ALLEGATO "A"

CAPITOLATO SPECIALE PER IL MANTENIMENTO DELLA CERTIFICAZIONE ISO 27001 PER IL PROCESSO CRS E IL SERVIZIO ELETTRONICO DI RECAPITO CERTIFICATO

Oggetto

La presente Asta pubblica, costituita da un unico lotto, ha per oggetto le attività di supporto al rinnovo della certificazione ISO 27001:2013 "Sicurezza delle Informazioni dei servizi: CRS (Common Reporting Standard), SERC (Servizio Elettronico di Recapito Certificato), RDD (Registro dei Domicili Digitali), all'interno della struttura IT (Information Technology) della Pubblica Amministrazione della Repubblica di San Marino. Dichiarazione di Applicabilità Rev. 3 del 20/09/2021".

- Numero del certificato: 71347/A/0001/UK/It Data Revisione 15 Gennaio 2022.

Dichiarazione di confidenzialità

I documenti e le informazioni trasmessi nell'ambito della presente Asta pubblica, sono da considerarsi strettamente confidenziali; in particolare, le informazioni contenute nei relativi allegati non possono essere copiate, riprodotte, divulgate, trasferite, trasformate in qualsiasi forma, trasmesse o pubblicate.

Riservatezza

L'impresa partecipante, e tutte le figure ad essa collegate, dovrà tenere riservate tutte le informazioni concernenti le attività di cui sia venuta o potrà venire a conoscenza in occasione della definizione ed esecuzione della presente Asta. Il medesimo impegno sarà a carico dell'Ufficio Informatica, Tecnologia, Dati e Statistica dal momento della ricezione delle offerte.

Attività di analisi, redazione della documentazione e coordinamento per l'ottenimento della certificazione ISO 27001

Si richiedono le attività necessarie per il mantenimento dell'attuale certificazione ISO 27001:2013 relativa al processo di scambio automatico delle informazioni in ambito OCSE denominato CRS (di cui al certificato N. 71347/A/001/UK/It rilasciato in data ottobre 2016 da URS - United Registrar of Systems - con 2ª emissione in data 23 ottobre 2019, e con estensione al Servizio Elettronico di Recapito Certificato in data 15 gennaio 2022 da URS - United Registrar of Systems).

Il perimetro di certificazione individuato comprende i luoghi fisici dei Datacenter, i luoghi di lavoro dei sistemisti, le centrali di rete, i dipendenti degli uffici Pubblici con le loro postazioni abilitate a Tnotice, il personale sistemistico della Cooperativa di lavoro in outsourcing, gli apparati attivi e passivi (server, switch, cablaggi e punti di connessione alla rete interna alla PA - PANET), sistemi di sicurezza come firewall, sonde, analizzatori di traffico, canali VPN, gestione certificati SSL, reti di accesso dedicate.

Il perimetro di certificazione non comprende i server ed i database del servizio SERC, gestito direttamente dal servizio di manutenzione Tnotice. I server sono all'interno del Datacenter PA in hosting. Non sono compresi nel perimetro di certificazione gli utenti esterni (imprese e cittadini) e gli sportelli postali che svolgono il ruolo di RAO e l'attività commerciale. Gli uffici postali sono gestiti da Poste SM capogruppo dell'ATI che eroga il servizio SERC.
Il servizio Tnotice è certificato ISO27001.

Al fine della certificazione ISO 27001 di cui sopra si richiedono le seguenti attività:

- analisi ed eventuale aggiornamento delle politiche di sicurezza già implementate nel CRS ed estese per il SERC;
- analisi ed eventuale aggiornamento dell'ambito di applicazione del SGSI già implementate nel CRS con estensione per il SERC;
- analisi ed eventuale aggiornamento della valutazione del rischio già implementate nel CRS con estensione per il SERC;
- analisi ed eventuale aggiornamento della gestione del rischio già implementate nel CRS con estensione per il SERC;
- definizione degli obiettivi e dei relativi controlli da realizzare con estensione per il SERC;
- analisi ed eventuale aggiornamento della dichiarazione di applicabilità con estensione per il SERC;
- esecuzione audit interno generale di sistema in conformità allo standard ISO 27001;
- attività di supporto / affiancamento nelle giornate di audit dell'Ente di Certificazione per la certificazione estesa CRS+SERC;
- quant'altro si ritiene necessario per l'ottenimento della certificazione ISO 27001.

Di seguito si riportano i riferimenti normativi reperibili all'url
https://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti.html

- Decreto Delegato 30 gennaio 2020 n. 9
- Regolamento 22 novembre 2018 n.7
- Decreto Delegato 26 luglio 2018 n.92
- Decreto Delegato 15 giugno 2018 n.65
- Legge 23 agosto 2016 n.114
- Decreto Delegato 11 aprile 2016 n.46
- Legge 29 maggio 2013 n.58
- Regolamento 30 dicembre 2015 n.20
- Decreto 8 novembre 2005 n.156
- Legge 20 luglio 2005 n.115

Si allega il documento N°5 dell'attuale Manuale ISO 27001 denominato ADC Analisi Del Contesto, mentre i seguenti documenti posso essere ritirati presso l'Ufficio Informatica, Tecnologia, Dati e Statistica, a seguito della firma del documento di riservatezza, che si allega:

1) Documento 10 - SoA Dichiarazione di applicabilità.pdf Manuale Iso27001
2) Documento 07 - Certificato di Registrazione
3) Documento 30 - PR14 Audit del SGSI
4) Documento 2019 - Valutazione del rischio - Mod. PR_03.01
5) Rapporto Audit 2018 (solo frontespizio)
6) Rapporto Audit 2019 (solo frontespizio)
7) Rapporto Audit 2020 (solo frontespizio)

8) Rapporto Audit 2021 (solo frontespizio)

Per motivi di riservatezza non possono essere forniti i documenti relativi agli Audit Interni e gli esiti del VAPT (Vulnerability Assessment e Penetration Test).

Le attività devono prevedere l'analisi del contesto, la predisposizione dei documenti, il coordinamento delle attività e tutto quanto necessario al fine di conseguire la certificazione ISO 27001.
Nell'attività di analisi richiesta dovrà essere fornita una schedulazione a calendario degli interventi necessari per il controllo, le verifiche nonché per l'audit interno.

La certificazione ISO 27001 attuale coinvolge i seguenti siti fisici, tutti ubicati all'interno del territorio della Repubblica di San Marino con una distanza massima di circa 10km:
1) Server Farm CIS
2) Server Farm CU
3) ITDS
4) CLO
5) Ufficio Tributario
6) Centrale Rete CU
7) Centrale Rete Begni
8) Centrale Rete Dogana

Gli indirizzi dei sopra indicati siti fisici, per motivi di riservatezza, non possono essere forniti in fase di gara.

Le uniche attività esterne al territorio di San Marino sono relative ad attività di verifica e controllo del servizio SERC da parte del fornitore Inposte.it spa tramite collegamento VPN direttamente gestito e monitorato da ITDS.

Si richiede inoltre l'attività di "Test di Sicurezza" attraverso tecniche di Vulnerability Assessment e Penetration Test in modalità Black Box su indirizzi esposti alle reti esterne.
L'attività di "Test di Sicurezza" si dovrà svolgere in due fasi, la prima da remoto con l'esecuzione dei test e la raccolta delle vulnerabilità, la seconda dove verranno presentati i report, discusse e analizzate le vulnerabilità riscontrate, valutando le possibili soluzioni applicabili per mitigare o eliminare le minacce riscontrate.
L'impresa aggiudicataria, nel pieno rispetto degli standard ISO, dovrà possedere un'organizzazione, mezzi e risorse idonee ed adeguate sotto il profilo dei servizi professionali ed essere in grado di offrire un servizio con elevato standard di qualità.
Il servizio dovrà essere eseguito dall'impresa aggiudicataria, con la massima cura, diligenza, tempestività e riservatezza, mediante l'impiego di una organizzazione efficiente, risorse e mezzi adeguati.
La ditta aggiudicataria si impegna, inoltre, a svolgere tutte le attività, anche se non espressamente indicate negli atti di gara e nel contratto, necessarie al fine di garantire l'efficiente svolgimento del servizio.

Per il Vulnerability Assessment e Penetration Test possono essere considerati i seguenti elementi: almeno 22 indirizzi IP pubblici e 60 URL esposti ad internet.

L'offerta dovrà contenere il progetto specifico relativo all'esecuzione di ogni attività richiesta, indicando l'impegno espresso in giorni/uomo per l'esecuzione di ciascuna di esse; potranno essere richiesti maggiori dettagli per comprendere meglio le specificità, data la riservatezza del processo alcune informazioni potranno essere fornite solo previa sottoscrizione di un accordo di riservatezza (NDA).

Il piano di lavoro sarà definito in comune accordo pianificando un calendario di incontri e di attività. Per ogni incontro/attività si dovrà produrre un report di quanto è stato svolto.
Le attività dovranno concludersi entro il mese di settembre 2022 per poi procedere con la verifica ispettiva dell'organismo di sorveglianza dell'Ente di Certificazione.

Roberta Mularoni
Roberta Mularoni
2022.08.02 12:44:32 +02'00'