Agenzia Entrate Riscossione

Progetto Tecnico ai sensi dell'art. 23 comma 15 D.Lgs. n. 50/2016

Certificazione ISO 27001/2013

CVP 79132000-8

Sommario

Premessa

Il corretto esercizio delle attività istituzionali inerenti la riscossione nazionale e l'amministrazione dei processi corporate da parte dell'Agenzia delle entrate-Riscossione è strettamente correlato alla disponibilità, all'integrità e alla riservatezza dei dati contenuti nel proprio sistema informativo.

AdeR, a tal riguardo, in considerazione di quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017 - 2019, emanato dall'Agenzia per l'Italia Digitale ha deciso di definire ed attuare un efficace Sistema di Gestione per la Sicurezza delle Informazioni (di seguito anche "SGSI"), a norma UNI EN ISO 27001:2013.

Il SGSI, che si innesta all'interno dei processi già presidiati dall'Ente in coerenza con il modello organizzativo ed il sistema delle responsabilità da quest'ultimo adottato, è gestito all'interno dell'Area Innovazione e Servizi Operativi dall'ufficio SGSI Governance.

Agenzia delle entrate-Riscossione ha intrapreso un percorso finalizzato all'adozione del Sistema SGSI per tutte le informazioni e i dati gestiti, sia nell'ambito delle attività di riscossione che nell'ambito dei processi amministrativi/corporate.

L'adozione del Sistema SGSI seguirà un approccio di tipo modulare, venendo via via implementato, a partire dalle informazioni e dai dati trattati nell'ambito del Data Center allocato presso le sedi di Roma e di Torino, fino ad estendersi progressivamente a tutti i dati e le informazioni dell'Ente.

Agenzia delle entrate-Riscossione ha, l'obiettivo di conseguire entro il 2019 la certificazione UNI CEI/ISO 27001:2013 del proprio SGSI, con riferimento ai processi ed ai servizi gestiti da AdeR a partire da quelli erogati per la gestione del Data Center, allocato presso le sedi di Roma e di Torino. A tal fine occorrerà acquisire per tempo i relativi servizi di certificazione, da parte di uno degli Organismi certificatori accreditati.

Descrizione del fabbisogno

La richiesta è relativa ai servizi necessari per la certificazione ISO 27001 del SGSI di AdeR, con riferimento ai processi ed ai servizi gestii da AdeR a partire da quelli erogati per la gestione del Data Center allocato presso le sedi di Roma e Torino. Di seguito si riporta un riferimento indicativo delle attività da richiedere al certificatore:

1. Audit preliminare (pre-Audit);
2. Audit iniziale, scomposto a sua volta in:
    a. Audit di Stage 1: comprende una prima visita e l'esame dei documenti del SGSI;

b. Audit di Stage 2: comprende l'esame della conformità ai requisiti della norma presso i siti compresi nell'ambito della certificazione;
3. Esame dei risultati ed eventuale rilascio del certificato;
4. Visite annuali periodiche di sorveglianza per controllare il miglioramento continuo.

Al termine di ogni audit e visita il certificatore dovrà redigere e rilasciare uno specifico rapporto.

Per ottenere la certificazione entro l'anno 2019, è opportuno condurre e concludere le attività di Audit preliminare entro luglio 2019 e le altre entro il secondo semestre di ogni anno del triennio di certificazione a partire dall'Audit iniziale dell'anno corrente (per i punti 2 e 3).

Strategia per l'acquisizione dei Servizi

Con riferimento alla tipologia acquisitiva, stante il valore di riferimento per il contratto, i cui criteri di determinazione sono illustrati di seguito, si propone l'affidamento della fornitura dei servizi, tramite la "Procedura sotto soglia ex art. 36 del D. Lgs. 50/2016, mediante RDO MePA aperta a tutti gli operatori del bando "Servizi" categoria "Servizi di Valutazione della Conformità" (CPV 79132000-8 Servizi di certificazione dei sistemi di gestione) ed aggiudicata al minor prezzo in base all'art. 95, co.4, lett. C, del D. Lgs. 50/2016".

Requisiti di partecipazione

Si precisa che per la partecipazione alla RDO MePA, i Fornitori concorrenti, devono essere Organismi di certificazione per la norma **UNI CEI ISO/IEC 27001:2013** accreditati da Accredia, l'Ente Italiano di Accreditamento, ovvero da equivalenti enti certificatori esteri equiparati, per i settori di accreditamento IAF EA 33 (Tecnologia dell'informazione), EA 35 (altri Servizi) ed EA 36 (Pubblica amministrazione). I Fornitori dovranno mantenere tale accreditamento per tutta la durata della certificazione.

I fornitori, nel pieno rispetto degli standard ISO e dei regolamenti di ACCREDIA, dovranno possedere organizzazione, mezzi e risorse idonee e adeguate, sia sotto il profilo dei requisiti normativi, sia sotto il profilo dei servizi professionali, ed essere in grado di offrire un servizio con elevato standard di qualità, alle condizioni previste dal capitolato d'appalto e dai documenti da esso richiamati.

Il servizio dovrà essere eseguito con la massima cura, diligenza, tempestività e riservatezza, mediante l'impiego di un'organizzazione efficiente, risorse e mezzi adeguati. I fornitori, inoltre dovranno essere in regola con tutte le prescrizioni di legge attinenti ai servizi appaltati, gestiti

a proprio esclusivo rischio e sotto la propria direzione, sorveglianza e diretta responsabilità.

I fornitori si impegnano, inoltre, a svolgere tutte le attività, anche non espressamente indicate negli atti della gara e nel contratto, che si rendessero necessarie per garantire l'efficiente svolgimento del servizio.

Il servizio deve essere organizzato e svolto con disponibilità di risorse umane e tecnologiche adeguate e a norma di legge rispetto alla consistenza qualitativa/quantitativa e all'osservanza dei parametri di sicurezza delle persone fisiche e delle strutture coinvolte.

Impegno di spesa

Nel mercato di riferimento le attività richieste sono quotate a corpo rispetto al valore contrattuale secondo il seguente impegno minimo di giornate:

Attività	**Giornate/persona**[1]
Audit preliminare	5
Audit iniziale e rilascio del certificato	15
1° sorveglianza	5
2° sorveglianza	5

In base alle stime sopra indicate l'impegno di spesa stimata risultante per i servizi richiesti è pari ad un complessivo di € 24.000,00[2] i.e., comprensive di oneri accessori e sicurezza.

Indicazioni per la stesura dei documenti inerenti la sicurezza

In ragione della tipologia dell'affidamento, ai sensi dell'art. 26 c. 3 del D. Lgs. 81/2008 e s.m.i. e della determinazione dell'ANAC nr. 3 del 05/03/2008, si esclude la predisposizione del DUVRI e la conseguente stima di costi per oneri della sicurezza per rischi interferenziali e, pertanto, gli stessi dovranno essere pari a € 0,00.

[1] le stime sono state fatte attraverso la norma ISO/IEC 27006 relativa alle specifiche seguite per la verifica di conformità dei SGSI certificati ai sensi della UNI CEI ISO/IEC 27001:2013 ed in particolare all'ANNEX A, afferente la particolare complessità dell'Organizzazione da certificare, e l'ANNEX C sulle giornate uomo previste per gli External Audit

[2] la stima si basa su quanto indicato nel tariffario Accredia per i servizi di Verifiche Ispettive di valutazione (preliminare, in sede, in accompagnamento, supplementari, straordinarie, market surveillance visit, di estensione, sorveglianza e rinnovo). Il tariffario Accredia prevede 875,00 euro g/u (per un loro ispettore esperto), i.e. Il costo giorno/uomo di uno specialista di un certificatore accreditato è sicuramente inferiore; ad ogni buon conto si ritiene congrua una stima massima di 800 euro g/u.

Il Responsabile del
Procedimento
Valerio Ricciardi
(Firmato Digitalmente)