



Settembre 2026

Rapporto esplicativo concernente la modifica di maggio 2027 dell'ordinanza sull'energia nucleare

Indice

1. Punti essenziali del progetto1

2. Ripercussioni finanziarie, sull’effettivo del personale e altre ripercussioni per Confederazione, Cantoni e Comuni1

3. Ripercussioni sull’economia, sull’ambiente e sulla società.....1

4. Commento ai singoli articoli1

1. Punti essenziali del progetto

Secondo l'articolo 2 capoverso 3 dell'ordinanza del 12 novembre 2008 sull'Ispettorato federale della sicurezza nucleare (OIFSN; RS 732.21), l'Ispettorato federale della sicurezza nucleare (IFSN) ha l'obbligo giuridico di fare verificare periodicamente da esperti esterni l'adempimento delle esigenze dell'Agenzia internazionale dell'energia nucleare (AIEA). Nell'autunno 2023 un team internazionale di esperti (International Physical Protection Advisory Service, IPPAS) ha verificato la vigilanza nucleare in Svizzera per quanto riguarda la sicurezza esterna, formulando raccomandazioni («recommendations») e proposte («suggestions») in un rapporto¹. Per l'attuazione di singole proposte, l'IFSN è giunto alla conclusione che è necessario un adeguamento delle condizioni quadro giuridiche. Le modifiche riguardano segnatamente l'interfaccia tra la sicurezza nucleare interna e la sicurezza nucleare esterna, le responsabilità nel settore della sicurezza informatica² nonché la protezione di impianti nucleari contro le cyberminacce. La sicurezza informatica comprende, tra l'altro, la protezione contro le cyberminacce e tiene pertanto conto sia delle esigenze relative alla sicurezza esterna degli impianti nucleari sia di quelle relative alla sicurezza nucleare interna. Poiché la protezione dei sistemi d'informazione, dei dati e dell'infrastruttura digitale garantisce in misura sempre maggiore l'esercizio sicuro di un impianto nucleare, i provvedimenti di protezione corrispondenti devono essere intrinsecamente robusti e resilienti.

Le modifiche proposte consistono in precisazioni e integrazioni conformi allo standard internazionale.

2. Ripercussioni finanziarie, sull'effettivo del personale e altre ripercussioni per Confederazione, Cantoni e Comuni

Le modifiche non hanno alcuna ripercussione finanziaria, a livello di personale o di altro tipo su Confederazione, Cantoni e Comuni. Le modifiche previste costituiscono semplicemente precisazioni e integrazioni relative alla vigilanza nucleare esercitata dall'IFSN.

3. Ripercussioni sull'economia, sull'ambiente e sulla società

Le modifiche non hanno alcuna ripercussione sull'economia, sull'ambiente e sulla società. Esse rispecchiano la prassi attuale. Di conseguenza, per gli esercenti di impianti nucleari non ci sono ripercussioni né finanziarie né a livello di personale.

4. Commento ai singoli articoli

Art. 9 cpv. 1^{bis}

Una proposta del team internazionale di esperti riguarda l'introduzione di disposizioni giuridiche esplicite sulla sicurezza informatica («computer security») negli impianti nucleari nonché la disciplina delle relative competenze. Il team consiglia di definire chiaramente le responsabilità di tutti i servizi coinvolti per la corretta interpretazione e attuazione dei rispettivi obblighi giuridici nel settore della sicurezza informatica. Questa proposta viene già parzialmente tenuta in considerazione, in quanto dall'introduzione, il

¹ International Physical Protection Advisory Service (IPPAS), International Atomic Energy Agency (IAEA), IPPAS Follow-up Mission Report: Switzerland, 30 October – 10 November 2023

² Per sicurezza informatica si intende la protezione dei sistemi d'informazione, dei dati e dell'infrastruttura digitale dall'accesso non autorizzato, da manipolazioni, da guasti e da abusi, con l'obiettivo di garantirne la disponibilità, l'integrità, la confidenzialità e l'autenticità.

1° aprile 2025, dell'obbligo di segnalare i ciberattacchi a infrastrutture critiche, l'IFSN è tenuto a notificare all'Ufficio federale della cibersicurezza (UFCS) i ciberattacchi agli impianti nucleari che soddisfano i requisiti dell'articolo 74d della legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni (LSIn; RS 128). Continua tuttavia a mancare una norma esplicita che disciplini la competenza generale in materia di sicurezza informatica negli impianti nucleari.

L'articolo 5 capoverso 3 della legge federale del 21 marzo 2003 sull'energia nucleare (LENu; RS 732.1) prevede che vengano presi provvedimenti di sicurezza esterna, in particolare per impedire che la sicurezza interna di impianti nucleari e materiali nucleari sia ridotta da effetti non autorizzati. Tra questi rientrano anche gli effetti non autorizzati su sistemi computerizzati o su sistemi informatici di un impianto nucleare, qualora possano pregiudicare la sicurezza nucleare interna. Ciò significa che la sicurezza informatica di un impianto nucleare è parte integrante della sua sicurezza esterna e, di conseguenza, anche della sua sicurezza interna ai sensi della LENu.

L'articolo 9 dell'ordinanza del 10 dicembre 2004 sull'energia nucleare (OENu; RS 732.11) viene pertanto integrato con un capoverso 1^{bis}, che ora menziona espressamente la sicurezza informatica negli impianti nucleari come parte della sicurezza interna ed esterna. Poiché secondo l'articolo 6 lettera a OENu l'IFSN è l'autorità di vigilanza per quanto concerne la sicurezza nucleare e la sicurezza esterna, è anche chiaramente definita la sua competenza in materia di sicurezza informatica.

Art. 9a

Per quanto riguarda le disposizioni in materia di sicurezza informatica, il team internazionale di esperti ha constatato che, nella direttiva IFSN-G22³ che si basa in particolare sui principi per la progettazione di centrali nucleari (art. 10 cpv. 2 OENu) e altri impianti nucleari (art. 12 cpv. 3 OENu), l'IFSN ha definito principi fondamentali essenziali per la sicurezza informatica negli impianti nucleari. Ha tuttavia anche riconosciuto che in Svizzera non esistono attualmente basi legali esplicite e vincolanti in questo settore.

Il nuovo articolo 9a introduce una disposizione che obbliga gli esercenti di impianti nucleari a prevedere adeguati provvedimenti di protezione contro le cyberminacce. A tal proposito, l'IFSN è incaricato di precisare i relativi requisiti in direttive. La direttiva IFSN-G22 trova così una base esplicita nell'ordinanza.

Il nuovo articolo si basa sull'articolo 5 capoversi 3 e 4 LENu, che stabilisce che vanno presi provvedimenti di sicurezza esterna per impedire che la sicurezza interna di impianti nucleari e materiali nucleari sia ridotta da effetti non autorizzati, demandando al Consiglio federale la determinazione dei provvedimenti di protezione necessari.

Art. 9b

L'AIEA rimanda nei propri documenti all'interfaccia tra la sicurezza nucleare interna e la sicurezza nucleare esterna. In tutti i documenti più recenti dell'AIEA (ad es. Safety Standards e IAEA Nuclear Security Series) è infatti contenuta una clausola generale secondo cui i provvedimenti di sicurezza interna («safety») e i provvedimenti di sicurezza esterna («security») devono essere concepiti e attuati in modo integrato, affinché i provvedimenti di sicurezza esterna non pregiudichino la sicurezza interna (cfr. International Atomic Energy Agency, Fundamental Safety Principles, No. SF-1, Vienna 2006, paragraph 1.10).

In questo contesto il team internazionale di esperti ha constatato che la distinzione degli aspetti della sicurezza interna e della sicurezza esterna viene applicata correttamente dall'IFSN nella pratica, ma che manca un disciplinamento esplicito a livello di legge o di ordinanza. I provvedimenti di protezione sono descritti nell'articolo 5 del capitolo 2 «Principi della sicurezza nucleare» della LENu. I provvedimenti relativi alla sicurezza interna e quelli relativi alla sicurezza esterna sono descritti in capoversi separati, rispettivamente nel cpv. 1 e 2 e nel cpv. 3, ma non viene stabilito alcun collegamento tra questi

³ Direttiva IFSN-G22 sulla sicurezza informatica negli impianti nucleari («Richtlinie ENSI-G22, IT-Sicherheit in Kernanlagen»), edizione dicembre 2019 (non pubblicata).

due aspetti. Nell'OENu i requisiti in materia di sicurezza interna sono disciplinati nell'articolo 7 e i requisiti in materia di sicurezza esterna nell'articolo 9, senza alcun riferimento reciproco. Anche l'articolo 10 non fornisce alcuna indicazione in merito alla distinzione tra sicurezza interna e sicurezza esterna.

Una normativa giuridica che disciplini l'interfaccia tra sicurezza nucleare interna e sicurezza nucleare esterna, che preveda una visione integrata dei provvedimenti in entrambi gli ambiti ed eviti che si pregiudichino reciprocamente, aiuta la Svizzera ad adempiere alle proprie responsabilità e a esercitare la propria vigilanza in linea con l'approccio condiviso a livello internazionale nel settore nucleare. Un tale approccio è inoltre conforme alla prassi internazionale.

Art. 30 cpv. 4

La crescente digitalizzazione degli impianti nucleari ha aumentato significativamente l'importanza della sicurezza informatica. Tale tendenza proseguirà anche nei prossimi anni. Nella prassi, gli esercenti di impianti nucleari hanno già creato adeguate strutture organizzative e predisposto le necessarie risorse umane per definire con chiarezza le responsabilità nell'ambito della sicurezza informatica. La presente modifica dell'articolo 30 capoverso 4 OENu tiene conto di tale situazione, conferendo una base legale alla prassi esistente e apportando così un importante contributo al rafforzamento della sicurezza nucleare interna ed esterna.

Art. 36 cpv. 1, art. 62 cpv. a, all. 5

Secondo il team internazionale di esperti, l'impiego dei termini «sicurezza interna» e «sicurezza esterna» nelle disposizioni giuridiche non è sempre chiaro né coerentemente delimitato nei singoli articoli. Alla luce di tale lettura, il tenore delle disposizioni lascia un certo margine interpretativo e può dar luogo a una comprensione diversa, di conseguenza, a potenziali incertezze giuridiche. Si raccomanda pertanto di distinguere sistematicamente i termini nelle disposizioni pertinenti e di utilizzarli correttamente.

Ai fini di una maggiore precisione, il termine «sicurezza esterna» è aggiunto all'articolo 36 capoverso 1, all'articolo 62 lettera a e all'allegato 5 in relazione al rapporto mensile, poiché tali disposizioni riguardano entrambi gli aspetti, ossia sia la sicurezza interna che la sicurezza esterna.

Secondo l'articolo 36 capoverso 1, il titolare di una licenza d'esercizio è tenuto a seguire le conoscenze acquisite mediante la ricerca per quanto concerne la sicurezza esterna del proprio impianto.

In caso di domanda di un'autorizzazione di massima per un deposito in strati geologici profondi, il richiedente deve presentare un rapporto secondo l'articolo 62 che consideri anche l'aspetto della sicurezza esterna in riferimento alle opzioni disponibili. La documentazione relativa alla domanda da presentare conformemente all'articolo 23 OENu, cui si rinvia nella frase introduttiva, comprende anche un rapporto relativo alla sicurezza esterna (art. 23 lett. a).

Secondo l'allegato 5, nel rapporto annuo sulla sicurezza degli impianti nucleari devono essere trattati sia l'aspetto della sicurezza interna che quello della sicurezza esterna. Di conseguenza, anche nel rapporto mensile delle centrali nucleari sull'esercizio dell'impianto devono essere considerati entrambi gli aspetti. Nella pratica, il rapporto mensile comprende già oggi alcuni aspetti relativi alla sicurezza esterna. Inoltre viene apportata una correzione all'ultimo periodo della riga concernente il rapporto mensile della versione francese dell'ordinanza.