

INTEGRARE I SISTEMI PER MIGLIORARE
LA QUALITÀ DELL'ASSISTENZA, Bologna 7 aprile 2006



L'approccio integrato alla gestione del rischio clinico, organizzativo e strutturale

Esperienze a confronto: l'approccio integrato alla gestione del rischio clinico, organizzativo e strutturale
Prof. Bruno Turinetti - Hesperia Hospital, Modena

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

Decreto Legislativo 196/2003

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (Normativa sulla privacy)

Glossario

Trattamento

Qualunque operazione o complesso di operazioni, effettuata anche senza l'ausilio di strumenti elettronici, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati .

Dati sensibili

Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Misure minime

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Problematiche

La **tutela della privacy del paziente** caratterizza in modo totale il sistema di gestione per la sicurezza delle informazioni (e viceversa)

Le **informazioni** sono dati gestionali informatici, dati clinici su supporto cartaceo, dati clinici su apparecchiature

I **dati su supporto cartaceo** sono in quantità rilevante

Le **cartelle cliniche** sono quasi esclusivamente su supporto cartaceo

Il **controllo accessi** (sicurezza fisica) contrasta con la cultura/storia delle strutture sanitarie di fatto "open space"

Aspetti sociali e legali della sicurezza

Livello minimo di protezione dei dati

- Sanzioni penali per mancata applicazione:
Reato contravvenzionale (art. 169: arresto fino a due anni o ammenda da € 10.000 a 50.000)
- La sanzione penale è evitabile con l'adempimento ed il pagamento sanzione amm.va (1/4 del massimo)

Sicurezza Sistema Informatico

Dipende da aspetti:

- **Tecnici**
- **Organizzativi**

Aspetti tecnici della sicurezza - Misure minime

- Credenziali di autenticazione
 - Sistema di autorizzazione
 - Antivirus
 - Firewall (accessi illeciti)
- Backup dati (copie di sicurezza)
 - Hardware duplicato

Aspetti organizzativi della sicurezza

Documento Programmatico sulla sicurezza (DPS):

Deve essere redatto entro il 31 marzo di ogni anno dal titolare del trattamento dei dati sensibili o giudiziari.

Regolamento Aziendale:

Determina le modalità di applicazione del D.Lgs n.196 30 giugno 2003 (non previsto dalle vigenti leggi)

DPS : i contenuti

- elenco dei trattamenti dei dati personali;
- distribuzione dei compiti e delle responsabilità nelle strutture preposte al trattamento dei dati;
- analisi dei rischi che incombono sui dati;
- misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali deputati alla loro custodia e accessibilità;
- criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (**DISASTER RECOVERY**);
- formazione degli incaricati del trattamento;
- misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno;
- misure per la protezione dello stato di salute e la vita sessuale.

Rischi potenziali

- Indisponibilità temporanea dell'accesso ai dati
- Distruzione con perdita parziale o totale dei dati
- Alterazione dei dati e della relativa organizzazione
- Conoscenza dei dati da parte di soggetti non autorizzati, interni o esterni alla struttura

Le conseguenze

- Danni patrimoniali diretti per la struttura
- Danni patrimoniali indiretti (aumento dei costi gestionali, danno all'immagine)
- Responsabilità contrattuali
- Responsabilità civile nei confronti dei danneggiati
- Sanzioni amministrative
- Sanzioni penali

Piano di disaster recovery

- Prevede il ripristino dei dati entro 7 giorni.
- Ogni reparto deve mettere a punto un protocollo operativo contenente le procedure che, in caso di interruzione del servizio del sistema informatico, garantiscono la continuità del flusso informativo
- Competenza, prettamente tecnica, affidata al CED ed al servizio assistenza

Pertanto è consigliabile:

Predisporre moduli da compilare a cura dell'operatore fra cui :

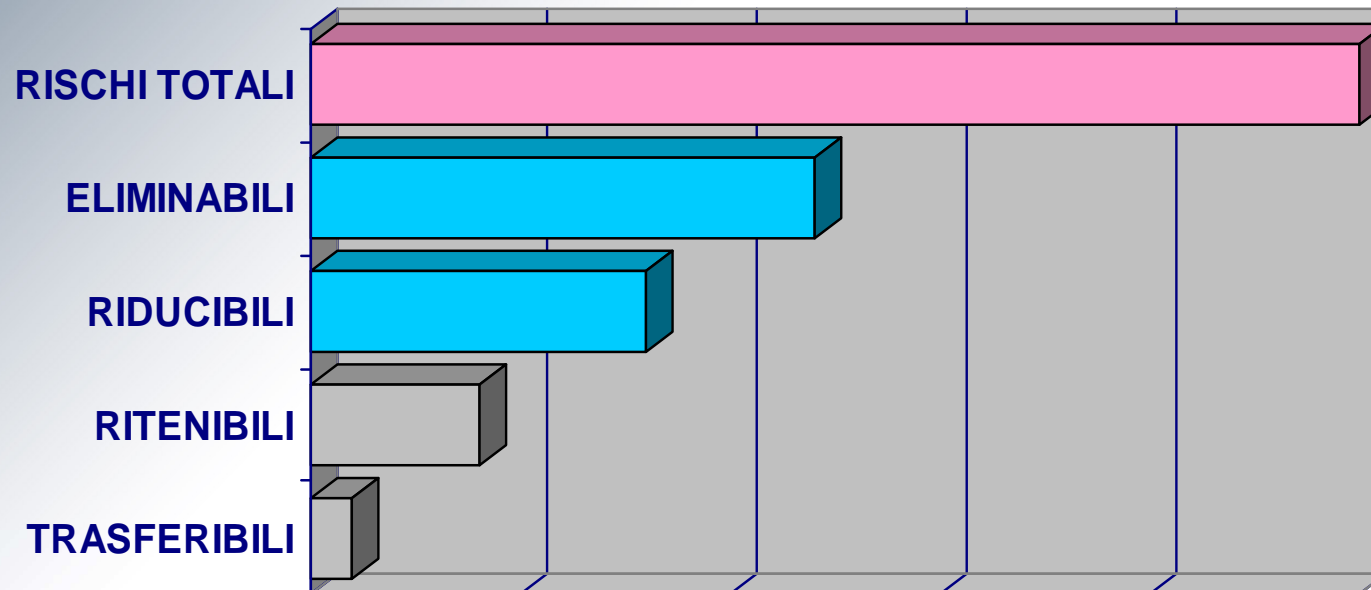
- Frontespizio Cartella Clinica
- Lettera per USL
- Etichette per ricovero
- Modulo ordini Esami di Laboratorio
- Modulo ordini Esami Diagnostica Strumentale

Analisi dei rischi

E' una fase fondamentale nella realizzazione di un sistema di sicurezza per le informazioni. Aiuta a delineare la direzione verso cui i futuri provvedimenti dovranno essere condotti e dà una buona valutazione per l'acquisizione e l'uso delle contromisure di sicurezza. La loro cieca applicazione, senza prima aver compreso i rischi a cui può essere soggetto un sistema di sicurezza per le informazioni, è quasi sempre poco produttiva, sia dal punto di vista economico che tecnico.

Quando si conduce un'analisi dei rischi per un sistema di sicurezza per le informazioni bisogna tenere presente che non è possibile avere un sistema totalmente libero da qualunque rischio

Classificazione dei rischi rilevati e potenziali



IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

Classificazione dei rischi rilevati e potenziali

- Eliminabili:** troppo pericolosi e facili da eliminare
- Riducibili:** si possono ridurre operando sulla limitazione del danno con l'adozione di sistemi di controllo e di prevenzione
- Trasferibili:** non convenienti da gestire per cui vengono trasferiti ad altri
- Ritenibili:** il danno probabile è inferiore al costo di gestione e di trasferimento

Schema delle minacce

- Danneggiamento di software e di dati dovuto ad errori colposi
- Sabotaggio dei dati o di risorse software
- Virus
- Intrusioni nel sistema da parte di hackers
- Accessi da parte di soggetti interni alla struttura non autorizzati o con un diverso ambito di autorizzazione
- Danneggiamento doloso o colposo delle risorse informatiche
- Eventi naturali (allagamenti, incendi, eventi sismici, ecc..)
-

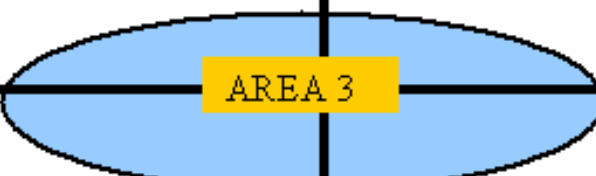



I beni sono compresi in 5 famiglie
cui è stata attribuita la seguente scala di valori:

– HW	valore 1	min
– SW	valore 2	
– RETI	valore 3	
– ORG	valore 4	
– DATI	valore 5	max

Per ogni evento esistono **scale relative** alla stima della **probabilità** e della **magnitudo**.

- Scala della **probabilità**:
 - 1- molto bassa;
 - 2- medio bassa;
 - 3-medio alta;
 - 4-elevata
- Scala della **magnitudo**:
 - 1- trascurabile;
 - 2- modesta;
 - 3-notevole;
 - 4-ingente

LA MATRICE DI RISCHIO

PROBABILITÀ					
ELEVATA					
MEDIO ALTA					
MEDIO BASSA					
BASSISSIMA					
	TRASCURABILE	MODESTA	NOTEVOLE	INGENTE	
		MAGNITUDO			

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

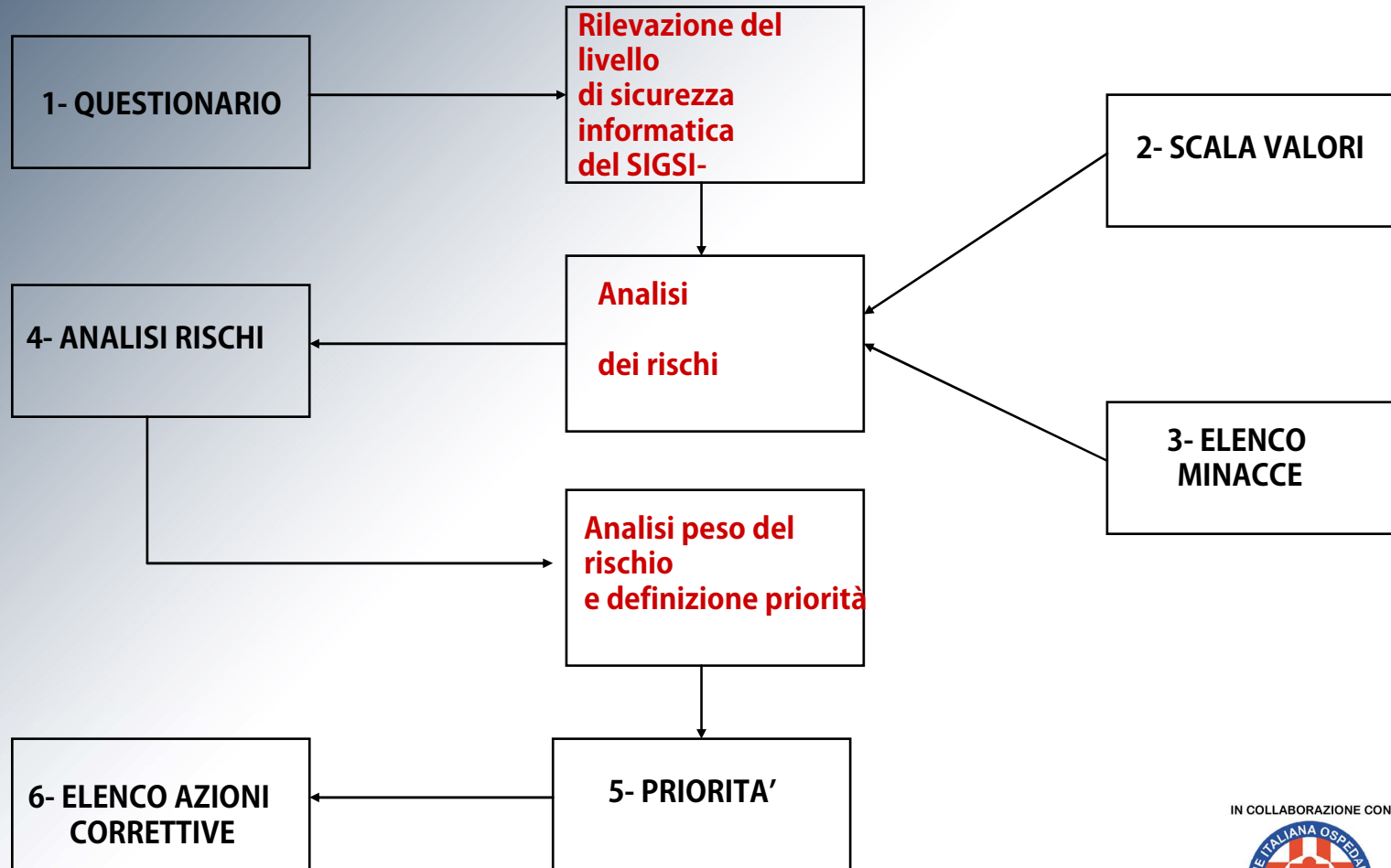
Rilevazione del livello di protezione

Dopo aver individuato i beni da proteggere e le minacce da cui difendersi, bisogna rilevare il livello di protezione del patrimonio informatico nei vari siti.

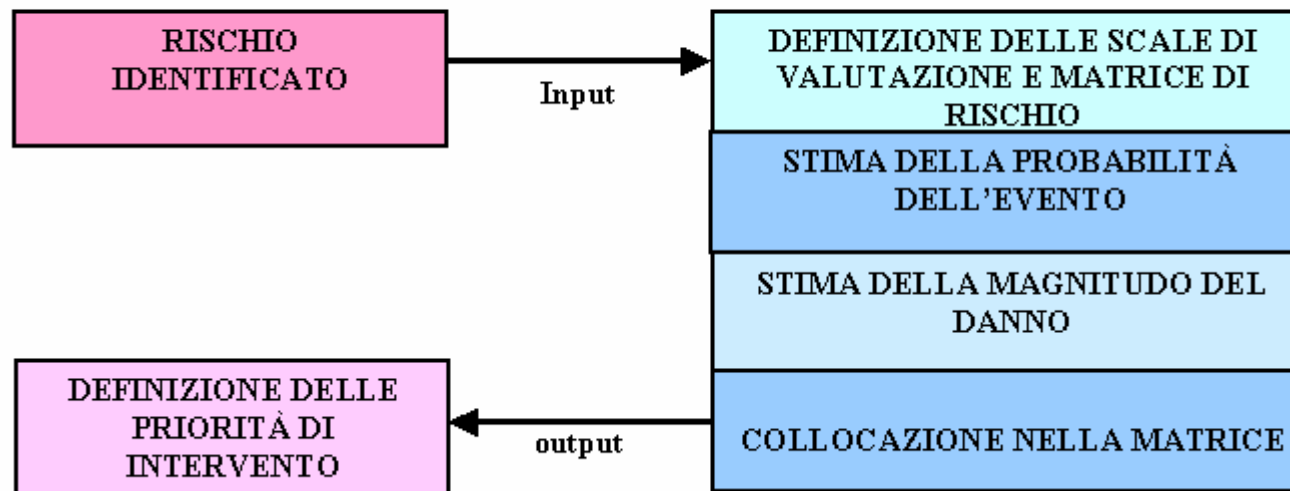
Lo strumento consigliato è quello dei questionari al fine di produrre valutazioni qualitative associando un punteggio alla risposta.

Il questionario mette oggettivamente in luce le carenze e permette di confrontare le valutazioni dei vari siti.

Schema della Procedura Analisi dei Rischi



VALUTAZIONE DEI RISCHI



Analisi Rischi Risultati

Tipo Minaccia	Priorità
Accesso nei locali di persone non autorizzate	17,42
Infiltrazione acqua nei locali server/supporti magnetici	14,40 (6,40)
Incendio locali supporti magnetici	13,50
Procedure non controllate di inserimento/variazione dati	11,90
Errore o cambio inserimento messaggi	11,43
Scarsa cultura aziendale in sicurezza delle informazioni	11,28
Errore non rilevato a carico Utente	11,20
Mancanza Piano di Gestione Continuità Aziendale	7,92

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

INTERVENTO PREVENTIVO E PROTETTIVO

PROBABILITÀ				
ELEVATA				
MEDIO ALTA			A	
MEDIO BASSA		B	prevenzione	
BASSISSIMA	protezione			
	TRASCURABILE	MODESTA	NOTEVOLE	INGENTE
MAGNITUDO				

ON

INTEGRARE I SISTEMI PER MIGLIORARE LA QUALITÀ DELL'ASSISTENZA, Bologna 7 aprile 2006



Livello sicurezza del patrimonio delle informazioni	Totali			
	Totalmente inadeguato	Inadeguato	Sufficiente	Totalmente adeguato
	1	2	3	4
1 Politica della sicurezza				
2 Organizzazione della sicurezza				
3 Classificazione delle risorse				
4 Sicurezza del personale				
5 Sicurezza fisica ed ambientale				
6 Gestione operativa del sistema informatico				
7 Controllo accessi				
8 Sviluppo e manutenzione del sistema informativo				
9 Gestione continuità				
10 Conformità				
11 Informazioni/trattamento dati personali sensibili su rapporto cartaceo				
12 Trattamento dati personali sensibili con sistemi PEMS				
Totale				
Totale generale				

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

Esperienze a confronto: l'approccio integrato alla gestione del rischio clinico, organizzativo e strutturale
Prof. Bruno Turinetti - Hesperia Hospital, Modena

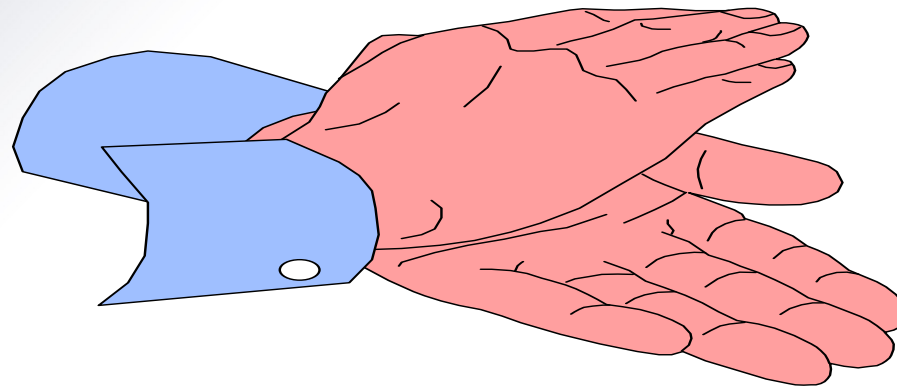
Riepilogo individuazione domini critici

	Obiettivi di controllo	Valutazione
11	<i>Trattamento dati personali su supporto cartaceo</i>	1,7
10	Conformità	2,3
7	Controllo accessi	2,6
12	<i>Trattamento dati personali con sistemi PEMS</i>	2,7
8	Sviluppo e manutenzione del sistema informativo	3,0
1	Politiche della sicurezza	3,0
9	Gestione continuità	3,0
3	Classificazione risorse	3,3
4	Sicurezza del personale	3,3
6	Gestione operativa del sistema informatico	3,3
5	Sicurezza fisica ed ambientale	3,3
2	Organizzazione della sicurezza	3,6

INTEGRARE I SISTEMI PER MIGLIORARE
LA QUALITÀ DELL'ASSISTENZA, Bologna 7 aprile 2006



GRAZIE
per l'attenzione...



Esperienze a confronto: l'approccio integrato alla gestione del rischio clinico, organizzativo e strutturale
Prof. Bruno Turinetti - Hesperia Hospital, Modena

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani