hisSA health information system Security Assessment

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

La sicurezza (e la qualità) nei sistemi informativi sanitari e nei dispositivi medici

Fabrizio Massimo Ferrara
FabrizioMassimo.Ferrara@unicatt.it

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

Laboratorio sui sistemi informativi sanitari per il governo dell'organizzazione

In una organizzazione sanitaria moderna, il sistema informativo non può (più) essere considerato come un insieme di tecnologie ed applicazioni variamente connesse, ma deve costituire uno strumento di governo per l'intera struttura, di rilevanza strategica ed in grado di influire significativamente sulla qualità, sicurezza ed economicità sia dei processi organizzativi che dei servizi erogati e –in definitiva- sulla stessa salute del paziente

Le attività del Laboratorio sono focalizzate sulle strategie, le metodologie e le best-practices per la valutazione, l'implementazione e l'evoluzione del sistema informativo sanitario in relazione alle esigenze organizzative, alla sicurezza e protezione dei dati ed al percorso assistenziale del paziente in un'ottica di continuità della cura.

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

Il sistema informativo

- è ormai diffusamente utilizzato in tutti i processi dell'organizzazione sanitaria, influisce quindi, direttamente o indirettamente
  - → sulla stessa salute dei pazienti stessi
  - → sull'efficacia e l'efficienza dell'organizzazione
- ha una incidenza economica non trascurabile sui costi dell'organizzazione
- costituisce (deve costituire) uno strumento strategico per il governo ed il miglioramento dell'organizzazione e della qualità dei servizi erogati

- **Sempre maggiore dipendenza dell'organizzazione dal sistema informativo**
- **La «sicurezza» dell'organizzazione è sempre più legata alla «sicurezza» del sistema informativo**

sicurezza = qualità

.. in uno scenario sempre più articolato e complesso

L'obiettivo di **riduzione dei costi e miglioramento della qualità** tramite

- incremento della de-ospedalizzazione
- regimi e percorsi assistenziali nuovi ed alternativi al ricovero (improprio)

comporta però:

- aumento del numero di episodi
- **frammentazione dei dati clinici**
- **discontinuità dei processi**
- separazione delle attività
- **aumento dei rischi** di
  - errore clinico e legale
  - inefficienza organizzativa

.. in un contesto di collaborazione

Rispetto ad altri settori, le organizzazioni sanitarie **non operano isolate, ma fanno parte di un sistema** caratterizzato da un insieme di strutture

- **peculiari** per la loro attività e la loro missione etica e sociale
- **diverse** sotto il profilo organizzativo, clinico, dimensionale, tecnologico
- **autonome** sotto il profilo organizzativo, sanitario e giuridico

ma con necessità di

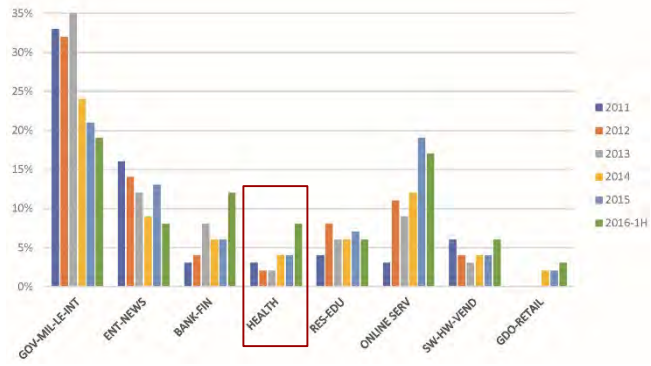
- **Condividere i dati** per cooperare nella cura del paziente durante il suo percorso, ottimizzando efficacia, risorse e costi

- **Massimizzare i dati** raccolti per
  - ✓ disporre di un quadro clinico il più completo possibile
  - ✓ consentire la prevenzione
  - ✓ supportare la ricerca

La «cyber-security» ha diverse prospettive

- Sicurezza dell'attività clinica
- Continuità del percorso di cura
- Integrazione, utilizzo e possesso dei dati
- **Protezione (utilizzo corretto) dei dati personali**
- Efficienza organizzativa
- Sicurezza dell'infrastruttura tecnologica

Rapporto Clusit 2016 Attacchi informatici dall'esterno



Ministero della Salute

5° Rapporto di monitoraggio degli eventi sentinella

2.000 episodi in sette anni → circa 300 l'anno
Il 35% con esito di morte del paziente

Cyber è un confisso ricavato dal sostantivo inglese cybernetics, cibernetica, parola derivata dal greco dove κυβερνήτης (kybernetes) aveva il significato letterale di 'timoniere, pilota di una nave' e per estensione 'colui che guida e governa una città o uno Stato'. *Accademia della Crusca*

Un approccio HTA per la sicurezza dei dati e del sistema informativo

La protezione dei dati e la sicurezza

- **non sono un solo fatto tecnologico circoscritto a singoli settori**
- **coinvolgono tutti gli aspetti dell'organizzazione e del sistema informativo**

per assicurare la sicurezza e la qualità dell'attività medica e dei processi aziendali

- **per la sicurezza del paziente**
- **nel rispetto del Regolamento UE 2016/679**
- in un quadro di **appropriatezza, qualità, efficacia ed economicità** delle prestazioni erogate al paziente

Difficoltà per una visione integrata

.. per la valutazione dell'esistente e per la definizione delle strategie evolutive secondo un approccio omogeneo e «sicuro»

- Limiti (tempi e costi) derivanti dalla frammentazione dei sistemi informativi, in massima parte costituiti ad «isole»
- Molteplicità delle soluzioni e delle tecnologie (spesso incompatibili)
- «Change management»: impatto organizzativo e formativo dell'evoluzione
- **Visione tradizionalmente «mono-dimensionale» e «technology-oriented» del sistema**

L' approccio multi-dimensionale

Metodologie e standard ICT

Per la rappresentazione delle caratteristiche dei sistemi informativi secondo indicatori omogenei non dipendenti da specifiche soluzioni tecnologiche

ISO 10746 – Open data processing – Reference model
- *Framework metodologico per l'analisi multidimensionale e multi-livello del sistema informativo*

ISO 12967 – Health Informatics – Service Architecture
- *Modello per la continuità di processi e l' integrazione delle informazioni cliniche e sanitarie nel sistema informativo*

ISO 27001- Information security management
- *"requirements for an Information Security Management System (ISMS)."*

Modelli di riferimento

Es. HiMSS EMR Adoption Model
- *strutturazione di livelli nelle caratteristiche del sistema informativo, in relazione alla rilevanza e gli ambiti di utilizzo*

Health Technology Assessment

Per l'identificazione e la valutazione di aspetti di specifica rilevanza nel contesto sanitario

- Aspetti relativi alla salute
- Efficacia clinica
- Prospettiva dei pazienti
- Aspetti economici, diretti ed indotti
- Aspetti organizzativi
- Aspetti socio-culturali ed etici
- Aspetti normativi e legali

hisSA health information system Security Assessment

Gli aspetti di rischio

.. dal punto di vista della sicurezza del paziente
- Identificazione sicura dell'individuo
- Correttezza della terapia
- Errore/incompletezza della comunicazione fra sanitari
- Dimenticanza
- Non considerazione di informazioni rilevanti
- Non disponibilità di informazioni rilevanti
- Errore nell'inserimento manuale dei dati
- Tempestività delle azioni a fronte delle esigenze

.. dal punto di vista legale e della protezione dei dati
- Obblighi verso l'interessato
- Obblighi nella gestione delle informazioni
- Obblighi nella struttura organizzativa
- Controllo nell'accesso alle informazioni
- Identificabilità dell'autore di una operazione
- Identificabilità dell'informazione ad una certa data
- Perdita delle informazioni

.. dal punto di vista economico
- Aumento dei tempi di degenza
- Duplicazione di esami e/o attività
- Non appropriatezza degli esami e/o attività
- Tempo e risorse usate per eseguire una attività
- Canoni di assicurazione
- Costi legali relativamente al risarcimento di eventuali danni

sono influenzati dalle caratteristiche del sistema informativo

In relazione alla organizzazione
- Struttura organizzativa
- Criteri di valutazione dei rischi
- Pianificazione
- Verifica e monitoraggio
- Risposta agli incidenti

In relazione alle informazioni
- Quantità e modalità di integrazione dei dati nel sistema informativo
- Permanenza dei dati su sistemi isolati
- Crittografazione dei dati
- Proattività nell'evidenziazione di situazioni di rischio

In relazione alle funzionalità
- Identificazione certa dell'individuo
- Autenticazione ed abilitazione utente
- Registrazione delle attività utente
- Log delle variazioni sui dati

In relazione alle tecnologie
- Conoscenza e monitoraggio della rete
- Modalità di comunicazione
- Controllo e rimozione software dannoso
- Continuità operativa (intero sistema e/o solo aree critiche)

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

2017 – Indagine sulle caratteristiche dei sistemi informativi sanitari in relazione alla sicurezza

hisSA health information system Security Assessment

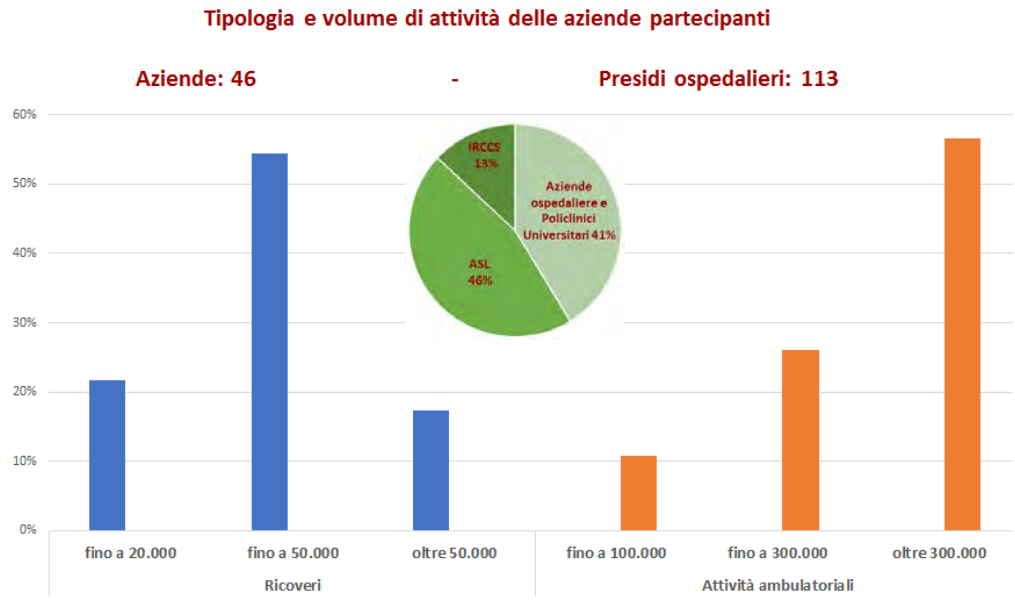
In collaborazione con

Ministero della Salute
DIREZIONE GENERALE della DIGITALIZZAZIONE, del SISTEMA INFORMATIVO SANITARIO e della STATISTICA

"fotografia" omogenea delle caratteristiche di sicurezza degli scenari nelle aziende sanitarie italiane

metodologia per l' analisi e modello di classificazione secondo "**livelli di sicurezza**",

basati su **indicatori** misurabili, indipendenti dalle specifiche soluzioni tecnologiche adottate



https://altems.unicatt.it/altems-i-sistemi-informativi-sanitari-per-il-governo-dell-organizzazione-analisi-della-sicurezza

I risultati dell'indagine

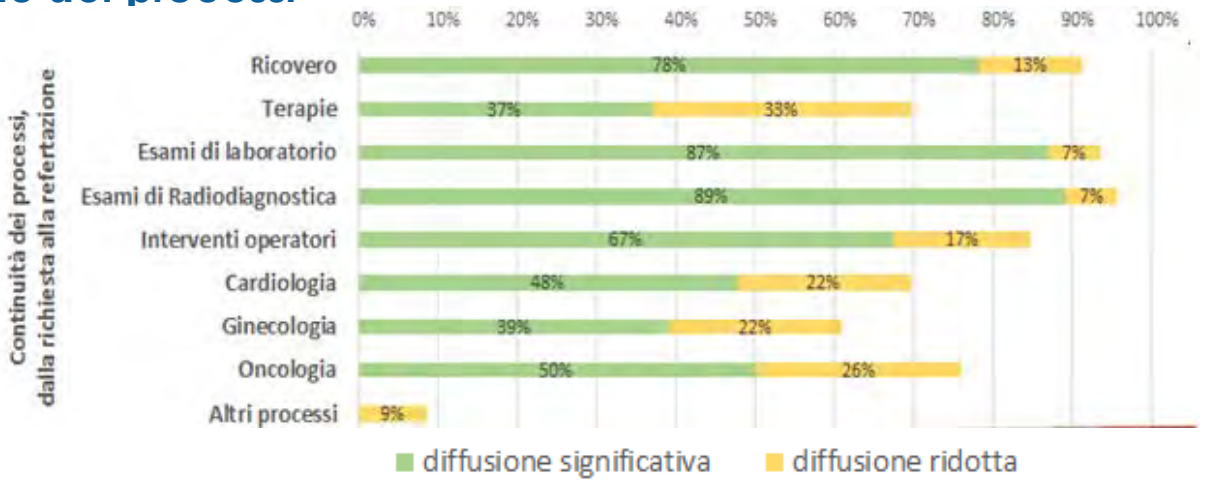
- Meno del 40% ha una funzione responsabile della sicurezza
- Meno del 30% effettua un piano per le attività inerenti alla sicurezza
- Meno del 50% effettua un assessment periodico della sicurezza

- **Il 37% registra nel sistema meno del 40% dei dati dei pazienti**
- Meno del 50% utilizza strumenti per il riconoscimento sicuro dei pazienti

- Meno del 35% adotta meccanismi integrati per l'identificazione e l'abilitazione agli accessi al sistema

- Solo il 43% dispone di una infrastruttura tecnologica di disaster-recovery

- **Discontinuità rilevanti nella gestione dei processi**



La crescita del volume dei dati

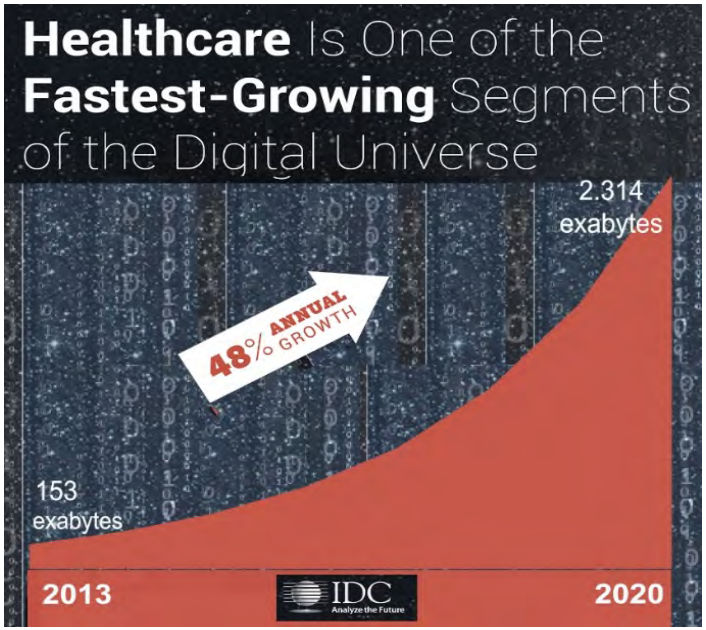
Volume dei dati sanitari

+ 48% anno

2013 : 153 exabyte
2020: 2.314 exabyte

1 exabyte = 1 miliardo di gigabyte

Tutto il materiale stampabile del mondo è pari a 5 exabyte



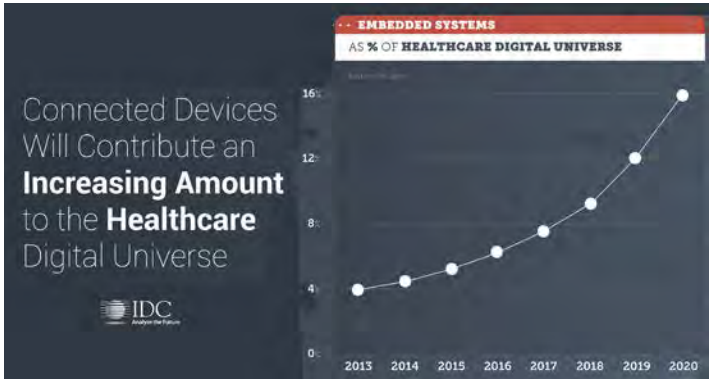
In questo scenario frammentato …

- **dove e come organizzarli ?**
- **come fare ad utilizzarli ?**
- **come fare a proteggerli ?**

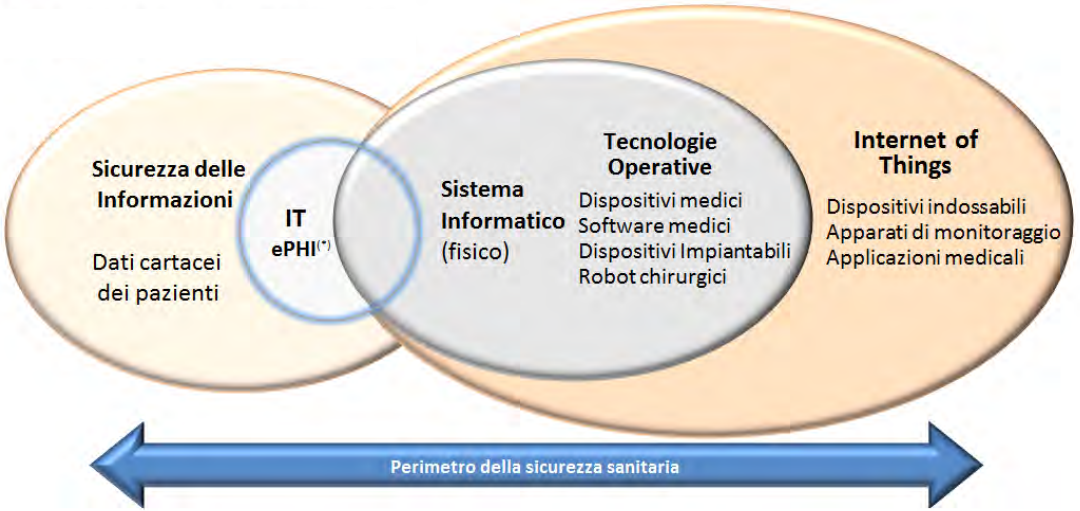
Il ruolo dei dispositivi medici

I dispositivi medici hanno **un ruolo sempre più rilevante**
- nell'ambito del processo di cura e di assistenza
- nella gestione (e protezione) dei dati del paziente

Non possono essere più considerati come apparecchiature autonome ed isolate



Entro il 2020, il 16% dei dati proverrà da dispositivi medici

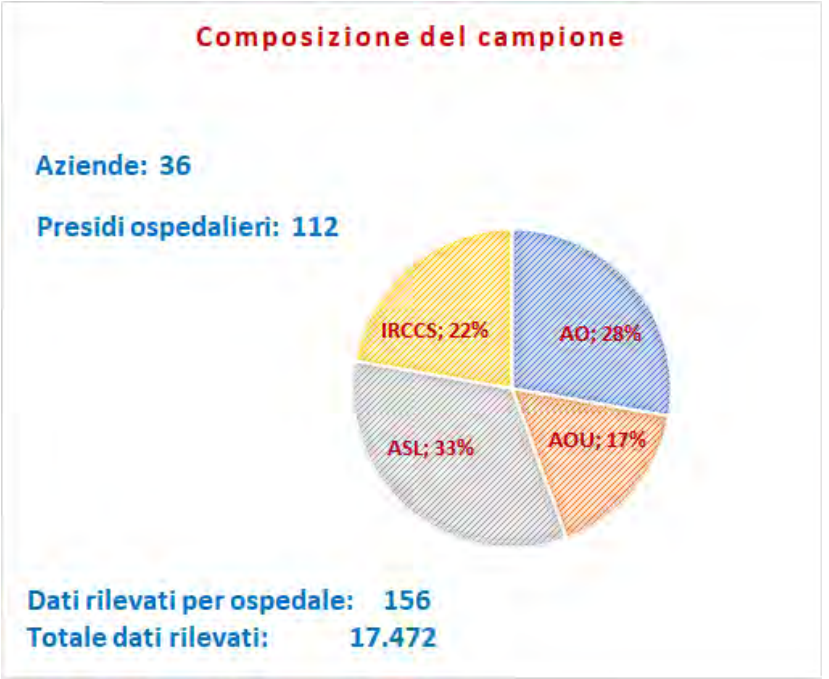


La sicurezza complessiva dipende sempre di più dalla sicurezza del binomio
sistema informativo + dispositivo collegato

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

2019 - indagine sulle caratteristiche dei sistemi informativi integrati con i dispositivi medici

hisSA health information system Security Assessment -MD



Un questionario su 40 argomenti

Aspetti organizzativi

Come è organizzata l'azienda nell'analisi e nella gestione dei vari aspetti inerenti alla sicurezza ed alla protezione dei dati con particolare riguardo ai dispositivi medici connessi al sistema informativo

Aspetti implementativi: informativi e funzionali

Le caratteristiche in termini di modalità di gestione dei dati e funzionalità operative e di controllo

Aspetti tecnologici

Le caratteristiche della infrastruttura, della rete e delle modalità di protezione e di comunicazione

Classificazione dei sistemi e dei dispositivi

centralizzati

quei sistemi, usualmente articolati e complessi, di uso diffuso all'interno della struttura, installati per i componenti centrali (server, basi dati, procedure applicative, etc.) in ambienti centralizzati e dedicati e gestiti centralmente da personale dedicato.

condivisi

quei sistemi installati anche nelle componenti centrali all'interno di diversi settori della struttura e utilizzati a supporto specifiche attività sanitarie e/o organizzative di interesse locale per il settore. Operano autonomamente (collegati o meno con il sistema centrale dell'organizzazione) e sono gestiti su chiamata dalla struttura centrale dell'organizzazione e/o da personale dello specifico settore di afferenza.

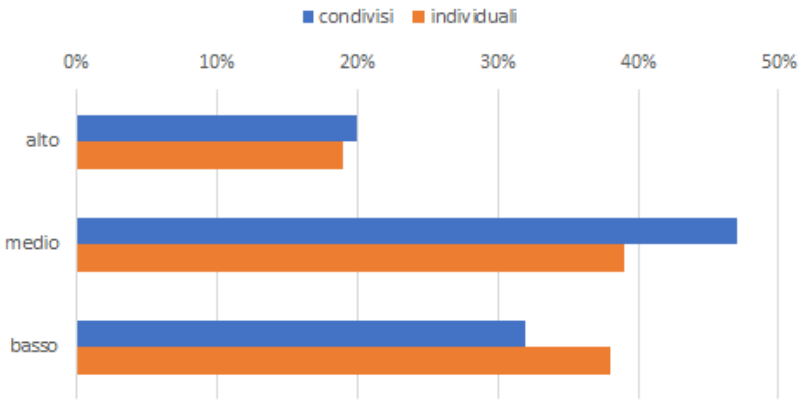
individuali

quei sistemi, generalmente mobili, utilizzati e gestiti individualmente da parte del paziente (all'esterno e/o all'interno del centro) e/o da personale sanitario nell'ambito dell'attività clinica e/o assistenziale.

Rischio crescente

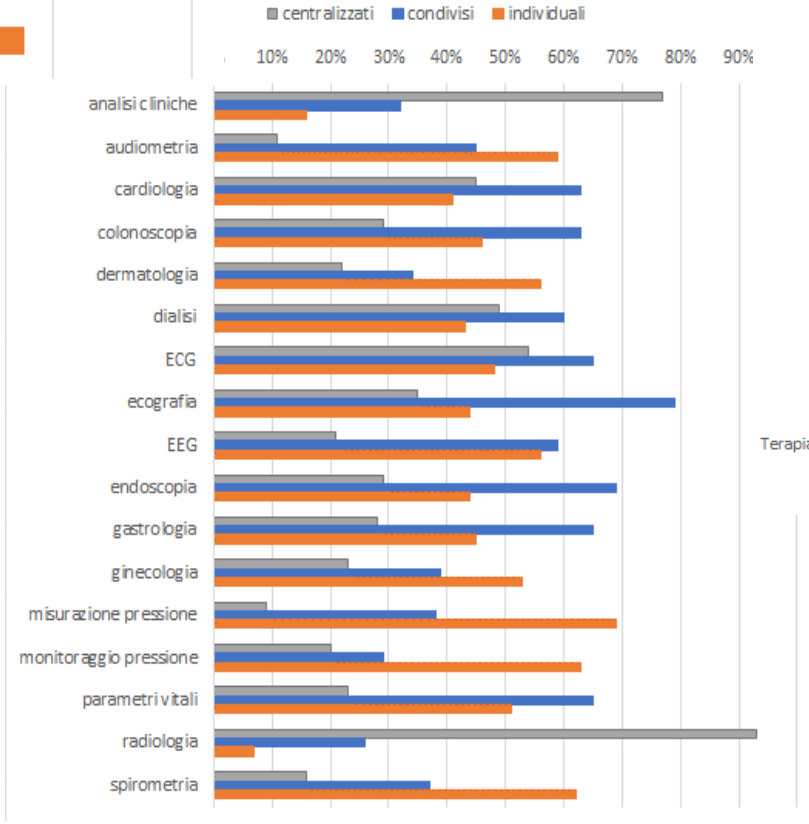
Diffusione e contesti di impiego

Diffusione dei dispositivi nella struttura

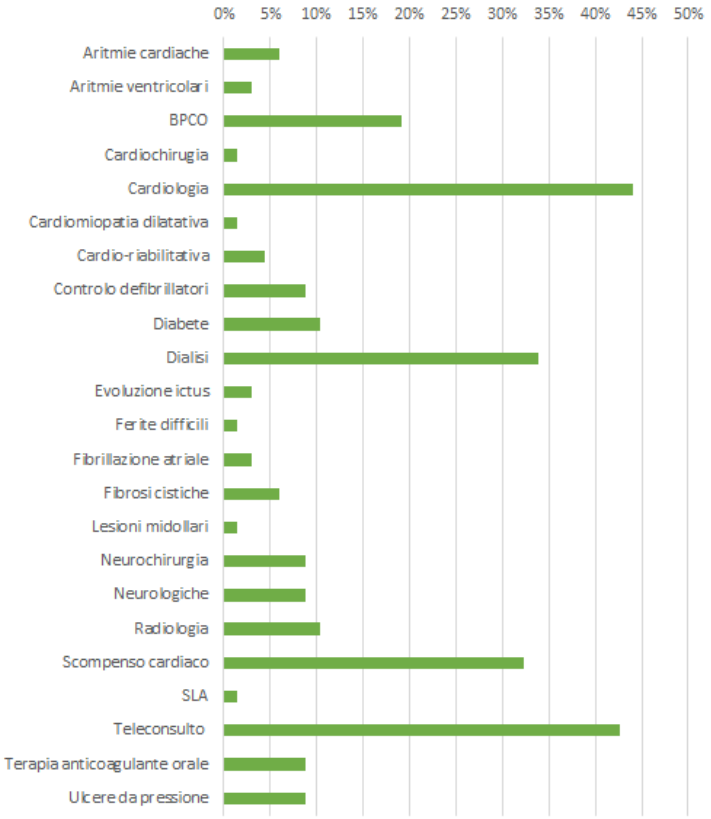


Crescente diffusione e rilevanza dei dispositivi condivisi ed individuali

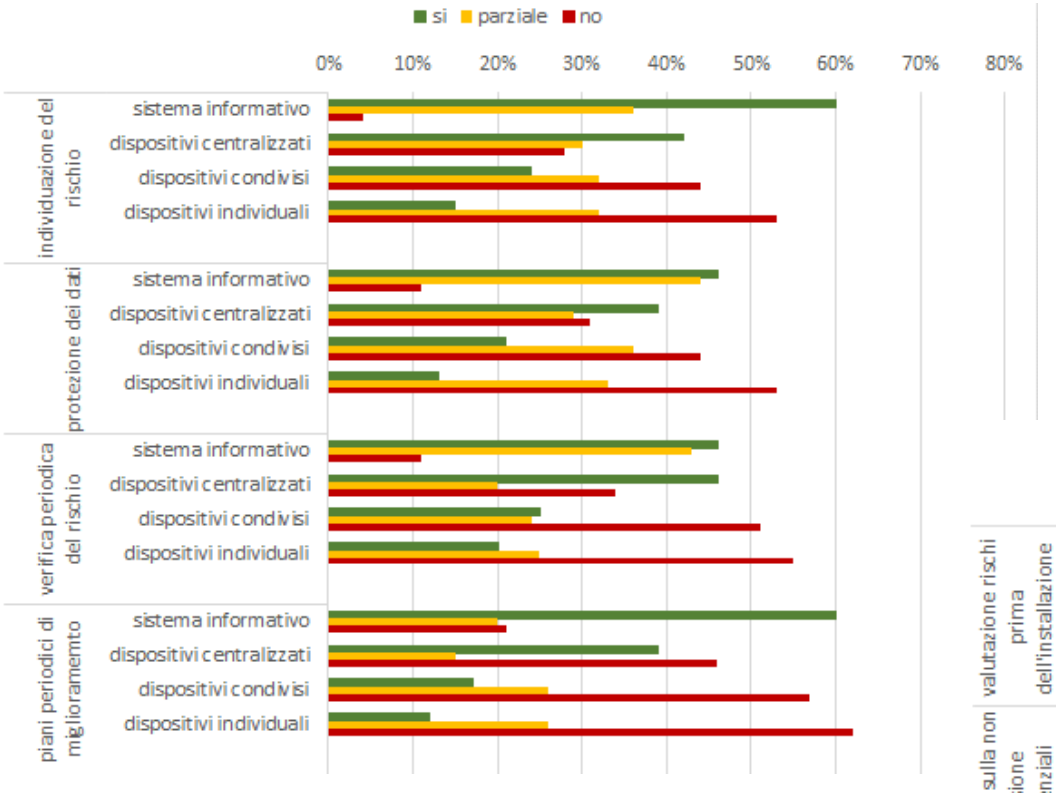
Attività supportate da dispositivi



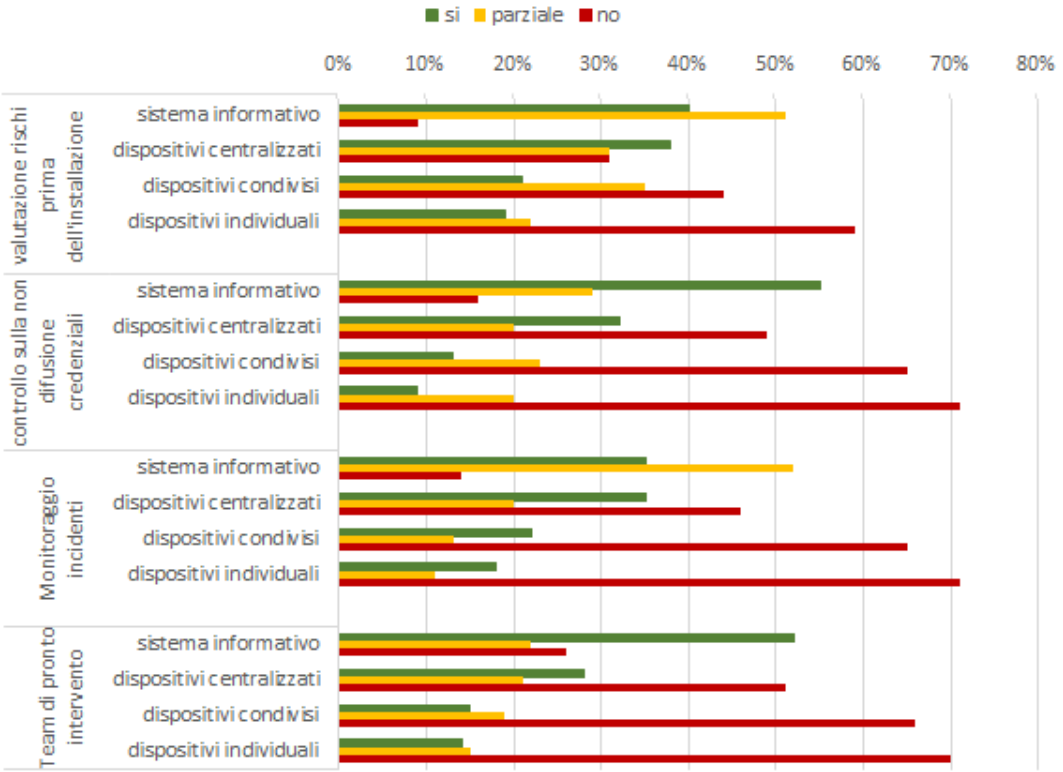
Aree di impiego della telemedicina



Aspetti organizzativi



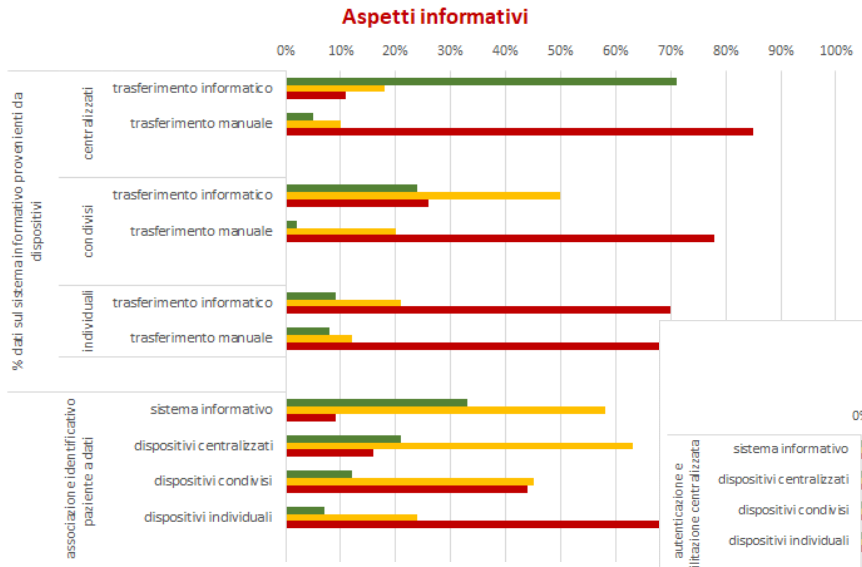
L'attenzione agli aspetti di rischio e la gestione della sicurezza nei dispositivi (in particolar modo quelli condivisi ed individuali) **sono di gran lunga inferiori rispetto a quanto presente nel sistema informativo**

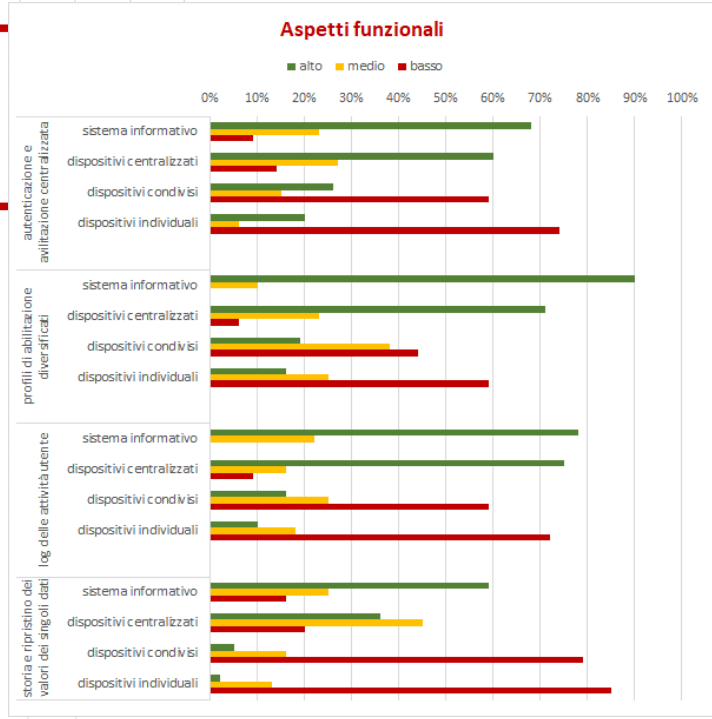


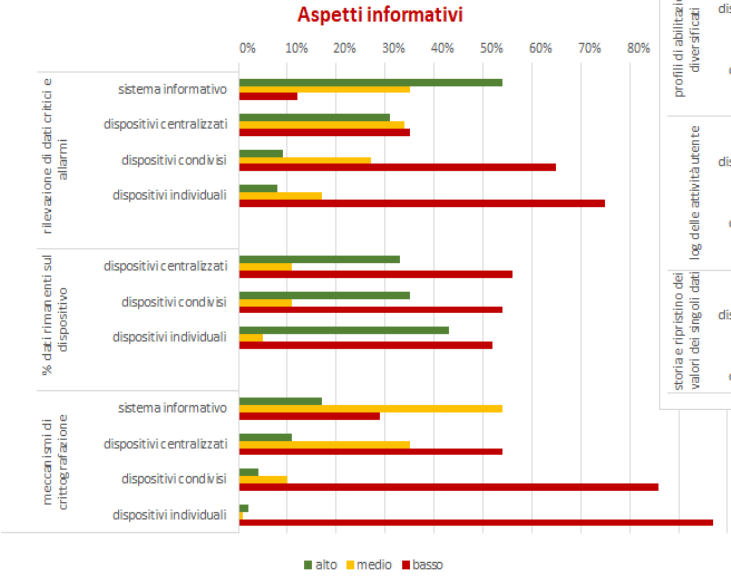
Aspetti informativi e funzionali

I dispositivi condivisi ed individuali presentano i più 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
- Gran parte delle **informazioni rimangono stabilmente registrate** sul dispositivo e non sono integrate nel sistema informativo





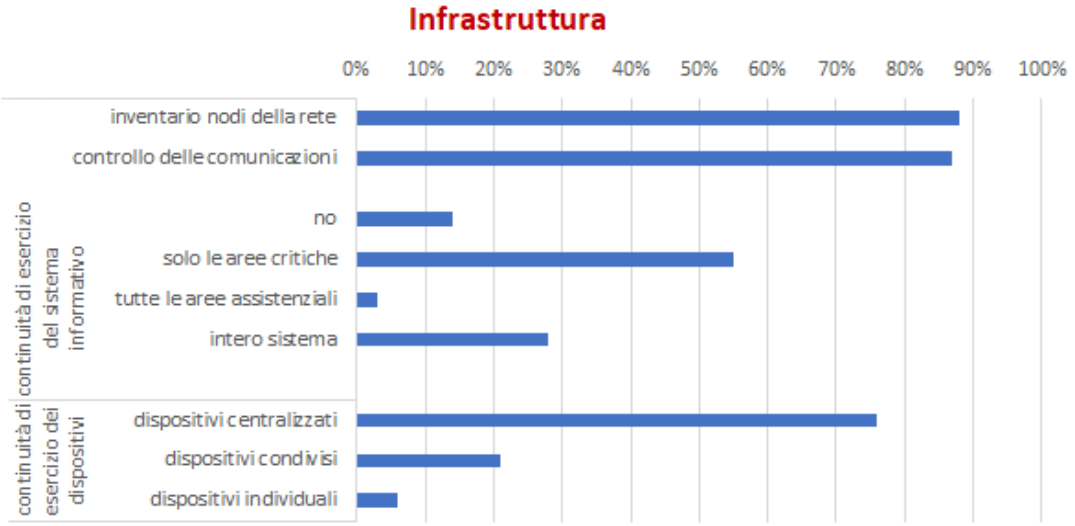


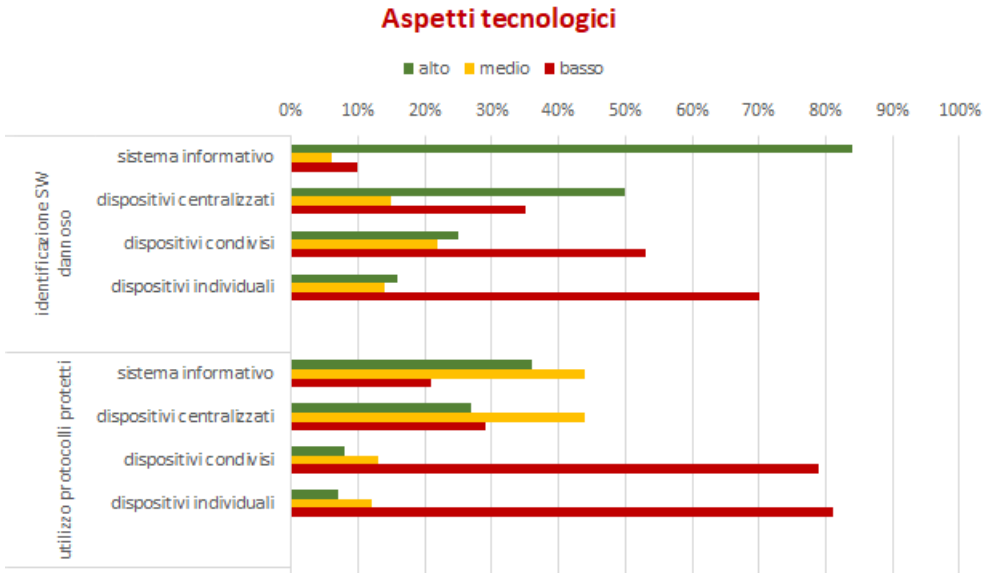
Aspetti tecnologici

In oltre il 10% dei contesti **non viene gestito un inventario** dei componenti collegati alla rete

La continuità di esercizio

- **nel 60% dei casi solo per le aree critiche** e solo per il sistema informativo ed i dispositivi centralizzati.
- **nei dispositivi condivisi in meno del 20% dei casi** ed in meno dell'8% dei casi per i dispositivi individuali.





Sui dispositivi condivisi e individuali

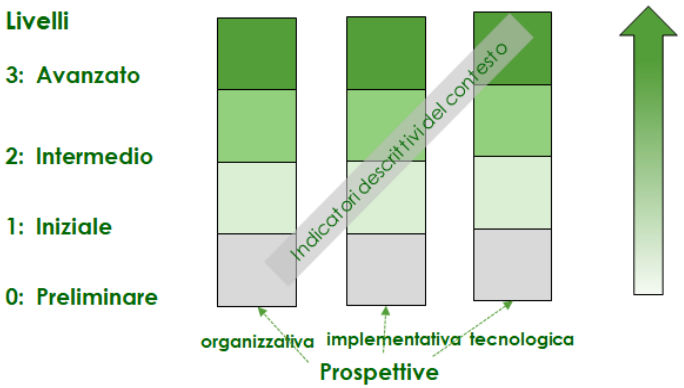
- È molto bassa la presenza di meccanismi di riconoscimento software dannoso
- E' molto basso l'utilizzo di protocolli di comunicazione protetti

Modello di maturità della sicurezza
secondo le diverse prospettive

Livello 0 - Preliminare

Le problematiche sono affrontate secondo criteri e soluzioni frammentate per i singoli dispositivi (essenzialmente quelli centralizzati), senza una visione integrata nell' azienda e delle diverse prospettive del rischio.

Maturità nella gestione della sicurezza nei dispositivi medici secondo le diverse prospettive



Livello 2 - Intermedio

L'organizzazione della gestione è organica e sono presenti caratteristiche implementative in grado di contribuire alla sicurezza dei dati e dei processi. Sono tuttavia presenti fattori di rischio non trascurabili: le attività di gestione e controllo sono focalizzate sui dispositivi centralizzati e parzialmente sui dispositivi condivisi, una elevata percentuale di dati permane stabilmente sui dispositivi senza particolari misure di protezione e l'infrastruttura di comunicazione presenta aspetti di criticità.

Livello 1 - Iniziale

L'azienda dimostra sensibilità e di aver cominciato ad affrontare in modo organico le problematiche.
Le 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 3 - Avanzato

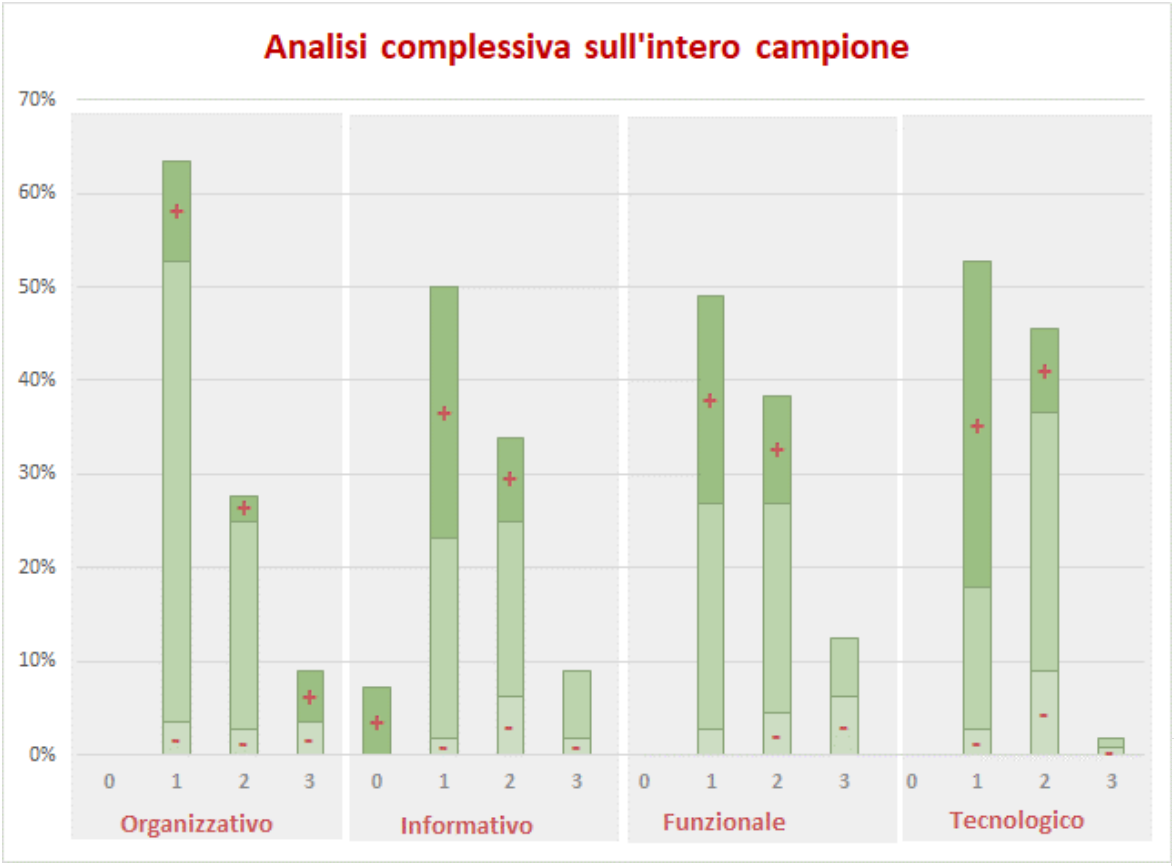
Le problematiche sono affrontate in modo organico operando secondo un approccio propositivo, di monitoraggio, pianificazione e di continuo miglioramento.
La gestione dei dispositivi centralizzati e condivisi, ed -in parte- anche di quelli individuali avviene secondo criteri omogenei, sia pur a livello implementativo diverso nei diversi settori.
Sono presenti caratteristiche in grado di contribuire alla sicurezza dei processi ed alla protezione dei dati, e meccanismi di protezione sui singoli dispositivi. L'infrastruttura tecnologica di comunicazione non presenta elementi di particolare criticità.
Sono presenti meccanismi proattivi per l'evidenziazione e per la prevenzione del rischio sia a livello funzionale che tecnologico.

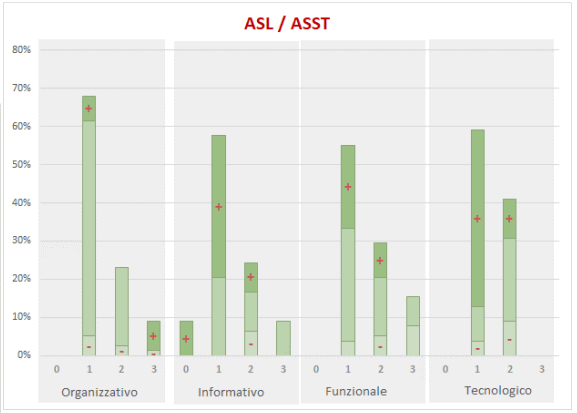
Modello di maturità

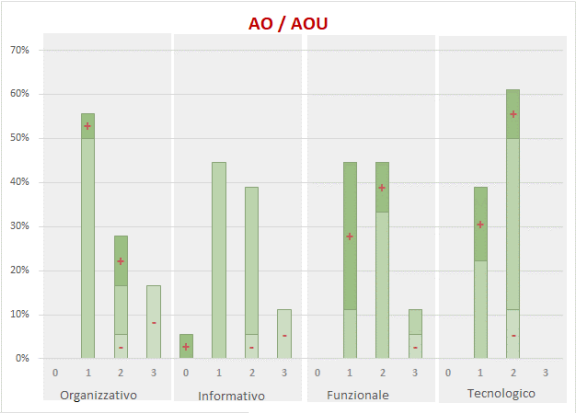
Check-list di autovalutazione in funzione dei valori degli indicatori

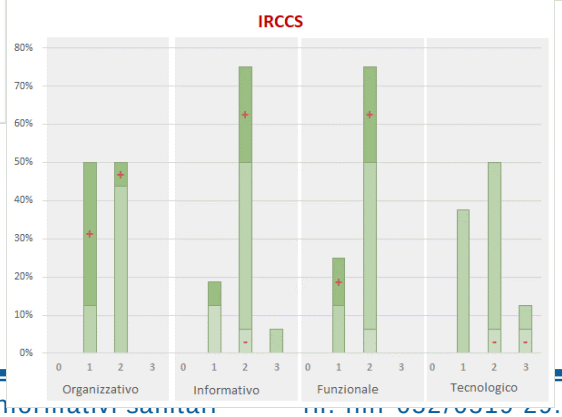
Check-list di valutazione del livello di maturità		SI / NO / PA(rziale)	Livello 0	Livello 1	Livello 2	Livello 3
Aspetti organizzativi			Preliminare	Iniziale	Intermedio	Avanzato
O1	Esistenza di funzione aziendale preposta alla sicurezza del sistema informativo		NO	NO	SI	SI
O2	Esistenza di funzione aziendale preposta alla gestione dei dispositivi		NO	NO	SI	SI
O3	Formalizzazione della collaborazione fra Sicurezza e Rischio clinico		NO	NO	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

Modello di maturità
applicato alle aziende che hanno partecipato allo studio









Fondazione Sicurezza in Sanità

Community per il governo dei dati

I dati sono frammentati fra applicazioni e basi dati proprietarie e non accessibili

- Difficoltà e costi nel recupero e nell'utilizzo dei dati per la cura, per la ricerca, e per l'efficienza dell'organizzazione
- Dipendenza dai fornitori e «vendor lock-in»
- Impossibilità di sicurezza e protezione

Dov'è il dato «buono» ?
Dove sono i dati che «servono adesso» ?
Come fare e quanto costa ottenerli ?

Non basta più la comunicazione fra le applicazioni che gestiscono ciascuna i propri dati, serve anche l'integrazione, la protezione e la disponibilità dei dati a livello aziendale

Clinical Data Repository una base dati aperta sotto il controllo dell'azienda

per

- integrare il patrimonio informativo aziendale clinico, economico e organizzativo
- assicurare all'azienda l'accessibilità e la proprietà dei propri dati senza dipendenze da singoli fornitori
- consentire l'evoluzione

http://fondazionesicurezzasanita.it

Fondazione Sicurezza in Sanità

Community per il governo dei dati

Coordinamento e collaborazione scientifica

Una community per studiare e condividere

- eventi e programmi formativi
- ricerche
- metodologie
- strumenti e componenti software **«open source» non proprietari**

per l'integrazione, la protezione e l'utilizzo dei dati

all'interno delle aziende sanitarie e nella continuità assistenziale sul territorio.

Ministero della Salute

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

Politecnico di Milano
Osservatorio Innovazione digitale in sanità

SAPIENZA
UNIVERSITÀ DI ROMA
Dipartimento di Ingegneria informatica, automatica e gestionale

HIMSS ITALIAN COMMUNITY

Un ambiente aperto in grado di integrare e proteggere i dati e di renderli disponibili per le evoluzioni

+

un insieme di componenti open-source direttamente condivisibili

FabrizioMassimo.Ferrara@unicatt.it

Grazie per l'attenzione