ALLEGATO "A"

CAPITOLATO SPECIALE PER L'ESTENSIONE DELLA CERTIFICAZIONE ISO 27001 AL PROCESSO DEL SERVIZIO ELETTRONICO DI RECAPITO CERTIFICATO

Oggetto

La presente Asta pubblica, costituita da un unico lotto, ha per oggetto l'estensione dell'attuale certificazione ISO 27001 "Sicurezza delle Informazioni CRS (Common Reporting Standard) all'interno della IT (Information Technology) della Pubblica Amministrazione della Repubblica di San Marino" - Numero del certificato: 71347/A/0001/UK/It - al processo del Servizio Elettronico di Recapito Certificato, considerate le strettissime analogie tra i due sistemi, infatti il nuovo servizio è direttamente associato al medesimo Ufficio richiedente e utilizza le medesime risorse sia in termini di infrastrutture informatiche, sia per il personale sistemistico, nonché nella gestione del servizio della sicurezza.

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, per il quale annualmente è stata effettuata la verifica ispettiva da parte dell'Ente Certificatore) e per l'estensione della stessa al Servizio Elettronico di Recapito Certificato.

Pertanto si propone un nuovo Campo di Applicazione che comprenda entrambi i servizi CRS e SERC:

Sicurezza delle Informazioni CRS (Common Reporting Standard) e SERC Servizio Elettronico di Recapito Certificato (Raccomandata Elettronica) all'interno della IT (Information Technology) della Pubblica Amministrazione della Repubblica di San Marino.

Il Servizio Elettronico di Recapito Certificato (SERC) della Pubblica Amministrazione, utilizzato anche da imprese e cittadini, è gestito attraverso un contratto di servizio con l'ATI Poste SM

tNotice costituita da Poste San Marino S.p.A. che mette a disposizione i servizi di sportello per il pubblico (registrazione ed associazione del domicilio digitale, formazione e call center di primo livello) e Inposte.it S.p.A., provider del Servizio Elettronico di Recapito Certificato che ha sviluppato il sistema di recapito certificato e che gestisce il software di corrispondenza e notifiche. Inposte.it S.p.A. è in possesso delle certificazioni reperibili sul sito http://open.inposte.it/category/aug/; i seguenti certificati possono essere anche richiesti all'Ufficio Informatica, Tecnologia, Dati e Statistica:
Tnotice Certification_27001.pdf
Tnotice CP-CPS_Certificate_Policy_and_Certification_Practice_Statement_for_ERDS-QeRDS_IT_v2.3.pdf
Tnotice Rapporto_INPOSTE 27001-signed.pdf
Tnotice ST2 27K_ReportPopup.pdf

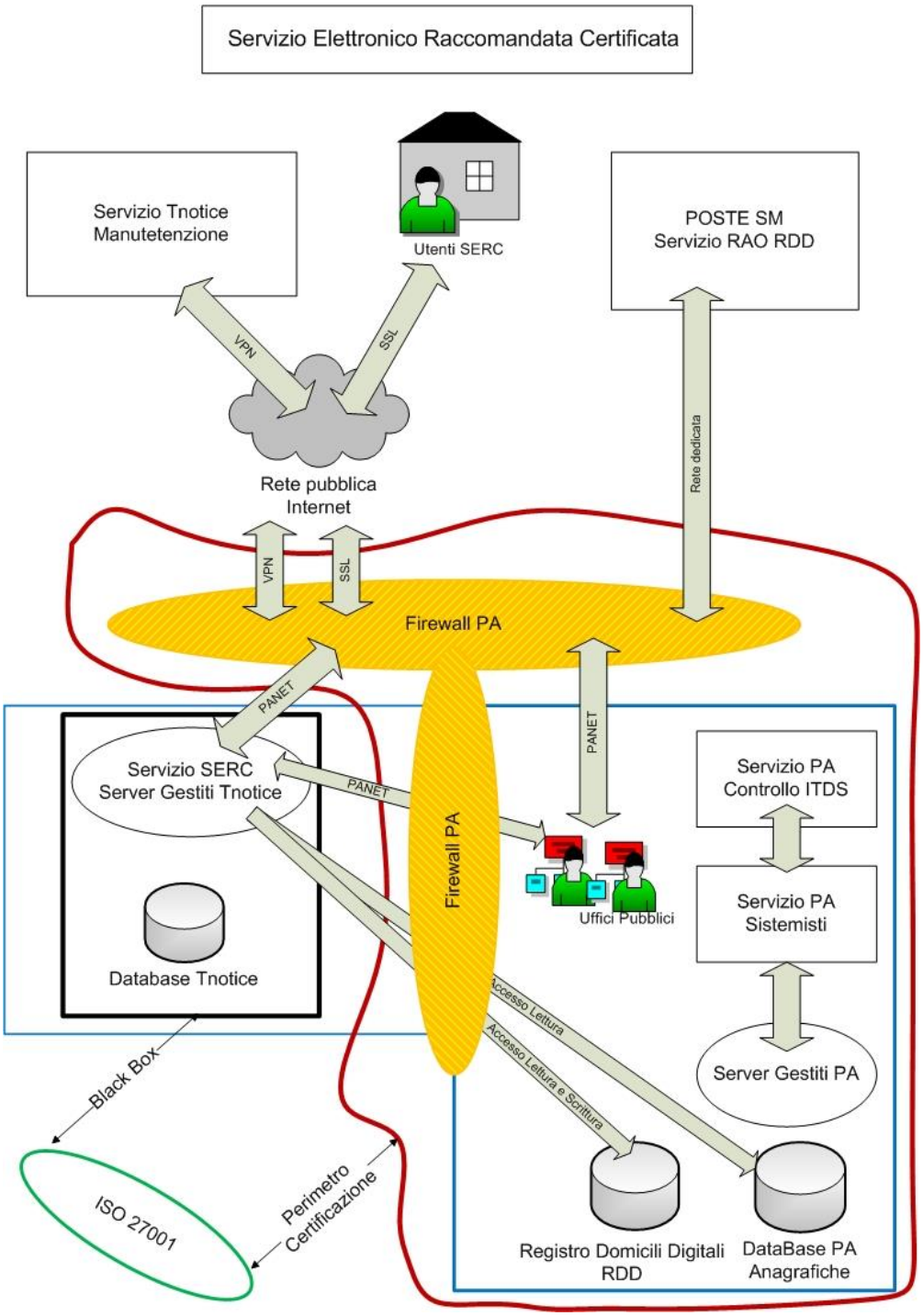
Il Servizio Elettronico di Recapito Certificato, brevemente SERC, è ospitato nel centro informatico della Pubblica Amministrazione in database che contengono i registri di anagrafiche, di messaggi e di log; il centro informatico della Pubblica Amministrazione è già compreso nel perimetro di certificazione del processo CRS ed è gestito dai sistemisti di Cis Coop arl, tramite apposito contratto di servizio.

Il flusso di informazioni SERC è sintetizzato in:

1) identificazione e registrazione del domicilio digitale riferito a operatori economici e persone. Questa fase viene svolta presso gli sportelli postali con ruolo di RAO;
2) identificazione e registrazione del domicilio digitale riferito ad uffici pubblici o specifici sevizi di uffici pubblici. Questa fase viene svolta dall'ufficio ITDS con ruolo di RAO per gli Uffici Pubblici;
3) attivazione del domicilio digitale e registrazione password per accedere al servizio on line di Tnotice, come attività dell'utente;
4) attività di invio Raccomandata Certificata ad un indirizzo del Registro dei Domicili Digitali;
5) consegna dell'avviso di giacenza presso il Domicilio Digitale;
6) attività di apertura tramite password personale del contenuto della Raccomandata Certificata sul sito/server Tnotice SERC;
7) invio automatico da parte del servizio SERC al mittente dl Certificato Forense di consegna e lettura della Raccomandata Digitale;
8) controllo, da parte del servizio di manutenzione Tnotice, dello stato di operatività del servizio, correzione delle anomalie, amministrazione dei server e del database Tnotice, attività di recupero informazioni e log di sistema, controllo stato dei backup;
9) servizi sistemistici per la Pubblica Amministrazione, controllo della disponibilità di risorse per i server, stato delle macchine virtuali, predisposizione ed attività di backup delle macchine virtuali, compresi i server Tnotice. Gestione, amministrazione e controllo del server PA e dei Data Base PA, compreso nello specifico il Registro dei Domicili Digitali;
10) controllo e supervisione dell'Ufficio ITDS verso l'intera procedura in particolare sulle attività sistemistiche, di rete, di sicurezza e di servizi verso uffici pubblici.

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 capofila 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)

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

L'estensione della certificazione al servizio SERC dovrà coinvolgere l'ulteriore sito fisico:

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 ed in modalità Gray Box su due reti interne dove verranno allocati e messi a disposizione due server, attestati nelle opportune reti, per poter effettuare i test di vulnerabilità.
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 presso il committente 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 test di sicurezza si dovrà prevedere:

- Presentazione del team e delle responsabilità (profili professionali)
- Definizione dello "scope" e degli obiettivi
- Definizione delle regole di ingaggio per i diversi target
- Definizione delle linee di comunicazione
- Analisi delle tecnologie adottate
- Presentazione della strategia di analisi

Attività di preanalisi:

- Network Footprinting
- Definizione di Tool
- Preparazione e customizzazione dei server di analisi

Attività di enumeration:

- Enumerazione dei sistemi e degli indirizzi IP
- Information gathering passivo
- Information gathering attivo (previa autorizzazione)
- Protocolli
- Stato dei sistemi

Attività di analisi:

- Analisi avanzata basata su tool specifici
- Analisi manuale
- Vulnerability assesment dei sistemi ed applicazioni (attività manuale e con scansioni previa autorizzazione)

Verifica delle vulnerabilità Penetration Test (previa autorizzazione):

- Attacchi automatici
- Attacchi manuali
- Exploitation delle vulnerabilità scoperte escluso Denial of Service:
  - Client-side attacks
  - Web Application attacks
  - Password attacks
  - Privilege escalation
  - Network attacks (Port Forwarding / Redirection e Tunneling)
  - Social engineering attacks (previa autorizzazione

Documentazione e reportistica:

- Raccolta e registrazione delle evidenze informatiche
- Redazione della documentazione
- Consegna, presentazione e discussione dei risultati

Viene richiesta la produzione di due report, uno di carattere tecnico ed uno executive che descriva:

- il target analizzato
- le metodologie ed i riferimenti utilizzati per l'analisi
- tutte le vulnerabilità ed in genere le anomalie riscontrate e per ciascuna la nomenclatura standard CVE associata (dove possibile)
- classificazione oggettiva (possibilmente basata su scoring riconosciuti come CVSS)
- descrizione della segnalazione e riferimenti per poterla riprodurre
- IP e relativo hostname affetto dalla vulnerabilità
- impatti derivanti
- soluzioni concrete per la remediation
- presenza di exploit pubblici della vulnerabilità
- riassunto delle segnalazioni e relativa remediation di alto livello per il management

Per il Vulnerability Assessment e Penetration Test possono essere considerati i seguenti elementi: 22 indirizzi IP pubblici, 100 server o apparati in area DMZ, 1000 pc o apparati in area utenti.

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 2021 per poi procedere con la verifica ispettiva dell'organismo di sorveglianza dell'Ente di Certificazione.

Firmato digitalmente da: Roberta Mularoni
Organizzazione: PARSM/01
Data: 24/06/2021 15:44:48