Misure di Sicurezza AgID

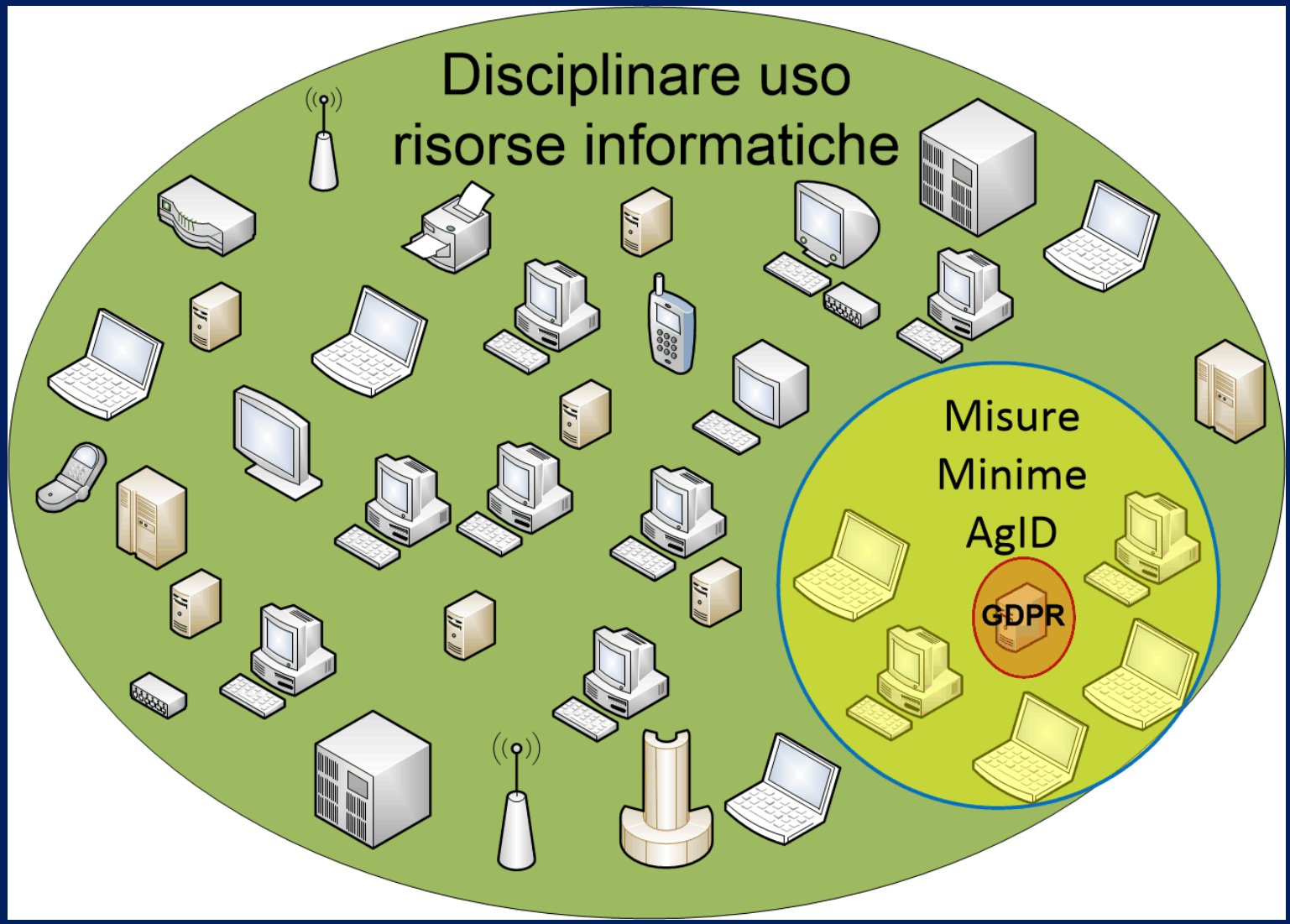
Mauro Nanni
Istituto di Radioastronomia
Sistemi Informativi per il Digitale

La sicurezza e' stato oggetto di attenzione da parte dei system

- Utilizzando regolamenti di utilizzo
  - Regole di accesso del GARR
  - Regolamenti delle singole strutture
- Seguendo le indicazioni del CERT
- Separando le reti (VLAN)
- Intervenendo sulle porte del router
  - a volte in modo eccessivo ☺

Non sempre in modo omogeneo all'interno dell'Ente !

Ambiti delle regole di sicurezza



Disciplinare uso risorse

Regolamento da applicare indifferentemente a tutte le risorse informatiche dell'Ente.

Per alcune di queste (15-20%) dovranno poi essere indicate regole piu' specifiche per ottemperare alle «**Misure Minime AgID**» ed alla «**GDPR**»

- Definire i soggetti
- Definire i compiti e responsabilita'
- Definire le regole di utilizzo
- Definire i tempi

La bozza e' disponibile sul DRIVE della GCSI in attesa di approvazione da parte del CdA

I Soggetti

- Utenti
- P.I. e Responsabile dei gruppi di ricerca
- Sistemisti
- Responsabile SID Locale
  - GCSI
  - CSIA
  - APM
- Direttore di Struttura
- Responsabile SID
- Responsabile ICT
- CPO

INAF e' : Una Pubblica Amministrazione Un Ente di ricerca

- Norme scritte per la P.A. pensando nei termini di Ministeri, Comuni, Regioni …

- >80% risorse dedicate alla ricerca astrofisica
  - tematica non sensibile e di interesse circoscritto

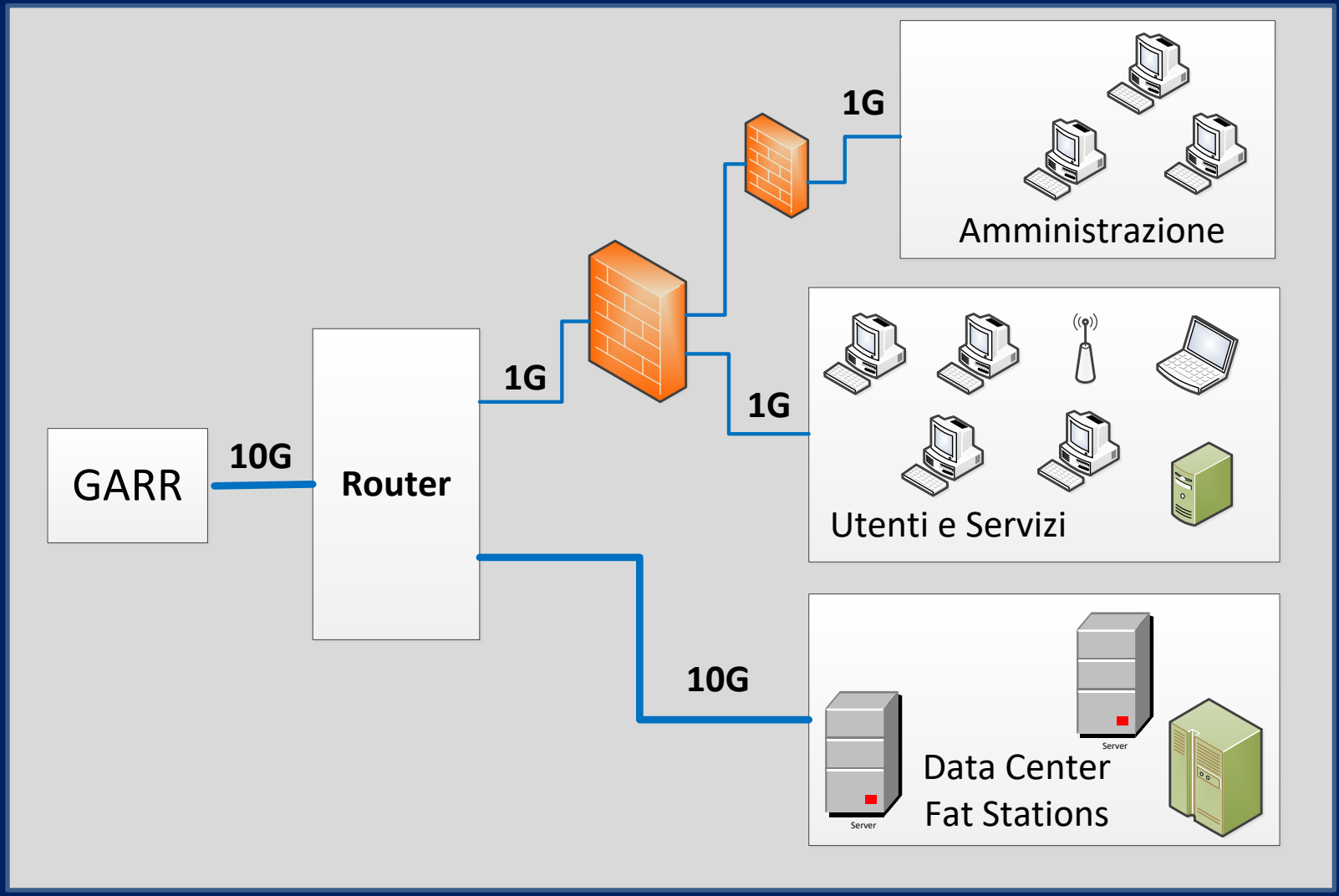
Da una parte :

Analisi dei rischi, Misure di sicurezza, Affidabilita'

Dall'altra:

Efficienza, larghezza di banda, open science

Separare i servizi dal calcolo



Misure di Sicurezza AgID

- Inventario dispositivi
- Inventario software
- Protezione
- Valutazione vulnerabilita'
- Privilegi amministratori
- Difese da malware
- Copie di sicurezza
- Protezione dati

Regole ragionevoli e coerenti. Alcune risultano particolarmente significative per applicazioni gestionali e appaiono naturali in un «ambiente Active Directory»

Regole Agid I

- Inventario dispositivi (Min++)
  - Gestione del DNS
  - Logging dei dispositivi DHCP (cellulari)
  - Monitoring traffico ed alert
  - Certificati
- Inventario dei Software
  - Software installato (Suite Office + ?)
  - Scansioni antivirus
  - S.O. delle WS «Standard» (le WS operano sopra tutto come terminali !)

Regole Agid II

- Protezione
  - Definire S.O. Standard (Win 10 ?)
  - Gestione del ripristino
  - Immagini memorizzate off-line (?)
  - Operazioni in ambiente sicuro
- Vulnerabilita'
  - Scansione delle vulnerabilita'
  - Aggiornamenti
  - Piano gestione dei rischi

Regole Agid III

- Administrator
  - Verifica competenze ed inventario admin
  - Registrare accessi con pw personali
  - Password > 14 caratteri ed aggiornate
  - Garantire disponibilita' e riservatezza (?!)
- Difesa da Malware
  - Rilevatori di presenza
  - Firewall ed IPS
  - Limitare dispositivi esterni (chiavette)
  - Filtrare Web e Spam e attachment
  - Disattivare automatismi (macro,mail)

Regole Agid IV

- Copie di sicurezza
  - Effettuare copie settimanali x ripristino
  - Proteggere i backup (riservatezza)
  - Mantenere copie off-line
  - Garantire disponibilita' e riservatezza (?!)
- Protezione Dati
  - Verificare quali sono «dati personali»
  - Bloccare traffico su siti in blacklist
  - Cifratura

Dove stanno i dati personali?

- Al Cineca (sensibili !)
- Al Sid (Bologna / Roma)

- Sui server delle amministrazioni
- Nei PC degli Uffici

L' Inventario delle utenze

In coerenza con la richiesta della Direzione di definire gli "organigrammi delle strutture" e per ottemperare alle "Misure di sicurezza AgID " che prevedono :

> "Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata."

Utenze attive al 7/6/2018 presso la struttura : **IAPS**

istruzioni per segnalare le variazioni	
Utente Eliminato	~~gino pino~~
Nuovo utente	gino pino
Servizio disattivato	~~SI~~
Servizio attivato	SI

Struttura	Cognome	Nome	CSA						TEAM				H1	TNSJ			Civilia	Folium					
			Econ. Pers	Giuridico	Tutte funz.	Missi	Non Strutt	Anag	Tutte Funz	Utente base	Cassa Econ	Invent	Utente	verif	liquid	consult	fattura	Amm AOO	OP	OP Riserv	OP Uscita	Utente Riservato	Utente
IAPS ROMA					SI													SI	SI				
IAPS ROMA									SI														
IAPS ROMA																							SI
IAPS ROMA				SI		SI				SI				SI	SI				SI				
IAPS ROMA																							SI
IAPS ROMA																			SI				
IAPS ROMA						SI				SI				SI	SI								
IAPS ROMA													SI										SI
IAPS ROMA										SI													
IAPS ROMA																			SI				
IAPS ROMA													SI						SI				SI
IAPS ROMA													SI						SI				SI
IAPS ROMA										SI									SI				
IAPS ROMA										SI									SI	SI			
IAPS ROMA										SI									SI				
IAPS ROMA					SI	SI			SI				SI	SI	SI		SI	SI	SI	SI			SI
IAPS ROMA																							SI
IAPS ROMA																							SI
IAPS ROMA										SI									SI				
IAPS ROMA											SI		SI										
IAPS ROMA																			SI				
IAPS ROMA					SI								SI						SI				
IAPS ROMA																			SI				

Tabella verificata in data: 12/07/2018 da :

Inviato ad ogni struttura lo stato delle proprie utenze al 6/6/2018 [Matrice di 300x21]

Con Richiesta di verifica, correzione del file excel invio con firma.

Creare un Database che descrivesse **l'organigramma dei ruoli operativi** per il coordinamento, l'informazione e la formazione

Al di la' dei dati una considerazione

La richiesta era quella di avere un file firmato digitalmente, tutte le 16 strutture hanno risposto:

- 2 Strutture hanno scelto la soluzione ottimale dal punto di vista giuridico e informatico inviando un file excel.P7M (firma CADES)
- 4 Strutture hanno inviato 2 file (excel e stampa PDF firmata PADES)
- 6 Strutture hanno siglato in ascii o gif il file excel inviato (firma leggera)
- 4 Strutture hanno inviato la stampa PDF del file excel firmato e quindi firmato PADES o CADES

Scarsa familiarita' tecnica con la firma digitale e difficolta' a staccarsi dal modulo cartaceo e dalla "firma iin calce" , anche se cio' distrugge il contenuto digitale.

La firma CADES "imbusta" e firma file di qualunque tipo. Richiede solo programmi appositi (Dike, Arubasign …) per estrarre il file dalla busta.

La firma PADES si applica solo a file PDF , ma mantiene il PDF leggibile

Misure di Sicurezza in INAF

Uniformare le regole di sicurezza a tutte le strutture INAF

Disciplinare in approvazione dal CdA

Separare fisicamente le reti amministrative e scientifiche

Applicare le regole di Sicurezza AgID soprattutto alle risorse amministrative/gestionali