

**APPENDICE 7 AL CAPITOLATO TECNICO**

**PROGETTO DEI FABBISOGNI INAIL-MINISTERO DELLA SALUTE**

**GARA PER L’AFFIDAMENTO DEI SERVIZI DI SUPPORTO, GESTIONE E  
SVILUPPO DEL SISTEMA INFORMATIVO SANITARIO NAZIONALE PER  
IL MINISTERO DELLA SALUTE – ID 1974**



## INDICE DEL DOCUMENTO

<b>1</b>	<b>OBIETTIVI DEL DOCUMENTO .....</b>	<b>4</b>
<b>2</b>	<b>CONTESTO DI RIFERIMENTO .....</b>	<b>5</b>
2.1	COMPRESIONE DELL'ESIGENZA / SERVIZI DA EROGARE .....	5
2.2	DESCRIZIONE DEL SERVIZIO .....	6
2.3	ORARIO DEI SERVIZI .....	6
2.4	MODELLO DI FUNZIONAMENTO DEL SERVIZIO .....	7
2.4.1	<i>Ruoli e responsabilità .....</i>	<i>7</i>
<b>3</b>	<b>GESTIONE OPERATIVA E HOSTING.....</b>	<b>11</b>
3.1	<b>GESTIONE OPERATIVA .....</b>	<b>11</b>
3.1.1	<i>Interruzione servizi agli utenti .....</i>	<i>11</i>
3.1.2	<i>Accesso per ispezioni del Ministero della Salute .....</i>	<i>11</i>
3.1.3	<i>Assistenza e supervisione terze parti.....</i>	<i>11</i>
3.1.4	<i>Gestione dei fabbisogni di evoluzione infrastrutturale e del change management.....</i>	<i>12</i>
3.1.5	<i>Gestione cataloghi .....</i>	<i>12</i>
3.1.6	<i>Asset Management .....</i>	<i>12</i>
3.1.7	<i>Classificazione sistemi e orari di riferimento.....</i>	<i>12</i>
3.1.8	<i>Misurazione della baseline di sistema .....</i>	<i>13</i>
3.1.9	<i>Manutenzione Licenze.....</i>	<i>13</i>
3.2	<b>HOSTING .....</b>	<b>13</b>
3.2.1	<i>Gestione dei sistemi .....</i>	<i>14</i>
3.2.2	<i>Installazione .....</i>	<i>14</i>
3.2.3	<i>Conduzione dell'infrastruttura .....</i>	<i>14</i>
3.2.4	<i>Assistenza Sistemistica .....</i>	<i>15</i>
3.2.5	<i>Gestione configurazioni hardware, software di base e applicativo e relativi ambienti ....</i>	<i>15</i>
3.2.6	<i>Manutenzione HW .....</i>	<i>15</i>
3.2.7	<i>Reti (Data Center).....</i>	<i>16</i>
3.2.8	<i>Connettività .....</i>	<i>18</i>
3.2.9	<i>Reti (uffici periferici) .....</i>	<i>18</i>
3.2.10	<i>Gestione dello spazio su disco (Storage Management) .....</i>	<i>18</i>
3.2.11	<i>Amministrazione database .....</i>	<i>20</i>
3.2.12	<i>Gestione Software .....</i>	<i>20</i>
3.2.13	<i>Backup.....</i>	<i>21</i>



3.2.14 Restore .....	22
3.2.15 Gestione delle elaborazioni .....	22
3.2.16 Servizi di Dominio .....	23
3.2.17 Transizione IPv4/IPv6 .....	23
3.2.18 Deploy applicativi .....	23
3.2.19 Sicurezza delle Informazioni .....	24
3.2.20 Governance di Sicurezza .....	25
3.2.21 Security Operation Center .....	25
3.2.22 Audit Di Sicurezza .....	26
<b>3.3 HOUSING .....</b>	<b>26</b>
<b>3.4 SERVIZIO DI MONITORAGGIO .....</b>	<b>27</b>
3.4.1 Service Control Room .....	28
3.4.2 Modalità di predisposizione monitoraggio .....	29
<b>4 MODELLO OPERATIVO DEL SERVIZIO .....</b>	<b>31</b>
4.1 MODALITÀ DI ATTIVAZIONE/TERMINAZIONE DEL SERVIZIO .....	31
4.2 PROCESSO DI GESTIONE RICHIESTE DI SERVIZIO .....	31
4.3 PROCESSO DI GESTIONE DEGLI INCIDENTI .....	32
4.4 PROCESSO DI GESTIONE DEI PROBLEMI .....	33
4.5 PROCESSO DI GESTIONE DEI RILASCI .....	34
<b>5 REPORTISTICA SULL'ANDAMENTO DEL SERVIZIO .....</b>	<b>36</b>
5.1 REPORTISTICA PERIODICA DI ESERCIZIO .....	36



## **1 OBIETTIVI DEL DOCUMENTO**

L'obiettivo del presente documento è descrivere il modello operativo del servizio di Hosting Evoluto che INAIL, e più nello specifico la Direzione Centrale Organizzazione Digitale dell'INAIL, di seguito DCOD INAIL, mettono a disposizione della PA Aderente, il Ministero della Salute, di seguito MdS.

Il Progetto dei fabbisogni, sulla base delle caratteristiche esigenze descritte all'interno del Piano dei fabbisogni, specifica le regole, gli standard e le procedure generali del servizio.

Contiene i volumi, i valori, le tipologie, i nominativi dei referenti della DCOD INAIL e tutti gli elementi specifici collegati al servizio di Hosting Evoluto oggetto dell'Accordo di Collaborazione tra INAIL e MdS di cui il presente documento costituisce un allegato.

E' intendimento della DCOD INAIL e del MdS impegnarsi, nel corso del periodo di collaborazione, nella ricerca di soluzioni tendenti all'ottimizzazione delle soluzioni tecniche e organizzative finalizzate al miglioramento continuo dell'efficacia e dell'efficienza dell'accordo stesso.



## 2 CONTESTO DI RIFERIMENTO

### 2.1 Comprensione dell'esigenza / Servizi da erogare

Dall'analisi dei documenti ricevuti, e principalmente dal Piano dei fabbisogni basato sull'attuale erogazione in outsourcing dei servizi IT di Gestione operativa e Hosting, è emerso che l'esigenza manifestata dal Ministero della Salute comprende i servizi rappresentati nella seguente tabella:

Servizio	Attività
Gestione Operativa	Asset management
	Monitoraggio e Gestione Problemi
	Amministrazione database
	Gestione software
	Backup
	Restore
	Gestione elaborazioni
	Disaster Recovery
	System & Application Monitoring and Management
	Assistenza sistemistica
	Capacity management e tuning di sistema
	Gestione configurazioni hardware, software di base e applicativo e relativi ambienti
	Gestione dello spazio su disco (Storage Management)
	Gestione dei rilasci applicativi
	Gestione della sicurezza logica e fisica
	Test di vulnerabilità
	Servizi di Dominio
	Transizione IPv4/IPv6
Hosting	Messa a disposizione infrastruttura tecnologica
	Conduzione operativa
	Manutenzione hardware e software
	Gestione reti di telecomunicazioni
	Housing
Evoluzioni Architettura tecnico applicativa	Realizzazione e installazione
	Test e collaudo
	Avviamento

Figura 1 - Servizi in outsourcing erogati per MdS



## 2.2 Descrizione del servizio

Il servizio di Gestione Operativa e Hosting prevede le attività di: conduzione, messa a disposizione e gestione delle infrastrutture fisiche e virtuali per l'erogazione dei servizi descritti nel presente Progetto dei fabbisogni per il Ministero della Salute, di seguito MdS. Il servizio si applica anche agli apparati di proprietà del MdS.

Le sedi di erogazione sono quelle in cui sono ubicati i Data Center della DCOD INAIL.

Il servizio comprende la manutenzione e gestione degli ambienti di collaudo, pre-produzione e di produzione dei sistemi in esercizio, la supervisione e monitoraggio dell'infrastruttura tecnologica del Data Center e di tutte le future evoluzioni nel corso di durata del contratto.

È incluso nel servizio il supporto al MdS nel coordinamento complessivo delle attività di tutti i fornitori e terze parti del MdS coinvolti nella gestione dei sistemi.

## 2.3 Orario dei servizi

Nella tabella seguente si riportano gli orari di servizio per ogni sottoservizio di gestione operativa:

Servizio	Sottoservizio	Orari servizio
Gestione operativa	Asset Management	Lun-Ven 8.00 – 20.00
	Monitoraggio e Gestione Problemi	Lun-Ven 8.00 – 20.00, Sab 8.00-13.00
	Amministrazione Database	Lun-Ven 8.00 – 20.00, Sab 8.00-13.00
	Gestione software	Lun-Ven 8.00 – 20.00, Sab 8.00-13.00
	Backup	Lun-Ven 8.00 – 20.00, Sab 8.00-13.00
	Restore	Lun-Ven 8.00 – 20.00, Sab 8.00-13.00
	Gestione elaborazioni	Lun-Ven 8.00 – 20.00
	Disaster Recovery	Durante i test (Lun-Ven 8.00 – 20.00, Sab 8.00-13.00) H24- 7 su 7 in caso di disastro
	System & Application Monitoring and Management	Lun-Ven 8.00 – 20.00, Sab 8.00-13.00
Hosting	Messa a disposizione infrastruttura tecnologica	H24 x 365 g/anno
	Manutenzione hardware e software	Lun-Ven 8.00 – 20.00, Sab 8.00-13.00
	Conduzione operativa	H24 x 365 g/anno
	Gestione reti di telecomunicazione	H24 x 365 g/anno
	Housing	H24 x 365 g/anno
Evoluzioni Architettura tecnico applicativa	Realizzazione e installazione Test e collaudo e Avviamento	Lun-Ven 8.00 – 20.00

Figura 2 - Orario dei Servizi



Per tutti i servizi che non sono H24 sarà garantita la reperibilità al di fuori dell'orario di servizio (domeniche e giorni festivi inclusi) entro 4 ore dalla chiamata.

Allo scopo saranno comunicati al Service Manager MdS i canali (telefono o altro) mediante i quali effettuare la richiesta di intervento.

## 2.4 Modello di funzionamento del servizio

Il modello di funzionamento proposto a supporto dell'erogazione del servizio di hosting evoluto rappresenta una "specializzazione" sul contesto Ministero della Salute del modello di funzionamento che la DCOD INAIL ha definito per supportare l'erogazione di servizi ad altre PA in logica PSN. Il modello è coerente con le *Best Practice* ITIL e tende a creare un chiaro, condiviso ed efficiente contesto di interazione fra la DCOD INAIL ed il Ministero della Salute. Il Modello di funzionamento proposto per gestire le interazioni chiave con il Ministero della Salute prevede tre fasi:

- Governo della relazione fra Ministero della Salute e DCOD INAIL;
- Progettazione e Avvio del servizio di Hosting Evoluto;
- Esercizio (gestione operativa, *day-by-day*) del servizio di Hosting evoluto.

In particolare, relativamente al contesto Ministero della Salute ed alle fasi prima riportate si rimanda al capitolo 4 "Modello Operativo del Servizio" per la descrizione dei processi e procedure relativi alla fase di Esercizio del servizio di Hosting Evoluto.

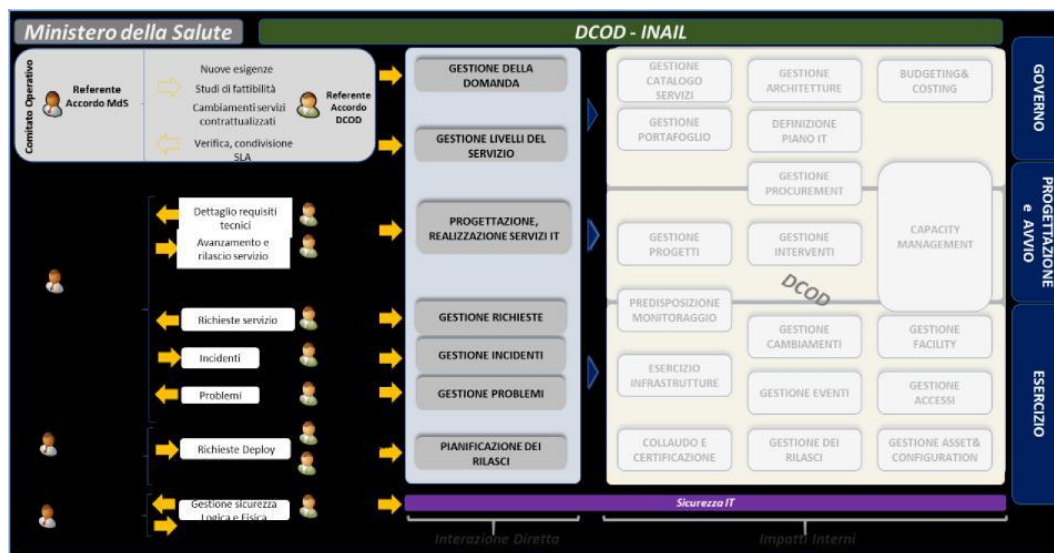


Figura 3 - Modello di funzionamento DCOD INAIL - MDS

### 2.4.1 Ruoli e responsabilità

Le attività svolte dalle risorse a copertura dei ruoli di seguito descritti, così come previsti dal modello di funzionamento riportato nella figura precedente, rientrano nel servizio di "Program



Management" che si attiva dalle fasi iniziali della progettazione dei servizi MdS e che resta attivo per tutta la durata dell'Accordo Quadro.

In particolare i ruoli proposti a supporto della gestione della relazione con il MdS sono:

- **Ruoli a supporto delle fasi di governo e Progettazione e Avvio:** sovrintendono alle attività di raccolta delle esigenze, pianificazione e progettazione dei servizi, verifica e condivisione degli SLA. In particolare, per quanto attiene ai ruoli e responsabilità dei ruoli che compongono il Comitato Operativo (Referente dell'Accordo DCOD INAIL e Referente dell'Accordo Ministero della Salute, si rimanda a quanto previsto nell'Accordo di Collaborazione).

Di seguito un dettaglio degli altri ruoli:

- **Service Manager DCOD INAIL:** è responsabile della corretta erogazione del servizio di Hosting Evoluto al Ministero della Salute, in tutte le sue componenti di servizio di dettaglio, nel rispetto dei livelli di servizio definiti. Inoltre:
  - partecipa alla fase di definizione delProgetto dei fabbisogni a supporto del Referente dell'Accordo DCOD INAIL;
  - partecipa alle fasi di verifica e collaudo del servizio di Hosting evoluto e nella pianificazione delle attività di attivazione del servizio;
  - partecipa agli incontri periodici di verifica dei livelli di servizio a supporto del Referente dell'Accordo DCOD INAIL;
  - partecipa ai tavoli congiunti con il Service Manager del MdS e con il Problem Manager DCOD INAIL in caso di problemi ripetuti o a seguito di Major Incident risolti con **workaround**;
  - indirizza, all'interno delle strutture di Operation DCOD INAIL, eventuali richieste specifiche da parte del Service Manager del MdS (gestione accessi, gestione adeguamenti del servizio, gestione manutenzioni, ...) che non hanno impatti significativi sul servizio in termini economici o di relazione.
- **Project Manager DCOD INAIL:** è responsabile del processo di pianificazione operativa e realizzazione delle attività necessarie per avviare l'erogazione del Servizio di Hosting Evoluto in tutte le sue componenti. Le figure di Project Manager possono variare nel corso del ciclo di vita del servizio erogato al Ministero della Salute. In particolare, oltre al Project Manager responsabile del progetto di Transizione (Avvio del servizio) potrebbero essere nominati altri Project Manager, successivamente all'avvio in esercizio del Servizio, in caso di significativi cambiamenti al Servizio stesso. Rappresenta la figura di





coordinamento delle attività progettuali e il garante del raggiungimento degli obiettivi di progetto definiti nel rispetto dei vincoli di tempo, qualità e costi definiti.

- **Security Manager DCOD INAIL:** è responsabile di tutti gli aspetti operativi e tecnologici necessari a garantire un'erogazione sicura dei servizi nei confronti del Ministero della Salute.
- **Ruoli Operativi a supporto della fase di esercizio del servizio:** sovrintendono alle attività di esercizio del servizio erogato (*day-by-day*) con l'obiettivo di garantirne la continuità, la disponibilità e le performance, nel rispetto dei livelli di servizio definiti e della complessità e specificità delle singole componenti di servizio che concorrono al Servizio di Hosting evoluto erogato al Ministero della Salute.

In particolare:

- **Incident Manager DCOD INAIL:** è responsabile del processo di gestione dei malfunzionamenti, con l'obiettivo di ripristinare il più rapidamente possibile le normali condizioni di operatività limitando gli impatti negativi sul business e quindi sulla disponibilità e performance delle applicazioni del Ministero della Salute presenti nell'Infrastruttura IT DCOD INAIL. Oltre a indirizzare e coordinare le attività di ripristino del servizio, è responsabile dell'attivazione dei necessari flussi di comunicazione verso il Service Manager del MdS in caso di potenziali o effettivi Major Incident (per una descrizione del processo di rimanda al par. 4.3 Processo Gestione degli Incidenti)
- **Problem Manager DCOD INAIL:** è responsabile del processo di rilevazione di eventuali situazioni "strutturali" o "continue" di disservizio, o impattanti sulla qualità percepita del servizio stesso, al fine di avviare delle analisi congiunte, anche con risorse definite dal MdS, volte all'individuazione di *workaround* ma soprattutto azioni risolutive delle problematiche riscontrate (per il dettaglio del processo vedi par. 4.4 Processo Gestione dei Problemi).
- **Release Manager DCOD INAIL:** è responsabile delle attività, in ottica end-to-end, di rilascio del software in ambiente di Collaudo, Pre-Produzione e Produzione garantendo:
  - Pianificazione congiunta e tempestività dei rilasci richiesti dal Release Manager del MdS;
  - Verifica della consistenza dei pacchetti SW rilasciati.

Di seguito sono descritti i ruoli previsti lato MdS:

- **Service Manager MdS:** è responsabile tecnico operativo del servizio di Hosting Evoluto per il MdS. È l'interfaccia unica verso i ruoli DCOD INAIL, prima descritti, relativamente a:



- definizione dei requisiti tecnici del servizio in fase di progettazione ed avvio ed in caso di cambiamento dello stesso;
  - gestione degli Incidenti e dei Problemi;
  - gestione delle richieste di servizio.
- **Release Manager Mds:** è responsabile di gestire la relazione con il Release Manager DCOD INAIL per gli ambiti applicativi di competenza, in termini di:
    - pianificazione congiunta dei rilasci applicativi
    - verifica dei rilasci applicativi
    - gestione di problematiche rilevate in fase di certificazione del rilascio.
  - **Security Manager Mds:** responsabile di tutti gli aspetti operativi e tecnologici necessari a garantire un'erogazione sicura dei servizi in coerenza.

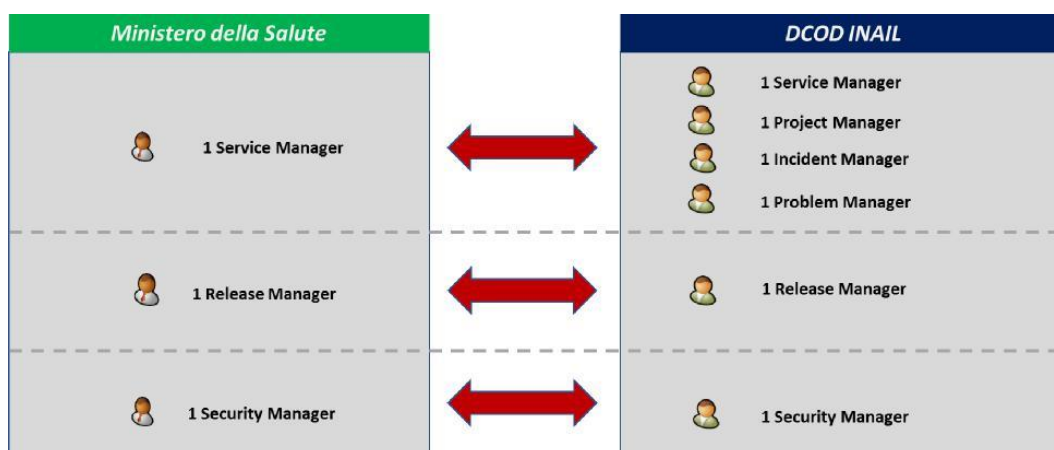


Figura 4 - Modello di funzionamento integrato MDS - DCOD INAIL



### **3 GESTIONE OPERATIVA E HOSTING**

#### **3.1 Gestione Operativa**

Il servizio di Gestione Operativa è l'insieme di tutte le attività necessarie a garantire il corretto funzionamento dell'infrastruttura tecnologica messa a disposizione dalla DCOD INAIL INAIL, e degli apparati di proprietà del MdS, ovvero di propri *outsourcer* (es. HSM, VDC, Firewall, IDS/IPS, WAF, ...), se presenti presso i CED della DCOD INAIL.

Le attività previste sono relative alla pianificazione e gestione operativa di tutte le attività tecnico-sistemistiche sui sistemi gestiti, volte ad assicurare la completa disponibilità ed operatività degli stessi.

Comprende inoltre le attività necessarie all'avvio in esercizio dei nuovi prodotti e/o servizi (es. installazione, parametrizzazioni, configurazioni, ecc.).

Per le attività svolte tramite terze parti, la DCOD INAIL supervisiona lo svolgimento di tali attività fino al loro completamento segnalando tempestivamente al MdS qualsiasi anomalia riscontrata che possa impedire l'uso operativo dei nuovi prodotti/servizi da parte degli utenti.

##### **3.1.1 Interruzione servizi agli utenti**

Le attività di gestione operativa saranno svolte senza discontinuità operativa nei servizi erogati agli utenti.

Per le attività che potrebbero creare interruzione dei servizi erogati agli utenti, e che non potessero essere effettuate al di fuori dell'orario di disponibilità dei servizi erogati agli utenti, sarà preventivamente richiesta al Service Manager MdS l'autorizzazione a procedere.

##### **3.1.2 Accesso per ispezioni del Ministero della Salute**

Sarà consentito, previa richiesta del MdS e susseguente autorizzazione della DCOD INAIL, l'accesso a tutti i siti e sistemi gestiti, compresi i sistemi di gestione, monitoraggio e controllo, al personale del MdS o di terze parti delegato.

##### **3.1.3 Assistenza e supervisione terze parti**

Nel servizio di Gestione Operativa sono comprese tutte le attività di assistenza e supervisione svolte a supporto del MdS o di terze parti coinvolte nella gestione del sistema informativo del MdS. Tale assistenza e supervisione consiste sia nella fornitura di informazioni e dati circa il sistema informativo del MdS sia nel supporto on-site allo svolgimento delle attività che comportino un qualsiasi cambiamento al sistema informativo del MdS (da semplice upgrade prodotti software di base a installazione nuovi apparati). Sarà garantito il conseguente aggiornamento del sistema di gestione della configurazione a fronte di qualsiasi modifica effettuata direttamente o da terze parti.



#### **3.1.4 Gestione dei fabbisogni di evoluzione infrastrutturale e del change management**

Per poter assicurare la coerenza tra le risorse IT e le effettive esigenze elaborative del MdS la DCOD INAIL utilizzerà il servizio di *Capacity Planning* per valutare ed effettuare i necessari interventi adeguativi in accordo con i responsabili di MdS.

A tal fine la DCOD INAIL, qualora si rendesse necessario un cambiamento significativo nel sistema informativo del MdS, metterà a disposizione sia le informazioni necessarie provenienti dai sistemi di controllo e monitoraggio sia le risorse tecniche per le valutazioni. Gli interventi di evoluzione infrastrutturale dovranno di norma avvenire senza discontinuità o degrado dei servizi erogati agli utenti.

La DCOD INAIL supporterà il MdS e le eventuali terze parti coinvolte nello svolgimento operativo delle attività di adeguamento. Quanto sopra dovrà avvenire nei tempi e nei modi da concordare in base all'entità degli interventi.

#### **3.1.5 Gestione cataloghi**

Saranno gestiti i Cataloghi realizzati dal Fornitore uscente acquisiti durante la fase di assessment.

Si garantiscono le successive attività di aggiornamento.

Eventuali evoluzioni saranno considerate nelle attività di Evoluzioni Architettura Tecnico Applicativa.

#### **3.1.6 Asset Management**

La DCOD INAIL attraverso il servizio di Asset Management realizza la gestione delle seguenti tipologie di "asset": software (applicativo, middleware, software di base e di sistema); hardware; sistemi di elaborazione fisici e virtuali; storage; apparati di rete, di sicurezza ed altri dispositivi.

Il servizio garantisce al MdS la costante disponibilità e aggiornamento delle informazioni circa gli asset gestiti anche attraverso l'accesso da remoto al sistema di gestione agli utenti che saranno indicati da MdS.

#### **3.1.7 Classificazione sistemi e orari di riferimento**

La classificazione dei sistemi, in relazione alla loro criticità, sarà recepita dal documento di BIA che il MdS renderà disponibile nella fase di assessment insieme all'elenco dei sistemi e degli apparati con l'indicazione della criticità degli stessi e Orari di Riferimento.

Tale "elenco" sarà oggetto di verifica con gli uffici del MdS responsabili dei servizi applicativi.

Sarà gestito l'aggiornamento dell'elenco dei sistemi e degli apparati a fronte di qualsiasi modifica apportata al sistema informativo.



### 3.1.8 Misurazione della baseline di sistema

Sarà garantito il massimo supporto per la raccolta di tutti i dati e le informazioni necessarie alla revisione dei parametri previsti nella Baseline di Sistema che il MdS fornirà durante la fase di assessment.

### 3.1.9 Manutenzione Licenze

I prodotti software compresi nel servizio di Hosting che saranno messi a disposizione dalla DCOD INAIL, nelle quantità necessarie per il funzionamento del sistema informatico del MdS, sono:

- le licenze di base e sistema dei server fisici e virtuali ricompresi nell'infrastruttura
- i software di virtualizzazione;
- i software e agent di monitoraggio e controllo dei sistemi di elaborazione;
- i software di gestione e di controllo del sistema informatico del MdS;
- i software necessari per la erogazione dei servizi di gestione del ciclo di vita del software e delle infrastrutture;
- i software infrastrutturali e di sicurezza;
- i software necessari ai sistemi di DR;

Sarà inoltre compresa nel servizio la fornitura delle suddette licenze, in caso di ulteriori sistemi di elaborazione attivati durante il periodo contrattuale.

Il MdS renderà invece disponibile l'utilizzo a titolo gratuito per tutta la durata del contratto i prodotti software *middleware* ed applicativi di cui è titolare di licenza d'uso, come da piano dei fabbisogni (allegato 'Licenziato MdS') per gli ambienti messi a disposizione dalla DCOD INAIL.

## 3.2 Hosting

Il servizio di Hosting comprende tutte quelle attività necessarie alla gestione operativa degli ambienti messi a disposizione per il Ministero della Salute, ovvero:

- Gestione Sistemi
- Reti (*Data Center*)
- *Storage*
- *Backup & Restore*
- *Deploy* applicativi
- Sicurezza delle informazioni
- Connettività

Di seguito si riporta una descrizione delle singole attività.



### 3.2.1 Gestione dei sistemi

La gestione sistemi ne comprende l'intero ciclo di vita, dall'installazione alla configurazione iniziale, alla manutenzione e fino alla loro dismissione.

Si descrive, di seguito sinteticamente, il ciclo di vita della gestione dei sistemi offerta al MdS.

### 3.2.2 Installazione

I sistemi fisici saranno posizionati nelle aree dei Data Center DCOD INAIL, messi a disposizione per MdS. L'ubicazione sarà scelta a valle di un assessment che terrà conto di fattori quali:

- Assorbimento elettrico;
- Calore dissipato;
- Relazioni con altri apparati (apparati di rete, altri server con cui si dovranno interfacciare, collegamento alla SAN)

A garanzia di affidabilità e rispetto delle specifiche tecniche richieste, il posizionamento e la configurazione iniziale dei nuovi sistemi fisici saranno affidati ai vendor di prodotto.

- L'installazione del software di base, vale a dire, sistemi operativi, hypervisor, piattaforme di DBMS e *Middleware* - sarà eseguita da personale esperto e certificato, nel rispetto di politiche di qualità e di sicurezza, ambito di Sicurezza e Protezione dei Sistemi stabilite dall'AgID;
- Per perseguire obiettivi di standardizzazione, i sistemi virtuali e gli oggetti Cloud, saranno basati su template standard, tenuti costantemente aggiornati, saranno rilasciati con strumenti di automazione e orchestrazione specifici di mercato per soddisfare, nel minor tempo possibile, richieste di ampliamento di capacità elaborativa e implementazione di nuovi servizi.

Che si tratti di sistemi fisici o virtuali, a valle delle installazioni, saranno effettuati test di *fault tolerance* (laddove applicabili) e di vulnerabilità.

### 3.2.3 Conduzione dell'infrastruttura

La conduzione degli ambienti elaborativi MdS sarà svolta utilizzando strumenti e processi di service operation già utilizzati e collaudati dalla DCOD INAIL, finalizzati alla sicurezza, alla stabilità e alla disponibilità degli stessi:

- **Accesso ai sistemi:** l'accesso ai sistemi, da parte di MdS, in modalità protetta e sicura sarà consentito al solo personale qualificato ed autorizzato, garantito da sistemi e protocolli di autenticazione adeguati e conformi alle politiche di sicurezza Agid già recepite da DCOD INAIL;
- **Aggiornamenti software:** saranno applicati con cadenza condivisa con MdS e, laddove si renda necessario con procedure d'emergenza, gli aggiornamenti rilasciati



periodicamente dai *software vendor*, per rimuovere bachi e vulnerabilità descritte nei propri bollettini di sicurezza. Tali aggiornamenti saranno applicati mediante prodotti di *software distribution* specifici per ogni piattaforma che la DCOD INAIL metterà a disposizione di MdS;

- **Gestione di eventi e anomalie:** il monitoraggio costante e proattivo, sia della disponibilità che delle prestazioni del singolo componente infrastrutturale, garantirà ad MdS tempestività nella presa in carico e risoluzione delle anomalie in conformità con il processo di Incident Management.
- **Tuning delle performance:** I sistemi saranno soggetti costantemente a verifiche di performance, mirate alla ottimizzazione delle configurazioni più adatte alle esigenze operative;
- **Supporto al processo di Capacity Management:** sarà periodicamente elaborata e prodotta una reportistica specifica per valutare la capacità elaborativa dell'infrastruttura, l'utilizzo delle risorse fisiche e il corretto utilizzo delle licenze SW. Queste informazioni saranno inoltre utilizzate per perseguire obiettivi di virtualizzazione di componenti infrastrutturali nonché di adozione di soluzioni Cloud, sia pubblico che privato.

#### **3.2.4 Assistenza Sistemistica**

Le attività di assistenza sistemistica sono relative alla gestione del software di base e di sistema e delle relative licenze software dei sistemi gestiti nei Data Center della DCOD.

Sarà garantito il costante aggiornamento del software e la disponibilità delle correzioni, nel rispetto dei vincoli e degli obblighi e dei livelli di servizio previsti, senza ulteriori oneri per il MdS. Pertanto sarà a carico della DCOD INAIL l'acquisizione di nuovo software al fine di garantire la continuità di gestione, l'ottimizzazione ed il miglioramento qualitativo dei servizi esistenti.

#### **3.2.5 Gestione configurazioni hardware, software di base e applicativo e relativi ambienti**

Saranno gestite e tenute sotto costante controllo:

- le configurazioni hardware, software di base e relativi ambienti;
- i software applicativi ed ambienti, relativi ai sistemi centrali;
- le reti in funzione delle necessità operative;
- le modifiche che fossero eventualmente necessarie;
- i piani di installazione

#### **3.2.6 Manutenzione HW**

La manutenzione hardware riguarda tutte le attività necessarie per ripristinare il funzionamento dei sistemi a fronte di guasti e comprende la responsabilità completa della riparazione dei



sistemi, inclusa la fornitura dei componenti da sostituire a quelli guasti/difettosi. La sostituzione dei componenti è effettuata solo ed unicamente con ricambi nuovi ed originali, salvo espressa autorizzazione di altre soluzioni (es. prodotti rigenerati).

Le attività previste sono di tre tipi:

- manutenzione preventiva, consistente nella verifica periodica e programmata delle apparecchiature con lo scopo di assicurare la perfetta funzionalità di tutti i componenti prevenendo possibili situazioni di errore e/o degrado;
- manutenzione correttiva ordinaria, consistente nelle attività volte ad eliminare i malfunzionamenti rimuovendo le cause che li hanno determinati e comprensiva della fornitura delle parti di ricambio;
- manutenzione adeguativa, consistente nelle attività volte ad assicurare la costante aderenza delle procedure e dei sistemi all'evoluzione dell'ambiente tecnologico ed al cambiamento dei requisiti (organizzativi, normativi e d'ambiente).

Il servizio è comprensivo di tutti gli oneri necessari per la perfetta e puntuale esecuzione del servizio stesso, quali a titolo esemplificativo e non esaustivo quelli relativi alla manodopera, parti di ricambio, materiali di consumo, ritiro, imballaggio, riconsegna, nonché ogni altro onere per mantenere e/o riportare in perfetto stato di funzionamento i Sistemi.

Nel rispetto dei livelli di servizio è effettuata la tracciatura sui sistemi di trouble ticketing della DCOD INAIL degli interventi in tutte le sue fasi, fino alla chiusura degli stessi, con il reporting di tutte le azioni intraprese al fine di consentire al MdS di avere la visibilità sulle attività svolte.

Alla fine di ogni trimestre verranno prodotti dei reports contenenti tutti gli interventi prodotti nel corso del periodo, con evidenziati quelli che non hanno rispettato gli SLA previsti e le note di intervento ad essi associate.

### **3.2.7 Reti (Data Center)**

I sistemi del MdS saranno ospitati nei due *Data Center* della DCOD INAIL, ubicati entrambi a Roma a una distanza di circa 30 km, collegati sia con connessioni di livello 2 che di livello 3, tramite vari collegamenti attestati su DWDM ridondati a 10 Gbps.

Sui DWDM insistono anche i collegamenti Infiniband e ISL, che permettono la sincronizzazione continua dello storage. Grazie a tali collegamenti ad alta velocità i due siti sono virtualmente, dal punto di vista della rete, come un sito unico.

Entrambi i siti erogano servizi, in configurazione di *Business Continuity*, in cui ognuno è in grado di sopperire ad un eventuale fault dell'altro.

Per la connessione dei sistemi all'interno del data center è prevista una connettività in fibra a 10 Gb in tecnologia *Unified Fabric* (LAN e SAN unificate). Sono anche possibili collegamenti a 1Gb, sia in fibra che in rame.





Sono presenti firewall e bilanciatori Citrix che permetteranno di suddividere la rete in diverse zone di sicurezza. Gli apparati attivi del CED sono prevalentemente di tecnologia Cisco sia per gli *switch* che per i *firewall*.

La gestione della rete è effettuata secondo un modello di gestione omogeneo, centralizzato e altamente integrato, abilitando così l'analisi di tutte le informazioni, la correlazione e la definizione di alberature auto-consistenti per la gestione degli eventi in funzione del loro impatto su una modellazione evoluta dell'IT.

I principali servizi di gestione relativi agli apparati di rete del Data Center sono:

- *Upgrading* software degli apparati
- Gestione baseline, inclusiva di salvataggio periodico e on-demand delle configurazioni
- Configurazione e ottimizzazione
- Gestione delle VPN
- Verifica *early warning*, attraverso i *release bulletin* comunicati dai produttori
- Verifica delle performance
- Gestione specifica degli apparati
- Analisi e risoluzione dei malfunzionamenti (*troubleshooting*).

Il servizio di gestione della rete del Data Center consiste in:

- Gestione di tutti gli elementi che costituiscono l'infrastruttura di rete (rete DC, apparati attivi, VPN IP, ecc.)
- Coordinamento ed esecuzione degli interventi di ripristino delle funzionalità del servizio di rete e/o di apparati TLC
- Riparazione di sistemi/componenti difettosi nel rispetto degli SLA applicabili
- Renderizzazione on-line di mappe di rete aggiornate, in grado di rendere visibile in ogni istante la situazione dei servizi di connettività
- Monitoraggio costante dei parametri significativi della qualità della rete
- Monitoraggio costante delle prestazioni della rete
- Gestione degli incidenti e dei problemi, in corrispondenza di fault non risolvibili al Livello 2 è prevista la "*escalation*" verso un supporto di Livello 3 (vendor) e, in casi specifici, è previsto l'allestimento di una "*crisis room*" mista
- Esecuzione di interventi periodici programmati per garantire il buon funzionamento dei sistemi
- Rendicontazione periodica sui livelli di servizio erogati.
- manutenzione evolutiva del software di rete;
- manutenzione evolutiva del piano degli indirizzi TCP/IP e del piano di naming;
- gestione dell'anagrafico di rete;



- *tuning* delle configurazioni di rete;

Le attività di configurazione e gestione della rete del Data Center sono svolte secondo requisiti di efficienza e sicurezza, con l'obiettivo di assicurare:

- la consistenza della rete e il salvataggio delle configurazioni degli apparati attivi
- l'attivazione del processo di gestione degli incidenti, quando non sia possibile raggiungere una terminazione di rete a livello fisico, di protocollo o di routing
- la gestione della LAN interna al CED e la verifica del corretto funzionamento dei sistemi di supporto alla gestione mediante:
  - controllo delle risorse HW e SW
  - monitoraggio dei processi attivi
  - monitoraggio dei sistemi di backup

### **3.2.8 Connettività**

Per la connessione della DCOD INAIL alla rete di MdS si dovranno realizzare collegamenti da entrambi i Data Center di DCOD Inail verso uno o più siti di MdS al fine di garantire una soluzione in alta affidabilità; tali collegamenti potranno essere realizzati in L2 oppure in MPLS.

Qualora le connessioni Infranet e Internet di MdS non fossero già realizzate presso le sedi di MdS stessa, si potrà provvedere a tali connessioni utilizzando quanto previsto per DCOD Inail in alta affidabilità con attestazioni delle linee in entrambi i due Data Center.

### **3.2.9 Reti (uffici periferici)**

Per uffici periferici si intendono tutte le sedi del Ministero distribuite sul territorio nazionale, comprese le sedi di Roma, Lungotevere Ripa e Carabinieri NAS di Roma, Viale dell'Aeronautica e tutti gli uffici periferici MdS, Centri trapianti d'organo e Carabinieri NAS.

Il servizio comprende:

- Gestione remota degli Switch e delle configurazioni
- Monitoraggio degli Switch
- Manutenzione evolutiva del software di rete
- Manutenzione evolutiva del piano degli indirizzi TCP/IP
- Manutenzione evolutiva del piano di naming;

N.B.: Il servizio non comprende eventuali interventi on-site, la riparazione o la sostituzione degli apparati.

### **3.2.10 Gestione dello spazio su disco (Storage Management)**

Nell'ambito della gestione dello spazio su disco la DCOD INAIL effettuerà per il MdS tutte le attività necessarie a garantire il controllo, il dimensionamento, l'ottimizzazione degli spazi assegnati sulle diverse tipologie di sistemi utilizzati per memorizzare i dati.



Le principali attività comprendono:

- la corretta gestione, manutenzione, installazione e configurazione degli apparati di storage;
- controllo della capacità dei dischi e rilevazione delle criticità;
- la gestione delle LUN e delle partizioni;
- gestione e controllo delle Virtual Tape Library.

Il servizio di archiviazione dati per il MdS è basato su architetture complesse ed eterogenee, costituite da sistemi di fascia *enterprise* e *multivendor*, mirate a soddisfare le diverse esigenze in termini di alta affidabilità, alte prestazioni e scalabilità, in ambito SAN-NAS e Cloud.

I volumi massimi previsti in gestione superano il *Petabyte* per sito.

La connettività è fornita da apparati Cisco, installati su entrambi i *Data Center* ed interconnessi in ISL tra di loro mediante dei DWDM, in due distinte *Fabric*.

L'infrastruttura SAN è già in grado di fornire o integrare soluzioni di:

- **Business Continuity** con la replica sincrona dei dati su base metropolitana;
- **Continuous Availability** per VMware supportando il *clustering active-active* tra due data center mediante i VPLEX unitamente allo storage EMC VMAX.

Di seguito sono descritte le principali attività di erogazione del servizio:

- **Implementazione di nuove configurazioni:** L'implementazione di nuove configurazioni avviene mediante i tool nativi degli apparati. L'implementazione può prevedere l'inserimento di nuovi host in SAN, a seguito di un'analisi sulle matrici di compatibilità.
- **Zoning e IVR** (Inter-VSAN Routing) per la connettività.
- **LUN Creation - LUN Masking - Pool Management - Data Replication** per la parte Storage.
- **Creazione e gestione share in ambito NAS.**
- **Monitoraggio / Gestione Guasti Hardware:** oltre al monitoraggio effettuato on-site, tutti gli apparati sono connessi ai centri di supporto dei vendor ai quali inviano, costantemente (24x7), le eventuali segnalazioni di anomalie. Ciò consente un monitoraggio costante e l'apertura automatica delle chiamate, per attivare immediatamente gli interventi tecnici on-site per la risoluzione dei guasti.
- **Data Replication Management:** La gestione della replica dei dati avviene in ambito SAN con la configurazione della replica di nuovi volumi.  
È prevista anche la replica delle share (su ISILON) in ambito NAS.
- **Capacity Management:** il processo di gestione del Capacity, è supportato attraverso il tool EMC ViPR SRM, che abilita all'elaborazione e all'inoltro schedato di report sulle percentuali di utilizzo dello spazio degli apparati storage in dotazione.



### 3.2.11 Amministrazione database

Le attività di amministrazione dei database svolte dalla DCOD INAIL per il MdS hanno l'obiettivo di:

- garantire la definizione delle procedure operative e le relative documentazioni;
- gestire le utenze e i profili di autorizzazione conformemente a quanto indicato dagli standard di sicurezza relativamente al controllo degli accessi ai database;
- effettuare l'aggiornamento delle release software e/o il livello di patching dei database
- eseguire la gestione e configurazione dei database (riorganizzazione, backup, creazione tabelle, creazione indici, caricamento dati)
- garantire il necessario supporto tecnico specialistico per il controllo, la gestione e l'immissione in esercizio delle funzioni applicative.

A titolo non esaustivo si elencano le principali attività che il team dedicato alla amministrazione dei database svolgerà per il MdS:

- Installazione e configurazione database.
- Ottimizzazione del disegno e delle relazioni della base dati;
- Gestione spazio dati;
- Tuning ed ottimizzazione delle performance;
- Configurazione e gestione delle repliche;
- Manutenzione preventiva e correttiva;
- Change management;
- Produrre output relativi alla gestione delle elaborazioni;
- Produzione della documentazione tecnica di backup e ripristino dei database;
- Controllo e validazione nella fase di rilascio in esercizio delle applicazioni.

### 3.2.12 Gestione Software

Le attività di gestione software sono relative agli interventi di installazione e configurazione del software oltre alla supervisione e supporto di eventuali fornitori esterni. Queste attività vengono svolte sia su base preventiva che correttiva relativamente al Software di base e di sistema messo a disposizione dalla DCOD INAIL e al Software *middleware* ed applicativo messo a disposizione dal MdS, di cui è titolare di licenza d'uso.

Il servizio garantisce l'aggiornamento software, previa verifica degli impatti degli aggiornamenti sulle applicazioni in esercizio. Nelle attività di installazione sono incluse sia le attività di *Software distribution* che di installazione delle componenti applicative.

In questo servizio ricadono quindi sia le attività di applicazione di un aggiornamento per la risoluzione di un malfunzionamento, sia il rilascio di nuove versioni di software conseguenti ad un aggiornamento tecnologico.



In generale, la DCOD INAIL dovrà:

- installare il software secondo un piano concordato con il MdS;
- installare e gestire gli strumenti informatici necessari alla distribuzione elettronica del software;
- parallelizzare il più possibile l'installazione del software in modo da garantire un pronto allineamento delle configurazioni.

L'infrastruttura dedicata alla *software distribution* verrà adeguata in funzione dei requisiti infrastrutturali che esprimerà il MdS.

### 3.2.13 Backup

Il servizio di backup offerto dalla DCOD INAIL mediante la propria infrastruttura, consiste nella gestione dell'archiviazione e ripristino dei dati utenti e di sistema, al fine di prevenire la perdita definitiva degli stessi in caso di eventi accidentali. Data la distribuzione dell'infrastruttura di backup sui due Data Center della DCOD INAIL, ove ciascun sito dispone di una VTL Data Domain 7200 di circa 186 TB, di una VTL Data Domain 990 di circa 275 TB, oltre che di Server fisici su cui è installato il software EMC Networker e Server fisici su cui è installato il software EMC Avamar, è possibile replicare (clonare) i backup tra i due siti.

Le soluzioni SW adottate per la gestione dei backup sono:

- EMC Networker per il backup delle basi dati (Oracle e SQL) e file system di server fisici. Per consentire il dialogo tra il server e i client è necessaria l'installazione dell'agent su questi ultimi.
- EMC Avamar per il backup dell'infrastruttura virtuale. L'ambiente Avamar viene utilizzato esclusivamente per il salvataggio dei dati provenienti da server virtuali, presenti su ciascun sito, per i quali viene effettuato il backup delle snapshot. Per consentire il dialogo tra il server Avamar e i vCenter, sono state installate, all'interno di questi ultimi, alcune VM utilizzate come proxy.

La DCOD INAIL potrà fornire diverse modalità di backup in base al software utilizzato e in base alle caratteristiche dei server oggetto di backup. In particolare, vengono eseguiti backup full per i database e backup delle *snapshot* per le Virtual Machine (VM).

Anche la schedulazione dei backup può variare a seconda dell'ambiente e della tipologia di backup ed è organizzata per ridurre al massimo i periodi di degrado prestazionale dovuto alla sovrapposizione dei job.

Di seguito qualche esempio di schedulazione già in erogazione per gli ambienti della DCOD INAIL:

- i backup full dei database (Oracle e SQL) vengono eseguiti con frequenza giornaliera al di fuori dell'orario di operatività,
- Archive database Oracle: ogni ora



- *Snapshot* di VM: due volte a settimana per i sistemi di produzione e certificazione, una sola volta per quelli di sviluppo e management.

Le policy di backup saranno definite in base alle specifiche esigenze del MdS. È possibile prevedere *retention* di durata diversa in base a specifici requisiti.

I backup saranno eseguiti con la periodicità fissata in accordo tra le parti.

#### **3.2.14 Restore**

A garanzia dell'effettiva possibilità di ripristino del dato, le policy della DCOD INAIL prevedono, per ogni job di backup, specifici test di restore.

Il restore di un backup viene solitamente effettuato per l'insorgere di una specifica esigenza (ad esempio in seguito a perdita accidentale o corruzione di dati su un sistema).

L'attuazione del restore prevede che siano specificate le informazioni relative al sistema da ripristinare e la versione dei dati da ripristinare.

Il gruppo di gestione dell'infrastruttura di Backup/Restore provvede quindi a ripristinare i dati e al termine informa il richiedente sull'esito dell'operazione.

#### **3.2.15 Gestione delle elaborazioni**

La gestione delle elaborazioni comprende tutte le attività che garantiscono la corretta esecuzione dei cicli elaborativi in base a quanto indicato dal MdS nelle specifiche tecniche e funzionali delle applicazioni.

In base alla pianificazione concordata o alle specifiche richieste del MdS verranno adottati dei meccanismi di controllo.

Un primo livello di controllo sarà di tipo sistemistico atto a verificare che le elaborazioni non si siano interrotte per problemi inerenti l'infrastruttura. In tal caso le azioni correttive potranno variare dal semplice rilancio dell'elaborazione (una volta risolto il problema infrastrutturale) al coinvolgimento di tecnici del Ministero della Salute nei casi in cui sia necessario prendere decisioni drastiche (i.e. cancellare un job che occupa il 100% della CPU introducendo problemi di *locking* su più tabelle).

In tutti i casi in cui l'elaborazione non va a buon fine verrà informata la controparte indicata dal MdS (i.e. una e-mail di struttura) per la verifica dei risultati e, nel caso emergano delle problematiche, saranno concordati gli interventi necessari alla rimozione dei malfunzionamenti.

Saranno inoltre condivise con il MdS le modalità di controllo degli output delle elaborazioni al fine di dare visibilità al MdS stesso sull'andamento delle elaborazioni effettuate sui sistemi informativi.



### 3.2.16 Servizi di Dominio

Il MdS con i servizi di dominio potrà effettuare la gestione degli utenti e delle risorse nonché utilizzare le directory dalle applicazioni opportunamente abilitate.

In questo ambito verrà garantita la gestione dell'intero ambiente *Active Directory*, con l'obiettivo di assicurare la disponibilità del servizio di directory per la gestione delle risorse (es. stampanti, cartelle condivise) degli utenti (account utenti e gruppi) e delle impostazioni di sicurezza.

La gestione include:

- Gestione Domini e trust;
- Gestione dei siti e delle subnet;
- Gestione delle Group Policy in ambito Server e in ambito PdL;
- Gestione infrastruttura PKI per i certificati interni al dominio;
- Monitoraggio e analisi log.

Inoltre con la gestione sistemistica dell'infrastruttura di Domain Controller presenti nei Data center INAIL verranno assicurate al MdS le seguenti attività:

- Gestione sistemistica server (verifica volumi, analisi dei log sistema, ecc.);
- Gestione del patch management dei server (Wsus);
- Gestione backup *system state* per tutti i domain controller;
- Monitoraggio per tutti i domain controller;
- Gestione Antivirus.

### 3.2.17 Transizione IPv4/IPv6

Qualora il MdS deciderà di procedere alla transizione dalla versione 4 alla versione 6 del protocollo di rete IP, la DCOD INAIL garantirà tutto il supporto necessario alla migrazione e all'adeguamento tecnologico.

### 3.2.18 Deploy applicativi

La standardizzazione del processo di rilascio consente di evitare problematiche tipiche del *deploy* quali disallineamenti delle configurazioni, errori nella costruzione dei package prima del rilascio, ecc.

Le attività di *deploy* sono gestite da un team dedicato, le cui responsabilità operative si possono riassumere come segue:

- Acquisizione delle richieste di deploy (RFC Deploy) già autorizzate dai Release Manager di MdS;
- Interazione e allineamento costante con il Release Manager DCOD INAIL;
- Approccio differenziato per gli ambienti di Collaudo, Pre Produzione e Produzione, date le diverse specificità degli ambienti.

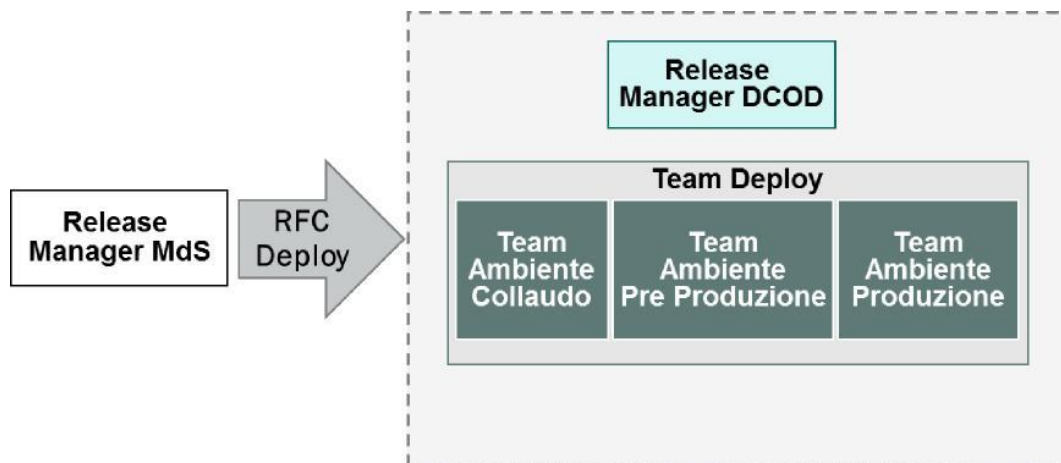


Figura 5 - Deploy

Sono utilizzate procedure specifiche per i diversi tipi di *deploy*:

- **Standard Deploy:** rilasci di applicazioni conformi agli standard architetturali;
- **Custom Deploy:** rilasci autorizzati ma che non rispettano gli standard architetturali o le linee guida di sviluppo del software; per loro natura queste tipologie di rilasci non sono automatizzabili o standardizzabili, ma richiedono attività specifiche. Le modalità operative per questa tipologia di deploy verranno stabilite successivamente sulla base delle necessità che emergeranno.

I principali ambienti interessati dal rilascio applicativo comprendono gli Application Server (*Weblogic, Jboss, SAG WebMethods e Websphere*) nonché i Data Base (DB2, Oracle, SQL, MySQL). Per ogni applicazione viene richiesta la documentazione contenente tutti gli elementi utili per il deploy e l'esercizio dell'applicazione stessa. La soluzione utilizzata per gestire i *workflow* autorizzativi per gli Standard Deploy è basata sul tool *Rational Team Concert* con utenze di accesso messe a disposizione da DCOD Inail per MdS.

### 3.2.19 Sicurezza delle Informazioni

La sicurezza delle informazioni è un requisito determinante per l'espletamento della *mission* istituzionale di INAIL poiché influisce sul corretto svolgimento delle sue attività e sulla sua immagine. La sicurezza delle informazioni è anche un obbligo di legge dal momento che il D.Lgs. 196/2003, e a partire da maggio 2018 il nuovo Regolamento europeo per la Privacy, stabiliscono precisi obblighi legati alle operazioni di trattamento di dati personali.

La sicurezza delle informazioni assume rilevanza ancora più grande in relazione al contesto tecnologico ed innovativo nel quale si inquadrano le attività della DCOD INAIL e questo è ancor più vero nel contesto di erogazione dei servizi IT verso il Ministero della Salute.

Per questi motivi la DCOD INAIL ritiene sia imprescindibile disporre di strumenti fortemente tecnologici nel contrasto al crimine informatico e al contempo di risorse professionali che





possano lavorare in sinergia con tali strumenti, e, a tal scopo, ha adottato un modello interfunzionale che è articolato su tre livelli, ognuno dei quali individuato da un preciso ambito di responsabilità:

- Il livello di **indirizzo** (*Governance di Sicurezza*);
- Il livello **operativo** (*SOC*);
- Il livello di **controllo** (*Audit*).

### 3.2.20 Governance di Sicurezza

La Governance di Sicurezza stabilisce, attua, mantiene e migliora il Sistema di Gestione per la Sicurezza delle Informazioni in conformità ai requisiti della norma ISO/IEC 27001. Supporta la DCOD INAIL nella definizione delle politiche per la Sicurezza delle Informazioni, stabilendo gli obiettivi e le regole per il raggiungimento dei livelli di sicurezza proposti, in linea con gli obiettivi istituzionali e nel rispetto delle normative vigenti in materia di sicurezza e privacy. Tali politiche, insieme a linee guida e procedure operative specifiche, sono distribuite a tutti gli interessati, in particolare ai gruppi di gestione IT che operano in conformità ai requisiti di sicurezza emanati dalla Governance.

### 3.2.21 Security Operation Center

Nel *Security Operation Center* (SOC) della DCOD INAIL confluiscono risorse tecniche altamente specializzate, norme/procedure comportamentali e piattaforme hardware e software dedicate alla gestione della sicurezza.

I servizi che vengono erogati nell'ambito del SOC sono i seguenti:

- **Servizio di Autenticazione e Autorizzazione per l'accesso ai server** basato su tecnologia Microsoft Active Directory, garantisce che la fase di autenticazione sia effettuata prima di ulteriori interazioni tra la risorsa ed il soggetto richiedente. Nel caso di necessità di uso delle utenze privilegiate non nominali, è messa a disposizione una Cassaforte Elettronica realizzata con il prodotto CyberArk.
- **Servizio di firewalling sulla rete interna** garantisce la protezione, attraverso una serie predefinita di regole di sicurezza, tra le reti interne che hanno livelli di sicurezza differenti, permettendo una segmentazione basata sul livello di esposizione e sul livello di criticità delle informazioni contenute sui sistemi.
- **Servizi proxy** consentono di proteggere la navigazione in ingresso e uscita dal data center. Nello specifico sono inclusi:
  - il servizio di Proxy che consente sia all'utenza interna che ai server e ai servizi, ove necessario, di navigare su Internet, applicando una serie di misure di sicurezza, quali il blocco di categorie di siti ritenute non attendibili o non



- opportune, il blocco di protocolli non necessari, il controllo antivirus sui contenuti scaricati;
- Il servizio di Reverse Proxy che consente di pubblicare le applicazioni web fornendo una serie di funzionalità specifiche di sicurezza, tra cui funzionalità per il monitoraggio del traffico, per il bilanciamento di carico verso i web server, così come altri controlli di sicurezza e *caching*.
  - **Servizio di Log Management e Correlazione (SIEM)** realizza le attività di *logging*, monitoraggio e correlazione degli eventi di sicurezza. La correlazione, mettendo in relazione gli eventi di diversa origine raccolti centralmente, evidenzia e segnala sequenze di attività potenzialmente ostili e/o non autorizzate. Il servizio può essere configurato per ricevere tutti i log delle attività degli Amministratori di Sistema, in conformità con la normativa sulla Privacy vigente.
  - **Servizio di gestione Antivirus e Host IPS** centralizza la gestione delle componenti antivirus e HIPS (*Host Intrusion Prevention System*) al fine di prevenire intrusioni illecite e contrastare le minacce legate a software malevolo. La soluzione prevede, a protezione di server e PdL, l'implementazione di regole di protezione tramite firme, sistemi comportamentali HIPS, funzione di *firewall stateful* dinamico, nonché regole di protezione specifiche per server database e web.

### 3.2.22 Audit Di Sicurezza

Il servizio di Audit presiede alla verifica della corretta attuazione delle strategie per la sicurezza delle informazioni, e della conformità alla normativa applicabile. Lavora in sinergia con la Governance, organizzando le campagne di audit sulla base delle indicazioni emanate.

### 3.3 Housing

Nell'ambito del servizio di *housing* la DCOD INAIL garantisce la sicurezza fisica per MdS attraverso il controllo all'accesso ai locali CED dei siti di erogazione con l'uso del badge personale e con la registrazione sui sistemi anti-intrusione. La gestione delle autorizzazioni è svolta dalla DCOD INAIL attraverso specifici processi interni. Oltre ad autorizzare le abilitazioni per il personale interno predispone e comunica alla sicurezza una lista di persone autorizzate ad accompagnare personale di terze parti o del MdS. Il servizio di guardiania presente H24 nei CED dei siti primario e secondario verifica la lista e rilascia badge di accesso temporaneo al personale autorizzato. Il personale della guardiania conduce delle ispezioni dei locali e dei sistemi di allarme più volte nella giornata in base ad una pianificazione predefinita.



I controlli ambientali prevedono la costante verifica degli ambienti e dei sistemi ausiliari attraverso un sistema automatico. Il servizio di guardiania garantisce il presidio e il monitoraggio di questo sistema e, in caso di malfunzionamenti o anomalie, attiva i servizi di manutenzione.

La manutenzione programmata esegue interventi di manutenzione periodica sui sistemi ausiliari dei Data Center, primario e secondario, per verificare e garantire il loro corretto funzionamento. È prevista la comunicazione dei piani di manutenzione programmata da parte della DCOD INAIL al MdS nonché l'evidenza dei test periodici eseguiti.

### **3.4 Servizio di monitoraggio**

Attraverso la Service Control Room la DCOD INAIL garantirà al Ministero della Salute un servizio di monitoraggio in logica End to End delle applicazioni ospitate sull'Infrastruttura IT della DCOD INAIL. La missione è quella di centralizzare le attività di monitoraggio per aumentare la conoscenza in real time della disponibilità e delle performance delle applicazioni con un duplice obiettivo:

- Tempestiva, e sempre più proattiva attivazione dei gruppi operativi (infrastrutturali o applicativi) per avviare interventi risolutivi di eventuali problematiche che potrebbero avere impatti sulla disponibilità e performance dell'applicazione;
- Fornire dati strutturati e complessivi in grado di favorire l'eventuale *troubleshooting* in caso di incidenti o a supporto delle attività dei Gestione dei Problemi.

In particolare, attraverso la Service Control Room, la DCOD INAIL garantirà al Ministero della Salute un monitoraggio integrato delle applicazioni correlando eventi e metriche di tutte le sue componenti: Transazioni applicative, Sistemi, Apparati di rete, Database, Apparati Storage e Percezione utente (end user monitoring).

I servizi di monitoraggio prevedono:

- la predisposizione dei modelli di servizio/applicazioni che correlano gli eventi/metriche delle componenti infrastrutturali, applicative e di percezione utente per la definizione dello stato di salute e di rischio potenziale dell'applicazione;
- la gestione degli eventi rilevati dagli strumenti di monitoraggio sulle componenti impattate attraverso l'apertura, il corretto indirizzo e controllo di ticket verso i gruppi di II livello applicativi ed infrastrutturali, come descritto nella sezione Esercizio relativamente alla gestione degli incidenti;
- elaborazione ed invio di reportistica operativa e direzionale relativa all'andamento e alle problematiche dei servizi/applicazioni monitorati;
- il monitoraggio dei livelli di servizio tecnologici (misurazioni oggettive attraverso l'acquisizione di dati mappati e tracciati su prodotti standard dello stato dell'arte, quale strumentazione ufficiale).



Nei paragrafi successivi si riporta una descrizione dell'organizzazione della Service Control Room e dell'architettura di monitoraggio di riferimento.

### 3.4.1 Service Control Room

La Service Control Room opererà in modalità h24 7 giorni su 7 con rotazione di risorse su 3 turni. Saranno impegnate sui servizi di monitoraggio le seguenti figure:

- **Coordinatori team di monitoraggio:** risorse Inail che monitorano ed indirizzano nel day by day le attività degli operatori di monitoraggio;
- **Coordinatori team di supporto:** risorse Inail che governano le attività di predisposizione del monitoraggio, di predisposizione reportistica, di misurazione SLA tecnologici e supporto al troubleshooting nella gestione di Major Incident e Problem;
- **Operatori del monitoraggio:** risorse esterne focalizzate sul monitoraggio continuativo delle applicazioni al fine di indirizzare in tempi ristretti gli eventuali ticket ai gruppi specialistici effettivamente impattati;
- **Sistemisti:** risorse esterne focalizzate sulla manutenzione continua dei modelli di servizio/applicazioni monitorati, elaborano la reportistica, misurano gli SLA e supportano il *troubleshooting* in caso di *Major Incident* o *Problem*.

L'architettura di monitoraggio proposta, nell'ambito del servizio di Hosting Evoluto per il Ministero della Salute, sarà organizzata sui seguenti livelli:

- **Livello 1:** sistemi verticali di monitoraggio che operano in modalità agent based e agentless che rilevano gli eventi (fault e superamento soglie delle metriche) sulle componenti dell'infrastruttura IT di riferimento:
  - a. CA APM e IBM ITCAM per monitoraggio applicativo
  - b. CA SPECTRUM, NAGIOS e TIVOLI per monitoraggio infrastrutturale e di rete
  - c. EMC VIPR per monitoraggio Storage
  - d. CA APM (componenti CEM e Cloud Monitor) per monitoraggio *end-user-experience* reale e simulata.
- **Livello 2:** strato di integrazione dei dati provenienti dai sistemi di monitoraggio verticali verso il sistema CA SOI attraverso dei connettori standard esistenti.
- **Livello 3:** sistema CA SOI, in cui sono definiti e gestiti i modelli di servizio/applicazioni in ottica end-to-end. Attraverso la correlazione dei dati provenienti dai sistemi di monitoraggio integrati viene presentata una situazione in termini di qualità e disponibilità del servizio erogato.

Il perimetro di monitoraggio tecnico, per ciascuna applicazione del Ministero della Salute, che verrà garantito è il seguente:

- Monitoraggio delle componenti infrastrutturali della catena tecnologica:



- Web Server
- Application Server
- DB Server
- Apparati di rete
- Storage.

Per ciascuna componente saranno monitorati i principali parametri tecnologici quale CPU, RAM, File System e UP/DOWN delle porte

- Monitoraggio della componente applicativa:
  - Transazioni ed attraversamento dei vari Tier applicativi (errori, tempi di attraversamento);
  - Utilizzo CPU, RAM, File System da parte delle specifiche applicazioni
  - Errori applicativi.
- Monitoraggio della componente End User (traffico Reale e simulato). Saranno garantiti:
  - monitoraggio sul traffico reale (Customer Experience Monitoring), errori e tempi di risposta delle transazioni web utente, in funzione dello specifico canale/device di accesso alla transazione
  - monitoraggio di percorsi di navigazione che simulano l'operatività e l'interazione dell'utente con l'applicazione (Cloud Monitor).

In termini operativi, la piattaforma integrata di Service Monitoring sarà condivisa, per la quota dei relativi servizi/applicazioni, con il Service Manager del MdS, in modo da garantire trasparenza sulle attività di monitoraggio. Oltre alla vista sintetica, lo strumento consente di visualizzare le componenti modellate a livello di servizio.

### **3.4.2 Modalità di predisposizione monitoraggio**

L'attività di predisposizione del monitoraggio dei servizi è un'attività che non si conclude con quanto previsto nel progetto di transizione per l'avvio del Servizio di Hosting evoluto. Il servizio di monitoraggio proposto dalla DCOD INAIL, attraverso la Service Control Room, prevede un *continuous improvement* ed aggiornamento delle catene tecnologiche, delle soglie, eventi e metriche oggetto di monitoraggio sulla base:

- delle evoluzioni funzionale delle applicazioni gestite
- sulla base dei dati raccolti dagli strumenti di monitoraggio. In particolare, la soluzione di monitoraggio prevede l'adeguamento dinamico delle soglie di monitoraggio sulla base dell'andamento storico rilevato.

Le attività di predisposizione del monitoraggio in fase di esercizio prevedono quindi:

- Aggiornamento da parte del Ministero della Salute delle informazioni di natura applicativa necessarie alla revisione del modello di monitoraggio;



- Analisi delle informazioni raccolte, definizione delle soglie ed eventi rilevanti, con il supporto del MdS, e definizione delle regole di correlazione degli eventi e metriche definite;
- Aggiornamento del modello di servizio, delle soglie e degli eventi rilevati sulla base di eventuali change sul servizio/applicazione e dall'analisi rilevata dai tool di monitoraggio.

La predisposizione del monitoraggio come descritto nei precedenti paragrafi è subordinata alla verifica, in fase di progettazione, delle caratteristiche tecniche delle componenti da monitorare.



#### **4 MODELLO OPERATIVO DEL SERVIZIO**

La fase di esercizio del servizio è basata su una continua e strutturata relazione con il MdS, nel rispetto dei processi DCOD INAIL e delle procedure operative che saranno definite e condivise durante la stesura del Piano di Subentro.

La fase di esercizio è incentrata su un modello di IT Service Management integrato, coerente con le *best practice* ITIL e che si basa sulla disponibilità di alcuni strumenti che la DCOD INAIL metterà a disposizione del MdS a supporto di specifici processi. In particolare:

- **Soluzione IT Service Management** a supporto dei processi di Gestione delle Richieste, Gestione degli Incidenti, Gestione dei Problemi, Gestione dei Change, con le modalità descritte nei paragrafi successivi;
- **Soluzione a supporto del processo di Gestione dei Rilasci.**

Con particolare riferimento alla soluzione ITSM si precisa che la stessa:

- Prevede, nella sua configurazione standard, la possibilità di gestire le interazioni previste con i referenti del MdS descritti nel modello di funzionamento, ed in particolar modo con il Service Manager del Ministero;
- Prevede un'integrazione via Web Service da e verso il sistema di TT utilizzato dal fornitore di servizi applicativi del MdS per gestire il trasferimento dei ticket tra gruppi applicativi del Ministero e gruppi infrastrutturali della DCOD INAIL nel rispetto dei processi di seguito descritti.

Nei paragrafi seguenti si riporta una descrizione sintetica delle interazioni DCOD INAIL e MdS relativamente ai seguenti processi:

- Modalità di attivazione/terminazione del servizio
- Processo di Gestione Richieste Servizio
- Processo di Gestione Incidenti
- Processo di Gestione Problemi
- Gestione dei Rilasci

##### **4.1 Modalità di attivazione/terminazione del servizio**

La DCOD INAIL si adegnerà alle indicazioni operative fornite dal MdS conformemente a quanto descritto nella documentazione tecnica ricevuta.

##### **4.2 Processo di Gestione Richieste di Servizio**

Il Service Manager del Ministero della Salute invia attraverso la soluzione di IT Service Management le richieste di servizio alla DCOD INAIL opportunamente catalogate e configurate nella fase di avvio e progettazione del servizio.



I ticket riguardano modifiche standard preautorizzate al servizio che vengono verificate ed approvate dal Service Manager DCOD INAIL per essere poi inoltrate ai gruppi operativi di II livello per la lavorazione. Alcuni esempi di richieste preautorizzate possono riguardare la modifica a soglie di monitoraggio applicative, l'attivazione di specifici monitoraggi (anche di natura temporanea) su specifiche transazioni applicative, richiesta di report specifici non previsti fra quelli periodici già previsti.

L'iter di evasione delle richieste prevede degli specifici stati di lavorazione la cui evoluzione viene visualizzata, dal Service Manager MdS, attraverso lo strumento di IT Service Management. È inoltre prevista la chiusura del ticket da parte del Service Manager MdS stesso una volta verificata l'effettiva evasione della richiesta inoltrata.

#### 4.3 Processo di Gestione degli Incidenti

Il processo di gestione degli incidenti è focalizzato sulla minimizzazione dei tempi di indisponibilità delle applicazioni gestite. Di seguito sono descritte, le modalità proposte di interazione fra DCOD INAIL ed il MdS, con riferimento a specifiche fattispecie:

- **Malfunzionamento di natura infrastrutturale rilevato dalla SCR:** gli operatori SCR che rilevano, attraverso la piattaforma di monitoraggio, un malfunzionamento/degrado sulle applicazioni e/o servizi del MdS, dovuto a componenti infrastrutturali, procedono con l'apertura di un ticket di incident che viene inoltrato e lavorato dai gruppi specialistici infrastrutturali della DCOD INAIL;
- **Malfunzionamento di natura applicativa rilevato dalla SCR:** gli operatori SCR che rilevano, attraverso la piattaforma di monitoraggio, un malfunzionamento/degrado sulle applicazioni e/o servizi del MdS, dovuto a componenti e problematiche applicative, procedono con l'apertura di un ticket di incident sulla soluzione di IT Service Management che viene inoltrato ai gruppi applicativi del MdS. Tale inoltro avviene attraverso l'integrazione con il sistema di Trouble Ticketing dal MdS. Il ticket rimane aperto fino alla chiusura da parte dei gruppi applicativi che lo hanno in gestione.
- **Major Incident rilevato dalla SCR:** qualora la Service Control Room dovesse rilevare un malfunzionamento di natura applicativa o infrastrutturale di tipo Major (indisponibilità o sensibile degrado su servizi critici o impattanti una popolazione rilevante di utenti) apre un incident ed attiva la procedura di escalation verso l'Incident Manager DCOD INAIL che è responsabile di:
  - dare tempestiva comunicazione al Service Manager DCOD INAIL, al Service Manager MdS;





- attivare se necessario dei team di risorse misti che gestiscano in modo rapido il ripristino della normale operatività del servizio/applicazione. L'Incident Manager può convocare anche risorse specialistiche applicative per il tramite del Service Manager del MdS;
- tenere aggiornati entrambi i Service Manager e di ogni evoluzione relativa al Major Incident gestito.
- **Malfunzionamenti applicativi segnalati dagli utenti del MdS e gestiti sul sistema di TT del MdS non rilevati dalla SCR:**
  - In caso di segnalazioni non risolvibili a livello applicativo o che richiedono un supporto di analisi infrastrutturale, i gruppi applicativi del MdS inoltrano il ticket, tramite l'integrazione tra gli strumenti di trouble ticketing, alla Service Control Room in modo che possa attivare i gruppi infrastrutturali competenti per le verifiche del caso;
  - In caso di potenziali major incident, i gruppi applicativi del MdS segnalano la problematica alla SCR tramite l'integrazione tra gli strumenti di trouble ticketing. Qualora la SCR dovesse constatare l'esistenza di un Major Incident attiva la procedura di escalation già descritta.

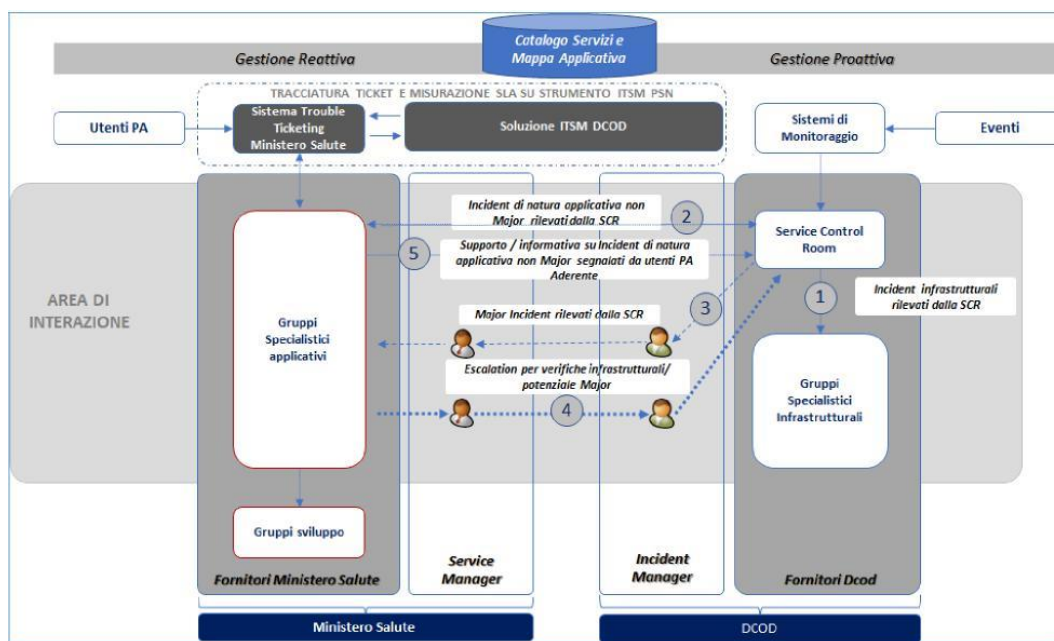


Figura 6 - Casistiche gestione Incidenti

#### 4.4 Processo di gestione dei Problemi

In caso di major incident gestiti con *workaround*, incident ripetuti nel tempo o reportistica ad hoc prodotta sui sistemi o sulle applicazioni, il Problem Manager DCOD INAIL è responsabile di:

- aprire un Problem tramite ticket sullo strumento di IT Service Management;



- informare e attivare il Service Manager DCOD INAIL e il Service Manager MdS;
- convocare e coordinare di concerto con il Service Manager di MdS un gruppo di analisi multidisciplinare (inclusivo di risorse DCOD INAIL e risorse MdS) necessario all'individuazione delle cause della problematica riscontrata;
- attribuire le azioni correttive individuate in fase di analisi al Service Manager DCOD INAIL e al Service Manager MdS, i quali sono responsabili di attivare, nell'ambito delle proprie esclusive aree di competenza, i gruppi specialistici (applicativi o infrastrutturali) che dovranno implementare le azioni definite
- verificare la soluzione applicata e chiudere il Problem.

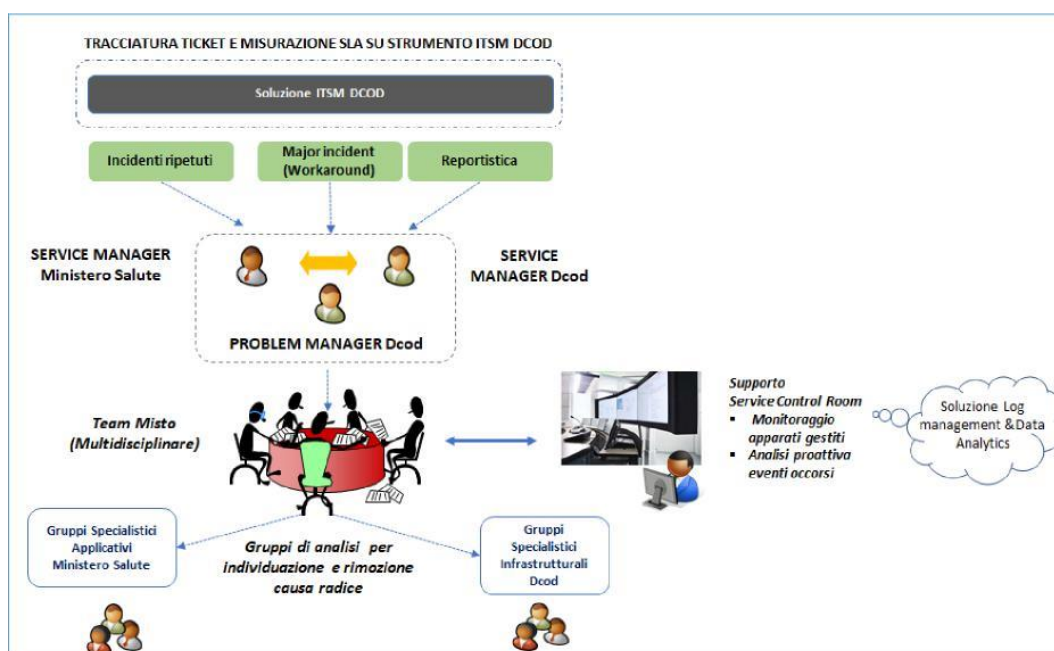


Figura 7 - Modello integrato di Problem Management

#### 4.5 Processo di gestione dei rilasci

Le richieste di rilascio di pacchetti applicativi nei vari ambienti devono essere gestite attraverso la soluzione messa a disposizione dalla DCOD INAIL. La gestione dei rilasci prevede una pianificazione degli stessi, condivisa fra il Release Manager del MdS ed il Release Manager della DCOD INAIL e gestita con il *tool Rational Team Concert (RTC)* con utenze di accesso messe a disposizione da DCOD Inail per MdS. Il processo di Gestione dei Rilasci è di seguito sinteticamente descritto:

- Il Release Manager del MdS:



- verifica la sussistenza dei report che attestano l'esecuzione dei test non funzionali (con relativo esito e soglie raggiunte) da parte del fornitore di sviluppo di MdS, e li consegna al Release Manager DCOD INAIL<sup>1</sup>;
  - fornisce tutti i dati necessari per il deploy e procede con la richiesta di deploy in ambiente di Collaudo.
- Il Release Manager DCOD INAIL, verificata la presenza delle informazioni necessarie al deploy, avvia le attività di deploy in ambiente di Collaudo;
  - Conclusa l'attività di deploy, il Release Manager MdS effettua le proprie verifiche nell'ambiente di Collaudo;
  - Concluse queste verifiche il Release Manager del MdS richiede il rilascio in ambiente di Pre-Produzione;
  - Conclusa l'attività di deploy, il Release Manager MdS effettua le proprie verifiche nell'ambiente di Pre-Produzione;
  - Concluse queste verifiche il Release Manager del MdS richiede il rilascio in ambiente di produzione;
  - Al termine del deploy in produzione il Release Manager MdS attesta la conclusione positiva del rilascio.

Qualora venisse attivato il servizio opzionale della "Certificazione del Software" il processo qui descritto dovrà essere rivisto.

---

<sup>1</sup> Il Release Manager del MdS può richiedere delle deroghe ai test non funzionali previa assunzione di rischio documentata.



## 5 REPORTISTICA SULL'ANDAMENTO DEL SERVIZIO

Al fine di fornire una vista aggiornata sull'andamento del servizio, la DCOD INAIL metterà a disposizione del MdS differenti tipologie di report il cui contenuto di dettaglio e la frequenza di elaborazione sarà definita nella fase di progettazione di dettaglio e darà oggetto di un *continuous improvement* nel corso di erogazione del servizio.

Oltre ai report periodici, che verranno di seguito sinteticamente descritti (elenco indicativo e non esaustivo), la DCOD INAIL si impegna a fornire, compatibilmente con le attività in corso e con la disponibilità dei dati, eventuale specifica reportistica su richiesta del Service Manager MdS.

### 5.1 Reportistica periodica di esercizio

Di seguito un primo e **non esaustivo** elenco di tipologie di report e relativa periodicità che la DCOD INAIL si impegna a fornire al Ministero della Salute:

- Report sulle performance e sulla difettosità delle applicazioni rilevate dagli strumenti di monitoraggio sulla base del traffico reale rilevato da appliance presenti nel *Data Center* DCOD INAIL. Periodicità mensile.

Esempi specifici di report riguardano:

- Andamento transazioni rispetto a soglie definite
- Tempo di risposta delle transazioni
- Altri da definire in fase di progettazione di dettaglio
- Report sulla numerosità e tipologia di ticket (Incident, Request, Change e Problem, Rilasci) gestiti sulle applicazioni del MdS, attraverso lo strumento di IT Service Management della DCOD INAIL. Tale reportistica distingue fra ticket infrastrutturali ed applicativi e consente ai Service Manager (DCOD INAIL e MdS) di avviare analisi di dettaglio per indirizzare azioni di miglioramento continuo sul servizio erogato. Si prevede una periodicità mensile.

Con particolare riferimento agli incidenti gestiti da DCOD INAIL, di seguito alcuni dettagli del report previsto:

- il numero di malfunzionamenti per tipologia rilevati nel mese;
- il numero di malfunzionamenti per tipologie chiusi nel mese;
- il dettaglio di ogni malfunzionamento chiuso nel mese, ed in particolare:
  - Id del malfunzionamento;
  - tipologia del malfunzionamento (preventivo /correttivo);
  - sistemi di elaborazione fisici/virtuali e applicazioni impattate;
  - data/ora di rilevazione;
  - data/ora di risoluzione del malfunzionamento (chiusura tecnica);



- data/ora di certificazione della risoluzione del malfunzionamento da parte del Fornitore (chiusura amministrativa);
- tutte le azioni effettuate dal Fornitore e dalle terze parti dalla rilevazione dell'Incidente fino alla sua completa risoluzione;
- necessità di aggiornamento Sistema di Gestione Configurazione (Si/No ed elenco item da aggiornare);
- data/ora di aggiornamento del Sistema di Gestione Configurazione (dettaglio di item aggiornato, autore aggiornamento, data/ora aggiornamento).

Ulteriori report di questa tipologia riguarderanno:

- Registro dei problemi
- Pianificazione dei rilasci
- Numero rilasci
- Report sui CI infrastrutturali a supporto dei servizi/applicazioni del MdS sulla base delle informazioni presenti nel CMDB DCOD INAIL. Si prevede una periodicità trimestrale.
- Ulteriori report che potranno essere definiti nel corso delle fasi di progettazione di dettaglio del servizio.