AdC SGSI
Analisi del contesto

Rev.	Data	Modifiche apportate		
03	28-08-2022	Aggiornamento Riferimenti Legali e Normativi		
02	20-09-2021	Aggiornamento per l'inserimento dei nuovi servizi SERC e RDD		
01	28-08-2019	Aggiornamento per l'inserimento di riferimenti legislativi		
00	01-10-2015	Prima emissione I Edizione		
		CLASSIFICAZIONE	**USO INTERNO**	**UI**
	Funzione	**Responsabile**	**Firma**	**Data**
Redatto				
Verificato				
Approvato				

1. Introduzione

Nel 2021 il perimetro dei servizi certificati secondo lo standard ISO 27001 si è allargato a comprendere sia il servizio CRS che alcune componenti tecnologiche dei servizi SERC (Servizio Elettronico Recapito Certificato) e RDD (Registro dei Domicili Digitali).

Il CRS è il nuovo standard globale per lo scambio automatico di informazioni finanziarie tra Autorità Fiscali, elaborato dall'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) con l'obiettivo di individuare e scoraggiare l'evasione fiscale internazionale da parte di contribuenti che, direttamente o indirettamente, investono all'estero attraverso istituzioni finanziarie straniere.

Questo standard mira a conseguire una maggiore trasparenza fiscale, estendendo gli obblighi di reporting di determinate informazioni finanziarie da parte degli intermediari esteri e richiede agli intermediari finanziari di identificare tra la propria clientela i soggetti non residenti titolari di conti finanziari rilevanti e di segnalare determinate informazioni sugli stessi alle Autorità Fiscali locali che, a loro volta, le trasmetteranno alle Autorità Fiscali degli altri Paesi coinvolti nello scambio multilaterale di informazioni.

Il Congresso di Stato della Repubblica di San Marino si è impegnato nell'attività di rafforzamento delle intese in materia di cooperazione e assistenza amministrativa, attraverso la sottoscrizione di accordi con gli Stati e le giurisdizioni interessate, con particolare riferimento alle convenzioni per lo scambio di informazioni sulla base degli standard e dei modelli definiti dall'OCSE.

Il Riferimento normativo è la Legge 27 Novembre 2015 N.174 "Cooperazione Fiscale Internazionale" che disciplina la cooperazione fiscale internazionale attuata dalla Repubblica di San Marino in esecuzione degli accordi internazionali, bilaterali o multilaterali, stipulati con Paesi o giurisdizioni estere.

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 S.r.l., tramite apposito contratto di servizio.

Il flusso di informazioni SERC è sintetizzato come segue:

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 servizi 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 della notifica di consegna e lettura della Raccomandata Digitale.

Il servizio di manutenzione tNotice esegue un controllo dello stato di operatività del servizio, la correzione delle anomalie, l'amministrazione dei server e del database tNotice, l'attività di recupero informazioni e log di sistema ed il controllo stato dei backup.

L'Ufficio ITDS eroga servizi sistemistici per la Pubblica Amministrazione che comprendono la disponibilità di risorse per i server, il controllo dello stato delle macchine virtuali, la predisposizione e l'attività di backup delle macchine virtuali (compresi i server tNotice e RDD), la gestione, amministrazione e controllo del server PA e dei Data Base PA, compreso nello specifico il Registro dei Domicili Digitali RDD.
Inoltre, l'Ufficio ITDS opera una supervisione generale verso l'intero servizio ed in particolare sulle attività sistemistiche, di rete, di sicurezza e di servizio verso uffici pubblici.

Il gestore del servizio SERC accede in modo esclusivo ai server relativi. I server sono all'interno del Datacenter PA in hosting, ma sono gestiti da tNotice in completa autonomia.

IL servizio RDD invece viene erogato come un *database-as-a-service*, gestito da ITDS ed utilizzato dal gestore tNotice.

2. Riferimenti legali e normativi

ISO e Leggi Generali

ID	RIFERIMENTO	DESCRIZIONE
ISO 01	ISO/IEC 27001	Tecnologia delle informazioni – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti
ISO 02	Legge n.115/2005	Legge sul documento informatico e la firma elettronica
ISO 03	Legge n.114/2016	Disciplina dei Reati Informatici
ISO 04	NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
ISO 05	NIST SP 800-61	Computer Security Incident Handiling Guide

AMMINISTRAZIONE

ID	RIFERIMENTO	DESCRIZIONE
AMM 01	Legge n.30/1998	Norme Generali sull'Ordinamento Contabile dello Stato
AMM 02	Legge n.49/2002	Legge sul contratto di fornitura o somministrazione della PA e degli Enti Pubblici
AMM 03	Decreto n.53/2003	Regolamento di Contabilità
AMM 04	Decreto Delegato n.26/2015	Norme di attuazione della Legge n.49/2002 – Legge sul contratto di fornitura o somministrazione della PA e degli Enti Pubblici

PERSONALE PA

ID	RIFERIMENTO	DESCRIZIONE
PER 01	Legge n.41/1972	Legge Organica per i dipendenti dello Stato
PER 02	Legge n.106/2009	Norme di disciplina per i dipendenti pubblici
PER 03	Legge n.188/2011	Riforma della struttura e del modello organizzativo dell'amministrazione pubblica
PER 04	Legge n.141/2014	Codice di condotta per gli agenti pubblici
PER 05	Decreto Delegato n.132/2021	Secondo Fabbisogno generale del settore pubblico allargato

TRATTAMENTO DATI PERSONALI

ID	RIFERIMENTO	DESCRIZIONE
TDP 01	Legge n.171/2018	Protezione delle persone fisiche con riguardo al trattamento dei dati personali
TDP 02	Decreto Delegato n.138/2021	Revisione e aggiornamento della disciplina vigente in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali di cui alla Legge n.171/2018 + Errata Corrige del 4 agosto 2021

CRS – COMMON REPORTING STANDARD

ID	RIFERIMENTO	DESCRIZIONE
CRS 01	Legge n.174/2015	Cooperazione Fiscale Internazionale + Errata Corrige del 16 dicembre 2015
CRS 02	Regolamento n.20/2015	Regolamento tecnico per la protezione dei dati personali in applicazione dello scambio di informazione in materia fiscale
CRS 03	Decreto Delegato n.119/2016	Modifica alla Legge 27 novembre 2015 n.174 – Cooperazione fiscale internazionale
CRS 04	Decreto Delegato n.44/2017	Modifica alla Legge 27 novembre 2015 n.174 – Cooperazione Fiscale Internazionale e successive modifiche
CRS 05	Linee Guida Luglio 2017	Scambio Automatico di Informazioni
CRS 06	Regolamento Interno CLO	Plan for Breaches - ver.1.1 del 18 settembre 2020
CRS 07	Delibera C.d.S. n.13/2020	Cooperazione fiscale internazionale – lista delle giurisdizioni oggetto di comunicazione da parte degli istituti Finanziari in applicazione del CRS ai fini dello scambio automatico delle informazioni finanziarie

SERC – RDD (tNotice)

ID	RIFERIMENTO	DESCRIZIONE
SERC 01	Decreto n.156/2005	Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici
SERC 02	Legge n.58/2013	Legge sull'uso delle comunicazioni elettroniche e dell'E-Commerce
SERC 03	Regolamento UE n.910/2014	Regolamento in materia di identificazione elettronico e servizi fiduciari per le transazioni elettroniche nel mercato interno – abroga direttiva 1999/93/CE (come riferimento)
SERC 04	Decreto Delegato n.46/2016	Disposizioni per l'utilizzo di servizi elettronici di recapito certificato qualificato
SERC 05	Decreto Delegato n.65/2018	Modifiche al Decreto Delegato 11 aprile 2016 n.46 - Disposizioni per l'utilizzo di servizi elettronici di recapito certificato qualificato
SERC 06	Decreto Delegato n.92/2018	Modifiche al Decreto Delegato 11 aprile 2016 n.46 - Disposizioni per l'utilizzo di servizi elettronici di recapito certificato qualificato
SERC 07	Legge n.137/2018	Art. 22 – Disposizioni relative al registro pubblico dei Domicili Digitali
SERC 08	Regolamento n.07/2018	Regolamento per l'utilizzo del Registro Pubblico dei Domicili Digitali
SERC 09	Decreto – Legge n.81/2019	Differimento del termine d'iscrizione al registro Pubblico dei Domicili Digitali
SERC 10	Legge n.88/2019	Art.18 – Disposizioni aggiuntive sull'obbligo elezione del domicilio digitale ed in materia di notificazioni tramite servizio elettronico di recapito certificato
SERC 11	Decreto Delegato n.113/2019	Modifiche al Decreto 8 novembre 2005 n.156 e disposizioni sull'utilizzo di servizi elettronici di recapito certificato e di posta elettronica certificata
SERC 12	Decreto Delegato n.09/2020	Modifiche al Decreto 8 novembre 2005 n.156 e disposizioni sull'utilizzo di servizi elettronici di recapito certificato e di posta elettronica certificata
SERC 13	Decreto Legge n.85/2020	Disposizioni per l'utilizzo di strumenti informatici nell'ambito dell'attività giudiziaria

3. Responsabilità

La responsabilità dell'applicazione e dell'aggiornamento di questo documento è del Responsabile Gestione Sicurezza delle Informazioni (RSI).

4. Definizioni

- **PA** - Pubblica Amministrazione
- **ITDS** - Ufficio Informatica, Tecnologia, Dati e Statistica
- **CRS** - Common Reporting Standard
- **SERC** – Servizio Elettronico di Recapito Certificato
- **RDD** – Registro dei Domicili Digitali
- **IT -** Information Technology
- **SGSI** – Sistema di Gestione della Sicurezza delle Informazioni
- **RSI** - Responsabile SGSI
- **CIS** – Centro Informatico Statale
- **CU** – Centro Uffici

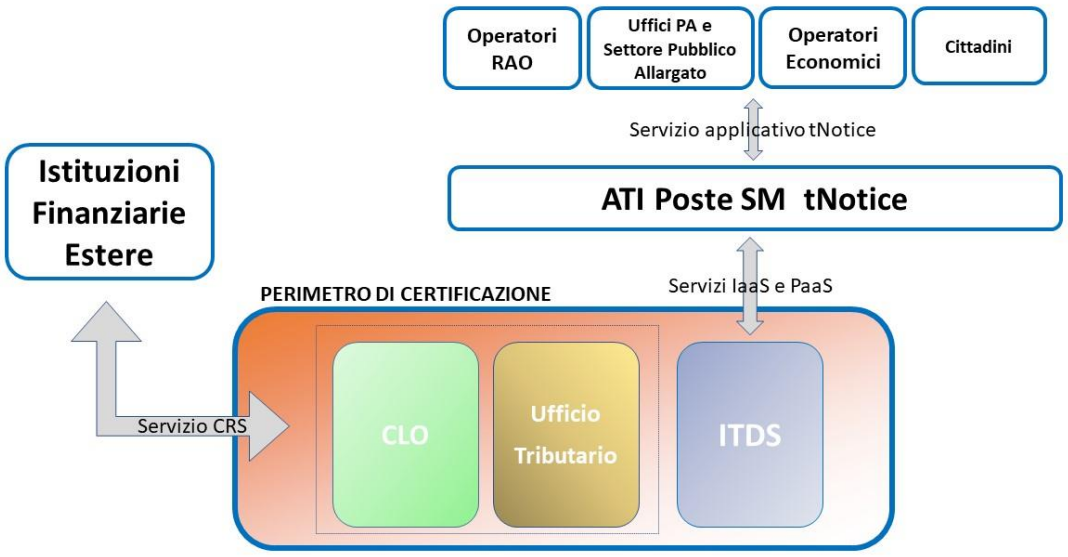
5. Procedura

5.1. Determinazione delle parti interessate

Per ITDS le parti interessate che concorrono e sono considerate nell'attuazione del sistema di gestione della sicurezza delle informazioni, comprendono:

- tutto il personale interno operante nelle varie funzioni dell'organizzazione;
- i fornitori strategici utilizzati per l'erogazione dei servizi;
- gli utenti utilizzatori dei vari servizi erogati, che a loro volta comprendono privati cittadini, dipendenti della PA, enti della PA ed operatori economici; per i servizi SERC e RDD assume particolare rilievo la ATI tra Poste San Marino SpA e Inposte SpA/tNotice®, che è il "cliente" del servizio.
- gli enti locali coinvolti.

La figura seguente rappresenta in modo grafico le parti e le loro relazioni con gli uffici soggetti a certificazione.



Le aspettative delle parti interessate, per quanto riguarda il personale interno sono stabilite a cura della Direzione di ITDS, per ogni singola persona, nel pieno rispetto dei requisiti contrattuali previsti nel contratto di lavoro.

Le aspettative per i fornitori strategici sono definite in appositi contratti per l'erogazione del servizio richiesto.

Le aspettative degli utenti utilizzatori (Ovvero: Cittadini, Operatori economici, Operatori RAO, PA) sono di avere un servizio con un elevato livello di sicurezza e di disponibilità. Poiché il servizio tNotice viene impiegato in tutte le comunicazioni tra la Pubblica Amministrazione di San Marino ed i suoi cittadini e gli enti economici, in base alla normativa vigente, una perdita di sicurezza (in termini di riservatezza, disponibilità, integrità) del servizio potrebbe generare vasti contenziosi con gli operatori interessati e, in ogni caso, una importante danno reputazionale per l'amministrazione dello stato.

Le aspettative degli enti coinvolti nella gestione delle **Informazioni CRS (Common Reporting Standard)** nei confronti di ITDS, riguardano le competenze professionali, in particolare per quanto riguarda la gestione in Sicurezza e la realizzazione di nuove infrastrutture adeguate alla situazione ed alla necessità di operare nel rispetto dei requisiti cogenti.

Le parti interessate rilevanti rispetto al SGSI e che possono avere influenza sulla sicurezza delle informazioni, durante lo svolgimento ed l'erogazione dei servizi sono:

- personale dell'area tecnica autorizzato all'accesso nelle server farm;
- responsabili di funzione e direzione autorizzati all'accesso nelle server farm;
- personale dell'area tecnica abilitato alla gestione dei flussi per garantire **i servizi in perimetro (CRS, RDD, SERC)**
- personale dell'area amministrativa coinvolto nella gestione dei **servizi in perimetro (CRS, RDD, SERC)**
- personale esterno che per manutenzioni viene temporaneamente autorizzato all'accesso in tutti i locali.

5.2. Requisiti delle parti interessate

I requisiti delle parti interessate rilevanti rispetto al SGSI che hanno influenza sull'erogazione dei servizi sono:

- requisiti cogenti richiesti da organismi internazionali (es. OCSE), Regolamenti dell'Unione Europea e norme tecniche ETSI;
- requisiti contrattuali dei servizi erogati nei confronti degli utenti;
- requisiti interni richiamati nelle procedure ed istruzioni operative che compongono il S.G.S.I.

Le norme e le leggi inerenti all'erogazione dei servizi, sono richiamate in apposito elenco di cui al paragrafo 2.

I requisiti nei confronti degli utenti che usufruiscono dei servizi della struttura di ITDS, vengono definiti dalle normative della Repubblica di San Marino.

5.3. Valutazione del contesto

5.3.1. Contesto esterno (Internazionale – Nazionale)

Gli standard internazionali rappresentano criteri, linee guida e orientamenti definiti e formalizzati nell'ambito di organismi internazionali, relativi all'applicazione della cooperazione fiscale quali, a titolo esemplificativo e non esaustivo:

- lo standard OCSE **per lo scambio automatico di informazioni** (Global standard for automatic exchange of financial account information);

- lo standard OCSE **in materia di scambio di informazioni su richiesta** (Model Agreement on Exchange of Information on Tax Matter e l'articolo 26 del Model Tax Convention on Income and on Capital);
  Nell'attuazione della cooperazione fiscale internazionale la Repubblica di San Marino applica gli standard richiamati per comunicare le informazioni relative ai Conti Oggetto di Comunicazione individuati come tali in applicazione delle norme attuative degli accordi internazionali in materia di scambio di informazioni finanziarie a fini fiscali secondo il common reporting standard.

  gli standard eIDAS (UE) definiti nel Regolamento Europeo 910/2014 (art. 5, art. 8, art.11, art. 13, art. 15, art. 17, art. 19, art. 22, art. 23, art. 24, art. 43, art. 44), qualità di Qualified Trust Service Providers (QTSP). Con una serie di Decisioni di esecuzione della Commissione (di cui la prima è la Decisione di Esecuzione 2015/1505) la descrizione degli standard tecnici di dettaglio è stata delegata alle norme ETSI.
  Nell'attivazione del servizio tNotice, l'adesione agli standard suddetti consentirà in futuro ad operatori economici e cittadini di San Marino interoperare con le controparti in altre nazioni europee in modo **sicuro**, **affidabile**, **economico** ed **utilizzabile in sede giudiziaria** in caso di contestazioni.

5.3.2. Contesto interno per il servizio CRS

L'Ufficio Centrale di Collegamento (CLO), già istituito con la Legge 18 giugno 2008 n.95, è designato quale autorità competente per implementare e dare seguito alla cooperazione amministrativa e allo scambio di informazioni in materia fiscale, conformemente agli accordi internazionali di cui all'articolo 2 della Legge n. 174/2015.

È esclusa la competenza del CLO nei rapporti di cooperazione con le autorità estere di vigilanza sui sistemi finanziari.

Il personale assegnato al CLO e coloro che collaborano con lo stesso nello svolgimento delle proprie funzioni sono obbligati al più rigoroso segreto per tutto ciò che riguarda l'attività dell'Ufficio e i suoi rapporti con i terzi. Le notizie, le informazioni e i dati in possesso del CLO in ragione dell'attività svolta sono coperti dal segreto d'ufficio.

L'obbligo di osservare il segreto d'ufficio permane in capo al personale anche dopo la cessazione del rapporto di lavoro o di collaborazione con l'Ufficio.

Sono parimenti assoggettati al rispetto del segreto tutti coloro che, in occasione di qualunque rapporto con il CLO, acquisiscano, anche involontariamente, informazioni sull'attività svolta dall'Ufficio.

Il segreto non può essere opposto all'Autorità Giudiziaria quando le informazioni richieste siano necessarie per le indagini relative a fatti penalmente rilevanti in materia fiscale.

Per lo svolgimento delle proprie funzioni l'Ufficio applica le procedure previste nel SGSI., redatte in coerenza con quanto richiesto dagli standard internazionali e periodicamente aggiornati.

Tali provvedimenti sono redatti anche sulla base delle indicazioni dell'amministrazione fiscale in materia di cooperazione internazionale.

Nello svolgimento delle proprie funzioni il CLO:

- può avvalersi della collaborazione dell'Ufficio Tributario, della Cancelleria Commerciale del Tribunale, dell'Ufficio di Controllo e Vigilanza sulle Attività Economiche, dell'Ufficio Industria Artigianato e Commercio, dell'Ufficio Informatica, Tecnologia, Dati e Statistica e degli altri Uffici della Pubblica Amministrazione;
- può richiedere la collaborazione dei Corpi del Dipartimento di Polizia, in particolare del Nucleo Antifrode della Polizia Civile, per l'acquisizione delle informazioni, nonché per il reperimento della documentazione presso i soggetti interessati;
- può richiedere la collaborazione della Banca Centrale della Repubblica di San Marino e dell'Agenzia di Informazione Finanziaria per l'approfondimento degli aspetti bancari e finanziari, fermo restando quanto disposto dalla Legge n.165/2005 e successive modifiche;
- i suddetti uffici e Autorità, così come ogni altro soggetto, sono tenuti ad evadere le richieste nelle modalità e nei tempi indicati dal CLO.

Appositi protocolli di intesa tra il CLO e, rispettivamente, l'Ufficio Attività di Controllo, la Banca Centrale, l'Agenzia di Informazione Finanziaria, l'Ufficio Tributario definiscono le forme di reciproca collaborazione e di accesso ai dati ed alle informazioni disponibili.

Analoghi protocolli possono essere definiti con altri uffici e Autorità.
I processi direttamente coinvolti nell'erogazione dei servizi sono:

- gestione del flusso delle informazioni CRS da parte dell'Ufficio Centrale di Collegamento;
- gestione del flusso delle informazioni CRS da parte degli Istituti Finanziari;
- gestione del flusso delle informazioni CRS da parte delle Autorità Competenti Estere;
- visibilità delle informazioni CRS da parte dell'Ufficio Tributario per quanto di competenza;
- assistenza tecnica alle infrastrutture che gestiscono le informazioni CRS, il relativo trasferimento attraverso le reti informatiche e le postazioni di lavoro per la gestione di tali informazioni.

Sulla base delle considerazioni fatte sopra le informazioni gestite dal Servizio CRS vanno considerate come "riservate esclusive". Non sono stati rilevati specifici vincoli riguardo alla disponibilità delle stesse eccezion fatta per la scadenza annuale delle comunicazione all'OCSE.

5.3.3. Contesto interno per i servizi tNotice (SERC e RDD)

Nel caso dei servizi SERC e RDD, come già visto, il perimetro di certificazione comprende il servizio di hosting dei server SERC e del database RDD, necessari all'erogazione del servizio.

I server SERC vengono gestiti direttamente dal fornitore del servizio tNotice (Inposte SpA). Il servizio di hosting erogato da ITDS comprende:

- la connettività, ed i relativi servizi di monitoraggio, di protezione della rete e di collegamento VPN ai sistemi;
- le risorse necessarie per l'esecuzione delle macchine virtuali;
- l'esecuzione dei backup delle macchine virtuali;
- il monitoraggio dello stato delle macchine e delle risorse utilizzate.

Il servizio relativo al database RDD erogato da ITDS in modalità "Platform as a Service" comprende:

- la connettività, ed i relativi servizi di monitoraggio, di protezione della rete e di collegamento VPN ai sistemi;
- le risorse necessarie per l'esecuzione delle macchine virtuali;
- l'esecuzione dei backup delle macchine virtuali;
- il monitoraggio dello stato delle macchine e delle risorse utilizzate;
- le macchine virtuali e la relativa gestione (licenze del sistema operativo, aggiornamenti e configurazione);
- il software per il database e la relativa gestione (licenze, aggiornamenti e configurazione).

Pertanto, nello svolgimento delle proprie funzioni il fornitore tNotice:

- riceve e filtra tutte le richieste e le segnalazioni degli utenti, comprendendo in questa categoria gli utenti esterni (imprese e cittadini) e gli sportelli postali che svolgono il ruolo di RAO e l'attività commerciale;
- esegue in completa autonomia le attività di gestione dei propri sistemi, inclusa l'applicazione degli aggiornamenti di sicurezza e degli aggiornamenti applicativi;
- può segnalare a ITDS anomalie nel comportamento delle macchine, del database e della rete (incidenti) e richiedere la cooperazione per l'analisi e la risoluzione delle stesse;
- in modo simmetrico, può ricevere segnalazioni da ITDS relativamente ad anomalie o incidenti rilevati sui sistemi, sul database e sulla rete e deve cooperare per l'analisi e la risoluzione delle stesse;
- può richiedere a ITDS una documentazione sull'utilizzo delle risorse, al fine di pianificare le future evoluzioni;
- deve segnalare preventivamente a ITDS eventi che potrebbero, anche potenzialmente, richiedere un aumento delle risorse necessarie al corretto funzionamento del sistema, come ad esempio nuove versioni del software oppure nuove modalità di utilizzo dello stesso.

Al fine di riuscire ad erogare un servizio performante ed affidabile, ITDS e tNotice dovranno instaurare un canale di comunicazione affidabile e continuo che consenta di analizzare e risolvere tutte le problematiche di carattere tecnico ed organizzativo che si possono presentare durante l'esercizio di un sistema informativo complesso.

Sulla base delle considerazioni fatte sopra le informazioni gestite dal Servizio SERC vanno considerate come "riservate". Il servizio è diretto ad un'utenza ampia e diversificata per cui va garantita una elevata disponibilità ed integrità dell'informazione.

Sulla base delle considerazioni fatte sopra le informazioni gestite dal Servizio RDD vanno considerate come "pubbliche". Risulta necessaria una elevata garanzia di integrità. Va garantita una elevata disponibilità.

5.3.4. Contesto interno per l'infrastruttura fisica

I luoghi fisici di applicazione del sistema di gestione della sicurezza delle informazioni, utilizzati all'interno della IT (Information Technology) della Pubblica Amministrazione della Repubblica di San Marino" per erogare i servizi in perimetro sono:

- Server Farm CIS
- Server Farm CU
- Ufficio Informatica, Tecnologia, Dati e Statistica - ITDS
- Ufficio Centrale di Collegamento - CLO
- Ufficio Tributario – Sezione CRS
- Centrale di rete CU
- Centrale di rete Begni
- Centrale di rete Dogana

Roberta Mularoni
Roberta Mularoni
2023.07.21
13:18:02+02'00'