A00097

CAPITOLATO TECNICO

ACQUISIZIONE SERVIZIO IN SAAS PER SOLUZIONE INFORMATICA DI GOVERNANCE RISK E COMPLIANCE (GRC)

CINECA - ***Consorzio Interuniversitario***

Sede legale amministrativa e operativa: via Magnanelli n. 6/3 - 40033 Casalecchio di Reno (BO)

C.F. 00317740371 - P. IVA 00502591209

Tel. +39 051.6171411 - Fax +39 051.2130217 - e-mail agbs@cineca.it - PEC agbs@pec.cineca.it

Altre sedi operative:

C.so G. Garibaldi, 86 - 20121 Milano (MI) Tel. +39 02.269951

Via dei Tizi, 6/B - 00185 Roma Tel. +39 06.444861

Via Medina, 40 - 80133 Napoli Tel. +39 081.5593711

INDICE

1. Oggetto dell'appalto

L'oggetto dell'appalto è l'acquisizione di un **servizio in cloud qualificato SaaS su infrastruttura all'interno della Comunità Europea**, per la gestione di tutte le principali funzioni e attività di **risk management, compliance e audit**.

Il servizio dovrà comprendere i seguenti moduli, meglio descritti nell'articolo 3:

- Risk Management;
- Audit Management;
- Compliance Management.

e le seguenti integrazioni, meglio descritte negli articoli successivi:

- Integrazione con SSO dell'organizzazione via IDEM, via LDAP o Identity provider.
- Integrazione con la soluzione CINECA relativa alle , strutture organizzative;
- Integrazione con il sistema di "ticketing" utilizzato internamente da CINECA per la registrazione delle attività di followup a seguito degli audit.

Nel seguito vengono adottate le seguenti convenzioni:

Stazione Appaltante	Si intende il Consorzio Interuniversitario CINECA che è il Committente del servizio.
Fruitori	Si intendono gli utenti CINECA.
Esecutore	Si intende il soggetto a cui verrà affidata la fornitura in oggetto e che dovrà fornire tutti i servizi qui descritti.
Sistema o Soluzione	Soluzione GRC in modalità SaaS

2. Caratteristiche del Servizio

È interesse del consorzio CINECA dotarsi di un sistema informatico Governance Risk Compliance (GRC) per la gestione del proprio Sistema di Controllo Interno e Gestione dei Rischi (SCIGR), che metta in relazione le varie componenti del Sistema, quali: le normative a cui è assoggettato Cineca, gli standard volontari adottati, i rischi e i relativi controlli, i processi e le strutture organizzative, attraverso l'implementazione del framework di riferimento "COSO Enterprise Risk Management – Integrated Framework" (COSO-ERM).

La fornitura deve prevedere:

- erogazione del servizio GRC in modalità SaaS;
- configurazione del servizio GRC con le impostazioni di CINECA;
- integrazione coi sistemi CINECA (applicazione CINECA di gestione delle strutture organizzative e sistema di tracciamento JIRA)
- formazione agli utenti finali di CINECA;
- supporto utenti sul prodotto a favore del personale CINECA;
- manutenzione correttiva del servizio GRC.

3 Requisiti Funzionali

Di seguito è riportato un quadro riassuntivo delle principali funzionalità attese, suddivise per ambito.

Configurazione

Il servizio GRC deve consentire una flessibilità nella configurazione, in particolare:

1) le interfacce utente delle forms delle principali funzioni devono essere configurate in base ai profili di utilizzo del sistema (es. le label dei campi e i campi presenti nella form);
2) il menu delle funzioni disponibili nel sistema deve essere configurabile sulla base delle entità gestite da CINECA e dai profili utenti;
3) la definizione dei processi di self assessment deve essere configurabile sulla base del tipo di assessment richiesto;
4) creazione di reportistica sulla base delle esigenze del CINECA.

Risk Management

Il servizio GRC deve supportare:

1) la gestione di una libreria dei rischi, ovvero la creazione dei rischi e la loro modifica/cancellazione, consentendo di definire delle categorie di rischio, il proprietario del rischio, il livello di tolleranza del rischio, gli eventi per i quali si può manifestare il rischio, e delle gerarchie di rischi con almeno tre livelli. Il rischio deve poter essere associato a una o più entità quali: unità organizzativa, processo aziendale, normativa o standard volontario, IT asset, obiettivo strategico, obiettivo operativo e controlli;
2) il "risk assessment" mediante sia la compilazione di una "form" per la valutazione diretta del rischio, che una eventuale compilazione di un questionario per il "self assessment". Durante il "risk assessment", per ogni rischio deve essere possibile definire il rischio accettabile, inerente, rischio residuo e le azioni o i controlli di mitigazione del rischio. Il valore del rischio deve essere calcolato come Impatto per Probabilità o con altro metodo equivalente, che possa essere configurato dalla funzione di risk manager o da una funzione equivalente. La rilevanza del livello di rischio (severity/risk matrix) deve essere configurabile

dalla funzione di risk manager o da una funzione equivalente. Il "risk assessment" deve prevedere di tracciare l'utente che ha valutato il rischio (es. il capo ufficio) e un approvatore del "risk assessment" (es. il Direttore/Responsabile dell'area);

3) la gestione di una libreria dei controlli, ovvero la creazione dei controlli di mitigazione dei rischi e la loro modifica/cancellazione, consentendo di definire il proprietario del controllo e delle tipologie di controlli. Il controllo deve poter essere associato a una o più entità quali: rischio, processo aziendale, procedura aziendale, normativa o standard volontario (requisito) e IT asset. I controlli possono essere valutati in termini di progettazione ed efficacia mediante autovalutazione o auditing da parte di un soggetto terzo;
4) la gestione della libreria dei processi, ovvero la definizione dei processi con le sotto attività e la loro modifica/cancellazione, consentendo di definire il proprietario del processo. Il processo deve poter essere associato a una o più entità quali: unità organizzativa, procedura aziendale, normativa o standard volontario, rischio, e controlli;
5) la gestione della libreria degli obiettivi strategici e operativi, ovvero la definizione degli obiettivi e la loro modifica/cancellazione, consentendo di definire il proprietario dell'obiettivo. L'obiettivo deve poter essere associato a una o più entità quali: unità organizzativa, normativa o standard volontario, rischio, e controlli (azioni di mitigazione);
6) la gestione della libreria degli asset aziendali (es. risorse IT), per la loro definizione modifica/cancellazione, consentendo la classificazione secondo standard descrittivi riconosciuti. Deve essere possibile raggruppare gli asset secondo diversi criteri (sede, tipologia, ecc.). L'asset aziendale deve poter essere associato a una o più entità quali: unità organizzativa, processo aziendale, standard volontario (es. UNI ISO 27001), rischio, e controlli.

Audit Management

Il servizio GRC deve supportare:

1) la gestione del programma annuale di audit mantenendo lo storico attraverso le seguenti attività:
    a. creare il programma di audit
    b. creare gli audit del programma
    c. approvare il programma di audit
    d. schedulare gli audit
    e. assegnare gli auditor agli audit
    f. generare una check list dei controlli da utilizzare in sede di audit ad esempio relativi ai rischi associati ad una normativa o standard volontario o a un processo;
    g. approvare il rapport di audit da parte del lead auditor e dai soggetti sottoposti agli audit
    h. inserire i rilievi emersi durante l'audit e la valutazione dei controlli in termini di efficacia e di adeguatezza;
    i. reporting sullo stato di esecuzione del programma di audit

2) la gestione dell'anagrafica dei singoli audit riportando le informazioni di riferimento quali ad esempio: lo scopo dell'audit, il responsabile dell'audit, il team di audit, la struttura sottoposta ad audit, lo stato, la data, ecc... L'audit deve poter essere associato a una o più entità quali: unità organizzativa, processo aziendale, procedura aziendale, normativa o standard volontario, rischio, obiettivo strategico, obiettivo operativo e controlli;
3) registrazione dei rilievi emersi nel corso degli audit.

Compliance Management

Il servizio GRC deve supportare:

1) la gestione di una libreria delle normative con inserimento degli articoli relativi ai reati presupposti, degli standard volontari con l'inserimento dei requisiti e delle "policy", ovvero la loro creazione e la loro modifica/cancellazione, consentendo alla funzione Compliance dell'azienda l'autonomia della gestione della libreria. La norma deve poter essere associata a una o più entità quali: unità organizzativa, processo aziendale, rischio, controlli e degli asset (per la ISO 27001);

Il servizio deve avere precaricato le seguenti norme e standard volontari:

a) D. Lgs 231/2001 con gli articoli relativi ai reati presupposti;
b) L. 190/2012 con gli articoli relativi ai reati attinenti alla legge;
c) Regolamento UE generale sulla protezione dei dati 2016/679 (GDPR) con gli articoli dei capi: II, III e V.
d) UNI ISO 27001 con i requisiti della norma.

Reportistica e cruscotti

Il servizio deve mettere a disposizione una funzione per degfinire report "su misura" e una serie di report predefiniti. In particolare, il servizio dovrà predisporre uno o più report (es. risk control matrix) che riporti i rischi associati a una normativa, o a uno standard volontario, o a un obiettivo strategico od operativo con i controlli applicati e la valutazione del rischio inerente e residuo.
I report prodotti sulla valutazione del rischio saranno utilizzati come parte integrante del Piano Triennale per la Prevenzione della Corruzione e Trasparenza (PTPCT) (L. 190/2012) secondo le linee guida ANAC e del Modello Organizzativo Gestionale 231 (D. Lgs. 231/2001).
La funzione di reportistica deve produrre la reportistica che la funzione di Internal Auditor deve presentare agli Organi di Governo (es. CDA) sulla valutazione dei rischi e dei controlli, anche con delle rappresentazioni di grafiche.
Deve inoltre mettere a disposizione una dashboard in cui evidenziare degli indicatori sulla situazione dei rischi (es. n. rischi per livello di gravità, risk rating con andamento storico), il livello di efficacia dei controlli e la situazione dell'attività di auditing.

Il servizio deve mettere a disposizione una serie di dashboard che consentano ai vari soggetti coinvolti nel sistema GRC, di avere un quadro preciso ed aggiornato della situazione dei rischi e dei rilievi emersi durante gli audit, nonché lo stato di avanzamento del piano annuale di audit. La dashboard dovrà presentare una visione di insieme della situazione dei rischi e dell'efficacia dei controlli ai responsabili delle strutture organizzative, alle funzioni di Internal Auditor, di Responsabile della Compliance, di Responsabile della Prevenzione della Corruzione, di Responsabile dei Dati Personali e agli Organi di Governo.

Gestione delle campagne

Il servizio deve consentire di generare questionari per la valutazione di diversi oggetti come rischi e controlli sulla base di quesiti e criteri/logiche di attribuzione del livello di valutazione definiti dall'utente.

Il servizio deve gestire le campagne mediante un sistema di "workflow" dove vengono configurati gli utenti che dovranno rispondere ai questionari, i livelli di approvazione, le tempistiche/fasi di somministrazione del questionario.

I risultati delle campagne in ambito della valutazione dei rischi e/o dei controlli devono essere riportati nella libreria dei rischi e/o dei controlli.

Utenti e Accesso al GRC

Il servizio deve prevedere la definizione di utenti con diritti autorizzativi diversi per tipologia di utenza.

Gli utenti previsti per il servizio sono:

Funzione/ruolo	**Profilo**	**N. utenti**
Internal Auditor	Gestisce la gestione del programma di audit e l'esecuzione degli audit. Definisce i questionari per il "self assessment" o intervista le strutture organizzative per la valutazione diretta dei rischi e/o dei controlli con apposita "form". Accedere ai report della valutazione rischi e controlli di tutta l'azienda.	1
Ufficio Compliance	Gestisce le anagrafiche, le librerie dei rischi e dei controlli. Gestisce l'anagrafica dei processi e delle sotto attività. Nell'ambito della Compliance, definisce i questionari per il "self assessment" o intervista	4

	le strutture organizzative per la valutazione diretta dei rischi e/o dei controlli con apposita "form". Accedere ai report della valutazione rischi e controlli.	
RPC – Responsabile prevenzione corruzione	Nell'ambito dell'anti corruzione, definisce i questionari per il "self assessment" o intervista le strutture organizzative per la valutazione diretta dei rischi e/o dei controlli con apposita "form". Accedere ai report della valutazione rischi e controlli.	1
RPD – Responsabile protezione dati	Nell'ambito del GDPR, definisce i questionari per il "self assessment" o intervista le strutture organizzative per la valutazione diretta dei rischi e/o dei controlli con apposita "form". Accedere ai report della valutazione rischi e controlli.	1
Direttore di Struttura	Partecipare all'analisi dei rischi e/o dei controlli mediante il "self assessment" o valutazione con apposita "form". Approvare il risultato dell'analisi dei rischi. Accedere ai report della valutazione rischi e controlli della struttura di appartenenza.	10
Responsabile di ufficio o area	Partecipare all'analisi dei rischi e/o dei controlli mediante il "self assessment" o valutazione con apposita "form. Accedere ai report della valutazione rischi e controlli della struttura di appartenenza.	15
Amministratore di sistema	Gestisce profili e accessi degli utenti al sistema.	1

Il servizio deve prevedere la possibilità di definire regole di accesso distinte per ogni funzione del sistema legate ai ruoli o funzioni organizzative. Deve essere possibile definire l'esecuzione di processi di "self assessment" in base ai ruoli o funzioni organizzative.

Integrazione con i sistemi CINECA per Strutture Organizzative, e di "ticketing"

Il servizio deve interfacciarsi con il sistema gestionale U-GOV di CINECA per il recupero, *near on line*, di organigramma delle strutture Organizzative e per consentire l'aggiornamento delle anagrafiche nell'eventualità di variazioni dell'organizzazione.

Integrazione con il sistema di "ticketing" Jira utilizzato internamente da CINECA per la registrazione delle attività di followup a seguito degli audit. Ovvero, da una registrazione nel sistema GRC di un rilievo in fase di audit il sistema deve aprire una "issue" nel sistema Jira e all'atto della chiusura della "issue" stessa riportare nel sistema GRC il n. della "issue", la data di chiusura e il trattamento attuato.

Integrazione con SSO aziendale

Il servizio dovrà essere integrabile con sistemi di autenticazione ed autorizzazione basati su tecnologie di single sign on (SAML e/o AUTH2) presenti in CINECA.

4. Requisiti tecnologici e di infrastruttura

Il servizio proposto deve essere per *default* in lingua italiana.

Deve essere pienamente rispondente alla normativa vigente europea e italiana in materia di protezione dei dati personali.

Si richiede le certificazioni dell'infrastruttura di erogazione del servizio alla norma ISO/IEC 27001, per i servizi Cloud erogati dall'Esecutore e in qualità di Cloud Service Provider, nei confronti del Committente in qualità di Cloud Service Customer.

La completa conduzione del servizio applicativo e della sottostante infrastruttura di erogazione, sia per gli ambienti di produzione che per gli eventuali ambienti di pre-produzione è a carico dell'Esecutore.

Requisiti di modularità

Rispetto a quanto richiesto nel precedente Art.3 "Requisiti Funzionali", le funzionalità della soluzione dovranno essere fornite da moduli integrati tra loro, affinché tutte le informazioni siano rese automaticamente disponibili tra i diversi moduli oltre che prevedere la massima rispondenza alle diverse esigenze di interoperabilità. La soluzione deve prevedere la fruizione di tutte le funzionalità utente da un unico ambiente integrato e disporre di un unico database integrato che ospiti tutti i dati gestiti.

Requisiti di usabilità e di accessibilità

Il sistema deve essere fruibile come "Web Application" e fornire interfacce utente di semplice utilizzo e complete, in cui ogni operatore coinvolto nel procedimento può trovare agevolmente tutte le informazioni di propria competenza.

Il sistema dovrà essere utilizzabile mediante tutti i più diffusi *web browser* senza richiedere interventi di installazione e di configurazione dei posti di lavoro; in particolare è richiesto il supporto per i browser Chrome, Firefox, Edge, Safari.

Interfacce per l'interoperabilità

La soluzione proposta dovrà comprendere una interfaccia di interoperabilità applicativa a servizi (API) opportunamente documentata e supportata che dovrà poter essere utilizzata per la realizzazione di integrazioni applicative con altri sistemi, anche al di fuori di quanto specificato nel presente capitolato. L'interfaccia a servizi dovrà consentire di effettuare tutte le operazioni e transazioni più importanti previste dal sistema.

Dovranno inoltre essere presenti opportune interfacce di caricamento dati da file per effettuare il caricamento massivo mediante procedure automatiche delle principali entità gestite.

Requisiti di sicurezza

Gestione dei profili di accesso utenti e privilegi

La piattaforma deve prevedere un sistema integrato di gestione di tutte le tipologie di utenze con la possibilità di operare per la creazione, modifica ed eliminazione di utenti.

Il servizio dovrà prevedere meccanismi di autenticazione, autorizzazione e profilatura per l'accesso alle funzionalità previste, ai dati e ai file trattati. L'accesso al servizio da parte dei vari utenti, per le diverse funzionalità disponibili, deve essere regolato mediante la creazione di adeguati profili con specifici privilegi.

Sicurezza e protezione dei dati personali, riservatezza

La soluzione deve garantire i requisiti di riservatezza, autenticità, integrità, disponibilità e non ripudio là dove richiesti. La soluzione proposta deve essere dotata di appositi sistemi di tracciamento e registrazione a livello di sistema (log applicativi) delle attività eseguite da tutti gli utenti del sistema siano essi interni o esterni, compresi gli utenti di amministrazione in accordo alla normativa vigente.

Nel caso di trattamento dei dati personali dovrà essere garantita la tutela e la riservatezza dei dati stessi in conformità con quanto disposto dalla normativa vigente, ivi comprese le relative misure di sicurezza previste dalla normativa vigente in materia di data protection, anche mediante l'adozione di idonee e preventive misure di

sicurezza, atte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Requisiti di infrastruttura tecnologica

L'Esecutore garantisce la sicurezza ed il costante aggiornamento delle tecnologie attraverso le quali eroga il servizio. A tal fine verrà valutata positivamente una descrizione precisa delle tecnologie e degli strumenti e procedure adottate per garantire la sicurezza del servizio.

L'Esecutore è chiamato a descrivere l'ambiente attraverso il quale viene erogato il servizio, compresi i meccanismi di backup e conservazione dei log ed eventuali modalità di accesso a dati o API, dichiarando la disponibilità giornaliera del servizio stesso, le contromisure pianificate in caso di indisponibilità del servizio ed i tempi massimi di riattivazione dello stesso in caso di grave incidente.

Il servizio web deve essere disponibile in cloud e deve essere erogato da una infrastruttura all'interno della Unione Europea.

Il servizio di SaaS dovrà sottostare ai livelli di servizio indicati nell'art. 7 "Livelli di servizio".

Disaster recovery

Il servizio SaaS erogato dall'Esecutore deve prevedere il servizio di *disaster recovery*. In particolare, dovranno essere esplicitate:

- la frequenza di copia dei dati (RPO – *Recovery Point Objective*);
- la ripartenza del servizio su sito di *disaster recovery* (RTO – *Recovery Time Objective*).

Disponibilità del servizio

L'Esecutore deve esplicitare tutti i soggetti terzi e servizi di terze parti dei quali si avvale per l'erogazione del servizio oggetto del presente capitolato.

In particolare, essendo il servizio in cloud, deve esplicitare la localizzazione geografica delle infrastrutture tramite le quali viene erogato il servizio stesso che deve essere all'interno della UE.

L'Esecutore garantisce la disponibilità immediata del servizio.

5. Servizi professionali

Servizi di formazione

Dovrà essere previsto un servizio di formazione per il personale CINECA per gli utenti interni del servizio, stimati al più in 8 unità.

La formazione dovrà essere adeguata all'utilizzo del sistema GRC e potrà svolgersi da remoto o presso la sede di CINECA, con la possibilità di effettuare registrazioni video.

Servizi di documentazione

Oltre alle sessioni di formazione, dovrà essere fornita adeguata manualistica utente (preferibilmente on-line) ad hoc per tutte le funzioni presenti nel sistema GRC.

Servizi di avvio

Dovranno essere forniti servizi di consulenza funzionale e organizzativa e attività tecniche per l'avvio del servizio GRC.

In particolare, le attività per l'avvio comprenderanno:

- Supporto consulenziale per la definizione delle entità informative (esempio: libreria delle normative, libreria dei rischi, processo di self assessment, profili utenti, ecc.);
- configurazione del sistema rispetto a quanto emerso al punto precedente;
- configurazione dei reports e cruscotti.
- integrazione con il sistema SSO e i sistemi CINECA (sistema di ticketing Jira e delle Struttura Organizzative nel sistema informativo U-GOV di CINECA)
- importazione delle risk/control matrix già presenti in Cineca;

e tutto ciò che è necessario al corretto funzionamento e uso della soluzione GRC da parte dell'utente finale.

L'avvio di produzione deve essere garantito entro 2 mesi dalla firma del contratto.

Servizi di manutenzione adeguativa e correttiva

Dovranno essere forniti servizi di manutenzione sul servizio in modo da garantire la correzione di eventuali problematiche e l'adeguamento del sistema che dovessero emergere dall'utilizzo del sistema stesso.

Per il sistema oggetto di fornitura dovrà essere erogato un servizio di manutenzione adeguativa e correttiva (MAC) a decorrere dalla data di stipula del contratto. Si precisa che:

− La manutenzione *correttiva* comprende la diagnosi e la rimozione delle cause e degli effetti dei malfunzionamenti delle procedure e dei programmi;

− La manutenzione *adeguativa* comprende l'attività di manutenzione volta ad assicurare la costante aderenza delle procedure e dei programmi alla evoluzione dell'ambiente tecnologico, del sistema informativo ed al cambiamento dei requisiti generali d'ambiente e di sicurezza.

SLA/Tempistiche per Manutenzione correttiva

Gli interventi di manutenzione correttiva dovranno sottostare ai livelli di servizio indicati nell'art. 7 "Livelli di servizio".

Servizi di assistenza ed help desk

Dovranno essere previsti nella fornitura adeguati servizi di assistenza e supporto funzionale e tecnico sul prodotto che verranno utilizzati da personale CINECA, a garanzia del corretto ed efficiente funzionamento del sistema in ogni sua parte, mediante un *help desk* multicanale (telefono, *e-mail, web*, etc,).

Il servizio di help desk dovrà essere disponibile dal lunedì al venerdì, dalle ore 9,00 alle ore 17,00 (almeno 8h).

Il servizio di assistenza e help desk dovrà sottostare ai livelli di servizio indicati nell'art. 7 "Livelli di servizio".

Servizio di migrazione dei dati

In caso di sostituzione della soluzione attuale con una nuova soluzione, dovrà essere fornito un servizio di esportazione dei dati del servizio secondo uno standard da concordare.

6. Livelli di servizio

Vengono di seguito descritti i livelli di servizio (*Service Level Agreement*, o SLA) che dovranno essere garantiti dall'Esecutore.

Al termine di ciascun periodo di monitoraggio verrà verificato il rispetto di ciascuno dei livelli di servizio stabiliti e, in caso di mancato rispetto, CINECA e l'Esecutore valuteranno gli interventi correttivi necessari. Nel caso non vengano rispettati gli SLA concordati, l'Esecutore dovrà provvedere con gli adeguamenti necessari e/o indicando al Committente interventi migliorativi a carico dello stesso Esecutore.

SLA-MANUT-01 Tempestività nella risoluzione anomalie

Relativamente alle funzionalità del sistema, per problemi tecnici che dovessero determinare malfunzionamenti, l'intervento deve essere garantito, a seconda della tipologia di problema determinata ad insindacabile giudizio della Stazione Appaltante, nei termini di seguito indicati:

Identificativo SLA	SLA-MANUT-01
KPI	Tempo di risoluzione
Descrizione	Risoluzione anomalia entro il tempo target stabilito
Algoritmo	Misurazione sul singolo intervento: $T_{ris} = T_{con} - T_{seg}$ T_{ris} = Tempo di risoluzione T_{seg} = Momento in cui è stato segnalato il problema T_{con} = Momento di consegna della soluzione
Sorgente informativa	Comunicazione formale. Reportistica dall'Esecutore e validata dalla Stazione Appaltante

Periodo di rilevazione	Trimestrale	
Reportistica	Trimestrale	
Tempi di risoluzione target (altre funzioni)	0–Anomalia Bloccante o emergenza	. Soluzione e ripristino completo **entro 16 ore lavorative** successive alla segnalazione.
	1 – Anomalia Grave	. Soluzione e ripristino completo **entro 32 ore lavorative** successive alla segnalazione.
	2 – Anomalia Normale	Soluzione e ripristino completo **entro 96 ore lavorative** successive alla segnalazione.
Livelli di Servizio	Tempo di risoluzione <= tempo target	

Per "Tempo di segnalazione" si intende il momento in cui il Committente invia all'Esecutore la segnalazione di guasto via *e-mail o piattaforma di trouble ticketing messa a disposizione dell'Esecutore*.

Per "Tempo di consegna della soluzione" si intende il momento in cui l'Esecutore invia *e-mail* all'ente preposto dal Committente con l'indicazione della messa in produzione della soluzione dell'anomalia.

Il "Tempo di risoluzione" è misurato in ore lavorative facendo riferimento alla finestra di servizio indicata in questo documento. Qualora la segnalazione di un'anomalia ad alta priorità avvenga prima della chiusura della finestra di servizio, si richiede all'Esecutore di completare l'attività avviata anche fuori della finestra di servizio. Nella seguente tabella è riportata la descrizione dei livelli di severità delle segnalazioni:

Severità	Descrizione
0- Bloccante o Emergenza	Malfunzionamento grave che rende impossibile operare con l'applicazione e/o comporta notevoli perdite di dati ovvero situazioni per le quali non è possibile la risoluzione alternativa del problema, con impatto bloccante su tutte (o su quelle che il Fruitore ritiene critiche) le operazioni utente e sull'utilizzo del sistema. In tal caso è richiesta la presa in carico immediata del problema e la sua risoluzione nel minor tempo possibile.
1 - Grave	Malfunzionamento che rende impossibile lavorare con una parte dell'applicazione e/o impedisce il flusso di lavoro e/o causa un degrado tollerabile di prestazione su una funzionalità, per periodi limitati; non richiede un intervento urgente.
2 - Normale	Tutte le altre tipologie di errore di minore entità che non pregiudicano l'operatività di base e le funzionalità chiave del sistema.

Fermo restando quanto sopra, si precisa che per *segnalazione del guasto/malfunzionamento* si intende la data e l'orario dell'effettuazione della chiamata telefonica e/o dell'invio del messaggio di posta elettronica e/o della segnalazione tramite portale web da parte della Stazione Appaltante verso l'Esecutore; per orario lavorativo s'intende il normale orario di lavoro, dal lunedì al venerdì, dalle 9.00 alle 17.00 (almeno 8 ore).

In ogni caso, resta inteso che la determinazione della causa del problema, l'individuazione del guasto ed il ripristino della piena funzionalità del sistema mal funzionante, sono interamente a carico dell'Esecutore.

SLA-HD-01 Tempi di risposta Help Desk

Relativamente al servizio di Help Desk oggetto di fornitura, deve essere assicurato il seguente livello di servizio con periodo di osservazione su base mensile:

Identificativo SLA	SLA-HD-01	
KPI	Tempo di risposta	
Descrizione	Risposta a un quesito entro il tempo target stabilito	
Algoritmo	Misurazione sulla singola risposta: $T_{ris} = T_{con} - T_{seg}$ T_{ris} = Tempo di risposta T_{seg} = Momento in cui è stato posto il quesito T_{con} = Momento di risposta al quesito posto	
Sorgente informativa	Comunicazione formale. Reportistica dall'Esecutore e validata dalla Stazione Appaltante	
Periodo di rilevazione	Trimestrale	
Reportistica	Trimestrale	
Tempi di risposta target (altre funzioni)	0–Segnalazione urgente	Risposta **entro 16 ore lavorative** successive alla segnalazione.
	1 – Segnalazione non urgente	Risposta **entro 32 ore lavorative** successive alla segnalazione.
Livelli di Servizio	Tempo di risposta <= tempo target	

SLA-SERV-01 Affidabilità/tolleranza ai guasti

Relativamente ai tempi di tolleranza ai guasti del servizio l'Esecutore dovrà garantire le seguenti SLA:

Identificativo SLA	SLA-SERV-02

KPI	Disponibilità del servizio – **DIS1**
Caratteristica	Affidabilità / Tolleranza ai guasti
Descrizione	La finestra di erogazione del servizio da considerare è H24 x 365. La disponibilità del servizio verrà calcolata al netto di: • fermi programmati richiesti da Esecutore che devono essere comunicati con un anticipo di due giorni lavorativi Il calcolo della Disponibilità si basa sulle misurazioni eseguite dall'Esecutore.
Unità di misura	Percentuale
Dati elementari da rilevare	• Data e ora di fermo (al minuto) • Data e ora di riattivazione (al minuto)
Periodo di riferimento	Trimestrale
Frequenza esecuzione misure	4 volte l'anno
Formula di calcolo	Dati necessari: • durata del fermo • tempo totale = tempo contrattuale di erogazione del servizio nel periodo di riferimento (esclusi i fermi programmati) $DIS1 = \frac{Tempo\_totale - \sum Durata\_fermo}{Tempo\_totale} \times 100$
Regole di arrotondamento	La percentuale va arrotondata alla frazione decimale di punto sulla base del secondo decimale: - per difetto se la parte decimale è 0,05 - per eccesso se la parte decimale è > 0,05
Obiettivi (valori soglia)	**DIS1** ≥ 99,5%

Dott. Stefano Roselli
CINECA - *Consorzio Interuniversitario*
Il Responsabile Unico del Procedimento
(Documento firmato digitalmente)