

Raccolta di strumenti sulla sicurezza della conoscenza e la scienza aperta

Allegato alla relazione “[Openness and Security: Two Pillars, One System](#)”

Partner del progetto:

Università di Berna (capofila del progetto)

Centro per gli studi sulla sicurezza (ETH)

Università di Scienze Applicate e delle Arti della Svizzera occidentale (HES-SO)

Con il sostegno di swissuniversities

Si tratta di una traduzione automatica della [versione originale in inglese](#), realizzata con DeepL Pro.

Indice

1.	Raccomandazione 1: Sviluppare una politica completa in materia di sicurezza della conoscenza. _____	5
2.	Raccomandazione 2: Istituire responsabili dedicati alla sicurezza della conoscenza o unità interne specializzate. _____	5
3.	Raccomandazione 3: Attuare programmi di formazione e sensibilizzazione sulla sicurezza della conoscenza. _____	8
4.	Raccomandazioni 5, 6 e 7: Misure di sicurezza della conoscenza nella scienza aperta e la scienza aperta come misura di sicurezza della conoscenza _____	8
5.	Incentivi e allineamento della valutazione _____	9
1.	Linee guida complete o valutazioni dei rischi _____	11
2.	Contenuto _____	11
2.1	Soggezione ai controlli sulle esportazioni	11
2.2	Elenchi delle tecnologie critiche	12
2.3	Determinazione del potenziale di doppio uso dei progetti di ricerca	12
3.	Partner _____	13
3.1	Strumenti di valutazione completa	13
3.2	Embargo e sanzioni	14
3.3	Valutazione delle reti di istituzioni o ricercatrici e ricercatori	15
3.4	Elenchi di istituzioni critiche a causa della vicinanza al settore militare	16
3.5	Altre considerazioni	16
4.	Infrastrutture _____	16
	Allegati _____	17

Questo toolbox è stato progettato per supportare le ricercatrici e i ricercatori e gli istituti di ricerca nell'orientarsi nel panorama in continua evoluzione della sicurezza della conoscenza, in particolare nel contesto della scienza aperta (Open Science).¹ Si basa sulla visione condivisa espressa nei «Valori e Principi comuni del G7 sulla sicurezza e l'integrità della ricerca», secondo cui «apertura e sicurezza non sono contraddittorie, ma complementari e si rafforzano a vicenda».

Nel suo rapporto, il gruppo di lavoro nazionale sulla sicurezza della conoscenza, guidato da swissuniversities, individua alcune carenze nel sistema svizzero di gestione della sicurezza della conoscenza, in particolare una mancanza di «competenze specifiche nella valutazione della sicurezza della conoscenza e nella gestione dei rischi»: «Gli amministratori accademici tradizionali potrebbero non disporre delle conoscenze specialistiche necessarie per valutare le complesse implicazioni in materia di sicurezza dei progetti di ricerca o delle collaborazioni internazionali. Questa lacuna di competenze rappresenta una sfida fondamentale che deve essere affrontata attraverso la formazione, l'assunzione di personale o meccanismi di supporto esterni».²

Il rapporto «*Openness and Security: Two Pillars, One System*»³ rappresenta un passo avanti verso il colmare tale lacuna. Questa raccolta di strumenti, che integra il rapporto più ampio, fornisce indicazioni pratiche, esempi e strumenti operativi.

La raccolta di strumenti è rivolta alla dirigenza universitaria e solo indirettamente ai ricercatori. Gli strumenti qui contenuti possono essere utilizzati e adattati al contesto specifico dell'istituzione e al quadro di governance.

Il suo obiettivo è aiutare a identificare, valutare e gestire i potenziali rischi, preservando al contempo l'apertura, la collaborazione internazionale e la libertà accademica, elementi fondamentali per il progresso scientifico. Le misure dovrebbero rimanere proporzionate ai rischi effettivi, evitare inutili oneri burocratici ed essere applicate in modo non discriminatorio.

La toolbox si basa su cinque principi fondamentali.

1. «Il più aperto possibile, il più sicuro necessario»: i risultati della ricerca, i metodi e le collaborazioni dovrebbero essere di default aperti, a meno che rischi legittimi non richiedano un accesso controllato.
2. Proporzionalità: i controlli di sicurezza dovrebbero essere proporzionati al rischio effettivo, evitando un eccesso di burocrazia che ostacoli la collaborazione o l'innovazione.
3. Supporto ai ricercatori: le ricercatrici e i ricercatori non dovrebbero sostenere da soli l'intero onere della conformità. Le istituzioni devono fornire infrastrutture, formazione, servizi di consulenza e supporto amministrativo.

¹ Per una definizione di «Open Science», si rimanda al rapporto a cui fa riferimento questa guida pratica: Università di Berna/Centro per gli studi sulla sicurezza/Haute école spécialisée de Suisse occidentale: Trasparenza e sicurezza: due pilastri, un unico sistema, Berna: 2026. Seguiamo la definizione dell'UNESCO e ci concentriamo sulle due dimensioni dell'accesso aperto e dei dati di ricerca aperti.

² [Swissuniversities – Sicurezza della conoscenza in Svizzera: un quadro strategico per gli istituti di istruzione superiore e le autorità](#), p. 8.

³ Il rapporto illustra il quadro normativo sulla sicurezza della conoscenza e sulla scienza aperta a livello internazionale e in Svizzera, individua quali rischi per la sicurezza della conoscenza esistono effettivamente nel contesto specifico della scienza aperta, spiega quali fattori determinano o aumentano tali rischi e descrive come le istituzioni in Europa e in Svizzera affrontano attualmente i rischi per la sicurezza della conoscenza nell'ambito della scienza aperta. Prima di concludere e fornire raccomandazioni, ci permettiamo di offrire una prospettiva sul futuro della sicurezza della conoscenza e della scienza aperta.

4. Trasparenza e responsabilità: le decisioni in materia di sicurezza della conoscenza devono essere documentate, verificabili e regolate da chiare procedure istituzionali.
5. Preservazione della collaborazione internazionale: l'obiettivo non è la deglobalizzazione della scienza, ma una collaborazione resiliente, etica e sicura.

La toolbox è strutturata in due sezioni: la sezione 1 elenca gli strumenti per affrontare la sicurezza della conoscenza nel contesto specifico della scienza aperta. La Sezione 2 è dedicata ad altri strumenti di valutazione e classificazione dei rischi e a linee guida che non sono specifici del contesto della scienza aperta, ma che le istituzioni potrebbero ritenere utili per affrontare i rischi legati alla sicurezza della conoscenza e per rafforzare i propri quadri di gestione del rischio.

La maggior parte, ma non tutti, gli strumenti citati nella raccolta sono stati sviluppati nell'ambito del progetto swissuniversities sulla sicurezza della conoscenza e la scienza aperta (contrassegnati di seguito come «Risultato del progetto»). Abbiamo inoltre raccolto risorse esistenti che abbiamo ritenuto utili. Nei casi in cui i link non siano più attivi, si invitano le utenti e gli utenti a cercare il titolo della pubblicazione online.

Le sezioni seguenti riprendono le raccomandazioni del Capitolo 6 del rapporto «*Openness and Security: Two Pillars, One System*» e suggeriscono strumenti pratici concreti per la loro attuazione.

1. **Raccomandazione 1: Sviluppare una politica completa in materia di sicurezza della conoscenza.**

La sicurezza della conoscenza dovrebbe essere integrata nella strategia istituzionale, nella governance della ricerca e nei quadri di riferimento per la gestione dei rischi. Le istituzioni dovrebbero stabilire politiche chiare in materia di sicurezza della conoscenza che coprano aree chiave quali le procedure di due diligence per le collaborazioni internazionali, i protocolli di trasferimento tecnologico, le misure di sicurezza delle informazioni e i meccanismi per segnalare eventuali problemi relativi alla sicurezza della conoscenza. Tali politiche dovrebbero essere allineate alle norme nazionali e istituzionali in materia di controlli sulle esportazioni, protezione dei dati e proprietà intellettuale.

Tali politiche dovrebbero essere elaborate in consultazione con la comunità di ricerca per garantire che siano pratiche, proporzionate e trasparenti. Allo stesso tempo, dovrebbero ridurre al minimo gli oneri amministrativi superflui, pur rimanendo sufficientemente flessibili per rispondere all'evoluzione dei rischi e dei requisiti normativi.

La scienza aperta dovrebbe essere presa in considerazione in questa politica e nell'ambito delle attività operative come prassi consolidata. Come buona prassi, le istituzioni dovrebbero inoltre adottare una politica specifica sulla sicurezza della conoscenza nella scienza aperta che:

- definisca la propensione al rischio a livello nazionale e dell'istituzione in merito all'apertura rispetto alle restrizioni
- fornisca indicazioni concrete e specifiche per l'istituzione
- distingua tra discipline e livelli di rischio (ad esempio, discipline umanistiche rispetto ai settori STEM a duplice uso).

In linea con le raccomandazioni 5, 6 e 7 del rapporto «*Openness and Security: Two Pillars, One System*», raccomandiamo che a livello operativo le pratiche di scienza aperta siano considerate e utilizzate come misure di sicurezza della conoscenza e che tali pratiche siano migliorate attraverso misure di sicurezza della conoscenza.⁴ Questo approccio garantisce che entrambi i settori si rafforzino a vicenda, riducendo al contempo il rischio di creare l'ennesima procedura amministrativa.

2. **Raccomandazione 2: Istituire responsabili dedicati alla sicurezza della conoscenza o unità interne specializzate.**

Al fine di sviluppare e attuare correttamente le politiche e le procedure menzionate sopra nel capitolo 1, sezione 1, le istituzioni devono investire in una struttura di supporto che copra sia gli aspetti legali, di conformità e di sicurezza, sia quelli relativi alla scienza aperta. Data la natura sovrapposta della sicurezza della conoscenza e della scienza aperta, le unità separate dovrebbero essere formate rispettivamente nell'altro ambito.

⁴ Nel capitolo 1, sezione 4 di questa guida pratica viene suggerito uno strumento concreto.

Si raccomanda alle istituzioni il seguente portafoglio di servizi:

1. Helpdesk per la scienza aperta: supporto alla pubblicazione e agli archivi

Questo servizio costituisce il punto di riferimento per le ricercatrici e i ricercatori che desiderano pubblicare i propri risultati in modo aperto e rispettare i requisiti dei finanziatori o delle istituzioni.

Funzioni principali

- Supporto alla pubblicazione ad accesso aperto: consulenza sulle politiche degli editori, sul finanziamento degli APC, sugli accordi trasformativi e sulla conservazione dei diritti
- Supporto agli archivi: deposito di articoli, set di dati, software, tesi e altri risultati in archivi istituzionali o disciplinari
- Metadati e reperibilità: garantire che i risultati siano correttamente descritti, collegati (ORCID, DOI, ID delle sovvenzioni) e indicizzati
- Orientamento sulle licenze: assistenza ai ricercatori nella scelta delle licenze appropriate (ad es. Creative Commons)
- Monitoraggio della conformità: verifica del rispetto dei requisiti imposti dai finanziatori e delle politiche istituzionali in materia di scienza aperta

2. Gestione responsabile dei dati: gestione dei dati conforme ai principi FAIR e sicura, compresi i rischi per la sicurezza delle conoscenze nell'ambito della scienza aperta

Questo servizio garantisce che i dati di ricerca siano sia riutilizzabili sia adeguatamente protetti.

Gestione dei dati secondo i principi FAIR

- Reperibili: identificatori persistenti e metadati dettagliati
- Accessibili: meccanismi di accesso controllato o aperto
- Interoperabilità: uso di standard e formati comuni
- Riutilizzabili: documentazione, provenienza e licenze

Funzioni di sicurezza e governance

- Classificazione dei dati (pubblici/ interni/ riservati/ a accesso limitato, oppure: aperti/ a accesso limitato/ classificati/ soggetti a controlli sulle esportazioni, ecc.)
- Archiviazione sicura e controlli di accesso
- Politiche di crittografia, backup e conservazione
- Supporto per i piani di gestione dei dati (DMP)

Il ruolo della sicurezza della conoscenza nella scienza aperta

Un'unità moderna di gestione responsabile dei dati valuta anche se la messa a disposizione aperta dei dati possa creare rischi per la sicurezza delle conoscenze. Ne sono esempi i dati di ricerca a duplice uso, le informazioni sensibili sulle infrastrutture, le tecnologie strategiche o i dati soggetti a restrizioni contrattuali o nazionali.

Il responsabile della gestione dei dati, pertanto, svolge o coordina, in collaborazione con i responsabili della conformità in materia di sicurezza delle conoscenze (vedi sotto):

- Identificazione dei rischi
- Valutazione dei rischi (probabilità e impatto)
- Mitigazione dei rischi (divulgazione parziale, embargo, accesso controllato, anonimizzazione)
- Documentazione delle decisioni

3. Responsabile della conformità in materia di sicurezza delle conoscenze

Le istituzioni dovrebbero nominare responsabili della sicurezza della conoscenza e/o istituire un comitato per la sicurezza della conoscenza a supporto dell'attuazione e del processo decisionale.⁵ Essi forniscono consulenza alle ricercatrici e ai ricercatori e alla dirigenza, coordinano le valutazioni dei rischi, esaminano casi complessi o ad alto rischio, definiscono percorsi chiari di escalation per le decisioni difficili e garantiscono un'applicazione coerente e proporzionata delle politiche in tutta l'istituzione, nonché l'integrazione efficace e armonizzata della sicurezza della conoscenza in altre unità all'interno dell'istituzione (ad esempio, uffici dedicati alla scienza aperta o agli affari internazionali, ecc.).

Responsabilità principali⁶

- Valutazioni della collaborazione internazionale: identificare partner, fonti di finanziamento, giurisdizioni e aree tecnologiche strategiche; valutare i rischi di trasferimento indesiderato di conoscenze, tecnologia, dati o competenze
- Screening per l'assunzione del personale: esaminare le nomine in aree di ricerca sensibili; identificare conflitti di interesse, affiliazioni non dichiarate o problemi relativi a sanzioni
- Screening degli studenti (ove consentito dalla legge e adottato a livello istituzionale): valutare l'accesso a strutture, set di dati o tecnologie altamente sensibili; applicare misure proporzionate e basate sul rischio
- Gestione dei rischi legati alla scienza aperta: verificare se le pubblicazioni pianificate, i preprint, il rilascio di software o la condivisione di dati possano creare problemi di sicurezza delle conoscenze; coordinare le misure di mitigazione prima del rilascio
- Formazione e sensibilizzazione: fornire indicazioni a ricercatori, supervisori, amministratori e dirigenti

Questo ruolo non dovrebbe fungere da filtro generalizzato per la collaborazione internazionale. Le buone pratiche sono basate sul rischio, proporzionate e trasparenti, e bilanciano la libertà accademica con gli obblighi di sicurezza.

4. Ufficio legale e di controllo delle esportazioni: supporto normativo

Questo servizio fornisce l'interpretazione giuridica e normativa formale su cui si fondano le altre funzioni.

Responsabilità tipiche

- Classificazioni relative al controllo delle esportazioni e screening delle sanzioni
- Revisione dei contratti
- Consulenza in materia di proprietà intellettuale
- Conformità in materia di protezione dei dati e privacy
- Tenuta dei registri e supporto alle attività di audit
- Collaborazione con le autorità nazionali

5. Come si integrano i quattro servizi

Helpdesk per la scienza aperta → Gestione dei dati → Responsabile della sicurezza delle conoscenze
→ Controlli legali e sulle esportazioni

⁵ Si veda anche la raccomandazione del gruppo di lavoro nazionale qui: [swissuniversities – Sicurezza della conoscenza in Svizzera: un quadro strategico per le istituzioni di istruzione superiore e le autorità](#), sezione 4.1, nonché la raccomandazione n. 2 del rapporto «Trasparenza e sicurezza: due pilastri, un unico sistema».

⁶ Si veda anche la raccomandazione del Gruppo di lavoro nazionale qui: [swissuniversities – Sicurezza della conoscenza in Svizzera: un quadro strategico per gli istituti di istruzione superiore e le autorità](#), sezione 4.2 e allegato 3.

Ad esempio:

- Un ricercatore desidera pubblicare un articolo e rendere pubblico un set di dati.
- L'helpdesk per la scienza aperta fornisce assistenza per il deposito nell'archivio e la concessione delle licenze.
- La gestione dei dati verifica la conformità ai principi FAIR, la riservatezza e le potenziali criticità di sicurezza.
- Se il progetto coinvolge dati sensibili, il responsabile della sicurezza delle conoscenze viene coinvolto nella valutazione e nella gestione dei rischi.
- Se sorgono questioni relative a tecnologie soggette a controllo o a sanzioni, l'ufficio Legale/Controlli sulle esportazioni determina i requisiti legali applicabili.
- Il ricercatore riceve un unico percorso decisionale coordinato anziché consigli contrastanti provenienti da più uffici.

3. **Raccomandazione 3: Attuare programmi di formazione e sensibilizzazione sulla sicurezza della conoscenza.**

Il presupposto per l'implementazione efficace delle misure di sicurezza della conoscenza nelle operazioni istituzionali è la consapevolezza e l'accettazione all'interno della comunità dei ricercatori. Avviare un movimento dal basso verso l'alto, anziché imporre requisiti dall'alto verso il basso, si rivelerà più efficace e sostenibile. Gli strumenti seguenti hanno lo scopo di supportare le istituzioni nella sensibilizzazione e nell'informazione sulla sicurezza della conoscenza (nella scienza aperta).

- **Risultato del progetto:** Cosa fare e cosa non fare per la sicurezza della conoscenza nella scienza aperta (allegato 1)

Strumento conciso di riflessione e orientamento, destinato a sensibilizzare il pubblico in generale

A chi è rivolto: ricercatrici e ricercatori

Quando: strumento senza limiti temporali

- **Risultato del progetto:** Diapositive su "Introduzione alla sicurezza della conoscenza nella scienza aperta" (allegato 2)

Cosa: diapositive che introducono alla sicurezza della conoscenza nella scienza aperta, da adattare in base alle esigenze e alle priorità di ciascuna istituzione.

A chi è rivolto: amministrazione universitaria, incaricata di sensibilizzare i ricercatori.

Quando: strumento senza limiti temporali; potrebbe essere condiviso durante l'inserimento del nuovo personale e/o durante i corsi di formazione periodici.

4. **Raccomandazioni 5, 6 e 7: Misure di sicurezza della conoscenza nella scienza aperta e la scienza aperta come misura di sicurezza della conoscenza**

Gli strumenti riportati di seguito hanno lo scopo di aiutare le istituzioni a integrare la sicurezza della conoscenza nelle pratiche di scienza aperta e a utilizzare tali pratiche come strumenti per la sicurezza della conoscenza.

- **Risultato del progetto:** Piano di gestione della sicurezza della conoscenza (per la scienza aperta, KSMP) (allegato 3)

Cosa: Proposta di un questionario completo che possa essere utilizzato come strumento di valutazione dei rischi per individuare i rischi legati alla sicurezza della conoscenza durante l'attuazione della scienza aperta. Si tratta di uno strumento volto a evidenziare determinati rischi e a sensibilizzare l'opinione pubblica.

A chi è rivolto: Da compilare da parte dei ricercatori in collaborazione con i responsabili della gestione dei dati e i responsabili della sicurezza della conoscenza.

Quando: il prima possibile nel processo di ricerca, ma al più tardi prima della pubblicazione dei dati.

- **Risultato del progetto:** Albero decisionale sulla condivisione dei dati (sicurezza delle conoscenze nella scienza aperta) (allegato 4)

Cosa: Un albero decisionale pratico che integra e rende operativo il Piano di gestione della sicurezza delle conoscenze (per la scienza aperta). Il KSMP può chiarire o fornire indicazioni su come rispondere alle domande poste nell'albero decisionale.

A chi è rivolto: ricercatrici e ricercatori, possibilmente in collaborazione con i responsabili della gestione dei dati e i responsabili della sicurezza delle conoscenze.

Quando: il prima possibile nel processo di ricerca, ma al più tardi prima della pubblicazione dei dati.

- **Risultato del progetto:** Rischi per la sicurezza della conoscenza nella scienza aperta: misure di mitigazione dei rischi (allegato 5)

Cosa: Raccolta di misure volte a mitigare i rischi identificati nel Piano di gestione della sicurezza delle conoscenze. Può essere utilizzata come strumento di follow-up del KSMP o dell'albero decisionale, una volta identificati i rischi e/o una volta presa una decisione in merito al livello di restrizione di un set di dati.

A chi è rivolto: ricercatrici e ricercatori in collaborazione con le persone responsabili della gestione dei dati e i responsabili della sicurezza delle conoscenze.

Quando: Non appena vengono identificati i rischi, ma al più tardi prima della pubblicazione dei dati.

5. Incentivi e allineamento della valutazione

Sia la sicurezza della conoscenza che la scienza aperta possono essere rafforzate attraverso incentivi e l'allineamento del sistema di valutazione di un'istituzione, in modo complementare agli eventuali standard CoARA. L'obiettivo è premiare le ricercatrici e i ricercatori per un'apertura responsabile e una condotta di ricerca sicura.

Ad esempio, i seguenti elementi possono essere inclusi in un quadro di criteri di promozione già esistente:

Ambito	Esempio di indicatore
Accesso aperto	Percentuale di pubblicazioni accessibili in modalità aperta
Dati aperti	Set di dati conformi ai principi FAIR depositati
Riproducibilità	Codice FAIR, flussi di lavoro, protocolli
Coinvolgimento del pubblico	Scienza dei cittadini e impatto sociale
Collaborazione responsabile	Completamento delle procedure di due diligence
Pratiche sicure di gestione dei dati	Gestione adeguata dei dati sensibili

Allo stesso modo, si potrebbero assegnare premi istituzionali per le stesse attività e le sovvenzioni interne potrebbero tenere conto dei criteri della scienza aperta e di sicurezza delle conoscenze.

u^b

u^b

Nel capitolo 3 del rapporto “Openness and Security: Two Pillars, One System”, analizziamo i fattori che determinano o aumentano i rischi per la sicurezza della conoscenza. Gli strumenti riportati di seguito aiutano le istituzioni a valutare la probabilità di rischi legali e di sicurezza al di là della scienza aperta, sulla base di questi fattori (contenuto della ricerca (risultati), partner e infrastrutture).

1. Linee guida complete o valutazioni dei rischi

I due strumenti seguenti coprono diversi rischi legali e di sicurezza e, pertanto, non rientrano in nessuna delle categorie (contenuto, partner, infrastruttura).

- Governo dei Paesi Bassi (2022): [Linee guida nazionali sulla sicurezza della conoscenza](#)
Cosa: *Linee guida sulla valutazione delle minacce, il quadro giuridico, la valutazione dei rischi, la gestione dei rischi, i partenariati internazionali, le assunzioni e la sicurezza informatica*
A chi si rivolge: *Istituzioni di istruzione superiore e il loro management*
Quando: *Prima o durante l’implementazione delle strutture di governance istituzionale*
- DLR Projektträger/Safeguarding Science (2024): [Due Diligence in ambito scientifico](#)
Cosa: *Linee guida principalmente sui rischi legati alle assunzioni e alle collaborazioni internazionali*
A chi: *Istituzioni di istruzione superiore e persone che dirigono le istituzioni*
Quando: *prima o durante l’attuazione delle strutture di governance istituzionale*

2. Contenuto

2.1 Soggezione ai controlli sulle esportazioni

- Elenchi svizzeri di controllo delle esportazioni
 - [Legge sul controllo delle merci](#)
 - [Ordinanza sul controllo delle merci](#)
 - [Legge sul materiale bellico](#)
 - [Ordinanza sul materiale bellico](#)
 - Ordinanza sul controllo delle sostanze chimiche (in [tedesco](#), [francese](#) o [italiano](#))
 - Ordinanza sull’esportazione e l’intermediazione di beni destinati alla sorveglianza delle comunicazioni via Internet e di telefonia mobile (in [tedesco](#), [francese](#) o [italiano](#))
 - Allegati contenenti l’elenco dei beni soggetti a controllo delle esportazioni (in [tedesco](#), [francese](#) o [italiano](#))
- Disposizioni estere con applicazione extraterritoriale
 - Le normative statunitensi in materia di sanzioni, embarghi e controlli sulle esportazioni hanno carattere extraterritoriale. Esse trovano applicazione in tutto il mondo qualora siano soddisfatti determinati criteri di collegamento:
 - Persone statunitensi: tutti i cittadini statunitensi, tutte le persone residenti negli Stati Uniti e le persone in possesso di un permesso di soggiorno statunitense (ad es. green card), indipendentemente dalla loro ubicazione;

- tutte le persone fisiche e giuridiche residenti o domiciliate negli Stati Uniti; e tutte le società domiciliate negli Stati Uniti e le loro filiali estere.
- Prodotti statunitensi, compresi quelli composti per almeno il 10% o il 25% da prodotti di origine statunitense (ad esempio, un drone che utilizza software statunitense per il controllo).
- Regimi di controllo delle esportazioni statunitensi:
 - Export Administration Regulation (EAR): beni a duplice uso ([Commerce Control List](#))
 - [International Traffic in Arms Regulations \(ITAR\)](#): beni militari
- Guida alla consultazione degli elenchi dei beni:
 - Gli elenchi dei beni sono disponibili solo in tedesco, francese o italiano. Se avete bisogno degli elenchi dei beni in una lingua diversa, potete consultare l'elenco dei beni a duplice uso dell'UE (Allegato 1 al [Regolamento \(UE\) 2021/821](#)), disponibile in tutte le lingue dell'UE. Non è identico al 100% all'elenco svizzero, quindi assicuratevi di verificare se la voce che avete trovato corrisponde a quella presente nell'elenco svizzero.
 - Indici per parole chiave per determinare se un determinato bene/tecnologia/software sia soggetto a controlli sulle esportazioni
 - Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA): [Glossario comune non vincolante per la Parte I dell'elenco delle esportazioni e l'Allegato I al regolamento UE sui beni a duplice uso](#) (in tedesco). Questo indice per parole chiave si basa sull'elenco dei beni a duplice uso dell'UE, pertanto è necessario verificare se la voce individuata corrisponda a quella presente nell'elenco svizzero.
 - Bureau of Industry and Security (BIS): [Interactive Commerce Control List](#). Si tratta dell'elenco statunitense dei beni a duplice uso, consultabile tramite parole chiave. Anche in questo caso, poiché l'elenco svizzero non è identico al 100% a quello statunitense, è necessario verificare se la voce individuata corrisponda a quella presente nell'elenco svizzero.

2.2 Elenchi delle tecnologie critiche

- DLR Projektträger/Safeguarding Science (2026): [Elenchi delle tecnologie critiche e sensibili – ambito di applicazione, finalità e destinatari](#) (questa pubblicazione illustra gli elenchi elaborati da diversi attori e paesi)
- [Elenco UE delle tecnologie critiche](#)
- Elenco statunitense delle tecnologie critiche ed emergenti ([gennaio 2026](#))
- [Elenco canadese delle tecnologie sensibili](#)
- Elenco delle tecnologie critiche dell'ETH (citato in questo articolo: [«Doppio uso e sanzioni: queste applicazioni richiedono un controllo di sicurezza» – Staffnet | ETH Zurigo](#))

2.3 Determinazione del potenziale di doppio uso dei progetti di ricerca

- **Risultato del progetto:** Questionario sul potenziale di doppio uso (Allegato 6)

Cosa: un questionario completo per determinare il potenziale di doppio uso di un determinato progetto di ricerca nei settori dell'intelligenza artificiale/apprendimento automatico, biotecnologia, chimica, robotica, sicurezza informatica, scienza dei materiali, sistemi energetici, tecnologie quantistiche, aerospaziale, biologia sintetica o neuroscienze. Uno strumento per sensibilizzare e determinare i rischi, le strategie di mitigazione o la supervisione istituzionale o governativa.

A chi è rivolto: Alle ricercatrici e ai ricercatori.

Quando: Durante l'intero ciclo di vita della ricerca: in fase di pianificazione del progetto, ogni volta che un progetto entra in una nuova fase o produce risultati inaspettati, prima di trasferire risultati o materiali ai collaboratori e prima della pubblicazione o di altra diffusione dei risultati della ricerca.

- Istituto Robert Koch (2013): [Potenziale di doppio uso della ricerca nelle scienze della vita](#) (Sezione 3)

Cosa: Il Codice di condotta per la valutazione e la mitigazione dei rischi dell'Istituto Robert Koch stabilisce principi e procedure per identificare, valutare e mitigare il potenziale di doppio uso della ricerca nelle scienze della vita, della salute e mediche.

A chi è rivolto: Principalmente a ricercatrici e ricercatori, responsabili di progetto e dirigenti, in particolare a coloro che conducono ricerche nel campo delle scienze della vita che coinvolgono agenti patogeni, tossine o altre attività di ricerca con potenziali implicazioni di doppio uso.

Quando: Durante l'intero ciclo di vita della ricerca: in fase di pianificazione del progetto, ogni volta che un progetto entra in una nuova fase o produce risultati inaspettati, prima di trasferire risultati o materiali ai collaboratori e prima della pubblicazione o di altra diffusione dei risultati della ricerca.

- Ufficio olandese per la biosicurezza (2021): [Dual-use Quickscan](#)

Cosa: Il Dual-Use Quickscan è uno strumento di autovalutazione online che aiuta le ricercatrici e i ricercatori nel campo delle scienze della vita a identificare potenziali aspetti a duplice uso della loro ricerca attraverso un questionario strutturato e sensibilizza sui rischi per la biosicurezza.

A chi è rivolto: Ricercatrici e ricercatori che lavorano con microrganismi o con conoscenze e tecnologie biologiche correlate.

Quando: In qualsiasi fase del ciclo di vita della ricerca, dalla progettazione del progetto alla pubblicazione.

- Centro comune di ricerca e Università di Liegi: [Piattaforma web TIM Dual-Use](#) (progetto STRIKE, Unità G.II.7 e T.5)

Cosa: TIM Dual-Use è una piattaforma web di text mining che mappa pubblicazioni scientifiche, brevetti e progetti di ricerca finanziati dall'UE per identificare le ricerche con potenziale rilevanza in materia di doppio uso sulla base dell'elenco di controllo dell'UE sui prodotti a doppio uso e delle tecnologie emergenti. Favorisce la sensibilizzazione, l'analisi delle tendenze e la conformità istituzionale aiutando gli persone che utilizzano lo strumento a identificare i risultati di ricerca potenzialmente sensibili. Può essere utilizzata per individuare retroattivamente (cioè dopo la pubblicazione) ricerche a doppio uso o che coinvolgono prodotti soggetti a controllo delle esportazioni.

A chi è rivolto: Istituti di ricerca, università, responsabili politici e persone esperte in materia di controllo delle esportazioni.

Quando: Per vagliare i risultati di ricerca esistenti e monitorare le tecnologie a duplice uso ai fini della sensibilizzazione, della conformità e dell'analisi strategica.

3. Partner

3.1 Strumenti di valutazione completa

- Risultato del progetto: Autovalutazione sulla sicurezza della conoscenza per le ricercatrici e i ricercatori e matrice di valutazione per la direzione dell'istituzione (Allegato 7)

Cosa: Autovalutazione per le ricercatrici e i ricercatori che intendono avviare collaborazioni internazionali, volta ad analizzare e sensibilizzare sui rischi legati alla sicurezza della conoscenza. La matrice di valutazione

(facoltativa) che la accompagna consente alla direzione dell'università di valutare l'autovalutazione attraverso un sistema a semaforo.

A chi è rivolta: L'autovalutazione è destinata alle ricercatrici e ai ricercatori che avviano una nuova collaborazione internazionale. La matrice di valutazione è uno strumento per la direzione/leadership universitaria che facilita il processo decisionale.

Quando: Prima della conclusione di una collaborazione internazionale.

u^b

- Servizio Tedesco per lo Scambio Accademico/Kiwi (2025): [La checklist KIWi sulla sicurezza della conoscenza](#) (in tedesco)

Cosa: La lista di controllo KIWi sulla sicurezza della conoscenza è uno strumento pratico di autovalutazione che aiuta a identificare e riflettere sui rischi legati alla sicurezza della conoscenza nelle collaborazioni di ricerca internazionali attraverso una serie strutturata di domande che riguardano i partner, i finanziamenti, i controlli sulle esportazioni, la proprietà intellettuale e l'etica della ricerca.

A chi è rivolta: alle persone che svolgono attività di ricerca, oppure alla direzione o all'amministrazione istituzionale in fase di attuazione dei processi istituzionali.

Quando: Prima o durante l'avvio di collaborazioni di ricerca internazionali, come valutazione iniziale dei rischi.

- Commissione europea (2024): [Sicurezza della ricerca – Elementi fondamentali per la valutazione dei rischi](#)

Cosa: Gli "Elementi fondamentali per la valutazione dei rischi" della Commissione europea forniscono un quadro di riferimento per la valutazione dei rischi legati alla sicurezza della ricerca nelle collaborazioni internazionali di ricerca e innovazione. Propongono una valutazione strutturata e basata sul contesto che copre il campo di ricerca, i partner, il contesto nazionale e i fattori specifici del progetto, al fine di supportare un processo decisionale informato piuttosto che limitare la collaborazione.

A chi è rivolto: Organizzazioni che svolgono attività di ricerca, enti finanziatori della ricerca e istituti di istruzione superiore.

Quando: Prima di instaurare partnership di ricerca internazionali o di assegnare finanziamenti alla ricerca.

3.2 Embargo e sanzioni

- Svizzera:
 - CH-SECO: [Motore di ricerca per individuare soggetti soggetti a sanzioni](#) (persone fisiche/giuridiche)
 - CH-SECO: [Misure sanzionatorie svizzere](#) (contenuti disponibili in tedesco, francese o italiano)
- Disposizioni estere con applicazione extraterritoriale
(Le sanzioni e gli embarghi statunitensi devono essere applicati a tutti i cittadini statunitensi e ai titolari di green card, indipendentemente dal loro luogo di residenza. Le sanzioni dell'UE devono essere rispettate da tutti i cittadini dell'UE e dalle persone giuridiche costituite o registrate ai sensi della legislazione di uno Stato membro dell'UE, indipendentemente dal loro paese di residenza o domicilio. Lo stesso vale per i cittadini del Regno Unito e le persone giuridiche in relazione alle sanzioni del Regno Unito)
 - Ufficio statunitense per il controllo dei beni stranieri (OFAC): [programmi di sanzioni e informazioni sui paesi](#)
 - OFAC degli Stati Uniti: [Ricerca nell'elenco delle sanzioni](#)
 - Sanzioni e embarghi dell'UE: [mappa delle sanzioni](#)

- Sanzioni ed embarghi del Regno Unito: [sanzioni commerciali, embarghi sulle armi e altre restrizioni commerciali - GOV.UK](#)

3.3 Valutazione delle reti di istituzioni o ricercatrici e ricercatori

Gli strumenti seguenti sono strumenti commerciali piuttosto costosi e la loro integrazione nei processi di due diligence di un'istituzione può creare dipendenze. La maggior parte degli strumenti presentati è incentrata sull'individuazione di reti che coinvolgono partner soggetti a sanzioni o militari.

La Commissione europea sta attualmente (2026) lavorando allo sviluppo di una piattaforma pubblica di due diligence.

- [China Defence Universities Tracker](#)

Uno strumento in abbonamento che monitora oltre 180 entità cinesi legate alla difesa, all'intelligence e alla ricerca tecnologica. Consente a chi utilizza lo strumento di esplorare potenziali capacità a duplice uso, consultare gli elenchi delle sanzioni pertinenti e valutare i rischi legati alla collaborazione globale. Il Tracker è concepito come una risorsa analitica mirata per comprendere le relazioni istituzionali. Non è né uno strumento di profilazione delle persone né una base per restrizioni generalizzate, e non deve essere interpretato come una lista nera. Il suo scopo è piuttosto quello di supportare un processo decisionale informato e proporzionato. Pur essendo ampio, il Tracker non è esaustivo. Le istituzioni non incluse potrebbero comunque presentare dei rischi, e le voci presenti nel database potrebbero non cogliere appieno la portata o la natura dei legami di un'istituzione con i settori della difesa e della sicurezza.

- [Strider Technologies](#)

Strider è uno strumento in abbonamento che offre una visione esterna e basata sull'open source intelligence del panorama della ricerca globale. Identifica le discrepanze tra l'esperienza dichiarata da un individuo e i dati pubblici disponibili, relative a precedenti risultati di ricerca, impegno istituzionale e presenza professionale a lungo termine. Offre inoltre una visione unificata di organizzazioni, personale e unità di ricerca, oltre a un monitoraggio continuo dei rischi legati agli Stati-nazione.

- [Kharon](#)

Kharon è una piattaforma di intelligence sui rischi che supporta la conformità alle sanzioni, la due diligence sul controllo delle esportazioni, la gestione dei rischi della catena di approvvigionamento e lo screening di terze parti. Utilizza l'intelligence open-source, l'analisi delle reti e l'analisi dei dati per identificare relazioni nascoste tra individui, organizzazioni, strutture proprietarie e attori soggetti a restrizioni o ad alto rischio.

- [Xapien](#)

Xapien è una piattaforma di due diligence e valutazione dei rischi di terze parti basata sull'intelligenza artificiale. Automatizza la ricerca di informazioni su individui e organizzazioni combinando dati provenienti dal web aperto, fonti giornalistiche, registri societari, elenchi di sanzioni e liste di controllo, nonché altri set di dati commerciali, in un unico rapporto supportato da fonti attendibili.

- [Dimensions Research Security](#)

Questo strumento, disponibile su abbonamento, mappa le affiliazioni internazionali, le collaborazioni e i flussi di finanziamento. Supporta l'identificazione di doppie cariche, la partecipazione a programmi

u^b

di talenti stranieri e potenziali collegamenti con entità soggette a sanzioni, aiutando così le istituzioni a valutare e gestire meglio i rischi legati alla collaborazione.

3.4 Elenchi di istituzioni critiche a causa della vicinanza al settore militare

- Governo del Canada: [Elenco delle organizzazioni di ricerca designate](#)
- [Entità identificate come società militari cinesi operanti negli Stati Uniti](#)
- [Elenco degli utenti finali giapponesi](#)
- Australian Strategic Policy Institute: [China Defence Universities Tracker](#)

3.5 Altre considerazioni

- [Indice dello Stato di diritto del World Justice Project](#)
- [Indice della democrazia](#)
- [Indice dei diritti umani 2025: classifica dei paesi migliori e peggiori](#)
- [Indice di libertà umana](#)
- [Indice di Freedom House](#)
- [Indice di libertà accademica](#)
- [Indice di percezione della corruzione](#)

4. Infrastrutture

I rischi per la sicurezza della conoscenza relativi alle infrastrutture possono essere valutati utilizzando il Piano di gestione della sicurezza della conoscenza proposto nel Capitolo 1, Sezione 4.

u^b

Allegati

Click to download for annexes in English:

1. [Do's and Don'ts for Knowledge Security in Open Science](#)
2. [Slides on "Introduction to Knowledge Security in Open Science"](#)
3. [Knowledge Security Management Plan \(for Open Science\)](#)
4. [Decision tree on data sharing \(Knowledge Security in Open Science\)](#)
5. [Knowledge Security risks in Open Science: mitigation measures](#)
6. [Questionnaire on Dual-use potential](#)
7. [Checklist for researchers and evaluation matrix for institutional management for international collaborations](#)

Le traduzioni degli allegati in italiano sono in fase di elaborazione. Se avete bisogno delle traduzioni in tempi brevi, potete contattare open-science@swissuniversities.ch,

u^b