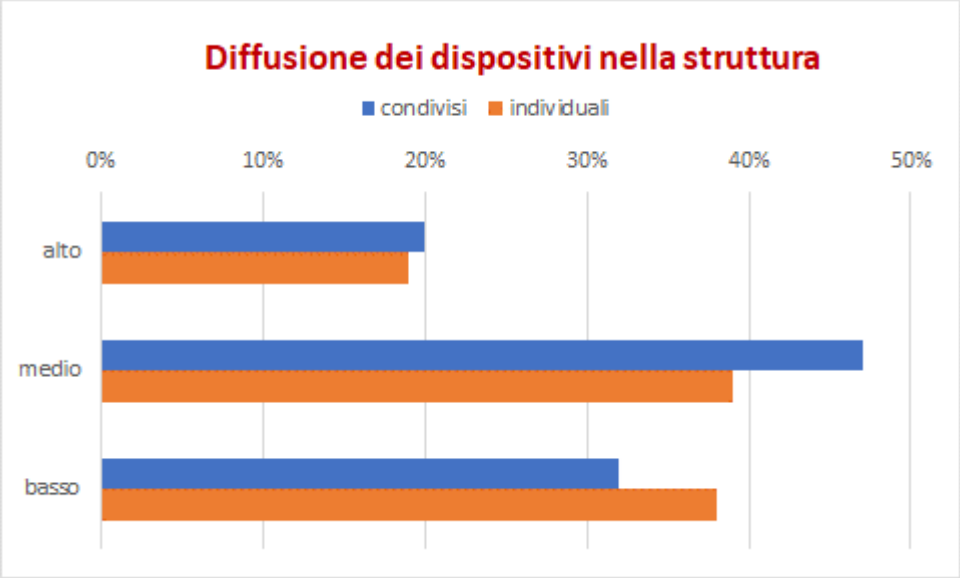
I dispositivi "individuali" e "condivisi" sono ampiamente diffusi nel contesto operativo. Per la loro stessa natura e per non essere -di norma e continuativamente- gestiti da un settore tecnico specializzato e dedicato, presentano tuttavia fattori di rischio più elevati sotto tutti i profili della sicurezza.

Il grafico indica in termini qualitativi il livello di diffusione dei dispositivi condivisi ed individuali, come percentuale rispetto al totale dei dispositivi installati.

Nota

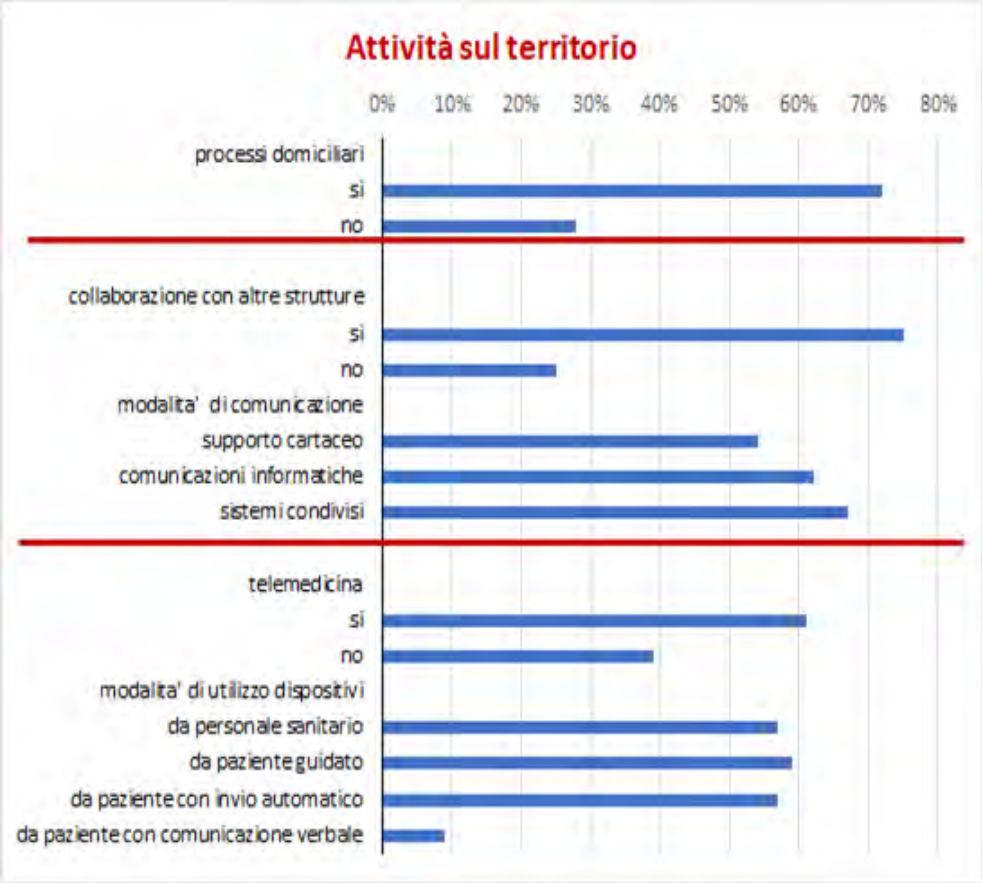
In tutti i prospetti dell'indagine

- *l'indicatore "basso" esprime un valore inferiore al 25%*
- *l'indicatore "medio" esprime un valore fra il 25% ed il 75%*
- *l'indicatore "basso" esprime un valore superiore al 75%*



3.4.3 Attività sul territorio

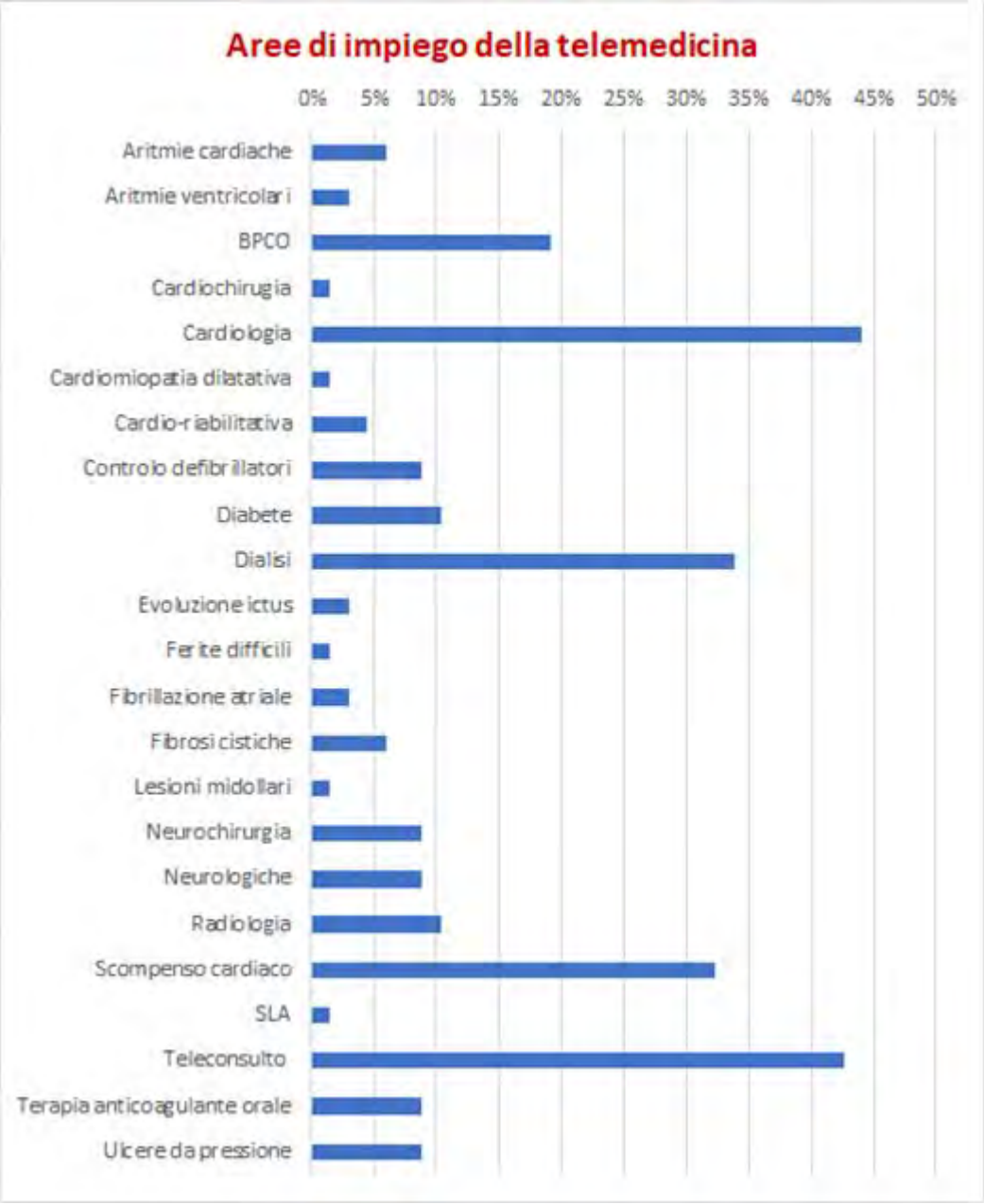
La crescente rilevanza delle attività svolte al di fuori della struttura, sia in assistenza domiciliare, sia in collaborazione con altre organizzazioni sanitarie, sia mediante l'uso di processi basati sulla telemedicina introduce fattori di rischio, in particolare dal punto di vista della protezione dei dati e della affidabilità delle informazioni acquisite.



Le principali tipologie di interazioni sul territorio sono evidenziate nei confronti di:

- Altri ospedali
- Medici di Medicina Generale
- Operatori socio-assistenziali
- Strutture ambulatoriali
- Strutture socio-sanitarie

Le principali patologie e condizioni di salute gestite regolarmente e/o seguite dopo l'episodio di ricovero mediante l'uso di processi basati sulla telemedicina sono evidenziate nel seguente grafico



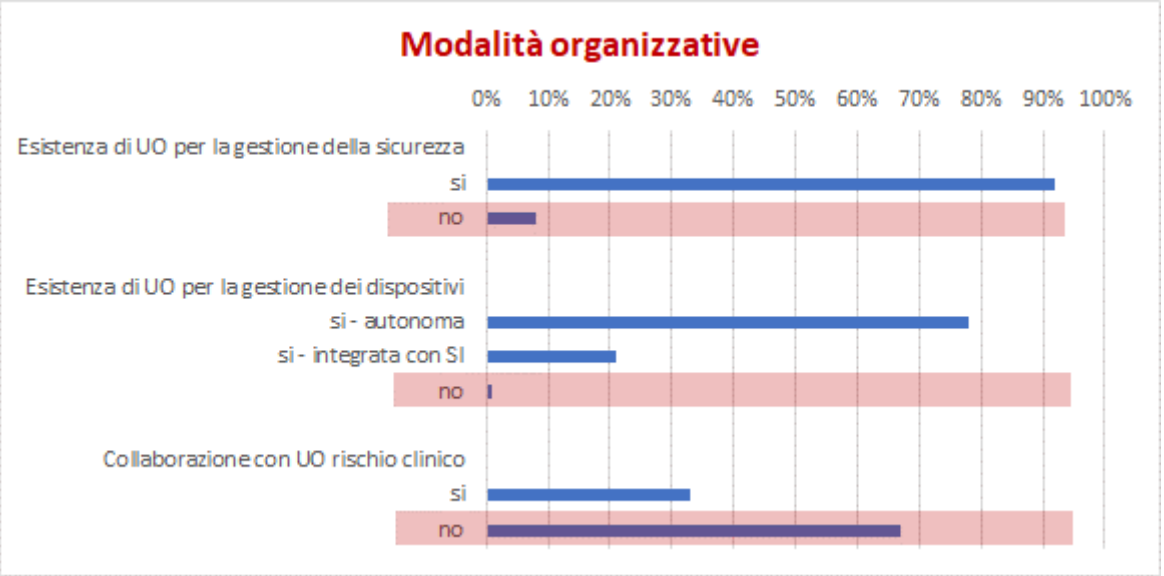
3.5 Aspetti organizzativi

3.5.1 Struttura organizzativa

Il seguente prospetto evidenzia le strutture organizzative implementate per la gestione della sicurezza.

Si evidenzia come

- circa il 10% delle aziende non disponga di una funzione aziendale (UO) preposta alla sicurezza del sistema informativo
- come in circa il 70% dei casi non ci sia collaborazione formalizzata fra la gestione della sicurezza e le problematiche inerenti il rischio clinico.

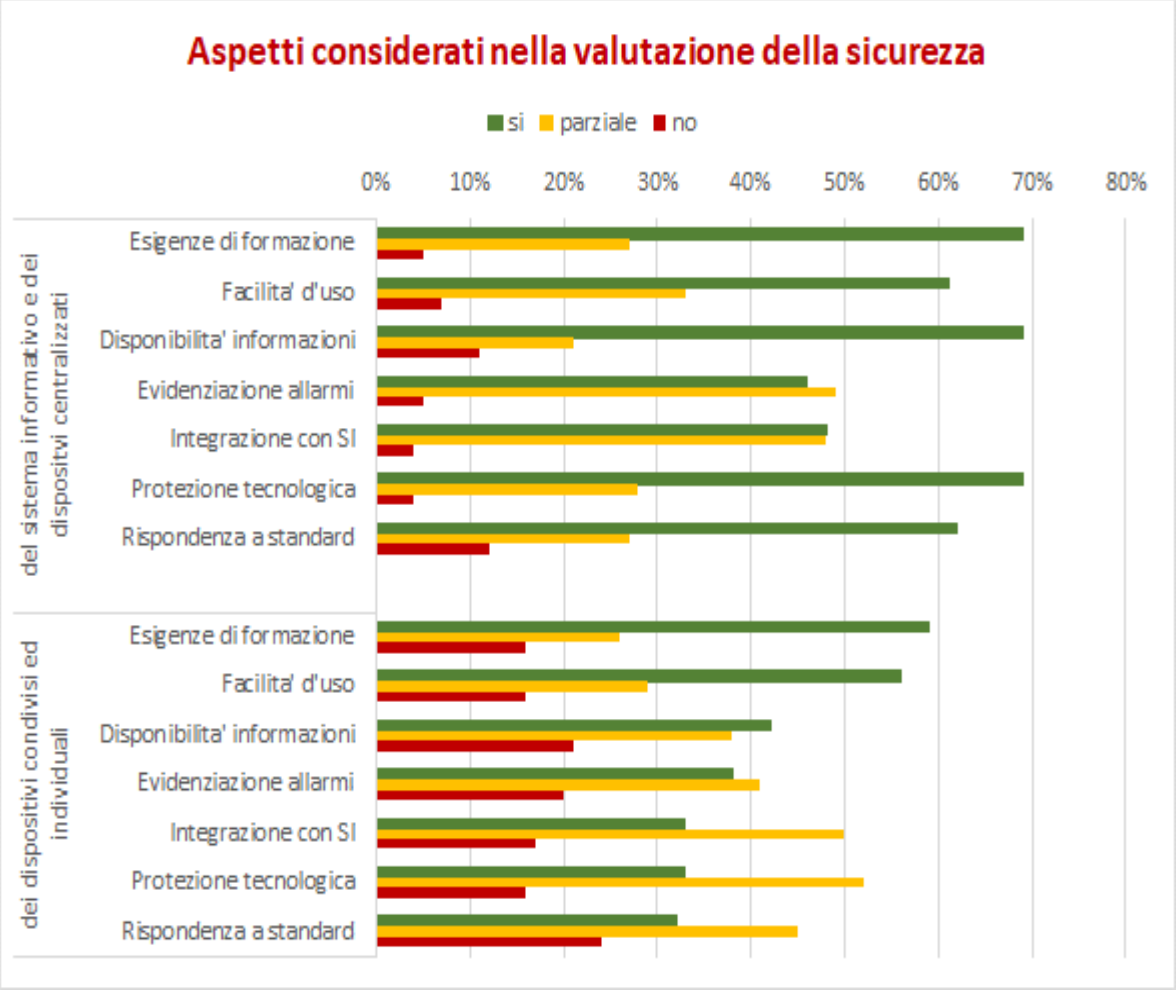


3.52 Valutazione dei fattori di rischio

Il seguente prospetto evidenzia gli aspetti considerati rilevanti ai fini della sicurezza.

Vale evidenziare come -nei dispositivi condivisi ed individuali- gli aspetti di protezione tecnologica, rispondenza a standard ed integrazione con il sistema informativo siano considerati meno rilevanti rispetto a quanto avviene per le apparecchiature centralizzate.

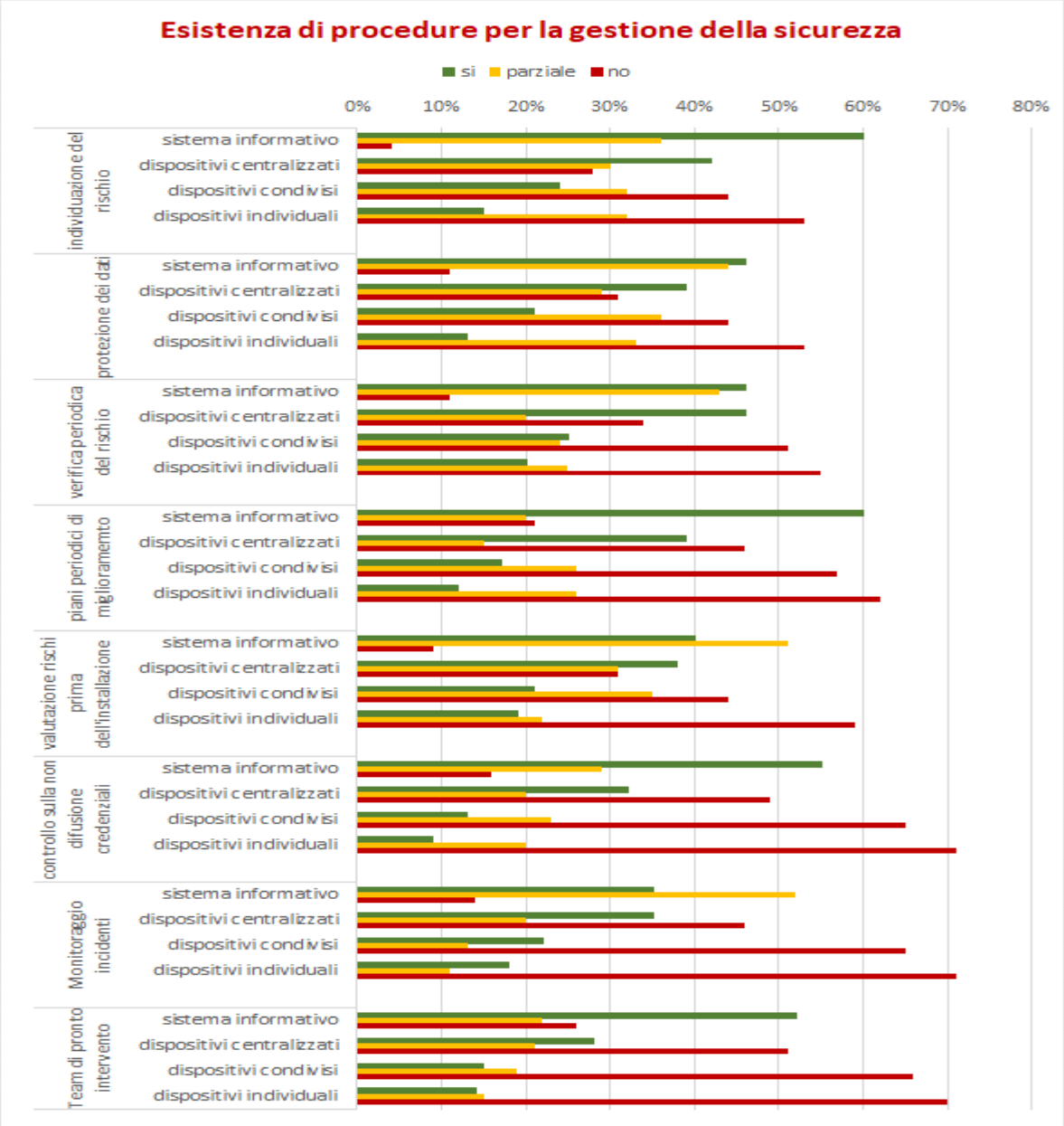
Questa minore percezione del rischio determina fattori di particolare criticità per tutto l'ecosistema, sia in termini di possibili vulnerabilità tecnologiche, sia in termini di disponibilità delle informazioni necessarie alle varie attività clinico-assistenziali.



3.5.3 Proceduralizzazione delle attività di valutazione e gestione

Il seguente prospetto evidenzia la presenza o meno di procedure formalizzate all'interno dell'organizzazione in merito ad alcuni aspetti rilevanti ai fini dell'analisi e della prevenzione dei rischi.

Anche in questo caso va osservato come i dispositivi condivisi ed individuali presentino un livello di attenzione e di gestione nettamente inferiore rispetto a quelli centralizzati, nonostante la loro significativa rilevanza e diffusione all'interno dell'organizzazione, come già evidenziato in precedenza.



3.6 Aspetti informativi

Il seguente prospetto evidenzia alcune caratteristiche inerenti la gestione delle informazioni considerate rilevanti ai fini della sicurezza.

In particolare viene considerata

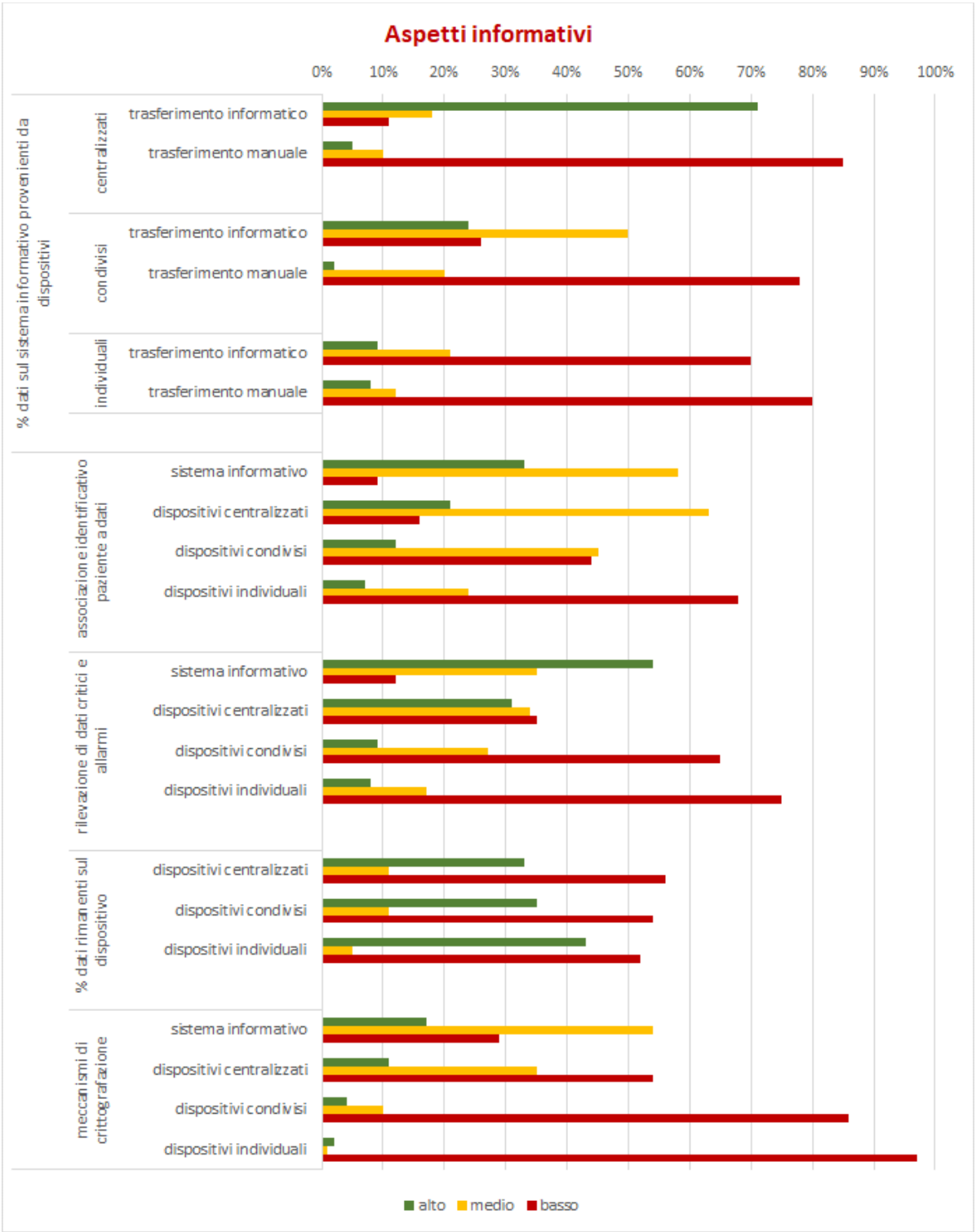
1. La rilevanza nel patrimonio informativo complessivo dei dati registrati per mezzo di dispositivi e le modalità secondo cui questi dati sono registrati nel sistema informativo.
   Va evidenziato come non sia marginale la percentuale dei dati registrati manualmente e come gran parte dei dati acquisiti dai dispositivi individuali non sia registrata affatto nel sistema informativo, e come sia alta la percentuale dei dati viene trascritta manualmente nel sistema informativo

2. Il quantitativo di dati che rimane registrato all'interno del dispositivo, che risulta essere molto elevato nel caso dei dispositivi condividi ed individuali.
   Questo, per le suddette condizioni di minore controllo di questi dispositivi espone a rischi notevoli in termini di protezione e di disponibilità dei dati.

3. La presenza di meccanismi in grado di evidenziare situazioni di criticità o di allarme nelle rilevazioni effettuate. Anche in questo caso, viene evidenziato un livello molto basso nei dispositivi condivisi ed individuali

4. La presenza di meccanismi in grado di crittografare i dati registrati. Anche in questo caso, viene evidenziato un livello molto basso nei dispositivi condivisi ed individuali, il che -unito alla alta percentuale di dati che rimangono memorizzati sugli stessi- amplifica i rischi in termini di protezione ed integrità dei dati.

Gli aspetti di cui al punto 1 e 2 determinano sia **limitazioni in termini di disponibilità di informazioni** complete a supporto delle attività cliniche in tutta la struttura, sia **rischi in termini di protezione dei dati**, stante la bassa integrazione dei dispositivi condivisi e individuali con il sistema informativo e la loro intrinsecamente maggiore vulnerabilità in termini di gestione e controllo.

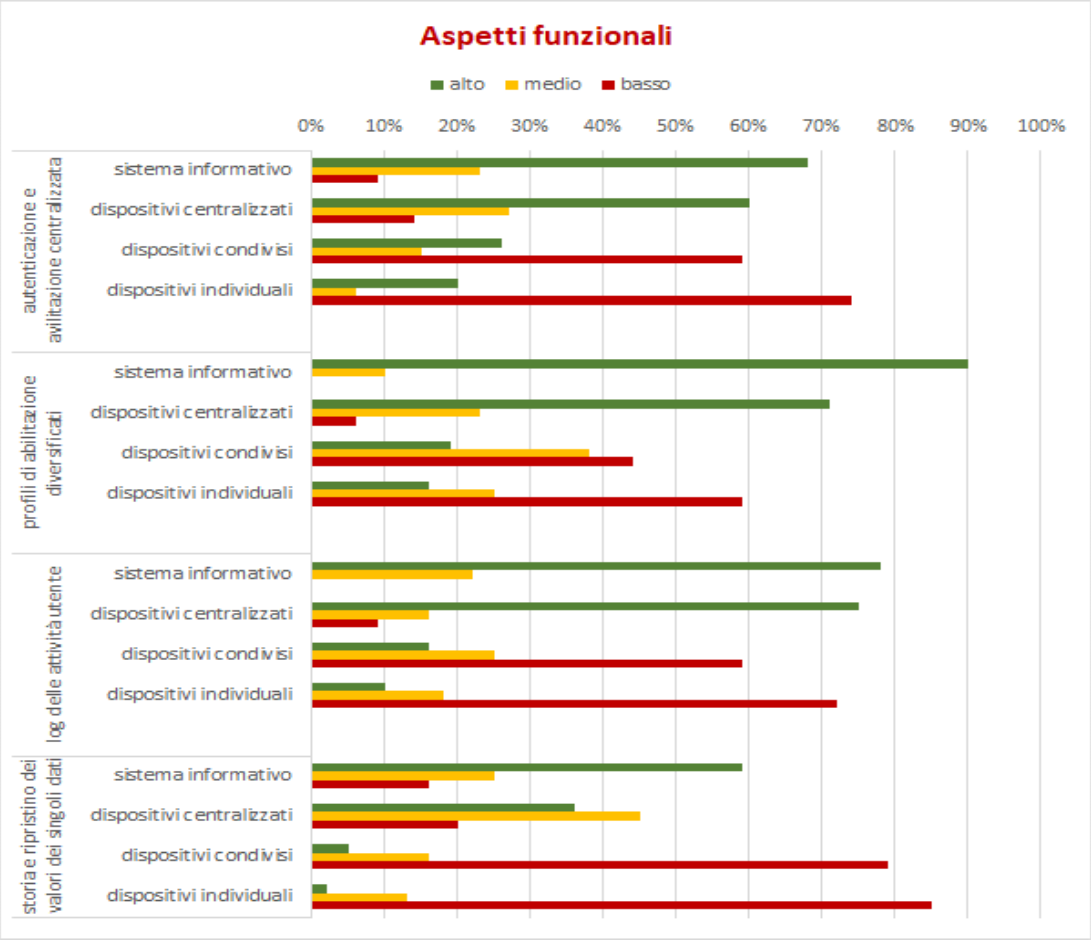

Aspetti informativi
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
% dati sul sistema informativo provenienti da dispositivi
centralizzati
trasferimento informatico
trasferimento manuale
condivisi
trasferimento informatico
trasferimento manuale
individuali
trasferimento informatico
trasferimento manuale
associazione e identificativo paziente a dati
sistema informativo
dispositivi centralizzati
dispositivi condivisi
dispositivi individuali
rilevazione di dati critici e allarmi
sistema informativo
dispositivi centralizzati
dispositivi condivisi
dispositivi individuali
% dati rimanenti sul dispositivo
dispositivi centralizzati
dispositivi condivisi
dispositivi individuali
meccanismi di crittografazione
sistema informativo
dispositivi centralizzati
dispositivi condivisi
dispositivi individuali
alto
medio
basso

3.7 Aspetti funzionali

Il seguente prospetto evidenzia alcune caratteristiche inerenti agli aspetti funzionali, principalmente in termini di riconoscimento ed abilitazione degli utenti e di registrazione delle attività effettuate.

Ancora, i dispositivi condivisi ed individuali, presentano -per tutti gli aspetti- livelli di controllo ed attenzione molto bassi, con conseguenti vulnerabilità significative in termini di sicurezza:

- è molto alta l'assenza di meccanismi di autenticazione e di abilitazione centralizzata nell'accesso;
- è molto alta l'assenza di meccanismi di log delle attività effettuate dagli utenti;
- sono praticamente assenti meccanismi in grado di tenere traccia della storia dei dati raccolti e di ripristinare versioni precedenti (questo unito al fatto che gran parte delle informazioni rimangono stabilmente registrate sul dispositivo aumenta il livello di rischio per la protezione e l'integrità dei dati stessi).



3.8 Aspetti tecnologici

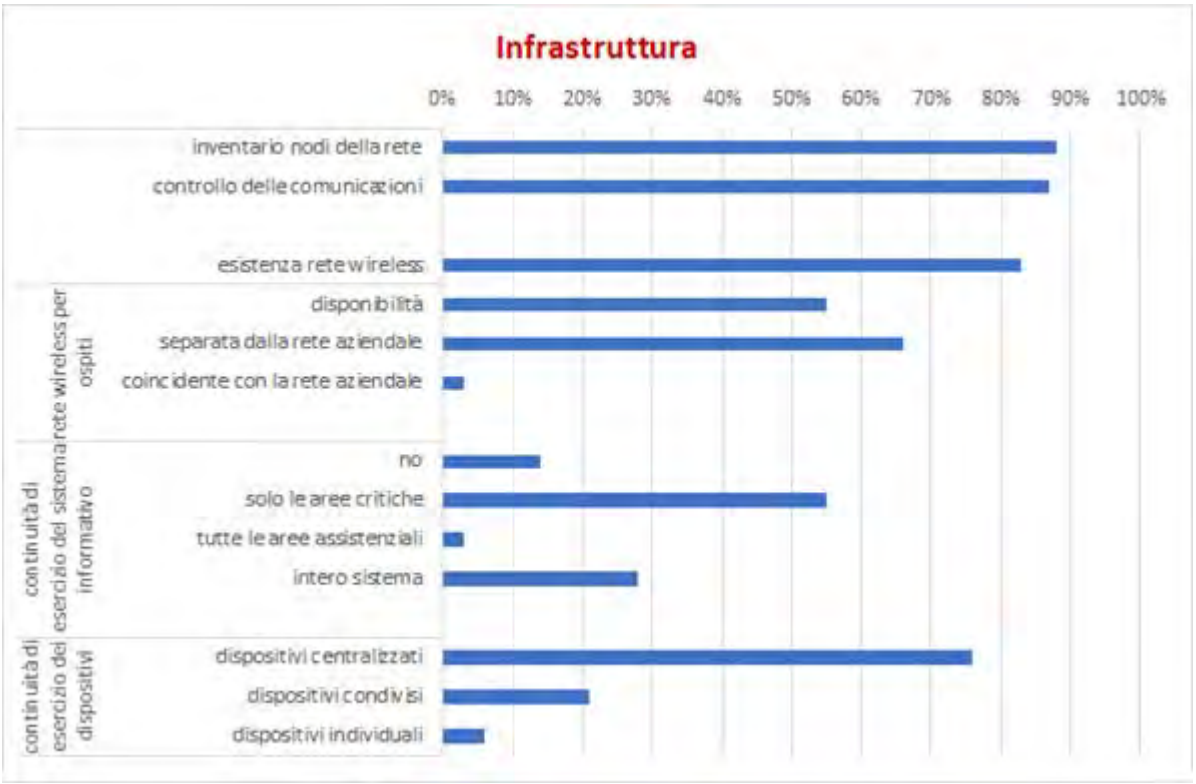
3.8.1 Infrastruttura

L'infrastruttura tecnologica, essenzialmente in termini di rete, è sicuramente uno degli aspetti più seguiti all'interno delle aziende.

Relativamente alla capacità dell'infrastruttura (in termini di apparecchiature, rete e procedure software) di assicurare la continuità operativa in caso di guasti:

- in **circa il 15%** dei casi il sistema informativo non fornisce questa possibilità, che è viene assicurata in oltre il 50% dei casi nelle aree critiche.

- al solito, i dispositivi condivisi ed individuali presentano bassi livelli di garanzia dal punto di vista della continuità di esercizio.



3.8.2 Altri aspetti tecnologici

Il seguente grafico individua altri aspetti dell'infrastruttura tecnologica ritenuti rilevanti ai fini della sicurezza.

Anche in questo ambito i dispositivi condivisi ed individuali presentano livelli di rischio più elevati:

- è molto alta l'assenza di meccanismi identificazione e rimozione di software dannosi;
- è molto alta l'assenza di protocolli protetti per la comunicazione sulla rete;
- è molto alta (ovvero poco controllata) la possibilità di comunicazione autonoma con l'esterno (ad esempio mediante modem locali), che amplifica i rischi riscontrati in termini di assenza di meccanismi centralizzati di identificazione ed autenticazione.

4. Indicatori di rilevanza ai fini della sicurezza

Sulla base delle informazioni raccolte mediante il questionario sono stati definiti indicatori sulle caratteristiche dei contesti "sistema informativo + dispositivo medico collegato" di rilevanza ai fini della sicurezza complessiva e della protezione dei dati, ripartiti, secondo tre prospettive:

a) sicurezza del paziente
b) protezione dei dati personali ed aspetti normativi
c) aspetti economici

Un primo criterio di valutazione è relativo alla rilevanza dei dispositivi medici nei processi medici ed assistenziali della specifica struttura, in funzione delle attività supportate all'interno della struttura stessa e delle eventuali attività condotte sul territorio, sia in collaborazione con altri centri, che direttamente in regime di assistenza domiciliare che mediante l'uso di protocolli basati sulla telemedicina.

Tanto maggiore è la rilevanza dei dispositivi medici misurata attraverso questi indicatori, tanto più significativi saranno per la struttura i rischi correlati alle varie caratteristiche del sistema.

Vengono quindi descritti gli indicatori di interesse circa le caratteristiche del binomio "sistema informativo + dispositivo medico connesso", suddivisi secondo le quattro prospettive tipiche del modello standard di rifermento ISO ODP 10746:

a) aspetti organizzativi
b) aspetti informativi
c) aspetti funzionali
d) aspetti tecnologici

Per ogni indicatore viene discussa l'incidenza dello stesso rispetto alle diverse prospettive di rischio e sicurezza.

4.1 Prospettive della sicurezza e fattori di rischio

Nell'accezione di intendere la sicurezza del sistema informativo sanitario come la capacità dello stesso di fornire un supporto completo ed affidabile ai processi dell'azienda, prendendo spunto dall'approccio dell'Health Technology Assessment, gli aspetti inerenti la sicurezza sono articolati secondo diverse prospettive, dal punto di vista dei rischi e delle possibili conseguenze sul contesto organizzativo ed operativo del sistema informativo sanitario come indicato nel seguito ([11],[12]):

Prospettiva inerente alla sicurezza del paziente [13]

1. Identificazione sicura dell'individuo
2. Correttezza della valutazione clinica
3. Errore/incompletezza della comunicazione fra sanitari
4. Dimenticanza
5. Non considerazione di informazioni rilevanti
6. Non disponibilità di informazioni rilevanti
7. Errore nell'inserimento manuale dei dati
8. Tempestività delle azioni a fronte delle esigenze

Prospettiva inerente agli aspetti legali e la protezione dei dati personali

1. Obblighi verso l'interessato
   a) descrizione dei dati gestiti
   b) trasportabilità dei dati
2. Obblighi generali del titolare nella gestione dei dati
3. Controllo nell'accesso alle informazioni
4. Identificabilità dell'autore di una operazione
5. Perdita di dati
6. Identificabilità dell'informazione ad una certa data
7. Ripristino di dati
8. Obblighi generali nell'organizzazione del titolare
9. Rispondenza leggi applicabili

Prospettiva economica

1. Aumento dei tempi di degenza
2. Duplicazione di esami e/o attività
3. Non appropriatezza degli esami e/o attività
4. Necessità di apparecchiature e meccanismi particolari
5. Costi di gestione
6. Tempo e risorse usate per eseguire una attività
7. Canoni di assicurazione
8. Costi legali anche relativamente al risarcimento di eventuali danni

[11] cfr F.M.Ferrara – S. Pillon "Medicina digitale: sicurezza per il medico e per il paziente", Progettare per la Sanità, Settembre 2016

[12] cfr National Data Guardian for Health and Care, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

[13] cfr anche Ministero della Salute, http://www.salute.gov.it/portale/temi/p2_6.jsp?id=250&area=qualita&menu=sicurezza

4.2 Caratteri che del contesto: rilevanza e diffusione dei dispositivi medici

Le organizzazioni sanitarie sono differenti l'una dall'altra, sia in termini di attività effettuate, che di dimensioni che di tecnologie utilizzate, e quindi anche di dispositivi nella quantità e nel ruolo dei dispositivi adottati.

Una metodologia di analisi e della sicurezza che non permetta di tenere conto di queste differenze sarebbe pertanto troppo rigida e non rappresentativa delle diverse realtà.

Un criterio che permetta di adattare l'analisi della sicurezza ed i livelli di rischio all'effettivo contesto operativo può essere individuato mediante la definizione dei **livelli di diffusione e di rilevanza** dei dispositivi medici nei processi di cura ed assistenziali erogati dalla specifica struttura

Con "**diffusione**" si intende una valutazione quantitativa del numero di attività effettuate con l'uso di dispositivi medici. In funzione di tale indice devono essere configurate le infrastrutture e dimensionati gli aspetti organizzativi.

Per definire un "**indice di diffusione**", si può fare riferimento alla percentuale di attività di un certo tipo (rispetto al totale delle attività clinico-assistenziali di quel tipo effettate dell'organizzazione) che sono eseguite con il supporto dei dispositivi medici.

Indice di diffusione		% rispetto al totale degli elementi di interesse
A	Alto	oltre 75%
B	Medio	fino a 75%
C	Basso	fino a 25%

Con "**rilevanza**" si intende il numero dei trattamenti clinico-assistenziali (es. pazienti/anno) basati sul supporto dispositivi medici rispetto al numero di trattamenti totali erogati dalla struttura.

Per definire una "**classe di rilevanza**", si può fare riferimento alla percentuale di pazienti (rispetto al totale dei pazienti trattati dall'organizzazione) per i quali si effettuano attività supportate dalle varie tipologie di dispositivi.

Classe di rilevanza		% rispetto al totale dei pazienti
A	Alta	oltre 75%
B	Media	fino a 75%
C	Bassa	fino a 25%

Questi descrittori di contesto rivestono una **particolare significatività in relazione ai dispositivi condivisi ed ai dispositivi individuali**, in quanto tali dispositivi -per come sono stati individuati e definiti - sono di norma gestiti e

monitorizzati al di fuori di processi strutturati delle unità operative dedicate e specializzate.

In questo senso, le implicazioni sul livello di sicurezza possono essere individuate come segue:

1. ***Tipologia delle attività clinico/assistenziali eseguite con l'uso di dispositivi e loro rilevanza nel contesto complessivo delle patologie e dei pazienti trattati dall'organizzazione.***

   Implicazioni sui fattori di rischio

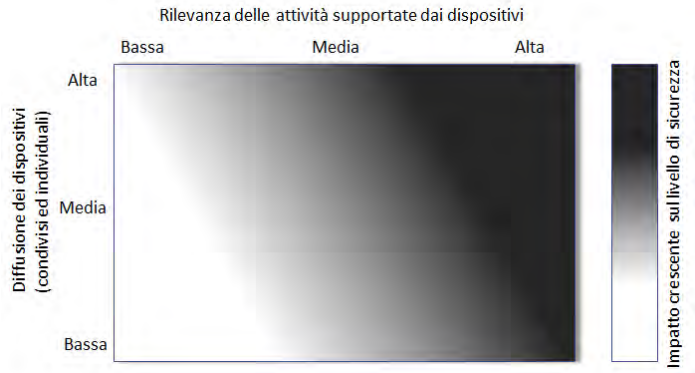
   - La rilevanza delle patologie trattate con l'ausilio di dispositivi, espressa in termini di numero di pazienti trattati rispetto al totale di quelli assistiti dall'organizzazione è un indicatore di quanto la sicurezza dei dispositivi incida sulla sicurezza totale del sistema informativo e dei processi clinici ed organizzativi connessi.

2. ***Livello di diffusione nella struttura delle apparecchiature condivise ed individuali***

   Implicazioni sui fattori di rischio

   - I dispositivi che presentano maggiori fattori di rischio -sotto tutte le prospettive- sono quelli condivisi e quelli individuali, in quanto per la loro stessa natura -così come sono stati definiti- sono di norma gestiti e monitorizzati al di fuori di processi strutturati delle unità operative dedicate e specializzate.

Questi due indicatori, correlati fra loro, hanno un impatto sui criteri di valutazione del livello di sicurezza finale, come rappresentato nella seguente figura.



4.3 Aspetti organizzativi

Struttura organizzativa

O1. Presenza di una unità operativa preposta alla sicurezza del sistema informativo nel suo complesso

Implicazioni sui fattori di rischio

- La formalizzazione nella struttura di una unità organizzativa esplicitamente preposta alla analisi e gestione della sicurezza del sistema informativo, tenendo conto delle diverse prospettive di rischio, è un aspetto qualificante evidenziare la sensibilità dell'organizzazione verso queste problematiche e per garantire che la gestione di tutti gli aspetti di sicurezza sia affrontata in modo organico e non episodica a fronte di problemi.

O2. Presenza di una unità operativa preposta alla gestione dei dispositivi

Implicazioni sui fattori di rischio

- La formalizzazione nella struttura di una funzione organizzativa esplicitamente preposta alla gestione dei dispositivi medici (eventualmente integrata o comunque cooperante con quella responsabile della gestione del sistema informativo), è un aspetto qualificante evidenziare la sensibilità dell'organizzazione verso la rilevanza assunta da questi dispositivi nell'ambito dei processi sanitari e per garantire che la loro gestione sia affrontata in modo organico e non episodica a fronte di esigenze contingenti.

O3. Formalizzazione della collaborazione fra l'unità responsabile del rischio clinico e quella/quelle responsabili della sicurezza del sistema informatico e dei dispositivi medici

Implicazioni sui fattori di rischio

- Considerata la missione e le attività condotte dalle organizzazioni sanitarie, la sicurezza e l'incolumità dei pazienti rappresenta un obiettivo fondamentale in termini di sicurezza. La collaborazione con le figure responsabili del rischio clinico ed il settore tecnologico (sistema informativo e dispositivi medici) è un aspetto qualificante per assicurare un approccio complessivo nella identificazione e valutazione di rischi e minacce, definire piani per la loro mitigazione e dare una adeguata risposta agli incidenti, garantendo prima di tutto la sicurezza e l'incolumità dei pazienti

Approccio alla valutazione dei rischi

O4. Argomenti presi in considerazione nella valutazione degli aspetti di rischio

a. esigenze di formazione
b. facilità d'uso
c. disponibilità tutte le informazioni utili
d. integrazione con il sistema informativo nel suo complesso
e. aspetti in termini di protezione tecnologica
f. rispondenza a standard per la gestione di informazioni e comunicazione in relazione a due categorie di componenti:

- sistema informativo nel suo complesso ed apparecchiature centralizzate
- apparecchiature condivise ed individuali

Implicazioni sui fattori di rischio

- La complessità della formazione necessaria e la difficoltà d'uso del dispositivo possono influire sulla possibilità di compiere errori da parte di personale non esplicitamente addestrato
- L'integrazione con il sistema informativo nel suo complesso, anche mediante l'uso di standard, contribuisce alla continuità dei processi (senza richiedere di passaggi manuali) ed alla integrazione delle informazioni sul paziente, utili nel processo di valutazione ed esecuzione dell'atto sanitario
- L'esistenza di meccanismi di protezione dal punto di vista tecnologico limita i rischi di vulnerabilità e di perdita/accesso non autorizzato ai dati.

O5. Presenza di procedure formalizzate per l'individuazione e la valutazione dei rischi dei rischi nel sistema informativo nel suo complesso
per l'intero contesto o parzialmente per settori specifici

Implicazioni sui fattori di rischio

- La presenza di procedure formalizzate per l'individuazione e la valutazione dei rischi -in modo tanto più rilevante quanto più estesa ai componenti del sistema e quanto più articolata nelle varie aree di rischio- denota una attenzione dell'organizzazione a questa problematica e garantisce una gestione non episodica delle problematiche connesse

O6. Presenza di procedure dettagliate per la gestione e la protezione dei dati personali
per l'intero contesto o parzialmente per settori specifici

Implicazioni sui fattori di rischio

- La presenza di procedure per la gestione e la protezione dei dati personali è richiesta dal Regolamento. Il dettaglio e l'estensione di queste procedure -fini alle operatività sui dispositivi- denota una attenzione dell'organizzazione a questa problematica e garantisce una gestione non episodica delle problematiche connesse

O7. Presenza di procedure per la valutazione e la verifica di problemi di sicurezza preventivamente all'installazione di un nuovo componente

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

per l'intero contesto di pertinenza o parzialmente per settori specifici

Implicazioni sui fattori di rischio

- La valutazione preventiva degli aspetti di rischio in termini di protezione dei dati personali è richiesta espressamente -almeno per i trattamenti più delicati- dal Regolamento (esplicitare GDPR?)
- La presenza di procedure formalizzate di verifica prima dell'installazione contribuisce -in misura tanto maggiore quanto più estesa nei vari settori ed alle varie tipologie di apparecchiature- ad evitare rischi in generale, ma con particolare riguardo agli aspetti di accesso non autorizzato e di distruzione / perdita di dati

O8. Presenza di procedure formalizzate per la verifica periodica dei rischi e dei livelli di sicurezza e protezione dati

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

per l'intero contesto di pertinenza o parzialmente per settori specifici

Implicazioni sui fattori di rischio

- La valutazione periodica degli aspetti di rischio in termini di protezione dei dati personali è richiesta espressamente dal Regolamento UE 679/2016 (GDPR)

O9. Presenza di procedure tecnico/organizzative per la protezione dei dati registrati localmente e per l'individuazione dei rischi

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Implicazioni sui fattori di rischio

- La protezione dei dati, come stabilito dal Regolamento, implica l'adozione di misure sia tecniche che organizzative.

Gestione e Monitoraggio

O10. Formalizzazione di piani periodici di analisi e miglioramento sui rischi e sui livelli di sicurezza

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

per l'intero contesto di pertinenza o parzialmente per settori specifici

Implicazioni sui fattori di rischio

- La formalizzazione di procedure aziendali per la valutazione ed il miglioramento dei livelli di sicurezza è un aspetto qualificante (previsto anche dal Regolamento) per assicurare che la gestione delle problematiche connesse sia organizzata e condotta secondo una visione ed un piano organico.

O11. Esistenza di meccanismi e di controlli periodici sulla non diffusione di credenziali

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

per l'intero contesto di pertinenza o parzialmente per settori specifici

Implicazioni sui fattori di rischio

- L'utilizzo delle stesse credenziali da parte di utenti diversi impedisce il tracciamento delle attività effettuate
- L'utilizzo delle stesse credenziali da parte di utenti diversi può consentire di accedere a dati o funzionalità alle quali gli utenti non sono abilitati

O12. Monitoraggio del sistema e rilevazione degli incidenti inerenti la sicurezza mediante una procedura formalizzata per il loro tracciamento

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

per l'intero contesto di pertinenza o parzialmente per settori specifici

Implicazioni sui fattori di rischio

- Il monitoraggio del sistema di protezione dei dati è esplicitamente previsto dal Regolamento
- La presenza di procedure formalizzate di monitoraggio riduce il rischio di incidenti, con possibili conseguenze sui pazienti e sui processi organizzativi

O13. Presenza di un team in grado di intervenire tempestivamente in caso di incidenti riguardanti la sicurezza

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

per l'intero contesto di pertinenza o parzialmente per settori specifici

Implicazioni sui fattori di rischio

- Il ripristino tempestivo del valore e della disponibilità dei dati personali è esplicitamente richiesto dal Regolamento
- La non tempestiva risoluzione di incidenti che comportino la indisponibilità di dati e/o di apparecchiature può incidere sulla esecuzione degli atti sanitari con conseguenze per il paziente
- La non tempestiva risoluzione di incidenti che comportino la indisponibilità di dati e/o di apparecchiature può incidere sulla esecuzione degli atti sanitari con conseguenze per il paziente
- La non tempestiva risoluzione di incidenti che comportino la indisponibilità di dati e/o di apparecchiature può incidere sulla efficienza dei processi organizzativi con conseguenti implicazioni anche di natura economica

4.4 Aspetti informativi

Archiviazione

I1. Volume dei dati clinico/assistenziali provenienti dai dispositivi che vengono integrati nel sistema informativo

a. relativamente alle apparecchiature centralizzate
b. relativamente alle apparecchiature condivise
c. relativamente alle apparecchiature individuali

In termini qualitativi, si può classificare in termini di percentuale rispetto ai dati raccolti dai dispositivi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- La quantità dei dati provenienti dai dispositivi che viene integrata nel sistema informativo (intesa come percentuale rispetto al totale dei dati clinico assistenziali registrati sui pazienti) indica la rilevanza dei dispositivi nella continuità del processo clinico assistenziale. Si sottolinea a questo proposito l'aspetto della integrazione, in quanto dati acquisiti dal dispositivo ma non integrati nel sistema informativo

non risultano fruibili per una visione complessiva dello stato del paziente e quindi incidono sul rischio di errore di valutazione.

- Devono inoltre essere considerate le modalità secondo cui tali dati vengono integrati: una modalità di integrazione mediante trascrizione manuale incide sul rischio di errore mentre, in caso di trasmissione automatica, vanno considerati gli aspetti di sicurezza dell'infrastruttura tecnologica.
- Anche in questo caso, i dispositivi che presentano maggiori fattori di rischio sono quelli condivisi e quelli individuali, in quanto per la loro stessa natura -così come sono stati definiti- sono di norma gestiti e monitorizzati al di fuori di processi strutturati delle unità operative dedicate e specializzate.

I2. Trasferimento via rete al sistema informativo dei dati provenienti dai dispositivi

a. relativamente alle apparecchiature centralizzate
b. relativamente alle apparecchiature condivise
c. relativamente alle apparecchiature individuali

In termini qualitativi, si può classificare in termini di percentuale rispetto ai dati raccolti dai dispositivi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- Le modalità secondo cui i dati provenienti dai dispositivi vengono registrati nel sistema informativo hanno influenza sugli aspetti di sicurezza: una modalità di integrazione mediante trascrizione manuale incide sul rischio di errore mentre, in caso di trasmissione automatica, vanno considerati gli aspetti di sicurezza dell'infrastruttura tecnologica.
- Anche in questo caso, i dispositivi che presentano maggiori fattori di rischio sono quelli condivisi e quelli individuali, in quanto per la loro stessa natura -così come sono stati definiti- sono di norma gestiti e monitorizzati al di fuori di processi strutturati delle unità operative dedicate e specializzate.

I3. Volume dei dati raccolti dall'apparecchiatura che rimangono memorizzati permanentemente nell'apparecchiatura stessa

a. relativamente alle apparecchiature centralizzate
b. relativamente alle apparecchiature condivise
c. relativamente alle apparecchiature individuali

In termini qualitativi, si può classificare in termini di percentuale rispetto ai dati raccolti dai dispositivi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- Se non integrati con il resto dei dati del sistema informativo, i dati registrati sull'apparecchiatura non sono utilizzabili nell'ambito della valutazione complessiva dello stato di salute del paziente
- Dati registrati su diverse apparecchiature comportano l'obbligo -ai sensi del Regolamento- di implementare su ogni apparecchiatura le appropriate misure di protezione e sicurezza, con conseguenti costi iniziali, di monitoraggio e di manutenzione
- Anche in questo caso, i dispositivi che presentano maggiori fattori di rischio sono quelli condivisi e quelli individuali, in quanto per la loro stessa natura -così come sono stati definiti- sono di norma gestiti e monitorizzati al di fuori di processi strutturati delle unità operative dedicate e specializzate.

I4. Presenza di funzionalità per la crittografazione dei dati personali registrati

a. nell'ambito del sistema informativo e delle apparecchiature centralizzate
b. relativamente alle apparecchiature condivise
c. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- L'assenza di meccanismi di crittografazione aumenta la vulnerabilità del sistema in termini di accesso non autorizzato ai dati (agendo direttamente sugli archivi)
- L'assenza di meccanismi di crittografazione su dati identificativi comporta l'adozione di altre procedure e meccanismi per consentire analisi epidemiologiche, statistiche e di ricerca nel rispetto di quanto previsto dal Regolamento
- Anche in questo caso, i dispositivi che presentano maggiori fattori di rischio sono quelli condivisi e quelli individuali, in quanto per la loro stessa natura -così come sono stati definiti- sono di norma gestiti e monitorizzati al di fuori di processi strutturati delle unità operative dedicate e specializzate.

Proattività

I5. Presenza di funzionalità in grado di rilevare e segnalare automaticamente e tempestivamente situazioni di criticità e/o allarme in funzione dei dati registrati

a. nell'ambito del sistema informativo e delle apparecchiature centralizzate
b. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- Il riconoscimento e l'evidenziazione automatica di situazioni critiche o di allarme riduce il rischio per il paziente

4.5 Aspetti funzionali

Identificazione della persona

F1. Presenza di meccanismi in grado di assicurare l'identificazione certa della persona (RFID, bracciali con codice a barre, etc.)

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- L'assenza di meccanismi in grado di assicurare l'identificazione certa del paziente comporta rischi in tutti gli atti sanitari, con conseguenti rischi per la salute del paziente (ed eventuali costi di risarcimento danni)

Abilitazioni

F2. Gestione centralizzata delle credenziali di accesso ai diversi componenti del sistema

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- L'assenza di meccanismi in grado di gestire centralmente le credenziali di accesso ha implicazioni sulla complessità (e quindi sui costi) delle attività di gestione che devono essere replicate su ogni componente
- L'assenza di meccanismi in grado di gestire centralmente le credenziali di accesso comporta il rischio di non allineamento simultaneo del sistema e quindi di possibili accessi non autorizzati ai dati ed alle procedure

F3. Gestione centralizzata dei profili di abilitazione all'esecuzione delle varie funzionalità nei diversi componenti del sistema

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- L'assenza di meccanismi centralizzati per la definizione e la gestione dei profili di abilitazione per tutti i componenti del sistema e della associazione degli utenti agli stessi lascia ai singoli settori l'onere di questa attività (con conseguenti aumenti in termini di costi di gestione) e genera rischi in termini di non allineamento delle abilitazioni all'interno della struttura, con conseguente accesso non autorizzato ai dati personali e/o indisponibilità di informazioni necessarie (con rischio per il paziente)
- L'assenza di meccanismi centralizzati per la definizione e la gestione dei profili di abilitazione per tutti i componenti del sistema e della associazione degli utenti agli stessi rende più complessa e soggetta ad errori la compilazione completa dei "Registri di trattamento" previsti dal Regolamento.

F4. Presenza di funzionalità di blocco automatico della sessione (con successiva necessità di re-identificazione dell'utente) dopo un certo periodo di inattività

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- L'assenza di meccanismi per il blocco automatico delle sessioni di lavoro dopo un certo periodo di inattività genera rischi in termini di visibilità ed accesso a dati personali da parte di personale non autorizzato.

Tracciabilità

F5. Presenza di meccanismi di log automatico circa le attività effettuate dall'utente attività

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- L'assenza di meccanismi per la registrazione delle attività effettuate dai singoli utenti non rende possibile la tracciabilità delle azioni effettuate con conseguenze sulla validazione dei dati (e possibili rischi per il paziente) e non rende possibile risalire alle responsabilità in caso di violazione delle regole, secondo quanto previsto dal Regolamento.

F6. Presenza di meccanismi (diversi dal backup completo) che consentano l'accesso ed il ripristino di singoli dati al valore assunto in un momento precedente (tendenzialmente a qualsiasi data precedente)

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- L'assenza di meccanismi (diversi dal ripristino dell'intero backup della base dati) che consentano di risalire al valore assunto da uno o più dati singolarmente ad una certa data non rende possibile la

rettifica tempestiva di informazioni, secondo quanto prescritto dal Regolamento

- L'assenza di meccanismi (diversi dal ripristino dell'intero backup della base dati) che consentano di risalire al valore assunto da uno o più dati singolarmente ad una certa data non rende possibile di ricostruire il quadro secondo cui sono state prese decisioni di natura clinica, con conseguenti rischi legali, economici e in termini di salute del paziente.

4.6 Aspetti tecnologici

T1. Gestione di un inventario dei dispositivi collegati alla rete

Implicazioni sui fattori di rischio

- Oltre ad essere prevista come obbligo dell'organizzazione nell'ambito delle "Norme minime di sicurezza ICT per le pubbliche amministrazioni" [14], la presenza e la gestione di un inventario di tutti i dispositivi collegati alla rete è necessaria per consentire una valutazione complessiva dei rischi e della sicurezza dei singoli contesti

Proattività

T2. Presenza -nell'infrastruttura tecnologica- di un meccanismo che riconosca ed evidenzi automaticamente la connessione alla rete di nuovi dispositivi

Implicazioni sui fattori di rischio

- L'assenza di meccanismi che consentano di rilevare automaticamente (e di autorizzare) il collegamento di nuovi dispositivi all'infrastruttura tecnologica -specialmente in caso di apertura verso gli ospiti o sul territorio- facilita la possibilità di accessi non autorizzati (con rischi sulla protezione dei dati) ed aumenta la complessità ed i costi di gestione per l'implementazione di soluzioni alternative per ovviare al problema.

T3. Presenza di un meccanismo che regolamenti le comunicazioni fra i diversi nodi, consentendo o meno l'interazione fra nodi specifici

Implicazioni sui fattori di rischio

- L'assenza di meccanismi che regolamentino le comunicazioni fra i diversi nodi della rete -specialmente in caso di apertura verso gli ospiti o sul territorio e di non presenza di meccanismi centralizzati di gestione delle abilitazioni- facilita la possibilità di accesso non

[14] Circolare dell'Agenzia per l'Italia Digitale n. 2/2017 del 18.4.2017

autorizzato ed aumenta la complessità ed i costi di gestione per l'implementazione di soluzioni alternative per ovviare al problema (ovvero la necessità di implementare e manutenere tali regole su ogni dispositivo/ applicazione).

Connettività

T4. Utilizzo di meccanismi e protocolli in grado di garantire la protezione della comunicazione (es. crittografazione) fra i diversi componenti del sistema

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise
d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- L'assenza di meccanismi e protocolli in grado di garantire la protezione delle comunicazioni influisce direttamente e sensibilmente sul rischio di accesso non autorizzato (intercettazione) ai dati oltre nonché, in caso di dolo, sul rischio di modifica dei dati stessi (con conseguenze sulla salute del paziente e dal punto di vista legale)

T5. Utilizzo della rete wireless per il collegamento delle apparecchiature

a. relativamente alle apparecchiature centralizzate
b. relativamente alle apparecchiature condivise
c. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- Di per sé non comporta fattori di rischio, purché venga validata (e opportunamente adeguata) la configurazione standard delle case produttrici che, molto spesso per mancanza di tempo, non configurano gli Access Point in maniera dettagliata. Le loro password, gli SSID e le chiavi WEP/WPA e crittografia di default sono facile preda di potenziali aggressori quindi questi aspetti necessitano di appropriate misure di protezione, in termini economici e di gestione.

T6. Presenza nella infrastruttura dell'organizzazione di una rete wireless accessibile ed utilizzabile dagli ospiti

Possono verificarsi tre scenari:

a. non è presente una rete accessibile agli ospiti;
b. è presente una rete wireless accessibile agli ospiti, ma è separata rispetto a quella usata dal sistema informativo
c. è presente una rete wireless accessibile agli ospiti ed è coincidente con quella usata dal sistema informativo

Implicazioni sui fattori di rischio

- La disponibilità di una rete wireless accessibile agli ospiti coincidente con quella usata dal sistema informativo aumenta sensibilmente i fattori di rischio in termini di accessi non autorizzato (protezione dei dati) e comporta l'adozione (in termini di costi di installazione, monitoraggio e gestione) di misure tecniche adeguate per evitare tali rischi (segmentazione, firewall, sistemi antintrusione, ecc.).

T7. Presenza di dispositivi per rilevare e rimuovere automaticamente software pericoloso

1. nell'ambito del sistema informativo
2. relativamente alle apparecchiature centralizzate
3. relativamente alle apparecchiature condivise
4. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- La presenza (centralizzata e gestita centralmente) dispositivi per rilevare e rimuovere automaticamente il software pericoloso diminuisce il rischio di in termini di a) accesso non autorizzato a dati, b) indisponibilità del sistema (con conseguenze economiche e per il paziente).
- La presenza (centralizzata e gestita centralmente) dispositivi per rilevare e rimuovere automaticamente il software pericoloso diminuisce i costi (ed i rischi di dimenticanze) connessi alla gestione indipendente dei singoli componenti del sistema

Comunicazioni

T8. Presenza di configurazioni e/dispositivi che consentano la comunicazione autonoma di singoli componenti con l'esterno, senza passare per la rete dell'organizzazione

a. nell'ambito del sistema informativo
b. relativamente alle apparecchiature centralizzate
c. relativamente alle apparecchiature condivise

d. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- La presenza di configurazioni e/o dispositivi che consentano la comunicazione autonoma di singoli componenti con l'esterno aumenta il rischio di accessi non autorizzati a tutti i componenti del sistema, con conseguenze in termini di protezione dei dati e di possibili interruzioni di funzionamento (con oneri in termini di costi e di tempo).
- L'implementazione di soluzioni atte a minimizzare tali rischi, comporta un incremento dei tempi e dei costi di implementazione, monitoraggio e gestione di meccanismi di protezione su ogni singolo dispositivo interessato.

Operatività

T9. Possibilità -per l'amministratore- di gestire da remoto le configurazioni e le caratteristiche delle apparecchiature

1. relativamente alle apparecchiature centralizzate
2. relativamente alle apparecchiature condivise
3. relativamente alle apparecchiature individuali

Si può classificare termini qualitativi, come percentuale rispetto al totale dei contesti operativi: "bassa" (meno del 25%), "media" (fra 25% e 75%) ed "alta" (oltre il 75%).

Implicazioni sui fattori di rischio

- La possibilità -per l'amministratore- di gestire da remoto le configurazioni delle apparecchiature riduce il rischio di dimenticanze ed il costo di gestione.
- D'altra parte, la possibilità -per l'amministratore- di gestire da remoto le configurazioni delle apparecchiature richiede l'implementazione di meccanismi di autenticazione e comunicazione affidabili e robusti.

T10. Presenza di configurazioni che consentano la continuità operativa anche in caso di guasti o incidenti nelle sole aree critiche

Si identificano quattro scenari:

1. nell'ambito del sistema informativo
2. relativamente alle apparecchiature centralizzate
3. relativamente alle apparecchiature condivise
4. relativamente alle apparecchiature individuali

Implicazioni sui fattori di rischio

- Per la missione e le attività delle strutture sanitarie, la continuità operativa del sistema informativo in alcuni settori (emergenza, sale operatorie, terapia intensiva, etc.) rappresenta un elemento fondamentale in termini di sicurezza dei processi e del paziente
- In funzione del ruolo e della rilevanza delle apparecchiature (essenzialmente trattasi di quelle centralizzate) nell'ambito dei processi interessati, la continuità operativa è possibile solo in presenza di adeguate configurazioni delle apparecchiature utilizzate a supporto delle attività critiche tali contesti.

T11. Presenza di configurazioni che consentano la continuità operativa anche in caso di guasti o incidenti per tutte le attività clinico assistenziali

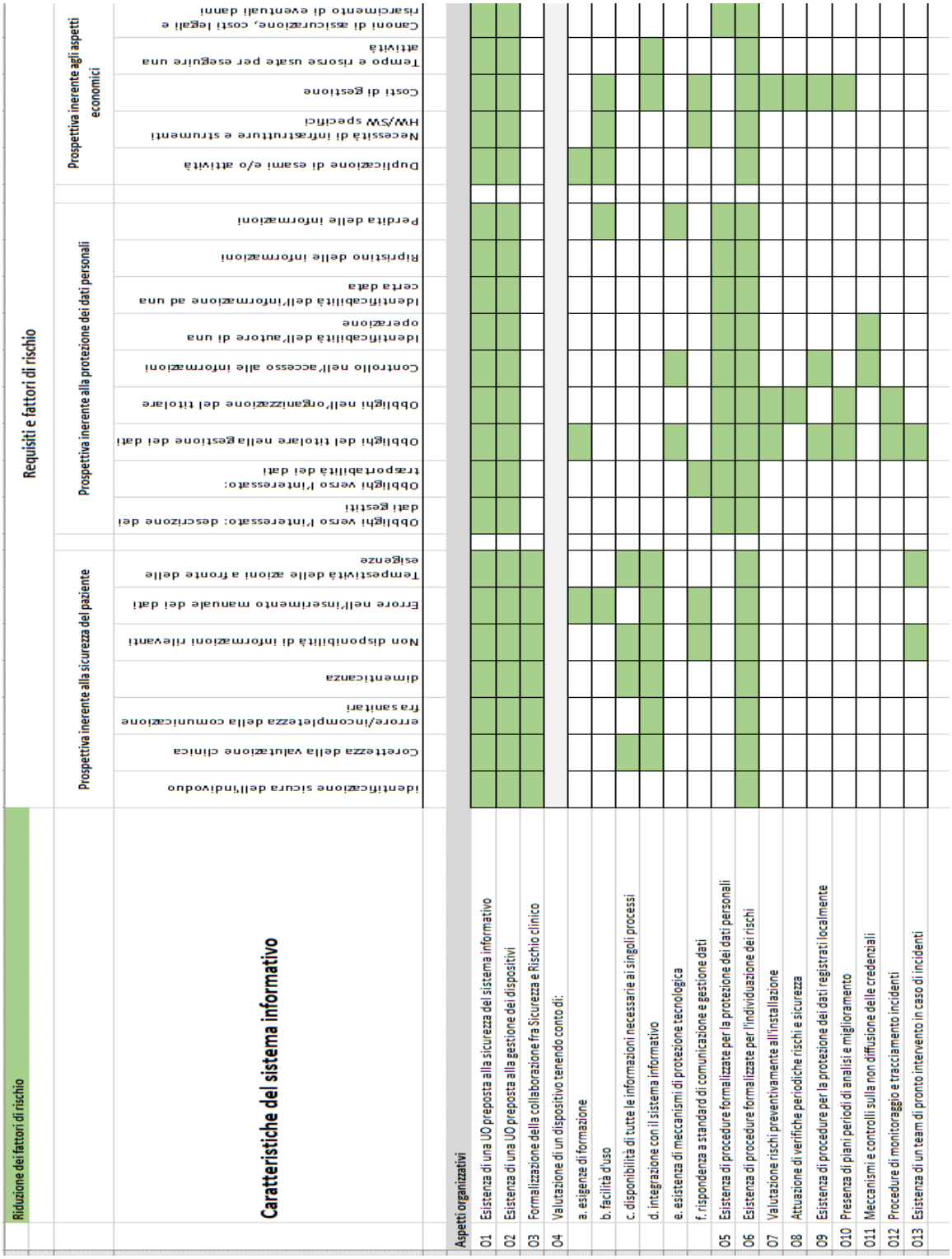
Si identificano quattro scenari:

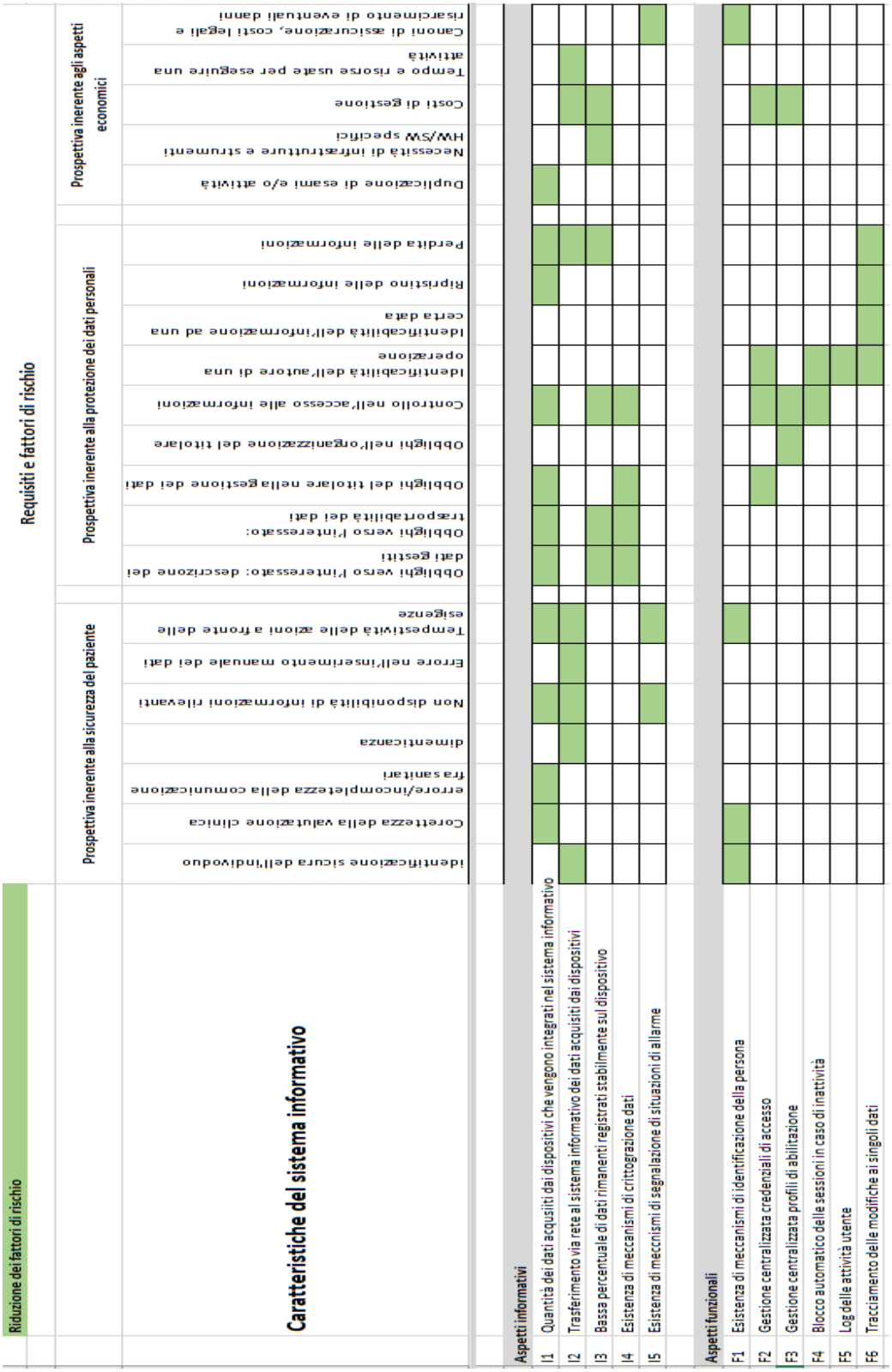
1. nell'ambito del sistema informativo
2. relativamente alle apparecchiature centralizzate
3. relativamente alle apparecchiature condivise
4. relativamente alle apparecchiature individuali

Implicazioni sui fattori di rischio

- Per la missione e le attività delle strutture sanitarie, la continuità operativa del sistema informativo in tutti i settori clinico assistenziali rappresenta un elemento qualificante in termini di sicurezza dei processi e del paziente
- In funzione del ruolo e della rilevanza delle apparecchiature (essenzialmente trattasi di quelle centralizzate) nell'ambito dei processi interessati, la continuità operativa è possibile solo in presenza di adeguate configurazioni anche delle apparecchiature utilizzate a supporto.

4.7. Schema complessivo di correlazione




Riduzione dei fattori di rischio
Requisiti e fattori di rischio
Caratteristiche del sistema informativo
Prospettiva inerente alla sicurezza del paziente
Prospettiva inerente alla protezione dei dati personali
Prospettiva inerente agli aspetti economici
Identificazione sicura dell'individuo
Correttezza della valutazione clinica
errore/incompletezza della comunicazione fra sanitari
dimenticanza
Non disponibilità di informazioni rilevanti
Errore nell'inserimento manuale dei dati
Tempestività delle azioni a fronte delle esigenze
Obblighi verso l'interessato: descrizione dei dati gestiti
Obblighi verso l'interessato: trasportabilità dei dati
Obblighi del titolare nella gestione dei dati
Obblighi nell'organizzazione del titolare
Controllo nell'accesso alle informazioni
Identificabilità dell'autore di una operazione
Identificabilità dell'informazione ad una certa data
Ripristino delle informazioni
Perdita delle informazioni
Duplicazione di esami e/o attività
Necessità di infrastrutture e strumenti HW/SW specifici
Costi di gestione
Tempo e risorse usate per eseguire una attività
Canoni di assicurazione, costi legali e risarcimento di eventuali danni
Aspetti informativi
I1 Quantità dei dati acquisiti dai dispositivi che vengono integrati nel sistema informativo
I2 Trasferimento via rete al sistema informativo dei dati acquisiti dai dispositivi
I3 Bassa percentuale di dati rimanenti registrati stabilmente sul dispositivo
I4 Esistenza di meccanismi di crittografazione dati
I5 Esistenza di meccnismi di segnalazione di situazioni di allarme
Aspetti funzionali
F1 Esistenza di meccanismi di identificazione della persona
F2 Gestione centralizzata credenziali di accesso
F3 Gestione centralizzata profili di abilitazione
F4 Blocco automatico delle sessioni in caso di inattività
F5 Log delle attività utente
F6 Tracciamento delle modifiche ai singoli dati

Riduzione dei fattori di rischio	Requisiti e fattori di rischio																				
	Prospettiva inerente alla sicurezza del paziente							Prospettiva inerente alla protezione dei dati personali									Prospettiva inerente agli aspetti economici				
Caratteristiche del sistema informativo	identificazione sicura dell'indivoduo	Correttezza della valutazione clinica	errore/incompletezza della comunicazione fra sanitari	dimenticanza	Non disponibilità di informazioni rilevanti	Errore nell'inserimento manuale dei dati	Tempestività delle azioni a fronte delle esigenze	Obblighi verso l'interessato: descrizione dei dati gestiti	Obblighi verso l'interessato: trasportabilità dei dati	Obblighi del titolare nella gestione dei dati	Obblighi nell'organizzazione del titolare	Controllo nell'accesso alle informazioni	Identificabilità dell'autore di una operazione	Identificabilità dell'informazione ad una certa data	Ripristino delle informazioni	Perdita delle informazioni	Duplicazione di esami e/o attività	Necessità di infrastrutture e strumenti HW/SW specifici	Costi di gestione	Tempo e risorse usate per eseguire una attività	Canoni di assicurazione, costi legali e risarcimento di eventuali danni
Aspetti tecnologici																					
T1 Presenza di un inventario di tutte le apparecchiature autorizzate																					
T2 Esistenza di meccaniscmi di evidenziazione automatica di nuovi dispositivi connessi																					
T3 Esistenza di meccanismi di controllo della comunicazione fra nodi della rete																					
T4 Utilizzo di protocolli protetti sulla rete																					
T5 Utilizzo di rete wireless per il collegamento dei dispositivi																					
T6 Esistenza di rete wireless accessibile ad ospiti separata dalla rete operativa																					
T7 Presenza di soluzioni per il rilevamento e rimozione automatica software pericoloso																					
T8 Possibilità di comunicazioni autonome con l'esterno																					
T9 Amministrazione remota dispositivi																					
T10 Continuità operativa nelle aree critiche																					
a. esclusivamente rispetto al sistema informativo																					
b. anche relativamente ai dispositivi centralizzati		+			+	+	+					+			+	+				+	
c. anche relativamente ai dispositivi condivisi		++			++	++	++					++			++	++				++	
d. anche relativamente ai dispositivi individuali		+++			+++	+++	+++					+++			+++	+++				+++	
T11 Continuità operativa per tutte le attività clinico-assistenziali																					
a. esclusivamente rispetto al sistema informativo																					
b. anche relativamente ai dispositivi centralizzati		+			+	+	+					+			+	+				+	
c. anche relativamente ai dispositivi condivisi		++			++	++	++					++			++	++				++	
d. anche relativamente ai dispositivi individuali		+++			+++	+++	+++					+++			+++	+++				+++	

4.8. Scenari

4.8.1 Tipologie

Oltre a questi aspetti, va anche tenuto conto dello scenario in cui opera la struttura, in particolare se effettua attività al di fuori della stessa e/o in collaborazione con le altre strutture sul territorio.

L'individuazione di queste situazioni è rilevante in quanto attività effettuate al di fuori della struttura sono più difficilmente strutturabili e controllabili sia dal punto di vista organizzativo che tecnologico.

In questa ottica si possono individuare tre scenari caratteristici.

S1. Presenza di processi assistenziali e/o di cura domiciliari, per la cui attuazione il personale preposto fa uso di dispositivi medici

Implicazioni sui fattori di rischio

- Ai fini della protezione dei dati e della sicurezza del processo sono rilevanti le caratteristiche degli strumenti e dei dispositivi utilizzati nel processo domiciliare, sia per quanto riguarda la disponibilità di informazioni generali sul paziente (specialmente nel caso di processi di cura) sia relativamente alla gestione dei risultati:
  a. registrati su supporti cartacei per poi essere consultati e/o registrati su un sistema informatico;
  b. registrati temporaneamente sugli strumenti ed i dispositivi utilizzati e poi trasferiti nel sistema complessivo al termine del turno di lavoro (in tal caso è necessario prevedere procedure per la cancellazione di dati personali che rimangano stabilmente registrati su dispositivi e strumentazione (es. PC) mobile;
  c. non registrati localmente ma direttamente integrati su un sistema centralizzato condiviso.

- In caso di comunicazione remota con il sistema informatico, ai fini della sicurezza e della protezione dei dati sono rilevanti i meccanismi di protezione delle comunicazioni

- Ai fini dell'affidabilità dei dati e, quindi, della sicurezza del paziente è rilevante la facilità d'uso dei dispositivi ed il livello di formazione del personale coinvolto

S2. Presenza di processi assistenziali e/o di cura basati sulla collaborazione sul territorio con altre strutture

Implicazioni sui fattori di rischio

- Ai fini della protezione dei dati e della sicurezza del processo sono rilevanti i metodi di trasmissione e condivisione delle informazioni di interesse:
  a. mediante supporti cartacei,
     L'utilizzo di supporti cartacei incide sul rischio di errore ed incompletezza delle informazioni

  b. mediante comunicazione informatica,
     In caso di utilizzo di comunicazione informatica è rilevante il livello di protezione del canale di comunicazione e -ai fini della sicurezza del paziente- la quantità e la tipologia di informazioni trasmesse

  c. mediante accesso a sistemi informatici condivisi
     Nel caso di accesso a sistemi informativi condivisi, sono rilevanti le modalità di accesso e autenticazione, i privilegi concessi, la disponibilità delle risorse, ecc. così come le modalità di protezione attuate per controllare il processo

  L'utilizzo di supporti cartacei incide sul rischio di errore ed incompletezza delle informazioni
  In caso di utilizzo di comunicazione informatica è rilevante il livello di protezione del canale di comunicazione e -ai fini della sicurezza del paziente- la quantità e la tipologia di informazioni trasmesse
  Nel caso di accesso a sistemi informativi condivisi, sono rilevanti le modalità di accesso e autenticazione, i privilegi concessi, la disponibilità delle risorse, ecc. così come le modalità di protezione attuate per controllare il processo

S3. Presenza di processi assistenziali e/o di cura basati sulla telemedicina

Implicazioni sui fattori di rischio

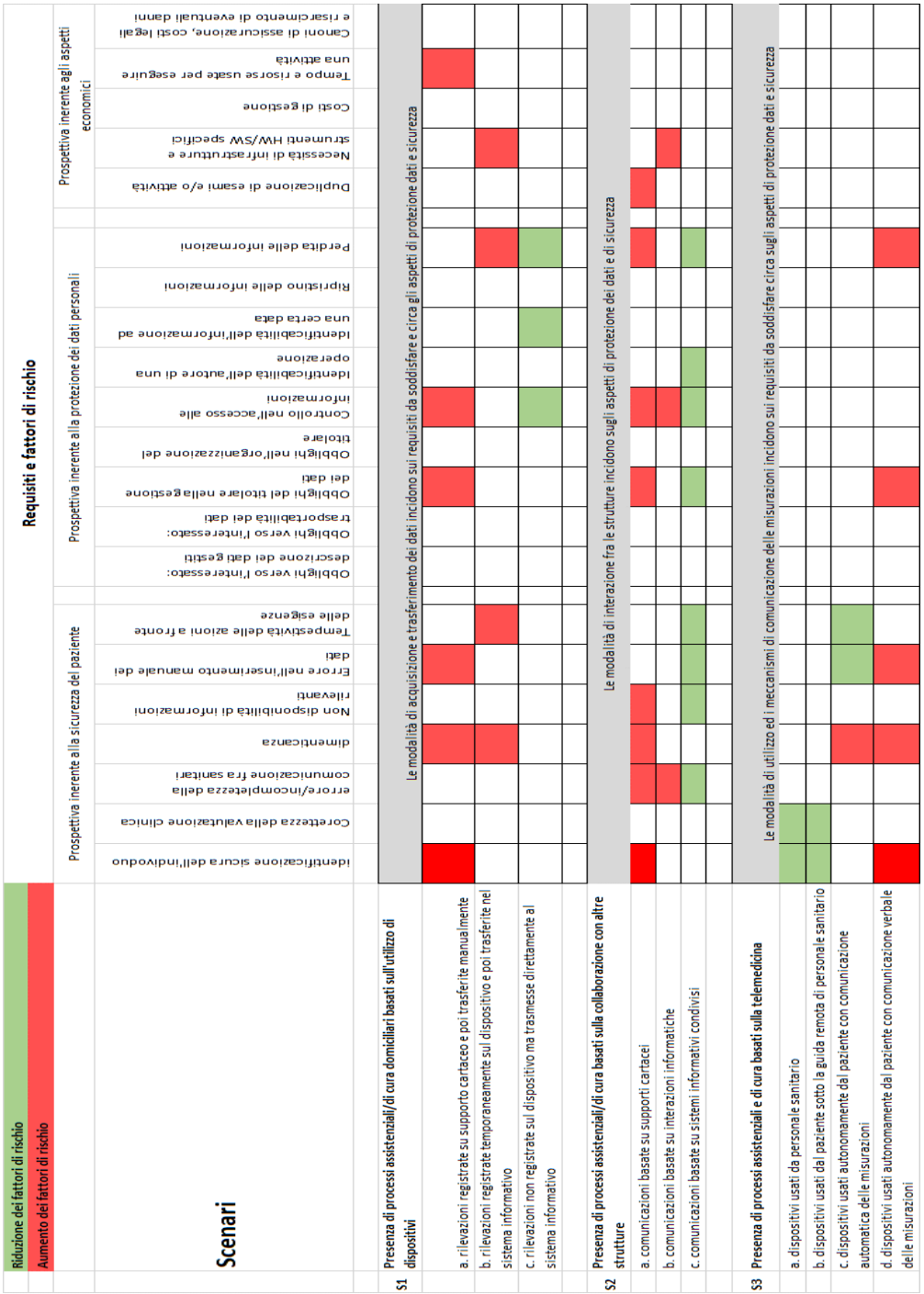
Ai fini della protezione dei dati e della sicurezza del processo sono rilevanti le modalità di utilizzo dei dispositivi e di comunicazione delle rilevazioni effettuate

a. Dispositivi usati da personale sanitario
b. Dispositivi usati dal paziente sotto la guida remota del personale sanitario
c. Dispositivi usati autonomamente dal paziente, con comunicazione automatica
d. Dispositivi usati autonomamente dal paziente, con comunicazione manuale (verbale o cartacea)

- Se usati direttamente ed autonomamente dal paziente la facilità d'uso e la capacità del paziente all'utilizzo del sistema incidono sul rischio di errore nella misurazione e, di conseguenza, sulla attendibilità del dato

- Il rischio in termini di affidabilità dell'informazione si accresce se la comunicazione della misurazione viene effettuata manualmente dal paziente.
- In caso di comunicazione automatica, incidono sui fattori di rischio gli aspetti tecnologici, la protezione del canale di comunicazione e la presenza di protocolli che assicurino l'effettiva ricezione dei dati trasmessi da parte del centro

4.8.2 Implicazioni sui fattori di rischio



5. Modello di maturità nella analisi e gestione della sicurezza dei dispositivi medici connessi con il sistema informativo

5.1 Organizzazione del modello

Il modello ha l'obiettivo di individuare un quadro complessivo delle modalità secondo cui l'azienda affronta le diverse problematiche inerenti alla sicurezza ed alla protezione dei dati nei dispositivi medici.

Simmetricamente rispetto alle tipologie di indicatori definiti, il modello si articola secondo le seguenti prospettive:

- **Prospettiva organizzativa**
  analizza le caratteristiche secondo cui è organizzata l'azienda dal punto di vista della valutazione, del controllo e della gestione dei rischi, sia a livello preventivo che in caso di incidenti

- **Prospettiva implementativa, suddivisa in aspetti funzionali ed informativi**
  analizza le caratteristiche del contesto dei dispositivi medici sotto il profilo delle operatività attualmente implementate nel supporto ai processi assistenziali, sia dal punto di vista funzionale che sotto il profilo della gestione e della protezione dei dati.

- **Prospettiva tecnologica**
  analizza le caratteristiche strutturali ed operative della infrastruttura tecnologica di supporto ai dispositivi medici nell'ambito del sistema informativo

Per ogni prospettiva sono stati definiti quattro livelli - dal valore 0 al valore 3- secondo una scala crescente di in cui 0 indica uno stato iniziale e 3 lo scenario più avanzato e, di conseguenza, più maturo e completo in termini di sicurezza.

Molto sinteticamente, gli scenari corrispondenti ad i singoli livelli sono descritti nel seguito.

Livello 0 - Preliminare

Denota un contesto in cui le problematiche inerenti all'integrazione dei dispositivi medici con il sistema informativo e di supporto all'operatività nonché la protezione dei dati sono ancora affrontate separatamente nei vari contesti operativi, secondo criteri e soluzioni frammentate per i singoli dispositivi (essenzialmente quelli centralizzati), senza una visione integrata nell'azienda e delle diverse prospettive del rischio.

Livello 1 - Iniziale

Denota un contesto in cui l'azienda dimostra sensibilità e di aver cominciato ad affrontare in modo organico le problematiche inerenti all'integrazione e la protezione dei dati nel collegamento con i dispositivi medici.
Le conseguenti caratteristiche operative sono però ancora ancora ad uno stato iniziale, circoscritte ad un numero limitato di settori e di processi, principalmente per quanto riguarda i dispositivi centralizzati. L'infrastruttura tecnologica presenta fattori di elevata criticità.

Livello 2 - Intermedio

Denota un contesto in cui l'azienda dimostra di affrontare in modo organico le problematiche inerenti la sicurezza e la protezione dei dati nella gestione dei dispositivi medici integrati con il sistema informativo.
L'organizzazione della gestione è omogenea e sono presenti caratteristiche implementative in grado di contribuire alla sicurezza dei dati e dei processi anche mediante la centralizzazione di informazioni, regole e funzionalità.
Il contesto presenta tuttavia ancora fattori di rischio non trascurabili: le attività di gestione e controllo sono focalizzate sui dispositivi centralizzati e -non totalmente- sui dispositivi condivisi, una elevata percentuale di dati permane stabilmente sui dispositivi condivisi (senza particolari misure di protezione) e l'infrastruttura di comunicazione presenta ancora alcuni aspetti di criticità.

Livello 3 - Avanzato

Denota un contesto in cui l'azienda affronta in modo organico le problematiche inerenti la sicurezza, tenendo in forte considerazione anche le problematiche relative al supporto integrato a processi clinici ed operando secondo un approccio propositivo, di monitoraggio, pianificazione e di continuo miglioramento.

La gestione dei dispositivi centralizzati e condivisi, ed -in parte- anche di quelli individuali avviene secondo criteri omogenei, sia pur a livello implementativo diverso nei diversi settori.

Sono presenti (sia pur a livello diverso nei vari contesti) caratteristiche implementative e procedure operative in grado di contribuire alla sicurezza dei processi ed alla protezione dei dati, anche mediante la centralizzazione di informazioni, regole e funzionalità di uso comune, l'esistenza di meccanismi di protezione sui singoli dispositivi. L'infrastruttura tecnologica di comunicazione non presenta elementi di particolare criticità.

Sono inoltre presenti meccanismi proattivi per l'evidenziazione automatica di situazioni di rilevanza e per la prevenzione del rischio sia a livello funzionale che tecnologico.

5.2 Aspetti qualificanti dei vari livelli

5.2.1 Livello "0": Preliminare

Dal punto di vista organizzativo

- Non esiste una funzione aziendale (es. UO) esplicitamente preposta alla sicurezza del sistema nel suo complesso; come spesso accade nelle piccole organizzazioni, il tema è affidato al solo responsabile complessivo del sistema informativo;
- Non si rileva collaborazione con il Rischio Clinico anche perché difficilmente sono presenti procedure strutturate e tanto meno piani periodici e puntuali di valutazione dei rischi e relativi piani di mitigazione e miglioramento;
- Questo comporta un incremento dei rischi dovuto alla mancanza di raccomandazioni di sicurezza durante l'installazione di nuovi elementi, meccanismi di monitoraggio e non diffusione delle credenziali, protezione dai malware, ecc.
- L'attenzione dell'organizzazione è centrata quasi esclusivamente sugli obblighi di legge.

Dal punto di vista implementativo (informativo e funzionale)

- L'identificazione certa del paziente e l'associazione delle informazioni al suo percorso clinico sono scarsamente garantite;
- Le modalità operative a questo livello sono tipicamente manuali tramite supporti cartacei, lasciando sui dispositivi grandi quantità di dati privi di protezione e mancano meccanismi di segnalazione degli allarmi;
- Escludendo (parzialmente) i sistemi centralizzati, per apparecchiature e dispositivi mancano quelle caratteristiche fondamentali richieste

dalle Misure Minime di Sicurezza AgID quali la gestione centralizzata delle credenziali e dei profili di utenza, la protezione da accessi non autorizzati nonché il tracciamento delle loro attività anche riguardo alla integrità del dato stesso.

Dal punto di vista tecnologico

- Mancano meccanismi (più o meno automatici) per l'enumerazione, l'identificazione e l'autorizzazione dei dispositivi durante l'accesso alla rete anche se esplicitamente richiesto dalle Misure Minime di Sicurezza AgID;
- Mancano anche meccanismi di protezione basati sulla segmentazione di rete e/o i protocolli di comunicazione sicura;
- L'infrastruttura tecnologica e tipicamente piatta e tecnologicamente poco evoluta;
- In genere mancano anche meccanismi di protezione contro gli attacchi e di rimozione dei software malevoli;
- I tempi di ripristino (anche parziale) dell'operatività della struttura sono elevati;
- Tutto questo comporta grosse difficoltà nel garantire continuità di esercizio sia in caso di incidenti che di guasti.

5.2.2 Livello "1": Iniziale

Dal punto di vista organizzativo

- Non esiste una funzione aziendale (es. UO) esplicitamente preposta alla sicurezza del sistema nel suo complesso; come spesso accade nelle piccole organizzazioni, il tema è affidato al solo responsabile complessivo del sistema informativo;
- Non si rileva collaborazione con il Rischio Clinico,
- Sono parzialmente presenti procedure strutturate, piani periodici e puntuali di valutazione dei rischi e relativi piani di mitigazione e miglioramento per il sistema informativo e i dispositivi centralizzati. Rimane scoperto il perimetro dei dispositivi minori;
- Il livello di rischio rimane abbastanza elevato a causa della non totale definizione di procedure di sicurezza durante l'installazione di nuovi elementi, di meccanismi di monitoraggio e non diffusione delle credenziali, protezione sistematica dai malware, ecc.
- L'attenzione dell'organizzazione continua ad essere centrata sugli obblighi di legge soprattutto riguardo al sistema informativo e i dispositivi centralizzati ma lascia ancora scoperta l'area dei dispositivi condivisi ed individuali.

Dal punto di vista implementativo (informativo e funzionale)

- L'identificazione certa del paziente e l'associazione delle informazioni al suo percorso clinico sono in parte garantite;

- Le modalità operative a questo livello sono caratterizzate da un sostanziale grado di manualità e dall'uso di supporti cartacei, lasciando ancora sui dispositivi una discreta quantità di dati privi di protezione e scarsi meccanismi di segnalazione degli allarmi;
- Per i sistemi informativi e dispositivi centralizzati, le caratteristiche fondamentali richieste dalle Misure Minime di Sicurezza AgID quali la gestione centralizzata delle credenziali e dei profili di utenza, la protezione da accessi non autorizzati nonché il tracciamento delle loro attività anche riguardo alla integrità del dato stesso vengono sostanzialmente rispettate mentre per i dispositivi condivisi e individuali il livello di attenzione è ancora insufficiente;

Dal punto di vista tecnologico

- Esistono meccanismi per l'enumerazione degli apparati come esplicitamente richiesto dalle Misure Minime di Sicurezza AgID, ma non quegli automatismi per il loro aggiornamento né per l'identificazione e l'autorizzazione dei dispositivi durante l'accesso alla rete;
- Mancano anche meccanismi di protezione basati sulla segmentazione di rete e i protocolli di comunicazione sicura;
- L'infrastruttura tecnologica è tipicamente piatta e tecnologicamente poco evoluta;
- In genere mancano anche meccanismi di protezione contro gli attacchi e di rimozione dei software malevoli;
- I tempi di ripristino (anche parziale) dell'operatività della struttura sono mediamente elevati;
- Tutto questo comporta ancora discrete difficoltà nel garantire continuità di esercizio sia in caso di incidenti che di guasti.

5.2.3 Livello "2": Intermedio

Dal punto di vista organizzativo

- Esiste una funzione aziendale preposta alla sicurezza del sistema informativo, ma non quella preposta ai dispositivi. Spesso questa realtà può essere riscontrata in organizzazioni di dimensione medio/grande dove il tema viene affrontato da un gruppo di persone.
- È definita la collaborazione con il Rischio Clinico poiché sono presenti procedure strutturate e piani periodici e puntuali di valutazione dei rischi e, in genere, anche i relativi piani di mitigazione e miglioramento del sistema informativo e dei principali dispositivi;
- Questo comporta una diminuzione dei rischi grazie all' applicazione delle principali raccomandazioni di sicurezza durante l'installazione di nuovi elementi, meccanismi di monitoraggio e non diffusione delle credenziali, protezione dai malware, ecc.
- L'attenzione dell'organizzazione riguardo agli obblighi di legge viene estesa fino ai dispositivi condivisi, tralasciando gli individuali.

Dal punto di vista implementativo

- L'identificazione certa del paziente e l'associazione delle informazioni al suo percorso clinico sono generalmente garantite;
- Le modalità operative a questo livello cominciano ad essere attuate mediante trasferimento dei dati via rete, lasciando, però, sui dispositivi ancora una discreta quantità di dati privi di protezione e buoni meccanismi di segnalazione degli allarmi;
- Per i sistemi informativi e tutti i dispositivi (anche se non totalmente per quelli individuali), esistono quelle caratteristiche fondamentali richieste dalle Misure Minime di Sicurezza AgID quali la gestione centralizzata delle credenziali e dei profili di utenza, la protezione da accessi non autorizzati nonché il tracciamento delle loro attività anche riguardo alla integrità del dato stesso

Dal punto di vista tecnologico

- Esistono meccanismi per l'enumerazione degli apparati come esplicitamente richiesto dalle Misure Minime di Sicurezza AgID, ma non quegli automatismi per il loro aggiornamento né per l'identificazione e l'autorizzazione dei dispositivi durante l'accesso alla rete;
- Esistono meccanismi di protezione basati sulla segmentazione di rete e vengono utilizzati i protocolli di comunicazione sicura;
- L'infrastruttura tecnologica inizia a garantire la separazione e segregazione dei sistemi e degli apparati poiché tecnologicamente più evoluta;
- Esistono anche meccanismi di protezione contro gli attacchi e di rimozione dei software malevoli seppur non totalmente diffusi e automatizzati;

5.2.4 Livello "3": Avanzato

Dal punto di vista organizzativo

- Esiste una funzione aziendale preposta alla sicurezza del sistema informativo e anche una preposta ai dispositivi di ogni categoria (eventualmente coincidenti, ma con esplicita definizione degli ambiti di responsabilità);
- La collaborazione tra Sicurezza e Rischio Clinico è consolidata da procedure strutturate, piani periodici e puntuali di valutazione dei rischi e relativi piani di mitigazione e miglioramento;
- Questo riduce i rischi grazie all'applicazione di tutte le raccomandazioni di sicurezza durante l'installazione di nuovi elementi, meccanismi di monitoraggio e non diffusione delle credenziali, protezione dai malware, ecc.
- L'organizzazione è conforme agli obblighi di legge sull'intero perimetro dei sistemi e dei dispositivi.

Dal punto di vista implementativo

- L'identificazione certa del paziente e l'associazione delle informazioni al suo percorso clinico sono completamente garantite;
- Le modalità operative di questo livello sono attuate completamente tramite trasferimento via rete, lasciando sui dispositivi una quantità minima, se non inesistente, di dati privi di protezione e ottimi meccanismi di segnalazione degli allarmi;
- Per i sistemi informativi e tutti i dispositivi, esistono quelle caratteristiche fondamentali richieste dalle Misure Minime di Sicurezza AgID quali la gestione centralizzata delle credenziali e dei profili di utenza, la protezione da accessi non autorizzati nonché il tracciamento delle loro attività anche riguardo alla integrità del dato stesso

Dal punto di vista tecnologico

- Esistono meccanismi automatici per l'enumerazione degli apparati, la loro identificazione e l'autorizzazione dei dispositivi durante l'accesso alla rete così come esplicitamente richiesto dalle Misure Minime di Sicurezza AgID;
- Esistono meccanismi di protezione basati sulla segmentazione di rete e vengono utilizzati i protocolli di comunicazione sicura;
- L'infrastruttura tecnologica garantisce la separazione e la segregazione dei sistemi e degli apparati poiché tecnologicamente più evoluta;
- Esistono anche meccanismi di protezione contro gli attacchi e di rimozione dei software malevoli e sono totalmente diffusi e automatizzati;
- I tempi di ripristino totale (o parziale) dell'operatività della struttura sono bassi;
- La continuità di esercizio sia in caso di incidenti che di guasti è totalmente garantita.

5.3. Check-list degli indicatori relativi ai vari livelli

Al fine di facilitare e di rendere più oggettivo e misurabile il processo di identificazione del livello di maturità, i valori assegnati agli indicatori sono di tipo binario (*SI/ NO/ Parziale*) o qualitativi relativi al contesto specifico (*Alto/ Medio/ Basso*).

Per quanto questo possa risultare limitante in alcuni casi, per gli scopi del progetto rappresentano comunque un adeguato indice di evoluzione e di miglioramento o di regressione del sistema di supporto informatico e degli apparati ad esso collegati (considerando le tecnologie implementate).

5.3.1 Aspetti organizzativi

Aspetti organizzativi		SI / NO / PA(rziale)	Livello 0	Livello 1	Livello 2	Livello 3
O1	Esistenza di funzione aziendale preposta alla sicurezza del sistema informativo	SI / NO	NO	NO	SI	SI
O2	Esistenza di funzione aziendale preposta alla gestione dei dispositivi	SI / NO	NO	NO	SI	SI
O3	Formalizzazione della collaborazione fra Sicurezza e Rischio clinico	SI / NO	NO	NO	SI	SI
O4	Valutazione della sicurezza nel sistema informativo e nei dispositivi centralizzati	SI/NO/PA				
	a. esigenze di formazione		NO	PA	SI	SI
	b. facilità d'uso		NO	PA	PA	SI
	c. disponibilità di tutte le informazioni necessarie ai singoli processi		NO	NO	PA	SI
	d. integrazione con il sistema informativo		NO	PA	SI	SI
	e. capacità di evidenziare situazioni anomale e di allarme		NO	PA	SI	SI
	f. esistenza di meccanismi di protezione tecnologica contro attacchi e contro accesso non autorizzato		NO	NO	PA	SI
	g. rispondenza a standard di comunicazione e gestione dati		NO	PA	SI	SI
O5	Valutazione della sicurezza nei dispositivi condivisi e individuali	SI/NO/PA				
	a. esigenze di formazione		NO	NO	PA	SI
	b. facilità d'uso		NO	PA	SI	SI
	c. disponibilità di tutte le informazioni necessarie ai singoli processi		NO	NO	PA	SI
	d. integrazione con il sistema informativo		NO	NO	PA	SI
	e. capacità di evidenziare situazioni anomale e di allarme		NO	PA	SI	SI
	f. esistenza di meccanismi di protezione tecnologica contro attacchi e contro accesso non autorizzato		NO	NO	NO	SI
	g. rispondenza a standard di comunicazione e gestione dati		NO	NO	PA	SI
O6	Esistenza di procedure formalizzate per l'individuazione dei rischi	SI/NO/PA				
	- sistema informativo e dispositivi centralizzati		NO	PA	SI	SI
	- dispositivi condivisi		NO	NO	PA	SI
	- dispositivi individuali			NO	NO	PA
O7	Esistenza di procedure formalizzate per la protezione dei dati personali	SI/NO/PA				
	- sistema informativo e dispositivi centralizzati		NO	PA	SI	SI
	- dispositivi condivisi		NO	NO	PA	SI
	- dispositivi individuali			NO	NO	PA
O8	Valutazione rischi preventivamente all'installazione	SI/NO/PA				
	- sistema informativo e dispositivi centralizzati		NO	PA	SI	SI
	- dispositivi condivisi		NO	NO	PA	SI
	- dispositivi individuali			NO	PA	SI
O9	Attuazione di verifiche periodiche rischi e sicurezza	SI/NO/PA				
	- sistema informativo e dispositivi centralizzati		NO	PA	SI	SI
	- dispositivi condivisi		NO	NO	PA	SI
	- dispositivi individuali			NO	PA	SI
O10	Presenza di piani periodi di analisi e miglioramento	SI/NO/PA				
	- sistema informativo e dispositivi centralizzati		NO	PA	SI	SI
	- dispositivi condivisi			NO	PA	SI
	- dispositivi individuali				NO	PA
O11	Meccanismi e controlli sulla non diffusione delle credenziali	SI/NO/PA				
	- sistema informativo e dispositivi centralizzati		NO	PA	SI	SI
	- dispositivi condivisi		NO	NO	PA	SI
	- dispositivi individuali			NO	PA	SI
O12	Procedure di monitoraggio e tracciamento incidenti (obbligo di legge da 6/2018)	SI/NO/PA				
	- sistema informativo e dispositivi centralizzati		PA	SI	SI	SI
	- dispositivi condivisi			PA	SI	SI
	- dispositivi individuali				PA	SI
O13	Esistenza di un team di pronto intervento in caso di incidenti	SI/NO/PA				
	- sistema informativo e dispositivi centralizzati		NO	PA	SI	SI
	- dispositivi condivisi			NO	PA	SI
	- dispositivi individuali				NO	PA

5.3.2 Aspetti implementativi (caratteristiche informative)

Aspetti implementativi (informativi)		Alto / Medio / Basso	Livello 0	Livello 1	Livello 2	Livello 3
I1	Quantità (percentuale) dei dati acquisiti dai dispositivi che vengono integrati nel sistema informativo	A / M / B				
	- *dispositivi centralizzati*		B	M	A	A
	- *dispositivi condivisi*		B	B	M	A
	- *dispositivi individuali*			B	B	M
I2	Trasferimento via rete al sistema informativo dei dati acquisiti dai dispositivi	A / M / B				
	- *dispositivi centralizzati*		B	M	A	A
	- *dispositivi condivisi*			B	M	A
	- *dispositivi individuali*				B	M
I3	Percentuale di dati rimanenti registrati stabilmente sul dispositivo	A / M / B				
	- *dispositivi centralizzati*		A	M	B	B
	- *dispositivi condivisi*		A	M	M	B
	- *dispositivi individuali*			A	M	M
I4	Esistenza di meccanismi di crittografazione dati	A / M / B				
	- *sistema informativo*		B	M	A	A
	- *dispositivi centralizzati*		B	M	M	A
	- *dispositivi condivisi*			B	M	A
	- *dispositivi individuali*				B	M
I5	Esistenza di meccanismi di segnalazione di situazioni di allarme	A / M / B				
	- *sistema informativo*		B	M	A	A
	- *dispositivi centralizzati*		B	M	M	A
	- *dispositivi condivisi*			B	M	A
	- *dispositivi individuali*				B	M

5.3.3 Aspetti implementativi (caratteristiche funzionali)

Aspetti implementativi (funzionali)		Alto / Medio / Basso		Livello 0	Livello 1	Livello 2	Livello 3
F1	Esistenza di meccanismi di identificazione certa della persona	A / M / B					
	- sistema informativo			B	M	A	A
	- dispositivi centralizzati			B	M	M	A
	- dispositivi condivisi				B	M	A
	- dispositivi individuali					B	M
F2	Gestione centralizzata credenziali di accesso (previsto dalle misure AGID)	A / M / B					
	- sistema informativo			M	A	A	A
	- dispositivi centralizzati			B	M	A	A
	- dispositivi condivisi			B	M	M	A
	- dispositivi individuali				B	M	A
F3	Gestione centralizzata profili di abilitazione (previsto dalle misure AGID)	A / M / B					
	- sistema informativo			M	A	A	A
	- dispositivi centralizzati			B	M	A	A
	- dispositivi condivisi			B	M	M	A
	- dispositivi individuali				B	M	A
F4	Blocco automatico delle sessioni in caso di inattività	A / M / B					
	- sistema informativo			B	M	A	A
	- dispositivi centralizzati			B	M	A	A
	- dispositivi condivisi			B	B	M	A
	- dispositivi individuali				B	M	A
F5	Log delle attività utente (previsto dalle misure AGID)	A / M / B					
	- sistema informativo			M	A	A	A
	- dispositivi centralizzati			B	M	A	A
	- dispositivi condivisi			B	M	M	A
	- dispositivi individuali				B	M	A
F6	Tracciamento delle modifiche ai singoli dati	A / M / B					
	- sistema informativo			B	M	A	A
	- dispositivi centralizzati			B	M	M	A
	- dispositivi condivisi				B	M	A
	- dispositivi individuali					B	M

5.3.4 Aspetti tecnologici

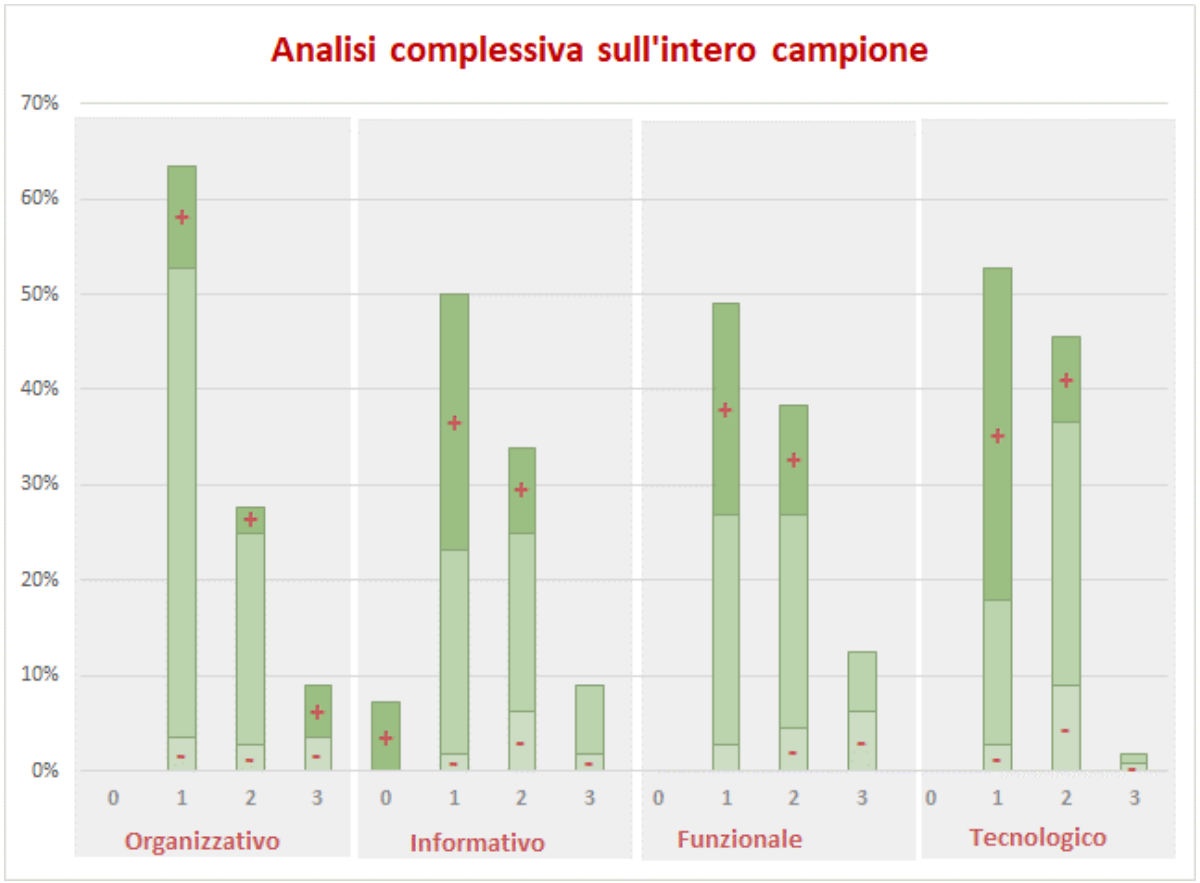
Aspetti tecnologici		Alto / Medio /	Livello 0	Livello 1	Livello 2	Livello 3
T1	Presenza di un inventario di tutte le apparecchiature autorizzate	SI / NO	NO	SI	SI	SI
T2	Esistenza di meccanismi di evidenziazione automatica di nuovi dispositivi connessi	SI / NO	NO	NO	NO	SI
T3	Esistenza di meccanismi di controllo della comunicazione fra nodi della rete	SI / NO	NO	NO	SI	SI
T4	Utilizzo di protocolli protetti sulla rete	A / M / B	NO	NO	SI	SI
T5	Utilizzo di rete wireless per il collegamento dei dispositivi	SI / NO	NO	NO	NO	SI
T6	Esistenza di rete wireless accessibile ad ospiti tramite rete operativa	SI / NO	NO	NO	SI	SI
T7	Rilevamento e rimozione automatica software pericoloso	A / M / B				
	- sistema informativo		B	M	M	A
	- dispositivi centralizzati			B	M	A
	- dispositivi condivisi				M	A
	- dispositivi individuali				B	M
T8	Possibilità di comunicazioni autonome con l'esterno	A / M / B				
	- sistema informativo		A	A	M	B
	- dispositivi centralizzati			A	M	B
	- dispositivi condivisi			A	M	B
	- dispositivi individuali				M	B
T9	Continuità operativa per le attività critiche	SI / NO				
	- sistema informativo		NO	SI	SI	SI
	- dispositivi centralizzati		NO	NO	SI	SI
	- dispositivi condivisi		NO	NO	NO	SI
T10	Continuità operativa per tutte le attività clinico-assistenziali	SI / NO				
	- sistema informativo		NO	SI	SI	SI
	- dispositivi centralizzati		NO	NO	SI	SI
	- dispositivi condivisi		NO	NO	NO	SI

6. Applicazione del modello alle strutture sanitarie che hanno partecipato all'indagine

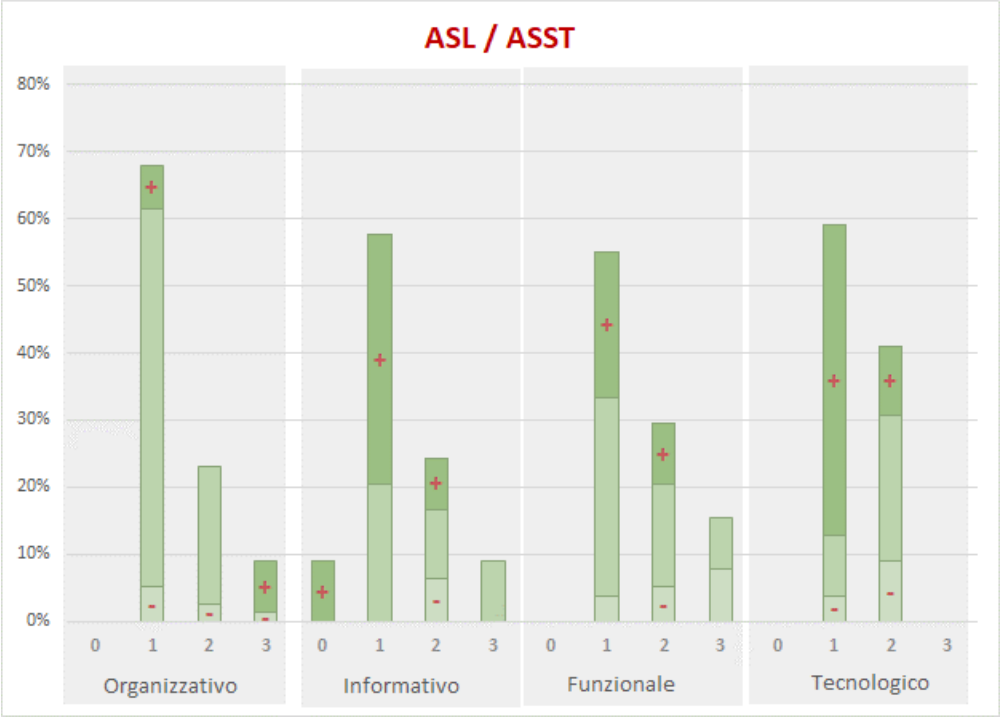
I dati raccolti dai 112 ospedali partecipanti all'indagine sono stati analizzati secondo gli indicatori ed organizzati nell'ambito del modello di maturità.

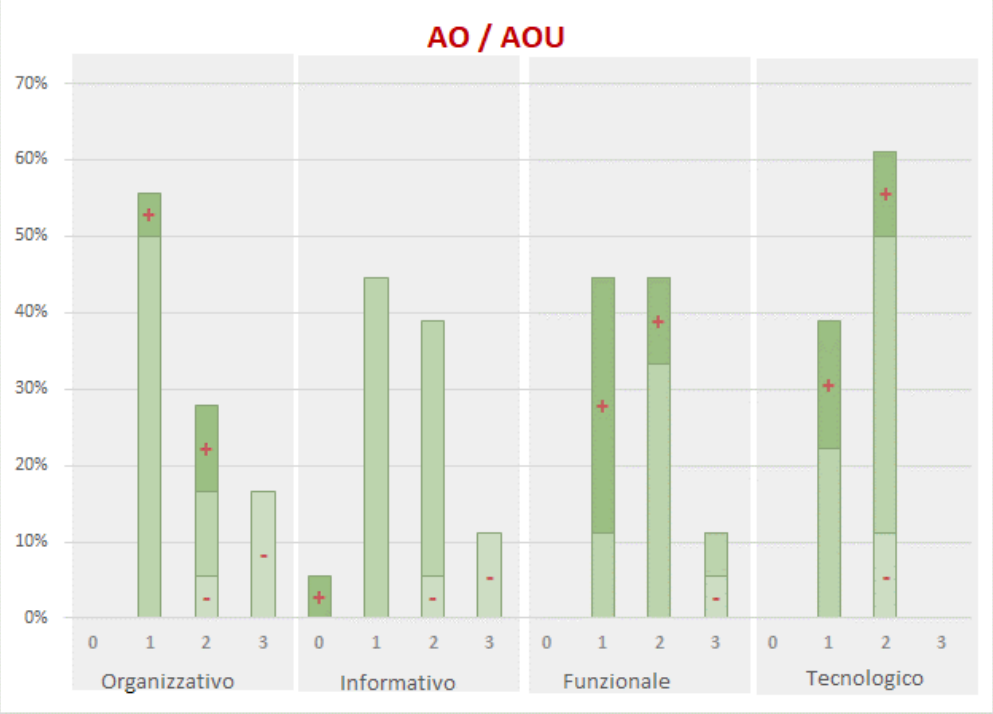
Mediante tale elaborazione (basata, si ripete, su 156 informazioni per ogni ospedale, per un totale di 17.472 dati analizzati) si è ottenuta la classificazione dei livelli di sicurezza nelle strutture sanitarie come rappresentata nei seguenti grafici.

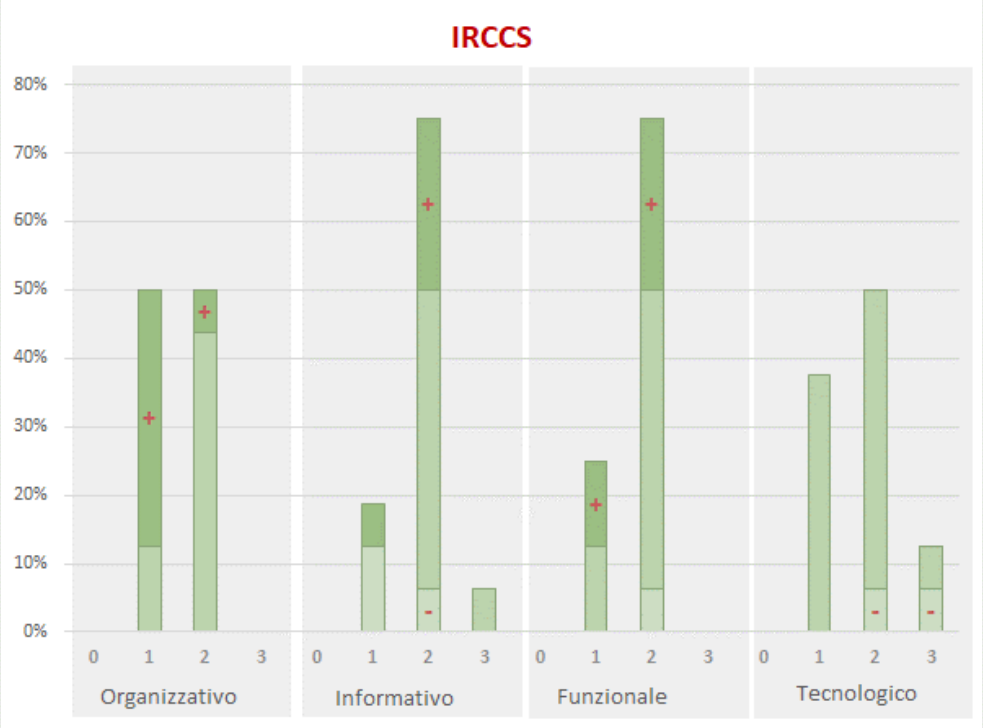
6.1 Classificazione complessiva del campione



6.2 Classificazione per tipologia di azienda sanitaria






IRCCS
80%
70%
60%
50%
40%
30%
20%
10%
0%
0 1 2 3
Organizzativo
0 1 2 3
Informativo
0 1 2 3
Funzionale
0 1 2 3
Tecnologico