La Cybersicurezza nelle Università e negli EPR

Prof. Paolo Atzeni, Ing. Monica Scannapieco

Roma, 29 Novembre 2023

Ricerca, Awareness e Formazione: il ruolo di ACN

Ricerca

*Considerato dall'art. 7, comma 1, lett. r) del D.L. n. 82/2021, l'**Agenzia per la Cybersicurezza Nazionale** supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionale, lo **sviluppo di competenze e capacità industriali, tecnologiche e scientifiche**. Inoltre, in considerazione e attuazione delle **misure #53 e #54** della **Strategia Nazionale di Cybersicurezza**, l'ACN promuove ogni iniziativa volta al rafforzamento dell'autonomia industriale e tecnologica in Italia e favorisce la ricerca e lo sviluppo, specialmente nelle nuove tecnologie.*

Awareness

*Considerato dall'art. 7, comma 1, lett. u) del D.L. n. 82/2021, l'**Agenzia per la Cybersicurezza Nazionale** svolge **attivita' di comunicazione e promozione della consapevolezza in materia di cybersicurezza**, al fine di contribuire allo sviluppo di una cultura nazionale in materia . Inoltre, in considerazione e attuazione della misure **#71** della **Strategia Nazionale di Cybersicurezza**, l'ACN promuove iniziative di sensibilizzazione volte a promuovere competenze e comportamenti responsabili nello spazio cibernetico.*

Formazione

*Considerato dall'art. 7, comma 1, lett. u) del D.L. n. 82/2021, l'**Agenzia per la Cybersicurezza Nazionale** promuove la **formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza**.*

ACN e la Ricerca

- La promozione e la valorizzazione della ricerca pubblica e privata sulla cybersicurezza sono elementi important della Strategia Nazionale di Cybersicurezza
  - 14 su 82 misure della Strategia sono esplicitamente legate alla ricerca

	Misura	Attori Responsabili	Altri Soggetti Interessati
53	Promuovere **ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica** dell'Italia, riguardo a prodotti e processi informatici di rilevanza strategica ed a tutela degli interessi nazionali nel settore, anche valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali.	ACN, DTD, MIMIT, MUR, MIN. Difesa	Atenei, Ricerca, Regioni e Province autonome
54	Favorire la **ricerca e lo sviluppo**, specialmente nelle **nuove tecnologie**, promuovendo l'inclusione dei principi di cybersicurezza e supportando, **anche mediante finanziamenti, investimenti pubblici e privati e meccanismi di semplificazione**, progetti di sicurezza cibernetica da parte del **settore privato** – con particolare riferimento alle startup e alle PMI innovative – e dei **Centri di competenza e di ricerca attivi sul territorio nazionale**	ACN, DTD, MEF, MUR, MIN. Difesa	Operatori privati, Atenei, Ricerca

Definizione di una **base** di conoscenza **di concetti condivisi** e indicazione di **argomenti di ricerca prioritari**

→

Agenda di Ricerca e Innovazione

Agenda di Ricerca e Innovazione sulla Cybersicurezza

Collaborazione ACN – MUR	• Programma Nazionale per la Ricerca 2021-2027 e allegato esteso sulla sicurezza dei sistemi sociali
Indicazioni a supporto	• CINI Laboratorio Nazionale di Cybersecurity • ACN Comitato Tecnico Scientifico • Ricercatori selezionati
Orizzonte Temporale 2023-2026	• Aggiornamenti periodici fino al 2026
Audience	• Attori che operano direttamente o beneficiano della ricerca sulla cybersicurezza, sia del settore pubblico sia del settore privato

AGENDA DI RICERCA E INNOVAZIONE

- *L'Agenda come risultato dell'attività congiunta tra* ***l'Agenzia per la Cybersicurezza Nazionale e il Ministero dell'Università e della Ricerca*** è stata ***pubblicata a Giugno 2023***
- Versione **italiana** e **inglese, https://www.acn.gov.it/strategia/agenda-di-ricerca-e-innovazione**

METODOLOGIA E CONTENUTI

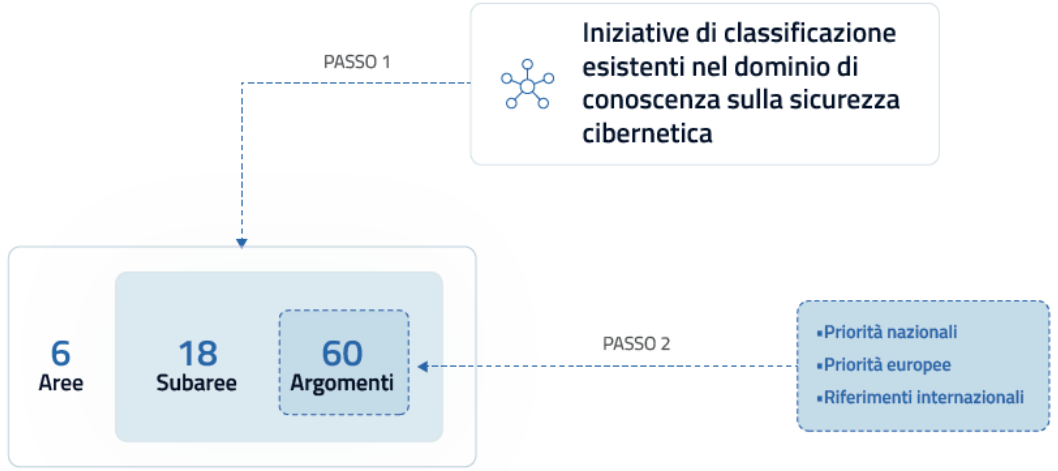
Passo #1

Identificazione di aree nel dominio di conoscenza della cybersicurezza raggruppando iniziative di classificazione esistenti (Fondazione **SERICS**, **ENISA**, **JRC**, **CyBOK**)

Passo #2

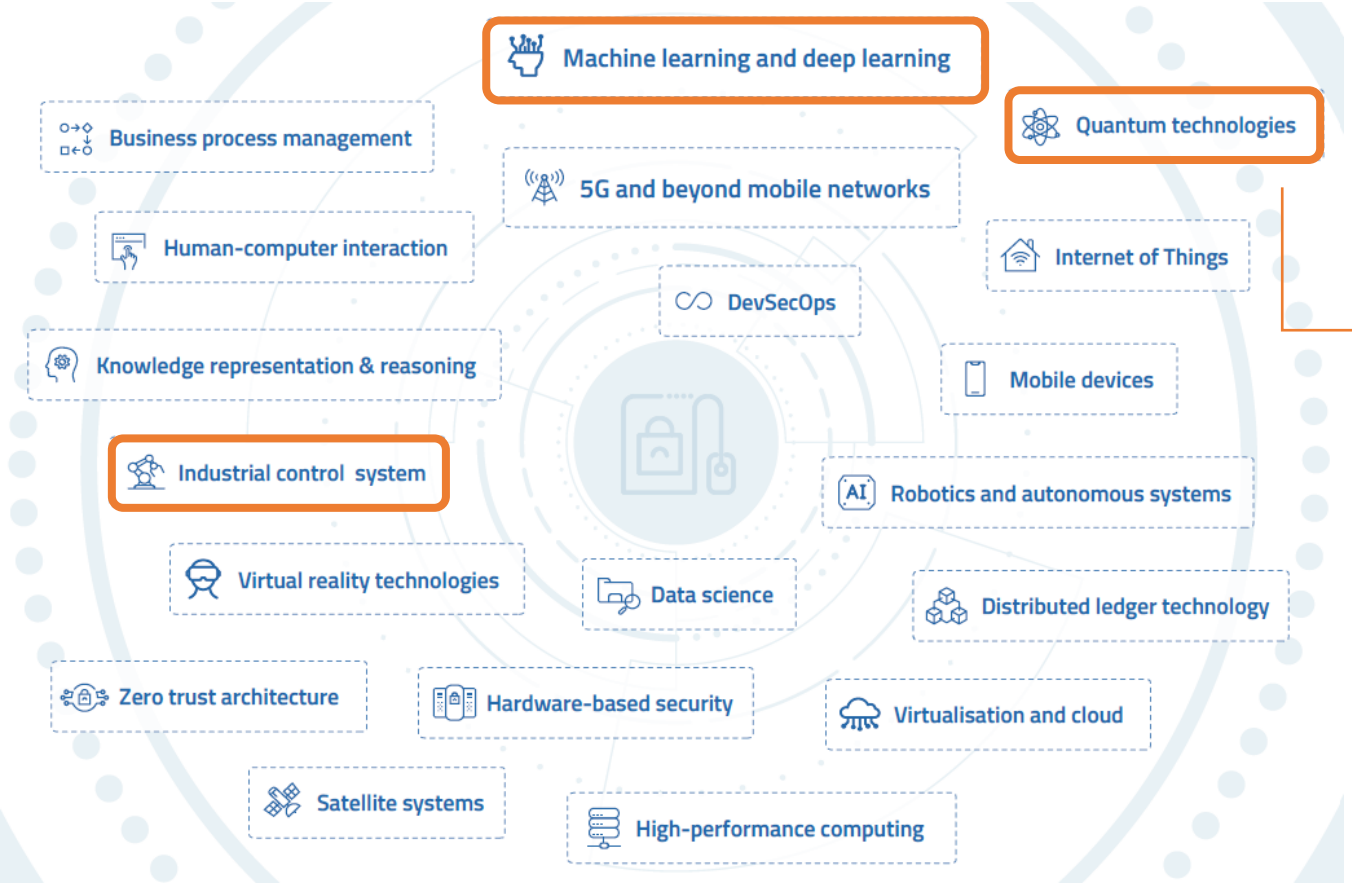
Definizione di subaree e relativi argomenti valutando sia le priorità italiane (e.g., MUR, Fondazione SERICS) ed europee (e.g., ENISA) sia riferimenti rilevanti sul piano internazionale (e.g., National Institute of Standards and Technology statunitense – NIST)

Sono stati identificati **60 argomenti** di ricerca prioritari afferenti a **18 subaree** raggruppate in **6 aree**



EDT E AREE DI R&I

*Si è ritenuto importante identificare un insieme di **Emerging and Disruptive Technology (EDT)** e metterle in corrispondenza con le subaree, nel ruolo di vincolo o supporto agli argomenti individuati.*



Le EDT considerate appartengono a diversi livelli di astrazione, includendo sia <u>paradigmi</u> sia <u>singole tecniche</u>

Queste EDT sono importanti nell'affrontare i problemi di cybersicurezza legati a:

- Sistemi di **intelligenza artificiale**
- **Crittografia** post-quantum
- Resilienza delle **infrastrutture critiche**

PROSSIMI PASSI - 1

54	Favorire la **ricerca e lo sviluppo,** specialmente nelle **nuove tecnologie,** promuovendo l'inclusione dei principi di cybersicurezza e supportando, **anche mediante finanziamenti, investimenti pubblici e privati e meccanismi di semplificazione,** progetti di sicurezza cibernetica da parte del **settore privato** – con particolare riferimento alle startup e alle PMI innovative – e dei **Centri di competenza e di ricerca attivi sul territorio nazionale**

Definizione di un'**Agenda di R&I per la cybersicurezza** che consideri le specificità del contesto nazionale.

Supporto ed indirizzo al sistema Italiano della Ricerca, con l'obiettivo di sviluppare nuove capacità e competenze nelle imprese e di colmare le carenze tecnologiche esistenti nel campo della cybersicurezza.

IN CORSO

PROSSIMI PASSI - 2

54	Favorire la **ricerca e lo sviluppo,** specialmente nelle **nuove tecnologie,** promuovendo l'inclusione dei principi di cybersicurezza e supportando**, anche mediante finanziamenti, investimenti pubblici e privati e meccanismi di semplificazione,** progetti di sicurezza cibernetica da parte del **settore privato** – con particolare riferimento alle startup e alle PMI innovative – e dei **Centri di competenza e di ricerca attivi sul territorio nazionale**

- Pubblicazione da parte di ACN di una **manifestazione di interesse** per **il finanziamento di 30 borse di dottorato a partire dall'A.A. 2024/2025**
- Il bando prevederà il finanziamento di borse di dottorato sui **temi dell'Agenda di Ricerca e Innovazione**
- Pubblicheremo **entro l'anno** la manifestazione di interesse **sul sito di ACN**
- **Programma di finanziamento pluriennale** finalizzato a creare una collaborazione strutturale tra ACN e le università

PROSSIMI PASSI - 3 : Struttura del programma «Cyber Innovation Network» - RICERCA

AREA DI INTERVENTO 1

[Progettualità avviata]

Sviluppo di **nuova imprenditorialità innovativa** (**startup e spin-off**) in collaborazione con primari **programmi di incubazione ed accelerazione**

Obiettivi

- ❑ Costruire una **rete stabile con l'ecosistema dell'innovazione,** per programmi congiunti con l'Agenzia.
- ❑ Creare e sviluppare **nuove realtà imprenditoriali** (startup e spin-off) ad alto contenuto di innovazione nelle aree tecnologiche dell'Agenzia.
- ❑ Supportare la **validazione e lo sviluppo di tecnologie emergenti,** per favorire innovazione e discontinuità tecnologiche.

Benefici alle startup

- ❑ Opportunità di **validare tecnologie e soluzioni** nei contesti di impiego dell'Agenzia.
- ❑ **Contributo a fondo perduto*** per progetti di validazione (fino a 50.000 €) e per progetti di sviluppo (fino a 150.000 €).

**Il contributo complessivo per startup non potrà superare 200.000 € nel rispetto della disciplina degli aiuti di Stato.*

AREA DI INTERVENTO 2

[Progettualità pianificata]

Valorizzazione dei risultati della ricerca pubblica in collaborazione con i *Technology Transfer Offices* di Università ed Enti Pubblici di Ricerca

Obiettivi

- ❑ **Ampliare l'Innovation Network** con il coinvolgimento dei TTOs.
- ❑ **Favorire i processi di trasferimento tecnologico,** innalzando il TRL dei risultati della ricerca.
- ❑ Creare una vera e propria **filiera integrata di sostegno all'innovazione,** partendo dalle fasi più a monte della ricerca.

Benefici ai gruppi di ricerca

- ❑ Opportunità di **validare i risultati della ricerca incrementandone il TRL** su filoni tecnologici ed impiego ad alto impatto.
- ❑ **Contributo a fondo perduto** erogato ai **gruppi di ricerca** attraverso il coinvolgimento dei TTOs

Cybersecurity Awareness: principali attività e risultati - 1

Obiettivo: favorire la sensibilizzazione sui temi della cybersicurezza nella popolazione e nelle imprese per la promozione di una cultura nazionale in materia

Programma per l'Awareness della Cybersicurezza 2023-2026

Piano di governance delle iniziative che identifica temi, destinatari, strumenti e canali di riferimento per l'Agenzia

Campagna ECSM
a tema social engineering
Ottobre 2023

Landing page della campagna italiana sul sito ufficiale
acn.gov.it/ecsm23

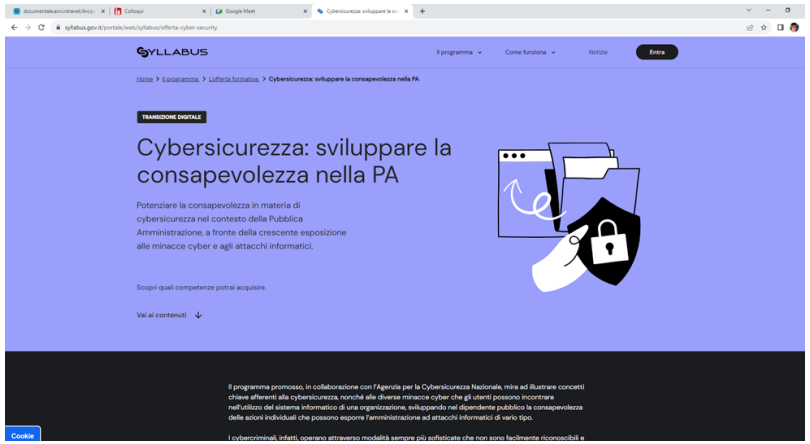
Contenuti della pagina:

- ✓ **Videoclip** di lancio che mostra **istanze tipiche di attacchi di tipo social engineering *(phishing, smishing, vishing, ecc.)*** ai danni di target differenziati per età
- ✓ **Pillole video «Red Flag»** sui 3 **segnali di allarme** più comuni
- ✓ **Video sul profilo dei cybercriminali**
- ✓ **Tips**: 9 Infografiche con consigli pratici su come limitare i rischi e proteggersi
- ✓ **Media kit** contenente il **logo** della campagna e un **poster scaricabile**

Cybersecurity Awareness: principali attività e risultati - 2

Obiettivo: favorire la sensibilizzazione sui temi della cybersicurezza nella popolazione e nelle imprese per la promozione di una cultura nazionale in materia

Syllabus
Modulo di cybersicurezza per la PA



- Investimento "1.5 Cybersecurity" del PNRR, **avviso pubblico n. 2/202**2, erogazione di interventi di potenziamento e miglioramento delle capacità cyber della Pubblica Amministrazione: circa **30 sessioni formative** che hanno coinvolto circa **2.200 dipendenti delle PA coinvolte**
- **Dipartimento della Funzione Pubblica**, l'Agenzia ha attivato una progettualità mirata alla creazione di **materiale formativo di consapevolezza cyber** - in modalità format video e slideshow, fruibile in autonomia dal personale discente mediante una piattaforma informatica dedicata - **Syllabus**.

Accordi e collaborazioni con organizzazioni italiane ed europee:
Dipartimento della Funzione Pubblica, ENISA, Banca d'Italia, Consorzio pubblico-privato a guida MIM SIC Italia – Generazioni connesse

FORMAZIONE

ACN e la formazione (DL 82/2021)

L'Agenzia:

- è Autorità nazionale per la cybersicurezza e […] assicura, nel rispetto delle competenze […] il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche […] nonché per il conseguimento dell'autonomia, nazionale ed europea […]
- predispone la strategia nazionale di cybersicurezza
- promuove la formazione […]

Cybersecurity skills shortage (ENISA 2019)

- https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

- *The lack of qualified cybersecurity professionals in the labour market, represents an issue for both economic development and national security, especially in the rapid digitisation of the global economy*

Ampliamo il contesto

- 2030 Digital Compass, pubblicato nel 2021: l'Europa afferma di essere in ritardo
  - obiettivo europeo: 20 milioni di specialisti ICT nel 2030
  - disponibilità al 2019: 7.8 milioni, crescita annua al 4.2%

https://commission.europa.eu/document/download/9fc32029-7af3-4ea2-8b7a-4cd283e8e89e_en?filename=cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf

Digital Economy and Society Index (DESI)

- 2022 DESI, l'Italia è in ritardo rispetto alla media europea

1 Human capital	Italy		EU
	rank	score	score
DESI 2022	25	36.6	45.7

	Italy			EU
	DESI 2020	DESI 2021	DESI 2022	DESI 2022
1a1 At least basic digital skills % individuals	NA	NA	46% 2021	54% 2021
1a2 Above basic digital skills % individuals	NA	NA	23% 2021	26% 2021
1a3 At least basic digital content creation skills[4] % individuals	NA	NA	58% 2021	66% 2021
1b1 ICT specialists % individuals in employment aged 15-74	3.5% 2019	3.6% 2020	3.8% 2021	4.5% 2021
1b2 Female ICT specialists % ICT specialists	15% 2019	16% 2020	16% 2021	19% 2021
1b3 Enterprises providing ICT training % enterprises	19% 2019	15% 2020	15% 2020	20% 2020
1b4 ICT graduates % graduates	1.3% 2018	1.3% 2019	1.4% 2020	3.9% 2020

- Gli indicatori sono relativi all'intero mondo ICT, la Commissione Europea sta valutando l'introduzione di indicatori specifici sulla cybersicurezza

Un inciso, cruciale e trasversale

- Sul fronte del genere siamo sotto la media (che comunque è insoddisfacente)
- Tutte le iniziative debbono realmente essere inclusive, con riferimento ai gruppi/insiemi sottorappresentati, ad esempio riguardo al genere:
    - in ogni contesto (scuola, università, mondo del lavoro) sono necessarie azioni specificamente volte a ridurre il divario di genere e le relative disparità di trattamento

La formazione nella Strategia Nazionale

- Formazione cyber strettamente connessa con la formazione nelle tecnologie informatiche
  - molte delle tecnologie cyber sono tecnologie informatiche
  - le carenze di forza lavoro e divario di competenze valgono per le une come per le altre
  - in entrambi i casi le tecnologie sono pervasive e presentano aspetti trasversali e applicativi

L'obiettivo complessivo è uno, con due facce

- La cybersicurezza va governata
  - serve un numero consistente di specialisti cyber
  - chi ha responsabilità aziendali, amministrative, operative, deve saper dare il "giusto" valore alle tecnologie
    - "giusto" significa accettazione, consapevolezza, approccio maturo e non fideistico, collaborazione fra soggetti con competenze diverse
      - al livello operativo è necessario saper utilizzare le tecnologie
      - ai livelli via via più alti è necessario saper governare le tecnologie, supervisionando chi le utilizza e dialogando con chi le promuove e sviluppa

Competenze cyber, varie prospettive

- Competenze di base, consapevolezza dei rischi (“awareness” – cultura della sicurezza cibernetica)
- Competenze specialistiche di cybersicurezza (dal punto di vista tecnologico o giuridico/amministrativo/gestionale)
- Competenze "complementari", per
  - funzionari e dirigenti a vari livelli, che hanno responsabilità in merito alla sicurezza delle attività di competenza delle proprie strutture
  - specialisti di domini applicativi (sanità, ricerca, finanza, diritto, infrastrutture

Come procedere per gli specialisti

- Approccio sistematico e obiettivo a medio termine
  - Aumentare il numero di laureati, almeno in discipline ICT, se possibile con "specializzazione" cyber
    - Richiede tempo e grande impegno di promozione, partendo anche dalla scuola
- Approccio pragmatico, ma comunque strutturato (già seguito per ICT negli anni '80 e '90)
  - Formare sul campo o con percorsi mirati (o con una combinazione) persone con diverso background
    - Informatici che non hanno competenze cyber
    - Laureati o diplomati in discipline diverse

ACN e la promozione di corsi di studio e dottorati

- ACN sta per lanciare
  - programma di finanziamento di borse di dottorato (già citato)
  - programma di incentivazione di corsi di laurea magistrale, con borse di studio e premi di laurea

Informatica e cybersicurezza vs domini applicativi

- Dobbiamo crescere
  - Molti informatici e specialisti cyber pensano che basti studiare le metodologie e tecnologie per poterle applicare a qualunque dominio
  - Molti degli altri pensano che le tecnologie informatiche siano "*commodity,*" come l'acqua, l'energia elettrica e il gas, e che si possano usare senza conoscerle per niente
- Purtroppo (o per fortuna!) non è così
  - Gli informatici debbono avere la consapevolezza dell'importanza dei domini applicativi
  - Gli specialisti dei vari domini (o almeno parte di loro), se vogliono utilizzare una tecnologia ricca e flessibile, debbono conoscere almeno qualcosa dei suoi principi

Percorsi formativi con competenze complementari

- Gli specialisti cyber e più in generale gli informatici debbono studiare e sperimentare i domini applicativi
- Economisti, giuristi, ingegneri, medici, umanisti debbono studiare le basi delle tecnologie (almeno informatiche, meglio se anche cyber), per poter interagire con gli specialisti

Cultura della sicurezza cibernetica

(ne ha già parlato l'ing Scannapieco ma è utile ripetere)

- È necessaria consapevolezza di tutti su rischi e minacce cyber: attacchi cibernetici, ma anche diffusione di contenuti fake
- Ogni singolo deve percepire il proprio ruolo quale parte responsabile, attuando comportamenti sicuri e virtuosi (dalla protezione delle password, all'attenzione ai link malevoli e alle “fake news”)
- È necessario un programma capillare di educazione digitale (in varie forme, online e presenza) diretto all’adozione di buone prassi
  - nel mondo lavorativo dai livelli apicali a quelli operativi (ciascuno secondo le relative responsabilità) ma anche nella cittadinanza, a cominciare dagli studenti

Cultura della sicurezza cibernetica (2)

- L'università è uno dei contesti in cui queste azioni vanno svolte
  - verso docenti, personale tecnico amministrativo e bibliotecario, studenti
- ACN promuove attività di sensibilizzazione, in collaborazione con il MUR e con il coinvolgimento della CRUI

Grazie per l’attenzione