Appendice integrativa – Norma di certificazione: ISO/IEC 42001:2023

Edizione: Marzo 2024

CAPITOLO 1 - GENERALITÀ

Nella presente Scheda sono definite le procedure supplementari e/o sostitutive, applicate da RINA per la certificazione di sistemi gestione dell'Intelligenza Artificiale (AIMS), rispetto a quanto già definito nel Regolamento per la certificazione di sistemi di gestione RC/C 40.

RINA rilascia la certificazione in accordo ai requisiti delle norme ISO/IEC 17021-1:2015 ed ISO/IEC DIS 42006 ad Organizzazioni il cui Sistema di Gestione sia stato riconosciuto conforme a tutti i requisiti previsti dalla norma:

ISO/IEC 42001:2023

CAPITOLO 2 - NORMA DI RIFERIMENTO / REQUISITI PER LA CERTIFICAZIONE

Oltre a quanto stabilito dal "Regolamento per la certificazione di Sistemi di Gestione" RC/C 40, per ottenere la certificazione da parte di RINA, un Sistema di Gestione per l'Intelligenza Artificiale deve soddisfare inizialmente e nel tempo i requisiti della ISO/IEC 42001:2023, quelli aggiuntivi previsti dagli Organismi di Accreditamento per lo schema AIMS, ed i documenti applicabili pubblicati dallo IAF (esempio: IAF MD01, ecc…).

CAPITOLO 3 - CERTIFICAZIONE INIZIALE

In aggiunta a quanto definito nel "Regolamento per la certificazione di Sistemi di Gestione" RC/C 40 e nelle "Condizioni generali di contratto per le attività di valutazione della conformità", si applica quanto segue.

Le Organizzazioni che desiderino ottenere la certificazione del loro Sistema di Gestione per l'IA devono inviare a RINA, oltre al modulo "Questionario Informativo", anche lo specifico "Allegato al questionario informativo per offerta ISO/IEC 42001 (AIMS)", disponibile sul sito www.rina.org, compilato in tutte le sue parti.

In particolare, l'Allegato al Questionario informativo richiede che siano fornite informazioni su:

- Ruolo dell'Organizzazione rispetto all'Intelligenza Artificiale (Producer, Developer, Provider, User, o combinazione di questi)
- Settore di attività per cui è utilizzata l'Intelligenza Artificiale
- Contesto legislativo in cui è utilizzata l'Intelligenza Artificiale
- Complessità dei dati gestiti dall'AIMS
- Complessità tecnologica dell'infrastruttura IT
- Utilizzo di outsourcing
- Trattamento di informazioni riservate
- Percentuale di persone che svolgono attività identiche

Queste informazioni devono pervenire da un rappresentante autorizzato dell'organizzazione richiedente.

Se il Sistema di Gestione per l'IA comprende documentazione (procedure, registrazioni, ecc.) classificata come "riservata" e/o comunque non disponibile ai fini della certificazione, RINA valuterà la sussistenza delle condizioni per poter proseguire l'iter di certificazione, rifiutando l'incarico qualora non sia in grado di ottemperare agli obblighi di riservatezza per il proprio personale utilizzato.

Per la definizione dei tempi di audit per la certificazione iniziale, le sorveglianze e la ricertificazione, si fa riferimento alla

norma ISO/IEC DIS 42006 (Tabelle A.1 ed A.2).

Prima dell'audit di certificazione, RINA e l'Organizzazione stabiliscono di comune accordo le azioni necessarie (contrattuali, operative e tecniche) da attuare affinché l'audit fornisca a RINA tutte le informazioni e le prove necessarie per la certificazione. Ciò può includere l'accesso al codice sorgente e ai dati "raw". In particolare, RINA e l'Organizzazione stabiliscono nell'accordo di certificazione e attuano reciprocamente eventuali misure specifiche di salvaguardia per le informazioni protette o sensibili, la proprietà intellettuale, i segreti commerciali, i mezzi tecnici e le infrastrutture da utilizzare.

Nel corso dello stage 1, tutti i processi coperti dall'AIMS collegati alle peculiarità regionali e normative devono essere censiti e valutati, al fine di consentire una selezione adeguata e orientata al rischio dei test funzionali da svolgere in stage 2.

Qualora il sistema di gestione AIMS sia integrato con altri sistemi di gestione (es.: ISO 9001, ISO/IEC 27001), RINA dovrà accertare la presenza di interfacce fra di essi, che assicurino la consistenza dei controlli implementati.

Se, per esigenze dell'Organizzazione, la certificazione del sistema di gestione AIMS deve essere utilizzata per l'accettazione secondo ISO/IEC 17065 come parte di una certificazione di prodotto, servizio o processo, devono essere prelevati campioni rappresentativi come parte dello stage 2.

CAPITOLO 4 - MANTENIMENTO DELLA CERTIFICAZIONE

In aggiunta a quanto definito nel "Regolamento per la certificazione di Sistemi di Gestione" RC/C 40 e nelle "Condizioni generali di contratto per le attività di valutazione della conformità", si applica quanto segue.

Nell'ambito degli audit di sorveglianza, RINA esamina la documentazione su eventuali ricorsi e reclami ricevuti. Nei casi di non conformità identificate e requisiti non soddisfatti, RINA verifica che il cliente abbia indagato sul proprio AIMS, e abbia adottato azioni correttive adeguate.

Il rapporto di audit di sorveglianza includerà anche informazioni sulla risoluzione delle non conformità precedentemente rilevate, nonché la versione della Dichiarazione di Applicabilità (SoA) e i cambiamenti significativi rispetto all'ultimo audit.

CAPITOLO 5 - RICERTIFICAZIONE

In aggiunta a quanto definito nel "Regolamento per la certificazione di Sistemi di Gestione" RC/C 40 e nelle "Condizioni generali di contratto per le attività di valutazione della conformità", si applica quanto segue.

In occasione dell'audit di ricertificazione del Sistema di Gestione, previsto ogni tre anni, l'Organizzazione deve inviare a RINA, oltre al modulo "Questionario Informativo", anche lo specifico "Allegato al questionario informativo per offerta ISO/IEC 42001 (AIMS)", disponibile sul sito www.rina.org, compilato in tutte le sue parti come descritto al punto 3 del presente regolamento.

CAPITOLO 6 - ESECUZIONE DEGLI AUDIT

In aggiunta a quanto definito nel "Regolamento per la certificazione di Sistemi di Gestione" RC/C 40 e nelle "Condizioni generali di contratto per le attività di valutazione della conformità", si applica quanto segue.

Il tempo di audit on site non può essere inferiore al 70% del tempo totale di audit oggetto di offerta.

CAPITOLO 7 -GESTIONE DEI CERTIFICATI DI CONFORMITA'

In aggiunta a quanto definito nel "Regolamento per la certificazione di Sistemi di Gestione" RC/C 40 e nelle "Condizioni generali di contratto per le attività di valutazione della conformità", si applica quanto segue.

Il certificato di conformità ISO/IEC 42001 è predisposto in conformità all'Annex B della norma ISO/IEC DIS 42006. In particolare, esso riporta le informazioni riguardanti la "Dichiarazione di Applicabilità" ("Statement of Applicability") predisposta dall'Organizzazione.

CAPITOLO 8 - MODIFICA DELLA CERTIFICAZIONE E COMUNICAZIONE CAMBIAMENTI

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40 e quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

CAPITOLO 9 - PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40.

CAPITOLO 10 - TRASFERIMENTO DI CERTIFICATI ACCREDITATI

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40.

CAPITOLO 11 - SOSPENSIONE, RIPRISTINO E REVOCA DELLA CERTIFICAZIONE

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40 e quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".

CAPITOLO 12 - RINUNCIA ALLA CERTIFICAZIONE

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40.

CAPITOLO 13 - CONDIZIONI CONTRATTUALI

Si applica quanto definito nel Regolamento per la certificazione di Sistemi di gestione RC/C 40 e quanto previsto dalle "CONDIZIONI GENERALI DI CONTRATTO PER LA CERTIFICAZIONE DI SISTEMI, PRODOTTI E PERSONALE".