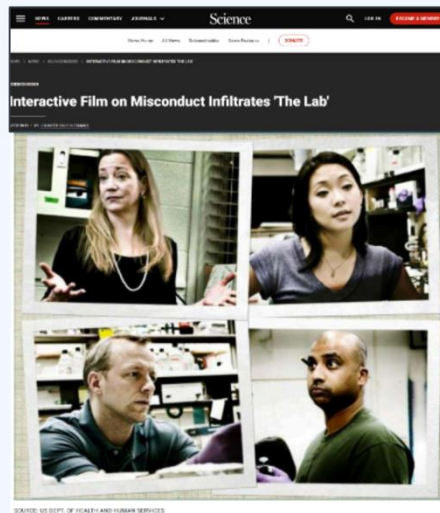


Verso un modello per la sicurezza e integrità della ricerca

Paolo Valente

Direttore Sezione INFN di Roma
Segretario CoPER

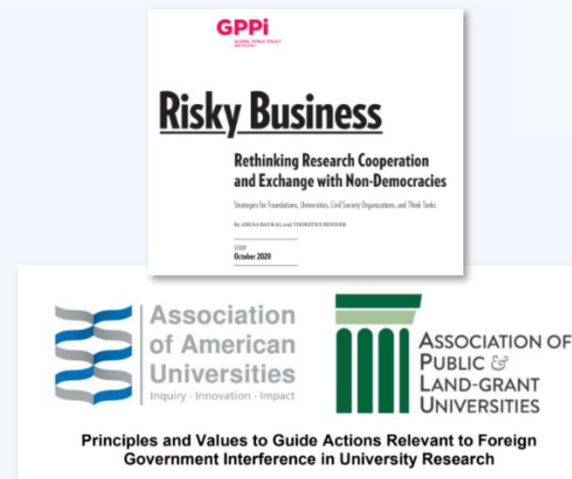




Il tema «*research security and integrity*» non è nuovo, ma ha acquisito maggiore visibilità e attenzione a partire dal 2020, declinato prevalentemente nella dimensione *foreign interference*

←
2011

→
2020



Cosa si intende per research security



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



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



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



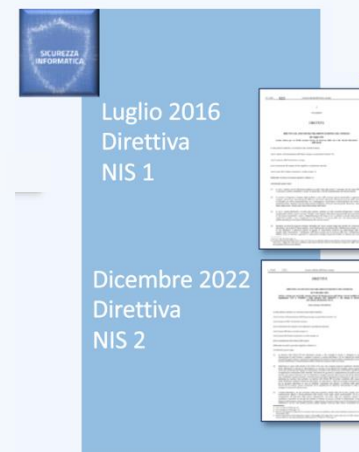
Il fenomeno della **Foreign Interference**, o interferenza straniera, si verifica quando le attività svolte da, o per conto di, un attore straniero a livello statale, sono **coercitive, segrete, ingannevoli o corruttive** e sono **contrarie alla sovranità, ai valori e agli interessi** dell'Unione Europea.

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
informaticaLuglio 2016
Direttiva
NIS 1Dicembre 2022
Direttiva
NIS 2

Un capitolo a sé:
la cybersicurezza

Il percorso della UE



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.



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:

Trasferimento indesiderato
di conoscenze e tecnologie critiche

a)

Ingerenze malevole
che possono sfociare nella strumentalizzazione

b)

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

c)

Europa

- Sostenere l'attuazione della Raccomandazione
- 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

Stati Membri

- Realizzare azioni strategiche per rafforzare la sicurezza della ricerca
- Rafforzare le conoscenze, attraverso l'analisi del panorama delle minacce, compresa cibersicurezza
- Creare una struttura di supporto ("research security advisory hub")

Organismi di ricerca

- i progetti di ricerca selezionati per il finanziamento siano sottoposti a un'analisi dei rischi proporzionata
- Introdurre procedure interne di gestione del rischio e garantire che i MoU siano validi dal punto di vista della sicurezza della ricerca

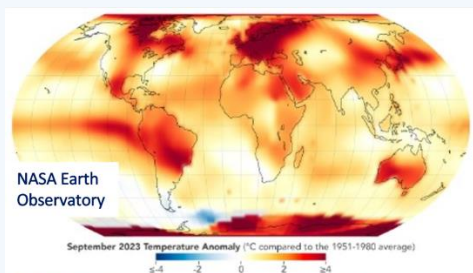
Soggetti finanziatori

- Integrare la sicurezza della ricerca nel processo di funding application
- Prendere in considerazione le salvaguardie previste dall'UE Horizon Europe
- Assicurarsi che le partnership (es. MoU) siano validi dal punto di vista della sicurezza della ricerca

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...*

Come affrontare il problema?



Il cambiamento climatico e le sue disastrose conseguenze

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

Le pandemie e la diffusione della resistenza agli antimicrobici



- **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**.

2



- **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

Luglio 2024 - Riunione
Ministeriale G7
Scienza e Tecnologia

Ottobre 2024
Workshop a Genova e
a Roma

2025 Avvio
sperimentazione

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

Settembre 2024
Erogazione
questionario

Dicembre 2024
Conferenza nazionale
e evento G7 a Bari

9 OTTOBRE 2024 p.^{le} Aldo Moro 7
SALA CONVEGNI CNR



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»:

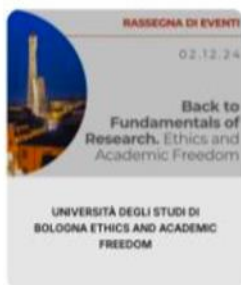
- Materiale informativo e **formativo** per aumentare la consapevolezza della comunità scientifica, tramite un **sito web** dedicato anche a raccogliere materiale utile
- Uno **strumento di autovalutazione** di possibili criticità
- **Raccomandazioni** e linee guida per la mitigazione del rischio come:
 - 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]



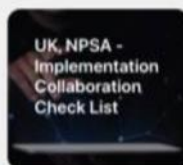
Struttura proposta per il sito Web



ULTIME NEWS



DOCUMENTI E MATERIALI UTILI



www.sicurezza.ricerca.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

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** ?

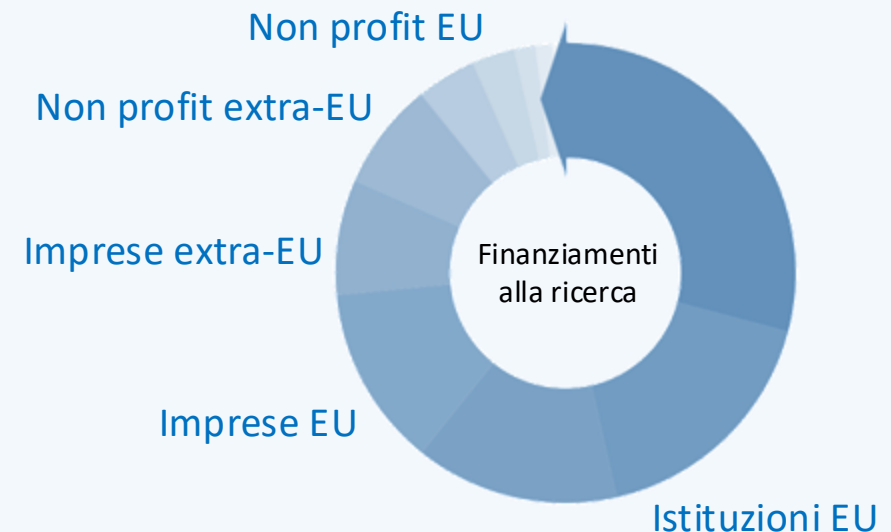
Che cosa si intende con ESTERNI?

- **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



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

Ministeri, Agenzie,
Istituzioni di ricerca
nazionali e internazionali,
Fondazioni, Aziende, ...

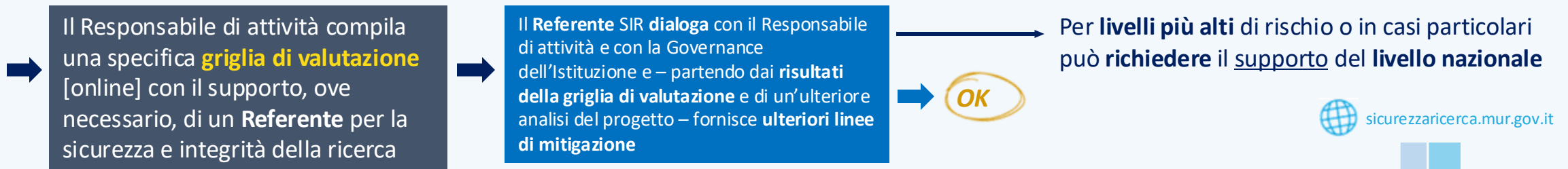


 sicurezza.mur.gov.it


Collaboratori esterni,
Studenti

Schema proposto

2



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:

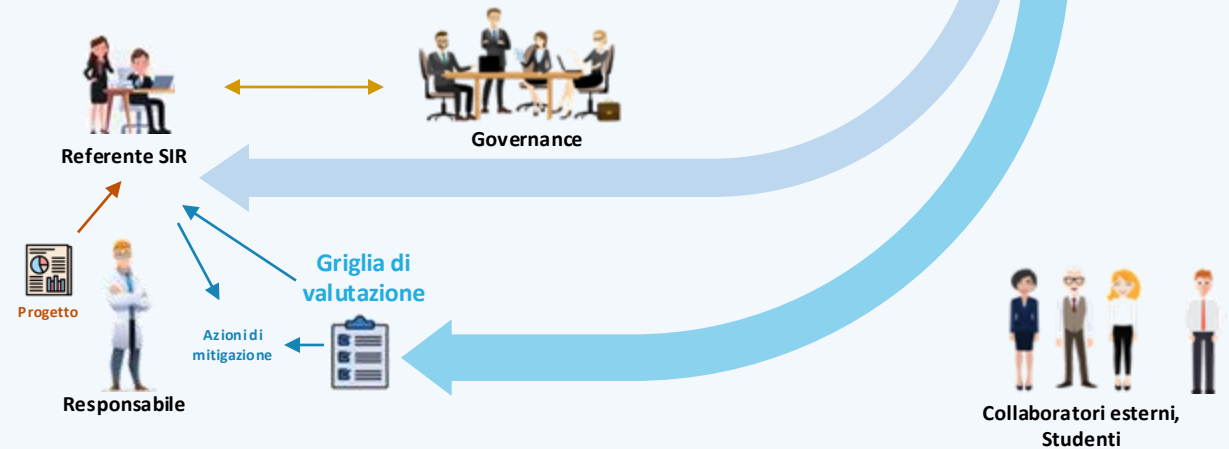
- Fornisce **azioni di mitigazione** al responsabile di attività;
- Fornisce **raccomandazioni alla governance** dell'Istituzione, anche su protocolli per **visite** di ospiti o **viaggi** in paesi con profilo di **rischio alto**
- Si occupa della **formazione** a livello di Istituzione
- Contribuisce 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

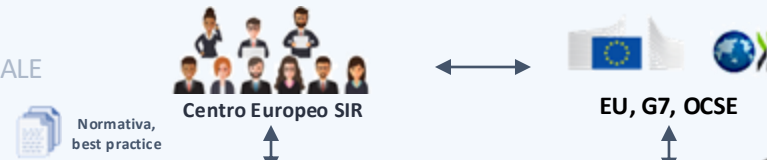
A livello di singola Istituzione [o più Istituzioni consorziate], **esamina i progetti** con indicatori di rischio **sopra soglia** e:

- 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

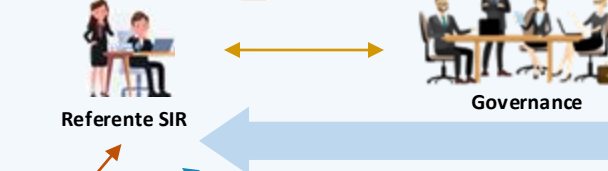
LIVELLO INTERNAZIONALE



LIVELLO NAZIONALE



LIVELLO ISTITUZIONE



LIVELLO ATTIVITÀ



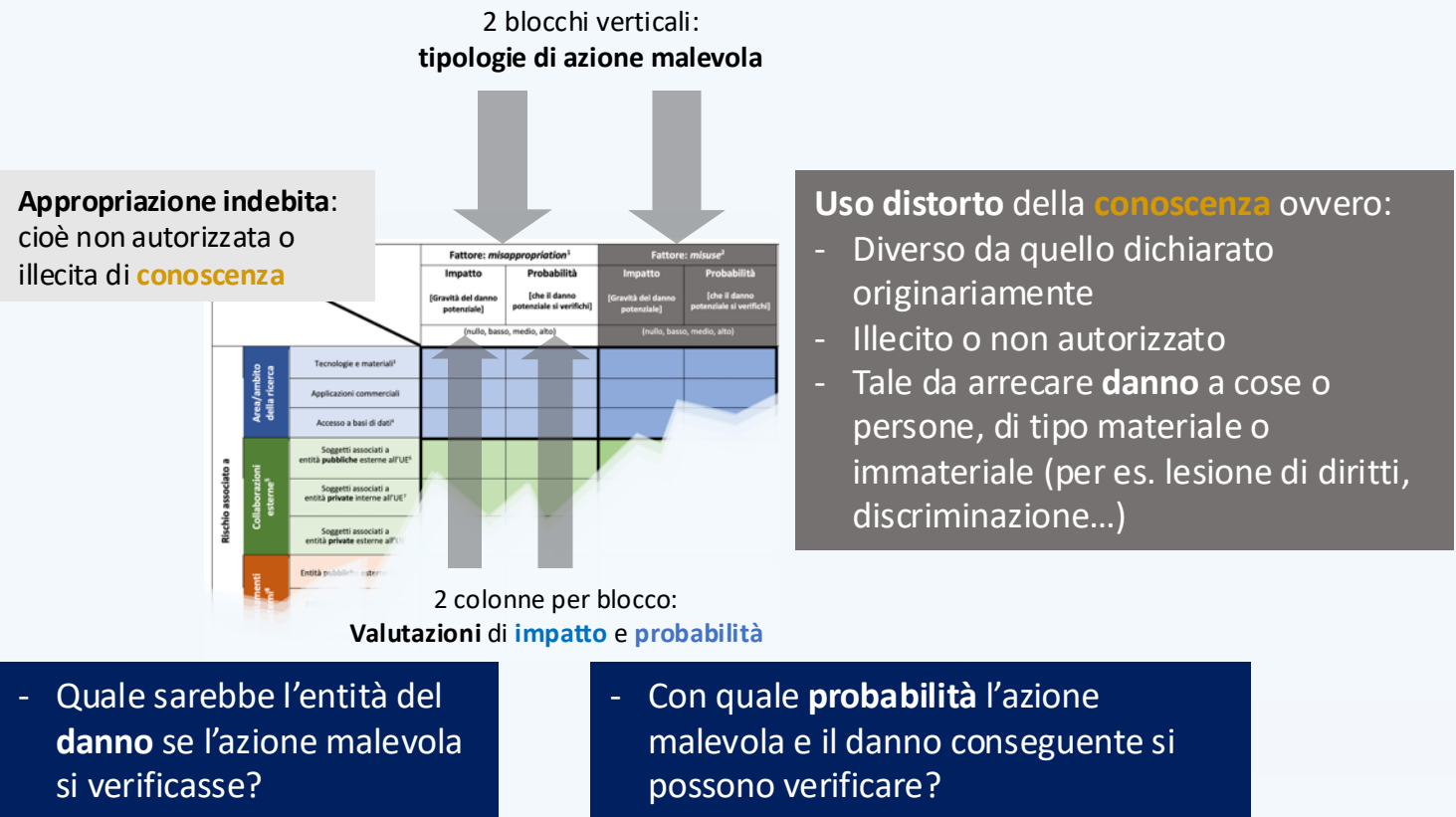
Griglia di valutazione

sicurezza.mur.gov.it

Pubblico

Collaboratori esterni,
Studenti

Griglia di valutazione



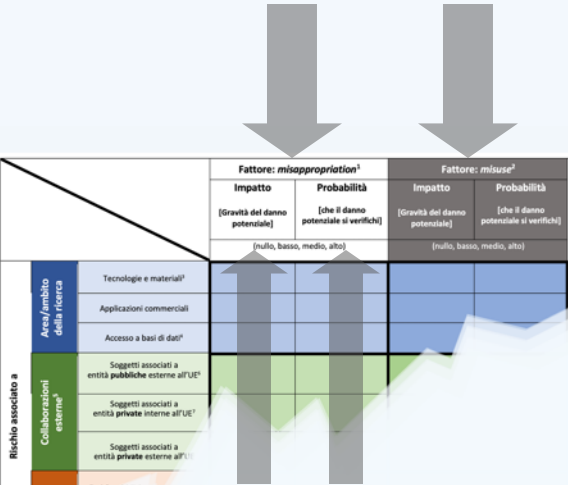
Conoscenza:

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**

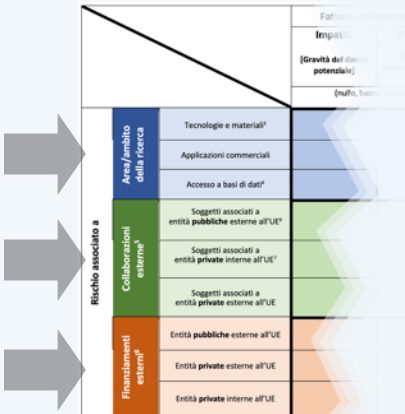
L'area disciplinare e in senso più lato la tematica e la tipologia dell'attività di ricerca (fondamentale, applicata, conto terzi, ecc.); il coinvolgimento o la disponibilità di asset (materiali e immateriali)

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 • Tecnologie fotoniche (inclusi i laser ad alta energia) • Chip ad alta frequenza • Attrezzature per la produzione di semiconduttori avanzati
INTELLIGENZA ARTIFICIALE	• Calcolo ad alte prestazioni • Cloud computing e edge computing • Tecnologie di analisi dei dati • Visione artificiale, elaborazione del linguaggio, riconoscimento degli oggetti
QUANTISTICA	• Calcolo quantistico • Crittografia quantistica • Comunicazioni quantistiche • Sensori e radar quantistici
BIOTECNOLOGIE	• Tecniche di modifica genetica • Nuove tecniche genomiche • Gene-drive (propulsione genetica) • Biologia sintetica
CONNETTIVITÀ, NAVIGAZIONE E DIGITALI	• Comunicazioni digitali e connettività sicure, come RAN e Open RAN (Radio Access Network) e 5G • Tecnologie di sicurezza informatica, incluse la cyber-sorveglianza, sistemi di sicurezza e intrusioni, informatica forense digitale • Internet delle cose e Realtà Virtuale • Tecnologie di registro distribuito e identità digitale • 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 • Magnetometri, gradiometri magnetici • Sensori di campo elettrico subacquei • 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 • Tecnologie per la sorveglianza spaziale e l'osservazione della Terra • Posizionamento spaziale, navigazione e temporizzazione (PNT) • Comunicazioni sicure, compresa la connettività in orbita terrestre bassa (LEO) • 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 • Idrogeno e nuovi combustibili • Tecnologie a emissioni zero, incluse le fotovoltaiche • Reti intelligenti e stoccaggio dell'energia, batterie
ROBOTICA E SISTEMI AUTONOMI	• Droni e veicoli (aerei, terrestri, di superficie e subacquei) • Robot e sistemi di precisione controllati da robot • Esoscheletri
MATERIALI, MANIFATTURA E RICICLAGGIO	• Sistemi abilitati dall'intelligenza artificiale • Tecnologie per nanomateriali, materiali intelligenti, materiali ceramici avanzati, materiali stealth, materiali progettati per essere sicuri e sostenibili • Manifattura additiva • Manifattura digitale di micro-precisione, e lavorazione/saldatura laser su piccola scala • Tecnologie per l'estrazione, la lavorazione e il riciclaggio di materiali preziosi critici (inclusa l'estrazione idrometallurgica, la bio-riciclaggio, la filtrazione basata sulla nanotecnologia, la lavorazione elettromeccanica e la massa nera)

Griglia di valutazione

2 blocchi verticali:
tipologie di azione malevola

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

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

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

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

		Fattore: <i>misappropriation</i> ¹		Fattore: <i>misuse</i> ²	
		Impatto	Probabilità	Impatto	Probabilità
		[Gravità del danno potenziale]	[che il danno potenziale si verifichi]	[Gravità del danno potenziale]	[che il danno potenziale si verifichi]
Rischio associato a	Area/ambito della ricerca	(nulla, basso, medio, alto)		(nulla, basso, medio, alto)	
		Tecnologie e materiali ³			
		Applicazioni commerciali			
	Collaborazioni esterne ⁴	Accesso a basi di dati ⁵			
		Soggetti associati a entità pubbliche esterne all'UE ⁶			
		Soggetti associati a entità private interne all'UE ⁷			
	Finanziamenti esterni ⁸	Soggetti associati a entità private esterne all'UE ⁹			
		Entità pubbliche esterne all'UE			
		Entità private esterne all'UE			
		Entità private interne all'UE			

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

blocchi orizzontali:
3 aree di rischio

		Fattore: <i>misappropriation</i> ¹		Fattore: <i>misuse</i> ²		Punteggio	
		Impatto	Probabilità	Impatto	Probabilità		
		[Gravità del danno potenziale]	[che il danno potenziale si verifichi]	[Gravità del danno potenziale]	[che il danno potenziale si verifichi]		
Rischio associato a	Area/ambito della ricerca	(nulla, basso, medio, alto)		(nulla, basso, medio, alto)			
		Tecnologie e materiali ³					
		Applicazioni commerciali					
	Collaborazioni esterne ⁴	Accesso a basi di dati ⁵					
		Soggetti associati a entità pubbliche esterne all'UE ⁶					
		Soggetti associati a entità private interne all'UE ⁷					
	Finanziamenti esterni ⁸	Soggetti associati a entità private esterne all'UE ⁹					
		Entità pubbliche esterne all'UE					
		Entità private esterne all'UE					
		Entità private interne all'UE					

3 righe owerò 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

		Fattore: <i>misappropriation</i> ¹		Fattore: <i>misuse</i> ²		Punteggio
		Impatto	Probabilità	Impatto	Probabilità	
		[Gravità del danno potenziale]	[che il danno potenziale si verifichi]	[Gravità del danno potenziale]	[che il danno potenziale si verifichi]	
Rischio associato a	Area/ambito della ricerca	(nulla, basso, medio, alto)		(nulla, basso, medio, alto)		
		Tecnologie e materiali ³				
		Applicazioni commerciali				
	Collaborazioni esterne ⁴	Accesso a basi di dati ⁵				
		Soggetti associati a entità pubbliche esterne all'UE ⁶				
		Soggetti associati a entità private interne all'UE ⁷				
	Finanziamenti esterni ⁸	Soggetti associati a entità private esterne all'UE ⁹				
		Entità pubbliche esterne all'UE				
		Entità private esterne all'UE				
		Entità private interne all'UE				

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**

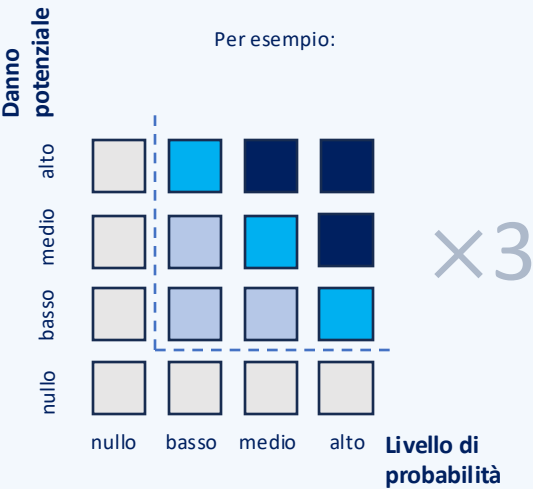
Per esempio:

			Fattore: <i>misappropriation</i> ¹		Fattore: <i>misuse</i> ²		Punteggio
			Impatto	Probabilità	Impatto	Probabilità	
			[Gravità del danno potenziale]	[che il danno potenziale si verifichi]	[Gravità del danno potenziale]	[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



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



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



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)

E l’Open Science?

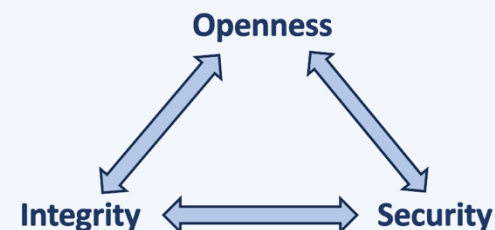
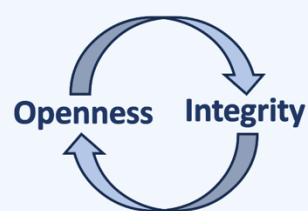
...Measures in one country stimulate countermeasures elsewhere, and in a changing world, it is important to make informed decisions on risks and threats and take considered and proportionate actions to mitigate and manage them.
...Naivety at one extreme and paranoia at the other extreme are perhaps the 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*

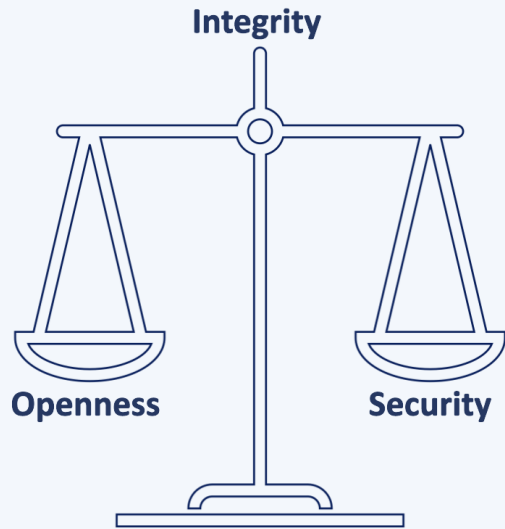
Approccio Open Science valido più che mai... con un elemento di complessità in più



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...

Grazie per l'attenzione



paolo.valente@roma1.infn.it

<https://sicurezzaricerca.mur.gov.it>

[coming soon]

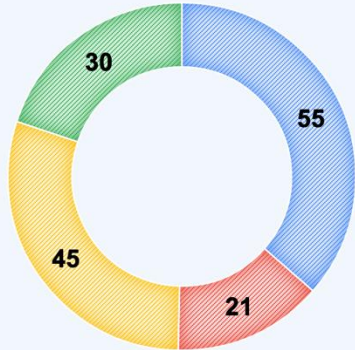
sicurezza.ricerca@mur.gov.it

[attivo]

Questionario

Chi ha partecipato

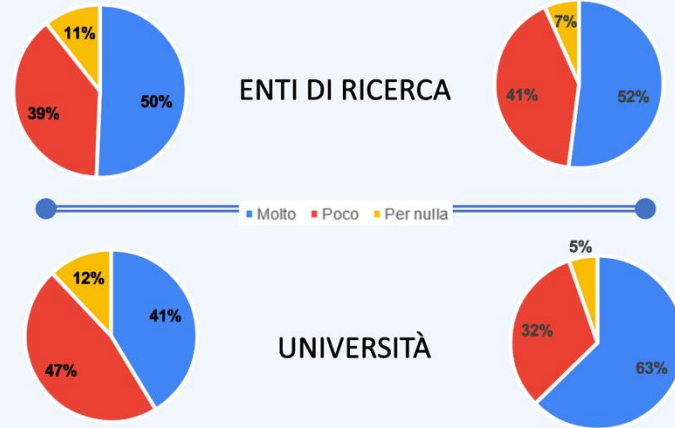
■ Università statale ■ Università non statale
■ Ente pubblico di ricerca ■ Altro Ente o Istituto di ricerca



Esigenze di sicurezza

Aumentate?

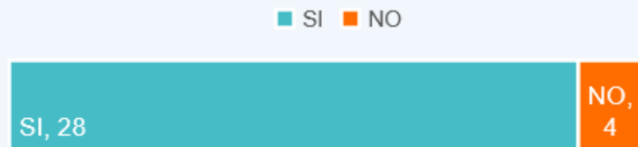
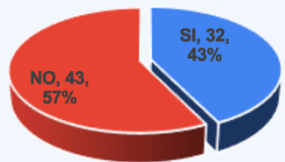
Aumenteranno?



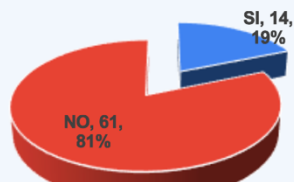
Disponete di un programma/regolamento a tutela della sicurezza della ricerca?

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

ENTI DI RICERCA



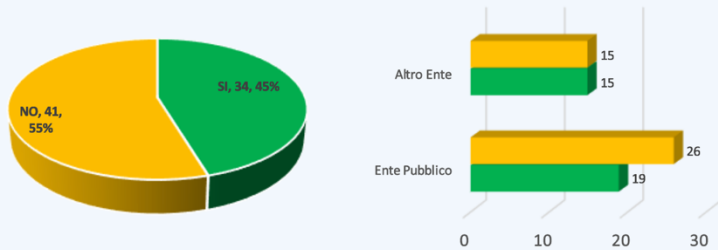
UNIVERSITÀ



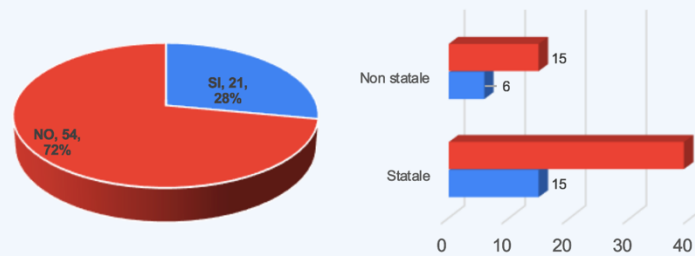
Questionario

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

ENTI DI RICERCA

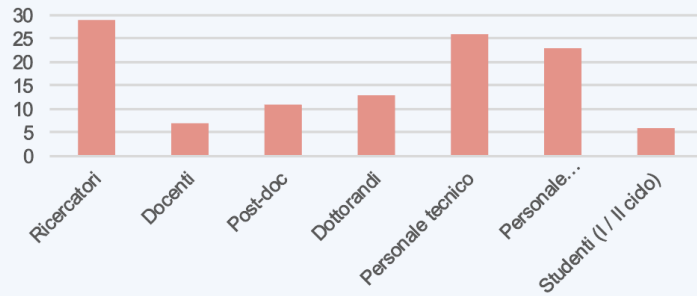


UNIVERSITÀ

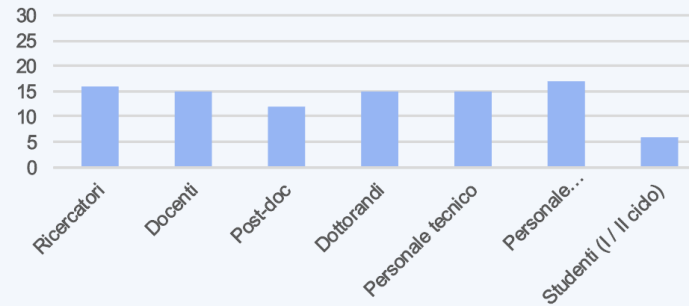


A chi è rivolta la formazione sulla sicurezza della ricerca?

Enti di Ricerca

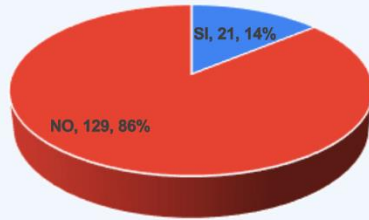


Università

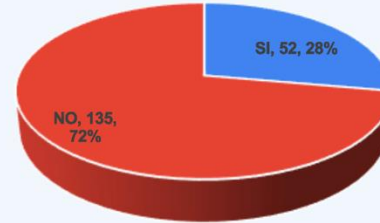


Questionario

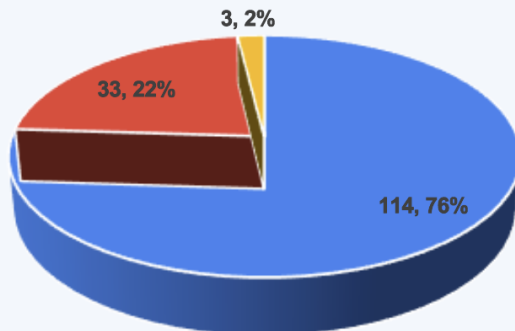
Avete procedure relative alla sicurezza della ricerca per il personale che viaggia per affari istituzionali, docenza, partecipazione a conferenze o per scopi di ricerca?



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?



■ Molto ■ Poco ■ Per nulla

Enti di Ricerca



Università

