

Principali criticità e vulnerabilità in una organizzazione sanitaria







Ing. Maurizio Grande (Direttore Northon M.C.)

Le minacce alla sicurezza delle informazioni

Le minacce

Una minaccia è un agente ostile che può potenzialmente causare una violazione dell'integrità, riservatezza e utilizzabilità dei dati e delle risorse del Sistema delle Informazioni. Le classificazioni che possono essere date delle minacce sono varie, ad esempio possono essere suddivise in *fattori accidentali* e *fattori intenzionali*.

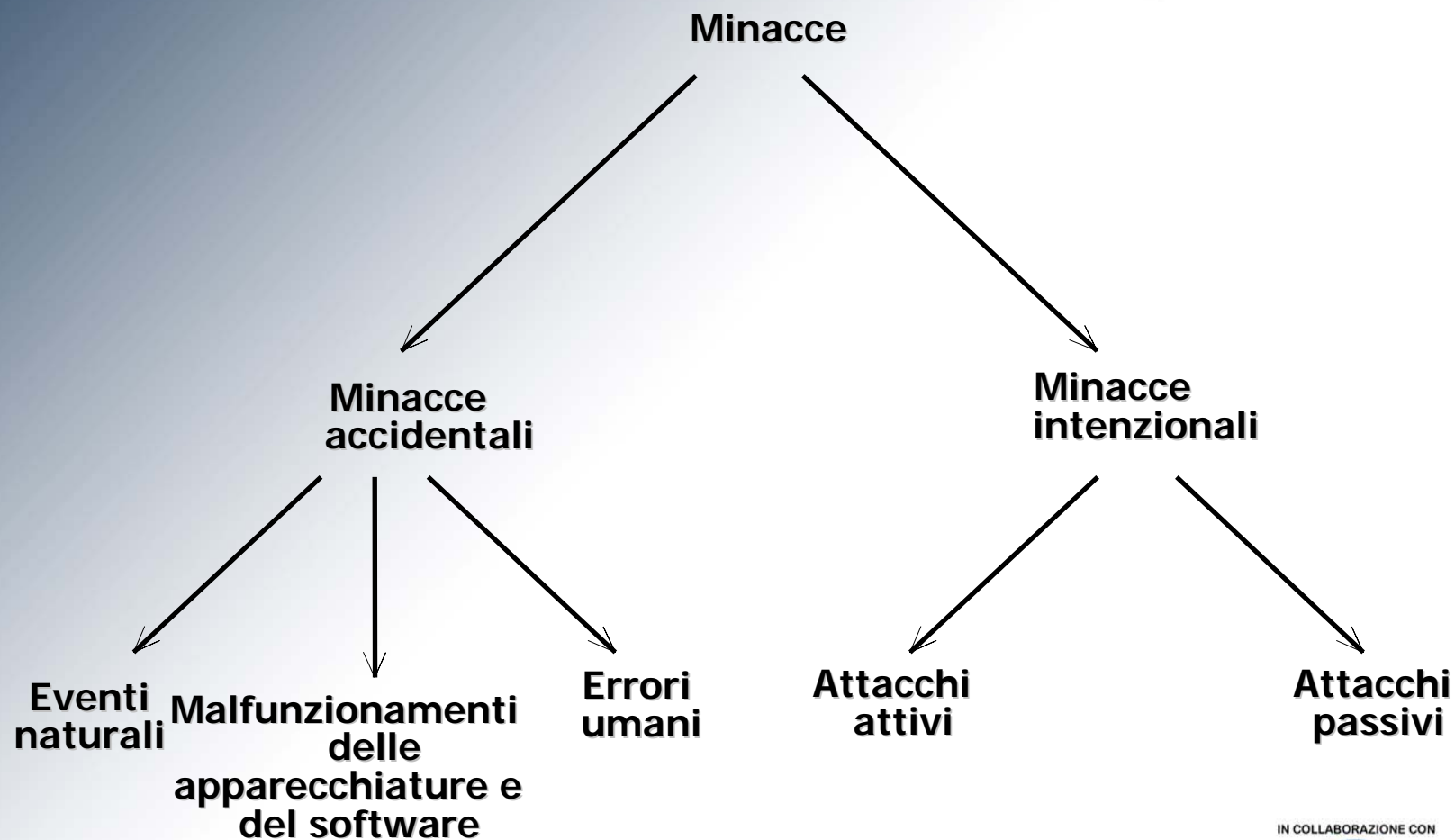
Classificazione delle minacce

-  **Fattori naturali**
-  **Errori ed omissioni**
-  **Personale scontento**
-  **Personale disonesto**
-  **Utenti autorizzati**
-  **Agenti ostili...**

Qualunque sia la classificazione che si dà alle minacce, esse, in generale, possono sempre essere viste come una qualsiasi cosa che può portare ad una violazione del Sistema delle Informazioni.

Le violazioni possono avere i seguenti effetti:

- 👉 **Rilascio di informazioni non autorizzato:** rientrano in questa categoria tutti gli attacchi alla riservatezza delle informazioni.
- 👉 **Modifica non autorizzata, accidentale o intenzionale, delle informazioni:** è la violazione della integrità dei dati, che porta ad una impropria manipolazione o modifica delle informazioni.
- 👉 **Non autorizzata negazione d'uso:** rientrano in questa categoria quelle azioni che possono impedire l'utilizzo delle risorse e l'accesso alle informazioni da parte di utenti autorizzati.



Minacce tipiche di un sistema informativo sanitario

Tipo di minaccia	Tipo di impatto	Strumenti o beni coinvolti
Minacce fisiche	Danni da incendio	Tutti i beni che si trovano nella stessa area
	Danni da acqua	Tutti i beni che si trovano nella stessa area
	Danni da intemperie od altri disastri naturali	Tutti i beni che si trovano nello stesso sito od in uno stesso edificio
	Sabotaggio e danno deliberato	Gruppi di beni che si trovano nella stessa area
	Furto	Beni singoli, beni isolati o gruppi di beni

IN COLLABORAZIONE CON



Consulta Nazionale Aioip Giovani

LA SICUREZZA DELLE INFORMAZIONI
IN UNA ORGANIZZAZIONE SANITARIA:
OBBLIGO O STRATEGIA? Bologna 16 giugno 2006



Minacce tecniche	Accesso non autorizzato	Potenzialmente, l'intero sistema
	Uso improprio di risorse informative	Potenzialmente, l'intero sistema
	Guasto del sistema	Potenzialmente, l'intero sistema
	Guasto HW	Beni individuali e gli strumenti connessi o dipendenti

LA SICUREZZA DELLE INFORMAZIONI
IN UNA ORGANIZZAZIONE SANITARIA:
OBBLIGO O STRATEGIA? Bologna 16 giugno 2006



Minacce ambientali	Mancanza di energia di alimentazione	Beni individuali o gruppi di beni che usano la stessa sorgente di energia (potenzialmente, l'intero sistema)
	Guasto dei controlli ambientali	Beni individuali o gruppi di beni che usano gli stessi controlli ambientali
Minacce da errore umano	Errore umano	Beni che sono gestiti, usati, sviluppati o mantenuti dal personale. Potenzialmente, intero sistema

Analisi dei rischi

Analisi dei rischi

- ➡ **Fondamentale nel realizzare un sistema di sicurezza delle informazioni**
- ➡ **Permette di delineare la strategia ottimale**
- ➡ **Valuta la corretta acquisizione ed il corretto uso delle contromisure da adottare**

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 che sia totalmente libero da qualunque rischio.

Metodo semi-qualitativo

Il metodo è una combinazione di analisi soggettiva e di pragmatico raziocinio che si basa sull'esperienza di chi effettua l'analisi e sulla capacità di stabilire termini reali di riferimento e di controllo.



Il termine *soggettivo* non deve essere inteso come arbitrario e la valutazione dei rischi con questo approccio deve essere vista come giudizio esperto, legata cioè alla *professionalità* derivante dall'*esperienza* e dalla *conoscenza* dei molteplici fattori in gioco.

L'approccio semi-qualitativo è basato sulla definizione di scale relative nella stima della probabilità e della magnitudo.





Esempi di scala della probabilità:

- 1- molto bassa;
- 2- medio bassa;
- 3- medio alta;
- 4- elevata

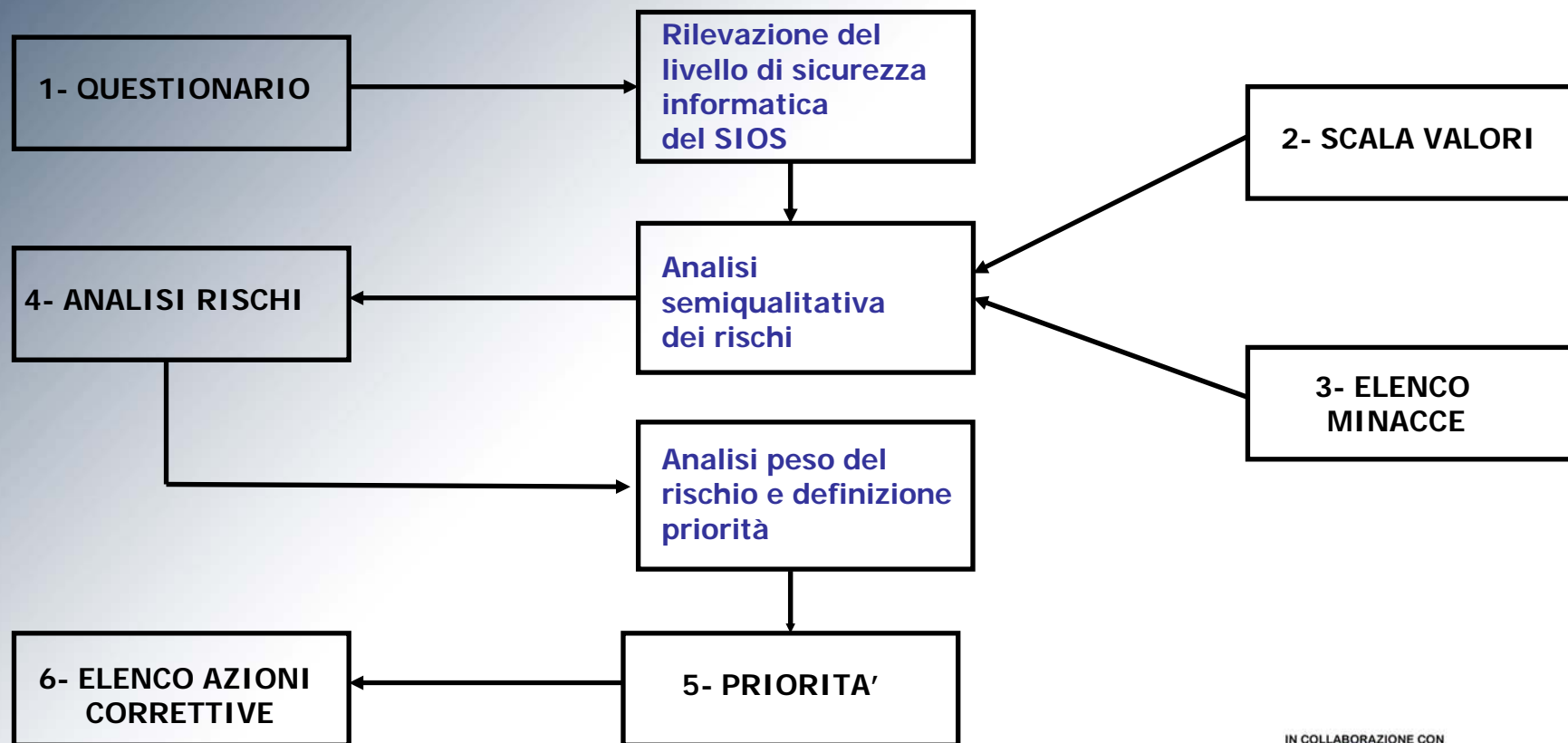
Esempi di scala della magnitudo:

- 1- trascurabile;
- 2- modesta;
- 3- notevole;
- 4- ingente

LA MATRICE DI RISCHIO

PROBABILITÀ				
ELEVATA	 <p>AREA 3</p>		 <p>AREA 1</p>	
MEDIO ALTA				
MEDIO BASSA	 <p>AREA 4</p>		 <p>AREA 2</p>	
BASSISSIMA				
	TRASCURABILE	MODESTA	NOTEVOLE	INGENTE
	MAGNITUDO			

SCHEMA DELLA PROCEDURA ANALISI DEI RISCHI



Risultati del questionario di analisi del rischio nel gruppo di lavoro progetto SIOS

Tabella Riassuntiva Analisi Rischi GdL/SIOS

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 instradamento o cambio instradamento 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

Domini critici individuati dal GdL/SIOS

	Obiettivi di controllo	Valutazione
11	Trattamento dati personali su supporto cartaceo	1,7
10	Conformità	2,3
7	Controllo accessi	2,6
12	Trattamento dati personali con sistemi PEMS	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






Specificità SIOS

- 👉 **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 da PEMS**
- 👉 **Le cartelle cliniche (GOLDEN DATA) sono su supporto cartaceo**

Specificità SIOS

- 👉 I dati da PEMS a volte stampati e sovrascritti a volte archiviati in modo digitale (responsabilità singola U.O.)
- 👉 I dati su supporto cartaceo sono in quantità rilevante
- 👉 Il Controllo Accessi (Sicurezza Fisica) contrasta con la cultura/storia delle strutture sanitarie di fatto "open space"

Principali Criticità SIOS

-  **Definizione del livello di struttura organizzativa su cui effettuare l'analisi rischio.**
-  **La gestione della Cartella Clinica cartacea è l'aspetto più critico: quale soluzione adottare?**
-  **Come gestire l'eterogeneità dei dati PEMS?**
-  **La sensibilità del personale medico e paramedico alla sicurezza delle informazioni: basta l'intervento della Direzione?**
-  **Le regole di comportamento organizzativo formalizzate per la privacy sono sufficienti per implementare un SIOS efficace e certificabile?**