



**ISTITUTO
ITALIANO DI
TECNOLOGIA**

| |
|--|
| <p>Procedura per l'acquisizione di beni e servizi in ambito ICT</p> |
|--|

| Revisione | Descrizione Modifica | Autore | Approvazione | Data |
|-----------|----------------------|--------|--------------|------------|
| 01 | Prima versione | ICT | S.D. D.G. | 20/05/2020 |

SOMMARIO

| | | |
|------|--|----|
| 1. | Obiettivi e finalità | 3 |
| 2. | Premessa e definizioni | 3 |
| 2.1. | Premessa | 3 |
| 2.2. | Definizioni | 4 |
| 3. | Principali attori e responsabilità | 4 |
| 4. | Documenti e strumenti | 5 |
| 5. | Acquisizione di beni e servizi | 6 |
| 6. | Flow chart | 10 |
| 7. | Allegati | 11 |

1. OBIETTIVI E FINALITÀ

Oggetto della presente Procedura è la gestione dell'acquisizione di beni e servizi in ambito ICT.

Ai soli fini della presente procedura, per beni e servizi in ambito ICT si intendono:

- applicativi software da installare sui sistemi della Fondazione o su sistemi esterni (cloud), avente licenza d'uso permanente o temporanea;
- servizi di sviluppo di nuovo codice o di modifica di codice esistente;
- servizi di supporto e manutenzione.

Ai soli fini della presente procedura, inoltre, per gestione dell'acquisizione si intende il processo relativo alla:

- valutazione preliminare del bene o del servizio;
- gestione degli aspetti di sicurezza informatica all'interno dei requisiti contrattuali per la fornitura del bene o servizio.


Destinatario della presente Procedura è il personale delle Direzioni/Uffici dell'Amministrazione Centrale nonché delle Linee di Ricerca e Facilities.

2. PREMESSA E DEFINIZIONI

2.1. Premessa

I beni e i servizi in ambito ICT della Fondazione costituiscono uno dei punti di forza di quest'ultima e occorre pertanto garantirne uno sviluppo e una gestione improntata a principi di efficacia ed efficienza; inoltre, allo stesso tempo, possono essere fonte di rischio per la sicurezza delle informazioni trattate e per l'immagine della Fondazione. Per questo motivo, la Fondazione intende assicurare che le iniziative di acquisizione di beni e servizi in ambito ICT siano aderenti alla strategia ICT della Fondazione, siano efficaci e sostenibili nel tempo e rispondano a requisiti di sicurezza coerenti con le esigenze della Fondazione stessa e con la normativa vigente. È necessario inoltre che la introduzione di nuovi sistemi e applicazioni risponda a criteri di economicità e sia ricondotta ad un quadro omogeneo di sviluppo.

A tal proposito, annualmente ICTD riceve da MCD il dettaglio estratto dal budget in fase di approvazione sulle spese per investimenti e costi di ambito ICT, al fine di programmare opportunamente le attività di supporto al processo di approvvigionamento e di gestione dei progetti di implementazione.


| | | |
|--|---------------------------------|----------|
|  ISTITUTO ITALIANO DI TECNOLOGIA | Acquisizione beni e servizi ICT | IO IT 06 |
|--|---------------------------------|----------|

2.2. Definizioni

| Nome | Sigla | Descrizione |
|----------------------------|-------|---|
| Utente | UT | Chiunque abbia un rapporto di lavoro dipendente, di collaborazione e il personale esterno affiliato alla Fondazione IIT che svolge attività di ricerca scientifica, professionale o di studio all'interno delle strutture di IIT. |
| Referente ICT | | Figura tecnica che ha in carico la gestione di sistemi ICT non gestiti direttamente dalla Direzione ICT. |
| Dati Personali | D.P. | Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. |
| Responsabile del Contratto | | È il responsabile della sottoscrizione del singolo atto, contratto o procedimento. |
| Rischio | | Eventualità di subire un danno connessa a circostanze più o meno prevedibili. |
| Request for Information | RFI | Indagine di mercato aperta, volta alla ricerca di dati generali che consentano una comprensione del fenomeno. |
| Request for Quotation | RFQ | Richiesta di offerta commerciale. |

3. PRINCIPALI ATTORI E RESPONSABILITÀ

| Attore | Sigla | Maggiori responsabilità |
|----------------------------|-------|--|
| Direzione ICT | ICT | Definire le misure di sicurezza da adottare per le diverse categorie di fornitori; definire, col supporto della Direzione Acquisti, le categorie di beni o servizi; supportare il responsabile del contratto nell'individuazione delle misure di sicurezza e nella valutazione delle risposte dei fornitori in merito alle misure di sicurezza implementate. |
| Amministrativi | | Verificare l'inserimento dell'allegato B in fase di acquisto. |
| Direzione Affari Legali | | Fornire supporto in ambito data protection laddove il bene o servizio ICT preveda il trattamento di dati personali. |
| Responsabile del contratto | | Individuare la categoria di classificazione del rischio dei dati e identificare le misure di sicurezza specifiche per l'acquisto. |
| Referente ICT | | Supportare il responsabile del contratto nell'individuazione delle misure di sicurezza. |
| Direzione MC | MCD | MCD comunica a ICTD il dettaglio dello stanziamento su budget per costi e investimenti di ambito ICT |

| | | |
|--|---------------------------------|----------|
|  ISTITUTO ITALIANO DI TECNOLOGIA | Acquisizione beni e servizi ICT | IO IT 06 |
|--|---------------------------------|----------|

4. DOCUMENTI E STRUMENTI

| Tipo | Nome | Utilizzo | Link |
|----------------------|--|---|---|
| Policy | Policy di sicurezza delle informazioni | Definisce le regole per l'utilizzo sicuro del sistema informativo della Fondazione IIT, compresa la classificazione delle informazioni. | https://short.iit.it/information-security-policy |
| Allegato alla Policy | Esempi di classificazione dei rischi delle Informazioni | Riporta esempi di valutazione dei rischi di sicurezza per le informazioni. | https://short.iit.it/risk-classification |
| Allegato alla Policy | Misure per la sicurezza delle informazioni | Riporta l'elenco delle misure di sicurezza da implementare sulla base della classificazione del livello di rischio della sicurezza delle informazioni dei sistemi ICT della Fondazione. | https://short.iit.it/information-security-measures |
| Allegato alla policy | Sistemi ICT approvati per livello di rischio di sicurezza delle informazioni | Riporta un elenco di sistemi ICT della Fondazione ed il livello di rischio della sicurezza delle informazioni per il quale ne è approvato l'uso. | https://short.iit.it/approved-services |

5. ACQUISIZIONE DI BENI E SERVIZI

L'acquisizione di beni e servizi ICT della Fondazione deve essere effettuata in conformità con tutte le relative Policy e Procedure di Acquisto della Fondazione.

Nello specifico, per i beni e servizi ICT di cui alla presente procedura, è necessario mettere in atto una fase di valutazione preliminare tesa a verificare che l'acquisto sia effettuato in coerenza con le iniziative strategiche della Fondazione come dettagliate nel paragrafo 5.1.

Successivamente è richiesta una valutazione del rischio associato ai dati gestiti utile alle attività precontrattuali come indicato nel paragrafo 5.2.

Infine, nella successiva fase di contrattualizzazione (paragrafo. 5.3), si dovrà garantire che siano inserite, ove applicabile, le adeguate misure di sicurezza all'interno delle condizioni speciali di acquisto (nel caso di affidamenti diretti) o nei capitolati tecnici (nel caso di procedure di gara).

5.1 Valutazione preliminare

L'acquisizione di beni e servizi in ambito ICT dev'essere effettuata in coerenza con le iniziative strategiche della Fondazione garantendo, quanto più possibile, la non duplicazione di beni e servizi esistenti e seguendo i principi di economicità ed efficientamento delle risorse della Fondazione.

Nel completo rispetto dell'autonomia garantita alle Direzioni dell'Amministrazione Centrale, alle Linee di ricerca e allea Facilities, la Direzione ICT, e ove necessario con il coinvolgimento di DG e DS, provvederà ad eseguire una valutazione preliminare dell'acquisto del bene o del servizio richiesto, sin dalle sue fasi progettuali, atta a garantire che:

- la roadmap di realizzazione ipotizzata sia compatibile con il contributo richiesto alla Direzione ICT ed alle altre Funzioni coinvolte nell'implementazione del bene o servizio stesso;
- La gestione dello sviluppo, del rilascio e della gestione in esercizio e manutenzione delle applicazioni sia economicamente sostenibile secondo le risorse disponibili e i vincoli imposti dalle normative interne ed esterne alla Fondazione; in tal senso i richiedenti avranno cura di indicare:
 - quali sono i benefici (tangibili ed intangibili) che derivano alla Fondazione a fronte dei costi di sviluppo e di esercizio delle applicazioni richieste;
 - in che modo si intende finanziare i costi relativi (p.es. Riduzione di altre voci di budget, richiesta di incrementi nella dotazione, overhead di progetti esterni, ecc.);
- le componenti tecnologiche, siano esse on-premise o cloud, che compongono il bene o servizio richiesto, non siano ridondanti e siano compatibili e sostenibili con il resto delle tecnologie presenti in IIT;

- siano garantiti gli aspetti di sicurezza informatica e data protection in conformità alle procedure e alle policy della Fondazione e alle normative vigenti.

Per le Linee di ricerca o le Facility, al fine di garantire la massima autonomia nello svolgimento dell'attività di ricerca, la fase di valutazione di cui sopra verrà fatta solo nei casi in cui i beni o i servizi che si intendono acquisire prevedano:

- Integrazione con i sistemi gestionali della Fondazione
- Ridondanza funzionale rispetto a beni/servizi già esistenti
- Complessità realizzativa e operativa particolarmente elevata che richiede il contributo della Direzione ICT

Per rendere esecutivo quanto sopra descritto, le Direzioni/Uffici dell'Amministrazione Centrale nonché le Linee di Ricerca e Facilities dovranno compilare il questionario presente nell'allegato A ai fini della raccolta delle informazioni con l'obiettivo di guidare il richiedente nelle fasi successive. La Direzione ICT si impegna a fornire un primo riscontro entro 15 giorni di calendario dalla ricezione dello stesso.

5.2 Conformità alle misure di sicurezza nelle attività precontrattuali

Nella fase precontrattuale di selezione del fornitore o di un soggetto terzo e nelle successive interazioni è di fondamentale importanza considerare esplicitamente i requisiti di sicurezza pertinenti così come derivabili dall'insieme di controlli, inclusi negli Allegati B1, B2, B3, che sono derivati secondo la classificazione del rischio sui dati come richiesto dalla P26 Policy di Sicurezza delle Informazioni adottata dalla Fondazione.

Nella selezione di un fornitore, ad esempio è utile tenere in considerazione l'eventuale disponibilità di certificazioni di sicurezza riconducibili all'ambito ed al perimetro del bene o prodotto di interesse nonché la sua capacità di indirizzare i temi di sicurezza indicati al fine di facilitare l'inserimento dei temi medesimi nei documenti contrattuali.

Qualora i dati trattati comprendano dati personali, la valutazione sarà svolta secondo le procedure e le policy adottate dalla Fondazione in conformità alla logica della data protection by design indicata nel GDPR.

Più in generale, il rispetto di tali requisiti dovrà essere compreso, nelle modalità di volta in volta più opportune:

- nell'ambito di attività di RFI/RFQ;
- nell'ambito della predisposizione della documentazione tecnica di bandi di gara;
- la responsabilità di assicurare l'adeguata valutazione dei requisiti, salvo nelle situazioni altrimenti normate dal codice degli appalti e relative policies e procedure della Fondazione, è in capo al Responsabile del Contratto, che a seconda dei casi Dove possibile e opportuno, i potrà avvalersi

del supporto della Direzione ICT o della Direzione Affari Legali (quest'ultima laddove il bene o servizio ICT preveda il trattamento di dati personali) .

- La documentazione relativa a queste valutazioni sarà acquisita e conservata dalla Direzione ICT.

Qualora condizioni oggettive prevedano la mancata adozione delle misure di sicurezza richieste, sentito il parere della Direzione ICT, dovrà essere verificata la possibilità di inserire misure compensative atte a garantire comunque:

- il rispetto di eventuali vincoli imposti dalle normative interne ed esterne alla Fondazione;
- la protezione del sistema informativo della Fondazione.

La Direzione ICT, qualora non ritenga adeguate tali misure compensative, potrà comunque richiedere o attuare opportune misure tecniche atte a salvaguardare il sistema informativo della Fondazione.

5.3 Requisiti di sicurezza per la fase di contrattualizzazione


L'insieme dei requisiti individuati nelle fasi precedenti e contenuti negli allegati B1, B2 e B3 dovranno essere inclusi direttamente fra le clausole contrattuali. Sarà compito del Responsabile del Contratto, di concerto con la Direzione ICT o con il referente ICT, indicare alla Direzione Acquisti le informazioni necessarie da inserire nella documentazione contrattuale.

Dove possibile e opportuno, i requisiti saranno corredati da SLA (Service Level Agreement), KPI (Key Performance Indicator), modalità di audit od altre azioni previste al fine di verificarne il rispetto da parte del fornitore.

Nell'acquisizione di beni o servizi ICT, i requisiti dovranno comprendere sempre:

- che il fornitore richieda contrattualmente ad eventuali sub-fornitori di operare secondo gli stessi standard e requisiti di sicurezza delle informazioni e protezione dei dati previsti per il fornitore stesso;
- la possibilità per la Fondazione di svolgere attività di audit sul fornitore ed i suoi eventuali sub-fornitori, nel perimetro rilevante per i beni e servizi forniti, o di richiedere un audit di terza parte o un rapporto di audit che la Fondazione stessa ritenga adeguato a soddisfare i propri requisiti di monitoraggio e controllo;
- l'obbligo di notificare alla Fondazione eventuali incidenti di sicurezza che interessino i dati della Fondazione stessa, nonché il supporto alla gestione efficace ed al contenimento di eventuali incidenti di sicurezza che interessino i dati stessi;
- le modalità di restituzione o cancellazione dei dati della Fondazione al termine del rapporto contrattualizzato.

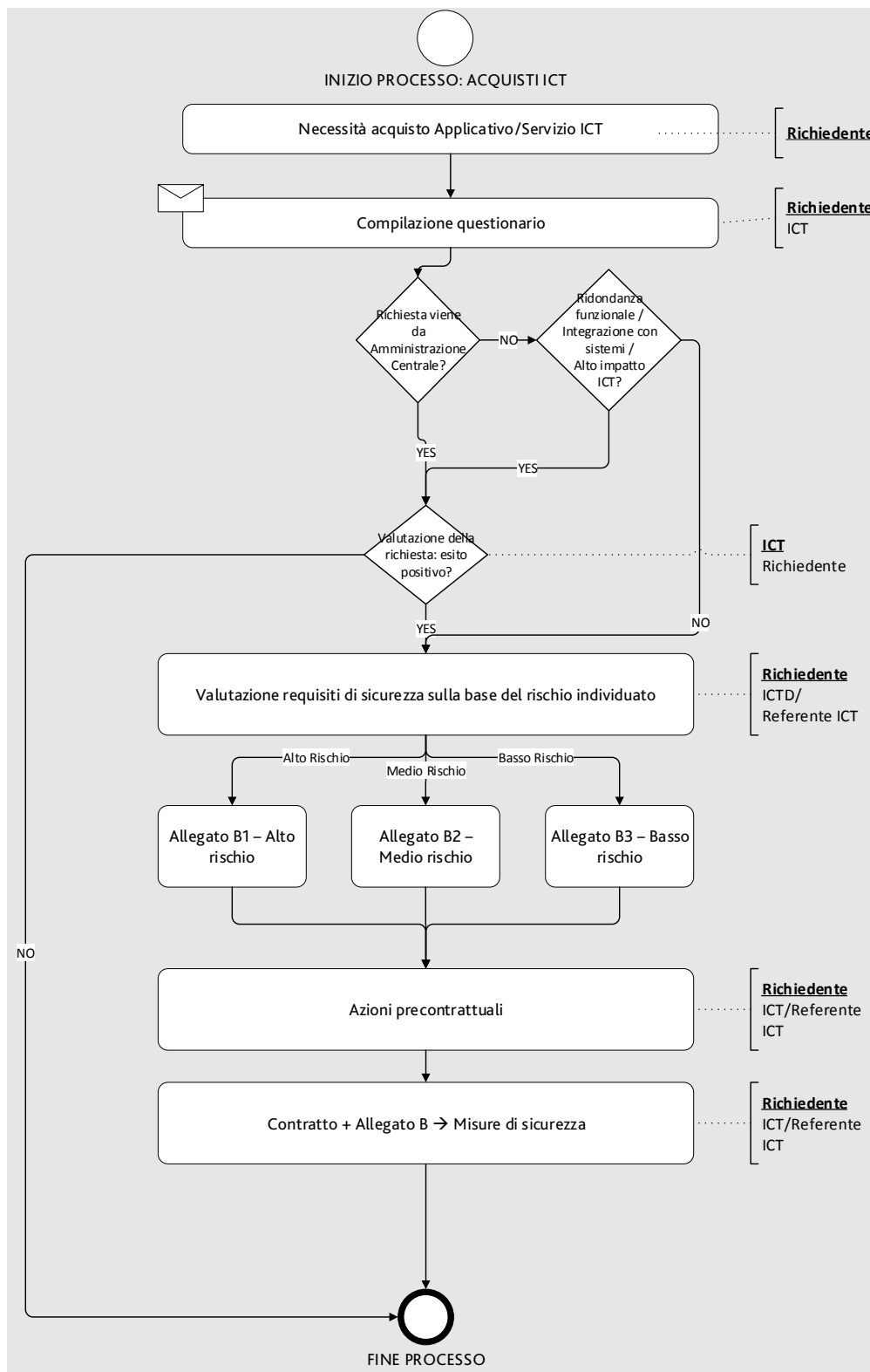
In aggiunta ai requisiti sopra indicati, chi richiede l'acquisizione del bene o servizio dovrà individuare eventuali ulteriori misure di sicurezza specifiche da contrattualizzare. Eventuali deroghe alle misure di sicurezza indicate dovranno essere motivate e documentate, e dovranno essere preventivamente approvate dalla Direzione ICT. Chi richiede l'acquisizione del bene o servizio dovrà, inoltre, indicare se attraverso il bene o servizio è previsto il trattamento di dati personali, ed in questo caso dovranno essere


| | | |
|--|---------------------------------|----------|
|  ISTITUTO ITALIANO DI TECNOLOGIA | Acquisizione beni e servizi ICT | IO IT 06 |
|--|---------------------------------|----------|

fornite tramite il supporto della Direzione Affari Legali le eventuali informazioni aggiuntive secondo le procedure e le policy adottate dalla Fondazione in conformità alla logica di data protection by design e di qualificazione e gestione terze parti (IO LO 09).

Il contratto dovrà, inoltre, indicare che il rispetto dei requisiti indicati non esime il fornitore dal rispetto di ogni ulteriore requisito di sicurezza definito in particolare dagli articoli 28 e 32 del GDPR.

6. FLOW CHART



| | | |
|--|---------------------------------|----------|
|  ISTITUTO ITALIANO DI TECNOLOGIA | Acquisizione beni e servizi ICT | IO IT 06 |
|--|---------------------------------|----------|

7. ALLEGATI

Di seguito in allegato:

- ALLEGATO A. Il Questionario che racchiude le domande preliminari per una valutazione a monte dell'acquisizione di prodotti e servizi ICT.
- ALLEGATO B. Il modello di allegato contrattuale comprendente le misure di sicurezza estratte dalla norma Standard ISO 27001:2013 che delineano i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni e includono aspetti relativi alla sicurezza logica, fisica ed organizzativa:
 - B.1: misure di sicurezza per applicazioni ad alto rischio
 - B.2: misure di sicurezza per applicazione a medio rischio
 - B.3: misure di sicurezza per applicazioni a basso rischio

| Titolo documento | Allegato |
|---|---|
| Allegato A – Questionario | https://forms.iit.it/view.php?id=261742 |
| Allegato B – Modello di allegato contrattuale | Allegato - B.1 - Misure di Sicurezza (Alto Rischio) Allegato - B.2 - Misure di Sicurezza (Medio Rischio) Allegato - B.3 - Misure di Sicurezza (Basso Rischio) |