Progetto Esecutivo per la fornitura dei servizi di posta elettronica e posta elettronica certificata (servizi di messaggistica) nell'ambito del sistema pubblico di connettività e cooperazione (SPC)

ASL ORISTANO

REDATTO: (Autore)	**B-PS/C.SS**	**Claudia Marchi**
APPROVATO: (Proprietario)	**B-PS/C.SS**	**Claudia Marchi**
LISTA DI DISTRIBUZIONE:		**Funzioni aziendali interessate, Amministrazione**
DESCRIZIONE ALLEGATI:	**Nell'indice**	

S O M M A R I O

Confidenziale – Tutti i diritti riservati

REGISTRAZIONE MODIFICHE DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

DESCRIZIONE MODIFICA	REVISIONE	DATA
Prima emissione	0	02/12/2013
Aggiornata sezione PEC, ed inserita sezione allegato 1	2	05/02/2014
Inserita NOTA PRELIMARE in testa ai paragrafi 5 e 7 Inseriti, in virtù della nota precedente, due nuovi paragrafi: 6.11 e 7.3 Inserita NOTA IMPORTANTE nel paragrafo 11.4 Eliminato il Work-Around sulla gestione dell'ODA a seguito dell'adeguamento del Portale ACQUISTINRETE Inserito nuovo capitolo 12	3	24/02/2014
Eliminato Allegato 1 Inseriti nuovi paragrafi su: • AntiSpam; • DOS, DDOS e FLOOD CONTROL	4	16/06/2014
Inserito dettaglio nel paragrafo "Policy di archiviazione implementate per l'Amministrazione" (01/10/2014) Inserite tabelle Riepilogo Servizi PEL e PEC (06/10/2014) Inserita tabella Elenco Referenti Specifici Fornitura (06/10/2014) Modifica Documenti di Riferimento CONSIP e PEC (17/11/2014) Aggiornamento Acronimi (17/11/2014) Inserimento nota per emissione certificato SSL(17/11/2014)	5	17/11/2014

1 SOMMARIO

Il presente documento descrive il Progetto Esecutivo del RTI Telecom Italia e Telecom Italia Trust Technologies, relativamente alla richiesta di fornitura dei servizi di posta elettronica e posta elettronica certificata (servizi di messaggistica) nell'ambito del sistema pubblico di connettività e cooperazione (SPC) per l'Amministrazione.

Quanto descritto, è stato redatto in conformità alle richieste dell'Amministrazione e sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e sulla base delle informazioni contenute nel Piano dei Fabbisogni.

2 AMBITO

Il contratto "CONTRATTO QUADRO PER LA FORNITURA DEI SERVIZI DI POSTA ELETTRONICA E POSTA ELETTRONICA CERTIFICATA (SERVIZI DI MESSAGGISTICA) NELL'AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE (SPC)" - CIG 460097088C stipulato in data 12/09/2013 ed il relativo "Addendum al Contratto Quadro per la fornitura dei servizi di posta elettronica e posta elettronica certificata (servizi di messaggistica) nell'ambito del Sistema Pubblico di Connettività e Cooperazione (SPC) in unico lotto" - CIG 460097088C del 12/9/2013 tra CONSIP S.p.A. ed il Raggruppamento Temporaneo di Impresa (RTI) formato da:

- **Telecom Italia S.p.A.** (mandataria) per la fornitura del servizio di PEL , del servizio di Supporto Specialistico e dei servizi a corredo
- **Telecom Italia Trust Technologies S.r.l.** (mandante) per la fornitura del servizio di PEC

prevedono la fornitura dei seguenti servizi nell'ambito del Sistema Pubblico di Connettività e Cooperazione (SPC):

a) Servizio di posta elettronica (PEL), nei due profili denominati:
   - Base
   - Avanzato

con il profilo Avanzato l'Amministrazione ha facoltà di richiedere i seguenti servizi opzionali:
   - "e-mail archiving";

b) Servizio di posta elettronica certificata (PEC), differenziato per tipologia di accesso/capacità della casella di posta e segnatamente:
   - "base"
   - "strutturata"
   - "massiva small"
   - "massiva medium"
   - "massiva large"

c) Servizio di supporto specialistico;

tutto secondo quanto stabilito nel Capitolato Tecnico e nell'Offerta Tecnica, nella misura richiesta dalle amministrazioni Contraenti con i Contratti di Fornitura.

Telecom Italia, in qualità di mandataria, avrà in carico tutte le attività propedeutiche all'attivazione dei servizi contrattualizzati dall'Amministrazione Contraente relative, sia alla ricezione dei Piani dei Fabbisogni ed al conseguente invio dei relativi Progetti Esecutivi, sia all'accettazione dei Contratti di Fornitura ed all'eventuale ingaggio di Telecom Italia Trust Technologies per l'attivazione dei servizi di PEC.

In particolare la procedura per l'affidamento dei predetti servizi è articolata attraverso la stipula da parte di Consip S.p.A. di un Contratto Quadro con l'Aggiudicatario della procedura medesima, che si impegna a stipulare, con le singole Amministrazioni Contraenti, Contratti di Fornitura aventi ad oggetto i predetti servizi alle condizioni stabilite nel Contratto Quadro.

Confidenziale – Tutti i diritti riservati

La durata del Contratto Quadro è fissata in 48 mesi a partire dalla data di sottoscrizione del contratto medesimo; il termine per la stipula dei Contratti di Fornitura attuativi del Contratto Quadro è fissata al termine del 36° mese di vigenza del Contratto Quadro, ovvero al minore termine determinato dall'esaurimento dell'importo massimo contrattuale del Contratto Quadro medesimo.

I singoli Contratti di Fornitura avranno una durata decorrente dalla data di ricezione del Contratto di Fornitura medesimo da parte del Fornitore sino alla scadenza ultima del Contratto Quadro, salva la previsione nei Contratti di Fornitura di una proroga tecnica di massimo 6 mesi ai soli fini di consentire la migrazione dei servizi ad un nuovo Fornitore al termine del contratto. In ogni caso, il singolo Contratto di Fornitura non può avere durata inferiore a 12 mesi, salva la facoltà del Fornitore di accettare, mediante esecuzione, Contratti di Fornitura di durata inferiore.

3 DEFINIZIONE ED ACRONIMI

La seguente tabella riporta le descrizioni o i significati degli acronimi e delle abbreviazioni presenti nel documento.

Acronimi	Descrizione
AgID	Agenzia per l'Italia Digitale
ACL	Access Control List
AD	Active Directory
AE	Archive Explorer
AID	Agenzia per l'Italia Digitale
BC	Business Continuity
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale
CMDB	Configuration Management DataBase
CED	Centro Elaborazione Dati
COS	Class of Service
DM	Decreto Ministeriale
DPCM	Decreto del Presidente del Consiglio dei Ministri
DRM	Disaster Recovery Manager
DRT	Disaster Recovery Team
DCS	Data Center Services
DSN	Delivery Status Notification
EAL	Evaluation Assurance Level
EV	(Symantec) Enterprise Vault
FIPS	Federal Information Processing Standard
HTTP	Hyper Text Transport Protocol
HTTPS	Secure HyperText Markup Language
HSM	Hardware security module
IMAP	Internet Messaging Access Protocol
IDS	Intrusion Detection System
IVR	Interactive Voice Response

Acronimi	Descrizione
IDS	Intrusion Detection System
IPv6	Internet Protocol version 6
IMAP	Internet Mail Access Protocol
IGPEC	Indice Pubblico dei Gestori di PEC
LDAP	Lightweight Directory Access Protocol
LDA	Local Delivery Agent
MTA	Mail Transfer Agent
MUA	Mail User Agent
MIME	Multipurpose Internet Mail Extensions
MDN	Message Delivery Notification
MS	Microsoft
NTP	Network Time Protocol
NFS	Network File System
NOC	Network Operation Center
OA	Outlook Anywhere
OWA	Outlook Web App
PEL	Posta Elettronica
PEC	Posta Elettronica Certificata
PDA	Personal Digital Assistant
POP	Post Office Protocol
PST	Personal information STore
PSTN	Public Switched Telephone Network
RFC	Request For Comment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTI	Raggruppamento Temporaneo di Imprese
SPC	Sistema Pubblico di Connettività
SPCoop	Sistema Pubblico di Connettività e Cooperazione
SSL/TSL	Secure Sockets Layer/ Transport Sockets Layer
SOC	Security Operation Center
SMTP	Simple Mail Transfer Protocol
SAN	Storage Area Network
TLS	Transport Layer Security
UCE	Unsolicited Commercial Email
WBS	Work Breakdown Structure

Tabella – Glossario

4 RIFERIMENTI

I documenti di riferimento della Convezione suddetta sono pubblicati sul sito www.acquistinretepa.it nella sezione “Sei un’Amministrazione” – “Che strumento vuoi usare?” – “Vetrina delle Convenzioni” – “Servizi di posta elettronica e posta elettronica certificata (servizi di messaggistica) - Contratto quadro ai sensi dell’art. 1, comma 192, Legge n. 311/2004” – “Documentazione”

4.1 Documenti contrattuali

Rif.	Documento
#1	PIANO dei Fabbisogni SERVIZIO PEC (richiesta del 28/11/2014)

Tabella dei documenti di contrattuali

4.2 Documenti di riferimento

La seguente tabella riporta i documenti che costituiscono il riferimento a quanto esposto nel seguito del presente documento.

Rif.	Documento
#1	BANDO DI GARA D’APPALTO – CONSIP S.p.A. data di spedizione 09/11/2012
#2	Allegato 5 – Capitolato tecnico – CONSIP S.p.A. Gara a procedura aperta ai sensi del D. Lgs. N. 163/2006 e s.m.i., per la fornitura dei servizi di Posta Elettronica e Posta Elettronica Certificata (servizi di messaggistica) nell’ambito del Sistema Pubblico di Connettivita e Cooperazione (SPC)
#3	Relazione Tecnica PROCEDURA APERTA PER LA FORNITURA DEI SERVIZI DI POSTA ELETTRONICA E POSTA ELETTRONICA CERTIFICATA (SERVIZI DI MESSAGGISTICA) NELL’AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE (SPC) Cod. Doc.13PA0116ATO - ver. 1 – Roma 30/01/2013
#4	CONTRATTO QUADRO PER LA FORNITURA DEI SERVIZI DI POSTA ELETTRONICA E POSTA ELETTRONICA CERTIFICATA (SERVIZI DI MESSAGGISTICA) NELL’AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE (SPC)” – CIG 460097088C stipulato in data 12/09/2013 ed il relativo “Addendum al Contratto Quadro per la fornitura dei servizi di posta elettronica e posta elettronica certificata (servizi di messaggistica) nell’ambito del Sistema Pubblico di Connettività e Cooperazione (SPC) in unico lotto” – CIG 460097088C del 12/9/2013”.
#5	Manuale Qualità di “Strutture Commerciali” – Clientela Affari – Codice Documento: MQSC
#6	Manuale della Qualità di Telecom Italia Trust Technologies S.r.l., cod. doc. CAITPRIN.IT.QUMQ10000
#7	Procedura operativa di Sistema Gestione Qualità: “Progettazione di

	sistemi/servizi personalizzati" (POSQG-PRG)
#8	Procedura operativa di Sistema Gestione Qualità: "Realizzazione con coordinamento" (POSGQ-RLZPRG)
#9	Procedura operativa di Sistema Gestione Qualità: "Assistenza tecnica ICT" (POSGQ-AT)
#10	Piano di Sicurezza – FORNITURA DEI SERVIZI DI POSTA ELETTRONICA E POSTA ELETTRONICA CERTIFICATA (SERVIZI DI MESSAGGISTICA) NELL'AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE (SPC)
#11	Piano di Collaudo per la piattaforma di Posta Elettronica e Posta Elettronica Certificata per Consip
#12	Piano di Qualità CONSIP (PEC - PEL)

Tabella dei documenti di riferimento

4.2.1 Documentazione disponibile sul sito Consip

https://www.acquistinretepa.it/opencms/opencms/main/pa/strumenti/dettaglio.jsp?idT=96237&tipoVis=catDoc&id_cat=976&vetrina=PA&idL=&nome=Servizi+di+posta+elettronica+e+posta+elettronica+certificata+%28servizi+di+messaggistica%29+-+Contratto+quadro+ai+sensi+del

4.2.2 Manualistica servizio PEC [in Allegato]

- LETTERA di VARIAZIONE della DENOMINAZIONE SOCIALE ITT-TITT
- CERTPECE.TT.SOMO14000.02 - Manuale Operativo PEC .pdf
- PECEMANU.IT.DMPS13000.03 - Posta Elettronica Certificata Guida all'Utilizzo delle Funzioni.pdf
- PECEMANU.IT.DMPS13001.05 - Manuale di configurazione del client di posta.pdf
- PECEMANU.IT.DMPS13004.01 - Guida alle funzionalità report PEC - Consip.pdf
- PECEMANU.IT.DMPS13012.03 - Posta Elettronica Certificata Guida Semplificata all'amministrazione del servizio.pdf

4.2.3 Schede di Adesione al servizio PEC [in Allegato]

- GRCONSIP.TT.MDRE13001.03 - CONSIP Scheda di Aggiornamento servizio PEC.pdf
- GRCONSIP.TT.MDRE13002.01 - CONSIP Scheda di Disattivazione servizio PEC.pdf

4.2.4 Documenti di progetto PEC [in Allegato]

- GRCONSIP.IT.DPMU13001.10 - Migrazione del servizio di PEC.pdf

5 PIANO DEI FABBISOGNI PEC

Nel seguito si riportano le consistenze che l'Amm.ne richiede di attivare nell'ambito del servizio di posta elettronica certificata (PEC).

QUADRO D: ELEMENTI DI SERVIZIO PEC

Id. servizio	Servizi Posta Elettronica Certificata	Quantità massima oggetto del Contratto di Fornitura (ODA)	Quantità da attivare (mailbox nella disponibilità del Cliente che saranno oggetto di fatturazione)
1	Casella PEC Base		
2	Casella PEC Strutturata (*)	200	100
3	Casella PEC Massiva – Small		
4	Casella PEC Massiva – Medium		
5	Casella PEC Massiva – Large		

In totale il piano dei fabbisogni contiene le consistenze da attivare con il presente Progetto Esecutivo.

5.1 Caratteristiche funzionali del servizio PEC

A livello funzionale il quadro regolatorio definisce in modo netto le caratteristiche sia infrastrutturali sia funzionali del servizio di posta elettronica certificata. AgID effettua, inoltre, delle visite ispettive con cadenza annuale che comprendono i test di interoperabilità con gli altri gestori accreditati. Pertanto il servizio di PEC offerto dal RTI, in quanto formalmente riconosciuto dal AID, è stato ritenuto conforme a tutti i requisiti minimi previsti dalle normative di riferimento indicate nel Capitolato:

- DPR 11 febbraio 2005 n.68 "Regolamento concernente disposizioni per l'utilizzo della posta elettronica certificata";
- D.Lgs. 7 marzo 2005 n. 82 "Codice dell'Amministrazione Digitale";
- DM 2 novembre 2005 del Ministro per l'Innovazione e le Tecnologie "Regole tecniche per formazione, la trasmissione, e la validazione, anche temporale, della posta elettronica certificata".

In aggiunta a quanto richiesto da Capitolato, il servizio è conforme agli ulteriori riferimenti normativi: Legge n. 2 del 28 Gennaio 2009 e DPCM del 6 maggio 2009. Il RTI garantisce, cosi come richiesto da Capitolato e senza oneri aggiuntivi, l'adeguamento del servizio alle ulteriori evoluzioni normative secondo i tempi previsti dalle stesse.

Nel seguito si riportano le caratteristiche generali del servizio focalizzando l'attenzione sulle caratteristiche funzionali prima delle singole mailbox e successivamente della piattaforma nel suo complesso.

Le caratteristiche funzionali delle mailbox, valide per tutte le tipologie di caselle, sono le seguenti:

- Invio e ricezione di messaggi asincroni sia con l'interno che con l'esterno dell'Amministrazione con garanzie in merito all'invio di un messaggio ed all'effettiva consegna dello stesso alla casella di posta certificata del destinatario. Recapito della ricevuta di accettazione (da parte quindi del Gestore del mittente) nell'arco di pochi secondi;
- Su richiesta dell'Istituto possibilità di inibire il colloquio con caselle di posta elettronica non PEC.
- Protezione e l'identificazione univoca dell'utilizzatore, mediante accesso controllato con identificativo utente e password.

Confidenziale – Tutti i diritti riservati

- Servizio fruibile in modalità:
  - Client – client di posta elettronica che sfrutti i protocolli di trasmissione standard IMAPs/POP3s e SMTPs, a titolo indicativo ma non esaustivo: MS Outlook 2007 e versioni successive , Outlook Express, Windows Live Mail, Mozilla Thunderbird, etc..
  - Web (HTTPs://www.telecompost.it/pec): utilizzo dei web browser più diffusi, ad esempio Internet Explorer, Mozilla Firefox, etc..;
  - Mobile: mediante applicazioni di posta elettronica disponibili su generici smartphone/tablet che utilizzano protocolli conformi agli standard riportati nelle regole tecniche della PEC (IMAPs/POP3s e SMTPs);
- Invio di allegati ad un messaggio di dimensione fino a 100 Megabyte. Elemento migliorativo rispetto alla normativa vigente che prevede allegati di dimensione massima di 30 Megabyte;
- Numero massimo di destinatari per un messaggio pari a 1.000. Elemento migliorativo rispetto alla normativa vigente che prevede un numero di destinatari massimo di 50;
- Nessun limite per i messaggi in ricezione.

Funzionalità aggiuntive offerte dal RTI per le singole mailbox:

- Archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella PEC, proteggendo l'utente da eventuali cancellazioni accidentali, con funzionalità aggiuntive per la ricerca e la consultazione di messaggi archiviati. Il servizio prevede l'archiviazione su supporto fisico (apposito spazio dedicato all'utente nell'infrastruttura di storage) di tutti i messaggi transitati in casella. L'accesso all'archivio, il quale è organizzato su base temporale, è possibile attraverso specifiche funzionalità aggiuntive disponibili all'utente all'interno dell'interfaccia di webmail. L'archivio è disponibile per 12 mesi ed è dimensionato in conformità ai volumi massimi di traffico espressi per ogni tipologia di casella nel capitolato tecnico.
- Avvisi via SMS/e-mail di una nuova mail PEC ricevuta, con possibilità di configurazione lasciata all'utente finale attraverso funzionalità fruibili tramite la propria interfaccia webmail;
- Inoltro dei messaggi ricevuti (di PEC e/o di PEL) verso un indirizzo secondario di PEL: consente di ricevere, anche su una o più caselle di posta ordinaria, tutti i messaggi in ricevuti nella casella di PEC, al fine di facilitare la gestione dei messaggi in ingresso alla casella di PEC stessa.
- Recupero della password, in caso di smarrimento, in maniera completamente autonoma con ricezione della stessa mediante OTP via SMS o risposta a domande segrete. Tale servizio è fruibile nella pagina web del servizio: https://www.telecompost.it/pec.

Le caratteristiche funzionali a livello di piattaforma offerta sono le seguenti:

- La sincronizzazione temporale dei sistemi e degli apparati utilizzati da T.I. Trust Technologies., rispetto alla scala di Tempo Universale Coordinato (UTC), è garantita dall'utilizzo di un sistema composto di due orologi di precisione in associazione con server NTP (Network Time Protocol)

incorporato. Gli orologi di precisione sono sincronizzati con continuità rispetto a due differenti sorgenti di tempo esterne di riferimento accedute con differenti tecnologie: il NIST americano, via telefono e il Sistema GPS internazionale, via radio. Gli orologi presenti sui server e sugli apparati di T.I. Trust Technologies sono sincronizzati in modalità automatica rispetto al sistema di sincronizzazione centrale e vengono sottoposti a continuo monitoraggio attraverso il quale si verifica il corretto allineamento dell'orologio del server rispetto a un ulteriore e differente riferimento temporale esterno italiano erogato dall'Istituto Nazionale di Ricerca Metrologica o INRIM.

- Per la protezione ed il filtraggio delle mail di PEC oggetto di fornitura la soluzione proposta dispone di misure di controllo antivirus e di antispam cosi come previsto dalla normativa vigente ed in accordo alla richiesta di Capitolato,
- Ad estensione di quanto previsto dalla normativa vigente (30 mesi), il RTI mantiene i log delle trasmissioni per un periodo maggiore pari al periodo della durata contrattuale.
- Al fine di consentire il colloquio delle caselle di PEC con la CEC-PAC è possibile pubblicare le caselle di PEC sull'Indice della Pubblica Amministrazione (IPA). Il RTI, garantisce, su richiesta dell'istituto, il supporto operativo alla pubblicazione degli indirizzi di PEC sull'Indice degli indirizzi della Pubblica Amministrazione e dei Gestori di Pubblici Servizi (INIPEC). L'Amministrazione manterrà la responsabilità delle informazioni pubblicate in coerenza con la normativa in materia.
- Per le caselle PEC strutturate e ad uso massivo, vengono prodotti dei report periodici relativi all'effettivo utilizzo delle stesse da parte delle applicazioni. [PECEMANU.IT.DMPS13004.00 - Guida alle funzionalità report PEC - Consip.pdf].

Funzionalità aggiuntive offerte dal RTI a livello di piattaforma:

- Conservazione Sostitutiva per le caselle strutturate: Sono sottoposti a conservazione i messaggi e le ricevute di tutte le mailbox di questa tipologia. Ogni Amministrazione nomina uno ed un solo incaricato al ruolo di Addetto alla Conservazione Documentale Sostitutiva (C.D.S.). Al momento dell'attivazione del servizio si comunicano all'Addetto alla C.D.S. le credenziali necessarie all'accesso al portale Web, per la ricerca e l'esibizione di documenti sottoposti a conservazione sostitutiva, tramite il quale l'Addetto potrà recuperare e consultare tutti i messaggi sottoposti al processo. La disponibilità in linea dei dati conservati è garantita per tutta la durata contrattuale. Il servizio consente la conservazione a norma di legge dei contenuti delle mailbox PEC garantendone la validità legale e preservandone nel tempo l'integrità e l'autenticità. Inoltre, per figure appositamente identificate ed autorizzate dall'Amministrazione è possibile ricercare, consultare ed esibire i messaggi quando occorre. Alla fine di ogni mese, per ogni casella, è automaticamente creato e sottoposto al processo di Conservazione Sostitutiva un lotto comprendente tutti i messaggi e le ricevute presenti per tale mese. L'Amministrazione ha la possibilità in ogni momento di estrarre una parte dei documenti conservati e produrre su supporti ottici lotti auto-consistenti di documenti per l'esibizione a norma degli stessi.
- Sistema di self provisioning: allo scopo di consentire all'Amministrazione di mantenere il controllo sulla gestione delle utenze, è prevista, in accordo con l'Amministrazione, l'individuazione di referenti di contratto per cui venga profilato un accesso sulla console di gestione del dominio. Nel caso di Amministrazioni con due o più domini di posta certificata, è possibile creare viste dedicate al singolo dominio oppure viste complessive che permettano di sovrintendere a più domini. Di seguito un elenco delle funzionalità fruibili attraverso tale console di gestione:
    - Profilare, registrare e disabilitare utenti;
    - Creare, modificare ed eliminare caselle, identificandone la tipologia tra quelle offerte ed il relativo utente Titolare. Nel caso di caselle strutturate è possibile associarla ad uno o più utenti. Inoltre per la singola casella è possibile abilitare l'accesso via client, abilitare il servizio di avviso via SMS o mail e di inoltro delle mail su indirizzo/i secondari/o di PEL,
    - Inibire il colloquio con caselle non-PEC sia a livello di dominio sia di singola casella e/o il colloquio con qualsiasi tipologia di casella (PEC/PEL) a livello di singola casella o lista di caselle;
    - Inibire l'utilizzo di liste di distribuzione globali;

- Creare, modificare, eliminare liste di distribuzione;
- Rigenerare le credenziali di accesso per gli utenti tramite invio di OTP via sms/mail. Una volta ricevuto tale codice l'utente, tramite il link apposito presenti sulla pagina di accesso al servizio di PEC (https://www.telecompost.it/pec), potrà impostare una nuova password di accesso ai servizi.

5.1.1 Caselle base

La Casella PEC Base è di esclusiva pertinenza di un singolo utente che vi accede mediante l'immissione delle proprie credenziali (userid e password).

Le caselle di tipologia Base presentano le seguenti caratteristiche:

- Numero massimo di invii giornalieri: 500;
- Numero massimo di invii al minuto: 50;
- Dimensione della mailbox: 2Gb;
- Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi;
- Dimensione massima dei messaggi: 100MB;
- Invio dello stesso messaggio fino a 1.000 destinatari;
- Recupero della password, in caso di smarrimento, in maniera completamente autonoma con ricezione della stessa mediante SMS o email di posta elettronica ordinaria;
- Avvisi via SMS o via email dell'arrivo di un nuovo messaggio di PEC;
- Forward dei messaggi di PEC ricevuti verso un indirizzo di posta elettronica ordinaria.

5.1.2 Caselle strutturate

È una tipologia di casella a cui è consentito l'accesso da parte di un gruppo limitato di utenti precedentemente autorizzati. Il RTI prevede un meccanismo di verifica dell'appartenenza dell'utente al gruppo di utenti associati alla casella che possono accedere alla casella multiutente: solo le persone preventivamente autorizzate potranno accedervi. L'accesso è profilato e con credenziali personali:Può avvenire attraverso webmail, applicazione o client.

- *Webmail.* È presente un meccanismo di controllo delle possibili sovrapposizioni tra i vari utenti appartenenti al gruppo, che inibisce la modifica dello stato di un messaggio di PEC preso in carico da un utente fino al suo rilascio. L'utente che ha in carico il messaggio può decidere di rilasciarlo (consentendo ad altri utenti di prenderlo in carico) oppure può decidere di completarlo. E' tracciata ogni singola operazione effettuata sul messaggio e lo storico delle operazioni può essere visualizzato dagli utenti associati alla casella. La presa in carico di un messaggio, da parte di un utente del gruppo, consente di rispondere, inoltrare ed inserire eventuali allegati al messaggio originale: si può prendere in carico un messaggio solo se nessun altro utente lo ha già preso in carico; il titolare della casella può vedere se il messaggio è completato. L'interfaccia Web per l'utilizzo delle caselle multiutente garantisce sicurezza nell'accesso e protezione dei contenuti: l'accesso alla casella è consentito ai soli utenti abilitati e autenticati. Le operazioni effettuate dagli operatori (replica, accesso alla corrispondenza elettronica, lavorazione etc.) sono registrate. Inoltre il sistema attribuisce a ciascun messaggio un codice identificativo progressivo che consente di gestire flussi consistenti di corrispondenza elettronica in entrata ed in uscita, garantendo le funzionalità di visualizzazione, ordinamento e lavorazione della corrispondenza elettronica. È infine previsto un meccanismo di controllo delle possibili sovrapposizioni tra i vari utenti appartenenti al gruppo che prevede la presa in carico di un messaggio da parte degli utenti per la lavorazione e che rende impossibile modificare un messaggio preso in carico da un altro utente, fino al suo rilascio.

- *Applicazione*. Nel caso l'Amministrazione disponga di applicativi che interfaccino la casella PEC per traffico non massivo, la profilazione degli utenti cosi come la gestione dei messaggi sono demandate a tale applicativo.
- *Client*. E' possibile, infine, utilizzare le caselle strutturate anche attraverso client di posta standard che utilizzino i protocolli POP3S/IMAPS e SMTPS. In tal caso le funzionalità lato utente sarebbero quelle native dei client di posta.

La casella PEC Strutturata prevede la possibilità di accesso alla mailbox da parte di un gruppo di utenti preventivamente autorizzati. Ciascuno degli utenti della casella farà accesso alla mailbox adoperando le proprie credenziali personali.

Le caselle di tipo Strutturato presentano le seguenti caratteristiche:

- Numero massimo di invii giornalieri: 500;
- Numero massimo di invii al minuto: 50;
- Dimensione della mailbox: 4Gb;
- Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi;
- Dimensione massima dei messaggi: 100MB;
- Invio dello stesso messaggio fino a 1.000 destinatari;
- Recupero della password, in caso di smarrimento, in maniera completamente autonoma con ricezione della stessa mediante SMS o email di posta elettronica ordinaria;
- Avvisi via SMS o via email dell'arrivo di un nuovo messaggio di PEC;
- Forward dei messaggi di PEC ricevuti verso un indirizzo di posta elettronica ordinaria.

L'Amministrazione nomina un incaricato al ruolo di Addetto alla Conservazione Documentale Sostitutiva (C.D.S.). Al momento dell'attivazione del servizio si comunicano all'Addetto alla C.D.S. le credenziali necessarie all'accesso al portale Web, per la ricerca e l'esibizione dei documenti sottoposti a conservazione sostitutiva, tramite il quale l'Addetto potrà recuperare e consultare tutti i messaggi sottoposti al processo. La disponibilità in linea dei dati conservati è garantita per tutta la durata contrattuale. Il servizio consente la conservazione a norma di legge dei contenuti delle mailbox PEC garantendone la validità legale e preservandone nel tempo l'integrità e l'autenticità. Inoltre, per figure appositamente identificate ed autorizzate dall'Amministrazione è possibile ricercare, consultare ed esibire i messaggi quando occorre.

Alla fine di ogni mese, per ogni casella, è automaticamente creato e sottoposto al processo di Conservazione Sostitutiva un lotto comprendente tutti i messaggi e le ricevute presenti per tale mese. L'Amministrazione ha la possibilità in ogni momento di estrarre una parte dei documenti conservati e produrre su supporti ottici lotti auto-consistenti di documenti per l'esibizione a norma degli stessi.

5.1.3 Caselle massive

La Casella PEC Massiva è in grado di gestire l'invio e la ricezione di un numero elevato di messaggi (e relative ricevute) in modalità completamente automatica, come tipicamente avviene nei casi di integrazione della PEC con strumenti di gestione del workflow documentale e/o altri strumenti software.

Sono disponibili 3 diversi formati per le caselle di tipo Massivo:

5.1.4 Casella Massiva Small

- Dimensione della mailbox: 4Gb;
- Numero massimo di invii giornalieri: 2.000;
- Numero massimo di invii al minuto: 200;

Confidenziale – Tutti i diritti riservati

- Dimensione media dei messaggi 200 kbyte;
- Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi;
- Dimensione massima dei messaggi: 100MB;
- Invio dello stesso messaggio fino a 1.000 destinatari;
- Recupero della password, in caso di smarrimento, in maniera completamente autonoma con ricezione della stessa mediante SMS o email di posta elettronica ordinaria.

5.1.5 Casella Massiva Medium

- Dimensione della mailbox: 12Gb;
- Numero massimo di invii giornalieri: 6.000;
- Numero massimo di invii al minuto: 600;
- Dimensione media dei messaggi 200 kbyte;
- Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi;
- Dimensione massima dei messaggi: 100MB;
- Invio dello stesso messaggio fino a 1.000 destinatari;
- Recupero della password, in caso di smarrimento, in maniera completamente autonoma con ricezione della stessa mediante SMS o email di posta elettronica ordinaria.

5.1.6 Casella Massiva Large

- Dimensione della mailbox: 24Gb;
- Numero massimo di invii giornalieri: 12.000;
- Numero massimo di invii al minuto: 1.200;
- Dimensione media dei messaggi 200 kbyte;
- Servizio di archiviazione automatica dei messaggi inviati e ricevuti dalla propria casella per 12 mesi;
- Dimensione massima dei messaggi: 100MB;
- Invio dello stesso messaggio fino a 1.000 destinatari;
- Recupero della password, in caso di smarrimento, in maniera completamente autonoma con ricezione della stessa mediante SMS o email di posta elettronica ordinaria.

5.1.7 Sistema di self provisioning

Allo scopo di consentire all'Amministrazione di mantenere il controllo sulla gestione delle utenze, è prevista, in accordo con l'Amministrazione, l'individuazione di referenti di contratto per cui venga profilato un accesso sulla console di gestione del dominio. Nel caso di Amministrazioni con due o più domini di posta certificata, è possibile creare viste dedicate al singolo dominio oppure viste complessive che permettano di sovrintendere a più domini. Di seguito un elenco delle funzionalità fruibili attraverso tale console di gestione:

- Profilare, registrare e disabilitare utenti;
- Creare, modificare ed eliminare caselle, identificandone la tipologia tra quelle offerte ed il relativo utente Titolare. Nel caso di caselle strutturate è possibile associarla ad uno o più utenti. Inoltre per la

singola casella è possibile abilitare l'accesso via client, abilitare il servizio di avviso via SMS o mail e di inoltro delle mail su indirizzo/i secondari/o di PEL,

- Inibire il colloquio con caselle non-PEC sia a livello di dominio sia di singola casella e/o il colloquio con qualsiasi tipologia di casella (PEC/PEL) a livello di singola casella o lista di caselle;
- Inibire l'utilizzo di liste di distribuzione globali;
- Creare, modificare, eliminare liste di distribuzione;
- Rigenerare le credenziali di accesso per gli utenti tramite invio di OTP via sms/mail. Una volta ricevuto tale codice l'utente, tramite il link apposito presenti sulla pagina di accesso al servizio di PEC (https://www.telecompost.it/pec), potrà impostare una nuova password di accesso ai servizi.

Il manuale di Amministrazione [in Allegato] è : "**PECEMANU.IT.DMPS13012.03 - Posta Elettronica Certificata Guida Semplificata all'amministrazione del servizio.pdf**".

Il Referente identificato dall'Amministrazione è :

NOMINATIVO: Ing. Dina Ari

CF:

TELEFONO:

EMAIL: dina.ari@asloristano.it

5.1.8 Elenco dei domini da migrare

L'Amministrazione ha richiesto la migrazione del dominio pec.asloristano.it già in gestione TI- TT

5.2 Piano temporale di attivazione del servizio PEC

Trattandosi di migrazione di contratto le tempistiche saranno concordate con l'Amministrazione.

6 ARCHITETTURA DELLA PIATTAFORMA PEC

Di seguito vengono descritte le caratteristiche architetturali e l'organizzazione logica delle componenti della piattaforma di posta elettronica certificata PEC.

6.1 Descrizione generale della piattaforma PEC

La soluzione di PEC che il RTI propone si basa su una piattaforma conforme agli standard normativi in materia, certificata con cadenza annuale da AID e che già eroga servizi per clienti privati e Pubbliche Amministrazioni centrali e locali.

La logica che sottende la soluzione è la multitenancy, l'utilizzo cioè di una singola istanza di piattaforma a servizio di molteplici clienti in cui i set di informazioni delle singole Amministrazioni sono isolati tra loro attraverso avanzate logiche di segregazione applicativa, implementate in tutti gli ambiti: gestione delle utenze, dei dati contenuti nelle caselle e dei relativi spazi di archiving. A livello applicativo la soluzione offerta dal RTI è proprietaria ed aggiornata all'ultima versione disponibile.

Nel descriverla se ne darà pertanto un approfondimento tale da garantire comunque la riservatezza sulle componenti tecnologiche o le soluzioni custom che contraddistinguono il servizio. La soluzione tecnologica, in aggiunta alle funzionalità elementari di invio e ricezione e-mail, prevede l'interazione con motori di cifratura e firma massiva delle mail, prodotti antivirus ed antispam con dinamiche ben definite nelle normative, archiviazione delle mail e logging delle transazioni.

Alle funzionalità core, strettamente attinenti al servizio di posta certificata, si aggiungono gli strumenti di gestione e self provisioning che conferiscono al servizio flessibilità ed adattabilità alle esigenze dell'Amm.ne.

Tali strumenti, rappresentano un valore aggiunto alla soluzione in quanto permettono all'utente finale o al referente tecnico, a seconda della profilazione, di compiere azioni attuative sul proprio dominio di posta.

Il RTI è consapevole che contestualmente alla scelta di prodotti tecnologicamente avanzati, funzionalità aderenti alle necessità dell'Amministrazione, è fondamentale garantire un servizio affidabile e con prestazioni adeguate attraverso l'utilizzo di soluzioni infrastrutturali ed operative che garantiscano elevati livelli di qualità.

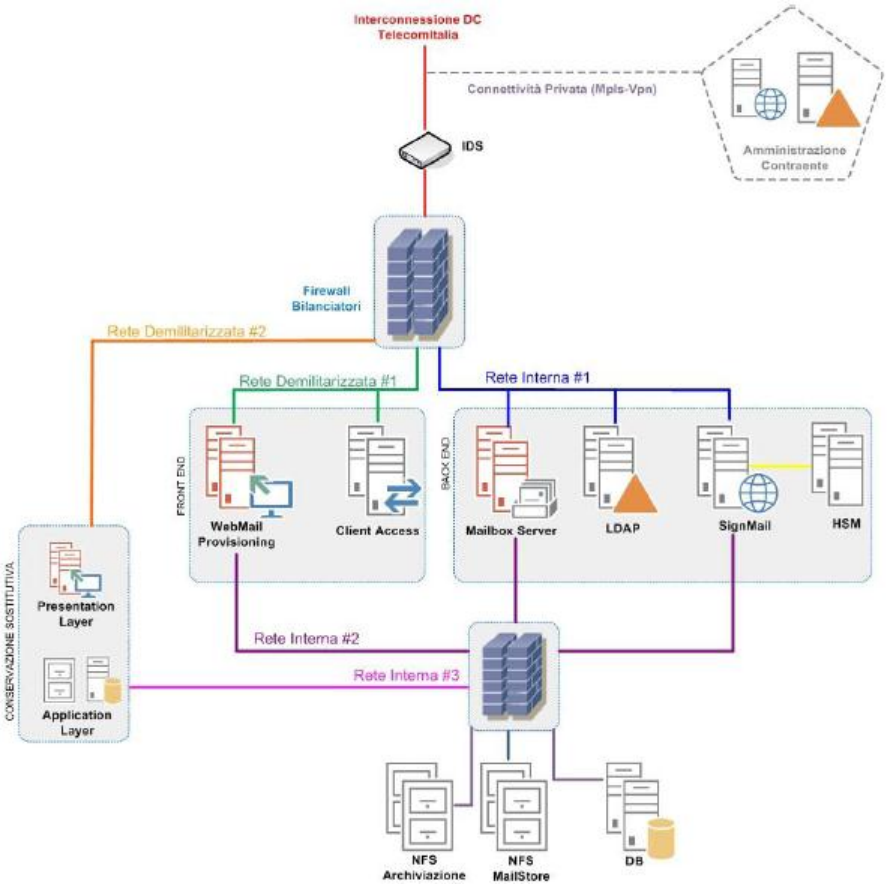
Per quanto riguarda le prestazioni della piattaforma, ogni componente logica e fisica della piattaforma è progettata per garantire la massima scalabilità verticale e orizzontale. La separazione dei ruoli applicativi e la modularità delle componenti software utilizzate consente di monitorare le prestazioni con un elevato livello di granularità, individuando rapidamente eventuali colli di bottiglia e agendo opportunamente sul dimensionamento delle stesse. A fronte di un rallentamento anomalo derivante da un particolare picco di traffico è possibile avviare più istanze delle stesse componenti (ad es. aumentando il numero delle code di traffico) al fine di incrementare il parallelismo e diminuire il tempo di elaborazione del singolo messaggio. La configurazione dei sistemi più critici, ovvero quelli più soggetti al carico derivante dagli utenti, consente di scalare rapidamente mediante l'aggiunta di nuovi nodi al pool di bilanciamento. A titolo di esempio è possibile citare il caso dei sistemi di front-end (WebMail-Provisioning, Client Access) o dei Mailbox Server che possono essere ampliati rapidamente per fronteggiare un trend crescente del traffico mail o l'acquisizione di un numero di mailbox più alto rispetto a quanto preventivato. I servizi ed i sistemi sono controllati in modo automatico da due diversi sistemi di monitoraggio che consentono la visualizzazione e la notifica degli allarmi:

- "Sistema Esterno" consente il controllo dei servizi erogati in rete dall'infrastruttura effettuando accessi periodici ai servizi tramite collegamento esterno in ADSL su rete Internet;
- "Sistema Interno" utilizza un Network Management System completamente gestito dagli addetti della CA che consente di mantenere il controllo della rete e dei sistemi fornendo importanti informazioni per la corretta gestione sistemistica. Le principali caratteristiche del sistema interno sono:
    - Il controllo del funzionamento dei sistemi in rete;
    - Il controllo della raggiungibilità dei sistemi;
    - Il controllo dello stato dei sistemi quali ad esempio utilizzo CPU e RAM, spazio disco ancora disponibile, corretto funzionamento delle schede di rete, controllo dei processi, ecc.;

- Il controllo del corretto allineamento dell'orologio dei server rispetto a un ulteriore e differente riferimento temporale esterno italiano erogato dall'Istituto Nazionale di Ricerca Metrologica o INRIM.

L'esecuzione giornaliera di appositi script segnala tramite Trap al sistema di monitoraggio eventuali modifiche anomale apportate al sistema (es. modifica degli eseguibili, modifica delle utenze). Le prestazioni generali del servizio vengono monitorate con due diverse modalità: on-demand mediante l'esecuzione da parte del personale di presidio di tool scritti ad hoc per effettuare l'analisi delle code di elaborazione dei messaggi ed automaticamente, mediante l'esecuzione periodica di script dedicati all'analisi statistica dei tempi minimi, medi e massimi di accettazione/consegna di un messaggio e delle login ai servizi di accesso (es. WebMail). La vista d'insieme, offerta dal monitoraggio, dello stato delle singole componenti hardware e software e dei flussi interni consente di identificare il trend di utilizzo delle risorse e gestire così i picchi periodici nonché pianificare per tempo eventuali scale-out di piattaforma.

La figura di seguito illustra la soluzione architetturale proposta per il servizio di PEC. Tale schema è un'astrazione logica volta ad identificare le componenti funzionali della piattaforma. A livello fisico, come verrà dettagliato in seguito, la piattaforma implementa soluzioni di ridondanza e high-availability per ogni singolo elemento infrastrutturale, nel seguito si dettagliano le singole componenti.



L"infrastruttura per l'erogazione del servizio comprende le seguenti componenti:

Intrusion Detection (IDS) SNORT, in tecnologia Open-Source, è integrato nei sistemi di protezione perimetrale e si occupa di controllare in tempo reale il traffico esplicitamente permesso identificando e prevenendo una grande varietà di attività di rete considerate sospette.

Firewall e Bilanciatori, tali apparati si occupano di isolare i diversi livelli della piattaforma e di bilanciare il traffico sulle varie componenti infrastrutturali, cosi da garantire le migliori prestazioni.

WebMail-Provisioning, che espone i servizi di Webmail e Provisioning, funzionalità di configurazione/Amministrazione della casella, per l'utente, e di gestione del dominio per i referenti autorizzati.

Client Access realizza tutte le funzionalità necessarie alla gestione perimetrale dei messaggi ed è inserita nella zona esposta su Internet/Intranet. Essa implementa le seguenti funzionalità: Proxy, Antivirus/Antispam, Mail Transfer Agent, Mail Relay, Class of Service- COS Manager.

COS Manager si occupa di controllare il rispetto dei limiti di traffico da parte delle caselle gestite. All'invio di una nuova mail in base alla Classe di Servizio assegnata alla casella mittente e al traffico già prodotto dalla stessa, determina se questa deve essere accettata o rifiutata. Le informazioni relative alla Classe di Servizio vengono reperite all'occorrenza mediante accesso alla componente LDAP.

SignMail, la componente di firma si occupa della certificazione dei messaggi, firma digitale per i messaggi in uscita e verifica di integrità per quelli in ingresso e firma dei messaggi di posta ordinaria in ingresso, secondo quanto previsto dalla normativa, e della loro consegna in casella.

LDAP Server, contiene il ramo dei provider e dei domini certificati, nonché l'elenco delle utenze e delle caselle gestite.

Mailbox Server, si occupa della gestione delle mailbox utente. Viene utilizzato per l'accesso da client alle caselle PEC e per la lettura della struttura e dei dati contenuti in casella, sia dall'interfaccia webmail sia da client di posta. Su questo sistema è implementata anche un'applicazione di controllo periodico delle tipologie di virus che non sono state rilevate dal sistema antivirus online, al fine di comprenderne le cause e verificare l'opportunità di eventuali interventi. Questa applicazione controlla periodicamente la presenza di eventuali virus nei messaggi contenuti nelle caselle ed emette un report riepilogativo di quanto riscontrato. Viene quindi eseguita la rimozione degli eventuali messaggi contenenti virus e inviata un'informativa al titolare della casella in merito alla rimozione effettuata.

Database server : mantiene i dati applicativi, sia per quanto riguarda l'anagrafica degli utenti del sistema di PEC che le tabelle contenenti i messaggi transitati nel sistema.

HSM: custodisce le chiavi private ed i relativi certificati necessari alle operazioni di firma dei messaggi.

NFS: sono le componenti storage che attraverso un Network File System consentono la memorizzazione della struttura IMAP delle caselle PEC esistenti sul sistema e delle relative caselle di archivio temporale.

La soluzione di Conservazione Sostitutiva è composta di due livelli logici. La parte di Application Layer gestisce le procedure di acquisizione dei dati dal sistema di Archiviazione, procede alla firma dei volumi ed allo storage sul DB di conservazione. Il livello di Presentation si occupa di esporre i servizi di retrieve ai responsabili designati dall'Amministrazione.

6.2 Soluzioni di connettività per l'erogazione del servizio PEC

Verrà utilizzata la connettività internet

6.3 Soluzioni di Alta Affidabilità dei dati

L'affidabilità del servizio in termini di erogazione e di disponibilità delle informazioni è ottenuta attraverso l'adozione di soluzioni di ridondanza infrastrutturale a più livelli.

Tutti i componenti critici della piattaforma di erogazione sono configurati per operare in modalità ridondata: configurazione in High Availability e in load sharing, cioè ogni singola funzionalità è erogata da più macchine, in configurazione cluster, così da garantire la continuità del servizio anche a fronte di eventuali fault. Se uno dei componenti si guasta la sua funzione può essere mantenuta da un componente di riserva senza interventi da parte degli operatori.

Gli apparati sono sottoposti a monitoraggio sistemistico, applicativo e prestazionale H24-365 giorni l'anno con possibilità di intervento delle strutture tecniche, di elevata professionalità e con una lunga e consolidata esperienza, per la risoluzione di problematiche bloccanti.

6.4 Soluzioni per la continuità operativa

Allo scopo di massimizzare l'affidabilità della soluzione proposta, il servizio di PEC viene erogato attraverso due piattaforme che operano in logica di Business Continuity, ospitate in Data Center Telecom Italia di Pomezia ad opportuna distanza l'uno dall'altro. Ciò assicura alle Amministrazioni contraenti la disponibilità del servizio a fronte di eventi avversi e guasti bloccanti sul sito primario, azzerando i tempi di ripristino senza perdita di dati**, RPO ed RTO uguali a zero**.

L'attività di ripristino totale o parziale di dati utilizza le componenti software ed infrastrutturali del sistema di back-up; tale attività si articola nei seguenti passi: identificazione del perimetro d'intervento, ovvero individuazione dei server sui quali deve essere eseguita l'attività di ripristino per rendere consistenti i dati, selezione dei dati di back-up in base all'identificativo temporale (giorno e ora), infine esecuzione del restore dei dati e verifica dell'esito positivo; nel caso in cui il restore non abbia esito positivo, viene effettuata un'operazione di roll-back.

A ciò si aggiunge un ulteriore grado di affidabilità proveniente dai seguenti elementi infrastrutturali: alimentazione elettrica duplicata grazie a sistemi STS, gruppi di continuità UPS, connessioni di rete ridondate, architettura della piattaforma implementata secondo la logica ridondata active-active (il software installato su tutti i nodi che costituiscono ogni singola componente dell'infrastruttura è allineato e costantemente aggiornato; in condizioni normali il traffico verso ogni componente viene bilanciato sui singoli nodi, nel caso invece un nodo fosse indisponibile, il traffico viene automaticamente indirizzato verso i nodi attivi). Tali accorgimenti pongono rimedio in caso di guasti più ad alto livello che impattano uno dei due CED (allagamento, incendio, sabotaggio, etc.). L'utilizzo di due piattaforme ubicate in due Data Center separati garantisce la disponibilità e l'indipendenza anche delle seguenti risorse: alimentazione a livello Data Center, alimentazione di continuità (UPS), Impianto Smaltimento Termico, impianto antincendio, protezione fisica.

In aggiunta, il RTI mette a disposizione un sito di Disaster Recovery, nel Data Center Telecom Italia di Oriolo Romano, come ulteriore protezione dei sistemi dagli eventi di natura disastrosa che si possono verificare sul sito di erogazione principale. Il DC di Oriolo è conforme ai principali standard di sicurezza internazionale ed in particolare implementa un Sistema di Gestione della Sicurezza delle Informazioni certificato ISO 27001. La piattaforma sul sito secondario è realizzata con caratteristiche funzionali simili a quelle del sito primario ma con capacità computazionali ridotte. Il servizio prevede la definizione di procedure per la replica dei dati ed il ripristino del servizio. Il sito di Disaster Recovery è sempre attivo e le informazioni contenute nel sito primario sono allineate sul sito secondario tramite l'infrastruttura di trasporto a 10 Gbps fra i due Data Center di Telecom Italia. Il Sito di Recovery inoltre non è normalmente raggiungibile dall'esterno: solo in caso di evento disastroso il sito di DR è reso raggiungibile dall'esterno mediante lo switch della rete di accesso effettuato in sinergia tra le strutture di rete geografica del RTI. L'attivazione del sito e delle procedure di Disaster

Recovery ed il ritorno alla normale operatività è regolata da appositi Piani Operativi. Le tipologie di incidenti prese in considerazione e a fronte delle quali è attivabile il Piano di DR sono:

- incidenti dovuti a cause naturali (uragano, terremoto, fulmine, alluvioni, esondazioni, altri eventi disastrosi);
- incidenti non naturali premeditati o accidentali (problemi di carattere ambientale, danni volontari, incendi, etc);
- incidenti alle facility/infrastrutture (malfunzionamento impianti, mancanza di alimentazione elettrica).

Le procedure descritte nei dettagli in tali Piani Operativi consentono al personale la gestione del traffico di rete e di cambiare le rotte di instradamento verso il nuovo sito di DR. Nei Piani Operativi sono inoltre descritte le procedure che permettono, in seguito alla riattivazione del sito primario, di fare un allineamento dei dati dal sito di DR così da garantire una continuità degli eventi accaduti. L'architettura High Level distribuita sui tre siti (Produzione, BC, DR) si compone di diverse tecnologie abilitanti al fine di indirizzare in modo ottimale le esigenze per ogni layer dello stack DR. In particolare si ottengono RPO ed RTO tendenti a zero tramite l'utilizzo di tecniche di replica sincrona dei dati su un sito locale di BC. Per il sito di DR si ottengono RPO tendente a zero con l'utilizzo delle seguenti tecniche:

- Replica dei dati residenti su DB utilizzando tecnologie di replica a livello software (log shipping e standby DB), che consentono di avere sul sito remoto una copia consistente a livello applicativo per architetture complesse multi-istanza;
- Replica dei dati residenti su file system effettuata attraverso tecnologie di data replication host-based.

Tale soluzione consente di garantire protezione e ridondanza dei dati rendendo possibile la ricostruzione completa degli ambienti tramite funzionalità di allineamento massivo offerte dalle tecnologie di data replication a livello array. La piattaforma di DR prevede la replica dei dati contenuti nei database e dei dati archiviati su file system, mentre l'allineamento delle configurazioni e del software (applicativi), oltre che dei software di base (S.O.), viene effettuata tramite copia dei file di configurazione su aree di filesystem oggetto di replica; tale soluzione richiede comunque l'attuazione di attività di ripristino (manuali o automatizzate tramite script) al fine di rendere operative le configurazioni sui sistemi di DR.

6.5 Livelli di sicurezza implementati

La PEC offre un servizio che garantisce all' utilizzatore integrità, autenticità e non ripudiabilità del messaggio che si sta inviando/ricevendo. Tali caratteristiche vengono assicurate da un lato da processi di emissione che sono identificati e certificati dalla normativa, dall'altro dall'adozione di accorgimenti a livello di infrastruttura centrale che riducano i rischi di vulnerabilità del sistema. In questo paragrafo viene descritta la sicurezza delle informazioni, attraverso soluzioni IT in modo da garantire la protezione e l'inaccessibilità delle informazioni ad eventuali attacchi esterni/interni.

Servizi perimetrali

Intrusion Detection (IDS), SNORT, controlla in tempo reale il traffico esplicitamente permesso ed identifica e previene una grande varietà di attività di rete considerate sospette. Tale controllo viene svolto confrontando le „signatures" di attacchi noti e eventuali anomalie sui protocolli del traffico in transito. Sia le signatures predefinite dell'IDS sia il motore IDS vengono costantemente aggiornati tramite l'apposita rete di distribuzione del fornitore, previa autenticazione e cifratura delle comunicazioni. La logica con la quale è costruito il sistema di IDS lo rende un sistema sia di alert che di prevenzione agli attacchi. Le configurazioni previste per l'IDS sono create in maniera da rilevare e fermare le minacce principali ma non inficiare la funzionalità della rete. Le porte di „sniffing" sono configurate in modalità passiva e non visibili sulla rete

Firewall. L'infrastruttura specifica della piattaforma PEC prevede un sistema firewall, configurato in alta affidabilità, che filtra il traffico da Internet/SPC verso la componente di Front-End, ed una seconda linea costituita da un altro sistema firewall che filtra il traffico tra la componente di Front-End e quelle di Back End. I servizi di Firewall costituiscono la prima barriera di protezione per l'accesso ai servizi erogati dal dominio di pertinenza, si basano su tecnologia Nokia IP1280 per il Front-End e Nokia IP560 per la parte di BackEnd.

Antivirus/Antispam: i flussi in ingresso/uscita dalla piattaforma vengono esaminati da un motore Antivirus ed uno Antispam integrati in Amavisd-new. Grazie all‟utilizzo del protocollo SMTP, Amavisd-new è compatibile con i più diffusi prodotti che realizzano funzionalità di MTA: PostFix, Sendmail, Sun Java Messaging etc. in quanto indipendente dalla piattaforma middleware. Nelle sue funzionalità di AntiSpam/AntiVirus, il modulo integra due componenti: ClamAV e SpamAssassin.

- Antivirus – ClamAV. Le basi virali dell‟Antivirus sono costantemente aggiornate dalla comunità Open Source e vengono scaricate automaticamente (o manualmente se necessario) ogni due ore. Le definizioni dei virus e malware di ClamAV, consistenti in un database attualmente contenente oltre due milioni di signature, sono aggiornate giornalmente mediante una connessione http/https; in particolare viene aggiornata solo una parte del database delle firme (“daily.cvd”) e non l’intero database, dato che si considerano ormai „stabili‟ circa 1.8M di firme. Il download delle firme ClamAV avviene utilizzando un gruppo di server selezionati per la nazione di provenienza della richiesta di download. Solo per l’Italia sono al momento disponibili 3 server, ma in tutto il mondo il numero di mirror è superiore alle cento unità. Qualora il software non riuscisse ad effettuare il download dal primo mirror, selezionato in round-robin, riproverà ad effettuare il download da uno degli altri mirror disponibili.
- Antispam – SpamAssassin. L’utilizzo di SpamAssassin come motore anti-spam garantisce una buona precisione nel filtering e nell‟identificazione dello spam, anche senza l’utilizzo di “bayesian analysis” e quindi senza la necessità di effettuare tagging e auto-apprendimento. Per la gestione dello spam viene impostato tra gli header del messaggio un tag che indica la percentuale di probabilità che il messaggio sia di spam. In caso di rilevamento di virus all’interno di una mail invece ci sono da distinguere diversi comportamenti a seconda che la mail sia di PEC o di PEL:
  - Mail di PEC: il messaggio viene opportunamente marcato e passato alla componente di Firma per la gestione secondo normativa dei messaggi con virus.
  - Mail di PEL: il messaggio viene scartato.

Le funzionalità offerte lavorano in modo totalmente trasparente per l’utenza (senza necessità di alcuna configurazione) in quanto sono gestite centralmente dal RTI. All’utilizzatore finale è lasciato solo il compito di verificare, nel caso dello spam, che eventuali messaggi scartati non siano realmente messaggi validi (gestione dei falsi positivi) mentre, in caso di rilevazione di virus viene generato un avviso di mancato invio/ricezione del messaggio contenente virus, così come previsto dalla normativa sulla PEC. È invece compito del RTI controllare almeno settimanalmente quali tipologie di virus non sono state rilevate dal proprio sistema antivirus al fine di comprenderne le cause e verificare l’opportunità di eventuali interventi.

Sicurezza nei flussi di dati

Nell’ambito dell’infrastruttura descritta vengono generati degli specifici flussi dati necessari per le comunicazioni tra differenti componenti della stessa. Tali flussi dati seguono percorsi predeterminati e controllati secondo le specifiche di sicurezza previste per l’infrastruttura del certificatore.

E‟ possibile individuare due tipologie di flussi di dati:

- Flussi dati interni allo stesso “layer” infrastrutturale (es. flussi di comunicazione tra componenti del livello “back-end”): riguarda esclusivamente le comunicazioni tra componenti dello stesso “strato”, sottoposte a regole di sicurezza specifiche che sono definite per la singola componente (server o gruppo di server). Un esempio di tali regole è certamente il controllo di accesso verso un sistema/servizio. Trattandosi di flussi dati interni ad uno stesso dominio vengono considerati flussi dati con scarsa criticità relativa alla sicurezza, soprattutto per quanto riguarda quelli interni al back-.end che, di fatto, sono scollegati da elementi di rete esterni.
- Flussi dati di comunicazione tra diversi “layer” infrastrutturali (es. il flusso dati in transito da back-end a front-end): servono ad alimentare lo scambio dati tra diversi livelli. Tipicamente si tratta di flussi che dai livelli più bassi si dirigono verso i livelli più alti per la presentazione dei dati (es. da back-end verso front-end). Il passaggio da un livello all‟altro è appositamente controllato e filtrato dalla componente di IDS e FW,per garantire i massimi standard e livelli di sicurezza necessari per le componenti “core” dell‟infrastruttura del certificatore.

I passaggi inversi, da livello superiore a livello inferiore, sono rigidamente normati sia a livello di politiche di sicurezza pre-determinate che a livello di controllo accessi real-time.

Vulnerability Assessment: Il servizio proposto si realizza attraverso la ricerca sistematica delle vulnerabilità di un sistema o di una rete, al fine di fornire una valutazione oggettiva del grado di adeguatezza delle misure di protezione poste in essere o da definire.

Penetration Test: Il servizio si colloca a complemento del Vulnerability Assessment ed è realizzato secondo metodologie riconosciute internazionalmente (OSSTMM-Open Source Security Testing Methodology Manual, OWASP-Open Web Application Security Project).

Hardening: sono apposite contromisure di hardening per le macchine componenti la struttura fisica e virtuale dell"infrastruttura ICT del Centro Servizi sono previste come prerequisito di base al rilascio di nuovi sistemi/applicazioni. Le attività di Hardening sono finalizzate all"eliminazione e/o mitigazione di eventuali vulnerabilità insite nelle configurazioni di default proposte dal costruttore e indotte dall"ambiente in cui l"applicazione opera.

.

7 PROGETTO DI MIGRAZIONE DEL SERVIZIO DI POSTA ELETTRONICA PEC

Trattandosi di migrazione di contratto le tempistiche saranno concordate con l'Amministrazione.

7.1 Esigenze dell'Amministrazione

Non vi sono esigenze specifiche dell'amministrazione

7.2 Piano temporale della migrazione del servizio di PEC

La data di migrazione del servizio sarà concordata con il Cliente successivamente all'inserimento dell'ODA sul portale www.acquistinretepa.it.

8 SERVIZIO DI HELP DESK

L'Help Desk è la struttura attraverso la quale vengono erogati alle Amministrazioni contraenti i servizi di assistenza inerenti ai servizi di servizi di Posta Elettronica Certificata (PEC) e di Posta Elettronica (PEL);

L'Help Desk è rivolto agli utenti finali del servizio e al referente Tecnico dell'Amministrazione, per l'inoltro di segnalazioni relative a malfunzionamenti, richieste di modifica e di informazioni.

Il servizio di Help Desk è offerto in modalità multicanale:

- **Telefonicamente**, mediante accesso al Numero Verde **800.849.849**. Il sistema IVR consentirà inoltre mediante il riconoscimento di un:
  - PIN dedicato per ciascuna Amministrazione, seguito da 2 Post Selezioni per la veicolazione delle segnalazioni rispettivamente ai servizi PEC e PEL;
  - PIN dedicato per il Referente Tecnico dell'Amministrazione;

  di identificare il gruppo di gestione di riferimento, dunque, l'operatore il cui skill meglio risponde all'ambito di servizio per cui l'Amm.ne richiede assistenza;
- **Via e-mail**, mediante comunicazione ad un indirizzo di posta elettronica dedicato alla singola Amministrazione ad es. NomeAmministrazione@telecomitalia.it ;
- **Via Fax**, contattando il Numero Verde **800.151.414**;
- **Via web**, mediante la compilazione di una form to mail dal Portale dedicato alla Convenzione (**www.assistenza-PEL-PEC.telecomitalia.it**);

Le richieste di assistenza vengono prese in carico dall'Help Desk nel normale orario di lavoro:

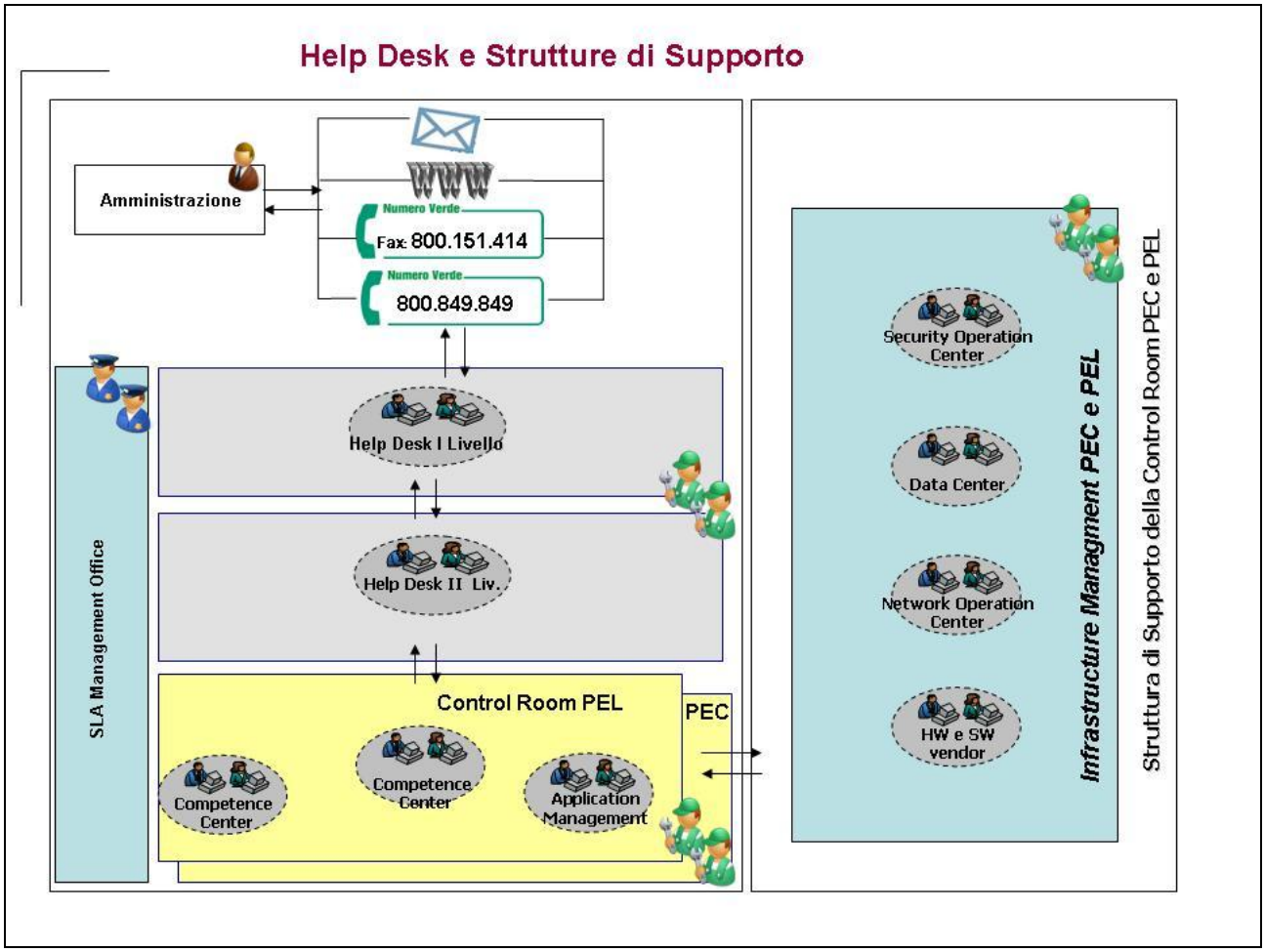
- dal Lunedì, al Venerdì dalle ore 8:00 alle ore 17:00 - escluso festivi;

- il Sabato dalle ore 8:00 alle ore 14:00 escluso festivi;

Tutte le segnalazioni (Mail, Fax e Web) che perverranno all'Help Desk al di fuori dell'orario sopra indicato, saranno prese in carico il giorno lavorativo successivo a quello di inoltro e smaltite secondo l'ordine di Priorità

Si riporta nella figura sottostante, il modello organizzativo dell'Help Desk e delle strutture di Supporto per l'erogazione dei servizi di Posta Elettronica e Posta Elettronica Certificata.

Confidenziale – Tutti i diritti riservati



L'Help Desk è governato da un responsabile che, ne coordina e gestisce le risorse previste, supervisiona attraverso la struttura di SLA Management gli indicatori di qualità del servizio erogato, governa l'andamento delle attività dello stesso e collabora direttamente alla risoluzione di casi di particolare criticità.

L'Help Desk di primo livello è composto da un pool di operatori che rappresenta il Singole Point of Contact (SPOC) verso l'Amministrazione. I principali obiettivi di questo reparto sono quelli di identificare l'Amm.ne, accogliere e tracciare le richieste di assistenza, evaderne quelle di complessità minore e/o maggiormente ricorrenti e di smistare le richieste di assistenza non evadibili dallo stesso verso l'Help Desk di II livello. Questa struttura avendo la supervisione del Trouble Ticket è anche responsabile di aggiornare l'Amm.ne sull'avanzamento della lavorazione dello stesso. Inoltre esegue l'analisi delle statistiche sugli interventi, identificando le esigenze e le azioni atte a prevenire le problematiche ricorrenti.

L'Help Desk di secondo livello è composto da un pool di operatori con competenza e seniority tecnica maggiore rispetto ai colleghi del primo livello. A tale struttura, l'HD di primo livello veicolerà tutte le richieste di assistenza, siano esse malfunzionamenti o richieste di change, la cui risoluzione ed esecuzione richiedono una competenza maggiore.

Questa struttura ha la responsabilità inoltre di interfacciare le Control Room PEC e PEL per le attività che richiedono il coinvolgimento di tali reparti.

A supporto dell'Help Desk operano le strutture di Control Room per i servizi PEC e PEL, queste sono organizzazioni che attraverso i loro centri di competenza altamente specializzati, forniscono supporto all'Help Desk per tutte le attività che richiedono competenza tecnica specifica, siano esse legate al processo di incident, change e/o problem Management.

Le Control Room hanno inoltre la responsabilità della conduzione delle infrastrutture e delle piattaforme attraverso le quali vengono erogati i servizi di PEC e di PEL.

Le **Control Room** interagiscono le strutture che compongono l'Infrastructure Management, avvalendosi degli strumenti e dei processi che le stesse hanno già in uso con questa.

L'**Infrastructure Management** è l'organizzazione deputata alla gestione dell'infrastruttura tecnologica con particolare riferimento alle architetture tecniche (componenti architetturali), alle piattaforme (storage, server, elementi di rete) ed ai servizi infrastrutturali (backup, monitoraggio, asset management, disaster recovery etc.).

In particolare essa è composta dalle seguenti strutture:

- **SOC** (Security Operation Center): è la struttura deputata al monitoraggio della sicurezza del Centro Servizi. In particolare è la funzione che si occupa di tutte le attività volte ad assicurare una corretta gestione delle configurazioni degli apparati (FW, IDS, Antivirus etc.) del Centro Servizi e delle attività di monitoraggio, gestione sistemistica ed applicativa dei diversi moduli della piattaforma di sicurezza tramite, ad esempio, l'esecuzione dei security assessment (Vulnerabilty Assessment e Penetration Test).

- **NOC** (Network Operation Center): è la struttura deputata al monitoraggio, gestione e configurazione dell'infrastruttura di rete (WAN e LAN dei Data Center e delle postazioni di lavoro) del Centro Servizi. Le attività svolte consistono nella supervisione proattiva/reattiva della rete, la ricezione di reclami e/o richieste di supporto relativamente a tematiche di Rete o dei Servizi da essa supportati, diagnosi di primo livello e di secondo livello, correlazione allarmi, intervento da remoto, dispacciamento delle segnalazioni verso altri enti in funzione delle competenze. Monitoraggio/supporto fino alla chiusura dell'anomalia. Il NOC provvede altresì al monitoraggio, gestione e configurazione della componente telefonica dell'Help Desk (Contact Center multicanale);

- **DCS** (Data Center Services): è la struttura deputata all'erogazione dei servizi di facilites (spazi, condizionamento, alimentazione, cablaggio), di prossimità e di gestione sistemistica dei sistemi sopra citati nei quali è calato il Centro Servizi. In particolare assicura la gestione e la logistica degli impianti industriali dedicati all'area produttiva ed anche il corretto espletamento delle attività di delivery dei sistemi e la successiva gestione sistemistica per l'ambito di competenza;

Lo **SLA Management** Office è la struttura deputata al monitoraggio degli SLA relativi ai servizi erogati ed alla produzione della reportistica prevista contrattualmente. E' costituito da un team di Service Manager che hanno il compito di tenere sotto costante controllo i livelli di servizio, attraverso il modulo di SLA Management del sistema di Trouble Management, e di porre in atto, in caso di mancato rispetto degli stessi, tutte le azioni necessarie al tempestivo ripristino dei livelli di servizio contrattualizzati.

La struttura di **Application Management** PEC e PEL al cui interno risiedono le figure specialistiche che si occupano della gestione applicativa delle piattaforma, è integrata all'interno delle rispettive Control Room PEC e PEL e ne rappresenta uno dei Centri di Competenza. Questa collocazione, consente di avere vantaggi di carattere operativo, in quanto, sistemisti, gestori di Data Base e gestori delle applicazioni possono operare in modo congiunto, nelle risoluzioni delle problematiche più complesse, nelle valutazioni di impatto legate ai change, nell'attuazione dei change, nelle analisi legate al Problem Management, ecc.

Le strutture che compongono l'Help Desk e la struttura di Infrastructure Management, gestiscono tutte le richieste di assistenza provenienti dagli utenti e le segnalazioni proattive, mediante l'impiego di Trouble Ticket, secondo lo schema sotto riportato:

Di seguito vengono riportate e descritte le attività di competenze delle strutture che compongono l'Help Desk.

Le attività previste nel perimetro di responsabilità **dell'Help Desk di I livello** sono:

- **Assicurare la comunicazione tempestiva ed efficace con l'utenza;**
- **Ricevere e registrare le segnalazioni degli utenti provvedendo alla comunicazione all'utente dell'identificativo univoco della richiesta di assistenza;**
- **Classificare la richiesta e se possibile fornisce direttamente una soluzione per i problemi più ricorrenti, di non elevata complessità, altrimenti smista la richiesta al secondo livello;**
- **Eseguire il reset delle password delle utenze di accesso alle caselle**
- **Eseguire le richieste di "change" riguardanti modifiche sull'anagrafica degli utenti presenti sulla rubrica, sugli attributi delle caselle e sulle liste di distribuzione;**
- **Controllare i processi di risoluzione attivati e ne verifica gli esiti, informando l'utente sullo stato dell'intervento**
- **Analizzare le statistiche sugli interventi, al fine di identificare i fabbisogni e definire azioni di prevenzione dei problemi;**
- **Documentare i livelli di servizio.**

-

Ciascun operatore dell'help Desk di primo livello è dotato di una postazione di lavoro con accesso al sistema di Trouble Management ed alle basi dati che contengono le informazioni che consentono all'operatore di identificare l'utente segnalatore, aprire, gestire e chiudere i Trouble Ticket relativi alle segnalazioni reattive e proattive per ciascuna Amministrazione aderente al servizio; nonché avere evidenza dello stato di lavorazione della segnalazione, attraverso l'accesso alle work info riportate nel Trouble Ticket.

Inoltre è garantito l'accesso al sistema di messaggistica elettronica, attraverso il quale gli operatori sono in grado di inviare e ricevere le segnalazioni provenienti dalle Amministrazioni e dal Fax server ed al tool di gestione dei servizi PEC e PEL per eseguire le attività di change;

Le attività previste nel perimetro di responsabilità **dell'Help Desk di II livello** sono:

- **Prendere in carico e tracciare le richieste di informazioni e le segnalazioni di guasti e malfunzionamenti non risolti dal primo livello, assegnando una priorità e provvedendo alla loro risoluzione e/o coinvolgere, se necessario, l'assistenza on-site di fornitori terzi ovvero le strutture informatiche dell'Amministrazione;**
- **Provvedere all'esecuzione delle richieste di "change" riguardanti la creazione, cancellazione, blocco delle caselle e delle liste di distribuzione;**
- **Notificare il ripristino delle funzionalità all'help desk di primo livello;**
- **Documentare i livelli di servizio del solo 2° livello.**

L'operatore dell'Help Desk di II ° livello provvederà, per quanto di propria competenza, a ricevere le richieste di assistenza provenienti dall'HD di I° livello e verificare se la richiesta può essere evasa direttamente, oppure

Confidenziale – Tutti i diritti riservati

è necessario provvedere ad inoltrarla verso la Control Room di riferimento rispettivamente per i servizi PEC o PEL.

8.1 Change management

Change management servizio PEL

Il Servizio di Change Management si occupa della pianificazione ed esecuzione delle attività operative relative ai change della configurazione di tutte le componenti infrastrutturali (HW e SW) ed, in particolare, include:

- Pianificazione, coordinamento e implementazione dei change sull'infrastruttura (sistemi, reti,software di gestione della sicurezza, etc.) e sul software di base (sistemi operativi e piattaforme applicative, software di ambiente/middleware) ed individuazione e minimizzazione degli impatti di qualsiasi tipo di change;
- Implementazione di procedure volte ad assicurare che le Amministrazioni ricevano adeguate notifiche su qualsiasi change che avrà o potrebbe avere un potenziale impatto sui servizi;
- Utilizzo di metodi e procedure standard per l'implementazione dei change;
- Utilizzo di processi autorizzativi e di criteri di accettazione delle richieste di change concordati con le Amministrazioni;
- Esecuzione della schedulazione dei rilasci in esercizio dei change secondo le finestre temporali concordate con le Amministrazioni, in modo da minimizzare l'impatto sugli utenti;
- Esecuzione dei change su tutti gli ambienti e gestione della loro distribuzione secondo le modalità concordate coordinandosi eventualmente con fornitori terzi coinvolti;
- Verifica dell'esito delle operazioni di change (Change Review) ed applicazione di eventuali processi di rollback;
- Esecuzione di comparazioni periodiche con i dati disponibili dalle attività di Incident e Problem Management.

Il processo di Change Management utilizzato da Telecom Italia permette di gestire tra differenti tipologia di change:

- **Standard Change**: relativo a richieste rientranti nel contesto del servizio, per questa tipologia di change esiste una definizione ben strutturata e documentata della modifica da effettuare essendo definibili a priori con template che necessitano di un iter approvativo ridotto.
  La richiesta di change viene registrata e classificata dall'operatore che avvia l'analisi della stessa, tale richiesta può avere origine dai processi di Incident Management e/o Problem Management oppure direttamente dagli utenti autorizzati; viene quindi effettuata una valutazione del rischio e dell'impatto legato all'implementazione della richiesta di Change per poter pianificare al meglio le risorse necessarie alle attività richieste.
  L'attività viene pianificata, eseguita e formalizzata nel TT di Change Management, quindi si avvia la verifica che l'esito della attività di Change sia conforme ai requisiti richiesti inizialmente e si procede alla chiusura del TT di Change Management.

- **Non-Standard Change**: relativo a richieste specifiche ma fuori dal normale perimetro progettuale. Tali tipi di change necessitano di un'analisi preliminare volta a definire le attività da svolgere con un piano di lavoro specifico ed un relativo flusso approvativo.
  La richiesta di change viene registrata e classificata dall'operatore che avvia l'analisi della stessa, tale richiesta può avere origine dai processi di Incident Management e/o Problem Management oppure direttamente dagli utenti autorizzati; viene quindi effettuata una valutazione del rischio e dell'impatto legato all'implementazione della richiesta di Change per poter pianificare al meglio le risorse necessarie alle attività richieste.In questa fase viene prodotto il piano di lavoro della change, ne quale sono contenute le informazioni relative, alle risorse coinvolte, ai rischi, alla schedulazione delle attività, al roll back plan, ecc)
  Il responsabile designato per l'attività di Change, verifica che le richieste di Change sottoposte ad approvazione contengano i dati necessari e che le valutazioni di rischio e impatto ed i piani di

recovery siano adeguati, assicura che non vi siano incompatibilità e/o conflitti tra le varie richieste di Change, per evitare che queste possano causare disservizi o problematiche.
La richiesta di Change viene approvata, in tale fase il Change Manager effettua considerazioni sul servizio e valutazioni di tipo tecnico, al fine di approvare o meno l'implementazione della richiesta di Change, gli specialisti eseguono quindi le attività previste, pianificate e formalizzate nel TT di Change Management.
Si avvia infine la verifica che l'esito della attività di Change sia conforme ai requisiti richiesti inizialmente e si procede alla chiusura del TT di Change Management.

- **Emergency Change**: relativo a richieste che risultano essere particolarmente critiche, sia per quanto riguarda l'infrastruttura architetturale che per i servizi. Nascono dalla necessità immediata di risolvere un incidente, ma che per la loro particolare natura di urgenza/emergenza hanno la necessità di essere implementate senza una fase di approvazione formale. La caratteristica che hanno questa tipologia di change è quella di non prevedere un processo autorizzativo che vede coinvolto il Referente Tecnico dell'Amministrazione, bensì, la change opportunamente documentata, viene autorizzata da Emergency Change Advisory Board (ECAB) i cui membri sono rappresentati da un sottoinsieme dei responsabili che compongono le funzioni di Controllo della struttura organizzativa del contratto quadro.
  Nel dettaglio l'ECAB è composto da:
  - Responsabile del Centro Servizi;
  - Responsabile dell'Application Management;
  - Responsabile dell'Infrastructure Management;

Change management servizio PEC

I documenti di seguito evidenziati riportano le procedure per la gestione delle seguenti attività, volte alla gestione delle variazioni hardware e software che interessano il servizio di PEC:

- Software Management: gestione del ciclo di vita del software;
- Versioning: gestione delle release software;
- Patch Management. gestione del patching dei sistemi operativi installati sui server dedicati al servizio, e del patching delle componenti software della piattaforma.

Documenti di riferimento:

- "CAIT2700.IT.QUPR13007 - Procedura di gestione delle Patch e degli Aggiornamenti dei Sistemi.pdf"
- "CAITSWMG.IT.DPIO11000.00 - IstruzioniOperative.pdf".

8.2 Incident management

Di seguito viene descritto il processo che il RTI ha deciso di adottare per gestire gli incidenti di sicurezza informatica e fisica, infrastrutturali e dovuti a malfunzionamenti e fault delle applicazioni e delle infrastrutture, con l'obiettivo di ripristinare la normale operatività del servizio il più velocemente possibile e minimizzare l'impatto negativo sul business e sulle caratteristiche di disponibilità, integrità e confidenzialità delle informazioni, assicurando il mantenimento del miglior livello possibile di qualità e di disponibilità del servizio di Posta Elettronica Tradizionale e Posta Elettronica Certificata in ambito SPC.

Si riportano le definizioni utilizzate nel documento e la tassonomia degli incidenti.

Disservizio/Malfunzionamento**:** ogni evento in cui il normale corso dell'operatività risulti alterata in misura non apprezzabile. In generale, il disservizio può essere caratterizzato dal fatto che la continuità delle operazioni e la qualità dei servizi erogati non vengono compromessi, gli utenti finali potrebbero non percepire le variazioni nella fruizione di servizi e, inoltre, i dati non sono esposti a rischi significativi di perdita di integrità o di riservatezza.

Incidente**:** un qualsiasi evento negativo, di natura casuale, colposa o dolosa, che possa arrecare danni alle persone, al patrimonio (asset materiali e immateriali) e/o pregiudizio alla capacità del RTI di rendere un servizio al livello previsto o di mantenere i livelli di ricavi attesi. E' dunque da intendersi Incidente ogni evento o attività non conforme alle politiche di sicurezza ed alle strategie dell'organizzazione.

Tra gli incidenti si distingue:

• Fatto Anomalo: Incidente che determina un danno di qualsiasi genere sistema ICT, senza per questo violare norme di carattere civile o penale.

• Illecito: Incidente provocato dalla violazione di norme di carattere civile o penale che cagioni un danno al RTI, alla PA o, se si configura un coinvolgimento o una responsabilità di qualsiasi tipo del RTI stesso, anche a terzi.

Incidente gestito: si tratta di un evento che causa un danno e/o richiede un'azione di contenimento e/o reazione da parte delle strutture preposte.

Tentativo di attacco: si tratta di un evento o una serie di eventi di sicurezza, che non causano danni e che non richiedono azioni di contenimento o reazioni, ma che è necessario registrare per una raccolta dei dati a fini statistici e di valutazione. In effetti l'evento è gestito "automaticamente" dalle contromisure tecnologiche messe in atto per diminuire i rischi di intrusione sui sistemi. Non è quindi necessario gestire tale categoria di incidenti in quanto già risolti da detti apparati.

Emergenza: situazione negativa, derivante da uno o più incidenti, che abbia un livello di criticità tale da richiedere l'applicazione di procedure specifiche per essere fronteggiata;

Crisi: evento caratterizzato da bassa probabilità di accadimento ma con gravi conseguenze che minaccia gli obiettivi fondamentali del Gruppo e richiede il ricorso a risorse umane, materiali e procedure organizzative straordinarie.

Gli incidenti relativi alla sicurezza delle informazioni possono essere classificati nelle seguenti tipologie, in funzione del loro carattere prevalente:

- incidenti infrastrutturali,
- incidenti di sicurezza fisica
- incidenti dovuti a malfunzionamenti e fault delle applicazioni e delle infrastrutture informatiche
- incidenti di sicurezza IT

Gestione incidenti servizio PEL

Modalità reattiva

ATTIVITÀ	DESCRIZIONE ATTIVITÀ

ATTIVITÀ	DESCRIZIONE ATTIVITÀ
Incident Registration	L'operatore dell'HD di I livello riceve la segnalazione di Fault attraverso uno dei canali di comunicazione (mail, telefono, web, Fax) e ne provvede ad eseguire il tracciamento, riportando nel Trouble Ticket le seguenti informazioni: • codice univoco di identificazione del ticket; • modalità di accettazione della segnalazione (telefono, fax, e-mail o web); • data e orario di apertura; • caratterizzazione della segnalazione (reattiva); • riferimento dell'Amministrazione che ha aperto la segnalazione ed eventuali altri riferimenti operativi da contattare; • elemento di servizio oggetto del malfunzionamento o dell'attività richiesta o elenco di elementi di servizio in caso di guasto multiplo; • descrizione generale del problema; • Severità;
Incident Management and Analysis	- Attività di analisi del Trouble Ticket; In prima istanza esegue l'analisi del trouble ticket l'operatore che lavora il Troublel Ticket, l'attività viene ripetuta da ciascuna struttura che riceve l'assegnazione dello stesso. L'analisi poggia sulle evidenze fornite dall'utente e sulle work info aggiunte dagli operatori che hanno contribuito alla lavorazione del Trouble Ticket. Ove necessario l'operatore che ha in lavorazione l'incident, può eventualmente procedere con l'esecuzione di ulteriori verifiche anche in collaborazione diretta con l'utente che ha avanzato la segnalazione.
Incident Resolution	Attività di risoluzione dell'anomalia segnalata. Nei casi di fault di complessità minore, la risoluzione dell'Incident viene eseguita direttamente dagli operatori dell'Help Desk di I e II livello, sono tipicamente incident gestibili mediante le funzioni disponibili dalle console di gestione PEL e PEC . Per gli Incident di complessità maggiore e/o che riguardano problemi infrastrutturali (hw e sw) intervengono gli specialisti delle CR PEL e PEC, invece, laddove il fault fosse di natura network (switch, bilanciatori, router, ecc) rimuoveranno l'anomalia gli operatori del NOC, così come in caso di fault legati al perimetro di security interverranno gli specialisti del SOC. Infine, laddove l'incident riguardasse ambiti gestiti dal Data Center, interverranno gli specialisti che operano in tale struttura. Nei casi più complessi quest'attività può attivare il processo di Problem Management specifico di ogni reparto.
Incident Assignment	Procedura mediante la quale una richiesta di Incident viene assegnata ad un particolare gruppo di competenza (albero di dispatching).
Incident Tracking	Ciascun operatore/specialista coinvolto nella lavorazione del Trouble Ticket provvede ad aggiornare le note di lavorazione dello stesso (ad es. inserendo in esse le verifiche interne eseguite ed i relativi esiti, le riconfigurazioni apportate, ecc.).

Confidenziale – Tutti i diritti riservati

ATTIVITÀ	DESCRIZIONE ATTIVITÀ
IT Security Incident	Documento di riferimento per la gestione degli incidenti di Sicurezza Informatica. L'operatore di Control Room nel caso riceva una segnalazione relativa ad un evento di Sicurezza, agisce in coerenza con quanto indicato nella procedura.

Modalità proattiva

ATTIVITÀ	DESCRIZIONE ATTIVITÀ
Incident Registration	Lo specialista della Control Room, riceve dalla struttura di Infrastructure Management o rileva dalla console di Event Management la segnalazione di Incident. A fronte di tale condizione lo specialista della Control Room provvede ad eseguire il tracciamento della segnalazione, riportando nel Trouble Ticket le seguenti informazioni: • codice univoco di identificazione del ticket; • modalità di accettazione della segnalazione (telefono, fax, e-mail o web); • data e orario di apertura; • caratterizzazione della segnalazione (proattiva); • riferimento dell'Amministrazione coinvolta nella segnalazione ed eventuali altri riferimenti operativi da contattare; • elemento di servizio oggetto del malfunzionamento o dell'attività richiesta o elenco di elementi di servizio in caso di guasto multiplo; • descrizione generale del problema; • Severità; Nell'orario di presidio dell'Help Desk, se il fault ha priorità ALTA la segnalazione viene inviata all'HD per la notifica all'Amministrazione.
Incident Management and Analysis	Attività di analisi del Trouble Ticket; In prima istanza esegue tale analisi lo specialista che lavora il Troublel Ticket, l'attività viene ripetuta da ciascuna struttura che riceve l'assegnazione di un Trouble Ticket. L'analisi poggia sulle evidenze fornite dall'utente e sulle work info aggiunte dagli operatori che hanno contribuito alla lavorazione del Trouble Ticket. Ove necessario l'operatore che ha in lavorazione l'incident, può eventualmente procedere con l'esecuzione di ulteriori verifiche anche in collaborazione diretta con l'utente che ha avanzato la segnalazione.

Confidenziale – Tutti i diritti riservati

ATTIVITÀ	DESCRIZIONE ATTIVITÀ
Incident Resolution	Attività di risoluzione dell'anomalia segnalata o rilevata. Per gli Incident che riguardano problemi infrastrutturali (hw e sw) intervengono gli specialisti delle CR PEL e PEC, invece, laddove il fault fosse di natura network (switch, bilanciatori, router, ecc) rimuoveranno l'anomalia gli operatori del NOC, così come in caso di fault legati al perimetro di security interverranno gli specialisti del SOC. Infine, laddove l'incident riguardasse ambiti gestiti dal Data Center, interverranno gli specialisti che operano in tale struttura. Nei casi più complessi quest'attività può attivare il processo di Problem Management specifico di ogni reparto. Lo specialista della Control Room che ha in carico il Trouble Ticket è responsabile della risoluzione dell'Incident ed è colui che eventualmente applica il processo di Escalation.
Incident Assignment	Procedura mediante la quale una richiesta di Incident viene assegnata ad un particolare gruppo di competenza (albero di dispatching).
Incident Tracking	Ciascun operatore/specialista coinvolto nella lavorazione del Trouble Ticket provvede ad aggiornare le note di lavorazione dello stesso (ad es. inserendo in esse le verifiche interne eseguite ed i relativi esiti, le riconfigurazioni apportate, ecc.).
IT Security Incident	Documento di riferimento per la gestione degli incidenti di Sicurezza Informatica. L'operatore di Control Room nel caso riceva una segnalazione relativa ad un evento di Sicurezza, agisce in coerenza con quanto indicato nella procedura.
Incident Escalation Procedure	Procedura di riferimento per la gestione dell'Escalation, essa coincide con la one minute escalation che ha l'obiettivo di attivare l'escalation all'interna alle struttura che l'attiva ed al contempo attivare il Comitato di Coordinamento previsto nell'ambito della Procedura di Continuità operativa. La procedura viene attivata dall'operatore che ha in carico la gestione dell'incident (responsabile dell'incident).
Incident Closure	Lo specialista prima di chiudere l'Incident, verifica o richiede verifica che la segnalazione di allarme presente sulla console di Event Management non sia più presente; Procede alla chiusura del Trouble Ticket; In orario di presidio dell'Help Desk, notifica allo stesso la chiusura dell'Incident, per la verifica congiunta con l'Amministrazione.

Gestione incidenti servizio PEC proattivo e reattivo

Il processo di gestione applicato per gli incidenti Infrastrutturali ed applicativi è lo stesso che Telecom Italia Trust Technologies usa nell'ambito dei propri processi e descritto nella Procedura Gestione Incidenti.

Documento di riferimento:

- "CAIT2700.IT.QUPR13000.00 - Gestione degli Incidenti di Sicurezza.pdf"

8.3 Tool di amministrazione

La soluzione di posta prevista per la convenzione è dotata di strumenti amministrativi integrati, fruibili tramite interfacce web di semplice utilizzo con accesso tramite credenziali di tipo username/password, da cui è possibile svolgere attività di governance del sistema di posta elettronica. Tali strumenti saranno customizzati in termini di profilazione degli utenti per i quali sarà richiesto l'accesso e in termini di componenti di cui si richiederà la disponibilità. Gli strumenti di amministrazione afferiscono a 3 aree di attività per ciascuna delle quali si riporta un esempio esplicativo ma non esaustivo di quanto può essere fornito:

1. gestione delle risorse (self-provisioning): ad es. gestione delle mailbox (creazione, modifica, eliminazione, disabilitazione della casella), gestione delle informazioni di login e password (creazione, reset della password), gestione delle DL centralizzate, gestione delle public folder, applicazione delle policy di archiviazione, etc.

2. visualizzazione dei dati di rendicontazione dell'utilizzo del servizio: ad es. statistiche di traffico (n° di messaggi inviati/ricevuti, …), risorse allocate (n° caselle attive, occupazione caselle, n° di contatti…), report sull'attività dell'antivirus/antispam, etc

3. visualizzazione dei dati aggregati originati dagli strumenti di monitoraggio:
    - dati relativi alla disponibilità delle componenti di servizio originati dal sistema di monitoraggio integrato nella piattaforma,
    - dati relativi alla disponibilità delle componenti di servizio originati dalle sonde di user experience.

Gli strumenti di gestione delle risorse (1) sono utilizzati dall'Help Desk di TI per le attività di governance del servizio e possono essere forniti (anche con profilazione diversa, ad es. in sola lettura o per utilizzo di funzionalità specifiche) anche all'Amministrazione.

Con riferimento specifico alla console di monitoraggio (3) i dati sono presentati in due sezioni:

- La sezione "Sistema" che visualizza gli indicatori raccolti dagli strumenti di monitoraggio delle componenti server.
- La sezione "Esperienza utente" che visualizza gli indicatori raccolti dagli strumenti di monitoraggio lato Amministrazione (sonde di user experience) per ogni sonda attivata. Oltre al dato di disponibilità in tempo reale è a disposizione il grafico che indica i tempi di risposta (nelle ultime 24 ore).

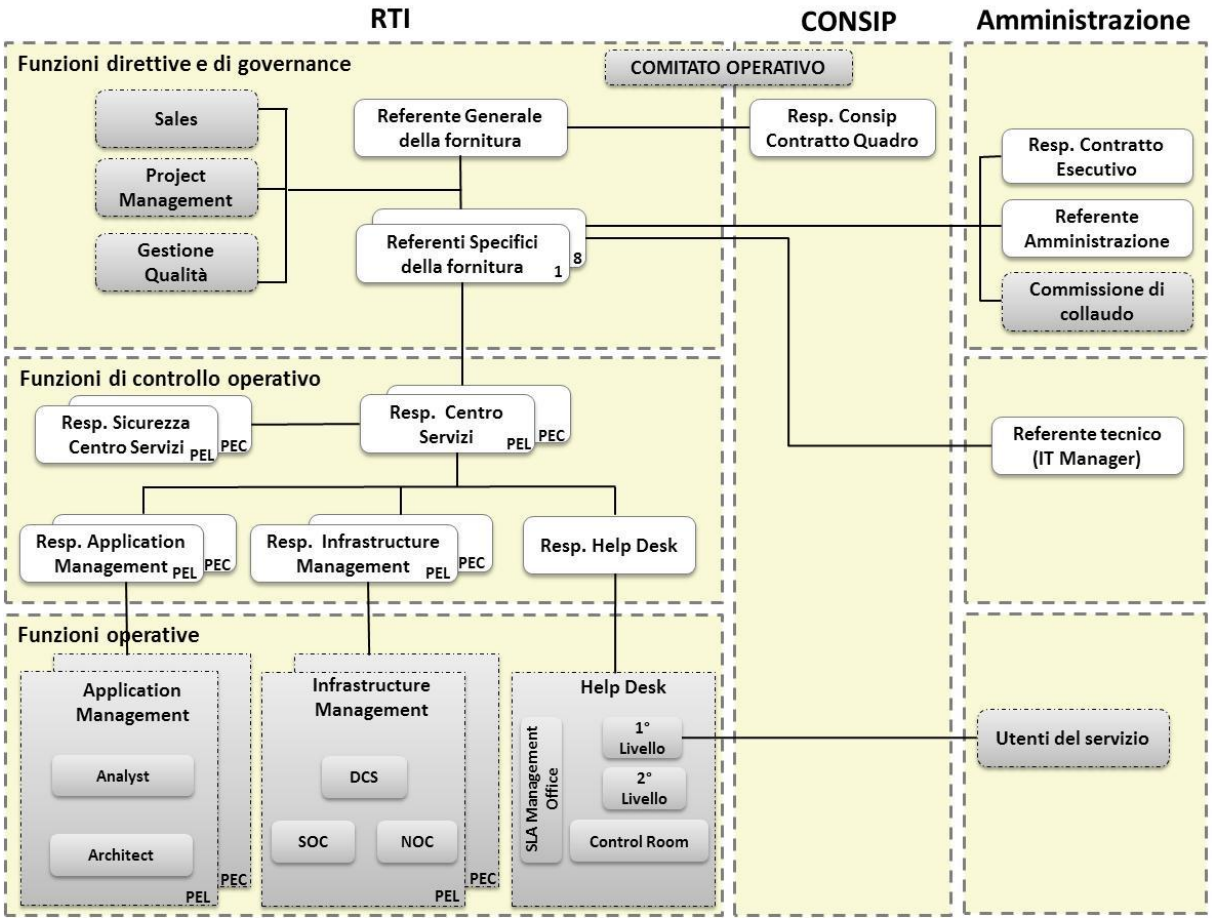
Confidenziale – Tutti i diritti riservati

9 GESTIONE DELLA FORNITURA

Nell'ambito della struttura organizzativa per la gestione della fornitura, Telecom Italia mette a disposizione, oltre ad un "Responsabile del Centro Servizi", un "Responsabile della sicurezza dei servizi erogati dal Centro Servizi", un "Referente Generale della fornitura", anche dei "Referenti specifici della fornitura" per tutta la durata del Contratto Quadro.

Inoltre a ciascuna Amministrazione Contraente verrà comunicato il Referente assegnato a seguito della ricezione del Contratto di Fornitura.

Come evidenziato nella figura seguente, la struttura organizzativa proposta si articola su tre livelli gerarchici, in conformità a tre tipologie di funzioni.



Funzioni Direttive e di Governance

Si tratta di funzioni di indirizzo e di controllo nell'ambito del Contratto Quadro. Nel caso specifico, per l'Amm.ne la figura del Referente Specifico sarà responsabile di tutte le attività e le problematiche relative alle fasi di consegna, realizzazione, collaudo e di assistenza per i servizi previsti nel Contratto di Fornitura e risponde direttamente al Referente Generale della fornitura. Tale figura si occuperà di redigere, nei termini e nei contenuti previsti, i "rapporti di progetto" e a conclusione delle attività un "Rapporto Conclusivo" contenente le date di inizio e fine attività. Hanno il compito di implementare tutte le azioni necessarie a garantire il rispetto delle prestazioni richieste e di gestire gli eventuali reclami o segnalazioni da parte dell'Amministrazione Contraente nel rispetto degli SLA contrattualizzati.

Per alcune tipologie di segnalazioni, aventi carattere di particolare urgenza (calamità naturali, disservizi gravi dovuti a malfunzionamenti di rete o mancata erogazione di energia elettrica, richieste della Magistratura/Autorità Giudiziaria), i Referenti possono avvalersi di un ulteriore supporto rappresentato da una figura in reperibilità H 24 7x7.

Confidenziale – Tutti i diritti riservati

Funzioni di Controllo Operativo

Si tratta di funzioni operative direttamente coinvolte nella gestione del Contratto Quadro. Tali funzioni sono ricoperte in primo luogo da:

- Responsabili dei Centri Servizi di PEC e PEL: garantiscono il coordinamento di tutte le attività necessarie all'erogazione dei servizi previsti nel Contratto Quadro. Ciascuno gestisce, per i servizi di propria competenza, i rapporti di natura tecnica con le Amministrazioni Contraenti. Entrambi partecipano al Comitato Operativo di gestione dei servizi assieme al Referente Generale della fornitura.
- Responsabili della Sicurezza dei Centri Servizi di PEC e PEL: garantiscono, ciascuno per i servizi di propria competenza, la governance delle attività inerenti la sicurezza fisica, logica e organizzativa del Centro Servizi stabilendo adeguate politiche di sicurezza nel rispetto delle normative previste dallo standard ISO27001. Rispondono direttamente al Responsabile del rispettivo Centro Servizi.
- Responsabili Application Management di PEC e PEL: sono i responsabili delle attività di delivery, esercizio, manutenzione per la corretta erogazione dei servizi di propria competenza (PEC o PEL) previsti nel Contratto Quadro. Rispondono direttamente al Responsabile del rispettivo Centro Servizi.
- Responsabili Infrastructure Management di PEC e PEL: sono i responsabili della gestione ed esercizio dell'area infrastrutturale dei rispettivi Centri Servizi (sicurezza, rete, sistemi) utilizzata per l'erogazione dei servizi PEC e PEL previsti nel Contratto Quadro. Rispondono direttamente al Responsabile del rispettivo Centro Servizi.
- Responsabile Help Desk: è il responsabile delle attività dell'help desk di 1 e 2 livello. Risponde direttamente ad entrambi i Responsabili dei Centri Servizi.
- Referente Tecnico dell'Amministrazione (IT Manager): è il responsabile tecnico, per l'Amministrazione Contraente, dei servizi sottoscritti nell' ambito del Contratto di Fornitura. Si interfaccia con il Referente Specifico dell'Amministrazione;

Funzioni operative

In questa area rientrano tutte le funzioni inerenti alla gestione operativa dei servizi. Tali funzioni si interfacciano con tutte le strutture della funzione di Controllo Operativo e rappresentano il punto di contatto con gli Utenti del Servizio e Referenti tecnici dell'Amministrazione. La struttura centrale di questa funzione è rappresentata dall'Help Desk di 1° e di 2° livello.

- Help Desk: è la struttura deputata alla gestione dei servizi di:
    - Help Desk 1° livello: è la struttura di accoglienza e risoluzione delle segnalazioni delle Amministrazioni;
    - Help Desk 2° livello: è la struttura di accoglienza e risoluzione delle segnalazioni delle Amministrazioni o delle problematiche complesse dispacciate dall'Help Desk di 1° livello.
    - Control Room: è costituita da un team di specialisti focalizzato su tutte quelle attività di analisi sistemistica delle risorse IT (sistemi operativi, database e middleware), per le quali è richiesta elevata specializzazione sulla tecnologia e/o servizio. In particolare al personale della Control Room sono affidate attività di capacity planning, attività di valutazione di impatto (impact analysis) che precedono il change management, la software distribution e la manutenzione evolutiva (ad es. inserimento di patch di aggiornamento software, ecc.) e che possono richiedere attività di test in ambiente di pre-produzione, per la verifica preventiva dei potenziali impatti sul servizio;
    - SLA Management Office: è la struttura deputata al monitoraggio dei SLA sui servizi erogati ed alla produzione della reportistica prevista contrattualmente. E' costituito da un team di Service Manager che hanno il compito di tenere sotto costante controllo i livelli di servizio, attraverso il modulo di SLA Management del sistema di Trouble Management, e di porre in atto, in caso di mancato rispetto degli stessi, tutte le azioni necessarie al tempestivo ripristino

dei livelli di servizio contrattualizzati.

Per la conduzione tecnica e amministrativa dei contratti di fornitura, la struttura di Help Desk interagisce inoltre con le strutture di Infrastructure Management e di Application Management.

10 SLA CONTRATTUALIZZATI

Per il dettaglio dei Livelli di Servizio contrattualizzati, le modalità di rendicontazione e le eventuali penali si rimanda al Piano della Qualità Generale redatto dal RTI ed approvato da Consip in fase di stipula dell'Accordo Quadro.

10.1 Servizio di PEL

CFR. "PIANO DI QUALITÀ - FORNITURA DEI SERVIZI DI POSTA ELETTRONICA E POSTA ELETTRONICA CERTIFICATA (SERVIZI DI MESSAGGISTICA) NELL'AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE (SPC)PIANO DELLA QUALITà GENERALE – **PAR. 7.1.1** "

10.2 Servizio di PEC

CFR. "PIANO DI QUALITÀ - FORNITURA DEI SERVIZI DI POSTA ELETTRONICA E POSTA ELETTRONICA CERTIFICATA (SERVIZI DI MESSAGGISTICA) NELL'AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE (SPC)PIANO DELLA QUALITà GENERALE - **PAR. 7.1.2** "

10.3 Servizio di Help Desk

CFR. "PIANO DI QUALITÀ - FORNITURA DEI SERVIZI DI POSTA ELETTRONICA E POSTA ELETTRONICA CERTIFICATA (SERVIZI DI MESSAGGISTICA) NELL'AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE (SPC)PIANO DELLA QUALITà GENERALE **PAR. 7.1.4** "

10.4 Rendicontazione dei livelli di servizio

CFR. "PIANO DI QUALITÀ - FORNITURA DEI SERVIZI DI POSTA ELETTRONICA E POSTA ELETTRONICA CERTIFICATA (SERVIZI DI MESSAGGISTICA) NELL'AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE (SPC)PIANO DELLA QUALITà GENERALE **PAR. 7.1.4** "

Confidenziale – Tutti i diritti riservati

11 CORRISPETTIVI ECONOMICI DEI SERVIZI OFFERTI

Di seguito, sulla base del listino di Contratto Quadro, si riportano i corrispettivi economici dei servizi richiesti dall'Amm.ne sulla base delle consistenze identificate nel Piano dei Fabbisogni

Sono riportate le tabelle dei corrispettivi economici per:

- le consistenze massimali oggetto del Contratto di Fornitura (ODA)
- le consistenze relative alle quantità da attivare e che saranno oggetto di fatturazione

I valori espressi sono al netto dell'IVA.

Il Contratto Quadro prevede che, in caso di migrazione, le caselle PEL o PEC debbano essere attivate in un arco temporale massimo che non deve essere superiore a 4 mesi.

In tal caso, è possibile che le attivazioni non vengano effettuate tutte nello stesso momento, ma vengano effettuate in modalità differita prevedendo "n" lotti di attivazioni, definiti dalla progettazione sia in base alle esigenze dell'Amm.ne, sia in base alla programmazione delle risorse/gestione di piattaforma.

Per lotto di attivazione si intende quindi una trance di caselle PEC o PEL che vengono attivate in una certa data con relativo espletamento tecnico.

A titolo di esempio, l'Amm.ne richiede di attivare e migrare 5.000 caselle PEL BASE nell'arco dei 4 mesi.

Nel progetto esecutivo verranno definiti 3 lotti:

1) 1000 caselle con data di attivazione 15 marzo 2014
2) 1500 caselle con data di attivazione 10 aprile 2014
3) 2500 caselle con data di attivazione 15 giugno 2014. Quest'ultima data rappresenta anche la fine della migrazione e costituirà la data di espletamento commerciale.

Le singole trance di caselle attivate dovranno essere correttamente fatturate seguendo le regole di valorizzazione indicate nella Guida al Contratto a cui si fa rinvio.

Cio' significa che **per il primo lotto:**

1) le caselle matureranno ratei di canone dal 15 marzo al 31 marzo (16 gg)
2) matureranno 2 mesi di canone completi (aprile e maggio)
3) matureranno ratei di canone dal 1° al 15 giugno 2014 (15 gg)

La valorizzazione del primo lotto sarà quindi la seguente:

- **per i ratei di canone**, pari a 26 gg (16 di marzo + 15 di giugno) occorre dividere il prezzo mensile della casella base (0,60 euro) per il numero di giorni del mese, moltiplicando per i gg di ratei e poi per il numero di caselle.

  Marzo: (0,60/31*16)*1000 = 309,67 euro

  Giugno: (0,60/30*15)*1000 = 300 euro

Confidenziale – Tutti i diritti riservati

- **Per i mesi complessivi** (aprile e maggio): (0,60*2)* 1000 = **12000 euro**

TOTALE PRIMO LOTTO: 12609,67

Per il **secondo lotto**:

- Per i ratei:

  Aprile: 20 gg di rateo - (0,60/30*20)*1500 = 600 euro

  Giugno: (0,60/30*15)*1000 = 4500 euro

- 1 mese complessivo (maggio): 0,60*1500 = 900 euro

TOTALE SECONDO LOTTO: 6.000 EURO

Per il **terzo e ultimo lotto**:

Giugno: (0,60/30*15)*2500 = 750 euro

TOTALE TERZO LOTTO: 750 EURO

La fattura relativa ai 4 mesi di migrazione avrà quindi un valore complessivo di 19359,67 (12609,67 + 6000 + 750).

11.1 Servizio di Posta Elettronica Certificata (PEC)

Id.	Servizi Posta Elettronica Certificata	Quantità massima del Contratto di Fornitura (ODA)	Quantità da attivare (mailbo nella disponibilità del Cliente che saranno oggetto di fatturazione)	Canone mese unitario	Canone Annuo TOTALE (Euro)
2	Casella PEC Strutturata	200	100	3	€ 3.600

12 VALORI DELL'ODA

Servizio	Quantità	Totale Contrattuale
Casella di Posta Elettronica Certificata di tipo base		€ 0,00
Casella di Posta Elettronica Certificata di tipo strutturata	200	€ 19.158,48
Casella di Posta Elettronica Certificata di tipo massiva-small		€ 0,00
Casella di Posta Elettronica Certificata di tipo massiva-medium		€ 0,00
Casella di Posta Elettronica Certificata di tipo massiva-large		€ 0,00
Sistemista		€ 0,00
Sistemista senior		€ 0,00
Architetto		€ 0,00
VALORE CONTRATTUALE (IVA ESCLUSA)		€ 19.158,48
Data Ordine	04/01/2015	

Il valore contrattuale dell'ordine deve essere inserito nel modulo di Ordine Diretto d'Acquisto ed è necessario per il calcolo dovuto a Consip. La giusta compilazione del campo "Data Ordine" consente la valorizzazione corretta del valore complessivo dell'ODA

Confidenziale – Tutti i diritti riservati

13 REFERENTE SPECIFICO DELLA FORNITURA

Il **Referente specifico della fornitura** per questo progetto è:

Referente specifico fornitura	
Nome	Giovanni
Cognome	Izzo
Email	giovanni.izzo@telecomitalia.it
Telefono	070 5252786 335 7510139

Tra le funzioni del referente specifico della fornitura rientrano le seguenti attività:

- rispondono direttamente al Referente Generale della fornitura;
- redigono i “rapporti di progetto” e il “Rapporto Conclusivo” della fornitura;
- implementano tutte le azioni per il rispetto delle prestazioni richieste;
- gestiscono i reclami o segnalazioni da parte della PA contraente (rispetto degli SLA).

14 TABELLE RIEPILOGO SERVIZI

Servizio PEC					
Elementi di Servizio Base	Attivazione	NO			
	Migrazione Caselle	SI			
	Migrazione Contenuti	SI			
	Richieste Caselle Base	NO	Quantità		
	Richieste Caselle Strutturate	SI	Quantità	200 (massima)	
	Richieste Caselle Massive SMALL	NO	Quantità		
	Richieste Caselle Massive MEDIUM	NO	Quantità		
	Richieste Caselle Massive LARGE	NO	Quantità		
			Totale Caselle	*n. totale caselle*	
	Rete di Erogazione	Internet	Banda	52 Mbps in corso attivazione (attuale8M)	
	Domini SMTP	asloristano.pec.it			
Migrazione	Variazione di contratto (Amm.ne già cliente TITT)	SI			
	Migrazione da altro gestore	NO			
	Spazio totale occupato sulla posta attuale	MB/GB/TB			
Personalizzazioni	Richieste	NO	Elenco		
			* personalizzazione 1; * personalizzazione 2; … * personalizzazione n;		

Tabella 3 - Riepilogo Servizi PEC.