



Linee Guida

per le Istituzioni di Ricerca

Per l'Integrità e la Sicurezza della Ricerca



Linee Guida

Sommario

| | |
|-----------------------------------------------------------------------------------------|---|
| Linee guida per le istituzioni di ricerca | 2 |
| Consapevolezza e comunicazione | 2 |
| Compiti dei responsabili di attività | 3 |
| Protezione dei dati e cybersecurity | 4 |
| Beni e tecnologie a rischio dual use | 5 |
| Collaborazioni, sovvenzioni, contratti e donazioni..... | 5 |
| Revisione, aggiornamento e applicazione delle politiche di conflitto di interessi | 5 |
| Misure di sicurezza per i viaggi all'estero..... | 6 |
| Visite di personale esterno alle istituzioni di ricerca..... | 6 |

Il documento è stato elaborato e proposto dal Gruppo di lavoro sulla sicurezza della ricerca promosso dal Ministero dell'Università e della Ricerca, di cui fanno parte esperti della materia e rappresentanti della Conferenza dei Rettori Italiani (CRUI) e della Consulta dei Presidenti degli Enti Pubblici di Ricerca (COPER). Una presentazione delle esigenze e dei criteri generali in esso sintetizzati è stata fatta alla comunità dei ricercatori e accademica in occasione di due workshop tecnici organizzati nel mese di ottobre nonché della Conferenza Nazionale pubblica del 4 dicembre a Bari.



Linee guida per le istituzioni di ricerca

Le presenti Linee guida sono formulate con l'obiettivo di fornire alle istituzioni di ricerca¹ indicazioni operative per rafforzare la sicurezza della ricerca. Esse possono essere responsabilmente implementate per garantire una maggiore sensibilizzazione e un miglioramento della resilienza del sistema della ricerca, nonché lo sviluppo e l'attuazione di efficaci misure di salvaguardia.

Consapevolezza e comunicazione

Diffusione di comunicazioni a livello di istituzione - Diffondere comunicazioni tempestive ed efficaci al personale ricercatore, al personale tecnico e amministrativo, nonché ai collaboratori e agli studenti, per accrescere la consapevolezza e informare su eventuali ingerenze malevoli da parte di soggetti esterni. Queste comunicazioni includono informazioni, a titolo di esempio, su: iniziative che i ricercatori possono intraprendere per mitigare possibili criticità; requisiti e responsabilità per la segnalazione, la divulgazione, il controllo del trasferimento di conoscenze e tecnologie e altri controlli di sicurezza previsti dalle norme eurounitarie o nazionali; referenti a cui rivolgersi per assistenza.

Pubblicazione di newsletter e presentazioni sulla sicurezza - Pubblicare e distribuire periodicamente newsletter sulla sicurezza riguardanti temi, tra i quali: rischi provenienti dall'estero; preparazione per viaggi internazionali; organizzazione di seminari e presentazioni su integrità e sicurezza della ricerca rivolti ad audience specifiche (tesisti, dottorandi, ricercatori senior, project leaders, leadership accademiche ecc.).

Creazione di pagine web ad hoc nei siti istituzionali - Creare e mettere in evidenza nei siti web istituzionali pagine con link e informazioni su una pluralità di argomenti, tra i quali impegni di ricerca internazionali e collaborazione globale, influenze e interferenze indebite (per esempio, ma non solo, di governi stranieri) e mitigazione dei relativi rischi. Il sito web dovrebbe servire anche come 'sportello unico' telematico per accedere alle politiche e pratiche dell'istituzione in tema di integrità e sicurezza della ricerca, alle relative comunicazioni e informazioni, alle linee guida, nonché ai requisiti definiti dalle istanze nazionali (Governo, Ministeri, ecc.). Sarà presente il link al sito appositamente realizzato dal Ministero: <https://www.sicurezzaicerca.mur.gov.it>.

Promozione del confronto nella comunità - Promuovere discussioni durante le riunioni degli organi di governo dell'istituzione e della comunità di ricerca (ricercatori e personale tecnico e amministrativo coinvolto). Favorire incontri regolari a livello delle strutture interne (dipartimenti, istituti, divisioni ecc.) sui vari aspetti della integrità e sicurezza della ricerca.

¹ Come da definizione fornita nel "Modello Nazionale".

Formazione - Organizzare moduli formativi su tematiche, tra le quali: integrità e sicurezza della ricerca; linee di condotta per viaggi e soggiorni all'estero; linee di condotta in presenza di visitatori nelle strutture, protezione dei dati e cyber-security, attività soggette a controllo delle esportazioni, protezione della proprietà intellettuale.

A tal proposito, il Ministero dell'università e della ricerca ha realizzato una serie di moduli informativi — che saranno disponibili sul sito web dedicato <https://www.sicurezzaicerca.mur.gov.it>, nella sezione “Informazione/Formazione” dopo la fase di sperimentazione.

Compiti dei responsabili di attività

I responsabili di progetti di ricerca, programmi di collaborazione scientifica e didattica, attività di ricerca o innovazione commissionata o conto terzi sono invitati, prima dell'avvio della loro attività, a prendere conoscenza del modulo informativo “Integrità e Sicurezza”, che sarà reperibile nella sezione “Informazione/Formazione” del sito <https://www.sicurezzaicerca.mur.gov.it>, nonché a condurre un'autovalutazione preliminare delle eventuali criticità associate alla attività da intraprendere, accedendo all'area dedicata del sito <https://www.sicurezzaicerca.mur.gov.it> per compilare la scheda di autovalutazione. La scheda sarà resa disponibile al termine della fase di sperimentazione.

Se l'attività non implica il **coinvolgimento di partner e/o finanziamenti esterni** (si veda la definizione fornita nel modulo “Modello Nazionale”), sarà sufficiente dichiararlo. Diversamente, il responsabile effettuerà un'analisi che in una prima fase sperimentale riguarderà tre possibili categorie di criticità, cioè quelle connesse:

- a) all'ambito scientifico o tecnologico nel quale si colloca l'attività;
- b) alle persone e alle istituzioni con cui si collabora;
- c) alle entità che finanziano le attività.

Per ciascuna categoria, saranno presi in considerazione sia i rischi teoricamente possibili, sia quelli concretamente associati all'attività. Una volta riempiti i campi della scheda, verrà automaticamente calcolato, per ciascuna categoria, un **valore dei rischi** associati all'attività. In base ad essi, il responsabile otterrà un report con misure da adottare per mitigare le criticità indicate, ed eventualmente il suggerimento di rivolgersi al referente per la sicurezza e l'integrità della ricerca dell'istituzione di appartenenza, ove esistente, o agli organi di vertice dell'Istituzione per ottenere ulteriori indicazioni al fine di condurre l'attività. Il referente, qualora ne ravvisi la necessità, informando i responsabili dell'attività ed autorizzato dal responsabile legale dell'istituzione o suo delegato, potrà rivolgersi al Centro nazionale per la sicurezza ed integrità della ricerca per opportuni raggugli.

Il responsabile dell'attività potrà valutare di rivolgersi al proprio referente per la sicurezza e l'integrità della ricerca anche prima o durante la compilazione della scheda, qualora necessiti di un confronto preventivo per una migliore valutazione delle criticità associate alla propria attività. Sarà inoltre suo compito aggiornare la scheda di autovalutazione dell'attività ogniqualvolta ricorrano modifiche

riguardo collaborazioni e finanziamenti o ogni altra evoluzione delle attività che possa variare il livello di rischio.

Protezione dei dati e cybersecurity

Consapevolezza di rischi informatici nel contesto delle attività di ricerca scientifica – Informare e formare ricercatori, studenti e personale tecnico e amministrativo sulla sicurezza informatica di base, sulle misure di protezione dei dati² e sulle implicazioni della cybersecurity nella protezione delle attività di ricerca. Anche su questo aspetto, sono previsti moduli informativi che saranno pubblicati nel sito <https://www.sicurezza Ricerca.mur.gov.it> alla sezione “Informazione/Formazione”.

Analisi e misure di gestione del rischio – Condurre una analisi per la valutazione del rischio cyber associato alle attività di ricerca scientifica, coinvolgendo le parti interessate: personale ricercatore e personale tecnico e amministrativo dedicato (servizi IT). Sviluppare una procedura di gestione del rischio cyber delle attività di ricerca che includa l’identificazione degli asset informativi critici, la protezione dei dati, il controllo degli accessi, la sicurezza delle reti e dei sistemi informativi e le procedure di risposta agli incidenti. Le istituzioni collaborano con l’Agenzia per la Cybersecurity Nazionale³ (ACN) - con particolare riferimento alla conformità alla direttiva NIS-2 - con il Garante per la Protezione dei Dati Personali⁴ (GPDP), con l’Agenzia per l’Italia Digitale⁵ (AGID), e le altre autorità competenti.

Sicurezza informatica e sicurezza della ricerca – Adottare misure per la sicurezza informatica delle attività di ricerca e per la prevenzione delle violazioni interne, che siano proporzionate al livello di rischio, alla criticità della specifica attività e alle altre informazioni di contesto.

Aggiornamento continuo – Monitorare i cambiamenti normativi e adottare tempestivamente pratiche di aggiornamento continuo, con particolare riferimento alle norme europee e nazionali, in collaborazione con le autorità competenti e il Centro nazionale per la sicurezza e l’integrità della ricerca.

² Dal 2018 è diventato pienamente efficace in tutti gli Stati membri dell’Unione Europea il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, “Regolamento generale sulla protezione dei dati” che individua un quadro unitario di misure e adempimenti per assicurare che nella circolazione dei dati personali trovino sempre adeguata tutela i diritti e libertà fondamentali degli interessati contribuendo a creare quel clima di fiducia necessario per lo sviluppo dell’economia. Si segnala, infine, che il Regolamento generale per la protezione dei dati individua specifiche condizioni giuridiche per i trasferimenti di dati personali verso paesi terzi, non appartenenti all’Unione europea, affinché sia assicurato un livello di protezione adeguato dei dati oggetto di trasferimento. In particolare, è previsto che, in assenza di una decisione di adeguatezza adottata dalla Commissione europea ai sensi dell’art. 45 del Regolamento medesimo, i trasferimenti di dati personali verso Paesi terzi siano consentiti solo qualora il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (artt. 46 e 47 del Regolamento).

³ <https://www.acn.gov.it/portale/home>

⁴ <https://www.garanteprivacy.it/>

⁵ <https://www.agid.gov.it/it>

Beni e tecnologie a rischio dual use

I beni e le tecnologie “dual use” - che hanno la caratteristica di poter essere utilizzati sia per applicazioni civili che per applicazioni militari - sono regolamentati a livello eurounitario e nazionale.

L’attività di ricerca, costantemente innovativa, è particolarmente esposta a rischi di trafugamento e/o esportazione non autorizzata di tali beni e tecnologie. Inoltre, vi è anche la possibilità che soggetti ed organismi estranei agli obiettivi pacifici della ricerca siano interessati a raccogliere informazioni, conoscenze e materiale scientifico.

Al fine di gestire e mitigare le criticità provenienti da queste esposizioni, l’Italia, come gli altri Stati europei, destina da anni, nell’ambito delle attività dell’Autorità Nazionale UAMA⁶ del Ministero per gli Affari Esteri e la Cooperazione Internazionale, specifiche risorse per supportare l’attività di imprese e di istituzioni di ricerca nella valutazione e gestione di questi rischi, in applicazione del Regolamento (UE) 2021/821⁷ e nell’adozione dei Programmi Interni di Conformità relativi al controllo della ricerca riguardante i prodotti a duplice uso, come previsto dalla Raccomandazione (UE) 2021/1700⁸ adottata a specifico supporto delle istituzioni di ricerca.

Per ulteriori informazioni relative alla gestione delle sopra indicate attività si vedano i siti web delle autorità competenti e la sezione “Approfondimenti” del sito web <https://www.sicurezzaicerca.mur.gov.it>.

Collaborazioni, sovvenzioni, contratti e donazioni

La scheda di autovalutazione e le misure per la mitigazione dei rischi predisposte dal Centro nazionale per la sicurezza e l’integrità della ricerca sono applicabili a progetti, collaborazioni, contratti, accordi, sovvenzioni e donazioni, ogniqualvolta siano coinvolti soggetti esterni (come da definizione nel “Modello Nazionale”). L’analisi dovrà includere il controllo delle eventuali esportazioni di beni e tecnologie, la valutazione di termini e condizioni per l’erogazione delle sovvenzioni e la potenziale generazione e trasmissione all’esterno di dati o informazioni sensibili o riguardanti tecnologie critiche. Per le situazioni che richiedono uno screening aggiuntivo, i ricercatori potranno rivolgersi al referente per la sicurezza e l’integrità della ricerca dell’istituzione, il quale, a sua volta, valuterà se interfacciarsi con il Centro nazionale per la sicurezza e l’integrità della ricerca.

Revisione, aggiornamento e applicazione delle politiche di conflitto di interessi

Un Conflitto di Interesse (COI) indica qualsiasi circostanza in cui gli interessi personali, professionali, finanziari o di altro tipo di un individuo (inclusi i membri immediati della sua famiglia) possono potenzialmente o effettivamente divergere, o possono essere ragionevolmente percepiti come potenzialmente o effettivamente divergenti, dai suoi obblighi professionali verso l’istituzione di appartenenza e dagli interessi dell’istituzione stessa. Un COI può esistere ogniqualvolta un osservatore indipendente possa ragionevolmente mettere in dubbio che le azioni o decisioni

⁶ <https://www.esteri.it/it/ministero/struttura/uama/>

⁷ <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32021R0821>

⁸ <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32021H1700>

professionali dell'individuo, inclusa la condotta etica e obiettiva di studi, ricerche o attività cliniche, siano influenzate da considerazioni di guadagno personale, finanziario o di altro tipo. Le situazioni di COI si possono instaurare qualora il singolo ricercatore abbia interessi scientifici, finanziari o didattici con soggetti esterni all'istituzione di appartenenza. In questo ambito rientrano affiliazioni, relazioni e interessi che possono entrare in conflitto con le responsabilità del ricercatore verso la propria istituzione. A titolo di esempio, si menziona la partecipazione a programmi di reclutamento, l'attribuzione di posizioni accademiche, le collaborazioni (anche a titolo non retribuito), il ruolo di "*principal investigator*" in progetti in cui non è coinvolta l'istituzione di appartenenza.

Si raccomanda alle istituzioni che hanno già adottato codici di condotta relativi a COI di valutarne la coerenza con le presenti linee guida. Si raccomanda in ogni caso l'adozione di codici di condotta relativi a COI da parte delle istituzioni che non le avessero ancora approntate. A supporto dei ricercatori si suggerisce di visionare la sezione relativa al COI nell'area "Approfondimenti" del sito <https://www.sicurezzaicerca.mur.gov.it>.

Misure di sicurezza per i viaggi all'estero

Sviluppare o aggiornare vademecum per viaggi internazionali e prevedere un registro per tenerne traccia. Fornire briefing sulla sicurezza personalizzati, se necessario, per destinazioni o scopi del viaggio con margini di criticità non trascurabili.

Le istituzioni potranno fare riferimento al modulo informativo "Regole di base per Viaggi e Soggiorni all'Estero", che sarà reso disponibile dopo la fase di sperimentazione nella sezione "Informazione/Formazione" del sito governativo <https://www.sicurezzaicerca.mur.gov.it> e ne promuovono specificamente la conoscenza da parte dei ricercatori in procinto d'intraprendere il viaggio.

Visite di personale esterno alle istituzioni di ricerca

Sviluppare o aggiornare best practices e/o vademecum dedicati alle visite di personale esterno nelle istituzioni di ricerca. Prevedere registri per l'accesso al fine di tenere traccia di elementi quali: identità del visitatore/i, scopo della visita, personale incontrato e durata. Anche in questo caso, per le strategie da adottare le istituzioni possono consultare il modulo informativo "Protocollo per la gestione delle visite", che verrà reso disponibile nella sezione "Informazione/Formazione" del sito governativo <https://www.sicurezzaicerca.mur.gov.it>. Le istituzioni avranno cura che i responsabili dell'accoglienza prendano conoscenza del predetto modulo prima della visita.