CCR

Riunione Plenaria DSI – Milano
3/12/2024

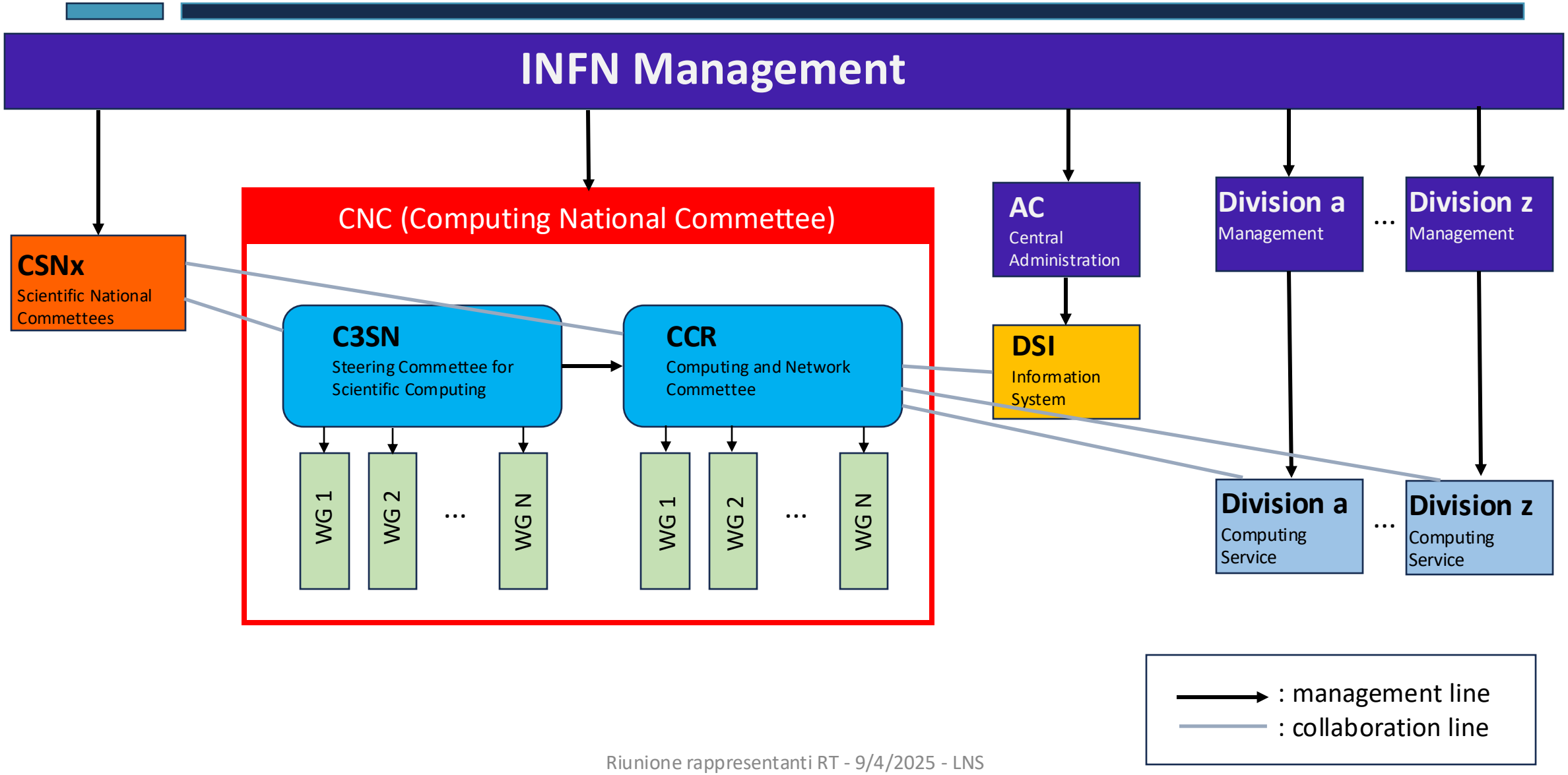
Alessandro Brunengo

Indice

- Organizzazione della CCR
- Infrastruttura di BC/DR
- Sicurezza informatica
- AAI
- Servizi nazionali
- Piattaforme sofwtare
- ChatGPT (AI?)

- Organizzazione della CCR
- Infrastruttura di BC/DR
- Sicurezza informatica
- AAI
- Servizi nazionali
- Piattaforme sofwtare
- ChatGPT (AI?)

Organizzazione del calcolo nell'INFN



La composizione della CCR

La CCR e' costituita da:

- il Presidente della Commissione
- i rappresentanti delle strutture: 20 sezioni, 4 laboratori, 3 centri
- il rappresentante del Tier1
- il rappresentante dei Tier2
- il license manager
- il responsabile della infrastruttura dei SSNN
- il responsabile della sicurezza informatica
- il direttore della DSI

a cui si aggiungono (ospiti permanenti):

- il Presidente del C3SN (Carlino)
- la segreteria (Chiaratti, Ubaldini)

Membro di Giunta di riferimento: Diego Bettoni

Il mandato della CCR

- Definire e armonizzare le attività dei Servizi Calcolo locali
- Mantenere ed evolvere l'infrastruttura di rete nazionale e i rapporti tecnologici con il GARR
- Mantenere ed evolvere l'infrastruttura di Business Continuity e Disaster Recovery per i servizi centrali dell'Istituto
- Sviluppare e mantenere l'infrastruttura di Autenticazione e Autorizzazione (AAI) dell'Istituto, i sistemi di mailing, i servizi multimediali i servizi web, gli strumenti collaborativi in uso nell'Istituto
- Gestire la sicurezza informatica dell'Istituto, di concerto col Responsabile per la Transizione Digitale
- Acquisire e gestire i software commerciali in uso nell'Istituto
- Supportare la Direzione Sistemi Informativi dell'Amministrazione Centrale
- Gestire la formazione, la divulgazione e la promozione delle competenze dell'INFN nelle proprie aree di competenza.

I gruppi di lavoro della CCR

- Asset strategici
  - AAI, Netgroup, NUCS (Security), Software, Infrastruttura BC/DR, OKD
- Gestione servizi nazionali e coordinamento servizi locali
  - SSNN CNAF, SSNN LNF, AFS, Mailing, Multimedia, Video, Ticketing, Web services, Windows
- Attivita' di R&D e task specifici
  - ASW, Condor, Hepix, Linux
- Conformita' a norme e regolamenti
  - Harmony
- Formazione

Referee

Gruppi di referaggio, per area tematica

- Server e Storage (sedi, infrastruttura SSNN)
- Rete (sedi, infrastruttura SSNN, linee dati, manutenzioni)
- Richieste infrastrutturali (sedi)
- Progetti CCR (gruppi di lavoro)
- Software
- Formazione (valutazione proposte da inoltrare alla CNF)

- Organizzazione della CCR
- Infrastruttura di BC/DR
- Sicurezza informatica
- AAI
- Servizi nazionali
- Piattaforme sofwtare
- ChatGPT (AI?)

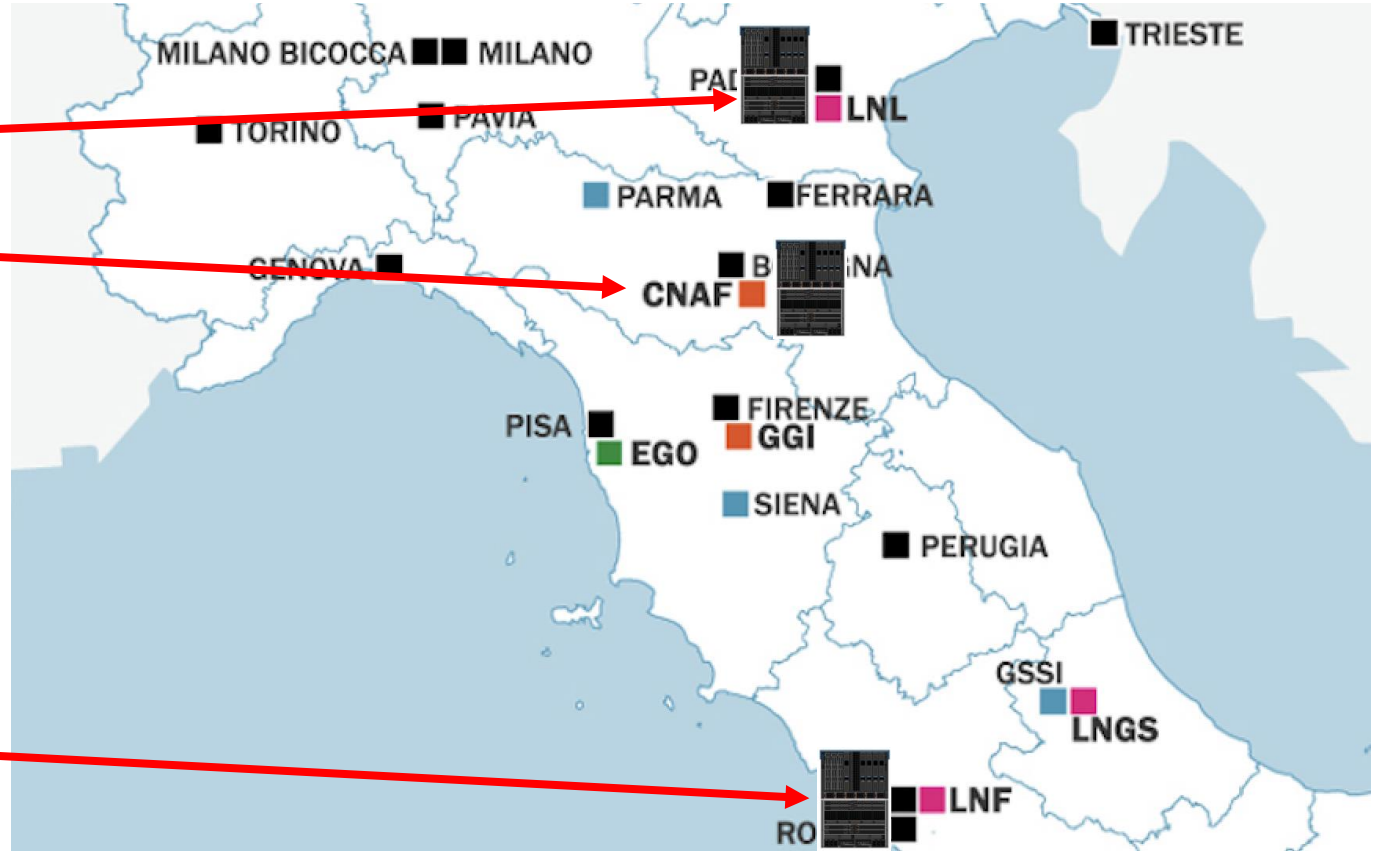
Infrastruttura di BC e DR

Business Continuity

site 2 (LNL)

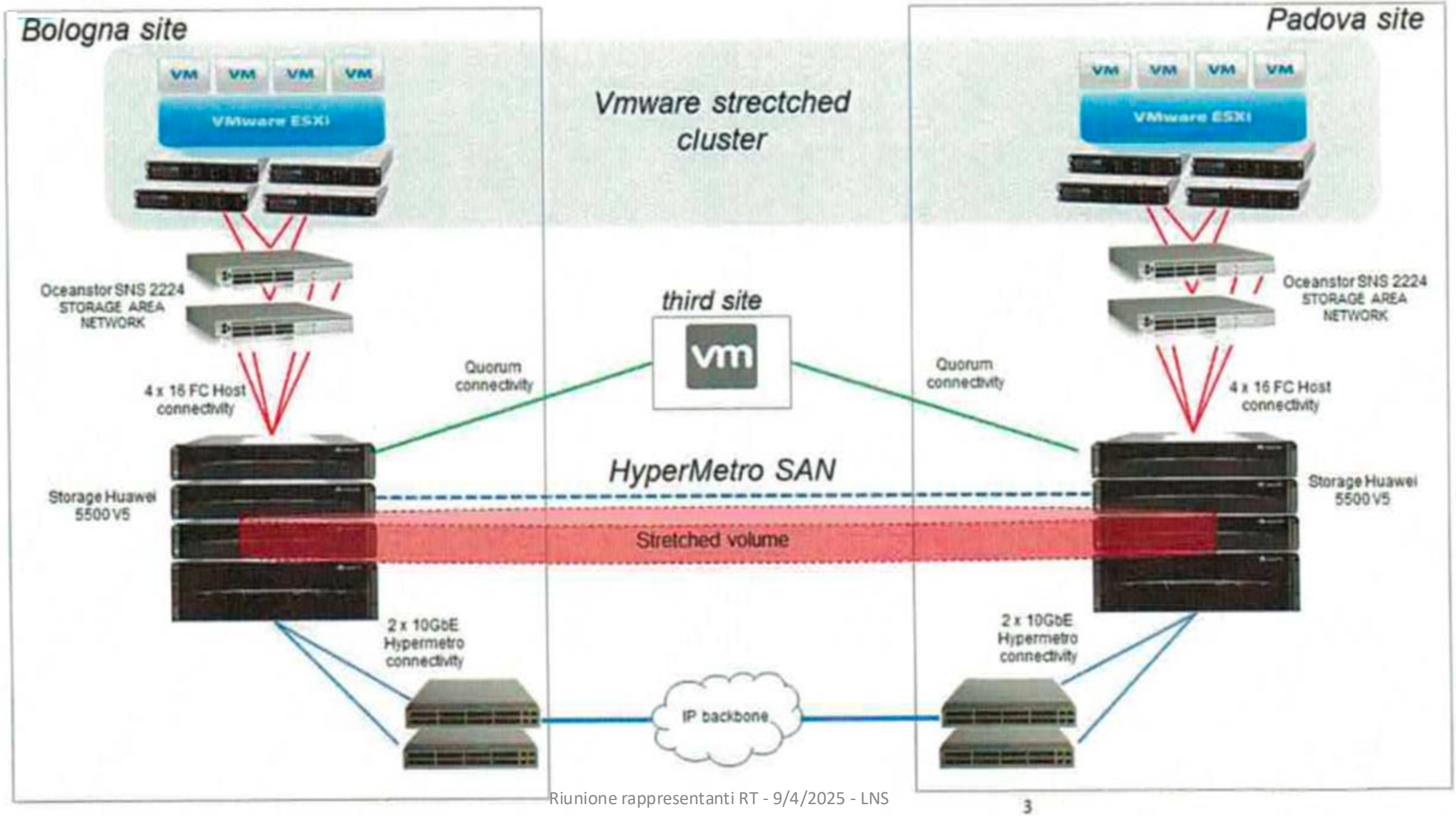
site 1 (CNAF)

- CPU: 1500 core
- VM: 500 VM
- RAM: 14 TB
- Storage: 300 TB

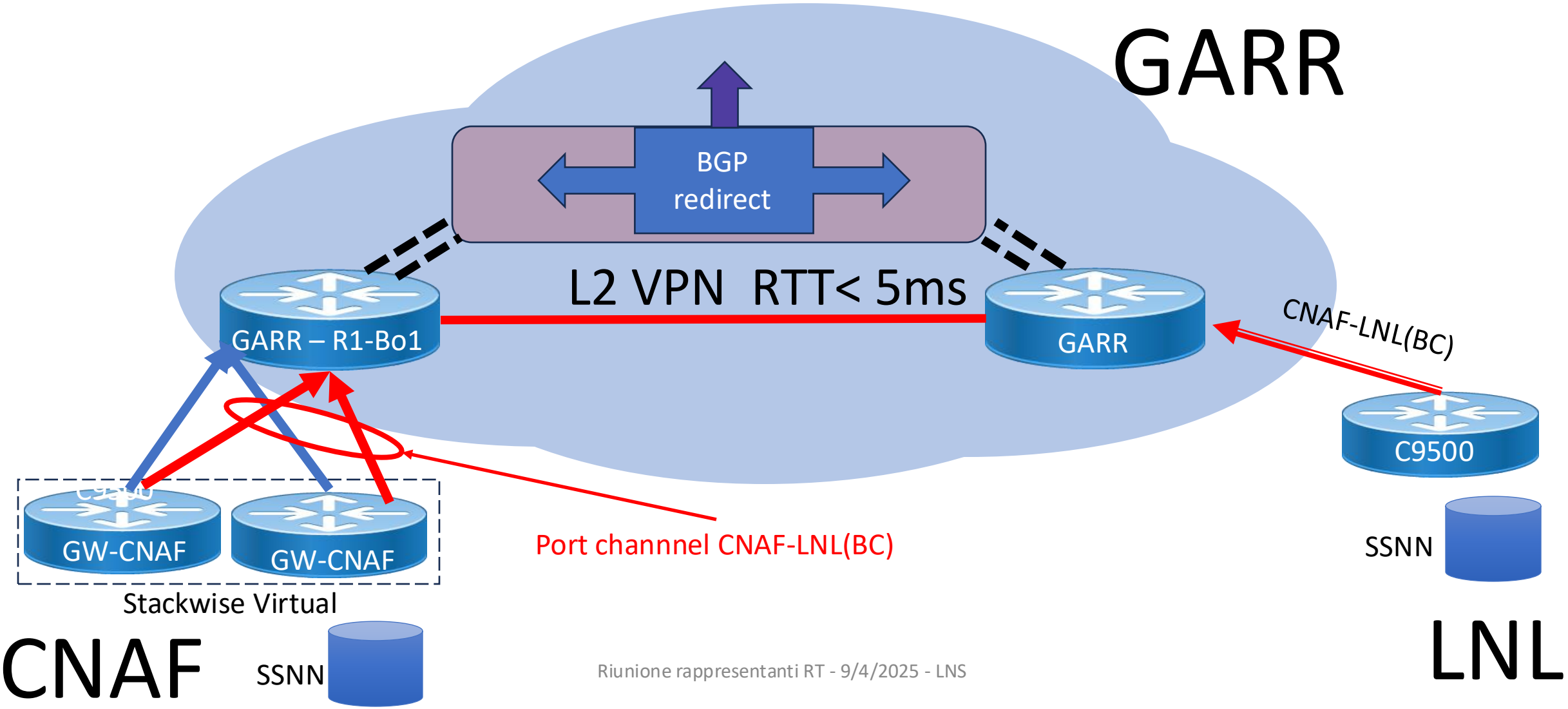


Disaster Recovery (LNF)

- CPU: 500 core
- RAM: 4 TB
- Storage: 200 TB


Bologna site
Padova site
VM
VMware ESXi
Vmware strectched cluster
Oceanstor SNS 2224 STORAGE AREA NETWORK
third site
vm
Quorum connectivity
4 x 16 FC Host connectivity
HyperMetro SAN
Storage Huawei 5500 V5
Stretched volume
2 x 10GbE Hypermetro connectivity
IP backbone

Connettivita’ dell’infrastruttura di BC



Attivita' in corso

- Sostituzione storage (2026)
  - 200+200 TB complessivi, supporto replica sincrona con rtt <= 5 ms

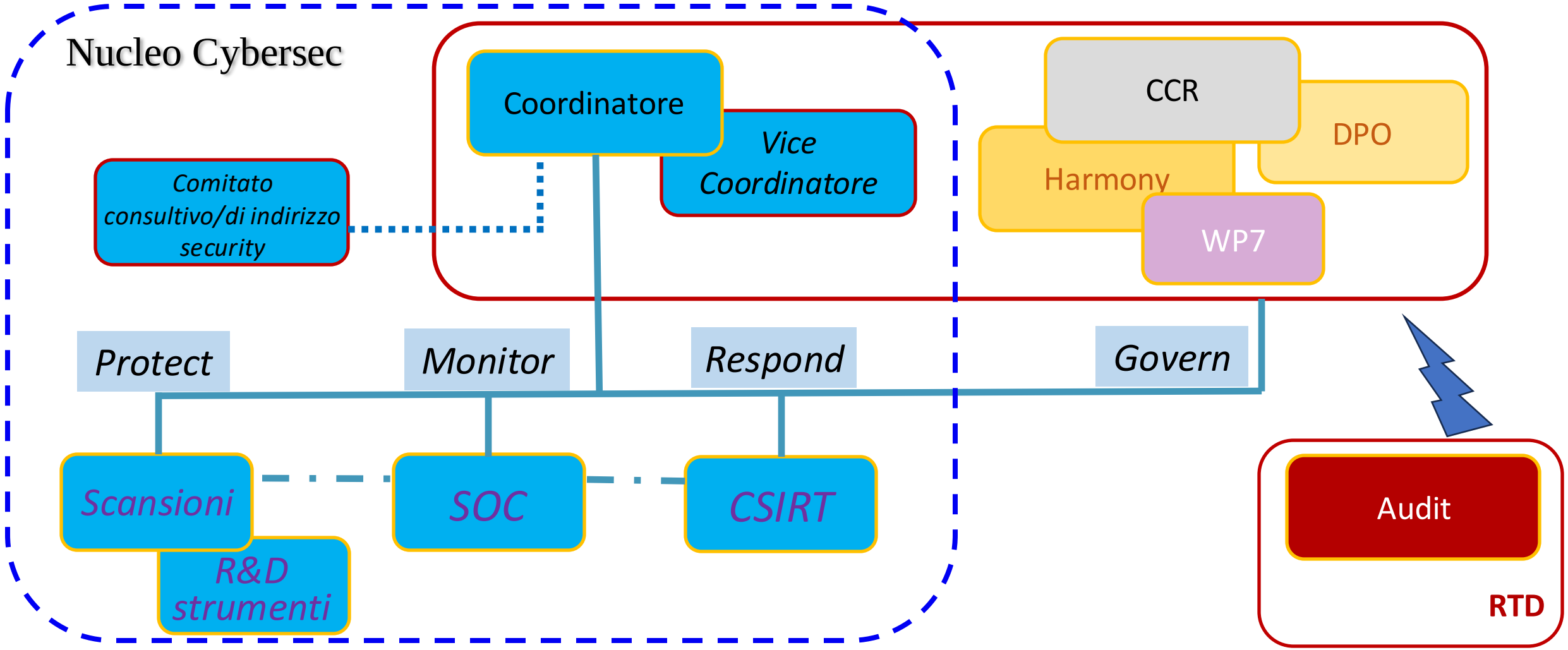
- Evoluzione tecnologica della connessione
  - rete (L2VPN) meno stabile negli ultimi mesi
    - 6 incidenti su 7 legati a malfunzionamenti della rete
  - analisi con GARR per individuare soluzioni piu' affidabili

- Migrazione infrastruttura CNAF al Tecnopolo
  - migrazione live di tutti i servizi a LNL e sito CNAF offline (14/4)
  - spegnimento infrastruttura CNAF e spostamento fisico al Tecnopolo (14-15/4)
  - accensione e verifica del routing (15-16/4)
  - sito CNAF online e redistribuzione dei servizi sui due siti (17/4)

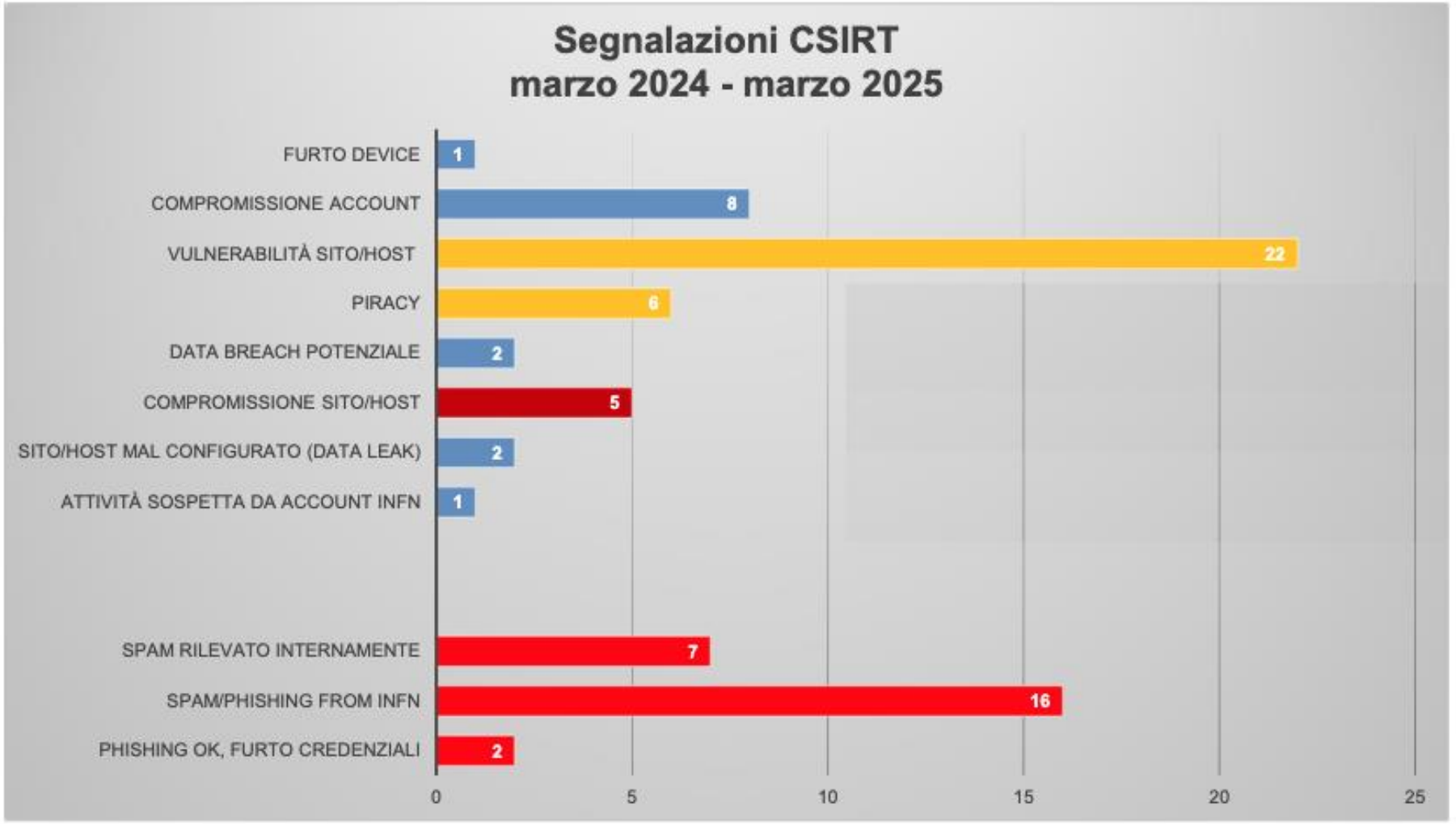
  - senza disservizio per gli utenti

- Organizzazione della CCR
- Infrastruttura di BC/DR
- Sicurezza informatica
- AAI
- Servizi nazionali
- Piattaforme sofwtare
- ChatGPT (AI?)

Il NUCS


Nucleo Cybersec
Coordinatore
Vice Coordinatore
Comitato consultivo/di indirizzo security
CCR
DPO
Harmony
WP7
Protect
Monitor
Respond
Govern
Scansioni
SOC
CSIRT
R&D strumenti
Audit
RTD

Segnalazioni CSIRT (2024-2025)



Revisione del disciplinare: obiettivi

- Includere le infrastrutture distribuite (INFN Cloud)
- Aggiungere possibilita' di delega ad istituzioni esterne per:
  a) identificazione ed autenticazione
  b) verifica sulle competenze informatiche (base e amministratore)
- Modulare il disciplinare con riferimenti a documentazione accessoria
  - Policy specifiche (dispositivi individuali, cloud esterne)
  - Policy tecniche (password policy, hardening dispositivi, protocolli encryption)

  aggiornamento a cura della CCR, da sottoporre al management
- Includere nuovi elementi (dispositivi personali, AI)
- Fornire dettagliata informativa agli utenti sull'utilizzo di dati personali

In fase di stesura definitiva

NIS2: principi generali

Ambiti di applicazione

Settori altamente critici, critici, Imprese e Pubbliche Amministrazioni, altri.

Governance

Autorita' nazionale competente NIS (ACN).
Autorita' di settore NIS (ministeri, conferenza permanente rapporti Stato Regioni).

Individuazione soggetti

Tipologie: essenziali e importanti (o fuori ambito).
Assegnazione basata su criteri oggettivi: grandi/medie imprese, tipologia di PA, modificabili a discrezione di ACN

Obbligh, monitoraggio e sanzioni

Registrazione, adozione di misure di sicurezza proporzionate al rischio, con approccio multi-rischio, processi di notifica degli incidenti.
Definisce chiara responsabilita' dei vertici dell'organizzazone.

Organizzazione cooperazione nazionale ed internazionale

Collegamento con organismi UE (Gruppo di cooperazione NIS, EU-CyCLONe, rete CSIRT nazionali).

Obblighi del decreto NIS (I/IV)

Registrazione

✓ Nomina punto unico di contatto:
delega firmata dal presidente (Enrico Pasqualucci)

✓ Registrazione dell'INFN sul sito ACN: completata

Termine: 28/2/2025

Obblighi del decreto NIS (II/IV)

Organi di amministrazione e direttivi

- approvano le modalita' di implementazione delle misure di gestione dei rischi
- ✓ sovrintendono alla registrazione
- **sono responsabili delle violazioni al decreto NIS**
- **sono tenuti a seguire una formazione in materia di sicurezza informatica**
- ✓ promuovono una formazione per i dipendenti in materia di sicurezza informatica
- sono informati periodicamente o puntualmente sugli incidenti e sulle notifiche

Termine: 18 mesi dalla registrazione (ottobre 2026), ma:

obbligo registrazione: 28/2/2025

obbligo notifica degli incidenti: 1/1/2026

Obblighi del decreto NIS (III/IV)

Misure di gestione dei rischi per la sicurezza informatica

Adozione misure tecniche, operative ed organizzative per la gestione dei rischi:

- adozione di misure di base (saranno definite entro aprile 2025)
  - per tutti i soggetti, tutte le attivita' e servizi
- adozione di misure a lungo termine (saranno definite entro aprile 2026)
  - graduate in base alla tipologia dei soggetti e categorizzazione dei servizi

Categorizzazione di attivita' e servizi

Termini:

adempimento degli obblighi base: ottobre 2026

categorizzazione di attivita' e servizi: non definito

adempimento degli obblighi a lungo termine: non definito

Obblighi del decreto NIS (IV/IV)

Notifiche degli incidenti informatici

Pre-notifica entro 24h

descrizione, se atto illegittimo, eventuale impatto trasfrontaliero

Notifica entro 72h

gravita', impatto, indicatori di compromissione

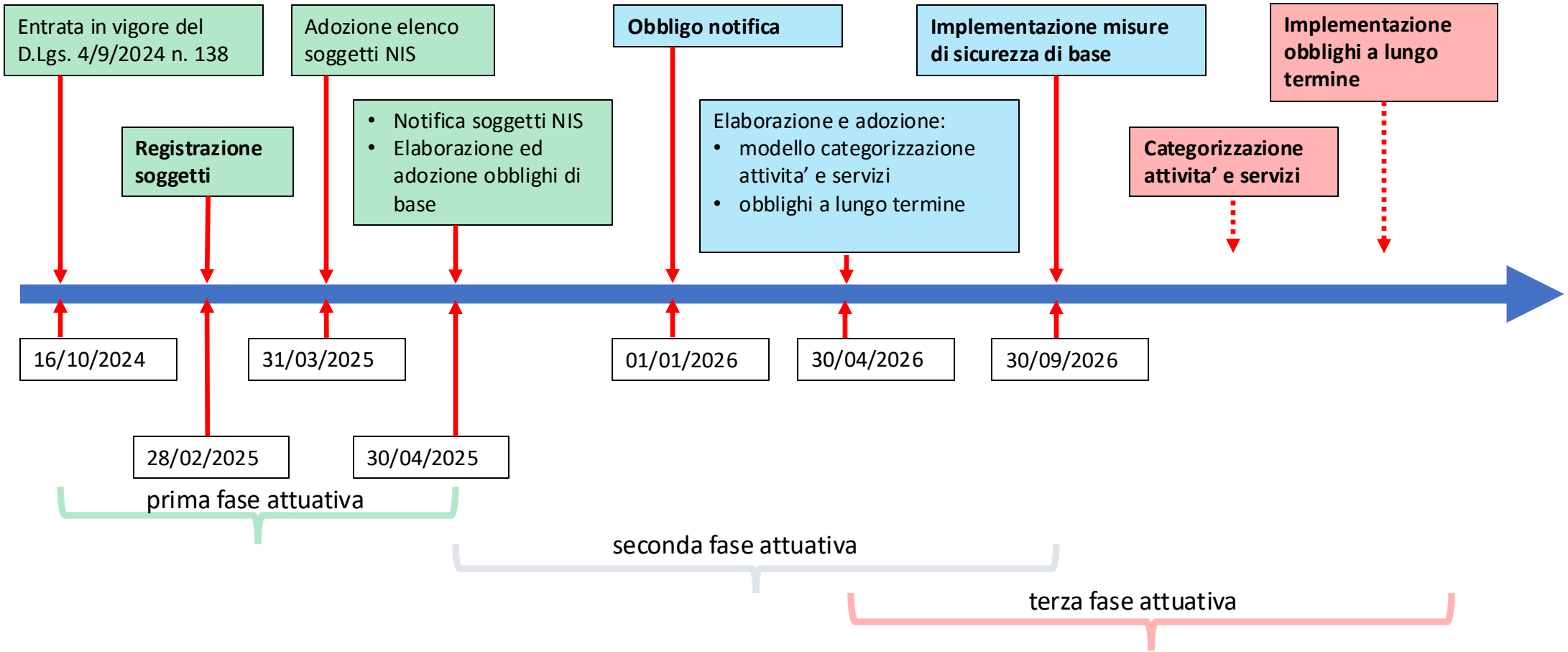
Relazione finale entro 1 mese dalla risoluzione dell'incidente

Solo incidenti significativi:

grave perturbazione operativa dei servizi, o perdite finanziarie per il soggetto
ripercussioni su altri causando perdite materiali o immateriali considerevoli

Termine: 1/1/2026

Recepimento ed attuazione direttiva UE 2022/2555 (NIS)



Proposta organizzativa per l'implementazione

Steering

- Membro di Giunta con delega al calcolo
- Presidente CCR
- Presidente C3SN
- RTD
- Responsabile Cybersecurity (NUCS)
- Coordinatore DPO
- Coordinatore WG Infrastruttura (DataCloud)
- Coordinatore EPIC

Report →

Management

Presidente
Giunta Esecutiva
Consiglio Direttivo

← Consulenza

Esperti

Ufficio Legale
Cybersecurity
Servizi e infrastruttura ICT
AC
Sviluppo software
...

Mandato

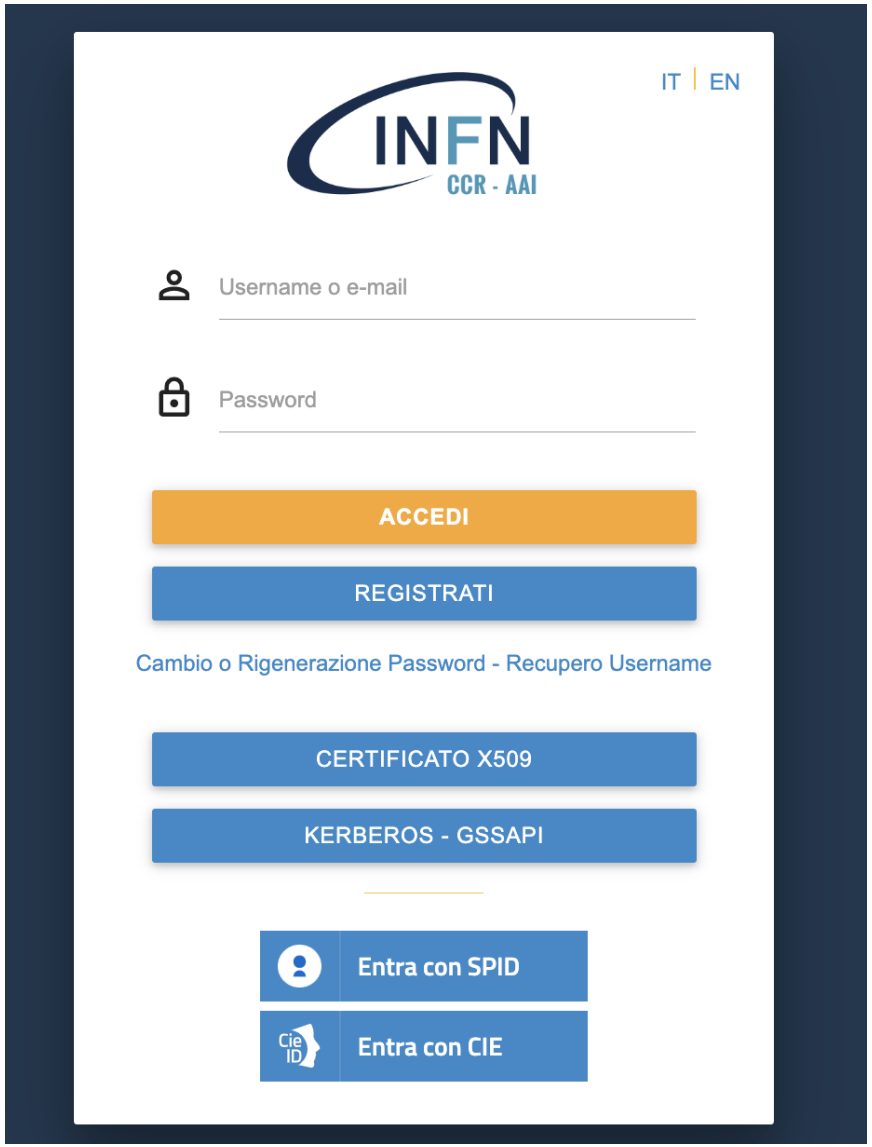
- coordinare lo sviluppo delle politiche di sicurezza dell'Ente
- definire un piano di implementazione per il decreto NIS e per la L. 90
  - definire un piano di formazione per il management
- monitorare la realizzazione del piano secondo le tempistiche pianificate
- valutare risorse finanziarie ad integrazione dei finanziamenti di CCR
- valutare criticita' su risorse umane

- Organizzazione della CCR
- Infrastruttura di BC/DR
- Sicurezza informatica
- AAI
- Servizi nazionali
- Piattaforme sofwtare
- ChatGPT (AI?)

INFN AAI

- Una sola identita’ digitale
- Supporto per diversi livelli di garanzia
- Supporto per diversi meccanismi di autenticazione
  - LDAP user/pwd, X.509 cert., KRB, SPID, CIE
- Supporto per SSO (SAML, OIDC)
- Supporto per 2FA
- Integrazione con servizi federati (IDEM, eduGAIN)

- Registrazione ed autorizzazione sono necessarie per accesso a servizi nazionali



Autenticazione a due fattori

- Il furto delle credenziali è una delle principali fonti di incidenti informatici
- Conseguenze:
  - invio di SPAM da server INFN (reputazione, black listing)
  - accesso non autorizzato alle risorse INFN
    - esfiltrazione e crittazione dei dati accessibili all'utente vittima
  - privilege escalation tramite attacchi interni
    - esfiltrazione e crittazione di tutti i dati e dei backup!
- Necessario proteggere gli account degli utenti ed i dati critici
  - limitazione dei privilegi di accesso
  - formazione, campagne di sensibilizzazione
  - utilizzo di autenticazione a più fattori indipendenti

- I fattori piu' comuni
  - qualcosa che sai (password, pin)
  - qualcosa che hai (smartphone, chiave USB, paper token)
  - qualcosa che sei (impronta digitale o altri fattori biometrici)

La soluzione adottata

- Open Source (anche in versione gratuita)
- Supporta vari tipi di «Tokens»
- Disponibilita’ di Plug-in (FreeRADIUS, SimpleSAMLphp, PAM, …)
- Multi-REALM
- Dispiegabile in modalità HA (DB singolo o clustered-DB)
- Free app (IOS & Android)
- Enterprise support

Scelte

- Token di tipo TOTP o paperToken

- TOTP
  - Cifratura SHA256 (SHA1 deprecata dal NIST)
  - Acquisizione Token self-service
    - Cancellazione solo tramite aai-support@infn.it
  - Validita' 12 ore
  - Max 10 token contemporanei (limite non ancora applicato)
  - Max 10 fallimenti (reset failcount alla prima autenticazione con successo)
    - dopo 10 fallimenti si blocca il token: sblocco tramite aai-support@infn.it
  - Opzioni: numero di cifre (6/8), tempo di validita' (30s/60s)

- PaperToken
  - 25 OTP per paperToken. Il primo OTP serve come verifica per completare l'enrollment)
  - Token disabilitato automaticamente all'utilizzo dell'ultimo OTP
  - Max 3 Token contemporanei

Policy

2FA richiesto per:

- Tutti i SP SAML registrati nell'IdP (incluso O365) con l'eccezione di
  - Agenda InDiCo (https://agenda.infn.it)
  - Vault bitWarden (https://vault.infn.it)
    - protetto da una sua password
- Tutti i SP OIDC registrati in INFN-AAI
  - DSI, microservizi CCR, Indigo-IAM (DataCloud)
- Tutti i SP di federazione IDEM/eduGAIN che lo richiedono
  - per la richiesta di certificati X.509 sara' forzato quando Harica sara' pronta

- L'accesso a servizi locali richiedera' il secondo fattore se autentica ed autorizza via INFN AAI.

Problemi

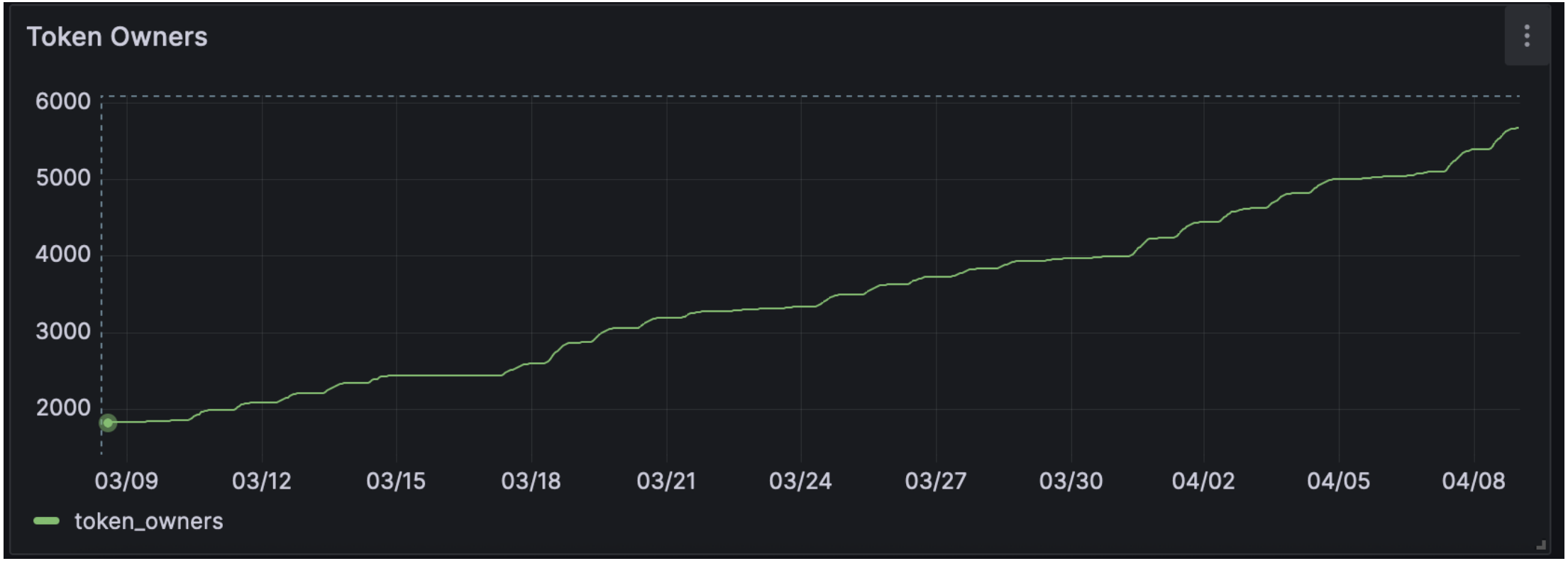
- Google e Microsoft authenticator non supportati
  - le app utilizzano SHA1 => sbagliano a generare il TOTP
  - sono app sconsigliate: per default salvano i token in chiaro sulla loro cloud
  - soluzione: usare l'app privacyIDEA, o altra app supportata (es: Aegis)

- Impossibilita' ad utilizzare uno smartphone: ci sono varie alternative
  - applicazione Ente Auth su desktop/laptop
  - inserimento del token su https://vault.infn.it (accessibile via browser)
  - utilizzo di paperToken

- Problemi successivi alla attivazione del token
  - perdita di smartphone, cancellazione della app, errori di configurazione
  - mitigati dall'inserimento di una procedura di verifica
  - unica soluzione: accedere al supporto aai-support@infn.it

- Alcune richieste di reinserimento prima della scadenza delle 12 ore
  - ci stiamo lavorando

Evoluzione temporale acquisizione token



~ 5100 token acquisiti su ~ 9500 utenti: ~3000 dip (91%), ~ 5200 ass (50%), 1700 ospiti (20%)

- Organizzazione della CCR
- Infrastruttura di BC/DR
- Sicurezza informatica
- AAI
- Servizi nazionali
- Piattaforme sofwtare
- ChatGPT (AI?)

Servizi nazionali della CCR

Portale di accesso: https://servizinazionali.infn.it

Document management

Alfresco

Enterprise Content Management

Document sharing, workflow

Pydio

Cloud storage

Sync and share

Office365

Sharepoint

Onedrive

Organizational tools

Indico

Event management.
Web site, agenda, registration, contributes, abstract, fees,...

SoGo

Manage personal and shared calendars

LimeSurvey

Create surveys, market research, user feedback

Dress

E-voting (even official)

Web services

Url Shortening

Get (short) URL alias in infn.it domain

Matomo Analytics

Web site statistics report: visitors, origin, keywords, most visited pages, etc.

Wiki

Get your wiki site based on dokuwiki

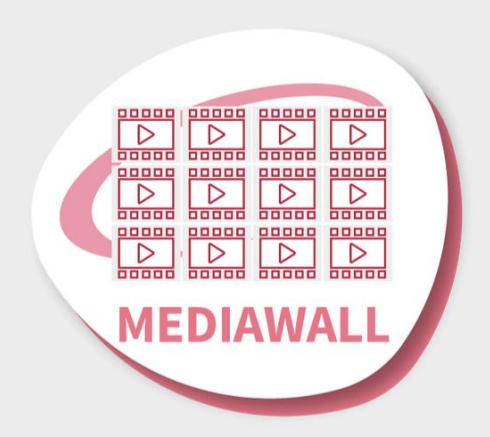
WebSite

Managed service to create WP/Joomla! web sites

Web services (cont.)

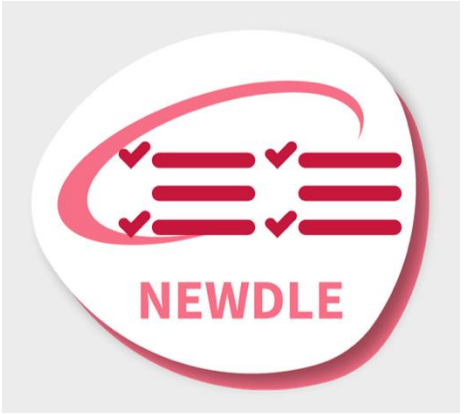
Vault

INFN credential manager



Mediawall

Open-source service for collecting and managing multimedia content



Newdle

Open source meeting organizer

Development collaborative platforms

Jira Software

Collaborative platform from the Atlassian suite designed to facilitate and make team project development more effective

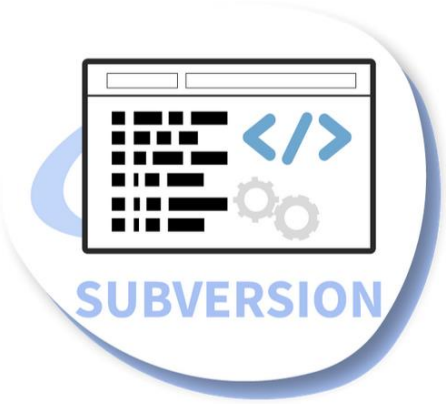
Jira Service Management

Ticketing system and asset management from the Atlassian suite

Confluence

Atlassian suite collaborative wiki for project and development documentation

Development collaborative platforms (cont.)

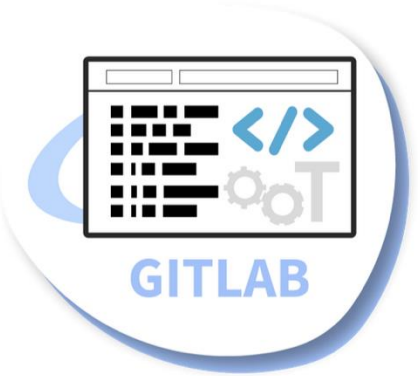


Subversion

software development version manager, based on Subversion VCS

Baltig

software development version manager, based on Gitlab VCS



Other services

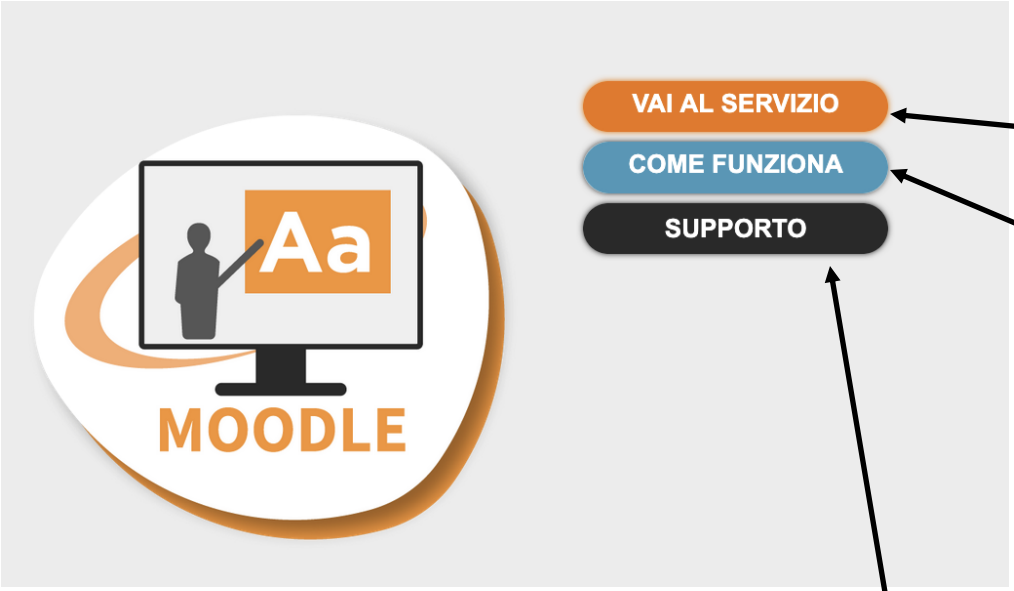
X.509 Certificate Service

Personal and server SSL certificate request

Moodle

INFN e-learning service
asynchronous online training

Get info, use the service, ask for support



Link to the service

How does it work

- Brief info
- Technical documentation
- Demo slides and training pills

Ask for support

Submit a ticket.
You will be redirected to the right place:

- local (INFN division) support
- national support

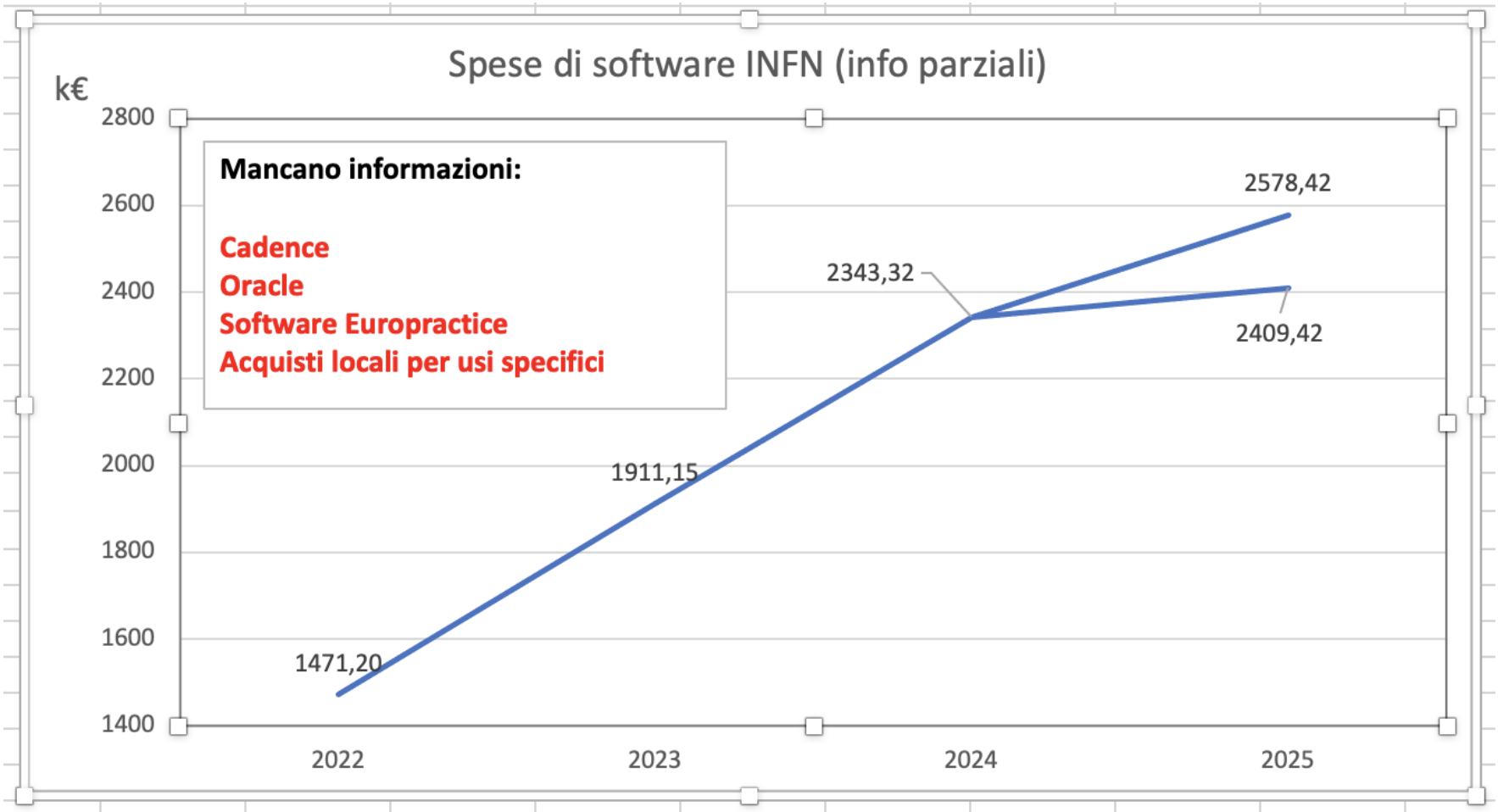
- Organizzazione della CCR
- Infrastruttura di BC/DR
- Sicurezza informatica
- AAI
- Servizi nazionali
- Piattaforme sofwtare
- ChatGPT (AI?)

Gestione piattaforme sofwtare

- Piattaforme sofwtare gestite o finanziate dalla CCR
  - prodotti per ICT (campus, per numero di utenti o licenza individuale)
    - pagati da CCR o CCR+contributi da utenti o sedi
  - prodotti per calcolo scientifico (campus, a licenza individuale, a licenza condivisa)
    - pagati dagli utilizzatori, a licenza individuale o per quote
    - alcuni (co-)finanziati da CCR (integrale: NI, parziale: Matlab)
  - prodotti per progettazione meccanica/elettronica (licenza individuale o condivisa)
    - pagati dagli utilizzatori, per licenza o per quote

- Non tutte le esigenze di software passano per la CCR
  - software per la DSI (Oracle)
  - Europractice
  - acquisti individuali

Storico costi



Problemi

- Manca visione complessiva delle spese per il software nell'INFN
- Manca la possibilita' di fare programmazione adeguata
  - analisi delle esigenze fatto al momento del rinnovo licenze
    - finanziamenti non sempre programmati nel normale flusso richiesta/referaggio/approvazione delle CSN
- Coordinamento da migliorare
  - condivisione delle scelte ad impatto comune (campus, quote)
  - ricerca di ottimizzazioni per economia o diffusione
- Operativita'
  - mancanza di referenti tecnici espressamente incaricati per ciascun software
  - complessita' nell'esecuzione degli storni

Proposta operativa (CSN, CCR, Strutture)

- Giugno: si rende disponibile un listino per le richieste di luglio
  - basato sui costi correnti e su previsioni
  - eventuale integrazione per nuovi prodotti
- Settembre: referaggio ed approvazione delle richieste
  - CSN/CCR: referaggio in riunione di bilancio
  - Strutture: referaggio a cura del Direttore
  - fondi in una tasca
  - Inoltro del dettaglio delle approvazioni alla CCR
- Ottobre: riunione del gruppo di coordinamento sw
  - valutazione su possibili sinergie, eventuale seconda interazione con CSN/Strutture
- Gennaio: assegnazione dei fondi sulla sigla *CCR_MEZZI_CALC* del CNAF
- In corso d'anno la CCR procede con contrattazioni e ordini
  - coadiuvata da referenti tecnici per ciascun software
  - eventuali esigenze non programmate vengono valutate col gruppo di coordinamento, referate in CSN e i fondi assegnati alla sigla

Obiettivi

- Permettere a CSN e strutture una pianificazione controllata
  - visione dei sofwtare disponibili e dei costi
- Coordinare le esigenze di piattaforme sofwtare
  - cercare sinergie, ottimizzare spese, opzioni campus
- Evitare partizionamento degli acquisti
- Monitorare la spesa complessiva per le piattaforme software
- Semplificare le procedure di storno
- Maggiore controllo sul rispetto delle EULA
- Integrazione autorizzazione licenze individuali con INFN AAI

Il gruppo di coordinamento

- Il gruppo e' gia' operativo:
  - license manager INFN (Cristina Vistoli)
  - referenti per le CSN
    - Bonacorsi, Travaglini, Duranti, Di Pierro, Lacognata, Ferrera, Retico, Lonardo
- Si aggiungeranno:
  - referee CCR per il software
  - referenti per le strutture

- Coordinamento tecnico:
  - referenti tecnici per ciascuna piattaforma software
    - coordinamento tra le strutture per la definizione delle esigenze
    - contrattazione

Piattaforme software disponibili (I/II)

Adobe Acrobat Pro

Adobe Creative Cloud

Atlassian Confluence

Atlassian Jira Software

Atlassian JSM

Microsoft 365 products

Microsoft 365 Copilot
Outlook
OneDrive
Word
Excel
PowerPoint
OneNote
SharePoint
Teams
Sway
Forms
Project
Visio
Planner
More apps

Zoom Pro
Large 500/1000
Webinar 500/1000

Overleaf

Piattaforme software disponibili (II/II)

Simulation

CDF, **EM**, **HFSS**, **Lumerical**, **Granta**, **Zemax**
fluid, em, multiphysics photon, optical

multiphysics numerical sim

Radiation sim

Dassault Opera / CST

Computation and data analysis

National Instruments
devel and test DAQ

Wolfram Mathematica
symbolic computation

PTC Mathcad

MathWorks Matlab
numerical comp. and stat.

Electronic and Mechanical Design

Autodesk PDM coll., AEC coll., Autocad, Inventor, Fusion

PTC Creo

Dassault SolidWorks

Dassault 3dexperience

- Organizzazione della CCR
- Infrastruttura di BC/DR
- Sicurezza informatica
- AAI
- Servizi nazionali
- Piattaforme sofwtare
- ChatGPT (AI?)

Contratto ChatGPT: in arrivo!

- Il gruppo CRUI-ICT ha raccolto manifestazione di interesse per un contratto con OpenAI per l'acquisto di prodotti ChatGPT
  - l'INFN ha manifestato interesse
- E' stata completata una contrattazione con OpenAI
  - procedura di affidamento in corso
- Per giugno dovrebbe essere disponibile un listino di prodotti
  - previsione di costi: ~ 50% dei costi di listino web
  - al momento non e' disponibile informazione sui prodotti
- Sara' quindi possibile acquistare licenze OpenAI
  - esclusivamente attraverso la CCR

Caratteristiche del contratto

- CRUI gestisce la negoziazione e la procedura di gara

- Saranno imposte a OpenAI alcune condizioni:
  - adozione di misure di sicurezza avanzate
  - gestione trasparente di eventuali sub-responsabili
  - notifica tempestiva in caso di data breach
  - OpenAI non potrà trasferire dei dati al di fuori dello Spazio Economico Europeo senza le dovute garanzie e al termine del contratto
  - OpenAI sarà obbligata a cancellare o restituire tutti i dati trattati

- Le Università e gli Enti aderenti avranno la facoltà di verificare la conformità di OpenAI tramite audit e richieste di informazioni

Di cosa ci dobbiamo preoccupare?

- La valutazione di compliance finale spetta a ciascuna università/ente

- Ogni università/ente partecipante ai contratti rimane autonomo titolare del trattamento e deve valutare autonomamente
  - il soddisfacimento dei requisiti della propria policy privacy e della normativa vigente
  - verifica di conformità all'AI Act
  - verifica di conformita' alle linee guida AgID
  - verifica di conformita' al GDPR in generale

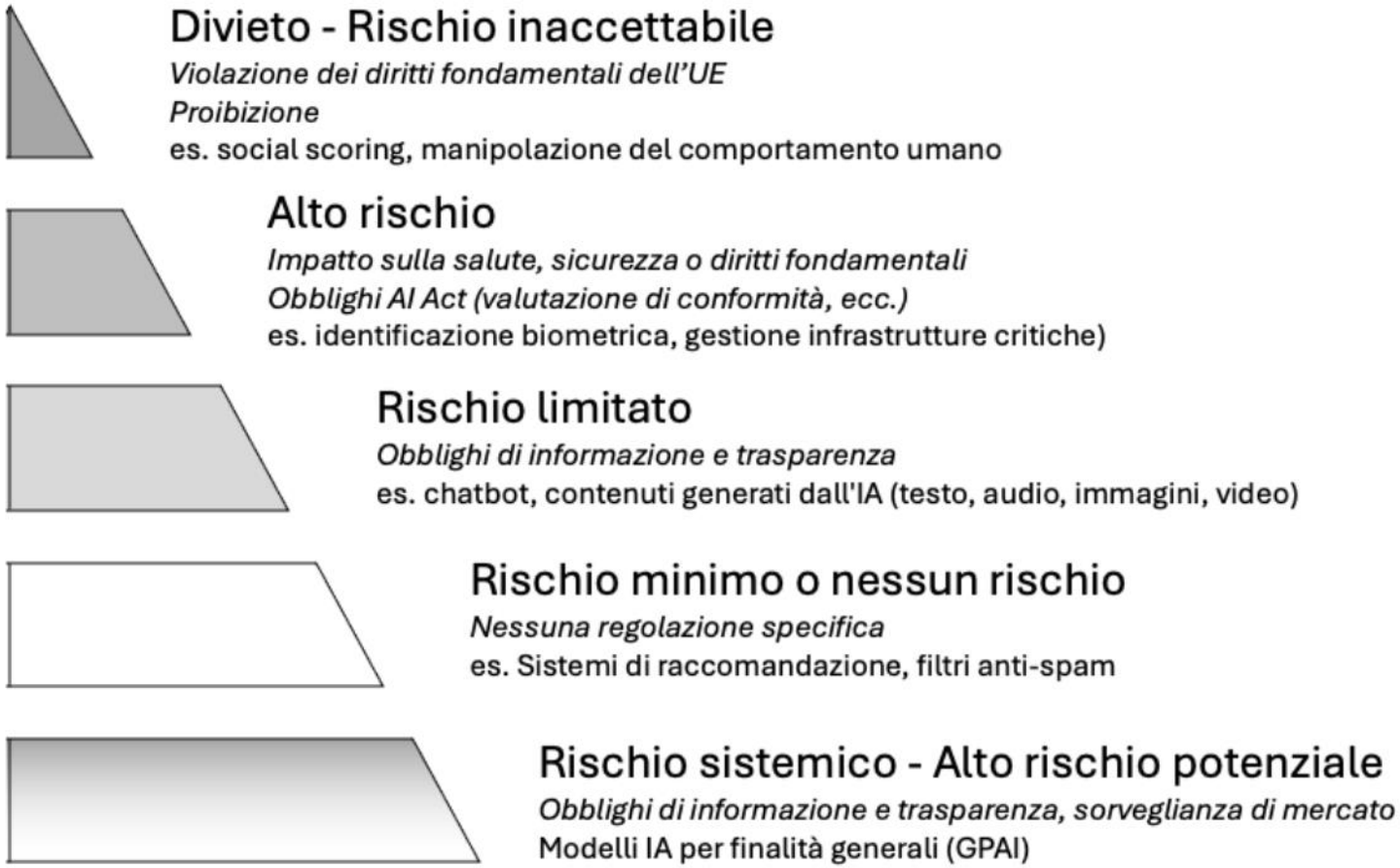
- Sono verifiche che dipendono dal proprio specifico utilizzo dello strumento.

AI act

- In vigore dal 2/8/2024

  - **i divieti**, le definizioni e le disposizioni relative all'alfabetizzazione in materia di AI che si applicheranno a partire dal 2 febbraio 2025
  - le **norme** sulla governance e gli obblighi per l'AI di uso generale che si applicheranno a partire dal 2 agosto 2025
  - gli **obblighi** per i sistemi di AI ad alto rischio classificati come ad alto rischio perché incorporati in prodotti regolamentati, elencati nell'allegato II (elenco della normativa di armonizzazione dell'Unione), che si applicheranno a partire dal 2 agosto 2027

Classificazione sistemi di AI (rischio)



Divieto - Rischio inaccettabile
Violazione dei diritti fondamentali dell'UE
Proibizione
es. social scoring, manipolazione del comportamento umano

Alto rischio
Impatto sulla salute, sicurezza o diritti fondamentali
Obblighi AI Act (valutazione di conformità, ecc.)
es. identificazione biometrica, gestione infrastrutture critiche)

Rischio limitato
Obblighi di informazione e trasparenza
es. chatbot, contenuti generati dall'IA (testo, audio, immagini, video)

Rischio minimo o nessun rischio
Nessuna regolazione specifica
es. Sistemi di raccomandazione, filtri anti-spam

Rischio sistemico - Alto rischio potenziale
Obblighi di informazione e trasparenza, sorveglianza di mercato
Modelli IA per finalità generali (GPAI)

Linee guida AgID per l'implementazione della AI nelle PA

- Pubblicate il 14/2/2025
  - Attualmente nella fase di consultazione popolare

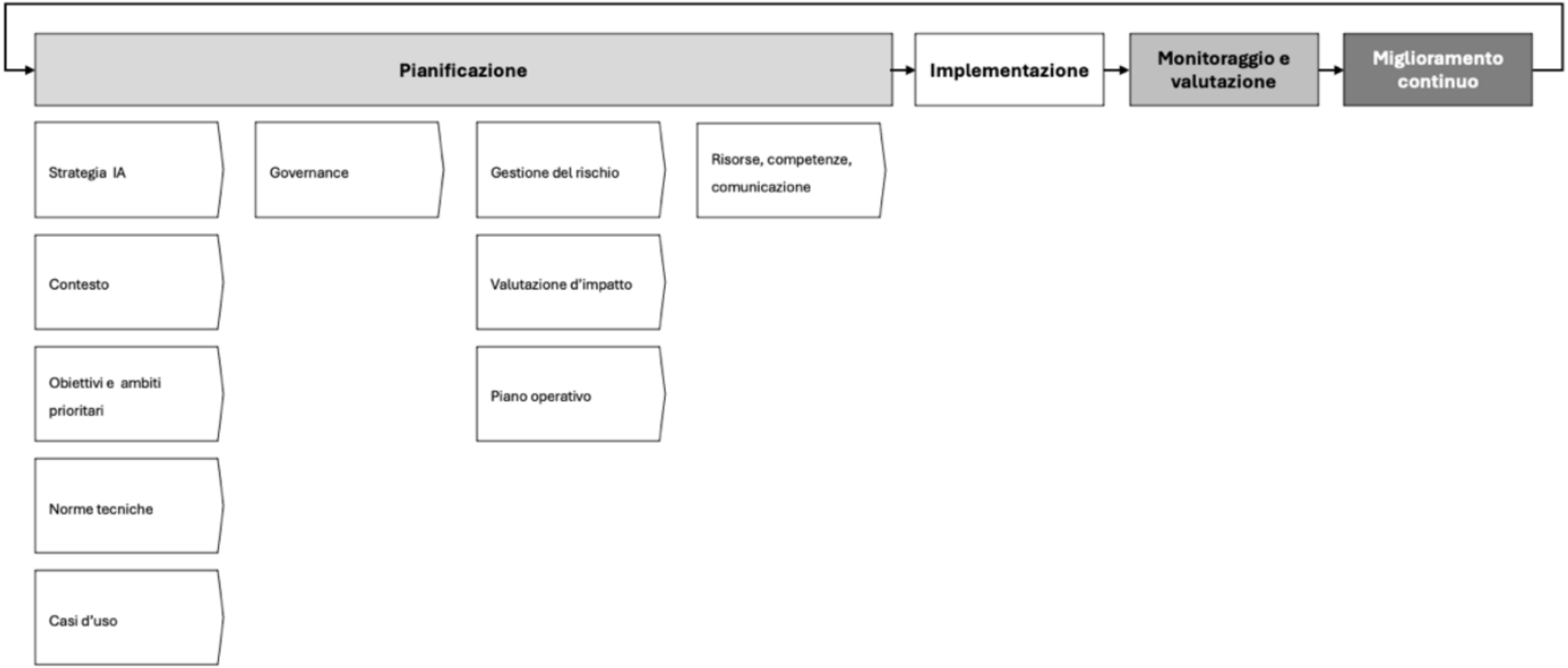
- Fornisce linee guida ed indicazioni dettagliate su cosa le PA devono o dovrebbero fare, e cosa NON devono fare, sulla base dell'AI Act.

Elementi trattati

- Modello di adozione
- Conformita’ delle soluzioni: monitoraggio e sorveglianza
- Governance dell’etica
- Trasparenza e comunicazione
- Formazione
- Gestione della qualita’ dei dati
- Protezione dei dati personali
- Sicurezza cibernetica

Include esempi e template per facilitare l’implementazione delle licee guida

Implementazione del modello di adozione



Work in progress: strategia ed introduzione della AI

- Documento di strategia sull'utilizzo della AI (2024)
  - posizionamento dell'INFN sull'utilizzo della AI nel settore della ricerca e di partecipazione al panorama di iniziartive europee (EOSC, Euro HPC)

- Piano triennale dell'Informatica per l'INFN (aggiornamento 2025)
  - introduzione di un capitolo relativi all'utilizzo della AI nel settore gestionale e amministrativo

- Disciplinare dell'utilizzo delle risorse informatiche
  - introduzione di un paragrafo generico sulla AI

E' necessario ampliare strategia e policy interne, anche etiche. Servono
informazioni approfondite sulla normativa (che e' in evoluzione)
competenze sullo strumento

Work in progress: attivita' tecnica

- In avvio la costituzione di un gruppo di lavoro (condivisione) per accelerare l'introduzione di questi strumenti in ambito anche non scientifico (C3SN-CCR-DSI).
  - raccogliere l'expertise attualmente sparpagliata e scoordinata
  - focalizzare attivita' su use case
- Attivita' focalizzata su use case. Esempi:
  - gestione di richieste di supporto
  - scrittura di best practices
  - gestione documentale
  - strumenti a supporto della cybersecurity
- Dedicata una sessione sulla AI al prossimo Workshop sul Calcolo dell'INFN (Elba, 26-30/5/2025)

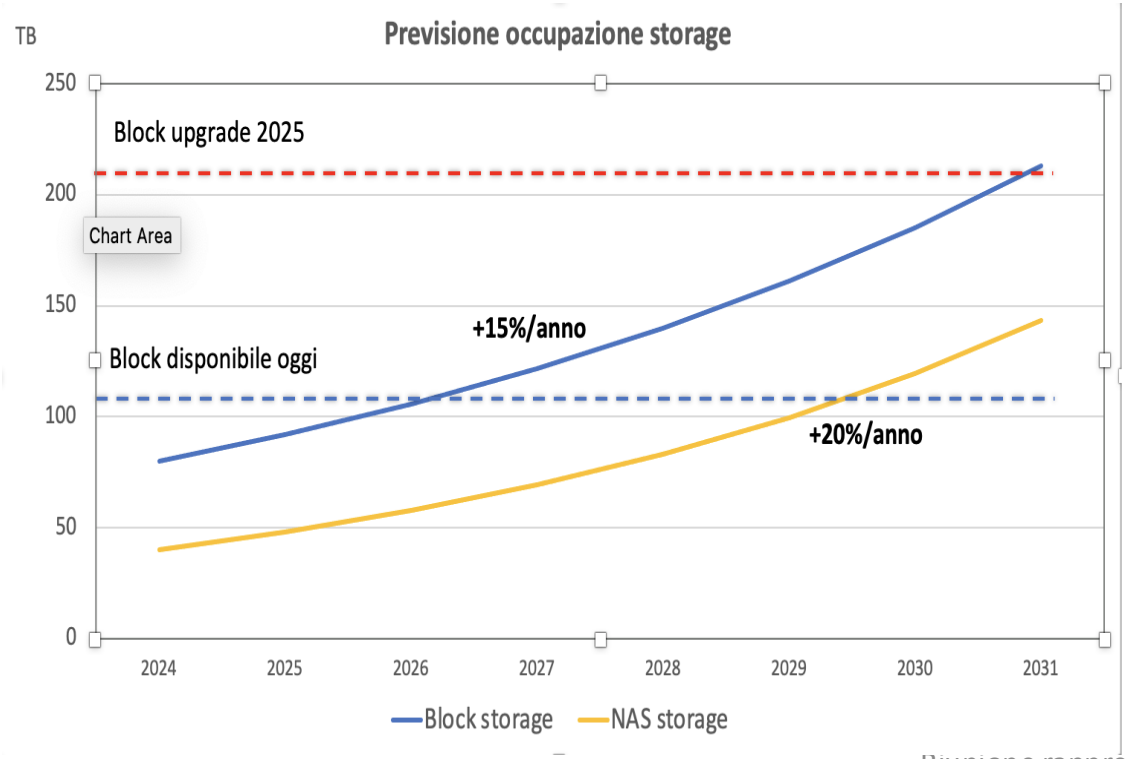
Discussione/Domande

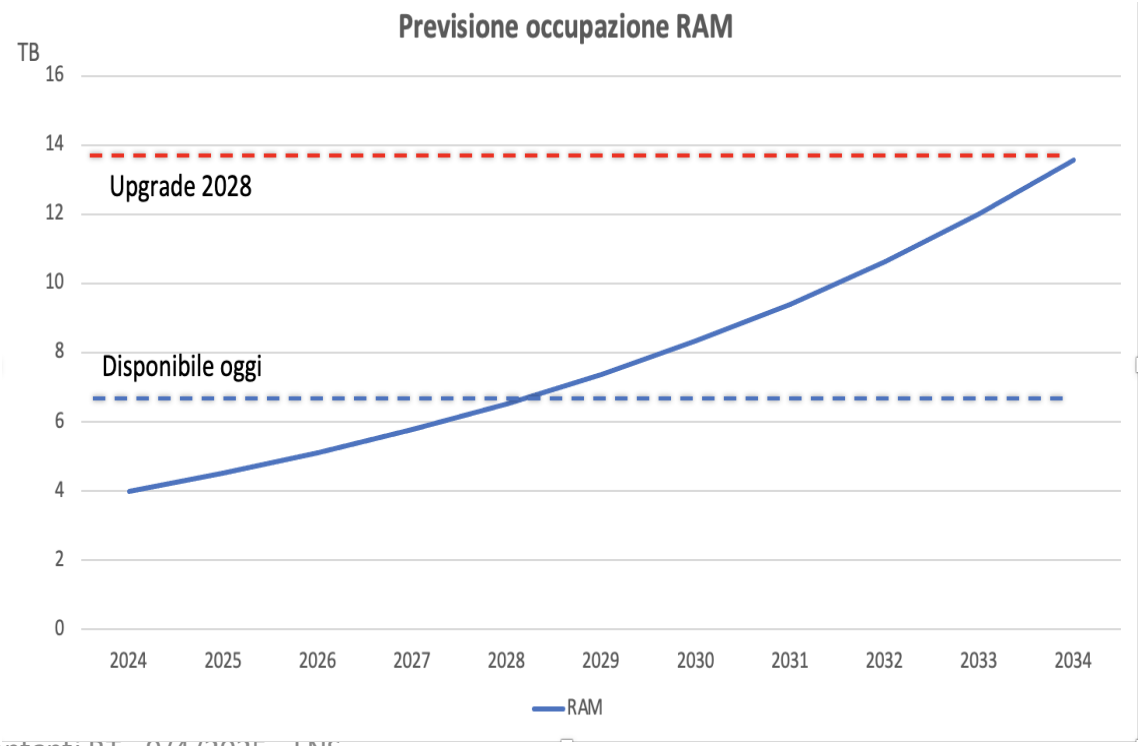
Backup slide

Previsione esigenza di risorse

- Sostituzione storage nel 2025 per motivi di eta’ (7 anni)
  - 220 TB block, 200 TB NAS
- Durata prevista: 6 anni

- Sostituzione CPU nel 2028 (eta’ e risorse)
  - almeno 12 TB
- Durata prevista: 6 anni



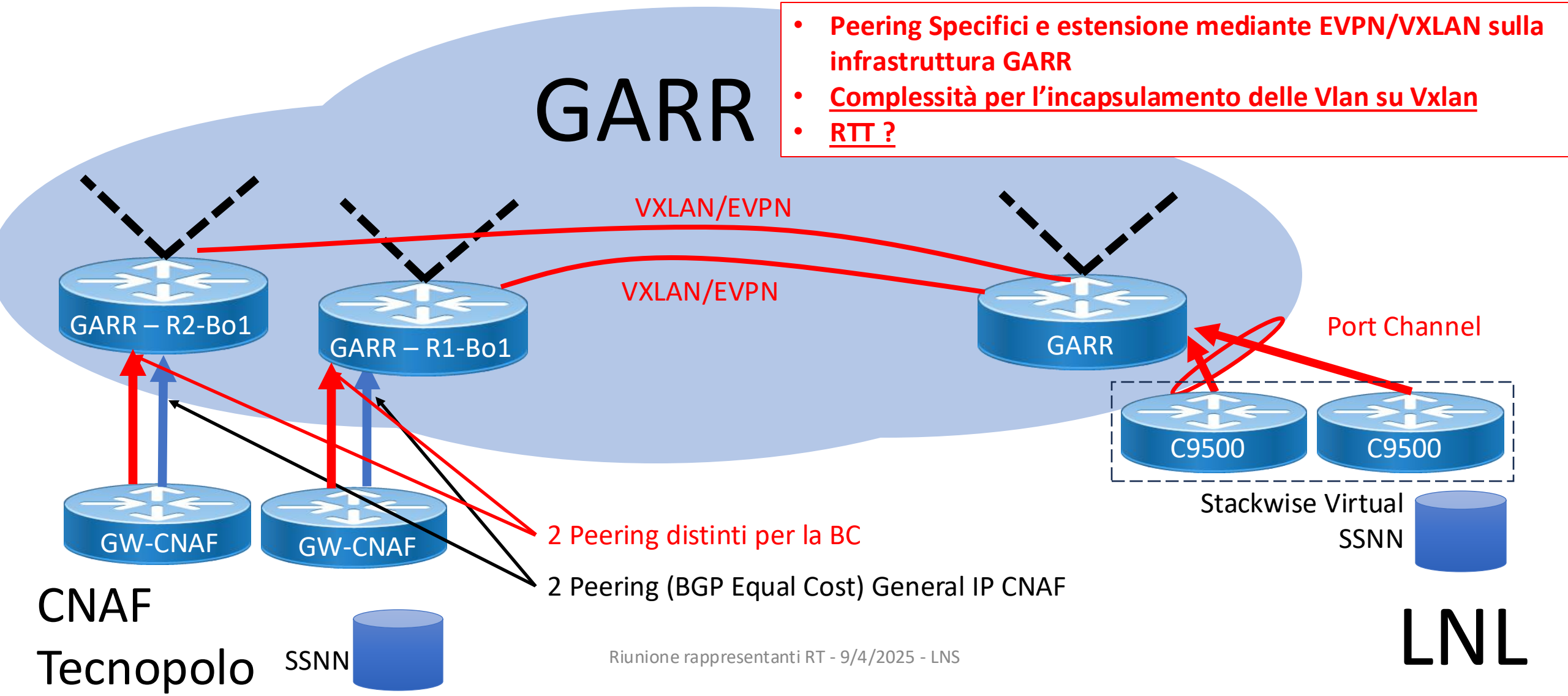


Incidenti (sola infrastruttura, non servizi)

- 04/01/2024 - Manutenzione non annunciata GARR. Effetto: failover LNL->CNAF. Ripristino automatico dei servizi as usual, bilanciamento ripreso appena ripristinato link CNAF-LNL
- 30/01/2024 (10:02) - Interruzione link CNAF-LNL a causa di un errore di configurazione del backbone GARR. Effetto: failover LNL->CNAF, come sopra, ripristino servizi as usual e bilanciamento ripresto appena ripristinato link CNAF-LNL
- 04/04: Down linea CNAF-LNL per manutenzione, senza preavviso. Effetto: failover LNL->CNAF, come sopra, ripristino servizi as usual e bilanciamento ripresto appena ripristinato link CNAF-LNL
- 24/04/2024 - Isolamento delle VM a causa di un problema di ACL (baco Cisco, quello di cui ha accennato Zani per capirci). Effetti: irraggiungibilità dei servizi, nessun failover o riavvio. Servizi tornati disponibili appena corretta l'ACL
- 03/10/2024 - Manutenzione GARR, VM preventivamente spostate su LNL. Dinamica ancora da chiarire, durante l'intervento comunque si è verificato un failover sul CNAF che non doveva accadere, causando il riavvio di una parte delle VM (alcune decine se ben ricordo, diciamo 15%). Sembra sia stato un problema di routing ma ad ora onestamente non mi è chiaro
- 23/10/2024 (10:37) - Interruzione non pianificata link CNAF-LNL. Effetto: inizio failover VM LNL->CNAF. Un paio di minuti dopo il link è stato ripristinato. Alcune VM sono state riavviate, ripristinato il link i servizi sono stati ribilanciati
- 30/10/2024 - Intervento manutenzione GARR. VM e routing spostato preventivamente su LNL. Connettività interrotta per VM multihomed per un doppio attraversamento ACL, tutti gli altri servizi sono rimasti online. Nessun riavvio o failover, funzionalità VM ripristinata con il ripristino del routing al CNAF.

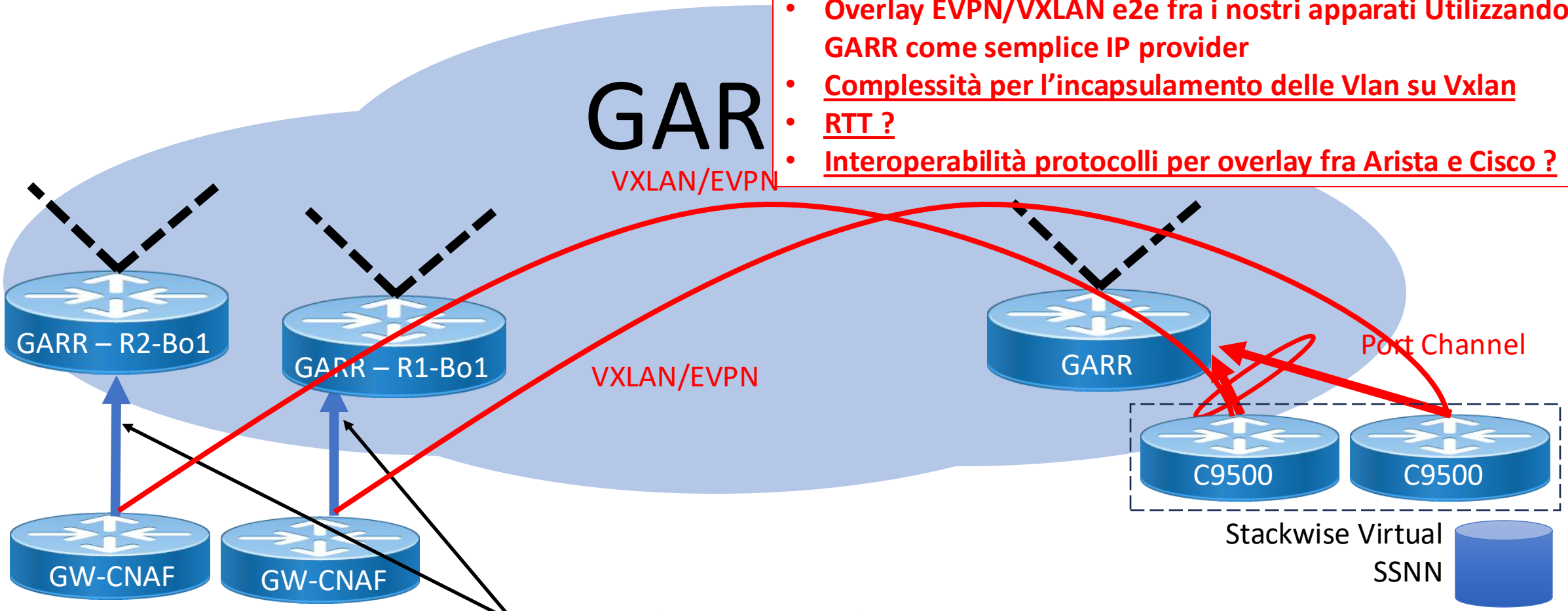
Ipotesi 3 Evoluzione da realizzare per il Tecnopolo
(Ancora da discuterte ed approfondire con GARR)

- **Peering Specifici e estensione mediante EVPN/VXLAN sulla infrastruttura GARR**
- **Complessità per l'incapsulamento delle Vlan su Vxlan**
- **RTT ?**



Ipotesi 4 Evoluzione da realizzare per il Tecnopolo
(Ancora da discuterte ed approfondire con GARR)

- **Overlay EVPN/VXLAN e2e fra i nostri apparati Utilizzando GARR come semplice IP provider**
- **Complessità per l'incapsulamento delle Vlan su Vxlan**
- **RTT ?**
- **Interoperabilità protocolli per overlay fra Arista e Cisco ?**



CNAF Tecnopolo

SSNN

LNL

Incident reporting nell'INFN

T0: scoperta incidente

*.infn.it

SOC/EDR

CSIRT ITALIA

GARR CERT

EGI CSIRT

T0: ricezione notifica

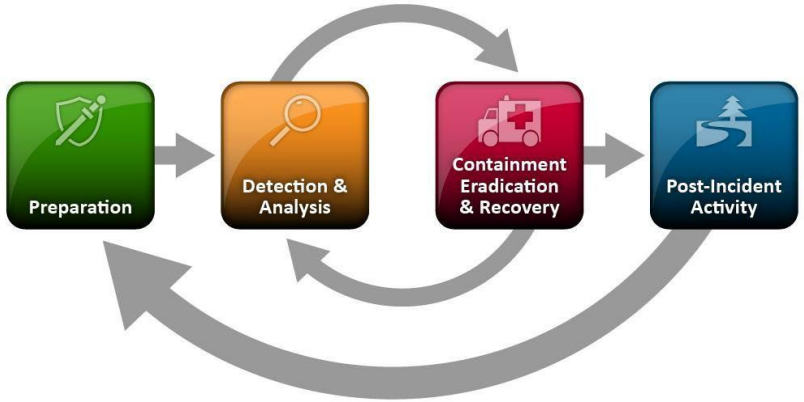
Un referente in ogni sezione (formazione a breve) è responsabile per la prima raccolta delle informazioni e la trasmissione entro 8-12 ore a INFN CSIRT, il quale offrirà collaborazione e si occuperà di inoltrare la segnalazione a CSIRT ITALIA o ACN (Autorità competente NIS2 per Italia) nei tempi prestabiliti.

INFN CSIRT
e-mail, PEC, form web, keybase

24/72/1 mese

CSIRT ITALIA ACN (obbligo di risposta e supporto)

L'abbozzo di Incident Response Plan attualmente in uso va espanso e trasformato in un vero IRP (vedi NIST 800-61r2)



AAI – 2FA: piano temporale adozione

- maggio-settembre: pilota esteso (personale del calcolo)
  - evidenziato un problema sulla gestione della cache non condivisa: configurato memcached
  - evidenziato un problema di risorse per la cache delle sessioni: incremento RAM
  - pianificata migrazione a simpleSamlPHP versione 2 (migliore gestione delle sessioni)
- luglio: presentazione in preCD
- settembre: comunicata disponibilita' del servizio
  - volontario fino ad aprile, obbligatorio dopo (dipendenti, associati, ospiti)
  - impatta solo sui servizi autenticati via IdP (SAML, OIDC)
- ottobre: individuati e risolti problemi iniziali
  - configurato di un test di funzionalita' prima di abilitare l'utente
  - migliorate le istruzioni (https://wiki.infn.it/cn/ccr/aai/doc/2fa)
- ottobre-novembre: webinar su configurazione ed utilizzo: due edizioni, 300 partecipanti
- marzo: adozione di configurazioni di convincimento (timer sulla autenticazione)
- 8 aprile: configurazione obbligatorieta' della 2FA

AAI – profili IDEM/Refeds

- Configurati profili IDEM/REFED Assurance Framework sulla infrastruttura INFN AAI
  - Oggi IDEM-P1 (tutti), IDEM-P2 (dipendenti)
  - Autoceritificazione sulla conformita' in procinto di essere firmata ed inviata ad IDEM

REFEDS Assurance Framework	RAF IAP low	RAF IAP medium	RAF IAP high	
IDEM Assurance Profiles	IDEM-P0	IDEM-P1	IDEM-P2	IDEM-P3
INFN AAI LoA	INFN AAI LoA1	INFN AAI LoA2		
eIDAS Levels of Assurance	eIDAS LoA Low		eIDAS LoA Substantial	eIDAS LoA High
NIST 800-63-3 IAL and AAL	NIST 800-63-3 IAL1/AAL1		NIST 800-63-3 IAL2/AAL2	NIST 800-63-3 IAL3/AAL3
Italian eGOV-ID	/	/	SPID-L1 SPID-L2 SPID-L3	CIE
ITU-T X1254 (09/2012)	LoA1	LoA2	LoA3	LoA4
ITU-T X1254 (09/2020)	/	AAL1	AAL2	AAL3

	IDEM-P0	IDEM-P1	IDEM-P2	IDEM-P3
Identifiers	Natural person, unique identifiers	Natural person, unique identifiers	Natural person, unique identifiers	Natural person, unique identifiers
Identity vetting	Contacts	Identity document	Identity document + verification	Electronic Identity Card or Passport
Attributes quality	-	Affiliation updated within one month*	Affiliation updated within one day*	Affiliation updated within one day*
Authentication	REFEDS SFA	REFEDS SFA	REFEDS MFA	REFEDS MFA

Ambiti di applicazione

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia	19 tipologie di soggetto	Essenziali	Importanti *	Fuori ambito **
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto		Importanti *	Fuori ambito **
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto	Importanti *		Fuori ambito **
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			
Fornitori di servizi digitali	4 tipologie di soggetto			
Ricerca	2 tipologie di soggetto	Importanti *		Fuori ambito **
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale	4 categorie di PA	Essenziali		
Pubblica Amministrazione regionale e locale	11 categorie di PA	Importanti *		
Ulteriori tipologie di soggetti	4 tipologie di soggetti	Identificazione dell'Autorità		

(*) possibile identificazione dell'autorita' come essenziale

(**) possibile identificazione dell'autorita' come importanti o essenziali

ChatGPT

ChatGPT è un chat bot basato su intelligenza artificiale e apprendimento automatico, sviluppato da Open AI e specializzato nella conversazione con un utente umano.

Wikipedia

ChatGPT è un'applicazione chatbot sviluppata da OpenAI che utilizza vari modelli di GPT (Generative Pre-trained Transformer) per generare testo in modo autonomo. Le versioni di GPT, come GPT-3.5 e GPT-4, rappresentano il "cervello" del chatbot, l'intelligenza artificiale che permette a ChatGPT di riconoscere, comprendere e generare testo in modo simile a quello umano.

Copilot

ChatGPT-3.5 vs ChatGPT-4

Caratteristica	ChatGPT-3.5	ChatGPT-4
Architettura e Parametri	175 miliardi di parametri, principalmente NLP	Architettura avanzata con capacità multimodali (>100000 miliardi di parametri)
Capacità Multimodali	Nessuna capacità multimodale avanzata	Riconosce e descrive immagini, spiega battute visive, propone didascalie per foto, comprende grafici, diagrammi e testi scritti a mano
Prestazioni e Accuratezza	Elabora fino a 16.000 token in un singolo prompt	Elabora fino a 128.000 token in un singolo prompt, risposte più accurate del 40% rispetto a GPT-3.5
Applicazioni e Utilizzo	Utilizzato per applicazioni NLP come traduzione, risoluzione di problemi logici e matematici	Utilizzato per una vasta gamma di applicazioni con interazioni utente più naturali e versatili