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

hisSA health information system Security Assessment MD

La sicurezza nei sistemi informativi sanitari e nei dispositivi medici connessi secondo un approccio di Health Technology Assessment

Fabrizio Massimo Ferrara
Coordinatore del "Laboratorio ALTEMS sui sistemi informativi sanitari per il governo dell'organizzazione"[1]

Abstract

Questo articolo riassume gli aspetti principali dello studio condotto dall'ALTEMS per analizzare, secondo l' approccio multi-dimensionale di Health Technology Assessment, il livello di sicurezza dei dispositivi medici connessi con il sistema informativo nel contesto delle aziende sanitarie italiane e definire un modello di maturità in grado di rappresentare le modalità secondo cui l'azienda affronta le diverse problematiche inerenti alla sicurezza ed alla protezione dei dati nei dispositivi medici. Si rinvia al sito ALTEMS per la versione completa della metodologia e del modello.

Lo studio è stato condotto con la collaborazione di HIMSS Italian Community, e si è avvalso del contributo di:

- Massimo Capponi, IoT
- Massimo Casciello, Direzione generale della vigilanza sugli enti e della sicurezza delle cure, Ministero della Salute
- 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 ALTEMS sui sistemi informativi sanitari

Indice

[1] https://altems.unicatt.it/altems-attivita-di-ricerca-i-sistemi-informativi-sanitari-per-il-governo-dell-organizzazione

L'ecosistema della sicurezza nei sistemi informativi sanitari e dei dispositivi medici connessi

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

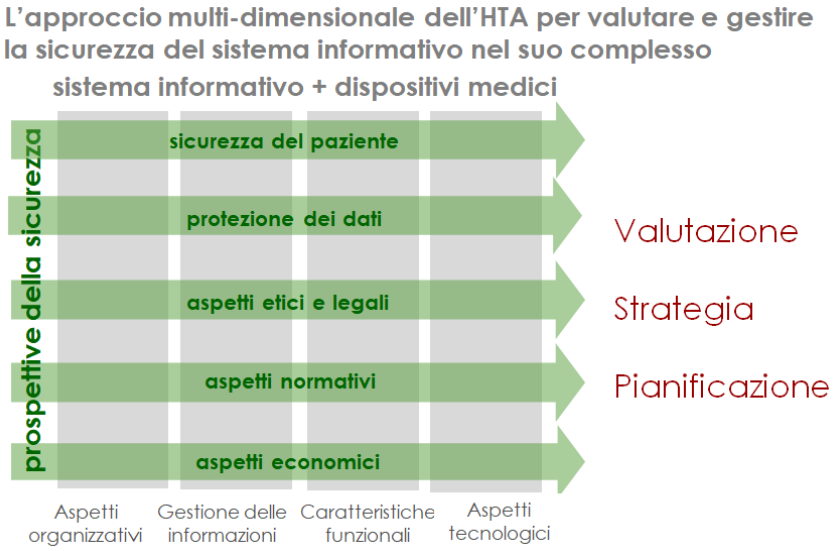
a) di seguire e supportare senza soluzione di continuità i processi dell'organizzazione (sia quelli che si esauriscono all'interno di un singolo settore che –soprattutto– quelli che si articolano attraverso settori diversi e sul territorio),
b) di integrare e proteggere i dati raccolti attraverso applicazioni, 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 deve**

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 2017, 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 -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[1,2], quali il rischio clinico[3], 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[4] 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.

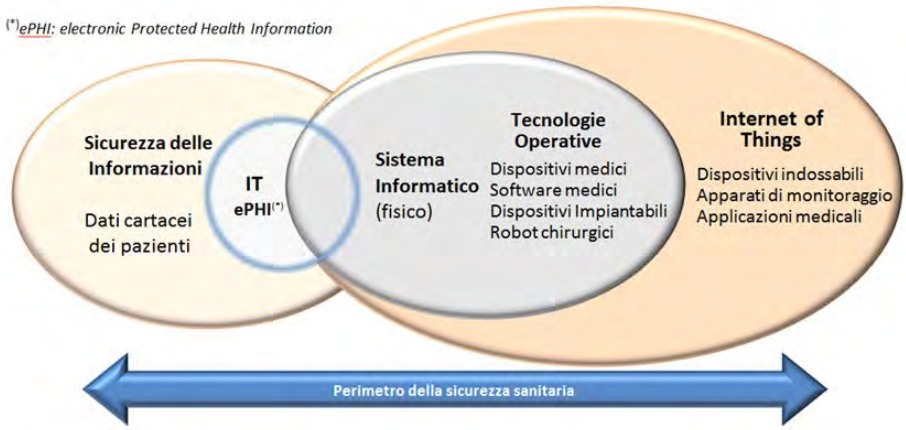
1 Ferrara, "ICT e HTA: il ruolo dell'HTA nella valutazione dei sistemi informativi sanitari"; IX congresso SIHTA, Ottobre 2016
2 Ferrara F.M., Cicchetti A., "I sistemi informativi e l'Health Technology Assessment", Progettare per la Sanità, Novembre 2016
3 Ferrara F.M., Pillon S. "Medicina Digitale –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

La sicurezza nei dispositivi medici connessi

Secondo questo approccio e partendo da questo quadro di validità generale per qualsiasi sistema informativo sanitario, nel 2018 è stato condotto un nuovo studio finalizzato a dettagliare 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 assistenziale e di cura.

Va infatti considerato che sempre di più 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).

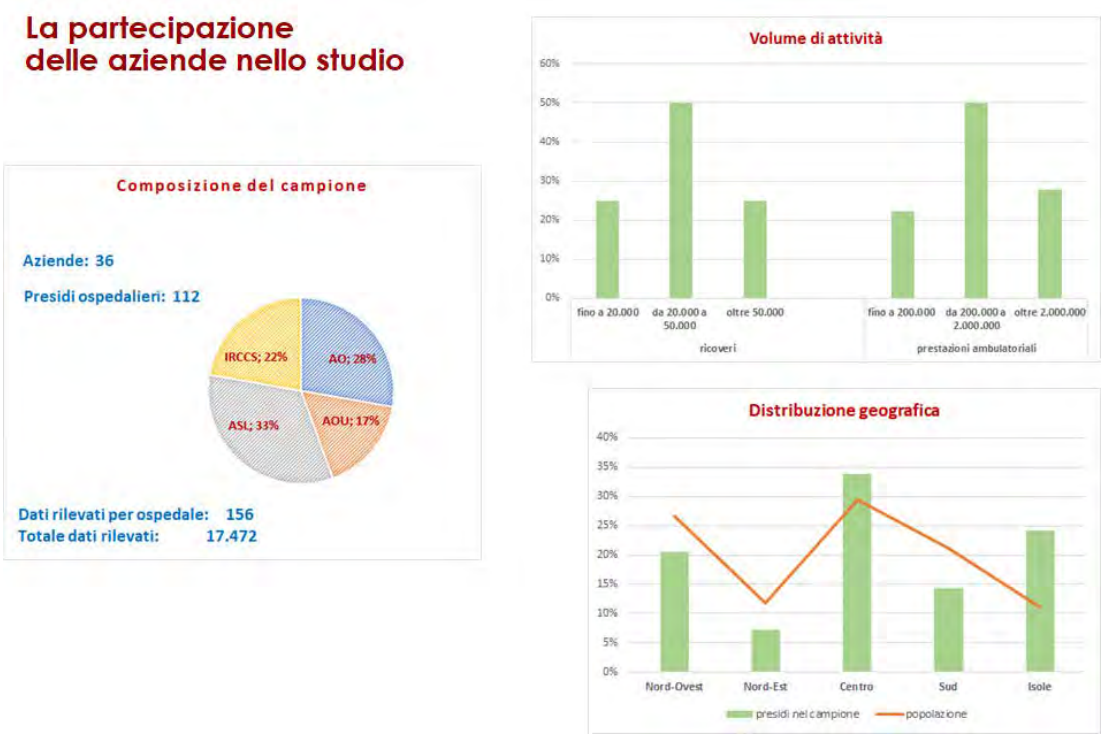
Il contesto del sistema informativo si amplia quindi fino ad includere dispositivi medici, e **la sicurezza complessiva dipende sempre di più dalla sicurezza del binomio "sistema informativo + dispositivi connessi"**, come schematizzato nella seguente figura.



Il progetto è collegato e sinergico alla parallela iniziativa (www.gdpr-sanita.it), promossa da ALTEMS e da 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.

Risultati dell'indagine

Anche per questo secondo studio è stata innanzi tutto effettuata una indagine a livello nazionale che ha coinvolto 112 presidi ospedalieri dalla quasi totalità delle regioni italiane, che hanno fornito informazioni (per un totale di oltre 17.000 dati raccolti) sulle caratteristiche del loro sistema informativo e dei dispositivi medici connessi.



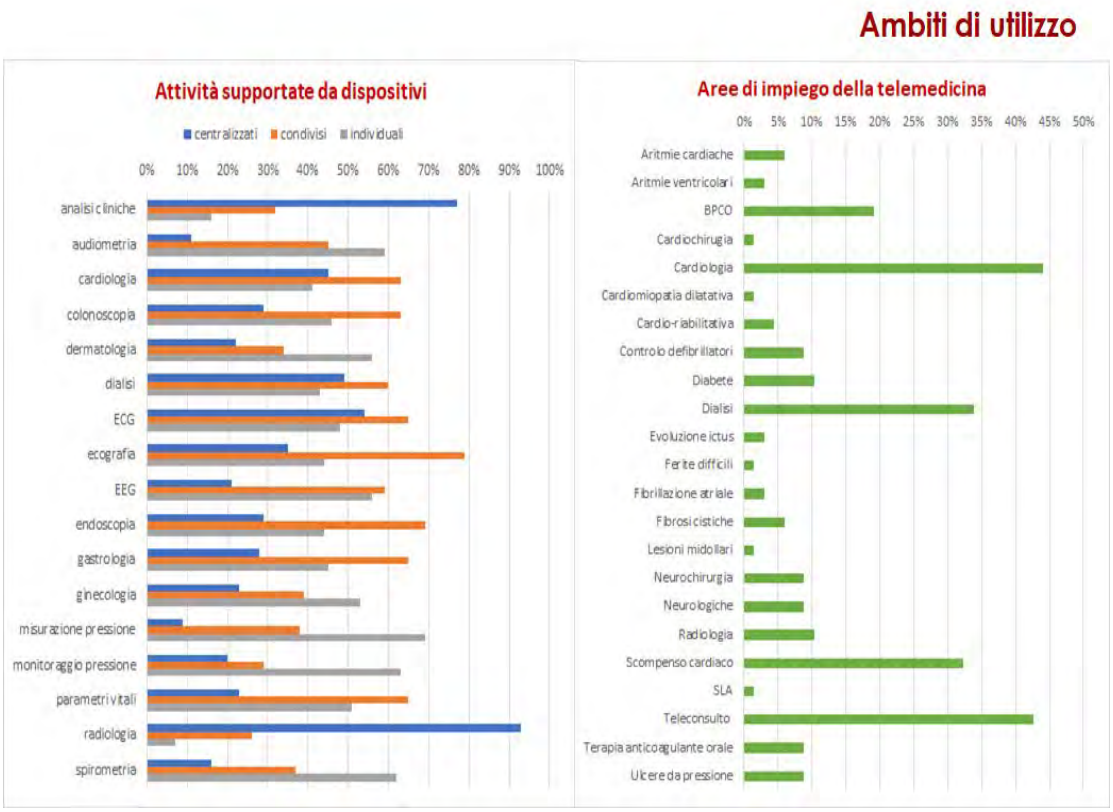
I dispositivi medici connessi presentano una varietà di caratteristiche e di utilizzo estremamente ampia (dal robot operatorio all'IoT). Una analisi indiscriminata di tutti i contesti non porterebbe quindi a risultati significativi. Per consentire la validità generale del modello, indipendente dalle specifiche patologie e processi clinici, i dispositivi sono stati quindi classificati in funzione del loro ruolo all'interno del processo assistenziale e delle modalità di utilizzo nel contesto organizzativo:

- dispositivi "**individuali**": quelle apparecchiature 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.). Rientrano in questo contesto anche i dispositivi genericamente individuati nel "mondo IoT".

- dispositivi "**condivisi**": quelle apparecchiature 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.

- dispositivi "**centralizzati**": quelle 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.

Secondo questi criteri, **i principali ambiti di utilizzo dei dispositivi**, all'interno dell'organizzazione ed in contesti di telemedicina, sono rappresentati nei seguenti grafici.



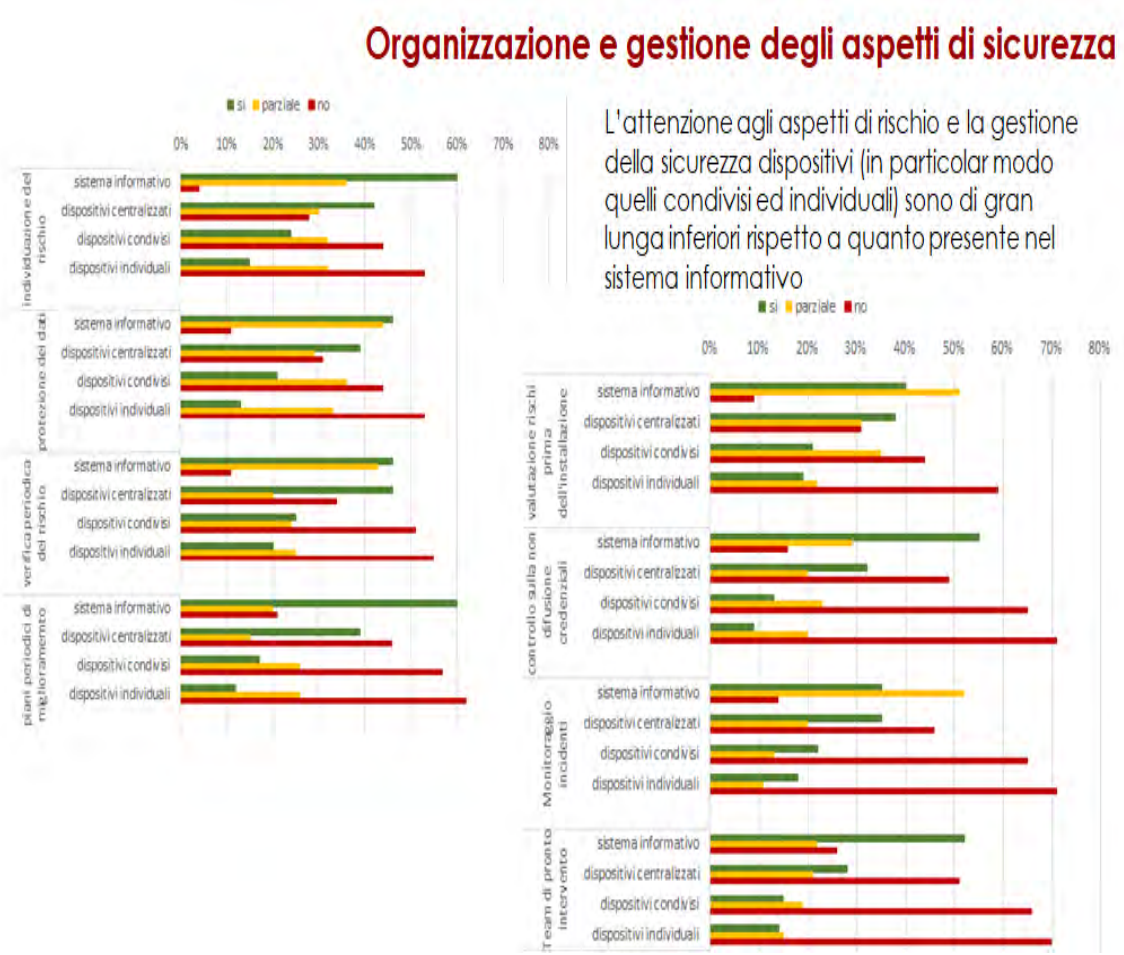
Gli indicatori raccolti mediante l'indagine si riferiscono alle quattro prospettive tipiche di analisi dei sistemi informativi, formalizzate nel modello standard di rifermento ISO ODP 10746: **aspetti organizzativi, aspetti informativi, aspetti funzionali, aspetti tecnologici.**

Dal punto di vista organizzativo, è da osservare come -a livello complessivo- **in circa il 70% dei casi non esista una collaborazione formalizzata** fra le funzioni responsabili della sicurezza del sistema informativo e quelle responsabili del rischio clinico.

Relativamente ai dispositivi, l'attenzione agli aspetti di rischio e la gestione della sicurezza nei dispositivi (in particolar modo quelli condivisi ed individuali) sono di gran lunga inferiori rispetto a quanto presente nel sistema informativo.

Questa situazione è riscontrata relativamente tutte le tipologie di rischio analizzato. In particolare va evidenziato come la diversità dei prodotti e delle tecnologie, insieme alla non integrazione e modalità di gestione frammentata specialmente per quanto riguarda i dispositivi condividi ed individuali, renda molto alta la percentuale dei casi in cui si riscontra anche un forte rischio in **termini di protezione dei dati personali**, in termini di

- assenza di procedure formalizzate a livello organizzativo circa le modalità di comportamento circa i dati stessi,
- assenza di procedure di verifica periodica del rischio
- mancanza di controlli (a volte impossibili, stante la distribuzione logistica dei dispositivi e la loro non integrazione con il resto del sistema) per quanto riguarda la non diffusione di credenziali



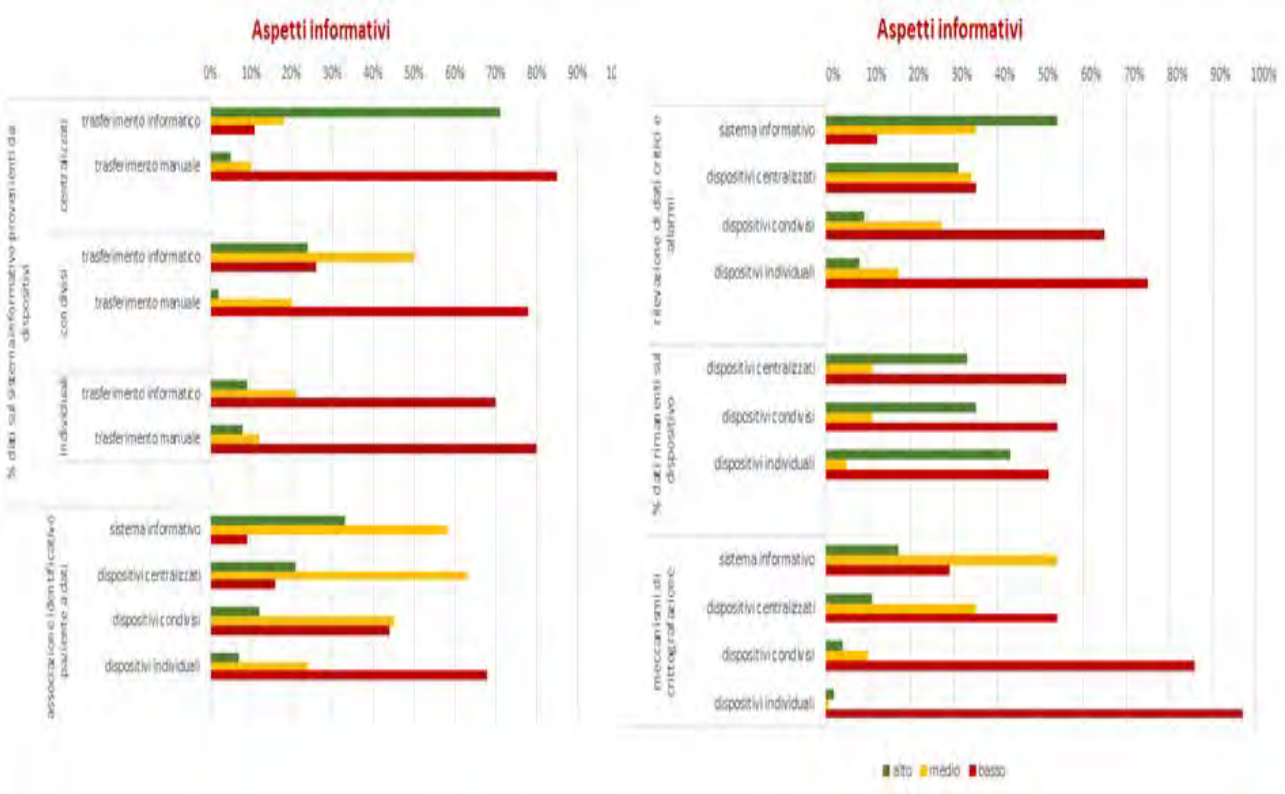
<u>Relativamente alla gestione delle informazioni</u>

Va evidenziato come i **dati acquisiti dai dispositivi** condivisi che vengono **integrati nel sistema informativo siano in quantità nettamente inferiore** di quanto avviene per i dispositivi centralizzati, per **giungere ad una percentuale trascurabile nel caso di dispositivi individuali**.

Parallelamente rimane **alta la percentuale dei dati che rimangono registrati permanentemente sui dispositivi condivisi e individuali**.

Questi aspetti 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.

Inoltre, sui dispositivi condivisi ed individuali **sono poco presenti** meccanismi di associazione sicura dell'identità del paziente ai dati rilevati e funzionalità in grado di evidenziare situazioni di allarme.

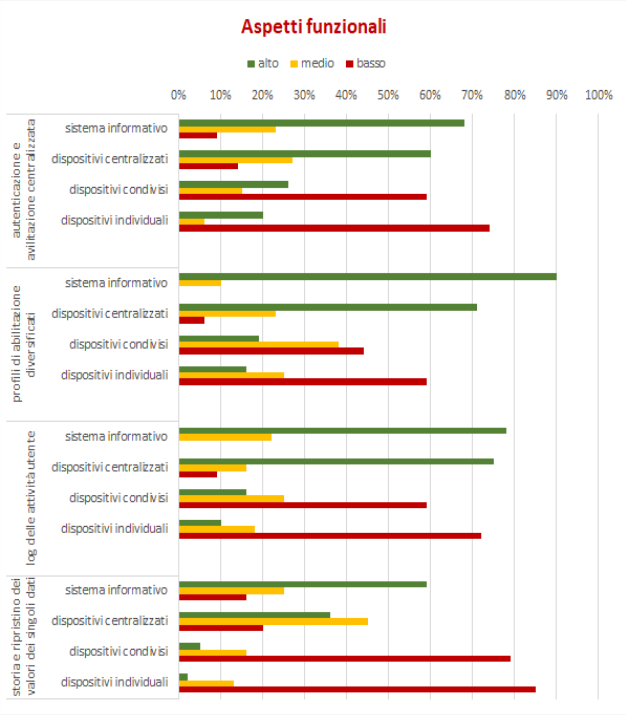


Relativamente agli aspetti funzionali, i dispositivi condivisi ed individuali presentano elevati livelli di rischio nella gestione delle attività e nella protezione e sicurezza dei dati:

- 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).

I dispositivi condivisi ed individuali presentano elevati livelli di rischio nella gestione delle attività e nella protezione e sicurezza dei dati

- E' molto alta l'assenza di meccanismi di autenticazione e di abilitazione centralizzata nell'accesso
- E' 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 (unito al fatto che gran parte delle informazioni rimangono stabilmente registrate sul dispositivo)



Per quanto riguarda le caratteristiche dell'infrastruttura tecnologica:

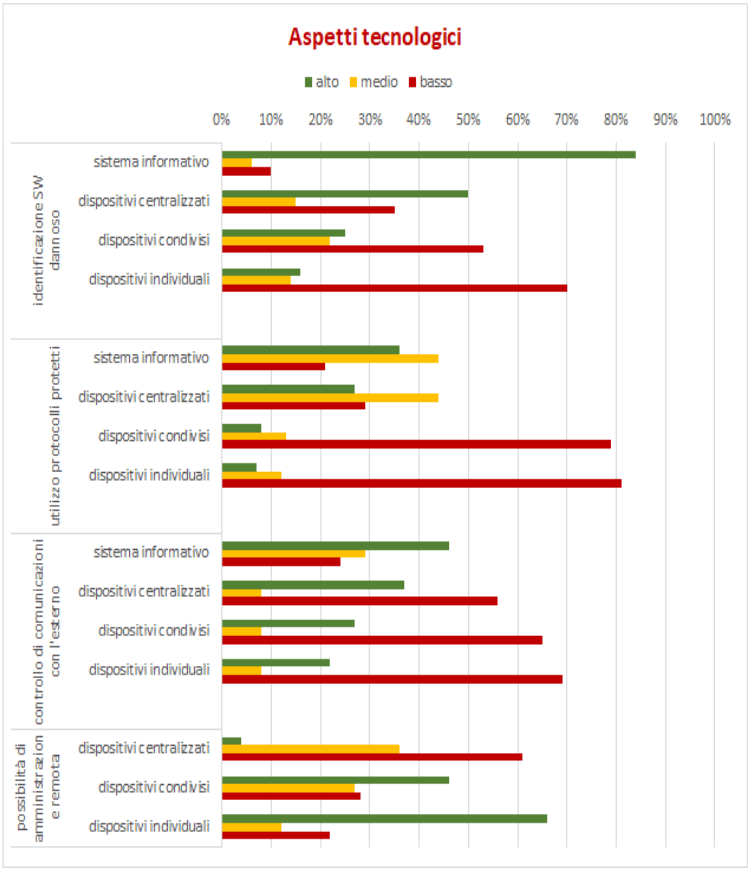
- in oltre il 10% dei contesti non viene gestito un inventario dei componenti collegati alla rete;
- la continuità di esercizio non è assicurata in circa il 15% dei casi ed è garantita solo per le aree critiche (Pronto soccorso, rianimazione, sale operatorie, etc.) in solo il 60% dei casi e solo per il sistema informativo ed i dispositivi centralizzati.
- La continuità di esercizio, nei dispositivi condivisi è assicurata in meno del 20% dei casi per i dispositivi condivisisi ed in meno dell'8% dei casi per i dispositivi individuali.

Per quanto riguarda l'operatività dei dispositivi sotto il profilo tecnologico, 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), il che amplifica i rischi riscontrati in termini di assenza di meccanismi centralizzati di identificazione ed autenticazione.

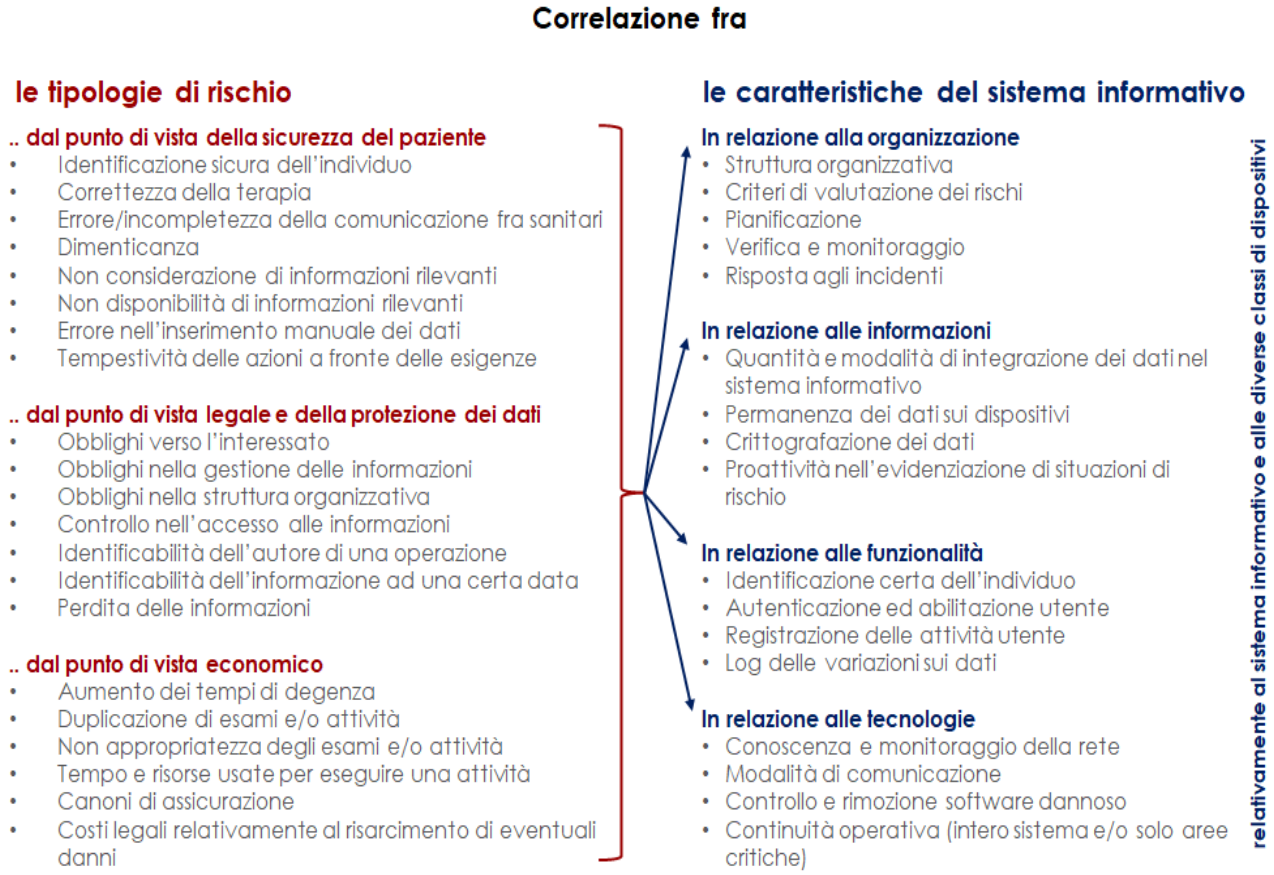
I dispositivi condivisi ed individuali presentano livelli di rischio più elevati anche sotto il profilo tecnologico

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



La correlazione con i fattori di rischio ed il modello di maturità per la sicurezza

Gli indicatori raccolti mediante il questionario sono stati correlati con le varie tipologie di rischio ([1],[2],[3]), classificate, secondo un approccio di Health Technology Assessment, in tre prospettive: **sicurezza del paziente**, **protezione dei dati personali**, **aspetti economici**.



Nella valutazione complessiva va anche tenuto conto de:

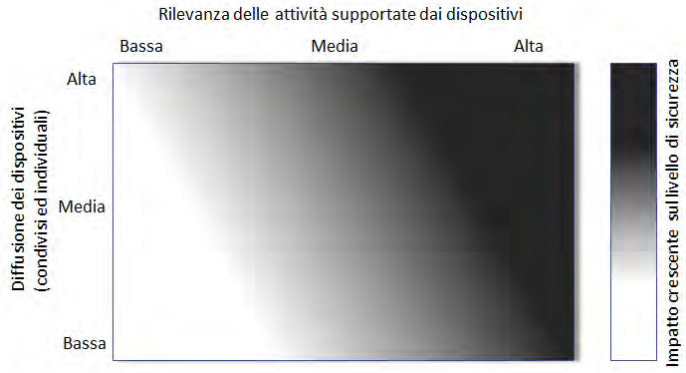
- la **diffusione** dei dispositivi medici all'interno della struttura, intesa come valutazione quantitativa del numero di attività effettuate con l'utilizzo di dispositivi medici.
  Per definire un "**indice di diffusione**", si può fare riferimento alla percentuale di attività di un certo tipo (rispetto al totale delle attività clinico-assistenziali di quel tipo effettuate dell'organizzazione) che sono eseguite con il supporto dei dispositivi medici.

- la **rilevanza** (ovvero la necessità e la criticità) dei dispositivi nell'ambito dei processi medici ed assistenziali, sia all'interno della struttura che nell'ambito delle eventuali

[1] cfr F.M.Ferrara – S. Pillon "Medicina digitale: sicurezza per il medico e per il paziente", Progettare per la Sanità, Settembre 2016
[2] cfr National Data Guardian for Health and Care, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
[3] cfr anche Ministero della Salute, http://www.salute.gov.it/portale/temi/p2_6.jsp?id=250&area=qualita&menu=sicurezza

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. 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.

Tanto maggiore è la diffusione e/o la rilevanza dei dispositivi medici, tanto più significativi saranno per la struttura i rischi correlati alle varie caratteristiche del sistema, come indicato in figura



Oltre a questi aspetti, va anche considerato **lo 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:

- presenza di processi assistenziali e/o di cura domiciliari, per la cui attuazione il personale preposto fa uso di dispositivi medici
- presenza di processi assistenziali e/o di cura basati sulla collaborazione sul territorio con altre strutture
- presenza di processi assistenziali e/o di cura basati sulla telemedicina

In tutti questi contesti, sono rilevanti ai fini del rischio e della sicurezza:

- le modalità di interazione (verbali, cartacee, mediante comunicazioni informatiche, mediante l'accesso a sistemi condivisi) fra diversi attori;
- le modalità di comunicazione dei dispositivi con il sistema informativo (se esistenti e se basate su protocolli protetti);
- le modalità di utilizzo dei dispositivi (se direttamente o sotto il controllo di personale sanitario o se autonomamente da parte del paziente).

Il modello di maturità

Tenendo conto di questi vari aspetti è stato definito un modello di maturità in grado di rappresentare le 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 aspetti informativi**
  analizza le caratteristiche del contesto 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[1].

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.

[1] Si rinvia al documento completo presente sul sito ALTEMS per il dettaglio delle correlazioni fra fattori di rischio e caratteristiche del sistema e la check-list con indicatori significativi nei vari livelli

Livello 2 - Intermedio

Denota un contesto in cui l'azienda dimostra di affrontare in modo organico le problematiche inerenti alla sicurezza ed alla 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

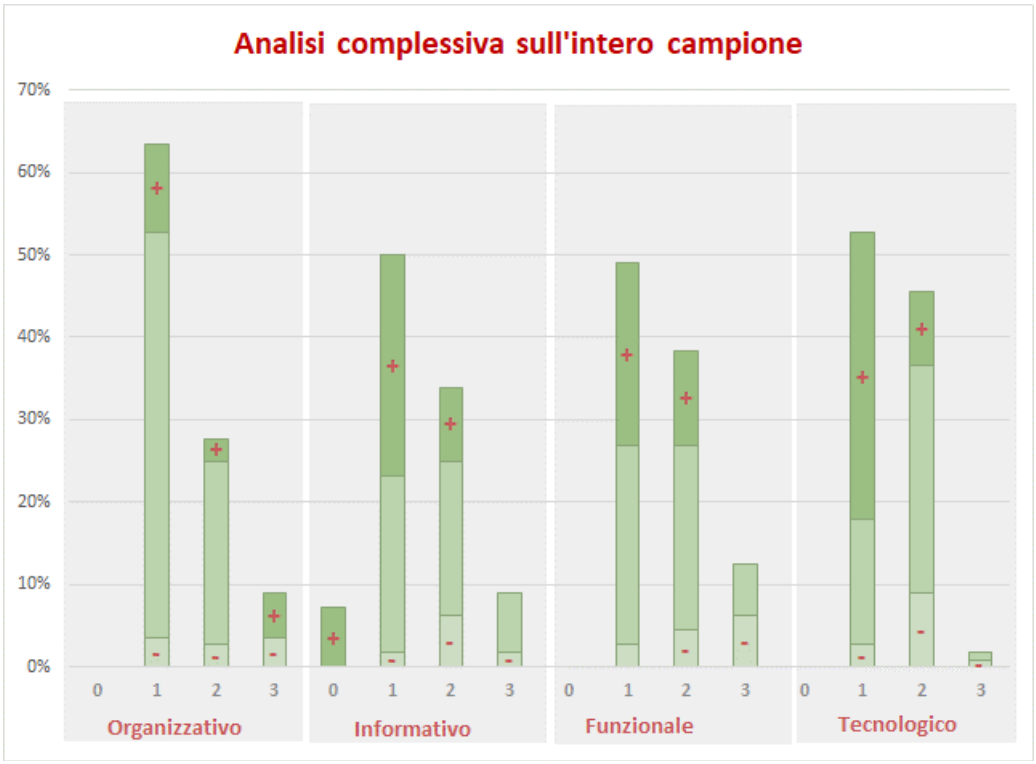
Denota un contesto in cui l'azienda affronta in modo organico le problematiche inerenti alla sicurezza, tenendo in forte considerazione anche le problematiche relative al supporto integrato a processi clinici ed operando secondo un approccio propositivo, di monitoraggio, pianificazione e di continuo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

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

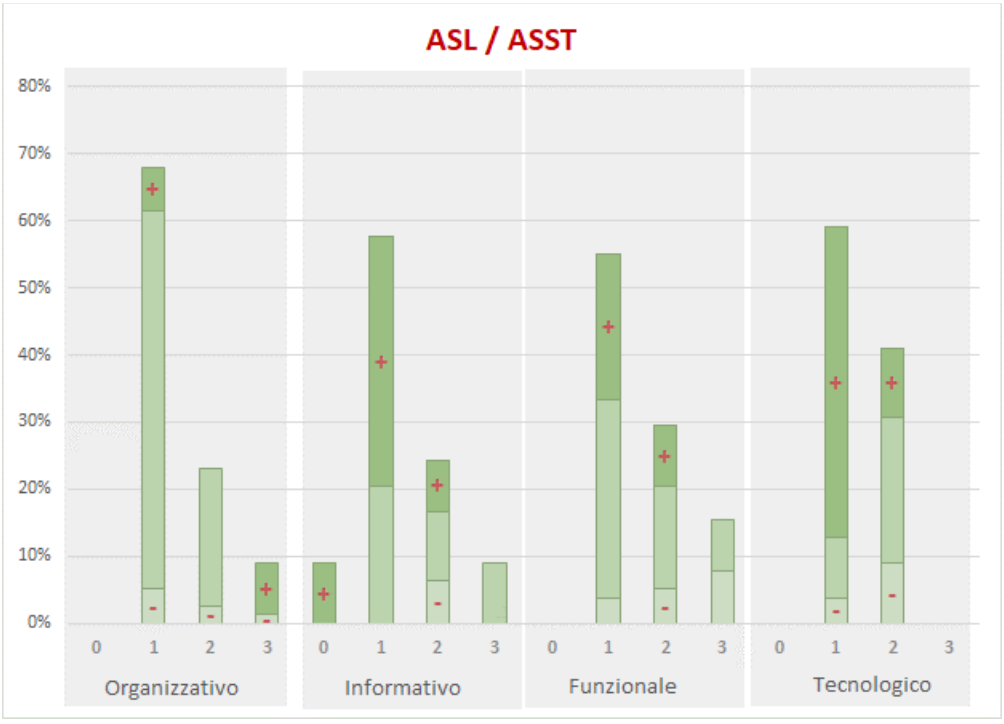
I dati raccolti dai 112 ospedali partecipanti all'indagine sono stati analizzati secondo gli indicatori ed organizzati nell'ambito del modello di maturità. Mediante tale elaborazione si è ottenuta la classificazione dei livelli di sicurezza nelle strutture sanitarie come rappresentata nei seguenti grafici.

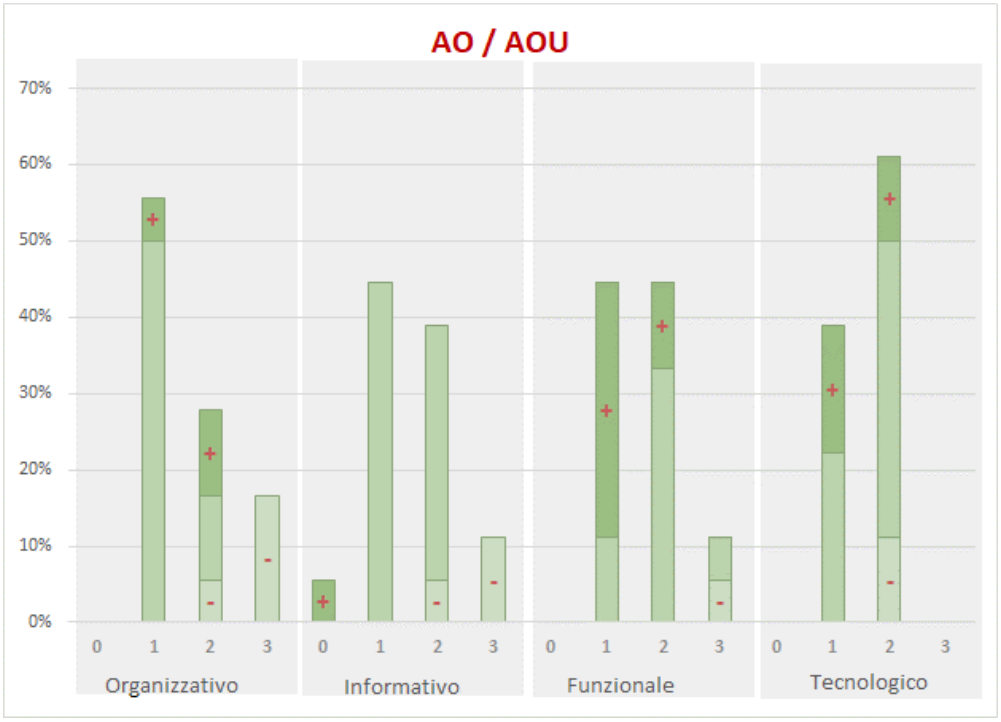
Come evidenziato, la composizione del campione, sia in termini geografici che di tipologia di aziende sanitarie è rappresentativa della realtà nazionale. L'applicazione del modello di maturità rappresenta pertanto una fotografia ragionevolmente significativa del livello di sicurezza dei dispositivi sanitari nel contesto dei sistemi informativi delle aziende sanitarie italiane.

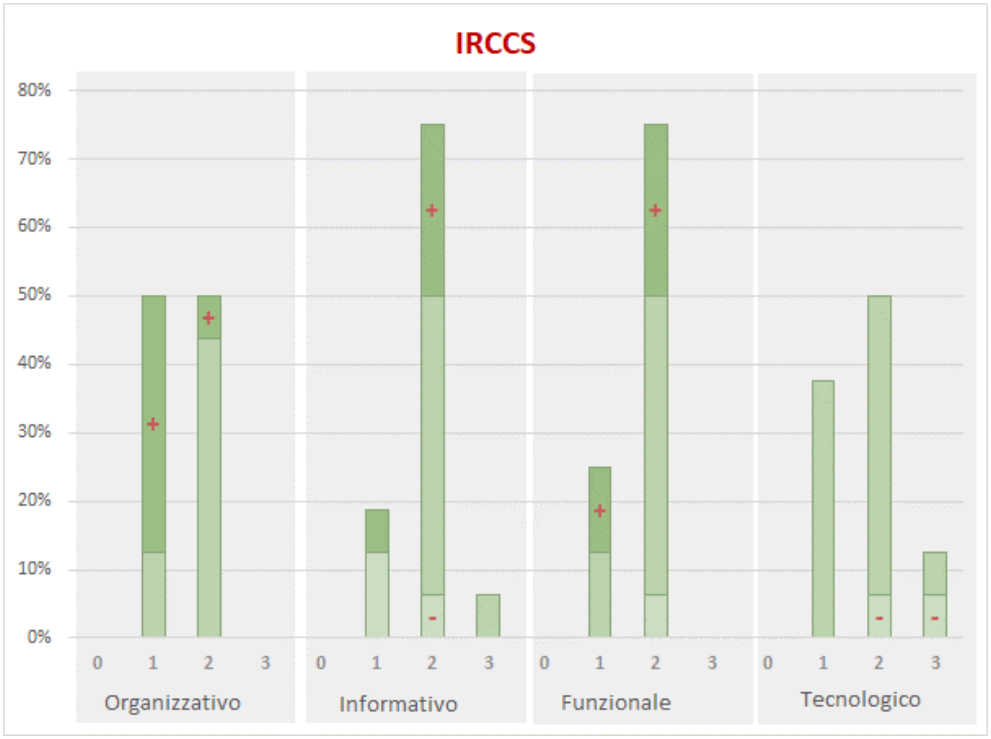
Va comunque considerato che le strutture che hanno partecipato all'indagine sono probabilmente caratterizzate da una maggiore sensibilità verso le problematiche della sicurezza. La percentuale delle strutture classificabili secondo livelli di minore maturità può pertanto essere, nella realtà, superiore a quella evidenziata dall'indagine.



Classificazione per tipologia di azienda sanitaria




AO / AOU
70%
60%
50%
40%
30%
20%
10%
0%
0 1 2 3
Organizzativo
Informativo
Funzionale
Tecnologico


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