# *Gli aspetti informatici e organizzativi secondo il D.Lgs. 196/2003*

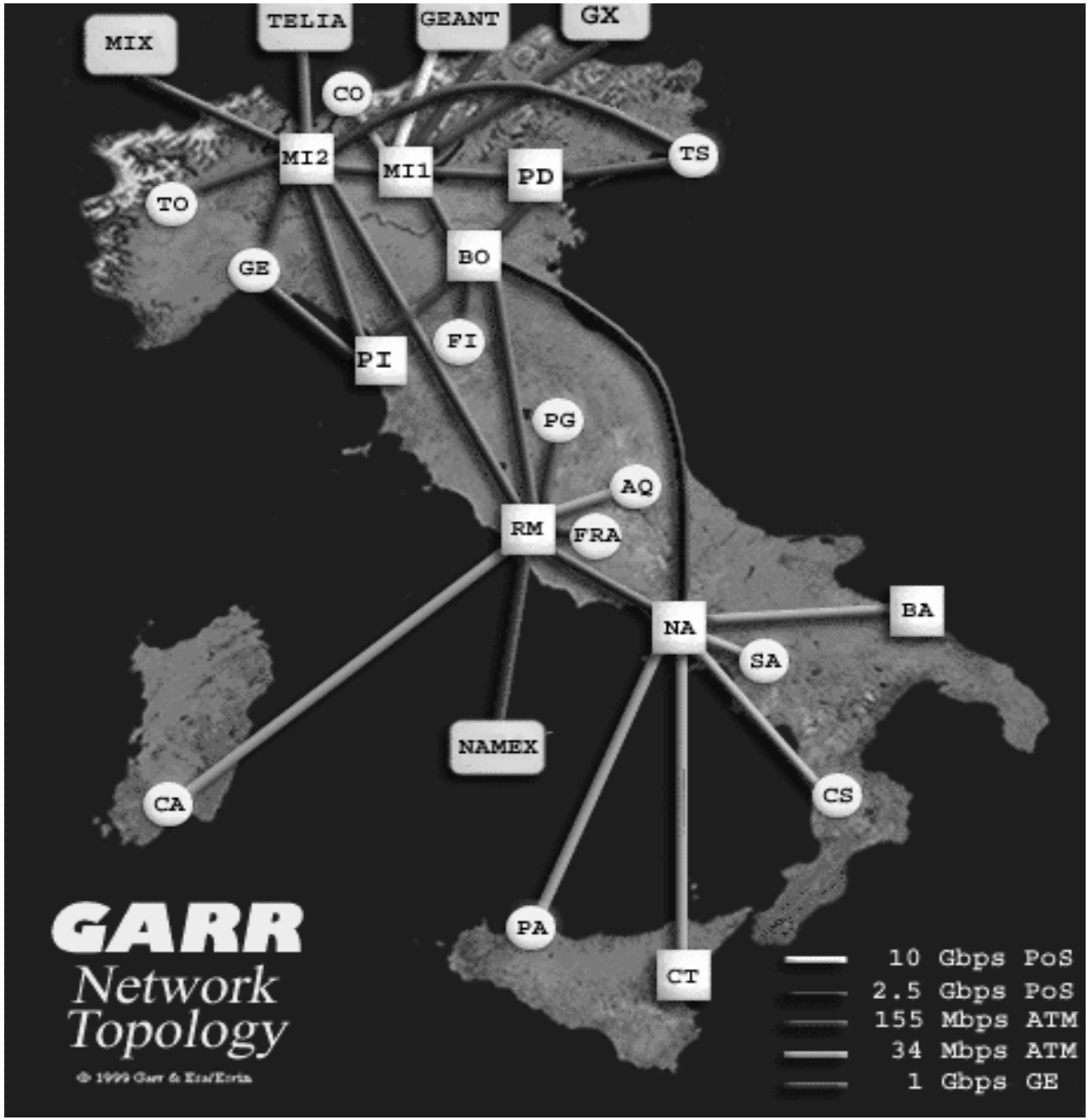
Dott. Massimo Tartamella

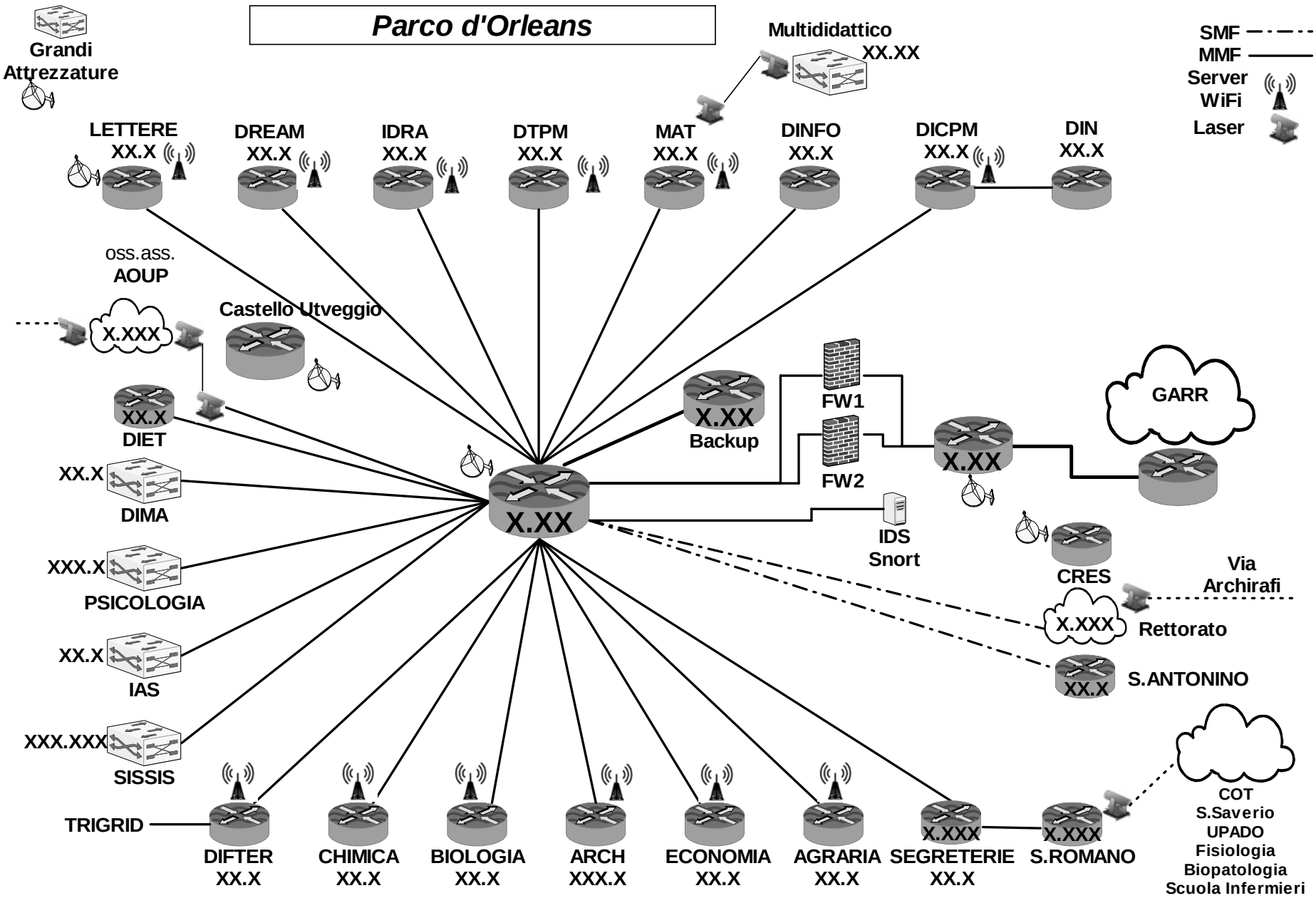
*Centro Universitario di Calcolo*

Università degli studi di Palermo

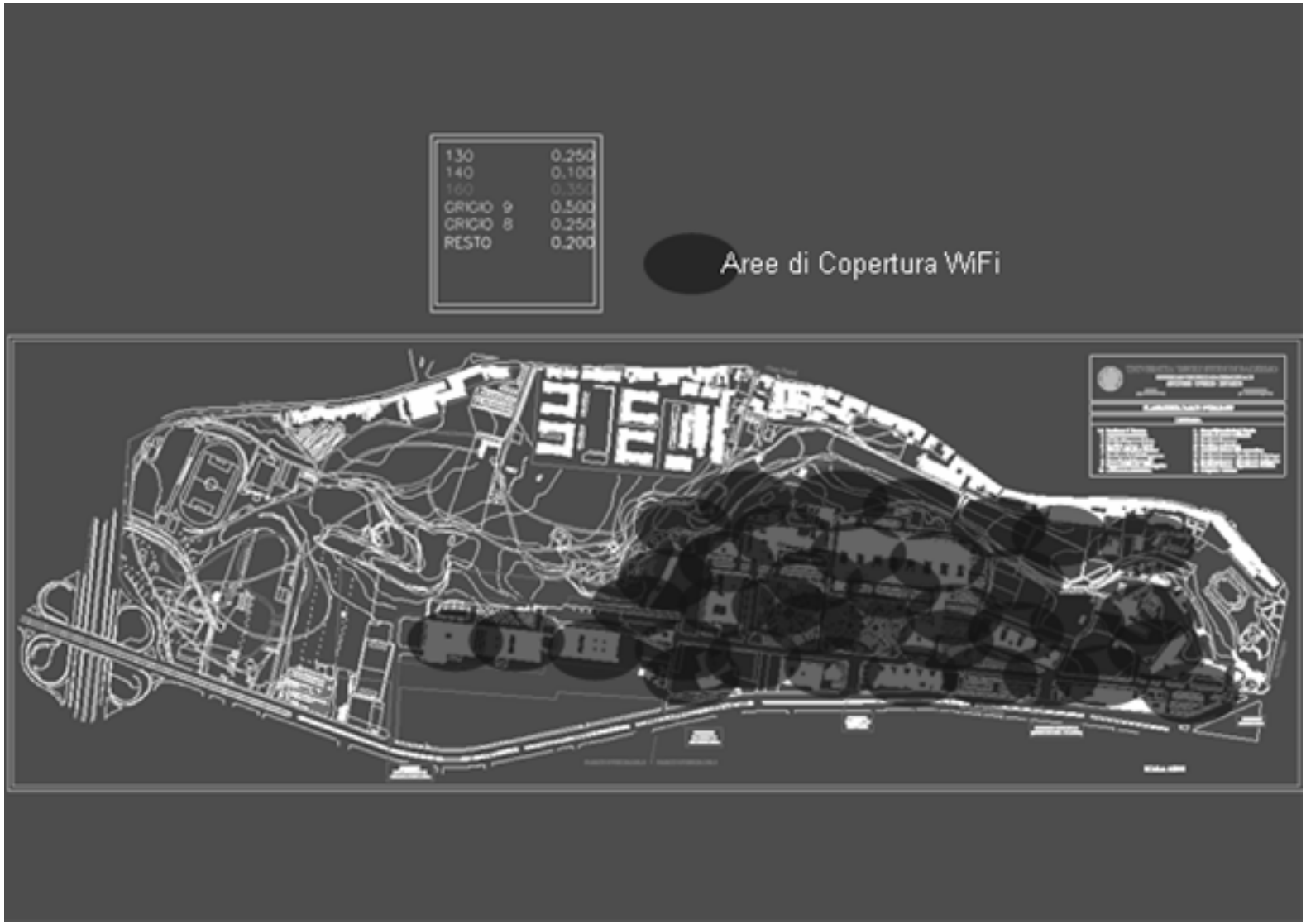
# D. Lgs 196/2003

- 01 PREMESSA: IL CONTESTO INFORMATICO UNIVERSITARIO
- 02 IL D. LGS. 196/2003 DAL PUNTO DI VISTA ORGANIZZATIVO
- 03 IL D. LGS. 196/2003 DAL PUNTO DI VISTA INFORMATICO


MIX
TELIA
GEANT
GX
CO
MI2
MI1
PD
TS
TO
GE
BO
FI
PI
PG
AQ
RM
FRA
BA
NA
SA
NAMEX
CA
CS
PA
CT
GARR
Network
Topology
10 Gbps PoS
2.5 Gbps PoS
155 Mbps ATM
34 Mbps ATM
1 Gbps GE

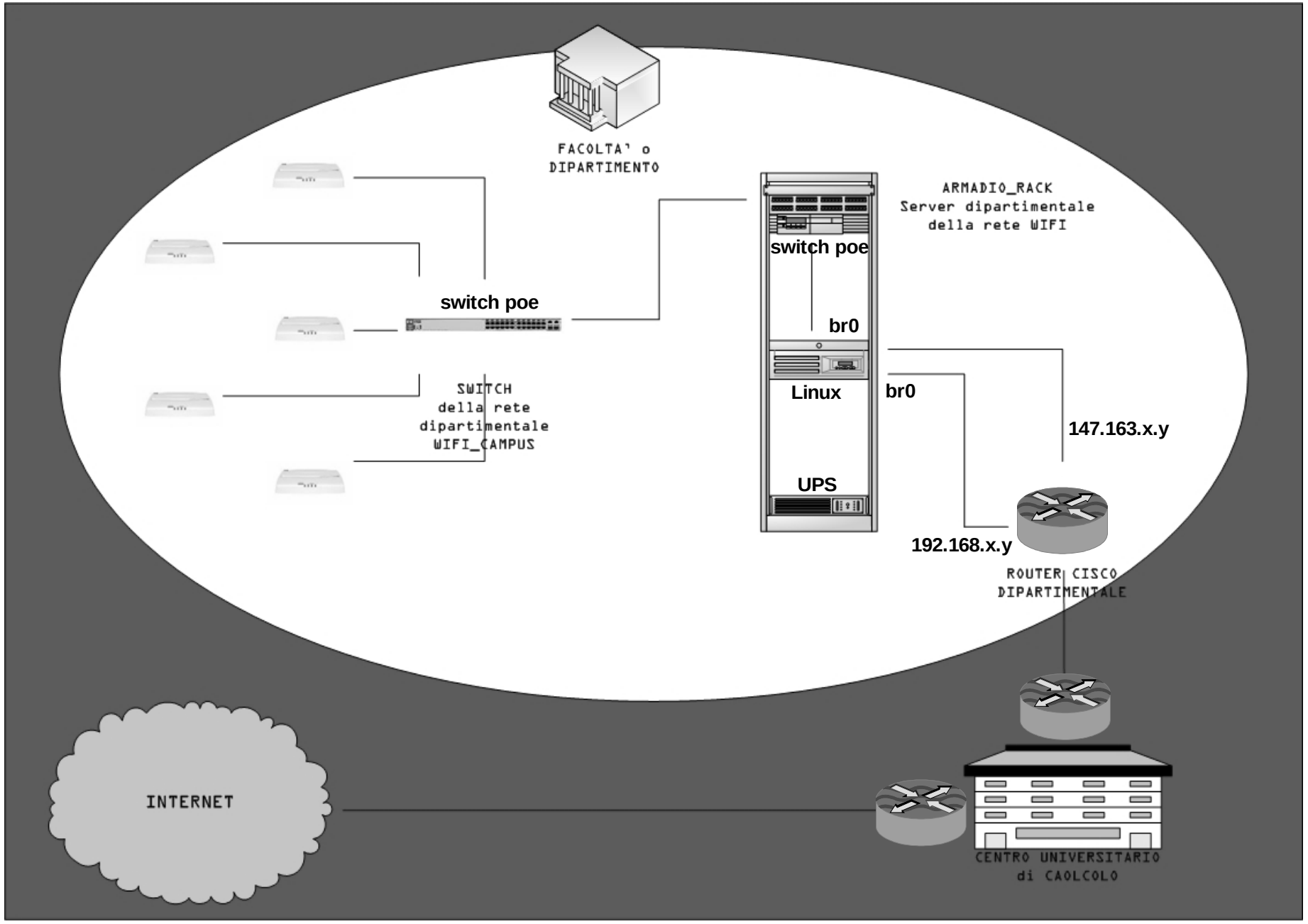

Parco d'Orleans
Grandi Attrezzature
Multididattico
XX.XX
SMF
MMF
Server WiFi
Laser
LETTERE XX.X
DREAM XX.X
IDRA XX.X
DTPM XX.X
MAT XX.X
DINFO XX.X
DICPM XX.X
DIN XX.X
oss.ass. AOUP
X.XXX
Castello Utveggio
XX.X DIET
XX.X DIMA
XXX.X PSICOLOGIA
XX.X IAS
XXX.XXX SISSIS
TRIGRID
X.XX Backup
FW1
FW2
X.XX
IDS Snort
GARR
CRES
Via Archirafi
X.XXX Rettorato
XX.X S.ANTONINO
DIFTER XX.X
CHIMICA XX.X
BIOLOGIA XX.X
ARCH XXX.X
ECONOMIA XX.X
AGRARIA XX.X
X.XXX SEGRETERIE XX.X
X.XXX S.ROMANO
COT
S.Saverio
UPADO
Fisiologia
Biopatologia
Scuola Infermieri

# Rete wireless di Parco d'Orleans

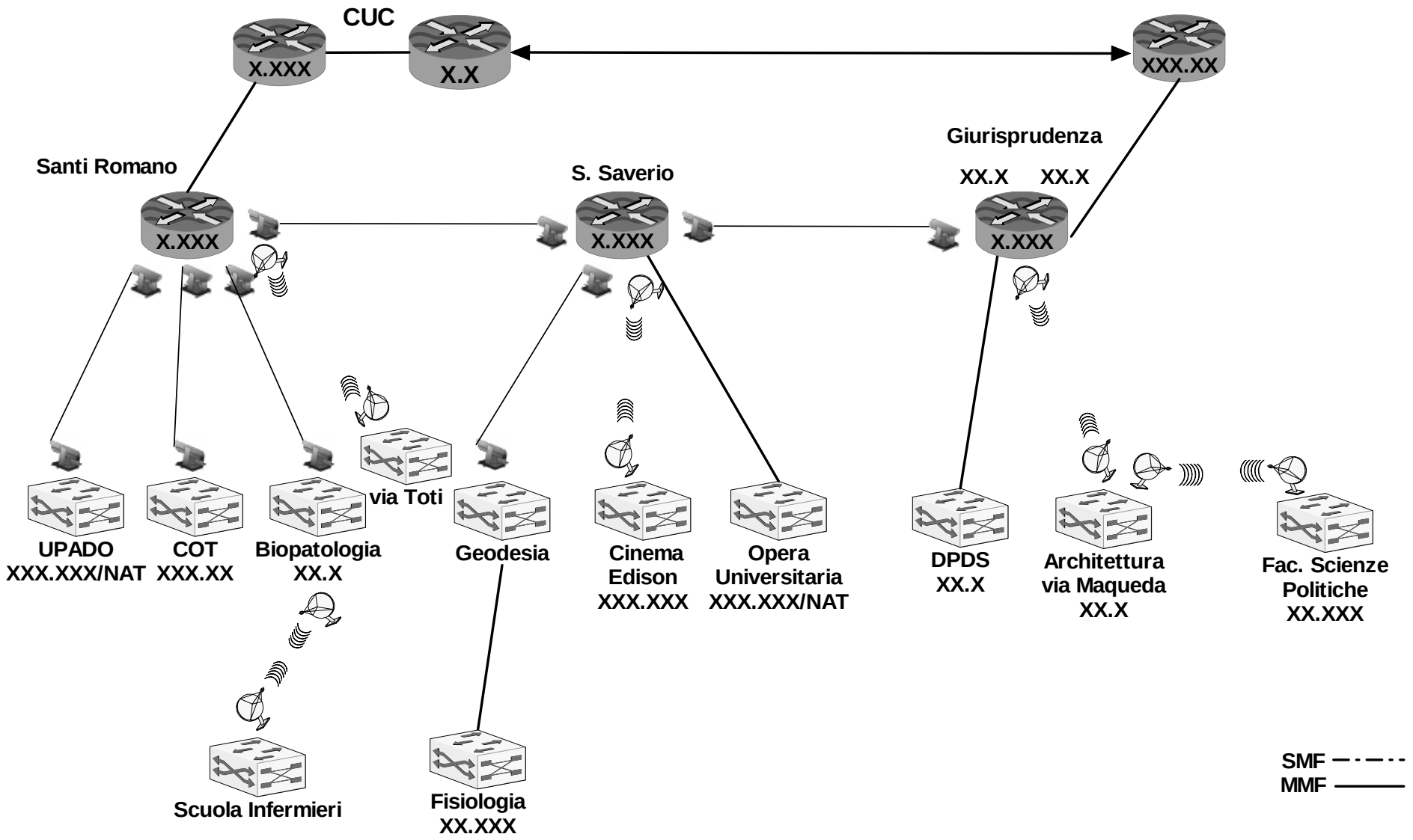


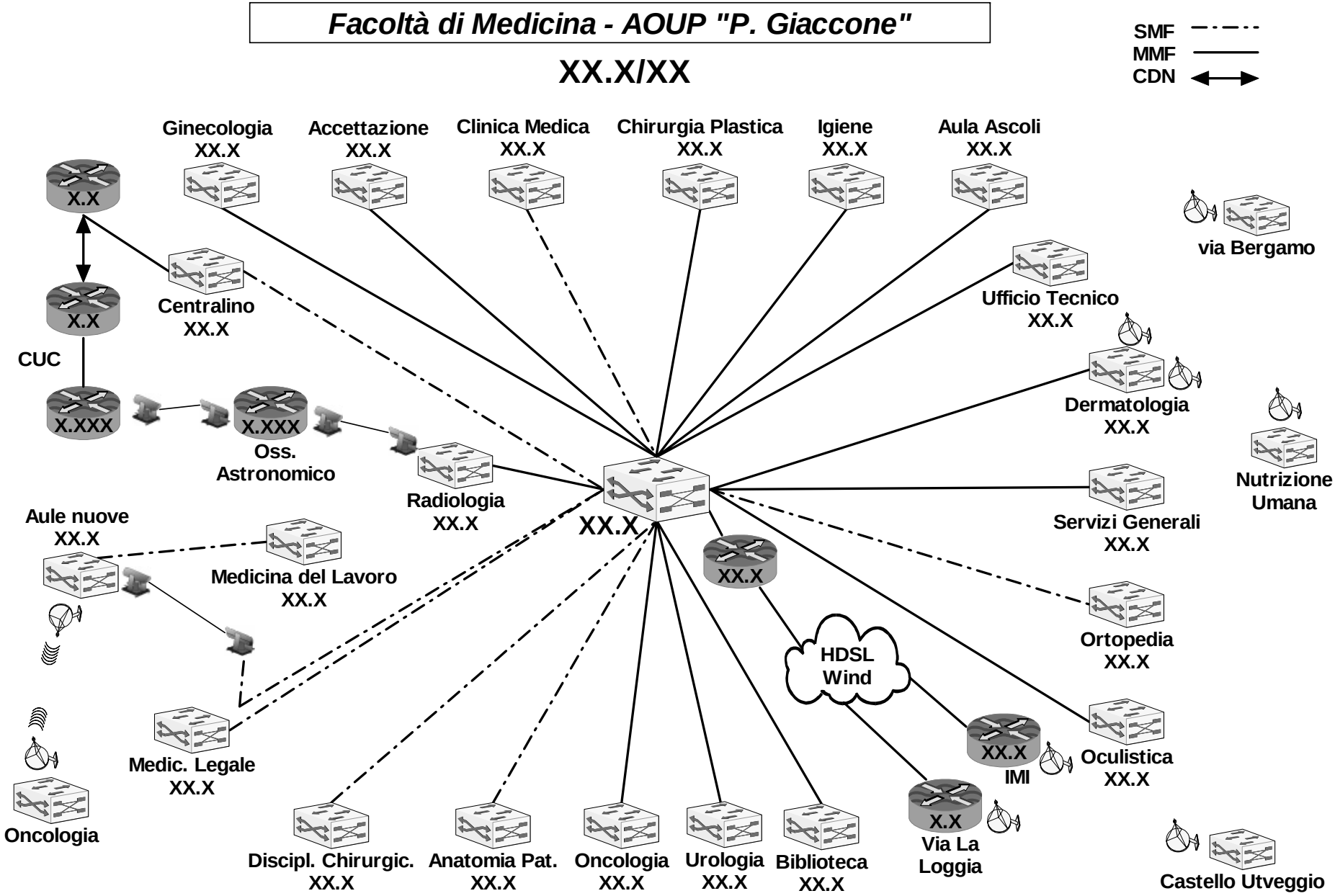
# Rete wireless di Parco d'Orleans

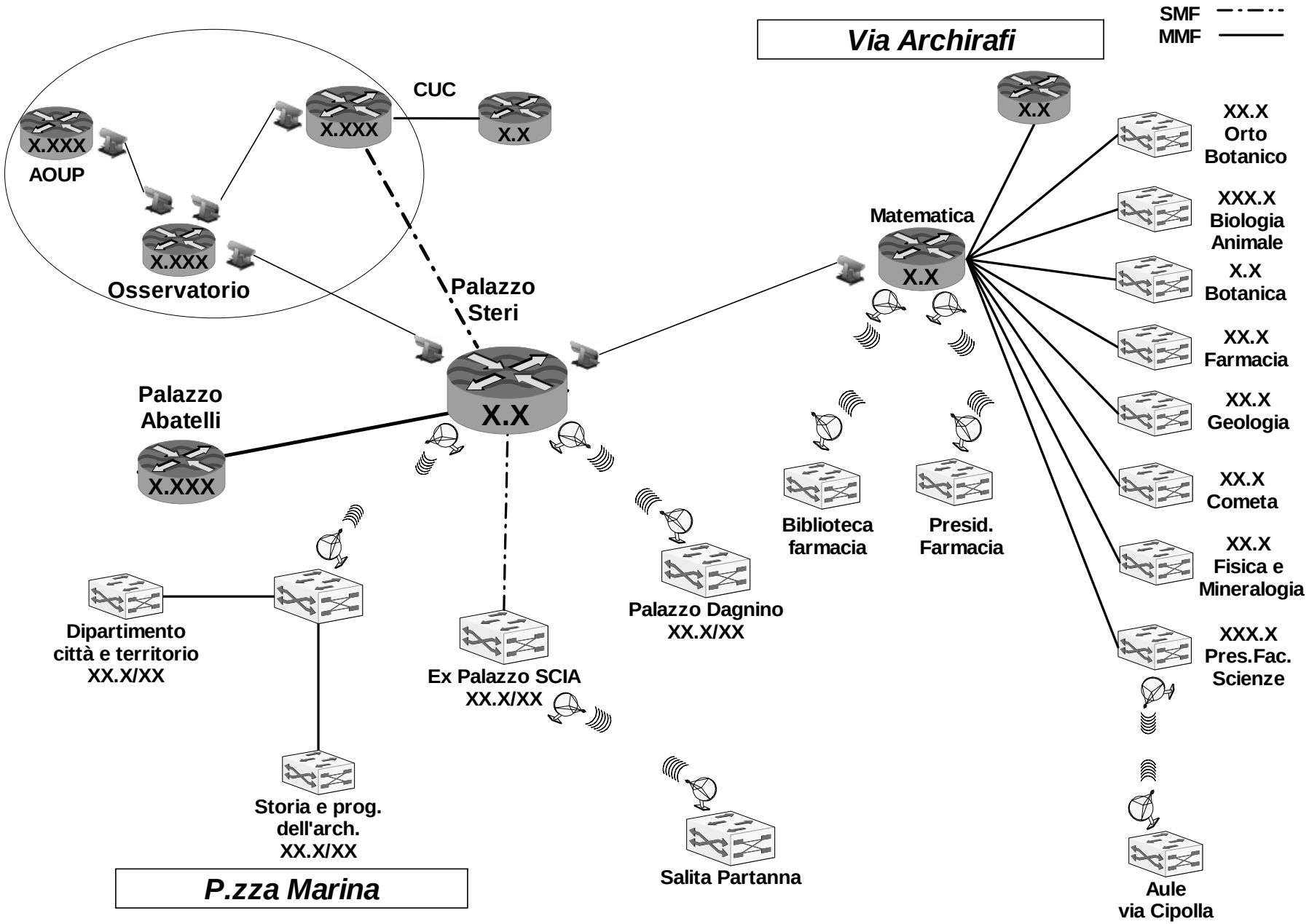
- 18 server Linux
- 29 switch HP e 13 switch Cisco
- Oltre 150 Access Point
- Consente l'accesso contemporaneo di oltre 1000 utenti (personale universitario, studenti e ospiti)

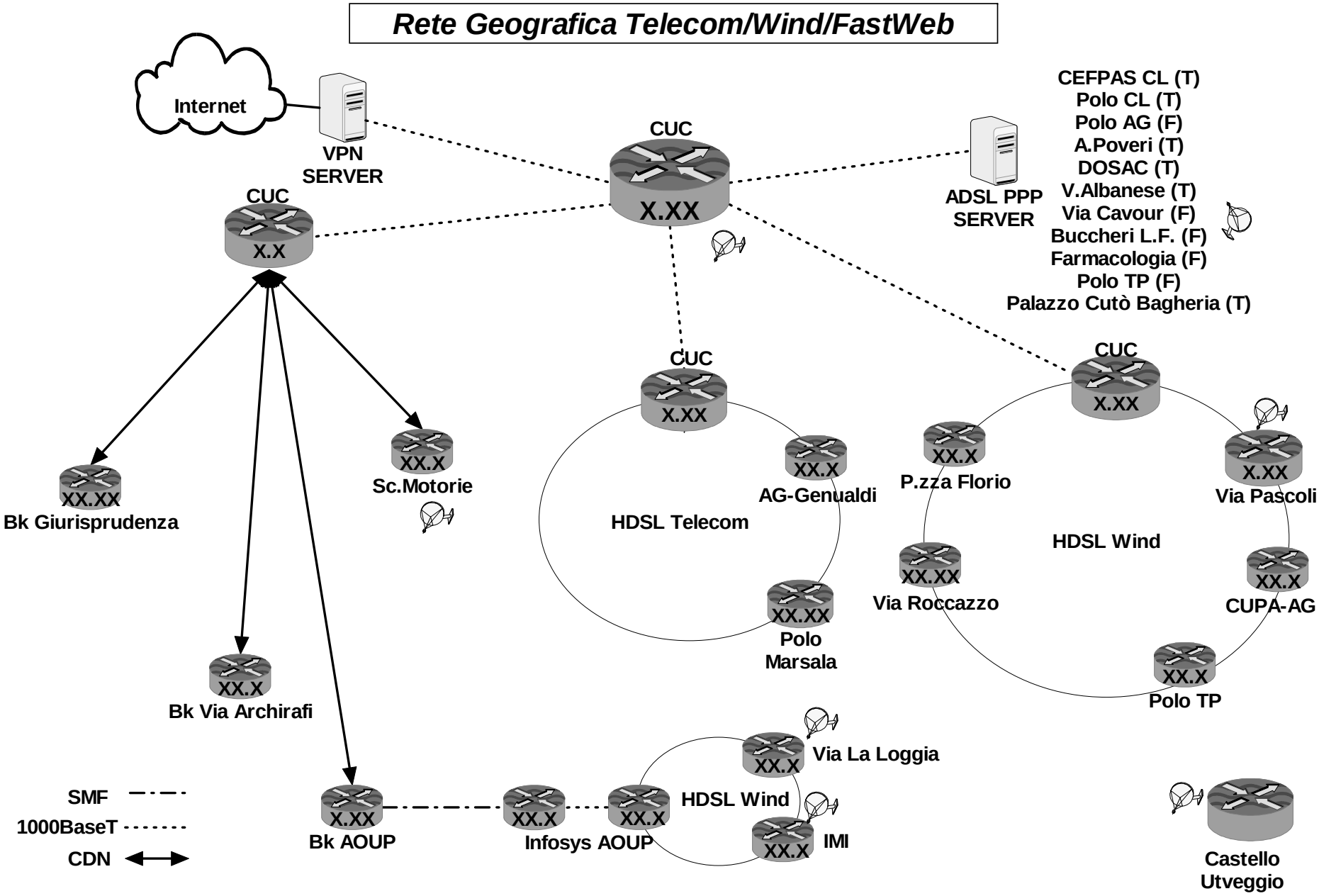

FACOLTA' o
DIPARTIMENTO
ARMADIO_RACK
Server dipartimentale
della rete WIFI
switch poe
switch poe
br0
SWITCH
della rete
dipartimentale
WIFI_CAMPUS
Linux
br0
147.163.x.y
UPS
192.168.x.y
ROUTER CISCO
DIPARTIMENTALE
INTERNET
CENTRO UNIVERSITARIO
di CALCOLO

# *Santi Romano - San Saverio - Via Maqueda*




Facoltà di Medicina - AOUP "P. Giaccone"
XX.X/XX
SMF
MMF
CDN
Ginecologia XX.X
Accettazione XX.X
Clinica Medica XX.X
Chirurgia Plastica XX.X
Igiene XX.X
Aula Ascoli XX.X
X.X
X.X
CUC
X.XXX
Centralino XX.X
X.XXX
Oss. Astronomico
Radiologia XX.X
XX.X
via Bergamo
Ufficio Tecnico XX.X
Dermatologia XX.X
Nutrizione Umana
Servizi Generali XX.X
Aule nuove XX.X
Medicina del Lavoro XX.X
XX.X
HDSL Wind
Ortopedia XX.X
Oculistica XX.X
XX.X
IMI
Medic. Legale XX.X
Oncologia
Discipl. Chirurgic. XX.X
Anatomia Pat. XX.X
Oncologia XX.X
Urologia XX.X
Biblioteca XX.X
X.X
Via La Loggia
Castello Utveggio


SMF
MMF
Via Archirafi
CUC
X.XXX
X.X
AOUP
X.XXX
Osservatorio
Palazzo
Steri
X.X
Matematica
X.X
XX.X
Orto
Botanico
XXX.X
Biologia
Animale
X.X
Botanica
XX.X
Farmacia
XX.X
Geologia
XX.X
Cometa
XX.X
Fisica e
Mineralogia
XXX.X
Pres.Fac.
Scienze
Palazzo
Abatelli
X.XXX
Biblioteca
farmacia
Presid.
Farmacia
Palazzo Dagnino
XX.X/XX
Dipartimento
città e territorio
XX.X/XX
Ex Palazzo SCIA
XX.X/XX
Storia e prog.
dell'arch.
XX.X/XX
Salita Partanna
Aule
via Cipolla
P.zza Marina


Rete Geografica Telecom/Wind/FastWeb
Internet
VPN SERVER
CUC
X.XX
CUC
X.X
ADSL PPP SERVER
CEFPAS CL (T)
Polo CL (T)
Polo AG (F)
A.Poveri (T)
DOSAC (T)
V.Albanese (T)
Via Cavour (F)
Buccheri L.F. (F)
Farmacologia (F)
Polo TP (F)
Palazzo Cutò Bagheria (T)
XX.XX
Bk Giurisprudenza
XX.X
Sc.Motorie
CUC
X.XX
XX.X
AG-Genualdi
HDSL Telecom
XX.XX
Polo Marsala
CUC
X.XX
XX.X
P.zza Florio
X.XX
Via Pascoli
HDSL Wind
XX.XX
Via Roccazzo
XX.X
CUPA-AG
XX.X
Polo TP
XX.X
Bk Via Archirafi
SMF
1000BaseT
CDN
X.XX
Bk AOUP
XX.X
Infosys AOUP
XX.X
HDSL Wind
XX.X
Via La Loggia
XX.X
IMI
Castello Utveggio

# Riepilogo connessioni in rete

- Il CUC è collegato alla rete Internet a 155 Mbps in tecnologia ATM
- 41 connessioni a 1000 Mbps:
  - 1 CUC - Steri
  - 1 CUC - San Antonino
  - 19 CUC – Edifici in Parco d'Orleans
  - 20 Infosys – Edifici in AOUP (Facoltà di Medicina)
- 10 connessioni 100 Mbps in f.o.:
  - DPDS/Giurisprudenza, Geodesia/Fisiologia, Steri/Scia e 8 in via Archirafi (Dip. Di Matematica – ed. di via Archirafi)

# Riepilogo connessioni in rete

- 8 connessioni attraverso ponti ottici a 100 Mbps:
  - DIET – Oss. Astr. – AOUP – Steri - Archirafi
  - S. Romano – S. Saverio – Giurisprudenza
  - S. Romano – COT via Veneziano
  - Pres. Di Ing. - Polo Multididattico
- 3 connessioni attraverso ponti ottici a 10 Mbps:
  - S. Romano – Upado, S. Romano - Patologia, S. Saverio - Geologia/Fisiologia
- 11 connessioni a 54 Mbps via radio:
  - Steri - Città e Terr./Storia e Progetto Arch., Ex-Scia – Geografia, , Lettere – Grandi Apparecchiature, Giurisprudenza – Scienze Politiche, S. Saverio – Via Divisi, Matematica – Biblioteca di Farmacia, Matematica - Presidenza Farmacia, Dermatologia - Nutrizione Umana, Dermatologia – Via Bergamo, S. Romano – Via Toti, CUC – Castello Utveggio
- 3 connessioni a 11 Mbps via radio:
  - Giurisprudenza/Architettura, A. Nuove – Onc./M.Ascoli, Steri – SESOF)

# Riepilogo connessioni in rete

- HDSL Wind: 5 link unipa (tra cui Polo di TP e CUPA di AG) e 2 link AOUP (IMI e via La Loggia)
- HDSL Telecom: 2 Link (Polo di Marsala e Villa Genualdi di AG)
- ADSL Telecom: 6 link
- ADSL FastWeb: 5 link
- CDN Telecom: 4 link (vie: Archirafi, Maqueda, Toselli e Vespro)
- Accessi analogici/ISDN: 60
- Possibilità di collegamento in VPN da ADSL/HDSL/UMTS/GPRS/EDGE/…

# La realtà informatica universitaria

**Il sistema di rete universitario (costituito da 100 collegamenti) collega circa 5000 risorse tra cui:**

- 200 server Linux con funzioni di: web, mail, proxy, dns, dhcp, nfs, ftp, log, mrtg, file & printer, backup, tftp, vpn, firewall, natting, ids, controllo vulnerabilità, antivirus, ldap, radius, ntp, Oracle 10g DB & AS
- 300 apparecchiature di rete: switch, router, access point
- 4500 stazioni di lavoro: Personal Computer con Windows, workstation con sistemi operativi Unix oriented, etc.
- 6.096 utenti su @unipa.it e oltre 21.000 utenti su @studenti.unipa.it

# Il sistema informativo

- Il sistema informativo è l'insieme degli strumenti e delle applicazioni utilizzati per il trattamento dei dati personali ed è anche un modello organizzativo tramite il quale avviene il trattamento di informazioni e dati all'interno e all'esterno della struttura
- Le funzioni di base sono:

  - acquisizione
  - archiviazione
  - elaborazione
  - comunicazione
  - diffusione

# La realtà informativa universitaria

**Il sistema informativo universitario conta 11 applicazioni fondamentali:**

- Contabilità, Patrimonio, Presenze (SELFIN)
- Studenti (KION)
- Stipendi (CINECA)
- Protocollo (3D Informatica)
- Biblioteche (Atlantis)

- Posta elettronica, portale studenti e docenti, siti web centralizzati
- Immatricolazioni e iscrizioni on line
- NILO (Network Industrial Liaison Office)

# D. Lgs 196/2003

- 01 PREMESSA: IL CONTESTO INFORMATICO UNIVERSITARIO
- 02 IL D. LGS. 196/2003 DAL PUNTO DI VISTA ORGANIZZATIVO
- 03 IL D. LGS. 196/2003 DAL PUNTO DI VISTA INFORMATICO

# Punti fondamentali del D.Lgs. 196/2003

- La distribuzione dei compiti e delle conseguenti responsabilità nell'ambito sia dei soggetti interni che esterni a cui vengono affidati trattamenti di dati od operazioni su di essi;
- La sensibilizzazione alle problematiche di sicurezza informatica di tutto il personale, indipendentemente dalla qualifica, che opera trattamenti sui dati personali (comuni, sensibili, giudiziari, particolari).

# Temi affrontati dal D. Lgs. 196/03

- Affronta la sicurezza non solo da un punto di vista tecnico ma anche e soprattutto da quello organizzativo e metodologico
- Fa riferimento alla emanazione di istruzioni organizzative/tecniche per la custodia dei dati; vedi “Regolamento  per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche”
- Fa riferimento a un piano di sicurezza denominato DPS (Documento Programmatico sulla Sicurezza) con l’obbligo di allegarlo alla relazione accompagnatoria del bilancio di esercizio
- Fa riferimento ad un piano di formazione periodico sul tema della sicurezza e della privacy da rivolgere a quasi tutto il personale

# continua …..

- Il D.Lgs. 196/2003 recepisce quanto previsto dalla normativa europea sulla privacy e tratta indistintamente la triade della sicurezza: integrità, riservatezza e disponibilità dei dati personali
- Fa riferimento a temi di forte attualità come: lo spamming, l'autenticazione forte (biometrica, etc.), l'autenticazione debole (password di almeno 8 caratteri), il salvataggio dei dati (backup) e il ripristino dell'accesso ai dati stessi (disaster recovery) entro tempi massimi prefissati (7 gg.)

# La formazione

- L’analisi e la spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, interessato
- Le misure minime di sicurezza adottate con particolare riferimento a: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software
- L’integrità dei dati: unificare il più possibile le informazioni e non avere più archivi analoghi distribuiti in diversi uffici
- Evitare la creazione di satelliti informativi avulsi dal contesto informativo universitario

# Il dato personale

- La legge prende in considerazione i *trattamenti dei dati personali*, effettuati per via cartacea o elettronica, intendendo per dato personale qualsiasi informazione (comprese immagini e suoni) che si riferisca o che sia riconducibile ad una persona fisica o giuridica
- I dati personali possono essere:

  - *comuni:* qualsiasi informazione di tipo anagrafico o identificativo relativa a persona fisica o giuridica

  - *sensibili:* ovvero dati che possano ricondurre, esplicitamente o implicitamente alle convinzioni politiche, religiose o sessuali ed allo stato di salute dell'interessato

  - *giudiziari:* ovvero dati che possano ricondurre alla situazione dell'interessato nei confronti della legge

  - *particolari*: dati che per la loro natura  o per la loro modalità di trattamento presentano rischi specifici (coordinate bancarie, numero di carta di credito, …)

# Il trattamento del dato personale

- Un trattamento è una qualsiasi operazione effettuata per qualsiasi motivo sui dati personali, sia in forma cartacea che elettronica
- I trattamenti previsti sono: la raccolta, la registrazione, la conservazione, la consultazione, l'elaborazione, la modifica, l'estrazione, la comunicazione esterna, la diffusione, …
- Ogni trattamento ha una *finalità*, cioè l'ambito lavorativo entro il quale i dati personali vengono trattati: le finalità tipiche per un Ateneo sono ad esempio:

  - gestione dello studente, del personale, delle prove d'esame, della organizzazione di corsi, …

# Figure coinvolte nel trattamento

- I dati personali che vengono trattati all'Università sono di proprietà degli *Interessati (l'Art. 1 del Decreto dice: "Chiunque ha diritto alla protezione dei dati personali che lo riguardano"): quindi di studenti, di docenti, di personale ATA, di fornitori,…*
- La legge prevede che per ogni trattamento di dati personali sia identificato un *Titolare* (persona fisica, giuridica o ente)
- Il Titolare di ogni trattamento di dati, nel nostro caso, è il rappresentante legale dell'Università e cioè il Rettore

# Figure coinvolte nel trattamento

- Il Rettore  nomina i *Responsabili* dei singoli trattamenti (tramite lettera di incarico);  i responsabili sovrintendono alle operazioni del trattamento dei dati e si assicurano che vengano rispettati determinati requisiti di sicurezza; nel nostro caso i Responsabili dei singoli trattamenti sono: i Dirigenti di Area, i Presidi di Facoltà, i Direttori di Dipartimento, il Direttore del C.O.T. il Direttore della SISSIS e il Direttore del Centro Universitario di Calcolo quest'ultimo con funzioni di responsabile informatico di Ateneo ai fini del D. Lgs. 196/2003
- I Responsabili nominano a loro volta gli *incaricati* ai trattamenti ovvero coloro che fisicamente effettuano il trattamento; esempi:

  segretario amministrativo di dipartimento, addetto allo sportello di segreteria, amministratore di sistema, …

# Figure coinvolte nel trattamento

- In dottrina è usuale distinguere due tipologie di figure di Responsabile e Incaricato:
  - Responsabile Interno
  - Responsabile Esterno
  - Incaricato Interno
  - Incaricato Esterno
- Essi operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni da esso impartite (art. 30)

# Gli amministratori di sistema

- il D.Lgs. 196/2003 li definisce precisamente “addetti alla gestione o alla manutenzione degli strumenti elettronici”
- il Direttore del Centro Universitario di Calcolo, nella qualità di responsabile informatico di Ateneo ai fini del D. Lgs. 196/2003, nomina gli amministratori di sistema di concerto con il Responsabile del trattamento dati di riferimento: Presidi di Facoltà, Direttori di Dipartimento e di Centri Interdipartimentali, Direttore Amministrativo, Direttore del C.O.T., Direttore della SISSIS e Dirigenti di Dipartimento o Area
- l'aggiornamento degli amministratori di sistema, come tutti gli altri incaricati, deve essere periodico con cadenza almeno annuale; ad oggi sono 37

# Gli amministratori di sistema nominati

- M. Scopelliti (Chimica)
- G. Ferrara (P. Steri e Abatelli)
- A. Genco (Fac. Scienze Motorie)
- S. Diliberto (Segr. Studenti)
- R. De Torrebruna (Biopatologia)
- G. Caruso (Idraulica)
- M. Cannella (Beni Culturali)
- A. Torregrossa (Fac. Lettere)
- G. Signorino (Uff. Tecnico)

# Gli amministratori di sistema nominati

- V. Lo Brano (DREAM)
- A. Misuraca (Fac. di Economia)
- G. Musacchia (Psicologia)
- C. Mussolin (Fac. Scienze Formazione)
- E. Pollari (Fac. Ingegneria)
- F. Vozza (Aule didattiche Ingegneria)
- G. Liuzza (Fac. Giurisprudenza e DPDS)
- C. Belfiore (DICPM)
- G. Russo (DISEG)

# Gli amministratori di sistema nominati

- C. Calì (CINAP)
- A. Lorello (DIIV)
- A. Provenzano (Fac. Agraria)
- G. Morici  (Biologia)
- L. Gatto (Geodesia)
- M. Glorioso  (DIFTER)
- N. Trapani (SISSIS)
- A. Inzerillo (AOUP – Facoltà di Medicina)
- E. Catanzaro (Chomica Inorganica)

# Gli amministratori di sistema nominati

- R. Grutta (DOSAC)
- N. Surano (Botanica)
- R. La Barbera (Biologia Animale)
- S. Mogavero (Rappresentazione)
- G. Russo (DISEG)
- A. Santoro (Storia e Progetto)
- V. Lanza  (Buccheri La Ferla)
- F. Munnia (DPCE)
- F. Di Lorenzo (Fac. di Scienze)

# Regolamento  per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche; Art. 1

- Responsabili del trattamento ai sensi dell' art. 29 del Codice sono : il Direttore Amministrativo, i Dirigenti di Dipartimenti e Aree, il Direttore del Centro Universitario di Calcolo, il Direttore del C.O.T., i Presidi di Facoltà, i Direttori di Dipartimento.
- Ai Responsabili del trattamento compete l'attuazione delle misure di sicurezza sia logiche che fisiche previste dal Codice, dal "Documento Programmatico per la Sicurezza" e dal "Regolamento".
- La nomina di ulteriori responsabili compete al rappresentante legale dell'Università e cioè il Rettore pro tempore.
- I compiti dei responsabili del trattamento sono: operare, direttamente o a mezzo di incaricati,  il trattamento dei dati personali e identificativi e di eventuali dati sensibili e giudiziari secondo il principio di pertinenza e non eccedenza dei dati stessi e conformandosi alle istruzioni di cui al "Regolamento", al "Regolamento  di Ateneo sul trattamento dati sensibili" e dal Codice.

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche; Art. 1

- I responsabili individuano con proprio provvedimento i soggetti incaricati del trattamento con indicazione nominativa della persona fisica e del ruolo ricoperto, stabilendo l'ambito del trattamento consentito.
- In particolare, per i soggetti nominati "amministratori di sistema" il Direttore Amministrativo, di concerto con il Direttore del Centro Universitario di Calcolo, individuerà tali figure professionali per singole unità (server), o gruppi di risorse informatiche (PC, server, switch, router, telecamere, stampanti, Access point, apparati wireless,…).
- Nel caso dei Dipartimenti, Facoltà o altre Strutture universitarie decentrate, la figura di amministratore di sistema dovrà essere indicata dal Responsabile del trattamento dei dati di concerto con il Direttore del Centro Universitario di Calcolo.
- Tutte le nomine devono essere controfirmate dagli interessati, sono trasmesse al Direttore Amministrativo e avranno validità fino a revoca della stessa.
- Tutti i soggetti incaricati devono evitare comportamenti che possano pregiudicare la riservatezza dei dati.

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche; Art. 3

- Per il trattamento dei dati personali viene rilasciata ad ogni singolo incaricato, a cura del Centro Universitario di Calcolo, una o più utenze, ciascuna identificata con una username e una password; l'utenza consente l'individuazione dell'incaricato stesso. La password deve essere composta da almeno 8 caratteri, non deve contenere riferimenti facilmente riconducibili all'incaricato e deve essere modificata da quest'ultimo al primo utilizzo e almeno ogni sei mesi (tre mesi nel caso in cui l'incaricato tratti dati sensibili e giudiziari).
- L'incaricato deve adottare le cautele necessarie ad assicurare la segretezza della password e la diligente custodia di tutti dispositivi assegnatigli: PC, penna USB, CD-ROM, DVD, floppy disk, etc.
- Al fine di evitare accessi non consentiti e trattamenti non autorizzati, tutti i supporti su cui sono memorizzati i dati devono essere conservati in contenitori dotati di serratura, armadi o altro ricovero atto a garantirne l'inviolabilità.

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche ; Art. 3

- Per assicurare la disponibilità dei dati in caso di prolungata assenza o impedimento dell'incaricato, lo stesso, dopo ogni modifica della password, deve consegnarla in busta chiusa e sigillata al proprio responsabile; le utenze non utilizzate per almeno sei mesi vengono disattivate dal Centro Universitario di Calcolo.

- Gli incaricati non dovranno mai lasciare incustodita e accessibile la propria stazione di lavoro durante una sessione di trattamento; le password non possono essere riutilizzate, neanche in tempi diversi.

- Il salvataggio dei dati trattati (backup) con strumenti informatici deve avvenire almeno settimanalmente ed, eventualmente, potrà essere concordata con il Centro Universitario di Calcolo sia la frequenza del backup che lo spazio disco necessario allo scopo.

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche ; Art. 3

- All’incaricato è affidata la responsabilità della corretta tenuta della\e password assegnategli ed è altresì responsabile per l’utilizzo di applicazioni informatiche e di elaborazioni effettuate attraverso l’utilizzo della propria utenza e, pertanto, è tenuto a non comunicare a nessun altro la\e propria\e password.

- L’incaricato che rilevi nell’utilizzo del PC o di un’applicazione informatica un problema che possa compromettere la sicurezza dei dati ne dà immediata comunicazione al Responsabile del trattamento ed al Centro Universitario di Calcolo, cui compete l’adozione delle misure tecniche necessarie alla risoluzione dello stesso.

## Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche ; Art. 3

- All’incaricato è fatto divieto di installare programmi non attinenti le ordinarie attività d’ufficio e nuovi programmi ritenuti necessari, senza il preventivo parere tecnico del Centro Universitario di Calcolo; è altresì fatto divieto di modificare le configurazioni hardware e software senza il succitato parere tecnico

- Nell’ambito delle misure minime di protezione previste dal Documento Programmatico per la Sicurezza e dal presente Regolamento possono essere adottati differenti profili di utenza specificando il tipo di accesso ai dati (ad esempio: solo visualizzazione o anche aggiornamento degli stessi).

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche ; Art. 4

Allo scopo di evitare i potenziali danni al sistema informativo dell'Ateneo e ai dati in esso contenuti, derivanti da un uso improprio della connessione alla rete Internet, tutti gli incaricati dovranno:

- Utilizzare la connessione in rete esclusivamente per lo svolgimento delle attività istituzionali;
- Comunicare ufficialmente al Direttore del Centro Universitario di Calcolo l'utilizzo di eventuali ulteriori connessioni (ADSL, HDSL, wireless o altro); in ogni caso, le apparecchiature collegate a reti non universitarie non possono essere collegate contemporaneamente in alcun modo alla rete universitaria;
- Adottare sistemi operativi che prevedano l'accesso con username e password e l'aggiornamento automatico dello stesso (dal 30.09.2005 non è possibile utilizzare sistemi operativi come Windows 95, 98, ME o NT);
- Adottare il sistema antivirus centralizzato di Ateneo fornito gratuitamente a tutti gli operatori universitari (personale docente e ATA) e studenti;

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche ; Art. 4

- Utilizzare mail server dotati di sistema antivirus;
- Non diffondere messaggi di posta elettronica di provenienza dubbia;
- Non utilizzare le caselle di posta elettronica rilasciate dall'Università per fini personali e avendo cura di inviare messaggi con allegati di peso non superiore a 5 MB;

  Al fine di un uso legittimo della connessione alla rete internet si ricordano gli artt. del codice penale 615\ter "accesso abusivo ad un sistema informatico o telematico", 615\quater "detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici", 615\quinquies "diffusione di programmi diretti a danneggiare o interrompere un sistema informatico" nonché della legge 21\05\04 n. 128 che sanziona la condivisione e\o la fruizione di files relativi a un'opera cinematografica o assimilata protetta dal diritto d'autore.

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche ; Art. 5

Relativamente agli incaricati con funzioni di amministratore di sistema si fa presente che tra i compiti principali dovranno:

- assicurare la buona funzionalità di ciascun server e stazione di lavoro tramite aggiornamento del sistema operativo e protezione con sistema antivirus;
- accertarsi che non vi sia risorsa come server, router, switch indirizzabile, telecamera IP, bridge wireless, ponte ottico, etc. che non abbia un amministratore di sistema di riferimento;
- tenere un elenco scritto e sempre aggiornato che comprenda:

  - locale in cui si trova la risorsa informatica ed eventuale detentore di chiave con relativo numero di telefono;

  - sistema operativo utilizzato (con il codice) ed eventuale numero di serie di ogni risorsa;

  - indirizzo IP e MAC;

  - eventuale nome mnemonico Internet (es. pc1.cuc.unipa.it);

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche ; Art. 5

- nome e gruppo di lavoro Microsoft;
- nome dell'utilizzatore;
- eventuale nome della ditta manutentrice;
- eventuale presenza di computer con funzioni di server;
- eventuale connessione in rete NON UNIVERSITARIA (ADSL, HDSL, CDN, wireless, …);
- inviare l'elenco in argomento, via posta elettronica, al seguente indirizzo di posta elettronica: *retiunipa@unipa.it*; l'elenco deve essere inviato ad ogni aggiornamento;
- gestire le eventuali aule didattiche con un piano di indirizzamento privato tipo 192.168.x.y con firewall e proxy server; deve essere disponibile in questo caso un registro degli utilizzatori, compilato eventualmente da altro personale incaricato;
- accertarsi che non vengano utilizzati hub ethernet e cavi coassiali che possono facilitare l'intercettazione del traffico di rete;

# Regolamento per la disciplina delle modalità di trattamento dei dati personali. Istruzioni organizzative e tecniche ; Art. 5

- Nei casi in cui l'amministratore di sistema nominato non sia presente, le operazioni ordinarie potranno essere svolte con il supporto del personale del Centro Universitario di Calcolo.
- Nelle Strutture con un numero di risorse umane superiore a 50 unità dovranno essere nominati almeno due amministratori di sistema.
- Tutti gli amministratori di sistema e gli afferenti ai gruppi del Centro Universitario di Calcolo sopra indicati dovranno essere istruiti almeno semestralmente sulle politiche di sicurezza dei sistemi e delle reti di Ateneo (art. 34, Comma b) a cura del Centro Universitario di Calcolo o da altri esperti indicati dal Direttore del Centro Universitario di Calcolo. L'organizzazione di tali incontri formativi sarà a carico del SESOF.
- Periodicamente, sempre a cura della direzione del Centro Universitario di Calcolo e del SESOF, saranno previsti interventi formativi sulla sicurezza dei dati anche per i Responsabili e gli incaricati del trattamento.
- Nel caso di incarico di amministratore di sistema a personale esterno all'Ateneo, gli oneri economici saranno a carico della struttura deficitaria di tale figura professionale e il coordinamento sarà a cura del Centro universitario di calcolo: la nomina verrà fatta solo a persona fisica.

# Ulteriori adempimenti a cura del Responsabile informatico di Ateneo

Costituire i seguenti gruppi di lavoro interni al Centro Universitario di Calcolo, designando, per ogni gruppo, i relativi coordinatori e il personale afferente:

- 1. Reti e sicurezza, per tutte le tematiche relative alle connessioni in rete e alla sicurezza informatica (M. Tartamella e G. Pisano);
- 2. Sistemi, RDBMS, Backup e Recovery, per tutte le tematiche relative ai database, al backup dei dati e al ripristino dei sistemi (D. Cardaci, M. Bonaccorso, B. Vassallo, M. Urbano, P. Frangipane);
- 3. Accesso al sistema informativo, per tutte le tematiche relative alle credenziali di accesso al sistema informativo (C. Lorenzini, M. Urbano, P. Frangipane, P. Sangineto, M. Verde);
- 4. Accesso ai servizi di rete, per tutte le tematiche relative alle credenziali di accesso ai servizi di rete (B. Vassallo, M. Bonaccorso, N. Bontempo)
- 5. Sviluppo Applicazioni e gestione software applicativo, per tutte le tematiche inerenti le procedure applicative (da nominare).

# D. Lgs 196/2003

- 01 PREMESSA: IL CONTESTO INFORMATICO UNIVERSITARIO
- 02 IL D. LGS. 196/2003 DAL PUNTO DI VISTA ORGANIZZATIVO
- 03 IL D. LGS. 196/2003 DAL PUNTO DI VISTA INFORMATICO

# Controllo e protezione dei sistemi

- Secondo le norme ISO la sicurezza è definita come: l'insieme degli sforzi dedicati ad assicurare la protezione dei dati e delle risorse di calcolo in termini di integrità, riservatezza e disponibilità.

# Art. 34 (Trattamenti con strumenti elettronici)

Il trattamento di dati personali con strumenti elettronici è consentito solo se sono adottate le seguenti misure minime:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilita' dei dati e dei sistemi;
- tenuta di un aggiornato DPS (Documento Programmatico sulla Sicurezza);
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

# Meglio specificate

- Per autenticazione informatica si intende “l’insieme degli strumenti elettronici e delle procedure per la verifica della identità o della dichiarazione di identità”
- Per credenziali di autenticazione si intendono “i dati e i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati dal sistema di autenticazione informatica per la verifica dell’identità”
- Per sistema di autorizzazione si intende “l’insieme degli strumenti e delle procedure che abilitano l’accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente”

## Il DPS dal punto di vista informatico: parte I

- l'elenco dei trattamenti di dati personali (regola 19.1 – R1);
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (regola 19.2 – R2);
- l'analisi dei rischi per i dati (regola 19.3 – R3);
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità (regola 19.4 – R4);

## Il DPS dal punto di vista informatico: parte II

- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a possibili eventi di distruzione o danneggiamento (backup e disaster recovery) (regola 19.5 – R5)
- la previsione di interventi formativi degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare (regola 19.6 – R6)

## Il DPS dal punto di vista informatico: parte III

- la descrizione dei criteri da seguire per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del titolare (regola 19.7 – R7);
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, inoltre il Codice prevede l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato (regola 19.8 – R8).

# R1: elenco trattamenti

Nel nostro caso, sono da ritenersi afferenti alla categoria “dati personali sensibili” alcuni dati relativi alle seguenti procedure:

- Stipendi, contabilità, patrimonio, studenti, protocollo, presenze
- selezione del personale
- archivi relativi alle imprese
- archivi sui pazienti della Facoltà di Medicina

Sono da ritenersi afferenti alla categoria “dati personali comuni” tutti i dati relativi alla posta elettronica e alle biblioteche

# R2: compiti e responsabilità

- Quanto già visto sul “Regolamento ….” e cioè la individuazione, tramite lettera d’incarico, dei Responsabili (interni o esterni) che a loro volta individuano gli Incaricati (interni o esterni). Dalle lettere d’incarico deve risultare evidente la distribuzione dei compiti e l’ambito del trattamento dei dati personali.
- In particolare, il Direttore del Centro Universitario di Calcolo (CUC), nel ruolo di Responsabile Informatico d’Ateneo per il D.Lgs. 196/2003, deve individuare i vari amministratori di sistema distribuiti in Ateneo e la creare specifici gruppi di lavoro interni al CUC.

# R3: Analisi rischi

Per analizzare i rischi che incombono sui dati occorre previamente individuare i beni da proteggere; possiamo suddividere le risorse da proteggere in Ateneo in quattro categorie:

- ***luoghi fisici;***
- ***risorse hardware;***
- ***risorse software;***
- ***risorse dati.***

# R3: Analisi rischi… luoghi fisici

È necessario individuare i luoghi in cui si svolgono i trattamenti dei dati, dove si trovano i sistemi di elaborazione e in cui sono conservati i dati.

# R3: Analisi rischi ... risorse hardware

La ricognizione e la relativa catalogazione delle risorse harware è un ambito di pertinenza degli amministratori di sistema distribuiti nelle varie aree di Ateneo. A tale proposito sarebbe opportuno etichettare ogni elemento afferente a questa categoria e cioè:

- le stazioni di lavoro
- i notebook o i  PC portatili;
- i server;
- le SAN (Storage Area Network), le unità a nastro/DVD/CD-ROM, le NAS (Network Attached Storage), i dispositivi USB,…
- switch, bridge, router, telecamere IP e sistemi wireless, …

# R3: Analisi rischi ... risorse software

Oltre ad individuare i vari software utilizzati per effettuare i trattamenti automatici dei dati personali, si dovranno raccogliere informazioni circa i seguenti aspetti:

- programmi utilizzati (contabilità, patrimonio, stipendi, protocollo, presenze, etc.)
- programmi per la produttività individuale (Office, AutoCAD, etc.) ed eventuale numero di serie;
- sistema antivirus utilizzato (Sophos, …)
- eventuali risorse dati utilizzate

# R3: Analisi rischi ... risorse dati

Rientrano in questa categoria:

- le basi di dati utilizzate per le attività (base dati contabilità, stipendi, studenti, presenze, protocollo, …);
- l'utenza centralizzata per l'accesso ai servizi di rete (posta elettronica, condivisioni di file, etc.)
- le copie di backup delle basi dati, dei file server, dei web server, dei mail server, etc.
- gli eventuali archivi cartacei.

Oltre a individuare ed elencare i dati, dovranno essere indicate le seguenti informazioni:

- tipologia di archivio (disco o altro);
- risorsa hardware che ospita l'archivio;
- natura dei dati personali (comuni, sensibili, giudiziari e particolari) presenti nell'archivio;
- strumenti e politiche di backup

# R3: Analisi rischi ...

**Analisi dei rischi**: l'analisi dei rischi viene effettuata considerando vari fattori di rischio tra cui, in prima istanza, le minacce che possono insidiare i luoghi fisici, le risorse hardware e software e i dati.

Tipicamente si hanno tre soglie di rischio:

- *basso.* Con questa soglia viene individuato un rischio molto basso che identifica una minaccia remota e comunque rapidamente reversibile od ovviabile;
- *medio*. Con questa soglia viene individuato un rischio superiore al precedente, identificante una minaccia remota, ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio;
- *alto/molto alto*. Queste soglie di rischio sono sicuramente inaccettabili, pertanto si dovranno sicuramente attivare un insieme di contromisure (di natura fisica, logica, etc..) per abbattere il rischio e contenerlo a livelli accettabili.

# R3: Analisi rischi ... luoghi fisici

Relativamente ai luoghi fisici i fattori di rischio sono:

- la possibilità di intrusione;
- gli eventi naturali (allagamenti, incendi, etc.);
- i furti;
- l'accesso di persone non autorizzate;
- l'impossibilità di controllare l'accesso ai locali, etc.

Queste problematiche tipicamente si risolvono con telecamere a circuito chiuso, controllo degli accessi con personale addetto allo scopo, etc.

# R3: Analisi rischi ... risorse hardware

In merito alle risorse hardware, alcuni elementi di rischio che possono minacciarle sono:

- uso non autorizzato;
- manomissione;
- probabilità/frequenza di guasto;
- sabotaggio;
- furto;
- intercettazione delle trasmissioni;
- eventi naturali (allagamenti, incendi, etc.);
- guasto ad apparecchiature connesse, etc.

Qui entra in gioco la professionalità dell'assegnatario della risorsa, ovvero l'amministratore di sistema di riferimento.

# R3: Analisi rischi .. risorse software e dati

Per quanto concerne le risorse software i fattori di rischio sono:

- possibilità di accesso non autorizzato a basi dati;
- errori software che minacciano l'integrità dei dati;
- presenza di codice non conforme alle specifiche del programma, etc

In merito alle "risorse dati" i fattori di rischio sono:

- accesso non autorizzato;
- cancellazione non autorizzata di dati;
- manomissione di dati;
- perdita di dati;
- incapacità di ripristinare copie di backup, etc.

# R4: Misure da adottare

Le possibili misure idonee e necessarie a tutelare con efficacia i dati oggetto del trattamento sono fisiche, logiche e organizzative e precisamente:

- **Fisiche:** tramite sistemi di rilevazione di intrusione, sistemi di vigilanza audiovisivi o tramite personale addetto, sistemi di protezione e sbarramento agli accessi, controllo degli accessi, registrazione degli accessi, predisposizione di armadi non accessibili da personale non autorizzato, custodia di dati o copie in armadi blindati e/o ignifughi, utilizzo della cassaforte, utilizzo di contenitori con serratura, presenza di dispositivi antincendio, continuità dell'alimentazione elettrica, verifica dei supporti magnetici per le copie, etc.;

# R4: Misure da adottare …

**- Logiche:** nomina ed indicazione dei compiti in forma scritta agli Incaricati, nomina dei Responsabili del trattamento, eventuale nomina dell'azienda esterna responsabile del trattamento, nomina ed indicazione dei compiti in forma scritta agli amministratori di sistema, predisposizione dell'utilizzo delle parole chiave ai sensi del comma 5 dell'allegato B, controllo delle stazioni di lavoro e server con antivirus, uso della crittografia per i dati trasmessi in rete, controllo degli accessi e dei log su ogni singolo elaboratore (server, stazione di lavoro, router, etc.);

**- Organizzative:** divulgazione dei Regolamenti e del DPS a tutte le funzioni universitarie, prescrizione di linee guida sulla sicurezza a tutti gli incaricati, formazione degli incaricati, redazione di appositi manuali, istituzione di un piano di verifica e di controllo delle misure adottate, distruzione dei supporti magnetici che non devono più essere riutilizzati

# R4: Misure da adottare …

La verifica dell'efficacia e della validità nel tempo delle misure di sicurezza adottate è punto fondamentale di tutto il processo per la sicurezza. Molto spesso il successo o meno della soluzione adottata dipende dagli effetti che s hanno nel tempo. In ogni caso le misure adottate devono essere periodicamente verificate. È dunque opportuno:

- verificare periodicamente (almeno ogni sei mesi) il corretto utilizzo delle parole chiave e dei profili di accesso degli incaricati e prevedere la disattivazione dei codici di accesso non utilizzati da più di sei mesi;
- verificare l'integrità dei dati e delle loro copie di backup;
- verificare la sicurezza delle eventuali trasmissioni in rete;
- verificare la bontà di conservazione dei documenti cartacei;
- verificare la distruzione dei supporti magnetici che non possono più essere riutilizzati;
- verificare il livello di formazione degli incaricati; prevedere sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica avvenuta in Università.

# R5: Modalità di ripristino e disponibilità

Devono essere descritti i criteri e le procedure adottate per il salvataggio dei dati personali e il loro ripristino in caso di danneggiamento degli strumenti elettronici utilizzati; vediamo alcune regole da seguire.

- *Database:* deve contenere l'identificativo del database o dell'archivio interessato; nel nostro caso, al Centro Universitario di Calcolo sono presenti i data base relativi a: *contabilità, patrimonio, stipendi, studenti, presenze, accettazione, biblioteche e protocollo*
- *Dati personali sensibili o giudiziari contenuti:* deve contenere l'elenco dei dati sensibili o giudiziari contenuti nel database o archivio

# R5: Modalità di ripristino e disponibilità

- *Criteri individuati per il salvataggio (procedure operative in essere):* deve contenere una descrizione della tipologia di salvataggio e della frequenza con cui viene effettuato: nel nostro caso le attività di salvataggio dei dati prevedono l'utilizzo di apposite apparecchiature dedicate al backup e al disaster recovery con supporti magnetici facilmente trasportabili altrove. Attualmente viene utilizzato un server per la memorizzazione di quanto è gestito dal Centro Universitario di Calcolo e un altro server viene utilizzato in un altro sito; la frequenza dei backup è giornaliera
- *Ubicazione di conservazione delle copie:* deve contenere l'indicazione del luogo fisico in cui sono custodite le copie dei dati salvate (CUC)

# R5: Modalità di ripristino e disponibilità

- *Struttura operativa o persona incaricata del salvataggio:* occorre individuare la persona incaricata al backup dei dati e al controllo dell'esito. Per quanto riguarda il ripristino dei dati, le informazioni necessarie che bisogna avere sono le seguenti:
- *Data base/archivio:* relativo all'identificativo del data base o dell'archivio interessato
- *Scheda operativa:* deve contenere il riferimento alla scheda operativa che descrive la procedura di ripristino
- *Pianificazione delle prove di ripristino:* contiene l'indicazione delle date in cui si prevede di effettuare dei test di efficacia delle procedure di salvataggio/ripristino e disaster recovery dei dati adottate (per quanto concerne il tempo e le modalità di ripristino tipicamente si ripristina il servizio nell'arco di una giornata lavorativa utilizzando gli stessi server o server ex-novo: Linux,Oracle, Application Server)

# R5: Modalità di ripristino e disponibilità

Da un punto di vista tecnico, quando si trattano dati oggetto del D. Lgs. in argomento o comunque riservati, bisogna adottare i seguenti criteri:

- non deve essere consentito l'accesso via rete alle memorie di massa di ciascuna stazione di lavoro;
- Utilizzare i server dedicati, che il Centro Universitario di Calcolo mette a disposizione in ogni macroarea (Parco d'Orleans, piazza Marina, Policlinico, etc.), per la condivisione di file e directory;
- i responsabili del trattamento dati devono indicare al Direttore del Centro Universitario di Calcolo chi sono gli incaricati al trattamento dei dati che devono condividere le informazioni;

# R5: Modalità di ripristino e disponibilità

L’accorgimento tecnico che tipicamente viene utilizzato è quello per cui ciascun file o directory possono essere cancellate solo da chi li crea; tutti gli altri afferenti al gruppo possono solo modificare i file;

- il personale del Centro Universitario di Calcolo relativo al gruppo “Reti e Sicurezza” curerà la parte sistemistica affinché possano essere condivise in rete, in sicurezza le informazioni; il personale del Centro Universitario di Calcolo relativo al gruppo “Accesso al Sistema Informativo” assegnerà le username e le password per i vari incaricati indicati dai responsabili del trattamento; il personale del Centro Universitario di Calcolo relativo al gruppo “Sistemi, RDBMS, Backup e Disaster Recovery” si occuperà del backup e dell’eventuale ripristino dei sistemi in caso di perdita dei dati; naturalmente, se occorrerà ripristinare un determinato server con attribuito un particolare amministratore di sistema, il ripristino verrà fatto congiuntamente.

# R6:Interventi formativi

Gli incaricati dovranno essere formati sui “rischi individuati e sui modi per prevenire i danni”.Il piano di formazione, per un'analisi dettagliata ed aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee,dovrà perciò prevedere sicuramente i seguenti punti:

- disposizioni legislative in tema di tutela dei dati e criminalità informatica;
- analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, custode delle password, interessato;
- rapporti con il Garante;
- misure minime ed appropriate di sicurezza con particolare riferimento a: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software (in particolare antivirus, antispam e misure anti hacker), contenitori di sicurezza, sistemi anti intrusione, importanza e modalità di realizzazione delle operazioni di backup, etc.
- periodicamente il coordinatore del gruppo Reti e Sicurezza o un incaricato del Direttore del Centro Universitario di calcolo deve tenere un corso ai vari amministratori di sistema sulle politiche di sicurezza dei sistemi, sul backup e sul disaster recovery.

# R7: Misure minime trattamenti esterni

Come Centro Universitario di Calcolo, le procedure attualmente affidate in manutenzione all'esterno sono le seguenti:

- STIPENDI a cura del CINECA (database Oracle);
- CONTABILITÀ, PATRIMONIO e PRESENZE a cura della SELFIN (database Oracle);
- BIBLIOTECHE ALEPH 500 a cura dell'ATLANTIS (database Oracle runtime);
- PROTOCOLLO TITULUS a cura della 3D Informatica (database proprietario).
- GEDAS ovvero procedura STUDENTI con il supporto della KION (CINECA).

Tutte le ditte con cui l'Università interloquisce dovranno indicare formalmente almeno una persona responsabile ai fini del trattamento dati.

# R8: cifratura e separazione dati

Cifratura dei dati sensibili e giudiziari:

- Occorre implementare dei file system crittografati cui accedere con password