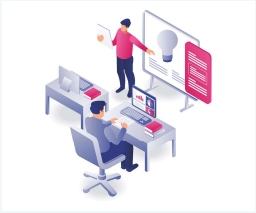

CONFERENZA NAZIONALE
SICUREZZA E INTEGRITÀ DELLA RICERCA
Moduli Formativi
Fabrizio Barberis, Delegato del Rettore Unige per la sicurezza della ricerca e dual use

L'attività di ricerca è intrinsecamente aperta ed internazionalizzata

Il progetto viene continuamente discusso nel team di lavoro

Viene illustrato nei vari appuntamenti intermedi fra i differenti enti partecipanti al progetto



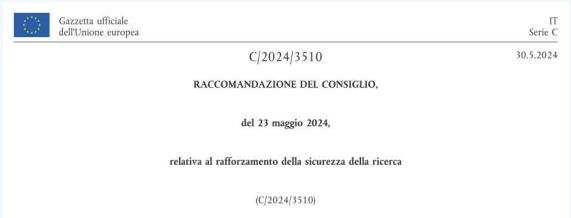
Viene infine presentato, nei risultati e nei possibili sviluppi, alla comunità scientifica ove possiamo reclutare nuove risorse e ulteriori spunti

sicurezzaricerca.mur.gov.it

In tutti questi passaggi possono verificarsi perdite di informazione o trafugamenti di dati sensibili

Come mantenere la necessaria mobilità dei ricercatori e delle idee senza incorrere in problemi inerenti alla security della ricerca?

La Sicurezza della ricerca è un punto seguito con attenzione in tutto il mondo, su questo la Commissione Europea ha presentato indicazioni così come è accaduto in USA, UK, Canada, NZ e nelle altre nazioni leader nella ricerca e trasferimento tecnologico



Gazzetta ufficiale dell'Unione europea

IT
Serie C

C/2024/3510

30.5.2024

RACCOMANDAZIONE DEL CONSIGLIO,

del 23 maggio 2024,

relativa al rafforzamento della sicurezza della ricerca

(C/2024/3510)

EU

sicurezzaricerca.mur.gov.it

USA

UK

CAN

La messa in atto di procedure per supportare la sicurezza della ricerca è strumento importante per la reputation degli istituti e mantenere il flusso di ricercatori nella comunità scientifica

Come supportare attivamente i Referenti di istituzioni, i PI, i ricercatori e gli studenti in scambio internazionale?

CONSAPEVOLEZZA
È importante trasmettere a ciascun attore della ricerca gli aspetti di security che lo riguardano direttamente

SPECIFICITÀ
Ogni ruolo ha una propria visione degli aspetti di security della ricerca ed è importante che siano fra loro allineati e sinergici per creare un sistema efficace

EFFICACIA
Occorre fornire una indicazione strutturata sulla importanza della security di modo che i vari ruoli possano cooperare in forma sinergica su scala nazionale

Moduli formativi

Basatati sulle best practices internazionali sono suddivisi su quattro livelli

- Responsabile di struttura
- Responsabile di attività
- Soggiorni all'estero per lavoro
- Gestione delle visite esterne

Modulo per il responsabile di struttura

sicurezzaricerca.mur.gov.it

Struttura/Dipartimento

Creare una cultura della Sicurezza e Integrità della Ricerca

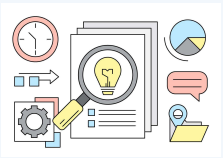
- Avere contezza dei vari aspetti della Sicurezza della Ricerca
- Valutare le esposizioni al rischio della propria struttura
- Individuare e nominare una o più persone come referenti per la struttura

Sinergia

- Creare e mantenere aggiornati protocolli interni atti a fluidificare la comunicazione puntando sui soli aspetti di sicurezza.
- Alcuni dei rischi non sono immediatamente percepibili dal Ricercatore: → il sito del MUR aggiorna costantemente le best practices più indicate

Governance

- Creare un dialogo continuo con i responsabili di attività
- Generare consapevolezza, applicando esempi e formazione continua
- Mantenere allineamento con le linee guida nazionali e con le indicazioni pubblicate sul sito del MUR



Efficacia

- Creare un sistema di semplice di segnalazione di possibili dubbi o problemi
- Definire un protocollo interno di valutazione di efficacia con analisi delle possibili difficoltà

Modulo per il responsabile di attività

Responsabile di Attività

- Costruire una relazione di fiducia
- Classificare e valutare la ricerca svolta
- Identificare i rischi anche in base al livello di sviluppo della attività
- Interagire con il responsabile della sicurezza della ricerca e ragionare anche sul modello di finanziamento seguito oltre che sulle possibili interazioni con soggetti ed enti esterni

- Seguire gli aggiornamenti MUR sulle tecnologie più esposte a possibili rischi di interessi indebiti
- Seguire lo sviluppo del progetto, dei partner presenti e delle loro effettive linee di ricerca nel progetto
- Confrontarsi periodicamente con il responsabile della sicurezza della ricerca

- Valutare il livello di attenzione agli aspetti della sicurezza della ricerca dei partner di progetto
- Applicare un metodo adeguato ai rischi individuati e bilanciato con le necessità della attività
- Informare e proteggere i propri ricercatori sia durante il lavoro in laboratorio che in tutte le altre occasioni di disseminazione o interazioni esterne

sicurezzaricerca.mur.gov.it

Settori di Ricerca Sensibili come da "ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States" del 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 6G • 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 • 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 • 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 grezzi critici (inclusa l'estrazione idrometallurgica, la bio-lisciviazione, la filtrazione basata sulla nanotecnologia, la lavorazione elettrochimica e la massa nera)

Regole di base per viaggi e soggiorni all'estero

sicurezzaricerca.mur.gov.it

Viaggi e soggiorni

Proteggere i valori della ricerca all'estero

La sicurezza e l'integrità della ricerca e dei ricercatori possono essere messe a repentaglio da attori potenzialmente ostili anche attraverso l'uso improprio o l'acquisizione illecita di informazioni secondo tre canali principali:

- ✓ Connessioni interpersonali
- ✓ Intrusione fisica
- ✓ Intrusione informatica.

Prima del viaggio

Processo di autovalutazione

- Si sta lavorando su tecnologie listate come «critiche» o di interesse nazionale?
- Si è in contatto con strutture, partner, persone con interessi scientifici in competizione con quanto si sta studiando?
- Se si è in dubbio: → **Contattare il responsabile della sicurezza**
- Applicare il principio del **«need to know»**

Durante il viaggio

- Evitare di esporre più del necessario
- Evitare di lasciare i dispositivi (computer, cell) non custoditi
- Ridurre il rischio evitando di portare con se' informazioni del tutto inutili per lo specifico progetto
- Usare connessioni preferibilmente in VPN
- Evitare di usare dispositivi USB ricevuti (congresso, persona non nota, etc.)

Dopo il viaggio

- Controllare eventuali compromissioni del materiale informatico
- Fare mente locale su episodi dubbi di conversazioni o situazioni con anomali interessi
- Se necessario fare un breve debriefing con il responsabile della sicurezza

Protocollo per la gestione delle visite

sicurezzaricerca.mur.gov.it

Protocollo Visite

Il **trasferimento indesiderato di conoscenze** può avvenire nell'ambito di progetti di ricerca pluriennali, in cui ricercatori afferenti a istituzioni straniere (compresi dottorandi) lavorano in Italia per **lunghi periodi** di tempo, o anche attraverso contatti di **breve durata** come partecipazione a conferenze o brevi visite di personale ricercatore ospite.

Creazione protocollo visite

caratteristiche dei luoghi oggetto della visita (attività svolte, presenza di infrastrutture critiche, accesso a informazioni sensibili, etc.) e della natura e dell'ambito di attività dell'istituzione di afferenza del visitatore (mondo accademico, aziende, governi).

Elementi fondamentali del Protocollo

- Valutare il livello di possibile rischio della visita:
  - Basso → prive di attività cliniche o laboratorio
  - Medio/Alto → con attività scientifica e produzione dati
- Predisporre la visita con i responsabili
- Informare il rappresentante della sicurezza
- Preregistrare i nomi della delegazione
- Valutare se distribuire un account all'ospite, e con quali limitazioni
- Non lasciare gli ospiti privi di accompagnamento
- Garantire che il protocollo sia facilmente reperibile sul sito della istituzione

- Luoghi
- Attività
- Motivi della visita

- Accordi scritti
- Informarsi su equivalenti policies di sicurezza degli ospiti
- Gestione oculata dei pass e limitazione dei loro periodi di attività
- Attenzione a interessi non allineati ai progetti o periodi di lavoro non consoni al progetto
- Valutare possibili variazioni di interessi o comparsa di possibili applicazioni commerciali non previste

Protocollo Visite

Il **trasferimento indesiderato di conoscenze** può avvenire nell'ambito di progetti di ricerca pluriennali, in cui ricercatori afferenti a istituzioni straniere (compresi dottorandi) lavorano in Italia per **lunghi periodi** di tempo, o anche attraverso contatti di **breve durata** come partecipazione a conferenze o brevi visite di personale ricercatore ospite.

Creazione protocollo visite

caratteristiche dei luoghi oggetto della visita (attività svolte, presenza di infrastrutture critiche, accesso a informazioni sensibili, etc.) e della natura e dell'ambito di attività dell'istituzione di afferenza del visitatore (mondo accademico, aziende, governi).

Protocollo per la gestione delle visite

sicurezzaricerca.mur.gov.it

Elementi fondamentali del Protocollo

- Valutare il livello di possibile rischio della visita:
  - Basso → prive di attività cliniche o laboratorio
  - Medio/Alto → con attività scientifica e produzione dati
- Predisporre la visita con i responsabili
- Informare il rappresentante della sicurezza
- Preregistrare i nomi della delegazione
- Valutare se distribuire un account all'ospite, e con quali limitazioni
- Non lasciare gli ospiti privi di accompagnamento
- Garantire che il protocollo sia facilmente reperibile sul sito della istituzione

- Luoghi
- Attività
- Motivi della visita

- Accordi scritti
- Informarsi su equivalenti policies di sicurezza degli ospiti
- Gestione oculata dei pass e limitazione dei loro periodi di attività
- Attenzione a interessi non allineati ai progetti o periodi di lavoro non consoni al progetto
- Valutare possibili variazioni di interessi o comparsa di possibili applicazioni commerciali non previste

Grazie