Progetto “Province & Comuni”, Programma Azione Coesione Complementare al PON Governance e Capacità Istituzionale 2014-2020

Appalti Edzione X
Lezione n. 1

02 Ottobre 2026
Università LUMSA

Cybersecurity nella PA: Normative e Framework - Quadro normativo nazionale ed europeo, NIS2, framework di sicurezza AGID

Ing. Giovanni Amato

A.A. 2025/2026

UPI

LUMSA UNIVERSITÀ

Cybersecurity nella PA: Normative e Framework

Il quadro nazionale ed europeo. NIS2. ACN. AGID.

Attacchi in crescita sulla PA

Nuove leggi. Nuove responsabilita'

Cybersecurity NON solo tecnica, è Governance

Cosa vedremo

In sintesi

- Norme europee
- Norme italiane
- Framework operativi
- Scadenze concrete 2026
- Cosa deve fare davvero una PA

Il quadro europeo

L'UE e la cybersecurity

- Il cyberspazio e' riconosciuto come **spazio di conflitto e instabilita'**
- Attacchi cyber **impattano servizi essenziali**, elezioni, sanita', economia
- L'UE punta a **resilienza sistemica**, non alla sicurezza del singolo ente
- Nasce un **approccio regolatorio**. Obblighi, controlli, sanzioni
- Gli Stati membri devono **allinearsi**, non decidere se aderire

Per l'Unione Europea la cybersecurity **non e' piu' solo tecnica**.

E' un **dominio strategico**, come energia o difesa.

Per questo l'UE usa **regolamenti e direttive vincolanti**, non piu' solo raccomandazioni.

Direttiva NIS2

La NIS2 cambia il modello di cybersecurity in Europa

Direttiva UE 2022/2555

- Approvata a dicembre 2022
- In vigore a livello UE
- Applicabile solo dopo recepimento nazionale

Recepimento obbligatorio

- Gli Stati membri **devono** recepirla
- Scadenza UE. 17 ottobre 2024

Sostituisce NIS1

- NIS1 troppo limitata
- Troppe eccezioni
- Poche sanzioni
- Controlli deboli

Direttiva UE 2022/2555

Recepimento obbligatorio

Sostituisce NIS1

Perche' la NIS1 era troppo limitata?

Limiti strutturali della NIS1

Perimetro troppo ristretto

- Pochi settori coperti
- Molti servizi digitali esclusi
- La PA spesso fuori o marginale

Gran parte delle infrastrutture critiche **non era obbligata** a fare nulla.

Perche' la NIS1 era troppo limitata?

Limiti strutturali della NIS1

Ampia discrezionalita' nazionale

- Ogni Stato decideva chi includere
- Criteri diversi tra Paesi
- Stesso operatore. Obblighi diversi

Nessun livello di sicurezza uniforme in Europa.

Perche' la NIS1 era troppo limitata?

Limiti strutturali della NIS1

Approccio reattivo

- Focus su notifica incidenti
- Poca attenzione alla prevenzione
- Nessun vero risk management strutturato

La sicurezza arrivava **dopo** l'incidente.

Perche' la NIS1 era troppo limitata?

Limiti strutturali della NIS1

Controlli e sanzioni deboli

- Ispezioni rare
- Sanzioni basse o inesistenti
- Compliance spesso formale

Paradossalmente conveniva rischiare che investire in sicurezza.

Perche' la NIS1 era troppo limitata?

Limiti strutturali della NIS1

Supply chain ignorata

- Nessun obbligo sui fornitori
- Nessun controllo sui servizi cloud
- Nessuna visione sistemica

Le evidenze degli ultimi anni dimostrano che **gli attacchi passano** (quasi sempre) **dai fornitori**.

Cosa cambia con la NIS2?

Copertura parziale vs Sicurezza sistemica

TEMA	NIS1 (2016)	NIS2 (2022)
Perimetro	Limitato a pochi settori	Esteso a 18 settori critici
PA	Spesso esclusa o marginale	Inclusa esplicitamente
Servizi digitali	Quasi fuori	Centrali (cloud, data center, DNS)
Criteri di inclusione	Decisi dallo Stato	Armonizzati a livello UE
Approccio	Reattivo	Preventivo e basato sul rischio
Supply chain	Ignorata	Obblighi sui fornitori
Controlli	Rari	Sistemi di vigilanza strutturati
Sanzioni	Deboli o simboliche	Elevate e dissuasive

Perche' NIS2 e' diversa

- + settori
- + soggetti
- + controlli
- Sanzioni vere

LUMSA UNIVERSITÀ

Unione Province d'Italia UPI

Decreto Legislativo 138/2024

Recepisce la Direttiva (UE) 2022/2555 e introduce importanti misure di sicurezza per l'Italia

1. Strategia Nazionale di Cybersecurity	Stabilisce una **strategia globale** per garantire un elevato livello di sicurezza informatica in tutto il paese.
2. Integrazione della gestione delle crisi	Introduce un quadro coordinato per la **gestione delle crisi informatiche**, mirando a una risposta più efficace.
3. Agenzia per la Cybersecurity Nazionale	Conferma l'**ACN come autorità** competente, responsabile per la sicurezza informatica e il punto di contatto unico.
4. Obblighi per soggetti identificati	Definisce criteri e obblighi specifici per i soggetti ritenuti **essenziali** o **importanti**, con focus sulla **segnalazione di incidenti.**
5. Misure di cooperazione e condivisione	Promuove la cooperazione e la **condivisione** delle informazioni tra le autorità e i soggetti coinvolti nella cybersecurity.

Settori coperti dalla NIS2 – Perimetro italiano

18 settori di cui 11 ***altamente critici*** *e 7* ***critici*** *per oltre 80 tipologie di soggetti, distinguendo i soggetti in* ***essenziali*** *e* ***importanti****.*

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia	19 tipologie di soggetto	Essenziali	Importanti *	Fuori ambito **
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto		Importanti *	Fuori ambito **
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto	Importanti *		Fuori ambito **
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			
Fornitori di servizi digitali	4 tipologie di soggetto			
Ricerca	2 tipologie di soggetto	Importanti *		Fuori ambito **
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale	4 categorie di PA	Essenziali		
Pubblica Amministrazione regionale e locale	11 categorie di PA	Importanti *		
Ulteriori tipologie di soggetti	4 tipologie di soggetti	Identificazione dell'Autorità		

https://www.acn.gov.it/portale/documents/d/guest/faq-1-5_dettaglio-ambiti-di-applicazione

PA e classificazione NIS2

Piccolo comune != piccoli obblighi

Le Pubbliche Amministrazioni **non sono tutte uguali** nella NIS2. Possono essere **soggetti essenziali** o **soggetti importanti**, in base alle funzioni svolte.

Per la PA **non** vale il criterio dimensionale. **Vale** il criterio funzionale.

In particolare conta:

- che servizio pubblico eroga l'ente
- che impatto ha l'interruzione
- che ruolo ha nel sistema nazionale

PA come soggetti essenziali

Quando una PA e' soggetto essenziale

- svolge **funzioni critiche per lo Stato**
- garantisce **servizi pubblici essenziali**
- ha impatto diretto su diritti fondamentali
- e' indicata negli allegati del D.Lgs. 138/2024
- oppure e' qualificata come tale da ACN

PA come soggetti importanti

Quando una PA e' soggetto importante

- eroga servizi pubblici **rilevanti ma non critici**
- l'interruzione non genera impatto sistemico nazionale
- i servizi sono localizzati o settoriali
- l'impatto e' significativo ma contenuto

Comuni medio-piccoli

Unioni di comuni

Enti strumentali locali

Agenzie regionali non critiche

Differenza pratica tra essenziale e importante

Tabella riepilogativa

Aspetto	Soggetto essenziale	Soggetto importante
Impatto	Sistemico	Rilevante ma limitato
Livello obblighi	Più elevato	Meno elevato
Numero misure	43	37
Vigilanza	Più stringente	Ordinaria
Aspettativa ACN	Massima resilienza	Adeguata resilienza

Valutazione ACN sulla PA

Ragionamento logico

Una PA puo' essere soggetto importante.

Ma non perche' e' piccola.

Perche' **l'impatto del servizio e' diverso.**

Misure di sicurezza richieste

Quante sono e di quale natura

- **43 misure** per i **soggetti essenziali**
- **37 misure** per i **soggetti importanti**

Tecniche

- sicurezza reti e sistemi
- controllo accessi
- logging e monitoraggio
- backup e ripristino

Organizzative

- gestione del rischio
- ruoli e responsabilita'
- procedure incidenti
- formazione del personale

Esempi di misure tecniche e organizzative

Queste misure **devono esistere, funzionare** e **scritte**

- Inventario asset ICT
- Segmentazione di rete
- Gestione delle vulnerabilita'
- Autenticazione forte
- Backup periodici e testati
- Monitoraggio degli eventi di sicurezza
- Politica di sicurezza formalizzata
- Processo di risk assessment
- Piano di gestione incidenti
- Continuita' operativa
- Ruoli cyber definiti
- Formazione e consapevolezza

Documentare sempre

La NIS2 richiede che la sicurezza sia governata

- **Definite**
- **Attuate**
- **Documentate**
- **Aggiornate**
- **Verificabili**

Timeline NIS2 in Italia

La NIS2 non parte tutta insieme. E' una sequenza obbligata di tre fasi.

1. **Registrazione**
2. Implementazione misure
3. Notifica incidenti

Censimento ufficiale dei soggetti NIS

Avviene tramite **portale ACN**

Vale per soggetti essenziali e importanti

Il termine per la registrazione è fissato al **28 febbraio 2025**.

E se non mi registro cosa succede? 😧

ACN
- valuta le informazioni
- comunica inserimento elenco NIS
- indica se sei essenziale o importante

Timeline NIS2 in Italia

La NIS2 non parte tutta insieme. E' una sequenza obbligata di tre fasi.

1. Registrazione
2. **Implementazione misure**
3. Notifica incidenti

A partire **dalla data di comunicazione ACN** e non dalla data di registrazione.

Abbiamo **18 mesi** per:

- implementare le misure
- rendere operative le procedure
- documentare tutto

Non per comprare software.

misure **attive**

processi **formalizzati**

responsabilita' **assegnate**

documentazione **disponibile**

evidenze **verificabili**

Timeline NIS2 in Italia

La NIS2 non parte tutta insieme. E' una sequenza obbligata di tre fasi.

1. Registrazione
2. Implementazione misure
3. **Notifica incidenti**

pre-notifica tempestiva

notifica completa secondo le tempistiche

uso esclusivo dei canali ACN / CSIRT Italia

Ruoli e Accountability del vertice

Se una persona va via e la funzione sparisce, non sei conforme

- **Struttura di cybersecurity**
- **Referente per la cybersicurezza**
- **Referente CSIRT**
- Coordinamento con **RTD**

Con la NIS2 e la Legge 90/2024, ACN ha i seguenti poteri:

- vigilanza
- ispettivi
- correttivi
- sanzionatori

Punto di Contatto ACN

Il Punto di Contatto e' il referente istituzionale verso ACN. Rappresenta l'ente

- Interlocutore ufficiale con ACN
- Gestisce comunicazioni formali NIS2
- Riceve notifiche, richieste, atti

Il Punto di Contatto non puo' essere esterno

- Dirigente
- Responsabile di struttura
- Figura organizzativa stabile

Referente CSIRT

Il Referente CSIRT e' il referente operativo verso CSIRT Italia. Parla di incidenti non di governance

- Gestione degli incidenti
- Comunicazioni tecniche
- Coordinamento in caso di attacco
- Scambio informazioni operative

Il Referente CSIRT puo' essere esterno

- Responsabile ICT
- Addetto sicurezza informatica
- Fornitore esterno formalmente incaricato

Ruolo **tecnico-operativo**

Deve essere reperibile

Deve conoscere i sistemi ICT

Punto di Contatto vs Referente CSIRT

Le due figure possono coincidere

Aspetto	Punto di contatto	Referente CSIRT
Natura	**Istituzionale**	**Operativa**
Interlocutore	ACN	CSIRT Italia
Tipo comunicazioni	Formali, amministrative	Tecniche, incidenti
Profilo	Dirigenziale / organizzativo	Tecnico-specialistico
Coinvolgimento	Continuo	Event-driven

Perchè notificare un incidente?

La notifica NIS2 non e' una comunicazione unica, ma un processo in piu' fasi.

Informare dell'accaduto

Coordinare le attività risolutive

Contenere l'impatto

Non si notifica al Garante, **non** alla Prefettura, non via PEC generica. **Solo** tramite il canale CSIRT tramite piattaforma ACN.

Quando scatta l'obbligo di notifica

incidente significativi

compromette disponibilita', integrita' o riservatezza di **dati digitali**

ha impatto sui servizi erogati

puo' produrre effetti verso l'esterno

🚫 NON va segnalato:

- un semplice tentativo bloccato
- un evento senza impatto
- un'anomalia non confermata

Fase 1: Early warning (pre-notifica)

La linea guida parla di scoperta, non di inizio dell'attacco

- conferma dell'esistenza dell'incidente
- natura dell'evento
- prima valutazione dell'impatto
- informazioni tecniche disponibili
- misure immediate adottate

Entro 24 ore dalla scoperta dell'incidente significativo.

Non vuol dire avere già il quadro completo, occorre aver riconosciuto l'incidente.

Fase 2: Notifica dell'incidente

Qui il ruolo centrale e' del Referente CSIRT

Entro 72 ore dalla scoperta

- descrizione dettagliata dell'incidente
- cause note o presunte
- impatti su servizi, utenti e sistemi
- misure di contenimento e mitigazione
- stato del ripristino

Fase 3: Aggiornamenti e chiusura

Ciclo di gestione

il soggetto **aggiorni** la notifica se emergono nuovi elementi rilevanti

venga trasmessa una **relazione di chiusura** dell'incidente

Riepilogo segnalazione

La notifica e' un flusso continuo

1. Identificazione incidente
2. Valutazione della significativita'
3. **Early warning (24h)**
4. **Notifica completa (72h)**
5. **Aggiornamenti successivi**
6. Chiusura e lessons learned

Tassonomia Cyber

Parlare la stessa lingua. Un vocabolario comune.

Un incidente cyber non e' solo "un attacco".

Senza un linguaggio comune, ogni amministrazione descrive lo stesso evento **in modo diverso**.

ACN introduce un **vocabolario condiviso** per descrivere cosa e' successo, come, perche' e con che impatto.

Due enti subiscono phishing con furto di credenziali di accesso.

- Uno dice "**problema email**".
- L'altro "**tentativo di truffa**".

Per ACN sono eventi confrontabili solo se classificati nello stesso modo.

Tassonomia != Burocrazia

Non serve a riempire moduli. Serve a prendere decisioni migliori.

La Tassonomia aiuta a capire se **un evento** e' grave, se va notificato, chi deve intervenire e con che priorita'.

Quante volte un incidente viene minimizzato perche' non sappiamo dargli un nome corretto?

Un database esposto su Internet.

Se lo classifichi come **Data Exposure** e **Severity Medium**, capisci subito che non e' un semplice disservizio IT.

Struttura a 4 blocchi

Ogni evento cyber viene visto da quattro angoli diversi.

Ransomware

- Impatto: Dati cifrati.
- Minaccia: Malicious Code.
- Attore: Criminale.
- Contesto: Account valido usato.

Cosa e' successo.

Che tipo di minaccia e'.

Chi c'e' dietro.

Che contesto aggiuntivo c'e'.

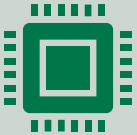
Da dove si inizia?

Prima di chiederti chi ti ha attaccato, guarda cosa ha rotto.

La prima domanda non e' "**chi e' stato**", ma "**che danno ho subito**".

Dati persi, servizi fermi, account compromessi.

Phishing andato a buon fine ma senza conseguenze. E' No Impact.



Stesso phishing con accesso a **PEC istituzionale**. Diventa Account Compromise.

La Severity

Grave non significa tecnico. Significa impatto sul servizio.

La gravita' **non** dipende dal tipo di **attacco**.

Ma dall'effetto sull'organizzazione e sui cittadini.

Un ransomware su un PC spento. **Low**.

Un guasto che blocca un servizio anagrafico online. **High**.

Non e' sempre colpa degli hacker

Molti incidenti nascono da errori interni o fornitori.

La tassonomia distingue:

- attacco malevolo
- errore umano
- guasto tecnico
- problema del fornitore

Server pubblico senza password: Non e' hacking. E' Human Error.

Cloud down per problema del provider: Third Party Failure.

Dare un nome alla minaccia

Phishing, ransomware, DDoS non sono sinonimi.

ACN separa bene i tipi di minaccia.

- Scansione
- Malware
- Frode
- Ingegneria sociale

Serve a capire cosa aspettarsi dopo.

La minaccia NON è un incidente.

Riconoscerla evita l'incidente

Active Scanning oggi.

Domani sfruttamento vulnerabilita'.

Era prevedibile!

Social Engineering

Il sistema piu' vulnerabile e' la persona.

Phishing, smishing, vishing.

Non sono problemi tecnici. Sono problemi organizzativi e culturali.

Email finta del dirigente che **chiede urgenza**.

- Nessun malware.
- Solo pressione psicologica.

Threat Actor

Capire chi attacca aiuta a capire perche'.

- Criminale
- Insider
- Hacktivist
- Stato

Ogni attore ha obiettivi diversi e tempi diversi.

La risposta a un attacco cambia se cambia la motivazione.

Ransomware chiede soldi. Motivazione: profitto.

Defacement sito istituzionale. Motivazione: ideologica.

Il contesto fa la differenza

Due incidenti identici non sono mai uguali.

Asset coinvolto, vettore di attacco, supply chain, account validi.

Qui si capisce dove occorre intervenire davvero.

Accesso con account valido....

Il problema **non e' il firewall** ma la **gestione identita'.**

Perche' questa tassonomia e' utile per la PA

La tassonomia ACN serve a governare il rischio.

Aiuta nella **notifica NIS2**, nella **gestione incidenti**, nel **dialogo con ACN e fornitori**.

E soprattutto crea consapevolezza.

Senza linguaggio comune, non esiste sicurezza sistemica.

Cybersecurity Act

*Regolamento UE che crea il quadro europeo di **certificazione della sicurezza informatica** e definisce il ruolo di **ENISA***

Con la **revisione del Cybersecurity Act**, proposta dalla Commissione nel 2026, la sicurezza della **supply chain ICT** diventa **oggetto di regolazione europea**, non solo per gli operatori NIS2, ma anche per i prodotti immessi sul mercato UE.

Regola **i prodotti e le supply chain ICT**.

Introduce certificazione, security by design, valutazione dei fornitori.

Guarda la tecnologia prima che arrivi sul mercato.

AGID, CAD e misure minime di sicurezza

AGID non e' autorita' di vigilanza cyber. Quel ruolo oggi e' in capo ad ACN

Le **Misure Minime di Sicurezza AGID** restano in vigore come riferimento per la **Pubblica Amministrazione italiana** e continuano a valere come base o punto di partenza per i controlli di sicurezza informatica delle PA.

Soprattutto per le organizzazioni pubbliche che **NON soggette a NIS2**.

Agenzia di indirizzo per la **trasformazione digitale della PA**

Produce **linee guida tecniche e operative**

Supporto architetture ICT

Supporto sicurezza by design

Supporto servizi digitali

AGID e i Trust Service Provider (eIDAS)

AGID e' autorita' nazionale di vigilanza sui prestatori di servizi fiduciari ai sensi del regolamento eIDAS

- firme elettroniche
- sigilli elettronici
- marche temporali
- certificati di autenticazione
- servizi di recapito elettronico certificato

Vigilanza, CERT-AGID e gestione degli incidenti

CERT-AGID supporta AGID nelle attivita' operative connesse ai servizi fiduciari

L'articolo 14-bis, comma 2, lettera i) del CAD attribuisce all'Agenzia funzioni di **Vigilanza sui servizi fiduciari** ai sensi dell'articolo 17 del Regolamento UE 910/2014 (Regolamento eIDAS), in qualità di organismo a tal fine designato sui gestori di posta elettronica certificata, sui soggetti che erogano servizi di conservazione a norma, nonché sui soggetti, pubblici e privati, che partecipano a SPID di cui all'articolo 64.

Resta in capo ad ACN:

- la risposta agli incidenti
- le notifiche
- le attivita' di crisi cyber

analisi tecnica delle vulnerabilita'

supporto alle verifiche di sicurezza

valutazione degli impatti cyber sui servizi fiduciari

collaborazione nelle attivita' di audit tecnico

Il CAD e la sicurezza nella PA

Il CAD rende la cybersecurity un dovere legale della PA, non una scelta tecnica

Il CAD **impone obblighi giuridici di sicurezza** alle Pubbliche Amministrazioni.

La cybersecurity e' parte integrante della qualita' del servizio pubblico digitale.

Art. 51 - Obbligo di garantire integrita', disponibilita' e riservatezza dei dati e dei servizi digitali. Continuita' operativa e protezione delle infrastrutture ICT

Art. 17 - Il Responsabile per la Transizione Digitale (RTD) coordina la trasformazione digitale e promuove la **consapevolezza dei rischi cyber** all'interno dell'amministrazione

Artt. 12–13 - Obbligo di formazione del personale sull'uso sicuro degli strumenti ICT.

Perimetro di Sicurezza Nazionale Cibernetica

Cos'è e perché conta

È stato istituito dal **Decreto-Legge 105/2019**, convertito con modificazioni nella **Legge 133/2019**.

non è un "firewall nazionale", ma un **sistema di governance cyber nazionale**.

si applica ad **enti pubblici e privati** con impatti rilevanti per la sicurezza e la continuità dei servizi essenziali.

Il PSNC è un quadro normativo nazionale per proteggere **Reti**, **sistemi informativi** e **servizi ICT** da cui dipendono funzioni **essenziali dello Stato** o **servizi essenziali** per i cittadini.

PSNC: elementi chiave degli obblighi

Il PSNC non sostituisce NIS2

Infrastrutture critiche

- Soggetti pubblici e privati che erogano **servizi o funzioni essenziali** sono inclusi nel PSNC
- Settori tipici: telecomunicazioni, energia, trasporti, servizi digitali, economia e finanza, difesa, interno, spazio, tecnologie critiche

Regime speciale

- **Annualmente** gli asset ICT strategici devono essere elencati dai soggetti inclusi nel PSNC
- Tali asset sono quelli da cui dipende la fornitura di **servizi essenziali o funzioni essenziali**
- Obbligo di **misure di sicurezza elevate** e di gestione del rischio secondo criteri nazionali

Obblighi equivalenti e coordinamento con NIS2

- I soggetti PSNC devono comunque rispettare anche gli obblighi NIS2 se ricadono in quell'ambito, con coordinamento normativo tra le due discipline per evitare duplicazioni inutili

Riepilogando

Cosa fanno in sintesi

- **CAD** - Dice *che cosa e' obbligatorio* per la PA digitale
- **AGID** - Spiega *come farlo bene*, dal punto di vista tecnico
- **NIS2** - Introduce *nuovi obblighi europei* su rischio, incidenti e governance
- **ACN** - E' *chi controlla, coordina e sanziona*
- **PSNC** - E' il *regime piu' forte*, per asset davvero critici

Minacce reali per la PA

Non si attacca la PA per errore. Si attacca per impatto

Il numero di incidenti **in aumento costante.**

La PA e' un **bersaglio strutturale**, non occasionale

Motivazioni:

- valore dei dati
- continuita' dei servizi
- bassa tolleranza all'interruzione

Cosa deve fare una PA oggi

La cybersecurity parte dall'organizzazione, non dai tool

- Capire se rientra in **NIS2** o **PSNC**
- Registrarsi sul **portale ACN** se obbligata
- Nominare i **ruoli formali** (RTD, Punto di Contatto, Referente CSIRT)
- Pianificare le misure con **tempi, responsabilita' e priorita'**

Grazie per l'attenzione

Gianni Amato

LUMSA
UNIVERSITÀ