# Il trattamento di dati sanitari: l'esperienza dell'Istituto di Fisiologia Clinica

*Raffaele.Conte @ ifc.cnr.it*

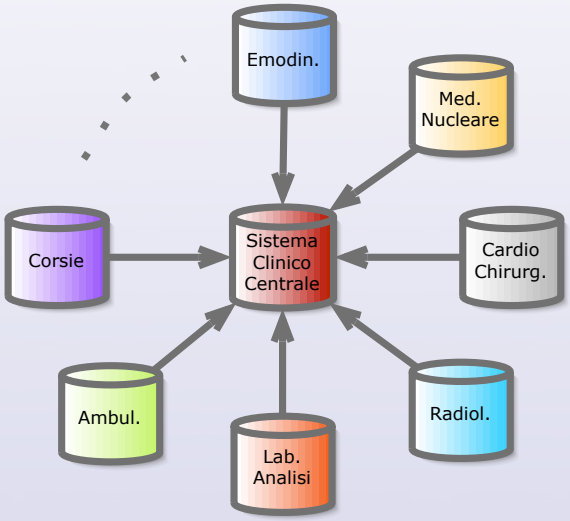
*STeP - Sicurezza Tutela e Privacy, 6 Dicembre 2006*

Istituto di Fisiologia Clinica

# Il contesto: l'Istituto di Fisiologia Clinica

Sede e sezioni IFC


Organizzazione logica sistema clinico




Istituto di Fisiologia Clinica

# Problematiche di una rete particolare

- Conciliare la “libertà” tipica di un ambiente di ricerca con la necessità di rendere “sicuro” il sistema informativo

# Il sistema informativo

- sistema: insieme organizzato di elementi, di natura diversa, che interagiscono tra loro (uomini, risorse, strumenti e procedure)
- informativo: tutto ciò che è finalizzato alla gestione delle informazioni (raccolta, archiviazione, elaborazione e scambio)

# Sicurezza in un sistema informativo

Secondo la definizione ISO la sicurezza di un sistema informativo è l'insieme delle misure atte a garantire

- ☑ la disponibilità,
- ☑ l'integrità,
- ☑ la riservatezza,

delle informazioni gestite.

Tutte caratteristiche critiche in IFC!!

# Obiettivo della sicurezza

- Ridurre al minimo le possibilità di compromissione del sistema informativo
- Essere preparati a ripristinare il servizio in tempi rapidi (*disaster recovery*)

# L'approccio al problema

| | Eventi accidentali | | Eventi dolosi | |
|---|---|---|---|---|
| | Fisici | Logici | Fisici | Logici |
| Disponibilità | 1 | 2 | 3 | 4 |
| Integrità | 1 | 2 | 3 | 4 |
| Riservatezza | ! | ! | 3 | 4 |

1. *Fallimenti hardware, interruzione dei sistemi di alimentazione o condizionamento, disastri*
2. *Errori umani*
3. *Furti o danneggiamenti di strumenti o supporti di memorizzazione*
4. *Intrusioni, intercettazioni (sniffing), attacchi di disturbo (virus, worm, Denial of Service)*

# Prime soluzioni adottate

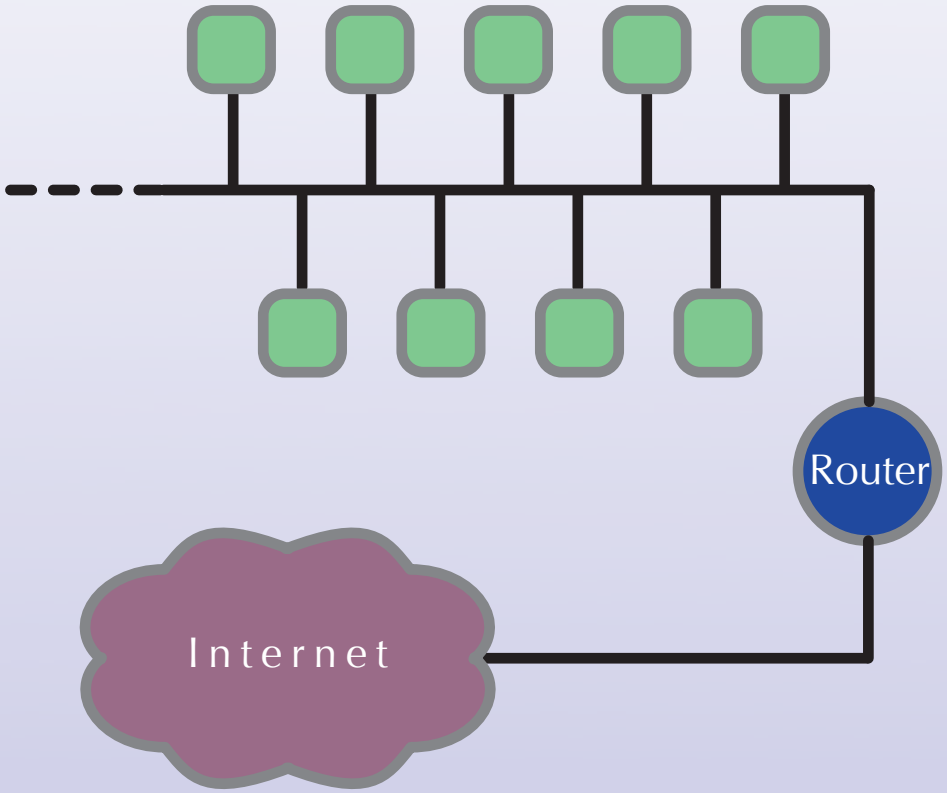
Sicurezza fisica

- ☑ ups (gruppi di continuità), doppia alimentazione
- ☑ siti ad accesso limitato
- ☑ sistemi duplicati in siti distanti e su linee elettriche diverse
- ☑ sist. di condizionamento aggiuntivi
- ☑ backup su nastro
- ☑ ridondanza hw (macchine di backup, RAID ecc.)

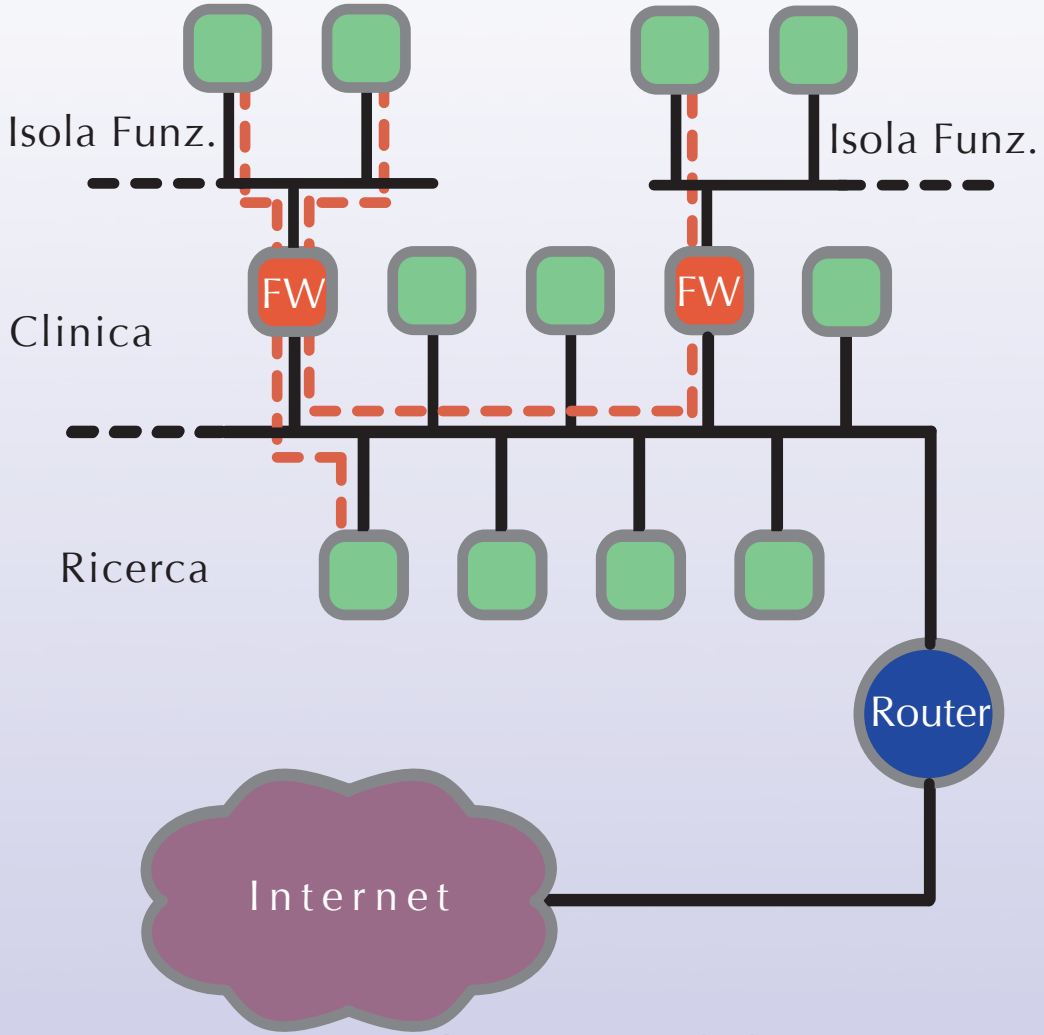
Sicurezza logica

- ☑ fw “a ridosso” delle macchine critiche
- ☑ cifratura delle comunicazioni (ssl/tls, vpn)

# L'infrastruttura: prima soluzione



# L'infrastruttura: prima soluzione



# Problemi irrisolti

- Difficoltà nel cifrare tutte le connessioni (dati sensibili esposti ad utenti ospiti)
- Eventuali malfunzionamenti su un apparato di rete in area si ripercuotevano anche sulla rete di IFC
- I FW costituiscono dei Point Of Failure, bloccando l'attività clinica

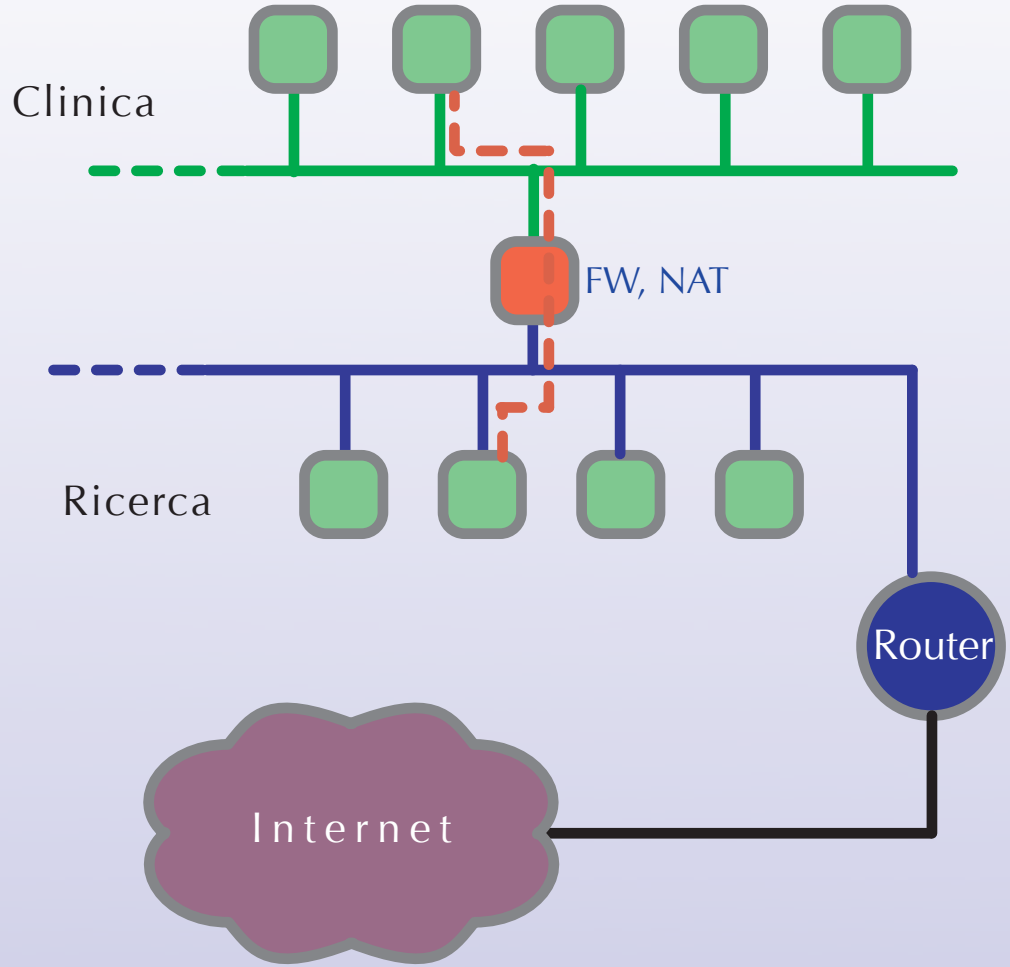
# Problemi irrisolti

- Manutenzione dei server e disponibilità dei servizi
- Autenticazione e Autorizzazione
- Uso improprio degli strumenti

# Attività conseguenti

- Separazione del traffico clinico/ricerca
- Riorganizzazione dei servizi di rete
- Sistemi di monitoraggio
- Sistemi per autenticazione centralizzata e gestione dei diritti di accesso (AAI)
- Documentazione / DPS

# Separazione traffico clinico/ricerca



# Separazione traffico clinico/ricerca: benefici

- Tutti i dati sensibili non transitano dalla rete di ricerca
- Eventuali malfunzionamenti sul FW non bloccano l'attività clinica
- Malfunzionamenti sugli apparati in area possono ripercuotersi sulla rete di ricerca ma non su quella clinica

# Separazione traffico clinico/ricerca: effetti collaterali

Rete clinica

- maggiori restrizioni da e verso rete IFC/ Internet

Rete ricerca

- maggiore complessità per l'accesso alla rete clinica

# Riorganizzazione servizi di rete

- Ridurre il periodo di interruzione del servizio (*downtime*) cercando un equilibrio fra la centralizzazione e la distribuzione
- Avere la conoscenza di ciò che avviene sulla rete (monitoraggio)

  es.
  - https://medusa.ifc.cnr.it/nagios/
  - https://medusa.ifc.cnr.it/cacti/

# Autenticazione e Autorizzazione: problemi

- Assunzione di responsabilità
- Debolezza credenziali di accesso
- Password di reparto!!!
- Accesso ai dati differenziato per tipologia di utenza (infermiere, medico, amministrativo, ecc.)
- Coerenza delle informazioni sugli utenti gestite su diversi sistemi
- Estrema volatilità del personale (laureandi, dottorandi, specializzandi, infermieri, ospiti ecc.)

# Gli obblighi di legge 1/2

**“Codice in materia di protezione dei dati personali” (D.L. 30/6/2003, n. 196)**

**Art. 3 (Principio di necessità nel trattamento dei dati)**

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

**Art. 34 (Trattamenti con strumenti elettronici)**

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate [...] le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

...

# Gli obblighi di legge 2/2

**D. L. 196/2003, ALLEGATO B - DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA**

**Sistema di autenticazione informatica**

[...]

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

[...]

**Sistema di autorizzazione**

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

# Autenticazione e Autorizzazione: soluzione

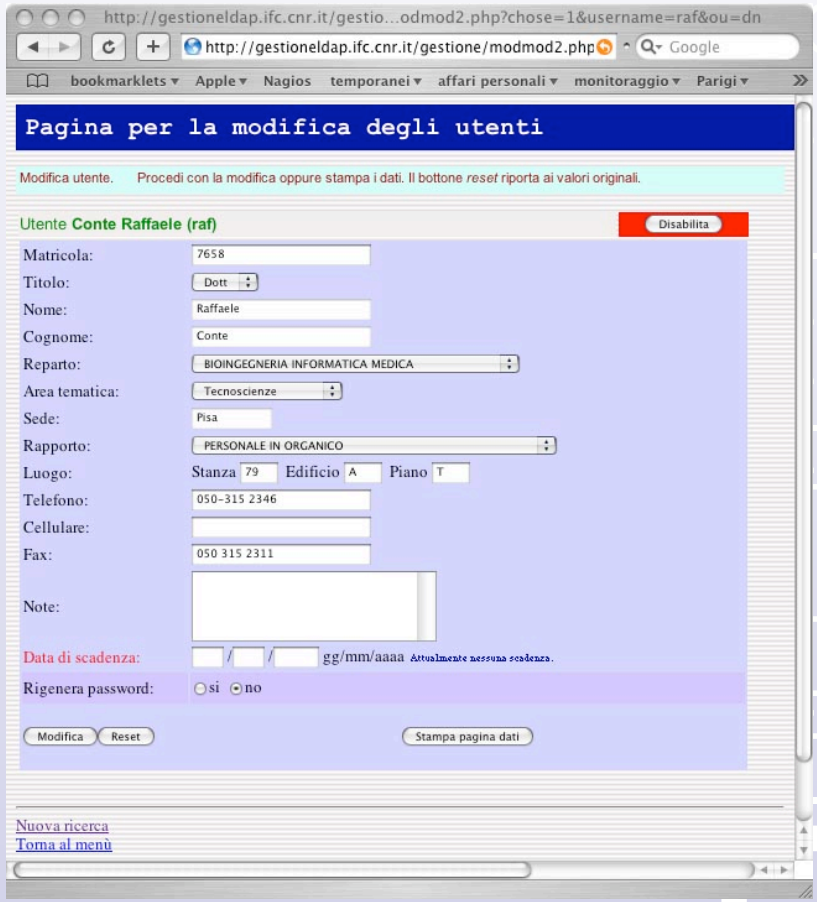
Sistema centralizzato per la gestione dei profili utente (AAI - *Authentication and Authorization Infrastructure*)

- Standard: LDAP (RFC 1777, RFC 2251)
- Propedeutico all'utilizzo di meccanismi di autenticazione forte

# AAI: centralizzazione del profilo utente 1/2

Il profilo è gestito esclusivamente dall'"Ufficio del personale"

- ☑ conosce la situazione aggiornata sul movimento del personale
- ☑ può gestire i dati in maniera "distribuita" fra le diverse sedi/ sezioni
- ☑ crea il profilo solo dopo aver ottenuto il modulo di "Assunzione di Responsabilità"
- ☑ può gestire più rapidamente rinnovi e scadenze



# AAI: centralizzazione del profilo utente 2/2

È possibile soddisfare alcune misure richieste dal DL 196/'03

- ☑ scadenza password (art. 5, all.B)
- ☑ assegnazione univoca degli userid (art. 6, all. B)
- ☑ disabilitazione account per inutilizzo (art. 7, all. B)

# AAI: autorizzazione “implicita”

- Filtri

  es.

  1. cerca l’utente con il profilo:
     username = *raf*
     reparto = *BIM*
     qualifica = *medico*

  2. **Se esiste**: autentica con password xxxxx

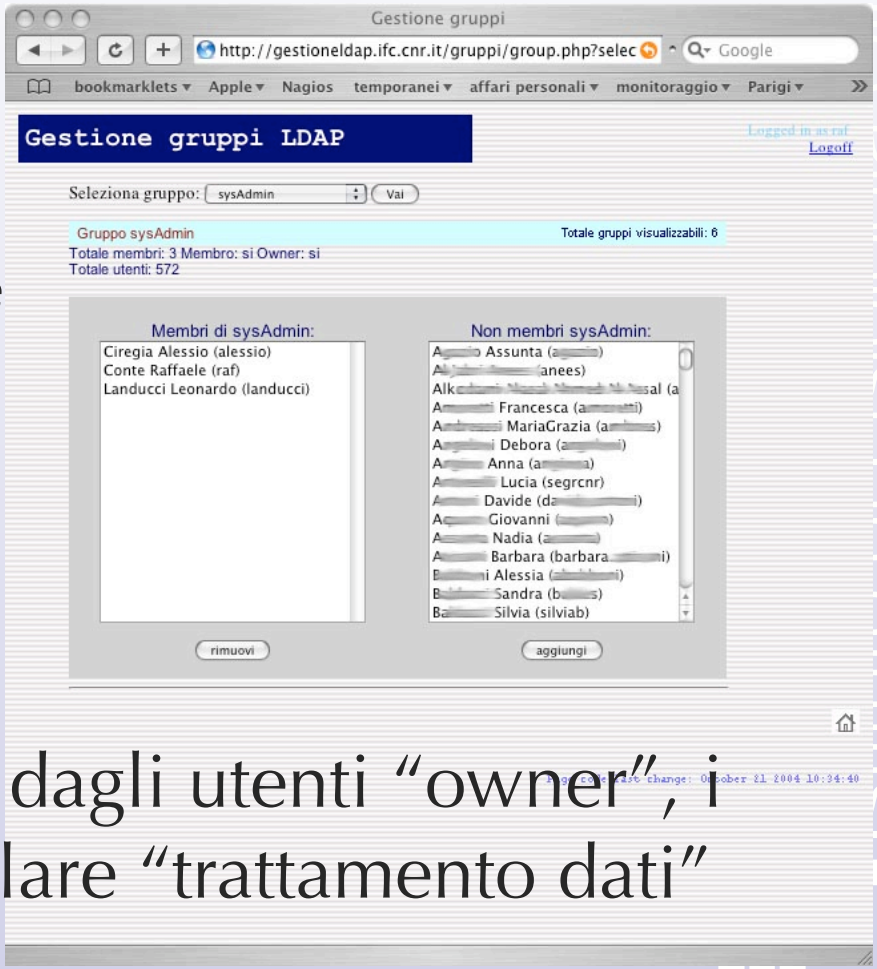
- I filtri vengono impostati preventivamente sui servizi che devono offrire accesso ai dati

# Autorizzazione “esplicita”

- Gruppi:

es.

1. cerca l’utente con username = *raf* e appartenente al gruppo “Consiglio Scientifico”
2. **Se esiste**: autentica con password xxxxx




I gruppi vengono gestiti dagli utenti “owner”, i responsabili del particolare “trattamento dati”

# AAI: vantaggi e svantaggi

## vantaggi

- creazione e modifica dei profili utente gestita da chi possiede le informazioni sugli utenti (Ufficio del Personale) senza intermediari
- le informazioni sugli utenti sono centralizzate ma automaticamente replicate
- il personale tecnico cura gli aspetti tecnologici piuttosto che amministrativi
- gestione delle autorizzazioni effettuata dal responsabile del servizio o del particolare trattamento dati
- immediata propagazione della "revoca di tutti diritti" (disabilit. utente)

## svantaggi

- tutti i servizi che richiedono autenticazione devono essere cifrati o utilizzare meccanismi di *autenticazione forte*
- carpita la password di un utente si può accedere a tutti servizi per i quali questi è autorizzato (discutibile!!!)

# AAI: estensioni

- Single Sign-On in associazione
- autenticazione dispositivi di rete
- DNS e conseguente autorizzazione utenti/macchine centralizzata su LDAP
- indirizzario utenti
- autorizzazioni per ruolo/orario
- ...

# Uso improprio degli strumenti

Documentazione

- ☑ Seminari
- ☑ FAQ - Frequently Asked Questions
- ☑ DPS dettagliato

# Il Documento Programmatico sulla Sicurezza

in IFC:

- strutturato in tabelle e schede analitiche
- sezione comune per i punti 1,2 e 7
- documenti specifici, relativi ad ogni sottosistema (isola funzionale) per gli altri punti gestiti da persone diverse

# DPS: strumento utile o obbligo di legge?

Per tenerlo aggiornato occorre uno strumento per la stesura collaborativa di documenti in rete:

- Wiki http://it.wikipedia.org/wiki/Wiki

# Grazie!

Domande?