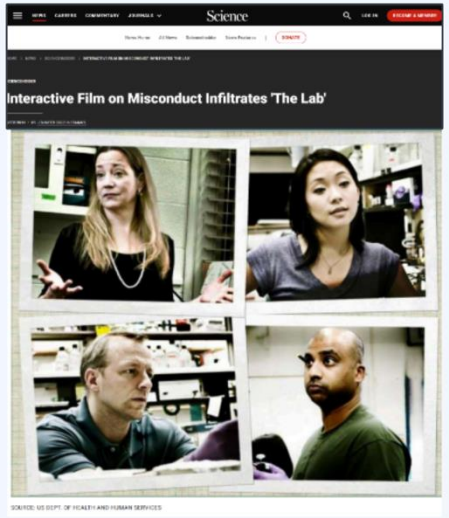
# Verso un modello per la sicurezza e integrità della ricerca

**Paolo Valente**
Direttore Sezione INFN di Roma
Segretario CoPER

# Cosa si intende per research security




Il tema «*research security and integrity*» non è nuovo, ma ha acquisito maggiore visibilità e attenzione a partire dal 2020, declinato prevalentemente nella dimensione *foreign interference*

⇦ 2011

2020 ⇨




Negli anni successivi il concetto si amplia – anche in USA – e attira l'attenzione di altri paesi e organizzazioni internazionali (es. OCSE)




Dopo un approccio iniziale (2022) molto indirizzato alla *foreign interference* da parte della Commissione, anche il Consiglio dell'UE adotta (maggio 2024) una Raccomandazione di più ampio respiro

# Il percorso della UE

## 2021

**Maggio**

**Commissione** pubblica una comunicazione sull'approccio globale alla ricerca e all'innovazione.
**Nuova strategia europea per la politica internazionale R&I**

**Novembre**

**Consiglio** adotta l'agenda politica dello Spazio europeo della ricerca (SER) 2022-2024 nell'ambito delle sue conclusioni.
**La lotta alle ingerenze straniere figura tra le azioni prioritarie**

## 2022

**Gennaio**

**Commissione** pubblica ***Tackling R&I foreign interference***. Staff Working Document European Commission

**Marzo**

**Parlamento europeo** adotta una **risoluzione sulle ingerenze straniere**.

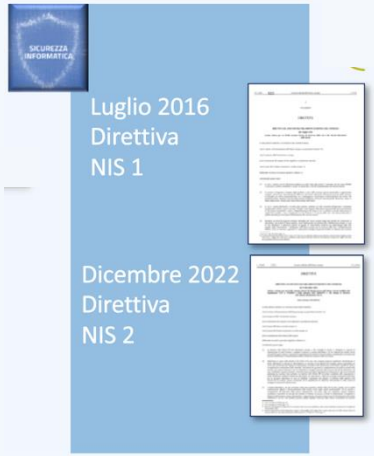
**Giugno**

**Consiglio** adotta conclusioni su valori e principi cooperazione internazionale in R&I.
Si sottolinea l'importanza della gestione di rischi e sicurezza.
Si invita la Commissione e gli S.M. a sviluppare buone pratiche


Il fenomeno della ***Foreign Interference***, o interferenza straniera, si verifica quando le attività svolte da, o per conto di, un attore straniero a livello statale, sono **coercitive**, **segrete**, **ingannevoli** o **corruttive** e sono **contrarie alla sovranità**, ai **valori** e agli **interessi** dell'Unione Europea.

Gli istituti di formazione superiore e gli organismi di ricerca possono trarre vantaggio da una strategia globale per affrontare le interferenze straniere che copra aree chiave di attenzione raggruppate nelle seguenti quattro categorie:

- **Valori**
- **Governance**
- **Partenariati**
- **Sicurezza informatica**




Un capitolo a sé: la cybersicurezza

## 2023

**Luglio**

**Commissione** lancia la ***Strategia di sicurezza*** economica dell'UE.
Tre pilastri: **promozione, protezione e partenariato**.
R&I sono rilevanti in tutti e tre i settori.

**Ottobre**

**Commissione** adotta la raccomandazione (UE) 2023/2113.
Sono individuati **10 settori tecnologici critici per la sicurezza** economica.

Avviate **4 valutazioni dei rischi** in quattro dei dieci settori tecnologici critici individuati:

- **semiconduttori avanzati**
- **intelligenza artificiale**
- **tecnologie quantistiche**
- **biotecnologie.**

## 2024

**Maggio**

- Definisce concetti chiave
- Formula 14 raccomandazioni agli S. M.
- Richiama il ruolo degli organismi di ricerca e dei soggetti finanziatori
- Affida alla Commissione il ruolo di monitoraggio

# Sicurezza della ricerca

## Anticipazione e gestione dei rischi relativi a:

a) **Trasferimento indesiderato** di conoscenze e tecnologie critiche

b) **Ingerenze malevole** che possono sfociare nella strumentalizzazione

c) **Violazioni dell'etica o dell'integrità** conoscenze e tecnologie utilizzate per reprimere, violare o minare valori e diritti

| Europa | Stati Membri | Organismi di ricerca | Soggetti finanziatori |
|---|---|---|---|
| • Sostenere l'attuazione della Raccomandazione<br>• Istituire un Centro europeo di competenze sulla sicurezza della ricerca per creare pratiche comuni e sviluppare la base di conoscenze per l'elaborazione delle politiche | • Realizzare azioni strategiche per rafforzare la sicurezza della ricerca<br>• Rafforzare le conoscenze, attraverso l'analisi del panorama delle minacce, compresa cibersicurezza<br>• Creare una struttura di supporto ("research security advisory hub") | • i progetti di ricerca selezionati per il finanziamento siano sottoposti a un'analisi dei rischi proporzionata<br>• Introdurre procedure interne di gestione del rischio e garantire che i MoU siano validi dal punto di vista della sicurezza della ricerca | • Integrare la sicurezza della ricerca nel processo di funding application<br>• Prendere in considerazione le salvaguardie previste dall'UE Horizon Europe<br>• Assicurarsi che le partnership (es. MoU) siano validi dal punto di vista della sicurezza della ricerca |

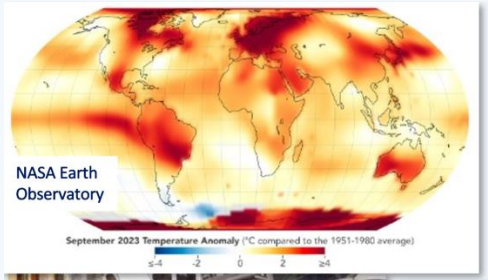
# Come affrontare il problema?

G7 Cornwall UK 2021

G7 Research Compact

G7 ('track' Science) entra nel dibattito sul tema nel 2021 con un approccio equilibrato ed... equilibrante: fiducia, collaborazione, trasparenza, integrità

*...Working together we will use our position as leading science nations to **collaborate on global challenges**, increase the **transparency and integrity** of research, and facilitate **data free flow with trust** to drive innovation and advance knowledge...*




Non si può rinunciare alla collaborazione internazionale nell'affrontare grandi sfide che trascendono i confini fra gli Stati


Il cambiamento climatico e le sue disastrose conseguenze


Le pandemie e la diffusione della resistenza agli antimicrobici


G7 ITALIA 2024

**G7 MINISTERS' MEETING ON SCIENCE AND TECHNOLOGY**
Bologna-Forlì 9-11 luglio 2024

- **Closing down** the free flow of information **will slow progress** in fields that are currently open...
- A **heavy-handed approach** could lead to the unintended consequence of **isolating our researchers** and their institutions from valuable global partnerships.

- This isolation could **diminish our collective scientific capacity** and hinder our ability to address global challenges effectively together.
- By adopting **a balanced approach**, we can enhance **research security** while maintaining the **openness** that is essential for scientific discovery.

- Let us work together to create **a secure yet collaborative research environment** that continues to drive innovation and address the pressing needs of our world.

*Intervento di Maria Leptin, Presidente ERC, alla Ministeriale dei Ministri della Scienza G7 a Bologna*

# Gruppo di lavoro MUR

**DECRETA**

**Art. 1**

Le premesse costituiscono parte integrante del presente decreto.

Per le finalità indicate in premessa, è costituito il Gruppo di Lavoro (nel seguito anche solo GdL) sulla sicurezza della ricerca nella seguente composizione:

- **Francesco Cupertino**, Rettore del Politecnico di Bari – **coordinatore.**



*Ministero dell'università e della ricerca*

Segretariato Generale

- **Fulvio Esposito**, già Rettore dell'Università di Camerino e rappresentante italiano nel SIGRE w.g..
- **Fabrizio Barberis**, Ricercatore Confermato di Ingegneria dei Materiali e delegato per "Beni e tecnologie dual use" per l'Università di Genova.
- **Alessandro Mei**, Professore ordinario di Informatica dell'Università "La Sapienza" di Roma.
- **Paolo Valente**, Direttore INFN di Roma e Segretario CoPER.
- **Michele Mazzola,** Dirigente MUR, Direzione generale dell'internazionalizzazione e della comunicazione.
- **Melissa Valentino,** Dirigente MUR – Direzione generale della ricerca.
- **Anna Zeppieri**, Dirigente applicato presso l'Ufficio del Consigliere Diplomatico del MUR.

# Crono-programma



Aprile 2024 - Missione in USA Dipartimento di Stato USA / MUR

Maggio 2024 Raccomandazione del Consiglio dell'Unione Europea relativa al rafforzamento della sicurezza della ricerca

Luglio 2024 - Riunione Ministeriale G7 Scienza e Tecnologia

Settembre 2024 Erogazione questionario

Ottobre 2024 Workshop a Genova e a Roma

Dicembre 2024 Conferenza nazionale e evento G7 a Bari

2025 Avvio sperimentazione


Sperimentazione su base volontaria con: un'università, un ente di ricerca e un IRCCS

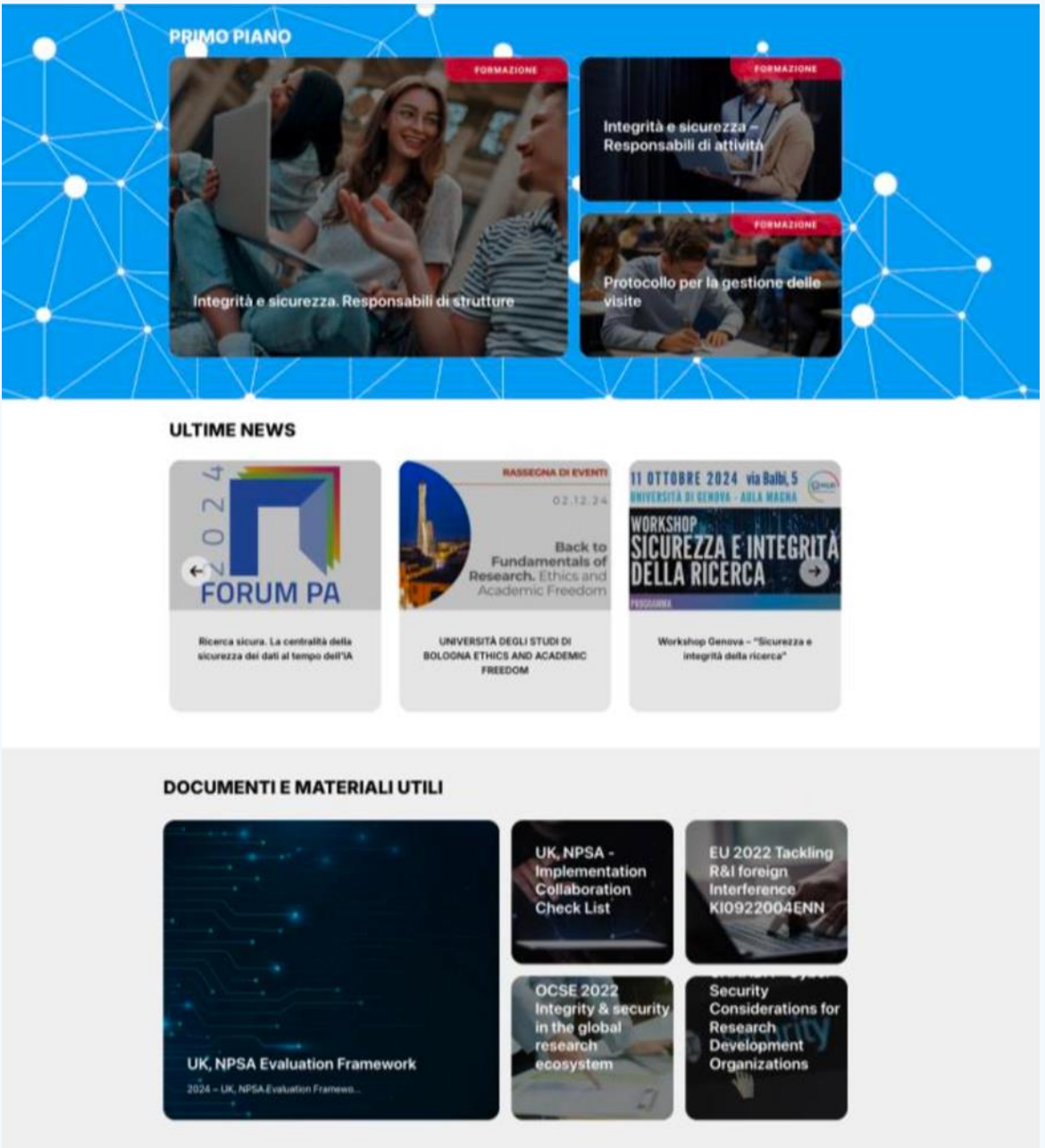
## **Input**:

- Normativa europea, in particolare Raccomandazione 23.5.2024 sulla Research Security e Direttiva sui **settori tecnologici critici**
- Direttiva e normativa nazionale su **NIS-2**
- ACN, per la parte di cybersicurezza
- Materiali **SIGRE** [G7 group on Security and Integrity of the Global Research Ecosystem] e dalla Virtual Academy [rappresentante italiano prof. Fulvio Esposito]
- Materiali di diversi **like-minded countries**
- **CRUI**: tavolo CRUI–Enti di ricerca su «Etica nella Ricerca» [coord. prof. Francesco Priolo]
- Consulta dei Presidenti degli enti di ricerca [**CoPER**]

## **Output**: proposta di «modello nazionale»:

- Materiale informativo e **formativo** per aumentare la consapevolezza della comunità scientifica, tramite un **sito web** dedicato anche a raccogliere materiale utile
- Uno **strumento di autovalutazione** di possibili criticità
- **Raccomandazioni** e linee guida per la mitigazione del rischio come:
  - Protocollo per l'accesso alle infrastrutture; protocollo per i viaggi; misure di cybersecurity; analisi dei rischi per collaborazioni e finanziamenti esterni; beni e tecnologie dual use
- Proposta di un **supporto** a livello di **istituzione** : referente per la sicurezza e integrità
- Proposta di un **livello nazionale**, di coordinamento e supporto per i referenti locali e di raccordo con le istituzioni rilevanti [ministeri vigilanti e agenzie]

# Struttura proposta per il sito Web




**www.sicurezzaricerca.mur.gov.it**

**Struttura del Sito**

**Area Riservata**

- Accesso Basato su SPID/LoginMUR
- Materiali Specifici
- Compilazione questionario per la valutazione dei rischi
- Invio Informazioni

**Considerazioni Tecniche**

- Sicurezza
- Scalabilità
- Analitiche

# Schema proposto

1

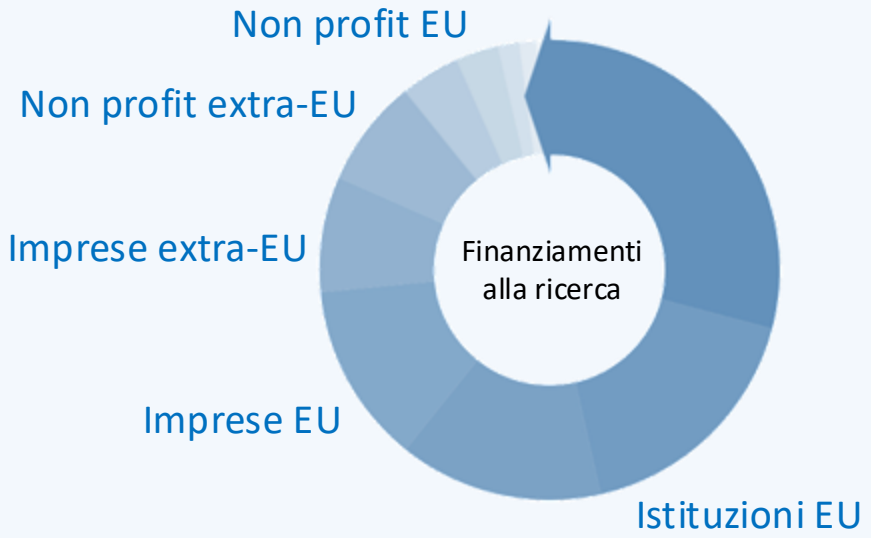
Per **individuare** possibili rischi per la sicurezza della ricerca si parte da alcune **domande di base**:

- Sono previste **collaborazioni esterne** ?
- Sono previsti **finanziamenti esterni** ?

## *Che cosa si intende con ESTERNI?*

- **Istituzioni di ricerca non EU**
- [escluse quelle regolate da **trattati**, come le agenzie ONU, CERN, ecc.]
- **Soggetti privati** come banche, industrie, imprese, che non sono **prevalentemente** impegnati in ricerca [escluse fondazioni e consorzi di ricerca]

Definizione che può essere **dinamica**, a seconda della situazione geopolitica e delle direttive governative



# Schema proposto

1

Per **individuare** possibili rischi per la sicurezza della ricerca si parte da alcune **domande di base**:

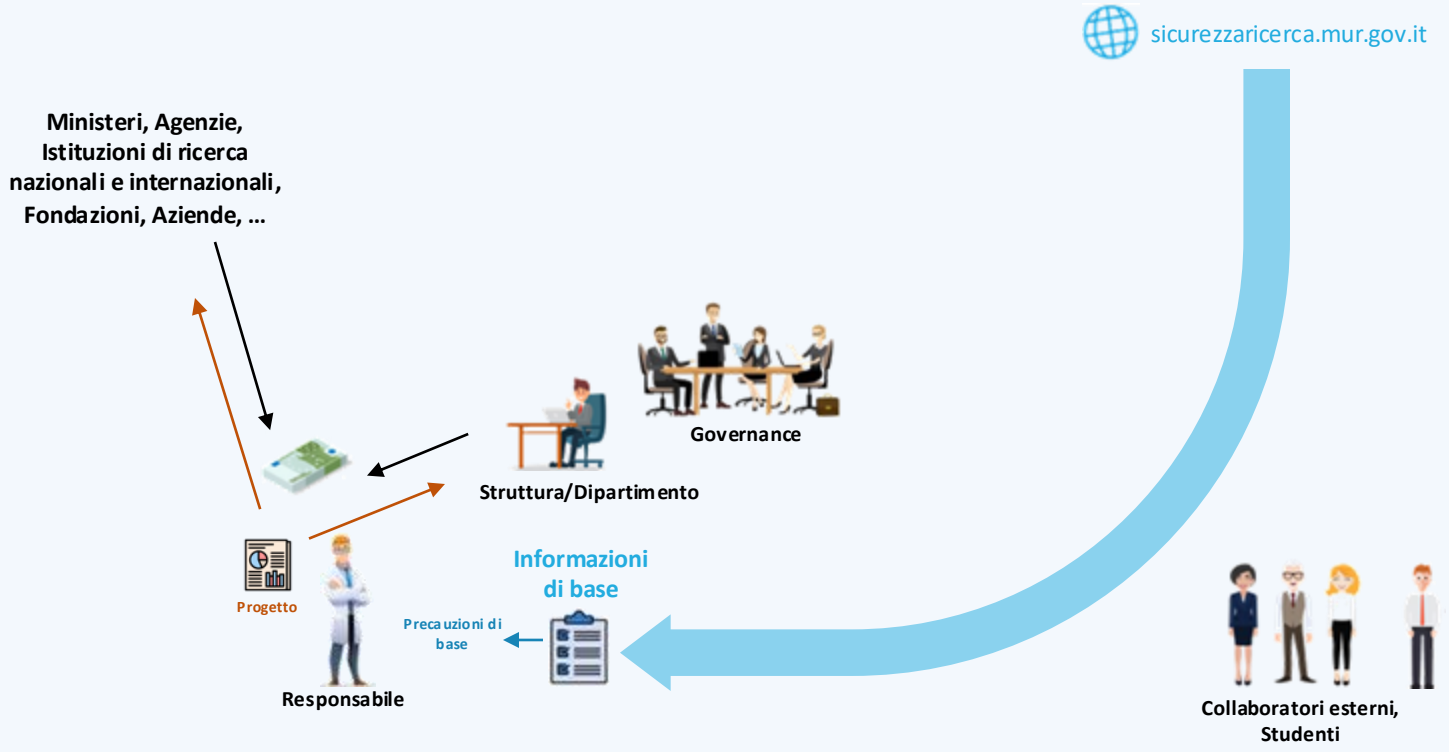
- Sono previste **collaborazioni esterne** ?
- Sono previsti **finanziamenti esterni** ?

Se **non ci sono** collaborazioni **né** finanziamenti **ESTERNI** si procede, ricordando le **precauzioni di base** e la normativa di riferimento

OK

Se ci sono collaboratori **oppure** fondi **ESTERNI** si passa a un'analisi dei rischi specifici tramite una **griglia di valutazione**

2



# Schema proposto

2

Il Responsabile di attività compila una specifica **griglia di valutazione** [online] con il supporto, ove necessario, di un **Referente** per la sicurezza e integrità della ricerca

Il **Referente** SIR **dialoga** con il Responsabile di attività e con la Governance dell'Istituzione e – partendo dai **risultati della griglia di valutazione** e di un'ulteriore analisi del progetto – fornisce **ulteriori linee di mitigazione**

OK

Per **livelli più alti** di rischio o in casi particolari può **richiedere** il <u>supporto</u> del **livello nazionale**

sicurezzaricerca.mur.gov.it

**Referente per la Sicurezza e Integrità della Ricerca**

A livello di singola Istituzione [o più Istituzioni consorziate], **esamina i progetti** con indicatori di rischio **sopra soglia** e:

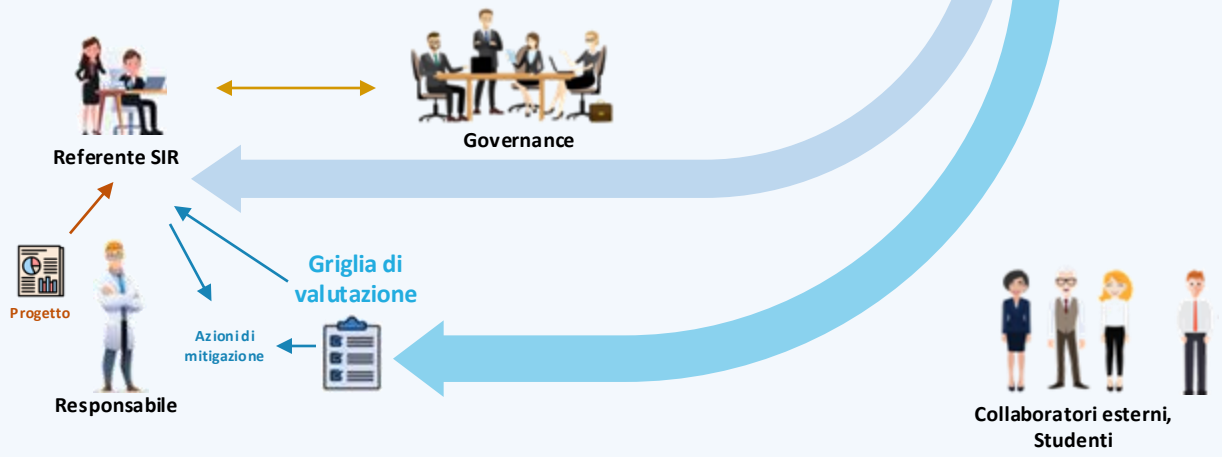
- Fornisce **azioni di mitigazione al responsabile di attività**;
- Fornisce **raccomandazioni alla governance** dell'Istituzione, anche su protocolli per **visite** di ospiti o **viaggi** in paesi con profilo di **rischio alto**
- Si occupa della **formazione** a livello di Istituzione
- Contribuisce all'implementazione delle politiche di **cybersicurezza**
- Contribuisce al rispetto delle politiche su **dual use** ed **exports control**

**Responsabile di attività**

- Presenta il **progetto di attività** di ricerca all'istituzione ed eventualmente altre agenzie di finanziamento
- Produce una **autovalutazione dei rischi** con l'aiuto di una **griglia** a livello ministeriale

LIVELLO ISTITUZIONE

LIVELLO ATTIVITÀ



# Schema proposto

**Centro Nazionale** per la Sicurezza e Integrità della Ricerca

- Agisce da **raccordo con ministeri e agenzie rilevanti**
- Predispone e aggiorna: **raccomandazioni** e **linee guida, matrici di rischio**
- Suggerisce azioni di **mitigazione dei rischi**
- Riceve richieste e **fornisce supporto ai referenti SIR**, anche tramite altre istituzioni
- Fornisce **materiale formativo**
- Agisce da **coordinamento nazionale** dei referenti SIR
- Dialoga con il **Centro Europeo SIR**

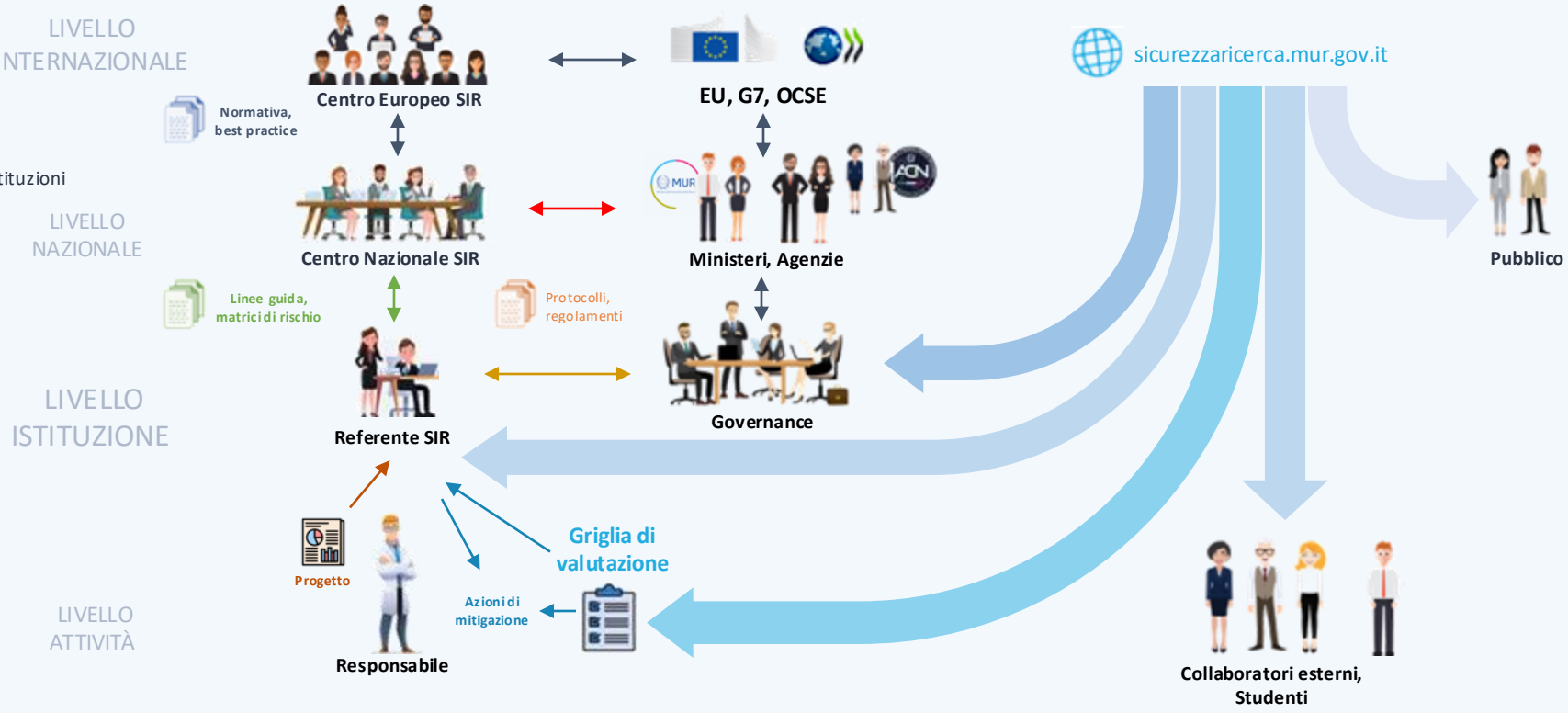
**Referente** per la Sicurezza e Integrità della Ricerca

A livello di singola Istituzione [o più Istituzioni consorziate], **esamina i progetti** con indicatori di rischio **sopra soglia** e:

- Fornisce **azioni di mitigazione al responsabile di attività**;
- Fornisce **raccomandazioni alla governance** dell'Istituzione, anche su protocolli per **visite** di ospiti o **viaggi** in paesi con profilo di **rischio alto**
- Si occupa della **formazione** a livello di Istituzione
- Contribuisce all'implementazione delle politiche di **cybersicurezza**
- Contribuisce al rispetto delle politiche su **dual use** ed **exports control**
- Riceve **linee guida e matrici di rischio** dal **Servizio Nazionale**
- Può richiedere **supporto** al **Servizio Nazionale**

**Responsabile di attività**

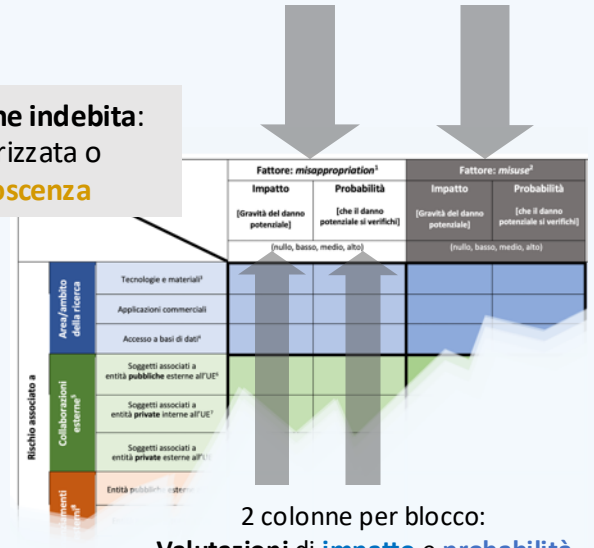
- Presenta il **progetto di attività** di ricerca all'istituzione ed eventualmente altre agenzie di finanziamento
- Produce una **autovalutazione dei rischi** con l'aiuto di una **griglia** a livello ministeriale



# Griglia di valutazione

2 blocchi verticali:
**tipologie di azione malevola**

**Appropriazione indebita**: cioè non autorizzata o illecita di **conoscenza**




2 colonne per blocco:
**Valutazioni** di **impatto** e **probabilità**

**Uso distorto** della **conoscenza** ovvero:
- Diverso da quello dichiarato originariamente
- Illecito o non autorizzato
- Tale da arrecare **danno** a cose o persone, di tipo materiale o immateriale (per es. lesione di diritti, discriminazione…)

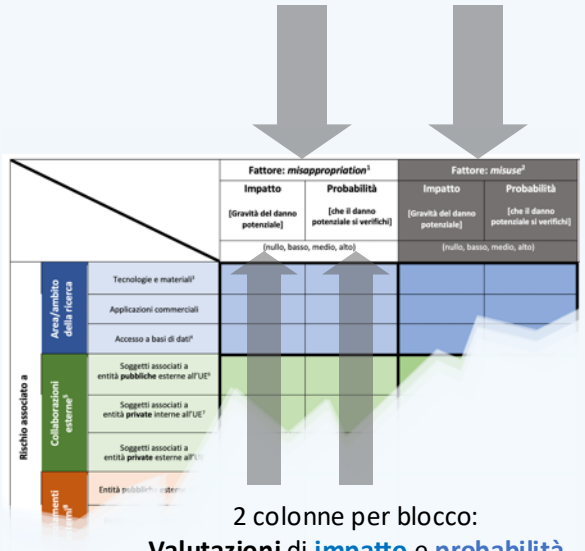
- Quale sarebbe l'entità del **danno** se l'azione malevola si verificasse?

- Con quale **probabilità** l'azione malevola e il danno conseguente si possono verificare?

**Conoscenza**:
quanto **disponibile** o **prodotto** nell'ambito dell'attività di ricerca in senso generale, ovvero:
- Dati
- Risultati e documenti
- Metodologie
- Tecnologie

# Griglia di valutazione

2 blocchi verticali:
**tipologie di azione malevola**




2 colonne per blocco:
**Valutazioni** di **impatto** e **probabilità**

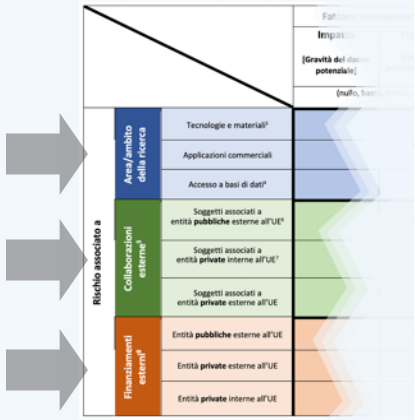
L'area disciplinare e in senso più lato la tematica e la tipologia dell'attività di ricerca (fondamentale, applicata, conto terzi, ecc.); il coinvolgimento o la disponibilità di asset (materiali e immateriali)

La collaborazione con partner non appartenenti a istituzioni EU

Fonti di finanziamento non provenienti da istituzioni EU

Area scientifica o tecnologie critiche o sensibili*

blocchi orizzontali:
3 **aree di rischio**

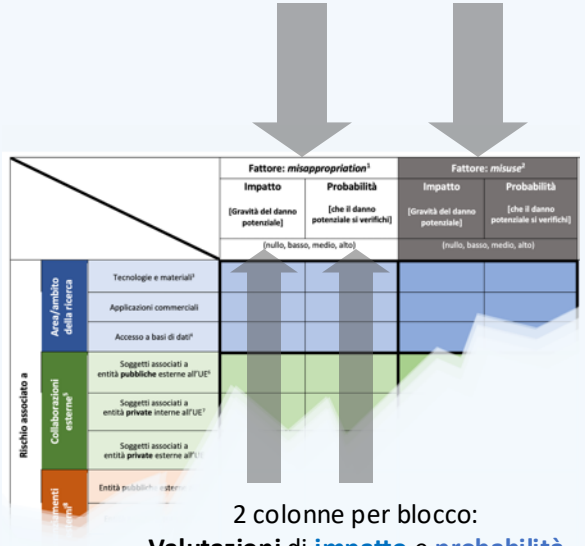



*"ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States", 3 ottobre 2023:*

| Area Tecnologica | Tecnologie |
|---|---|
| SEMICONDUTTORI | • Microelettronica, compresi i processori<br>• Tecnologie fotoniche (inclusi i laser ad alta energia)<br>• Chip ad alta frequenza<br>• Attrezzature per la produzione di semiconduttori avanzati |
| INTELLIGENZA ARTIFICIALE | • Calcolo ad alte prestazioni<br>• Cloud computing e edge computing<br>• Tecnologie di analisi dei dati<br>• Visione artificiale, elaborazione del linguaggio, riconoscimento degli oggetti |
| QUANTISTICA | • Calcolo quantistico<br>• Crittografia quantistica<br>• Comunicazioni quantistiche<br>• Sensori e radar quantistici |
| BIOTECNOLOGIE | • Tecniche di modifica genetica<br>• Nuove tecniche genomiche<br>• Gene-drive (propulsione genetica)<br>• Biologia sintetica |
| CONNETTIVITÀ, NAVIGAZIONE E DIGITALI | • Comunicazioni digitali e connettività sicure, come RAN e Open RAN (Radio Access Network) e 6G<br>• Tecnologie di sicurezza informatica, incluse la cyber-sorveglianza, sistemi di sicurezza e intrusioni, informatica forense digitale<br>• Internet delle cose e Realtà Virtuale<br>• Tecnologie di registro distribuito e identità digitale<br>• Tecnologie di guida, navigazione e controllo, incluse l'avionica e il posizionamento marino |
| SENSORI | • Sensori elettro-ottici, radar, chimici, biologici, di radiazioni e di rilevamento distribuito<br>• Magnetometri, gradiometri magnetici<br>• Sensori di campo elettrico subacquei<br>• Misuratori e gradiometri di gravità |
| TECNOLOGIE SPAZIALI E DI PROPULSIONE | • Tecnologie specifiche per lo spazio, che vanno dal livello di componente a quello di sistema<br>• Tecnologie per la sorveglianza spaziale e l'osservazione della Terra<br>• Posizionamento spaziale, navigazione e temporizzazione (PNT)<br>• Comunicazioni sicure, compresa la connettività in orbita terrestre bassa (LEO)<br>• Tecnologie di propulsione, incluse l'ipersonica e componenti per uso militare |
| ENERGIE | • Tecnologie di fusione nucleare, reattori e generazione di energia, tecnologie di conversione/arricchimento/riciclaggio radiologico<br>• Idrogeno e nuovi combustibili<br>• Tecnologie a emissioni zero, incluse le fotovoltaiche<br>• Reti intelligenti e stoccaggio dell'energia, batterie |
| ROBOTICA E SISTEMI AUTONOMI | • Droni e veicoli (aerei, terrestri, di superficie e subacquei)<br>• Robot e sistemi di precisione controllati da robot<br>• Esoscheletri<br>• Sistemi abilitati dall'intelligenza artificiale |
| MATERIALI, MANIFATTURA E RICICLAGGIO | • Tecnologie per nanomateriali, materiali intelligenti, materiali ceramici avanzati, materiali stealth, materiali progettati per essere sicuri e sostenibili<br>• Manifattura additiva<br>• Manifattura digitale di micro-precisione, e lavorazione/saldatura laser su piccola scala<br>• Tecnologie per l'estrazione, la lavorazione e il riciclaggio di materiali grezzi critici (inclusa l'estrazione idrometallurgica, la bio-lisciviazione, la filtrazione basata sulla nanotecnologia, la lavorazione elettrochimica e la massa nera) |

# Griglia di valutazione

2 blocchi verticali:
**tipologie di azione malevola**




2 colonne per blocco:
**Valutazioni** di **impatto** e **probabilità**

L'area disciplinare e in senso più lato la tematica e la tipologia dell'attività di ricerca (fondamentale, applicata, conto terzi, ecc.); il coinvolgimento o la disponibilità di asset (materiali e immateriali)

La collaborazione con partner non appartenenti a istituzioni EU

Fonti di finanziamento non provenienti da istituzioni EU

Area scientifica o tecnologie critiche o sensibili*

Potenziale sfruttamento commerciale non previsto

Potenziale accesso e uso non previsto/illecito di dati

blocchi orizzontali:
3 **aree di rischio**


3 righe ovvero **categorie** di rischio per ciascuna area

Istituzioni di ricerca extra-EU

Imprese

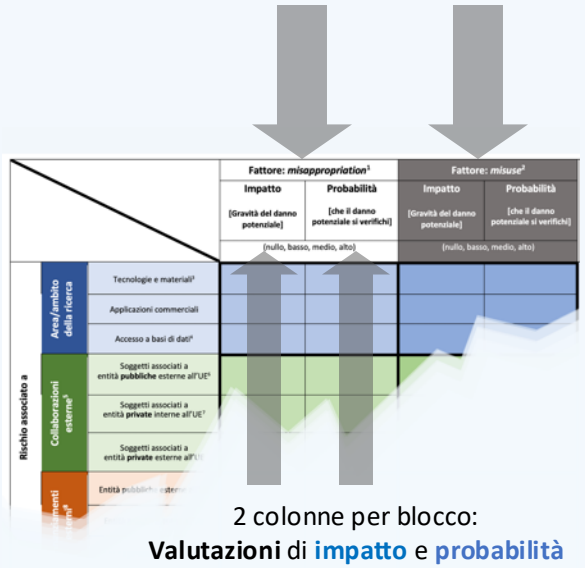
Nella EU

Extra-EU

** "ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States", 3 ottobre 2023:*

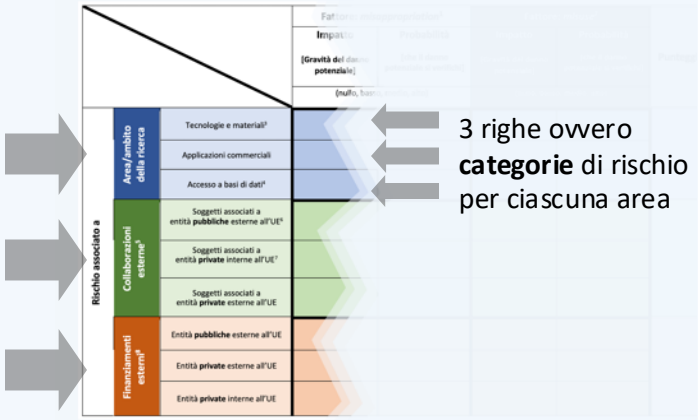
# Griglia di valutazione

2 blocchi verticali:
**tipologie di azione malevola**




2 colonne per blocco:
**Valutazioni** di **impatto** e **probabilità**

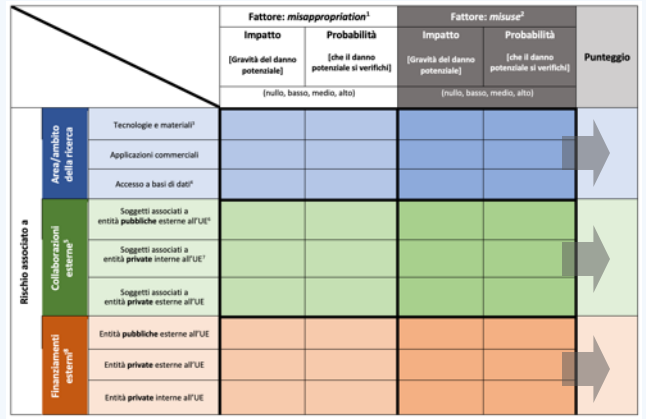
blocchi orizzontali:
3 **aree di rischio**




3 righe ovvero
**categorie** di rischio
per ciascuna area

Per **ogni campo** una **valutazione**

Le singole valutazioni (2× 2 ×3) si **combinano** a dare **3 score**, uno **ciascuna delle aree**



# Griglia di valutazione

A questa fase di autovalutazione arrivano attività che hanno o collaborazioni o finanziamenti esterni, e quindi possibilmente si possono verificare delle conseguenze non volute; si può graduare il **danno potenziale** semplicemente con dei livelli qualitativi: per esempio nullo, basso, medio o alto


Allo stesso modo per la **probabilità** che si verifichi una circostanza non voluta, e quindi un danno, si possono utilizzare gli stessi livelli

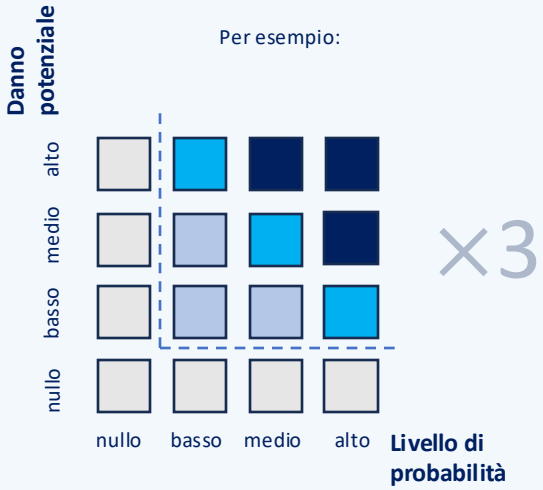
Per esempio:

| | | | Fattore: *misappropriation*[1] | | Fattore: *misuse*[2] | | Punteggio |
|---|---|---|---|---|---|---|---|
| | | | Impatto [Gravità del danno potenziale] | Probabilità [che il danno potenziale si verifichi] | Impatto [Gravità del danno potenziale] | Probabilità [che il danno potenziale si verifichi] | |
| | | | (nullo, basso, medio, alto) | | (nullo, basso, medio, alto) | | |
| Rischio associato a | Area/ambito della ricerca | Tecnologie e materiali[3] | basso | **medio** | basso | basso | **medio** |
| | | Applicazioni commerciali | **medio** | **medio** | basso | **medio** | |
| | | Accesso a basi di dati[4] | *nullo* | basso | *nullo* | basso | |
| | Collaborazioni esterne[5] | Soggetti associati a entità **pubbliche** esterne all'UE[6] | **medio** | basso | basso | basso | **medio** |
| | | Soggetti associati a entità **private** interne all'UE[7] | **medio** | basso | basso | basso | |
| | | Soggetti associati a entità **private** esterne all'UE | **medio** | basso | basso | basso | |
| | Finanziamenti esterni[8] | Entità **pubbliche** esterne all'UE | basso | *nullo* | basso | *nullo* | **basso** |
| | | Entità **private** esterne all'UE | basso | *nullo* | basso | *nullo* | |
| | | Entità **private** interne all'UE | basso | basso | basso | basso | |

# Griglia di valutazione

Per **ciascuna** delle tre aree della griglia si può ottenere uno **score** per il **rischio** combinando il **danno potenziale** con la **probabilità** che si verifichi

Per esempio:




Una **valutazione complessiva** del **rischio** può essere ottenuta **combinando gli score** per le tre aree: **tematica**, **collaborazioni** e **finanziamenti esterni**

Per esempio:

**Nota bene**: il dettaglio degli score e di come si combinano può essere meglio definito e adattato per es. sulla base di un periodo di test

# E l'Open Science?

La necessità di un **approccio equilibrato** è sottolineata nel documento "*Integrity and Security in the Global Research Ecosystem: an update on key policy actions and challenges*", un documento di lavoro prodotto dal *Global Science Forum* dell'**OCSE** (23/09/2024)

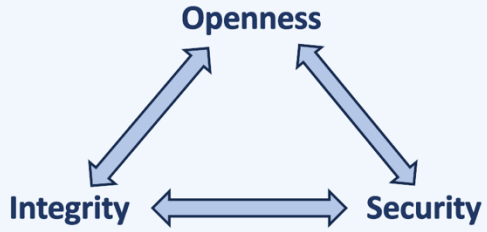
> *…**Measures in one country stimulate countermeasures elsewhere**, and in a changing world, it is important to make informed decisions on risks and threats and take considered and proportionate actions to mitigate and manage them.*
> *…**Naivety at one extreme and paranoia at the other extreme** are perhaps the most serious threats to the security and integrity of the global research ecosystem.*

**PERÒ**

G7 coglie la tensione tra le esigenze dell'approccio *Open Science* e quelle della *Security*

> *As our nations and communities start to recover from the pandemic and build resilience for future shocks, we will continue to work with our research and business communities to **remove barriers to the open and rapid sharing of knowledge, data and tools**, to the greatest extent possible, **recognising the importance of research security** in particular in cutting-edge fields*

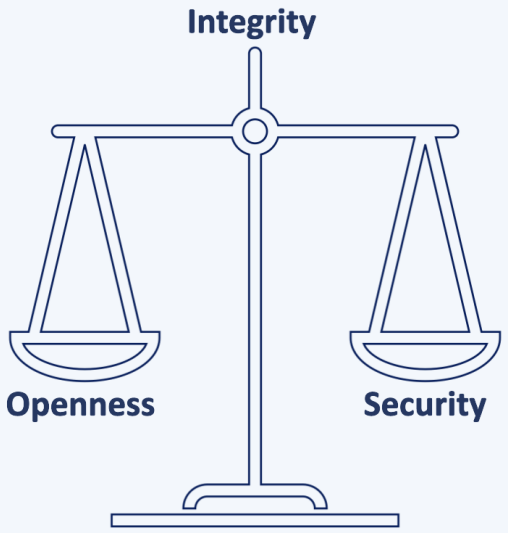
**Approccio Open Science valido più che mai… con un elemento di complessità in più**


FAIRS [Findable, Accessible, Interoperable, Reusable and Secure] DATA

…We commit to work together to uphold and protect the principles that underpin effective **international collaboration** that is **as open as possible and as secure as necessary**.

# E l'Open Science?




- In funzione delle circostanze, il fulcro della bilancia si può spostare in una direzione o nell'altra.
- Lo **scambio di idee ed esperienze** con colleghe e colleghi animati dagli stessi valori può essere d'aiuto a prendere decisioni equilibrate (*balanced approach*, *naivety and paranoia*…).
- G7-Scienza ha lanciato la *Virtual Academy on Research Security and Integrity*, ospitata sulla piattaforma SINAPSE della Commissione Europea "***to develop a shared understanding of research integrity and security*… …*allowing international collaboration to continue with confidence***". https://europa.eu/sinapse/sinapse
- I governi nazionali possono/devono fare la loro parte…

# Gruppo di lavoro INFN

- M. Pallavicini [GE], M. Citterio [Milano], P. Giannotti [LNF], M. Maggiora [Torino], P. Valente [Roma]

- Predisporre **proposte** al Direttivo per azioni INFN, in particolare per essere pronti a recepire le linee guida nella maniera più consona alle **specificità** della nostra comunità:
  - Federalismo: organizzazione sul territorio nelle Sezioni universitarie, nei laboratori e nei centri
  - Forte internazionalizzazione*

  *declinata sia come lavoro sistematico in laboratori internazionali [a partire dal CERN ma non solo], sia come apertura dei nostri laboratori nazionali alla comunità internazionale
  - Sinergia con le università/presenza degli incaricati di ricerca

- Coordinamento con le altre realtà/figure/problematiche già esistenti, per esempio:
  - TT e protezione della proprietà intellettuale
  - Open science, open data, valutazione
  - Cybersicurezza [CCR, Direttiva NIS-2, ecc.]
  - Protezione dati personali [DPO]

# Grazie per l'attenzione

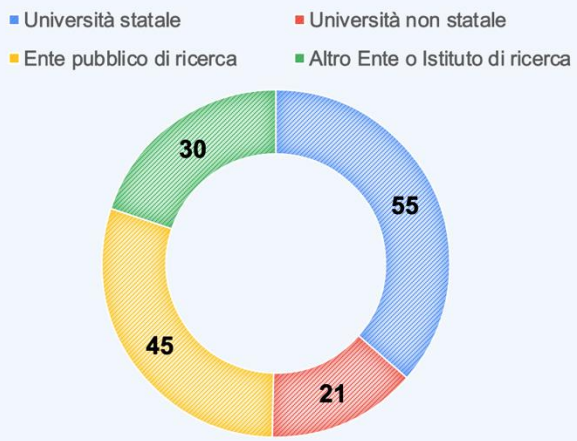
paolo.valente@roma1.infn.it

https://sicurezzaricerca.mur.gov.it
**[coming soon]**

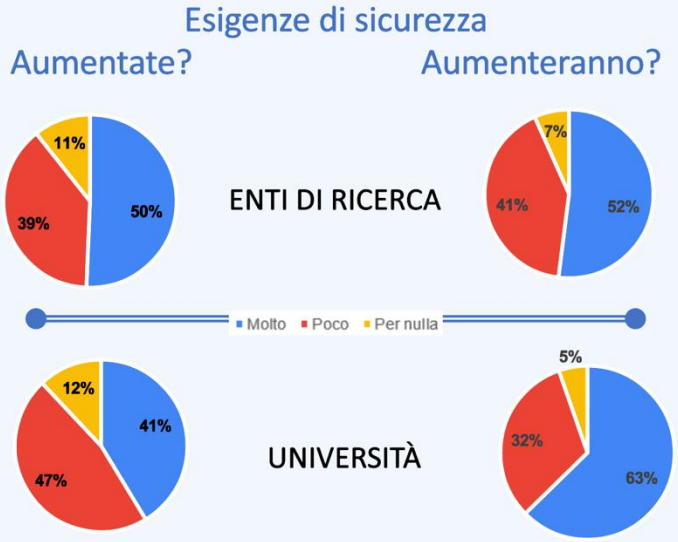
sicurezza.ricerca@mur.gov.it
**[attivo]**

# Questionario

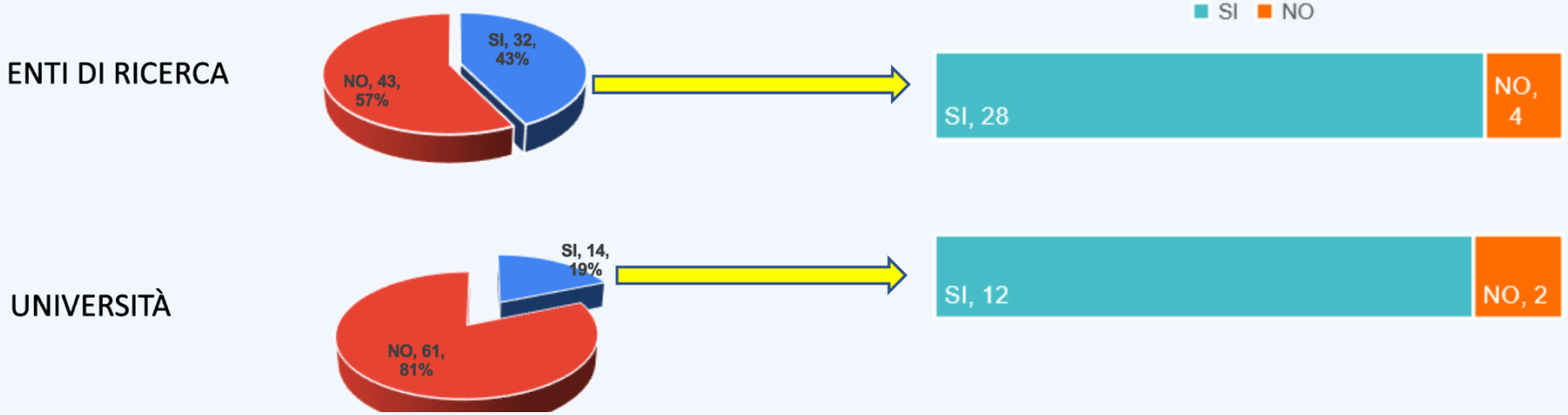
## Chi ha partecipato




## Esigenze di sicurezza




## Disponete di un programma/regolamento a tutela della sicurezza della ricerca?

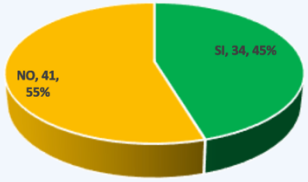


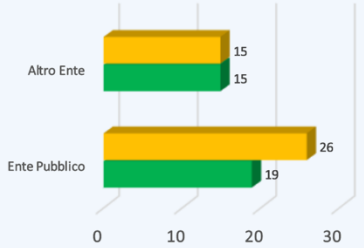

## Esiste una persona/struttura responsabile della supervisione del programma di sicurezza della ricerca?

# Questionario

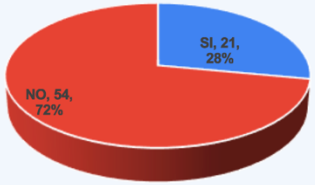
## Formate il personale pertinente sulla consapevolezza e l'identificazione dei rischi per la sicurezza della ricerca?

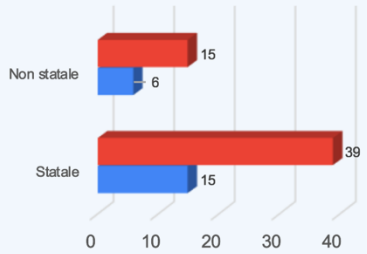
### ENTI DI RICERCA



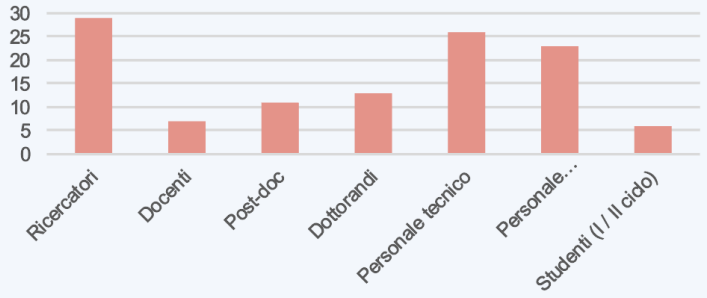

### UNIVERSITÀ



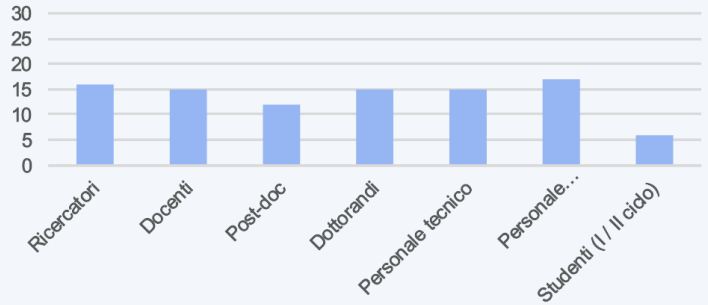




## A chi è rivolta la formazione sulla sicurezza della ricerca?

### Enti di Ricerca

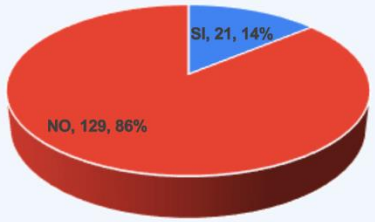



### Università

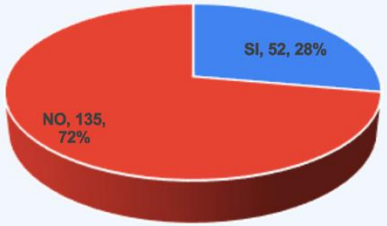


# Questionario

Avete procedure relative alla sicurezza della ricerca per il personale che viaggia per affari istituzionali, docenza, partecipazione a conferenze o per scopi di ricerca?




Vengono forniti briefing sulla sicurezza della ricerca ai partenti prima dei viaggi internazionali per garantire la consapevolezza dei potenziali rischi e delle relative misure di sicurezza?




Quanto sentite l'esigenza di un sistema nazionale che contribuisca ad assicurare la sicurezza della ricerca?