hisSA health information system Security Assessment

METODOLOGIA DI ANALISI E MODELLO DI CLASSIFICAZIONE DELLA SICUREZZA NEI SISTEMI INFORMATIVI SANITARI SECONDO UN APPROCCIO DI HEALTH TECHNOLOGY ASSESSMENT

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

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

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

- non può (più) essere considerato un insieme –più o meno omogeneo- di procedure e tecnologie variamente collegate per far fronte a singole esigenze, distinte e contingenti

- va pianificato, implementato, valutato, gestito secondo una visione integrata che tenga conto delle strategie aziendali e degli aspetti assistenziali, economici, organizzativi, etici e normativi

La sicurezza, incluso il rispetto delle normative sulla privacy

non è un solo fatto tecnologico circoscritto a singoli settori

ma coinvolge tutti gli aspetti del sistema informativo sanitario nella sua interezza

per assicurare la sicurezza e la qualità dell'attività medica e dei processi aziendali in generale, in termini di

safety	per evitare di fare danno per errore
security	per evitare danni a fronte di dolo
resilience	per operare in tutte le situazioni, anche in presenza di guasti
trust	per operare in qualità e nel rispetto delle normative

in un quadro di **appropriatezza, efficacia ed economicità** delle prestazioni erogate al paziente

i fattori 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 etico e legale

- 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 normativo

- Rispondenza alle normative sulla privacy
- Rispondenza alle leggi applicabili
- Rispetto del debito informativo

.. 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 anche relativamente al risarcimento di eventuali danni

sono influenzati dalle caratteristiche del sistema informativo

In relazione alle informazioni

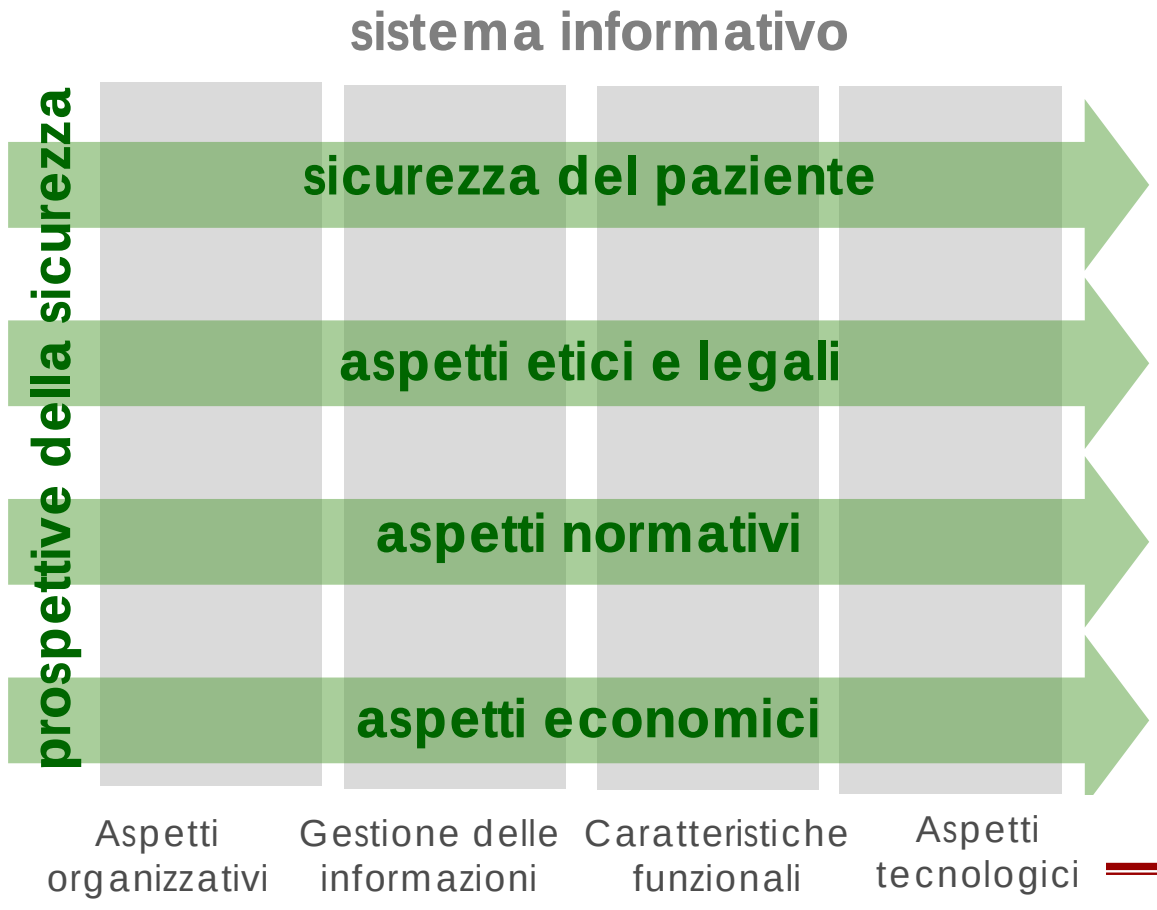
- **Disponibilità** delle informazioni necessarie
- **Accessibilità** ad informazioni esistenti e rilevanti
- **Proattività** nell'evidenziazione di informazioni rilevanti

In relazione ai processi

- **Completezza** del supporto alle varie attività senza bisogno di complementi verbali e/o cartacei
- **Continuità** del supporto alle varie attività, senza re-inserimento manuale di dati già disponibili

Occorre un approccio multi-dimensionale

in tutte le fasi, per garantire la rispondenza del sistema informativo alle esigenze di sicurezza complessive



Valutazione

Strategia

Pianificazione

L'adozione di un «approccio HTA»

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)."*

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

L'indagine sulle caratteristiche dei sistemi informativi sanitari

Con questa visione «olistica»

è stata condotta una indagine a livello nazionale

sulle caratteristiche dei sistemi informativi sanitari

di rilevanza per la sicurezza e per la privacy

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

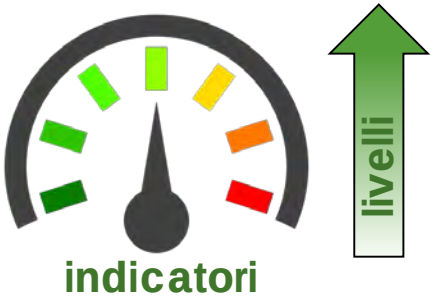
Ministero della Salute
DIREZIONE GENERALE della DIGITALIZZAZIONE, del SISTEMA INFORMATIVO SANITARIO e della STATISTICA

L'indagine sulle caratteristiche dei sistemi informativi sanitari

Obiettivi

ottenere una **"fotografia" omogenea** delle caratteristiche dei sistemi informativi delle aziende sanitarie italiane, in termini di sicurezza, intesa in questa sua accezione "totale" del termine

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

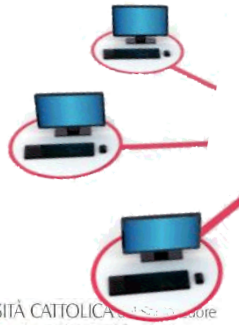


Il metodo di lavoro

ICT + HTA

progettazione di un questionario
su diversi aspetti dei sistemi informativi sanitari

Analisi dei sistemi con la collaborazione
di 46 aziende e 113 ospedali



Fotografia della situazione attuale secondo parametri omogenei

Definizione di un set di indicatori e di un modello per la classificazione dei livelli di sicurezza nei sistemi

diffuso ad un campione di aziende sanitarie in tutta Italia
e articolato in 40 argomenti, suddivisi in:

Aspetti organizzativi

Come è organizzata l'azienda nell'analisi e nella gestione dei vari aspetti inerenti la sicurezza e la privacy nel sistema informativo

Aspetti strutturali

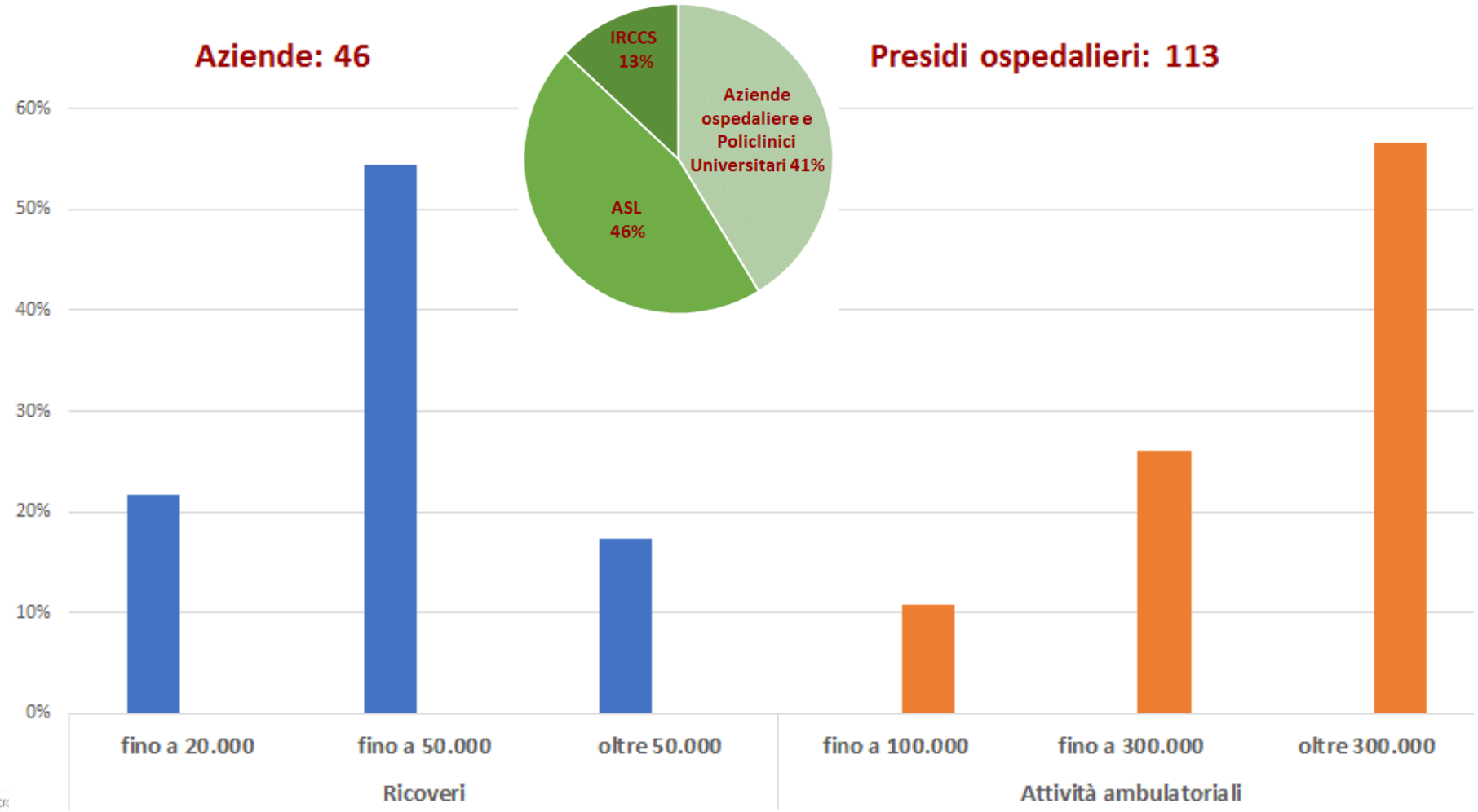
Le caratteristiche architetturali del sistema, di rilevanza generale per tutti i processi (es. disponibilità di informazioni, controllo accessi, privacy, etc.)

Aspetti implementativi

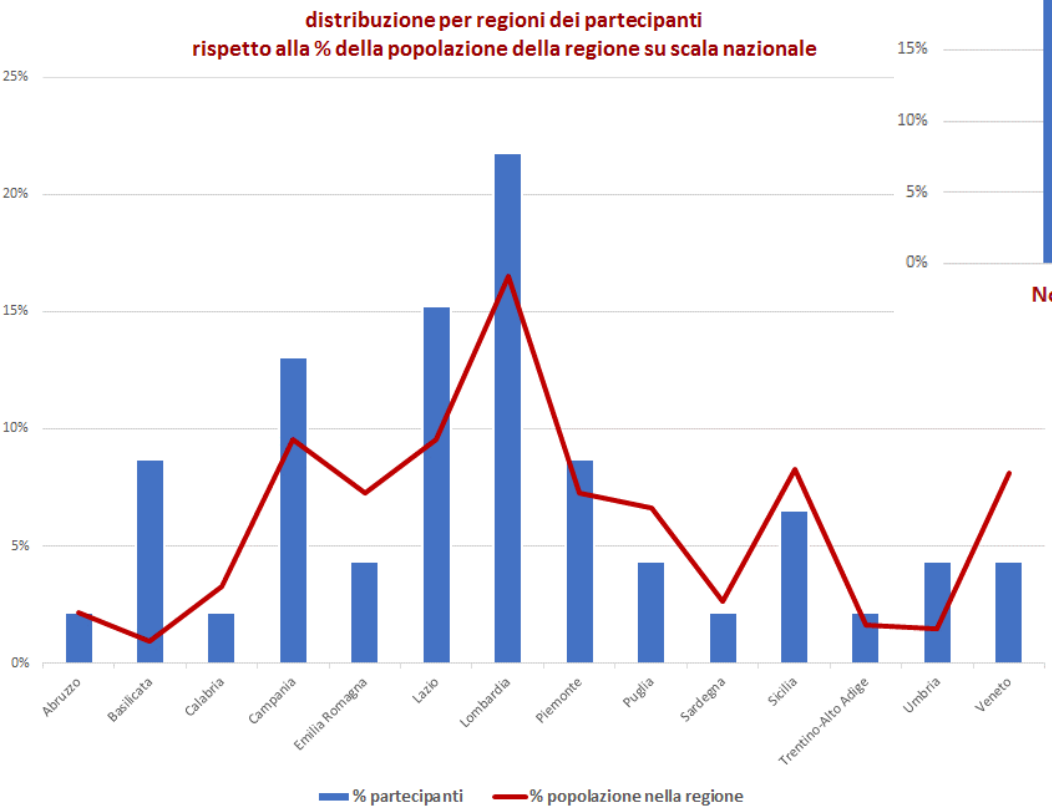
Quali funzionalità sono attualmente implementate nel sistema e come operano

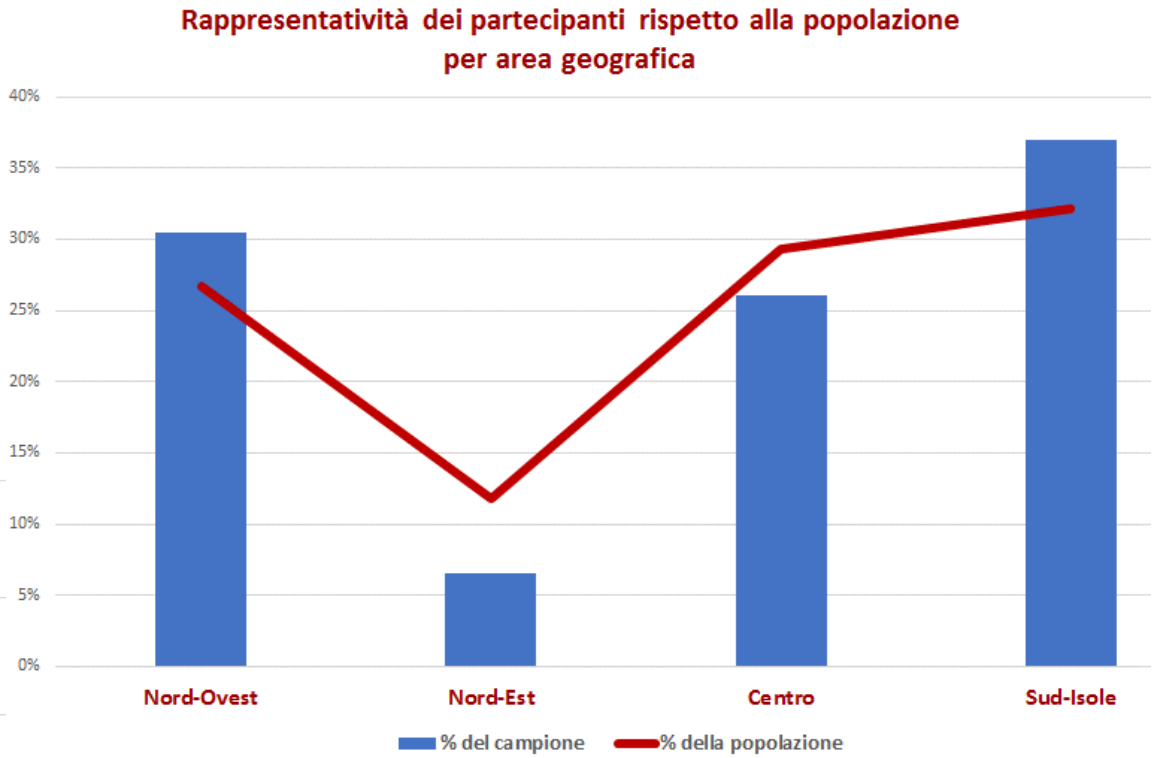
La partecipazione delle aziende nello studio

Tipologia e volume di attività delle aziende partecipanti



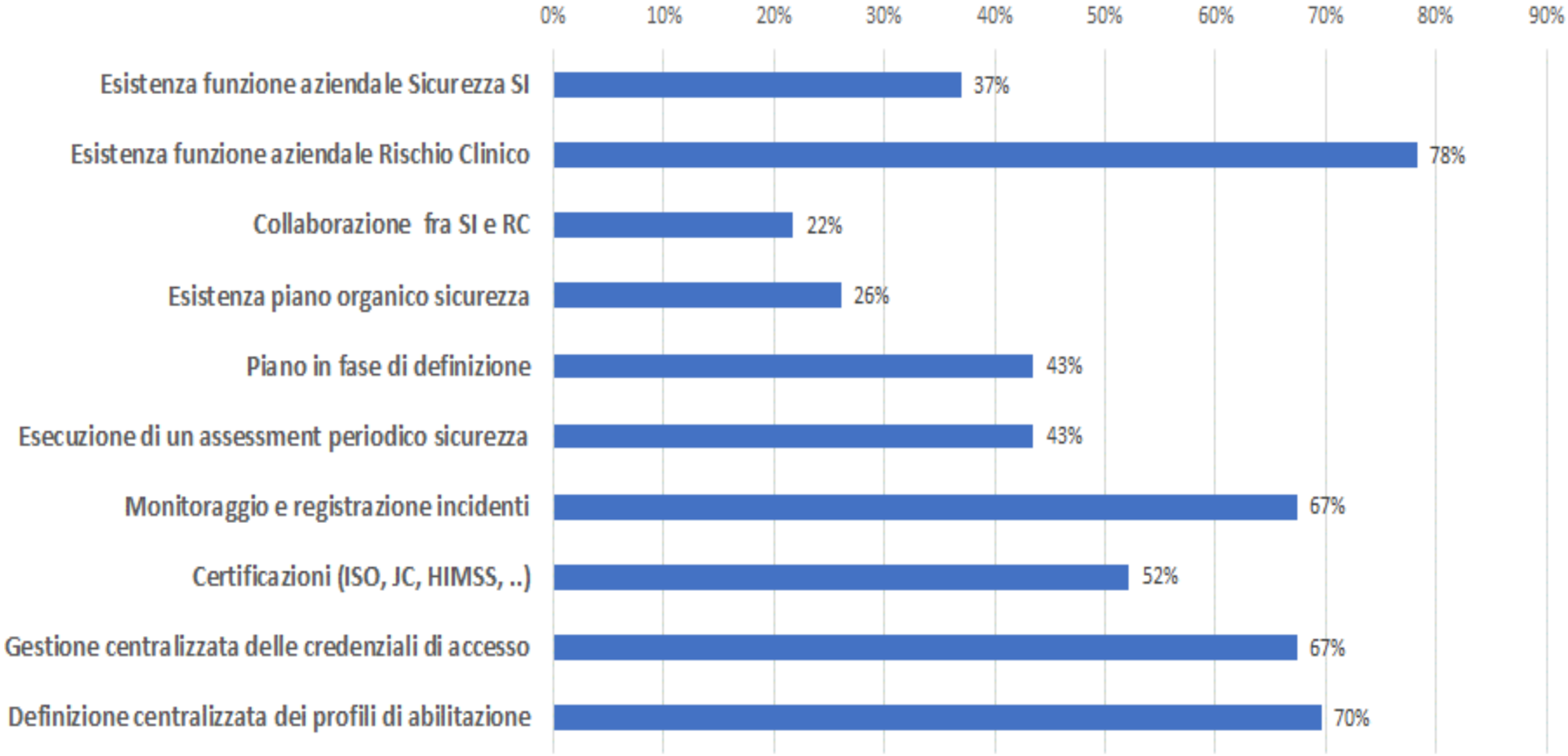
La partecipazione delle aziende nello studio



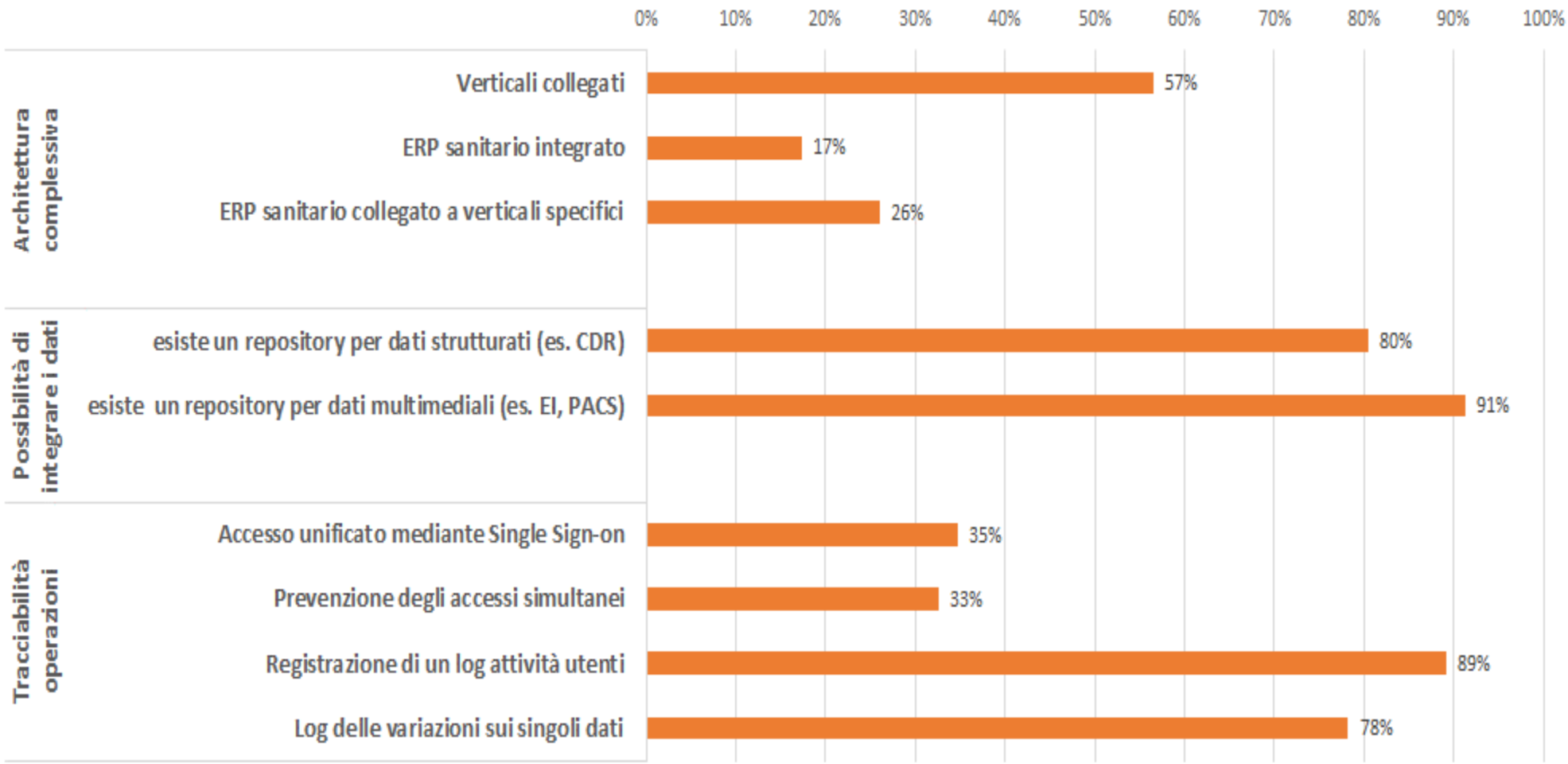


I risultati dell'indagine

Aspetti organizzativi



Aspetti strutturali: architettura e funzionalità di rilevanza generale



I risultati dell'indagine

Aspetti implementativi: servizi e funzionalità attualmente disponibili

L’indagine è ancora attiva

survey.sicurezza.his@gmail.com

Altre aziende possono partecipare compilando il questionario on-line

Gli indicatori

Ogni azienda presenta proprie peculiarità in funzione delle specialità mediche gestite e quindi delle esigenze e dei processi

Raramente il sistema informativo si evolve e si diffonde in modo perfettamente «identico» in tutti i settori dell'azienda

Semplici indicatori binari «ON / OFF» sarebbero riduttivi e poco rappresentativi della situazione reale

Gli indicatori sono correlati alla «**rilevanza**» ed alla «**diffusione**» dei dati e dei processi nello specifico contesto clinico ed organizzativo

Gli indicatori

rilevanza

Indica quanto il fenomeno misurato è significativo nel contesto clinico ed organizzativo dell'azienda, in percentuale rispetto al numero di pazienti trattati

Es.
La registrazione dell'anamnesi è molto rilevante in quanto interessa tutti i pazienti trattati, mentre un processo chemioterapico può essere molto o poco rilevante a seconda di quanti pazienti seguono questo trattamento

Indice di rilevanza		% rispetto al totale dei casi (pazienti)
A	Alto	oltre 70%
B	Medio	fino a 70%
C	Basso	fino a 30%

diffusione

Indica quanto la funzionalità del SI misurata è diffusa nel contesto dell'azienda in percentuale rispetto al totale dei casi

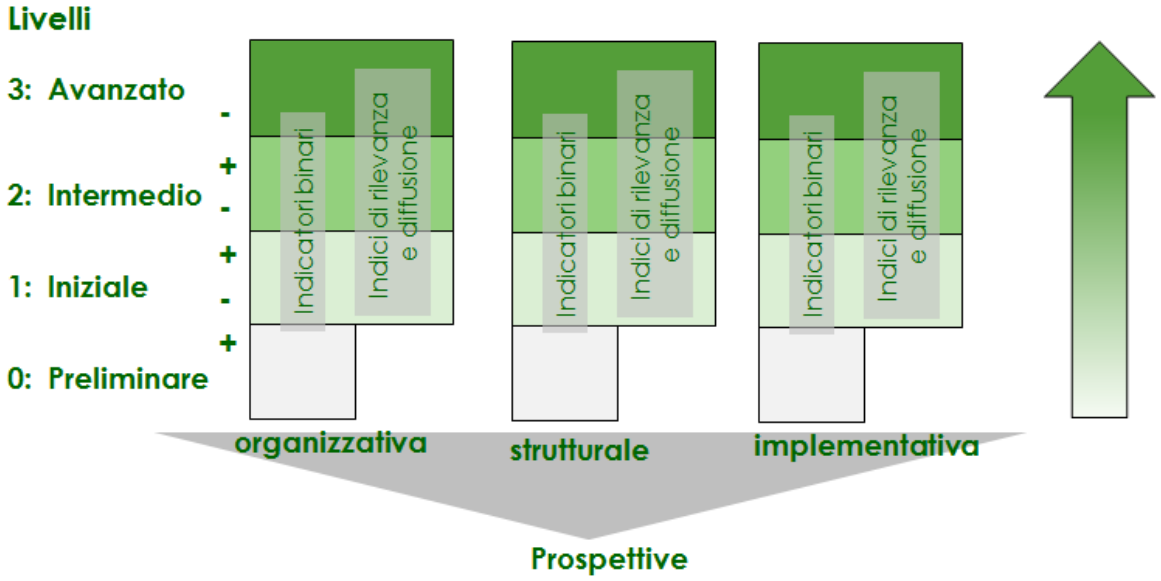
Es.
La diffusione della compilazione informatica del registro operatorio è la percentuale dei registri operatori compilati con il supporto del SI rispetto al totale

Indice di diffusione		% rispetto al totale delle occorrenze
A+	Molto alto	superiore a 85%
A	Alto	fino a 85%
B	Medio	fino a 65%
C	Basso	fino a 35%
C-	Molto basso	inferiore a 10%

Il modello di classificazione del «*livello di sicurezza del sistema informativo*»

Pesati anche secondo indici di rilevanza e diffusione per tener conto delle diverse esigenze e caratteristiche delle singole aziende

Classificazione dei sistemi informativi in funzione degli aspetti di sicurezza



Indice di rilevanza % rispetto al totale dei casi (pazienti)

A	Alto	oltre 70%
B	Medio	fino a 70%
C	Basso	fino a 30%

Indice di diffusione % rispetto al totale delle occorrenze

A+	Molto alto	superiore a 85%
A	Alto	fino a 85%
B	Medio	fino a 65%
C	Basso	fino a 35%
C-	Molto basso	inferiore a 10%

Suffissi «+» e «-» per evidenziare scostamenti marginali negli indicatori caratteristici del livello

Il modello di classificazione del «*livello di sicurezza nel sistema informativo*»

Livello 0 - Preliminare

Denota un contesto in cui le problematiche inerenti la sicurezza sono ancora affrontate quasi esclusivamente dal punto di vista tecnologico, secondo criteri e soluzioni frammentate senza una visione integrata nell'azienda.

Livello 1 - Iniziale

Denota un contesto in cui l'azienda dimostra sensibilità e di aver cominciato ad affrontare in modo organico le problematiche inerenti la sicurezza.
Le conseguenti caratteristiche strutturali ed operative del sistema informativo sono però ancora ancora ad uno stato iniziale, circoscritte ad un numero limitato di settori e di processi.

Modello di classificazione del «*livello di sicurezza nel sistema informativo*»

Livello 2 - Intermedio

Denota un contesto in cui l'azienda dimostra di affrontare in modo organico le problematiche inerenti la sicurezza.
Sono presenti nel sistema informativo caratteristiche strutturali in grado di contribuire alla sicurezza dei dati e dei processi anche mediante la centralizzazione di informazioni, regole e funzionalità.
Le operatività sono tuttavia ancora non ampiamente e non uniformemente diffuse in tutta la struttura.

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 rischio clinico ed operando secondo un approccio propositivo e di continuo miglioramento.
Sono presenti nel sistema informativo caratteristiche strutturali in grado di contribuire alla sicurezza dei dati e dei processi anche mediante la centralizzazione di informazioni, regole e funzionalità.
Le operatività sono ampiamente ed uniformemente diffuse in tutta la struttura.
Sono presenti meccanismi proattivi per l'evidenziazione automatica di situazioni di rilevanza e la prevenzione del rischio.

Prospettiva organizzativa

Prospettiva organizzativa					Livello			
					0	1	2	3
O1	Presenza di una funzione aziendale responsabile della sicurezza del SI nel suo complesso, secondo i diversi profili di rischio		SI/NO		NO	SI	SI	SI
O2	Collaborazione fra la funzione sicurezza e la funzione rischio clinico		SI/NO					SI
O3	Gestione di un piano organico per tutti gli aspetti inerenti la sicurezza		SI/NO		NO	SI	SI	SI
O4	Presenza di momenti di assessment periodico		SI/NO		NO		SI	SI
		frequenza						1 / anno
O5	Monitoraggio del sistema e registrazone incidenti		SI/NO			SI	SI	SI
O6	Gestione di un libro bianco dei miglioramenti		SI/NO					SI
O7	Definizione centralizzata delle credenziali di accesso		SI/NO			SI	SI	SI
O8	Definizione centralizzata dei profili di abilitazione		SI/NO					SI
O9	Utilizzo di vocabolari e codifiche uniformi		SI/NO				SI	SI
		Informazioni di Alta rilevanza	indice di diffusione				*medio*	*alto*
		Informazioni di Media rilevanza	indice di diffusione					*alto*
		Informazioni di Bassa rilevanza	indice di diffusione					*basso*
O10	Presenza di regole per l'utilizzo di dispositivi mobili e personali da parte di operatori sanitari e di pazienti							

Prospettiva strutturale

Prospettiva strutturale					Livello			
					0	1	2	3
S1	Presenza di un repository per l'integrazione di tutti i dati clinici, assistenziali, operativi (es. Clinical Data Repository)		SI/NO		NO	SI	SI	SI
S2	Presenza di un repository per l'integrazione di tutte le immagini e dati multimediali (es. Enterprise Imaging)		SI/NO		NO		SI	SI
S3	Presenza di un meccanismo centralizzato di identificazione utente e abilitazione accesso (es. single-sign-on)		SI/NO		NO	SI	SI	SI
S4	Presenza di ambiente centralizzato di gestione delle regole e dei profili di abilitazione		SI/NO				SI	SI
S5	Gestione di un log di accesso e di attività	minimale	SI/NO			SI	SI	SI
		sintetico	SI/NO				SI	SI
		dettagliato	SI/NO					SI
S6	Registrazione della storia delle variazioni ai dati	sintetico	SI/NO				SI	SI
		completo						SI

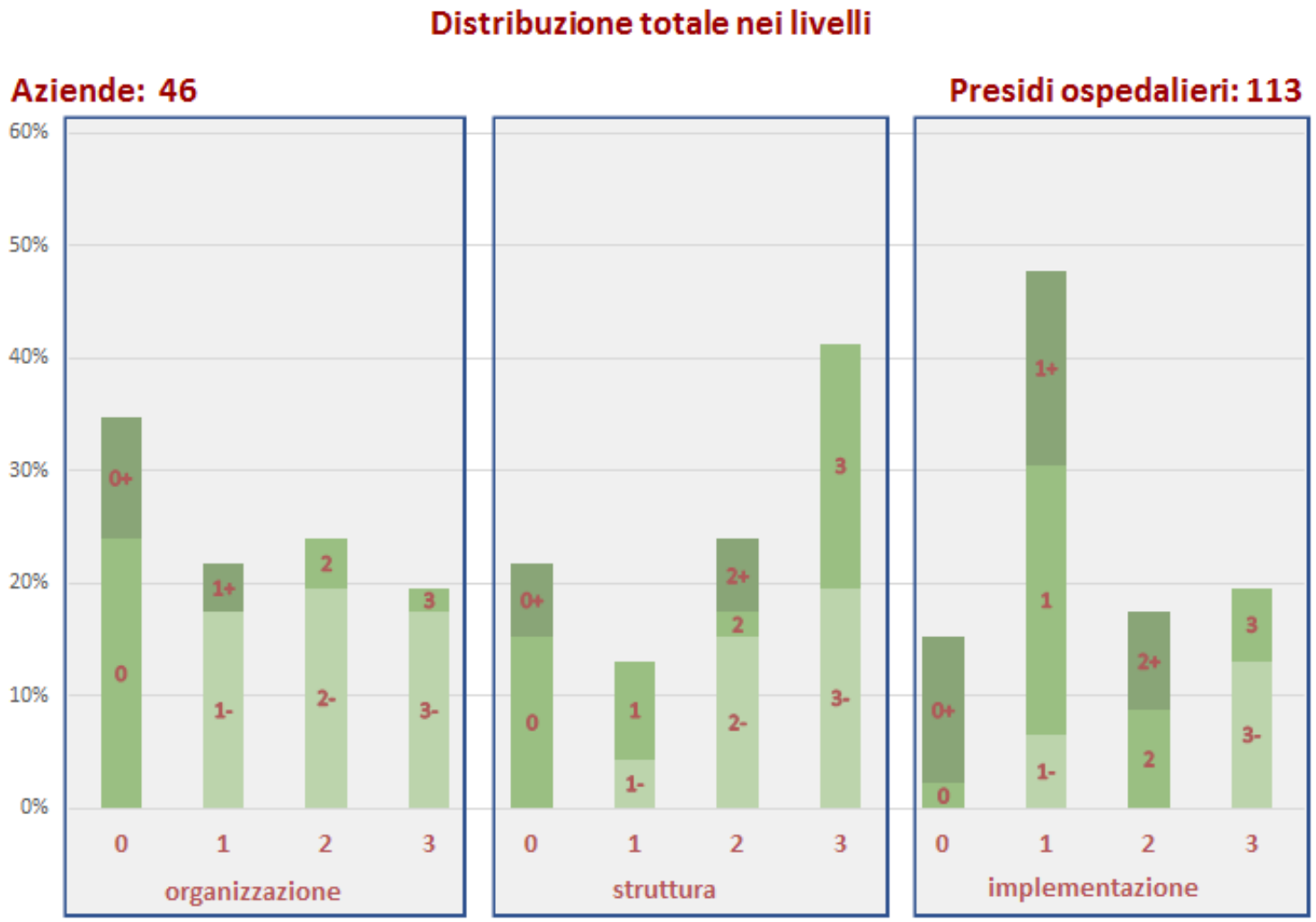
Indicatori e livelli di sicurezza

Prospettiva implementativa

Prospettiva implementativa				Livello			
				0	1	2	3
I1	Unicità di identificazione paziente e continuità dell'episodio assistenziale in tutte le fasi		SI/NO		SI	SI	SI
I2	Registrazione dei dati clinici	Dati di Alta rilevanza	indice di diffusione	*molto basso*	*basso*	*medio*	*alto*
		Dati di Media rilevanza	indice di diffusione		*molto basso*	*basso*	*medio*
		Dati di Bassa rilevanza	indice di diffusione				
I3	Registrazione dei dati assistenziali	Dati di Alta rilevanza	indice di diffusione			*basso*	*alto*
		Dati di Media rilevanza	indice di diffusione			*molto basso*	*medio*
		Dati di Bassa rilevanza	indice di diffusione				
I4	Utilizzo della firma digitale		SI/NO			SI	SI
		Diffusione				*basso*	*medio*
I5	Conitnuità del percorso di gestione della terapia		SI/NO			SI	SI
		Diffusione					*medio*
I6	Continuità del processo (extra-) operatorio		SI/NO			SI	SI
		Diffusione	indice di diffusione			*alto*	*molto alto*
I7	Conitnuità del processo di richiesta ed esecuzione di prestazioni di laboratorio e radiodiagnostica		SI/NO		SI	SI	SI
		Diffusione	indice di diffusione		*alto*	*molto alto*	*molto alto*
I8	Continuità del processso di richiesta ed esecuzione di altre prestazioni		SI/NO			SI	SI
		Prestazioni di Alta rilevanza	indice di diffusione			*alto*	*molto alto*
		Prestazioni di Media rilevanza	indice di diffusione			*medio*	*alto*
		Prestazioni di Bassa rilevanza	indice di diffusione				*medio*
I9	Integrazione dei dati e delle immagini nei repository centrali					SI	SI
		Dati di Alta rilevanza	indice di diffusione			*alto*	*molto alto*
		Dati di Media rilevanza	indice di diffusione			*medio*	*alto*
		dati di Bassa rilevanza	indice di diffusione				*medio*
I10	Utilizzo di funzioni centralizzate di identificazione utente ed abilitazione all'accesso		SI/NO			SI	SI
		Diffusione	indice di diffusione			*basso*	*medio*
I11	Utilizzo del sistema centralizzato delle regole e dei profili di abilitazione		SI/NO				SI
		Diffusione	indice di diffusione				*medio*
I12	Consultazione dati clinici in mobilità		SI/NO			SI	SI
		Dati di Alta rilevanza	indice di diffusione			*medio*	*alto*
		Dati di Media rilevanza	indice di diffusione				*medio*
		Dati di Bassa rilevanza	indice di diffusione				
I13	Esecuzione attività in mobilità		SI/NO			SI	SI
		Attività di Alta rilevanza	indice di diffusione			*medio*	*alto*
		Attività di Media rilevanza	indice di diffusione				*medio*
		Attività di Bassa rilevanza	indice di diffusione				
I14	Presenza di meccanismi di comunicazione informale fra operatori		SI/NO				SI
		Diffusione	numero processi				
I15	Presenza di meccansimi proattivi (allarmi e correlazioni automatiche)		SI/NO				SI
		Diffusione	numero processi				
I16	Presenza di meccanismi di riconoscimento automatico del paziente		SI/NO				SI
		Diffusione	numero processi				
I17	Configurazione di business-continuity	processi critici	SI/NO	NO		SI	SI
		tutti i processi assistenziali	SI/NO				SI
I18	Configurazione di disaster recovery		SI/NO				SI

Applicazione del modello alle aziende che hanno partecipato allo studio

Suffissi «+» e «-»
per evidenziare scostamenti marginali negli indicatori caratteristici del livello



Applicazione del modello alle aziende che hanno partecipato allo studio