# Piano della Sicurezza TITULUS

## CINECA

Versione 1.4

**EMISSIONE DEL DOCUMENTO**

| Azione | Data | Nominativo | Funzione |
|---|---|---|---|
| *Redazione* | 04/10/2017 | Paola Silvia Tentoni | Resp. Sicurezza ICT CINECA |
| *Verifica* | 23/10/2017 | Angelo Neri | Direzione IT&DP |
| *Verifica* | 24/10/2017 | Massimiliano Valente | BU Università |
| *Approvazione* | 26/10/2017 | Riccardo Righi | BU Università |

| N°Ver/Rev/ Bozza | Data emissione | Modifiche apportate | Osservazioni | Distribuito a |
|---|---|---|---|---|
| 1 Bozza | 04/10/2017 | Prima stesura | | |
| 2 Bozza | 16/10/2017 | Prima revisione | | |
| 3 Bozza | 23/10/2017 | Seconda revisione | | |
| 4 Finale | 26/10/2017 | Revisione finale | | |
| | | | | |
| | | | | |

**INFORMAZIONI SULLA CLASSIFICAZIONE DEL DOCUMENTO**

| Livello di classificazione | | Data di classificazione o di modifica alla classificazione iniziale | Responsabile della classificazione del documento | Destinatari del documento |
|---|---|---|---|---|
| **Riservato** | | | | |
| **Ad uso interno** | | | | |
| **Di dominio pubblico** | **X** | **04/10/2017** | **P. Tentoni** | **Atenei** |

# Indice del documento



# 1 PREMESSA, RIFERIMENTI ED ALLEGATI

Il presente Piano della Sicurezza (PdS) descrive l'implementazione della sicurezza delle informazioni riferita al contesto del prodotto TITULUS nel caso in cui questo sia in Hosting presso CINECA.

Il PdS fa riferimento a documenti e procedure che sono utilizzate all'interno della organizzazione stessa, ovvero agli aspetti della norma ISO/IEC 27001:2013, la cui certificazione è relativa ad ambiti specifici quali CONSERVA o l'infrastruttura di Hosting. TITULUS è fuori dallo scope della ISO 27001, tuttavia, come altri servizi CINECA, beneficia di una serie di procedure trasversali che si applicano quindi indirettamente anche a molti aspetti di erogazione del servizio TITULUS. Si considerano inoltre gli aspetti contemplati nella norma ISO 9001:2015, oltre che ad altre eventuali norme e/o dispositivi legislativi.

# 2 TERMINOLOGIA (GLOSSARIO, ACRONIMI)

| **Glossario dei termini - definizioni** | |
|---|---|
| ***Sistema*** | Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione. |
| ***Disponibilità richiesta*** | Tempo in cui il sistema deve essere utilizzabile in conformità alle funzionalità previste, esclusi i tempi programmati per la manutenzione, rispetto alle ore concordate per l'esercizio. |
| ***Periodo criticità servizio*** | Data/periodo in cui il dato o il servizio deve essere tassativamente erogato per esigenze specifiche del business, quali scadenze o presentazione dei dati. |
| ***Tempo ripristino richiesto (Recovery Time Objective)- RTO*** | Tempo entro il quale un processo informatico ovvero il Sistema Informativo primario deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili. |
| ***Obiettivo temporale di recupero (Recovery Point Objective) - RPO*** | Indica la perdita dati tollerata: rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di un evento imprevisto. |

| **Acronimi** | |
|---|---|
| ***CERT*** | Computer Emergency Response Team |
| ***DPO*** | Data Protection Officer |
| ***PdS*** | Piano della Sicurezza |
| ***SGQ*** | Sistema di Gestione della Qualità |
| ***SGSI*** | Sistema di Gestione della Sicurezza dell'Informazione |
| ***IT&DP*** | Infrastruttura Tecnologica & Delivery Produzione (UOR CINECA per la gestione ICT) |
| ***CoRiMa*** | Compliance e Risk Management (UOR CINECA che si occupa della Compliance normativa e Gestione rischio ICT) |

# 3 NORMATIVA DI RIFERIMENTO

Riportiamo le seguenti normative di riferimento per il servizio in oggetto:

- Misure minime di sicurezza ICT per le PA (Circolare n. 1/2017 del 17/3/2017).
- Regolamento europeo in materia di protezione dei dati personali (GDPR) 2016/679.

# 4 ORGANIZZAZIONE DEL SISTEMA

## 4.1 Ruoli e responsabilità della sicurezza informatica

CINECA ha istituito da alcuni anni un responsabile della sicurezza ICT (Area Security) e del CERT (Computer Emergency Response Team), ovvero l'organo che raccoglie le segnalazioni inerenti la sicurezza da qualunque fonte esse provengano, sovrintende la reazione o risposta sia essa preventiva o reattiva, attivando i team operativi per il trattamento della segnalazione e controllando l'attuazione nei tempi compatibili con la tipologia e gravità della stessa.

Il responsabile coordina l'Area Security, unità organizzativa che svolge attività di controllo continuo e miglioramento delle policy di sicurezza dei sistemi in genere, in particolare:

- a livello di service design, lo staff può/deve essere coinvolto per una preliminare impostazione del servizio in fase di progetto, secondo canoni che garantiscano la sicurezza dello stesso
- effettua i test di vulnerabilità richiesti dai responsabili dei servizi, in fase di deploy iniziale o anche successivamente ad ogni modifica significativa
- propone modifiche alle policy di sicurezza al fine di migliorare la sicurezza delle informazioni
- segnala l'uscita di bollettini su vulnerabilità particolarmente critiche riguardanti software di base o applicativo, indicando azioni tempestive di correzioni o workaround, in anticipo rispetto alla manutenzione ordinaria, per una reazione immediata e a protezione preventiva degli asset
- intraprende campagne di consapevolezza rivolte ai dipendenti per cercare di elevare il livello di attenzione da parte di tutti, soprattutto del personale non tecnico, sulle tematiche del phishing, delle mail malevole, del furto di credenziali e dell'utilizzo di credenziali forti
- risponde agli incidenti di sicurezza IT, in cooperazione con gli altri membri CERT, analizzando le cause , proponendo soluzioni per il ripristino del servizio in sicurezza.

Il CERT ha esclusivamente funzioni di segnalazione e controllo, non è un team operativo, ma si avvale del contributo del personale addetto alla gestione delle Operazioni, sia per la risposta ad incidenti sia soprattutto per la fase di prevenzione. Nel caso in cui si ravvedano vulnerabilità sul codice applicativo sviluppato da CINECA, vengono notificati i gruppi di sviluppo e relativi product owner per pianificare il corretto trattamento del rischio, qualunque azione questo comporti (trattamento, accettazione, trasferimento).

## 4.2 Ruoli e responsabilità della protezione dei dati

Il ruolo del ***Data Protection Officer*** (DPO) è una figura prevista dall'art. 37 del **G**eneral **D**ata **P**rotection **R**egulation (GDPR) ovvero il nuovo Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il nuovo regolamento fornisce un quadro di riferimento normativo moderno basta sul principio della responsabilità (accountability) per la protezione dei dati in personali.
La figura del Data Protection Officer rappresenta il fulcro di tale nuovo quadro normativo e deve agire da facilitatore al rispetto delle previsioni del GDPR anche tramite lo svolgimento di valutazioni di impatto sui dati personali e attività di audit.
Si precisa che il DPO non è responsabile in caso di non conformità con il GDPR.
La responsabilità della protezione dei dati resta infatti in capo al Titolare o Responsabile.

L'art. 38 del GDPR (General Data Protection Regulation) definisce la posizione del DPO il quale deve essere

tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
Gli "*interessati* " possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti previsti nel GDPR.
Il DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
I compiti del DPO, elencati nell'art. 30 del GDP, sono i seguenti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il DPO deve considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Al fine di stimolare l'effettivo coinvolgimento del DPO nei processi operativi aziendali si è inserito il ruolo del DPO all'interno della procedura "*PGS03 Gestione dei rischi nei progetti*" al fine di stimolare la consultazione del DPO nel caso di progetti che comportano il trattamento di dati personali e sensibili.

## 4.3 Gestione della Continuità operativa

L'operatività IT dipende dal funzionamento contemporaneo ed integrato di molteplici e distinti sottosistemi impiantistici. Il metodo di classificazione scelto da Cineca come riferimento è quello dell'Uptime Institute che pur non avendo l'ufficialità di una norma, definisce dei principi prestazionali generici applicabili a qualsiasi sistema o sottosistema che impatti sulla continuità operativa IT.

I sistemi di Tier Classification codificano la resilienza della infrastruttura impiantistica che supporta il funzionamento di un Data Center e delle relative applicazioni elaborative, e misurano la capacità dell'infrastruttura di agevolare la continuità di servizio dei sistemi IT.

L'infrastruttura a supporto della continuità operativa di Cineca (sede di Bologna, sito di produzione per il Sistema TITULUS) soddisfa i requisiti richiesti dalla classificazione TIER III, è dotata quindi, di componenti ridondati e di percorsi distributivi di alimentazione multipli e indipendenti. Qualsiasi componente e qualsiasi porzione di impianto, nella catena distributiva, può essere rimosso o posto fuori servizio (previa pianificazione dell'intervento) senza impattare sull'operatività del sito. C'è sufficiente potenza per sostenere l'operatività del sito anche quando, qualsiasi componente o porzione di impianto, nella catena distributiva, viene rimosso o posto fuori servizio. Ne consegue che tutte le attività di manutenzione possono avere luogo senza ripercussioni sui sistemi IT. Per questo motivo Cineca è "Manutenibile in Continuità Operativa" e, per lo stesso motivo, non vengono previsti per essa shutdown annuali per

manutenzione periodica.
Dal punto di vista delle infrastrutture tecnologiche la ridondanza è stata curata per garantire la modalità fault tolerant a ciascun livello:

- Networking
  - Carrier multipli per la connettività geografica
  - Apparati ridondati
  - Cablaggi ridondati
- Storage
  - Apparati ridondati
  - Uso estensivo di tecniche RAID (1,5,6,10) per la protezione dei dati
- Server
  - Tutti i sistemi dispongono di componenti HW ridondate (alimentazioni, schede di rete, schede FC, dischi ecc).
  - Uso estensivo di high availability cluster e server farm
- Monitoraggio dei servizi e dei sistemi
  - Sistema di monitoraggio con >10.000 servizi monitorati 7x24x365.

Per consentire la continuità operativa, la salvaguardia e il mantenimento dei dati, Cineca dispone inoltre di una significativa infrastruttura per il backup centralizzato e archiviazione dei dati e delle applicazioni. Attualmente vengono utilizzate i tipi di soluzioni qui elencate:

- Commvault: principalmente per il backup dei sistemi fisici, macchine virtuali e filesystem condivisi, per gestire le archiviazioni a lunga durata.
- NetApp Snaphot e SnapVault: per il backup dei database e per alcune tipologie di filesystem condivisi erogati da sistemi NetApp.

L'affidabilità dei backup viene verificata mediante l'ausilio di sistemi automatici che controllano quotidianamente la corretta esecuzione dei backup dei server, via mail. Quanto alla diversa localizzazione dei supporti di backup rispetto alla sorgente dei dati, la remotizzazione della copia degli stessi sul sito di DataDR soddisfa intrinsecamente il requisito.
Esiste inoltre un programma di verifica periodica dei restore, a campione viene effettuato un test su un intero sistema TITULUS restored.
Sulla infrastruttura di facility sono definite le misure di sicurezza che impongono la ridondanza citata in precedenza, il monitoraggio costante con gestione delle anomalie, (incidenti o carico inatteso), che prevede reperibilità e tempi di intervento stabiliti, sistemi centralizzati per il monitoraggio e la telesorveglianza di pronto intervento.
Sono inoltre eseguite le seguenti operazioni di manutenzione e verifiche di funzionalità anche predittive:

- Avvio settimanale di prova senza carico dei sistemi di generazione energia elettrica di emergenza (motogeneratori).
- Avvio annuale di prova con carico dei sistemi di generazione energia elettrica di emergenza
- Verifica visiva dei sistemi tecnologici
- Analisi annuale termografica dei sistemi tecnologici
- Manutenzioni ordinarie .

La frequenza e la natura degli interventi di manutenzione viene generalmente indicata:

1. da prescrizioni di legge
2. dal libro macchina contenente le istruzioni di manutenzione
3. dalla segnalazione di malfunzionamenti.

Il monitoraggio continuo della temperatura ed umidità delle sale tecniche, al fine di garantire il rispetto delle soglie stabilite ed una pronta reazione in caso di allarme, è supportato dai seguenti dispositivi di monitoraggio e misurazione:

- sonde posizionate in sala macchina per rilevazione temperatura ed umidità
- monitoraggio e allarmistica del sistema di condizionamento delle sale tecniche mediante specifico software (BMS).
- Monitoraggio e allarmistica dei sistemi a supporto della continuità Cineca mediante specifico software (BMS) e monitoraggio remoto da parte di ditta incaricata.

L'affidabilità delle sonde viene verificata almeno annualmente a cura del fornitore nell'ambito del contratto di assistenza.
Il fornitore è tenuto a rilasciare ai tecnici del gruppo "Servizi Generali e Tecnici" un report di intervento che deve riportare le sonde verificate, lo strumento utilizzato per la verifica, i risultati della verifica e gli eventuali interventi effettuati.

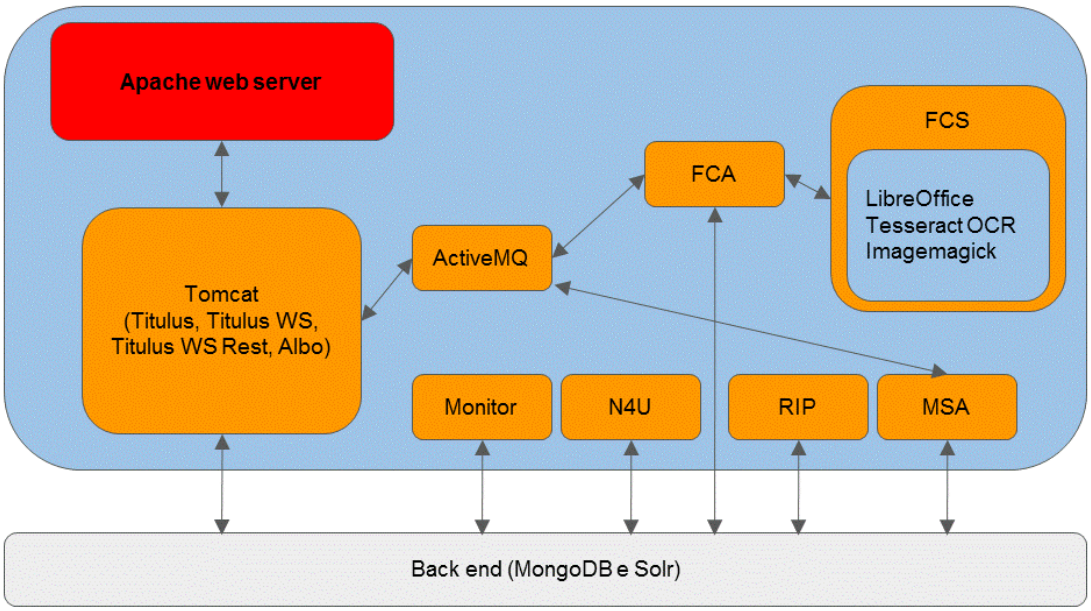
# 5 PERIMETRO DEL SISTEMA

La localizzazione del sito primario in cui è esercito il servizio TITULUS è presso CINECA sede Via Magnanelli 6/3, Casalecchio di Reno (BO) – CAP 40033.

## 5.1 Componenti fisiche

L' architettura del sistema presenta 2 ambienti coesistenti (ambiente di produzione e ambiente di pre-produzione) inseriti in due server distinti:

- Server di Frontend
- Server di Backend



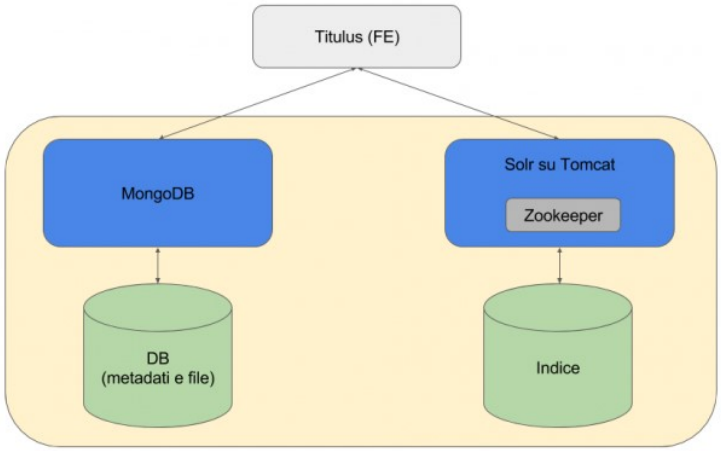



*Figura 1 - Architettura ambienti di Frontend e di Backend di produzione TITULUS*

Le componenti sono tutte virtualizzate. Tutti i cluster VMWare che ospitano le macchine virtuali sono composti da più nodi fisici, in configurazione di HA (High Availability) e DRS (Distributed Resource Scheduler).
Nello specifico i servizi di produzione del sistema TITULUS sono attualmente così configurati:

- frontend (business logic layer): un server, visibile da rete pubblica, con Apache e Tomcat Application Server.
- Sistema di backend (database e index layer): visibile solo da rete privata, Tomcat Application Server, Database MongoDB e SOLR. L'alta affidabilità è garantita dall'HA del cluster vmware.
- Sistema di autenticazione, normalmente in carico al cliente.

Per i servizi di PRE-PRODUZIONE (collaudo), l'architettura è simile e compresente alla produzione.

## 5.2 Piani di manutenzione delle infrastrutture

Sono presenti piani di manutenzione di tutti gli apparati fisici:

- Apparati di rete (LB, CORE, Distribution, Access): sono attivi contratti di manutenzione (smartnet) per tutti gli apparati fisici coinvolti, rinnovati annualmente.
- Storage (produzione + DataDR): sono attivi contratti di manutenzione rinnovati annualmente.
- Virtualizzazione: sono attivi contratti di manutenzione per tutti gli hardware coinvolti.

Sono in corso di finalizzazione processi atti a garantire l'aggiornamento automatico dei server esposti, in finestra off-peak, per tutto il software relativo al sistema operativo e pacchetti ad esso collegati, per garantire il rispetto delle misure minime e la riduzione dell'esposizione a vulnerabilità, mitigando il rischio di data breach. Tali aggiornamenti settimanali implicano un breve disservizio legato alla riattivazione dei servizi.

## 5.3 Servizi tecnici ed impianti

Rientrano in questa sezione tutte quelle apparecchiature tecniche presenti all'interno del CED e necessarie per garantire il corretto funzionamento degli apparati.

Sono presenti piani di manutenzione di tutti gli apparati a supporto della continuità operativa del Cineca in particolare:

- Sistema di Condizionamento di precisione.
- Sistema di continuità (UPS): sono attivi contratti di manutenzione orinaria e predittiva con monitoraggio remoto da parte del fornitore del tipo 24hx365gg e supervisione con software dedicato (BMS) che consente di intervenire in maniera preventiva in caso di malfunzionamenti.
- Quadri e impianto Elettrico.
- Allarmistica antincendio, antiallagamento.
- Controllo accessi (sorveglianza, accesso badge, sensori antiintrusione).

### 5.3.1 Impianto di anti intrusione e verifica accessi fisici

Dal punto di vista tecnologico, Cineca è protetto da un sistema integrato di sicurezza e controllo accessi di cui i vari sottosistemi interagiscono tra loro e con gli operatori secondo relazioni programmate. Un unico centro di elaborazione ha il compito di supervisionare l'attività del sistema, condizionandone le funzionalità a seconda delle programmazioni e delle scelte immesse nella configurazione. Gli impianti sono regolarmente mantenuti in efficienza da ditta specializzata nel rispetto delle normative del settore. L'architettura del sistema comprende:

- Sottosistema antintrusione: Fanno parte di questo tutti i sensori e segnalatori dedicati alla rivelazione antintrusione ed alla gestione locale delle zone di protezione
- Sottosistema controllo accessi: il sottosistema è costituito da lettori di badge di prossimità che controllano l'accesso alle sale macchine ed altre aree critiche e sensibili.
- Sottosistema di videosorveglianza: è costituito da un sistema misto analogico/digitale. I dispositivi in campo sono dislocati a copertura dell'intero perimetro esterno e degli accessi nonché delle sale macchine e tecnologiche.

Il controllo degli accessi di Cineca è garantito per 365 l'anno da personale interno (turno diurno feriale) ed esterno (Istituto di vigilanza - turno notturno feriale, h24 sabato e festivi). Gli addetti al servizio di reception provvedono al riconoscimento del personale e dei visitatori registrandone le generalità e rilasciando a questi ultimi i permessi di accesso nel rispetto delle procedure stabilite.
Cineca è protetto da una recinzione metallica perimetrale con accesso principale, per dipendenti e visitatori, collocato sulla via Magnanelli. Sono presenti altri varchi dedicati all'ingresso per il solo personale dipendente e per il carico/scarico delle merci. L'accesso ai varchi è controllato dal personale di presidio o tramite card personale per l'apertura degli stessi.
Le aree cosiddette "ad accesso pubblico" (uffici e zone comuni) sono separate fisicamente dai laboratori, sale macchine e tecnologiche le quali sono caratterizzate da un accesso controllato tramite badge di prossimità.

### 5.3.2 Impianto di alimentazione elettrica e di emergenza (Sistemi UPS)

Cineca è dotato di un "sistema" di alimentazione elettrica efficiente ed affidabile, che consente al centro di poter essere alimentato sia da rete pubblica che di poter funzionare in isola, a fronte di mancanza di erogazione da parte del gestore.
L'alimentazione primaria è fornita dalla rete pubblica in MT a 15kW ed è derivata dalla struttura ad anello dell'area industriale di Casalecchio di Reno.
In caso di interruzione della fornitura elettrica sono presenti anche 3 motogeneratori diesel da 1.75MVA

dimensionati in modo da supportare tutti i carichi critici, collegati ad adeguati serbatoi di gasolio, che consentono al Consorzio di funzionare in isola per tutto il tempo necessario agli eventuali ripristini.
L'infrastruttura a supporto della continuità operativa di Cineca (sede di Bologna) è "Manutenibile in Continuità Operativa" e non vengono previsti per essa shutdown annuali per manutenzione periodica ma solo prove di carico per la verifica del corretto funzionamento e la manutenzione ordinaria degli apparati e delle attrezzature. L'infrastruttura impiantistica di supporto all'operatività IT della sede di Bologna ottempera in modo sostanziale alle prescrizioni di classificazione Uptime Institute Tier III per un carico IT di 1.200kW.
Tutti gli UPS sono monitorati 24 h/giorno e 365 gg/anno tramite un servizio remoto di controllo, che consente di intervenire in maniera preventiva in caso di malfunzionamenti.

### 5.3.3 Impianto di condizionamento

Tutte le sale macchine sono dotate di sistema di condizionamento di precisione del tipo sia ad espansione diretta sia ad acqua con mandata sotto il pavimento flottante e ripresa dall'alto.
La temperatura interna delle sale viene mantenuta tra i 23C° e i 28C° a seconda dei sistemi e viene regolata anche l'umidità interna.
Il sistema di condizionamento, in configurazione ridondante è fornito senza interruzione per 24 h/giorno e 365 gg/anno ed è gestito da un sistema di controllo e verifica che permette - per le aree adibite a sale macchine - di garantire il livello servizio per il 99.9% del tempo su base annua.

### 5.3.4 Impianto antincendio

La protezione antincendio di Cineca è garantita dal sottosistema dedicato (meccanico ed elettronico) le cui caratteristiche vengono di sotto riportate.

- Rete di idranti
- Parco estintori portatili a polvere. Nei locali tecnologici e sale macchine sono utilizzati esclusivamente estintori a base Anidride Carbonica
- Impianto automatico di spegnimento a gas Argon IG01a protezione delle sale macchine e sale tecnologiche.
- Sottosistema di rivelazione automatica di incendio e allarme totalmente gestito dalle centrali analogiche indirizzate.

Tutti gli ambienti del complesso, compresi uffici, sale riunioni, disimpegni, magazzini, sale macchine e tecnologiche, sono monitorate dal sistema di rivelazione incendi.
Completa il sistema di sicurezza l'implementazione di misure antiallagamento sia fisiche che elettroniche di rivelazione. Per contrastare i rischi di alluvione è stata realizzata la recinzione perimetrale.
La manutenzione di tutti gli impianti è regolamentata dalla legge e dalle normative tecniche in vigore e la stessa è affidata a ditte specializzate regolarmente contrattualizzate.

### 5.3.5 Impianti di rete locale

L'architettura della rete Cineca ispirata alle Best Current Practice di networking è caratterizzata da:

- architettura multilivello (internet access, core, aggregation, access), in particolare con l'introduzione di un livello core ad altissime prestazioni, che funga da centro stella su cui attestare l'infrastruttura
- architettura suddivisa in vari tier funzionali (front-end, back-end, out-of-band management)
- virtualizzazione dell'infrastruttura nella dimensione dei diversi domini di indirizzamento/routing e dei diversi tier funzionali, mediante la creazione di opportuni ambiti VRF (Virtual Router

Forwarding)

- utilizzo di apparati in alta affidabilità ed elevate prestazioni allo scopo di conseguire:
  - una maggiore affidabilità e gestibilità, in particolare adottando apparati ridondati, con elevati MTBF (Mean Time Before Fault), senza SPF (Single Point of Failure),
  - una maggiore scalabilità (incremento porte accesso, incremento capacità di accesso, incremento capacità di distribuzione, incremento moduli di distribuzione)
- tecnologia di interconnessione a 10 Gbps fra i vari layer architetturali
- apparati di fascia alta, in grado di supportare in hardware feature tipo multicast, QoS, traffic engineering e shaping, fitraggio del traffico (ACL).

L'infrastruttura è scalabile, può crescere in modo naturale con l'aggiunta di elementi di distribution e access secondo le necessità.

# 5.4 Sistemi di sicurezza logica

L'accesso alle risorse delle web application del Sistema TITULUS è soggetto ad un processo di autenticazione. Il sistema di autenticazione non è un componente inglobato nella architettura applicativa di TITULS in quanto scelto e fornito direttamente dal cliente. Il sistema di autenticazione del cliente viene innescato da una appropriata configurazione di Apache da effettuare in fase di avviamento del sistema. Quando il cliente non manifesta la necessità di utilizzare un proprio sistema di autenticazione verrà sempre abilitata l'autenticazione locale di Tomcat.
La comunicazione tra client e server avviene solo tramite protocollo cifrato SSL.

# 5.5 Continuità Operativa

## 5.5.1 Continuità operativa

La continuità operativa nel contesto ICT è la capacità di una organizzazione di adottare - per ciascun processo critico e per ciascun servizio istituzionale critico erogato in modalità ICT, attraverso accorgimenti, procedure e soluzioni tecnico-organizzative - misure di reazione e contenimento ad eventi imprevisti che possono compromettere, anche parzialmente, all'interno o all'esterno dell'organizzazione, il normale funzionamento dei servizi e delle funzioni istituzionali.
Le procedure di backup comprendono le seguenti modalità, frequenze e ritenzioni:

**Backup standard:**

| Funzione | Nome | Modalità | Ritenzione | Freq. |
|---|---|---|---|---|
| **Presentation** | TITULUS Frontend | CommVault | 30 | 1/g |
| **Business Logic** | TITULUS Backend DB | CommVault | 30 | 1/g |

Dal punto di vista delle tempistiche di ripristino da backup, esse dipendono fortemente dalla dimensione delle VM e quindi non è possibile indicare un dato che abbia validità generale anche se, trattandosi di immagini presenti su storage, e non di nastri, la tecnologia attuale garantisce comunque una velocità sicuramente accettabile per tutte le situazioni (ordine di grandezza medio di "qualche ora", inferiore alla giornata). Il ripristino può essere effettuato anche con l'utilizzo della copia di Roma, con qualche ritardo rispetto al precedente, legato alle inferiori prestazioni della rete geografica.

**Data Disaster Recovery:**

Il software di backup si occupa di sincronizzare dati e sistemi operativi tra le infrastrutture di Bologna e una infrastruttura appositamente realizzata per il DataDR, in colocation temporanea presso Unidata a Roma. Tale sede di colocation è connessa con percorsi ridondati 10Gbps alla sede CINECA Roma, e con un link in fibra 8Gbps, risultando a tutti gli effetti un'estensione del Datacenter CINECA Roma.

| Funzione | Nome | Modalità | Ritenzione | Freq. |
|---|---|---|---|---|
| Copie remote delle VM | DataDR | CommVault | 15 | 1/g |

E' incluso quindi nell'hosting il DataDR delle VM costituenti il servizio, in altre parole è garantita la conservazione dei contenuti e la potenziale riattivazione del servizio, ma, in questo caso, non è possibile indicare un tempo di Recovery Operativo (RTO), garanzia che può essere associata solo ad un contratto di Disaster Recovery, disponibile con contrattazione separata.

### 5.5.2 Ridondanza geografica

Il Consorzio dispone di 3 sedi geograficamente distanti: Segrate (MI), Casalecchio di Reno (BO), Roma. Pertanto, in caso di inagibilità della sede primaria di Casalecchio, saranno sempre disponibili uffici e personale tecnico sistemistico di pronto intervento sia presso Roma (sede secondaria), sia presso gli uffici di Milano, in grado di ospitare eventualmente colleghi privi di ufficio, o di agire in loro vece, qualora si rendesse necessario.
Dal punto di vista dei sistemi, il sito di DataDR dispone della stessa tecnologia in uso presso il sito primario, secondo un opportuno fattore di scala. Anche nel sito secondario sono rispettati tutti gli accorgimenti di alta affidabilità e ridondanza delle componenti coinvolte.

### 5.5.3 Infrastruttura di rete (geografica e locale)

Riguardo alla parte di connettività di rete geografica per la connessione al sito secondario si ha:

- 1 link dedicato GARR a 10Gbps per la replica dei dati via snapmirror da Bologna a Roma.
- due Load Balancer per il bilanciamento di carico verso le farm,
- una parte di connettività internet verso rete GARR e rete Commercial.

E' presente inoltre un accordo con GARR e il provider Commercial (Fastweb, Unidata) per annunciare le reti pubbliche Cineca della sede di Casalecchio di Reno dalla sede di Roma, in caso di disastro.
L'annuncio diventa operativo grazie a una serie di script che riconfigurano automaticamente gli apparati di rete presso Roma.

# 6 MONITORAGGIO E CONTROLLI

Descrizione delle procedure di monitoraggio e di controllo del funzionamento del sistema.

## 6.1 Procedure di monitoraggio

Tutta l'infrastruttura tecnologica e applicativa è mantenuta sotto controllo dal sistema di monitoraggio Tutta l'infrastruttura tecnologica e applicativa è mantenuta sotto controllo dal sistema di monitoraggio continuo (365/24/7) che consente di misurare lo stato della stessa e dei servizi in ogni momento.

In caso di anomalie rilevate, il sistema allerta i gruppi di gestione infrastrutturale ed applicativa per la

gestione degli incidenti o per intervenire in modo proattivo per evitare l'occorrenza di situazioni che possano creare discontinuità del servizio.
Il monitoraggio consente di misurare lo stato e le metriche di funzionamento della maggior parte dei sistemi applicativi, ed in grado di dialogare secondo i protocolli più diffusi delle applicazioni quali ad esempio http, https, pop3/s, imap/s, smtp, snmp, ed in grado di intercettare le metriche di funzionamento quali CPU, uso della memoria, della rete, I/O, disco, stato complessivo del sistema operativo, raggiungibilità IP, icmp ecc… di ogni sistema e/o servizio applicativo. In particolare consente:

- la rilevazione degli incidenti
- il monitoraggio del funzionamento dei servizi e delle risorse relative ai "livelli funzionali"
- di avere un servizio di allerta basato su una vasta gamma di parametri e di soglie di allerta configurabili
- di avere uno strumento per misurare il rispetto dei livelli di servizio
- di codificare le procedure di reazione agli alert che rappresentano criticità sui "livelli funzionali" o sui servizi
- evitare falsi allarmi su oggetti che non sono realmente down ma sembrano tali a causa del malfunzionamento di un altro oggetto,
- l'analisi proattiva degli indicatori di performance

Ogni anomalia rilevata viene gestita secondo i processi di event, incident, problem management secondo le procedure che si ispirano alle linee guida ITILv3.