CCR

Riunione Plenaria DSI – Milano
3/12/2024

Alessandro Brunengo

Indice

- Bilancio
- Infrastruttura
- Disciplinare
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

- Bilancio
- Infrastruttura
- Disciplinare: modifiche rilevanti, approvazione
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

Bilancio 2025

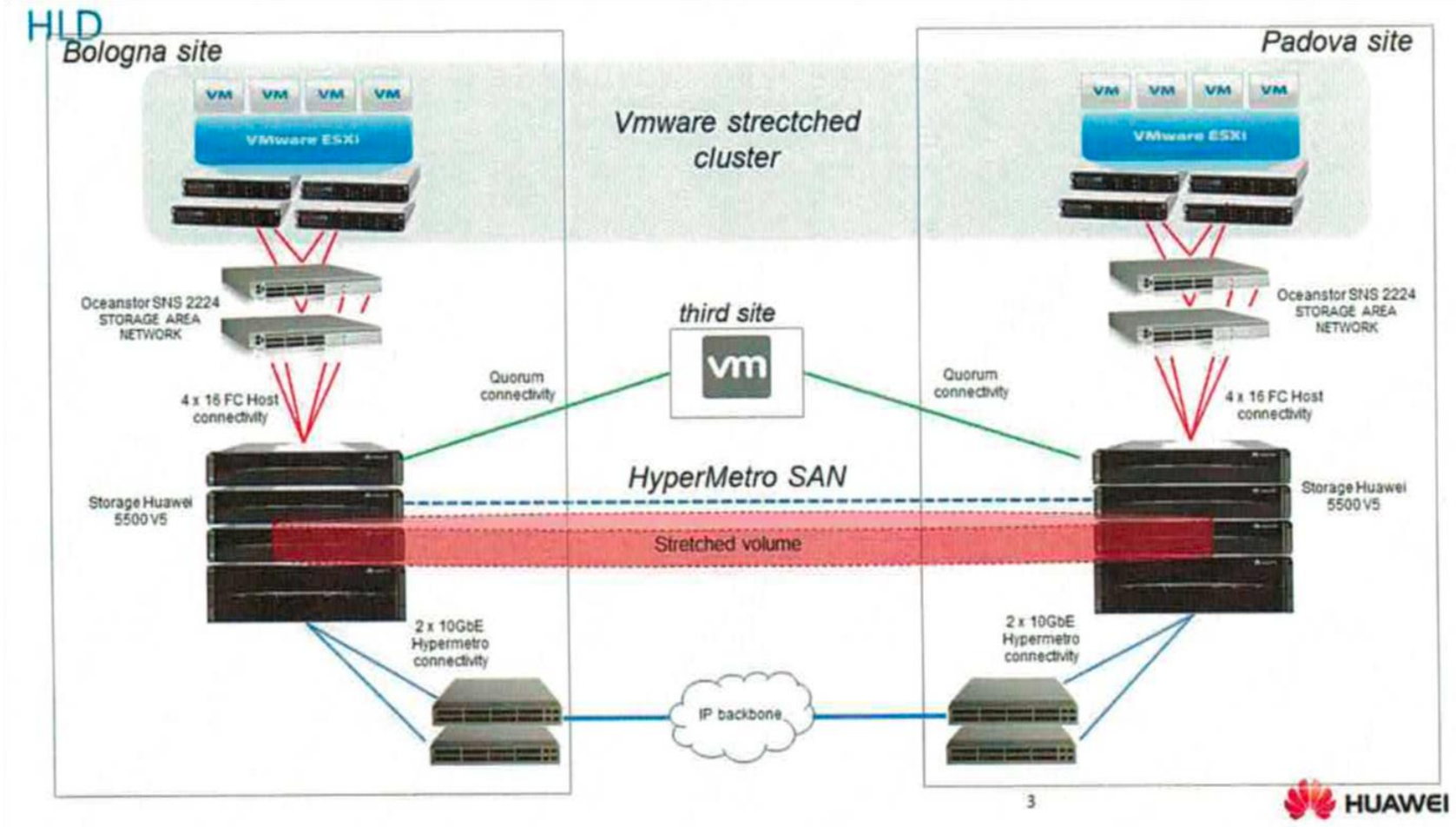
- Richieste alla Giunta:
  - 2175 k€ bilancio ordinario (include 1190 k€ di licenze sofwtare)
  - 700 k€ straordinario per sostituzione storage della BC

- Finanziamenti assegnati: 985 k€
  - potenziamento, attivita' dei gruppi, manutenzioni
- Non ancora confermati:
  - 1190 k€ licenze software: ipotesi finanziamento in due parti
  - 700 k€ storage per la BC: da definire

  Spese non comprimibili, mi aspetto che verranno finanziate

- Bilancio
- Infrastruttura
- Disciplinare: modifiche rilevanti, approvazione
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

Schema dell'infrastruttura di BC



Infrasrtruttura BC

- Risorse: immutate dell'ultima volta
  - nodi: 15 lame, 576 core, 6.6 TB RAM (per sito)
  - storage: 100 TB block storage, 200 TB NAS storage

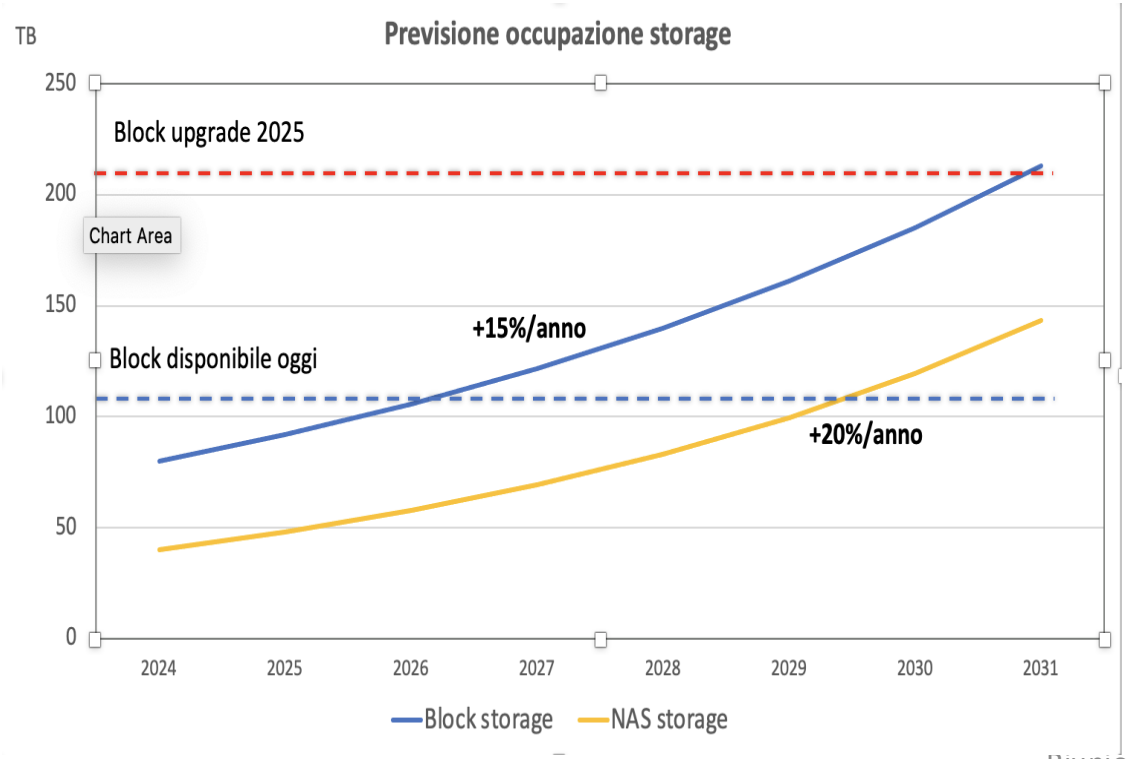
- Occupazione:
  - nodi: RAM ~5 TB (~ 75%)
  - storage: 80 TB block (80%), 40 TB NAS (20%), entrambi thin provisioning

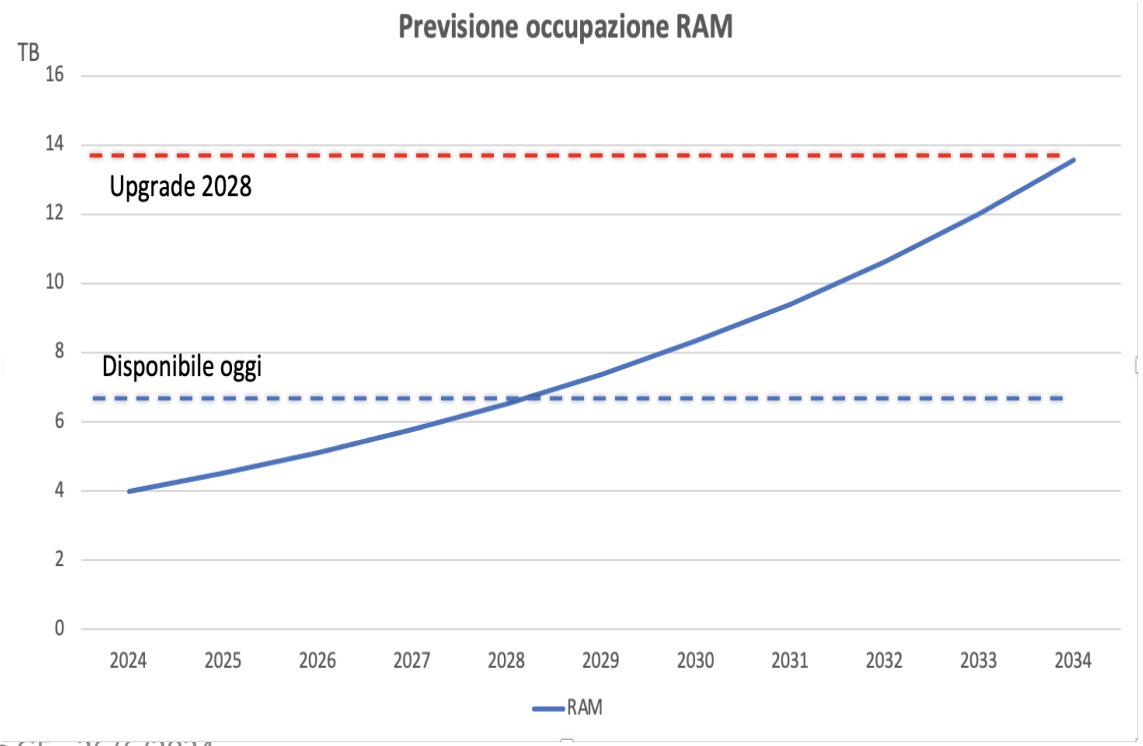
- Criticita'
  - storage da sostituire: 7 anni, elevato costo di manutenzione
    - pianificato per il 2025 rinnovo 220 TB block + 200 TB NAS
  - nodi: siamo al limite
    - probabile acquisto di lame nel corso del 2025
  - costi elevati
    - modello di finanziamento penalizzante
    - soluzioni tecnologiche forse non piu' economicamente sostenibili (blade)

Previsione esigenza di risorse

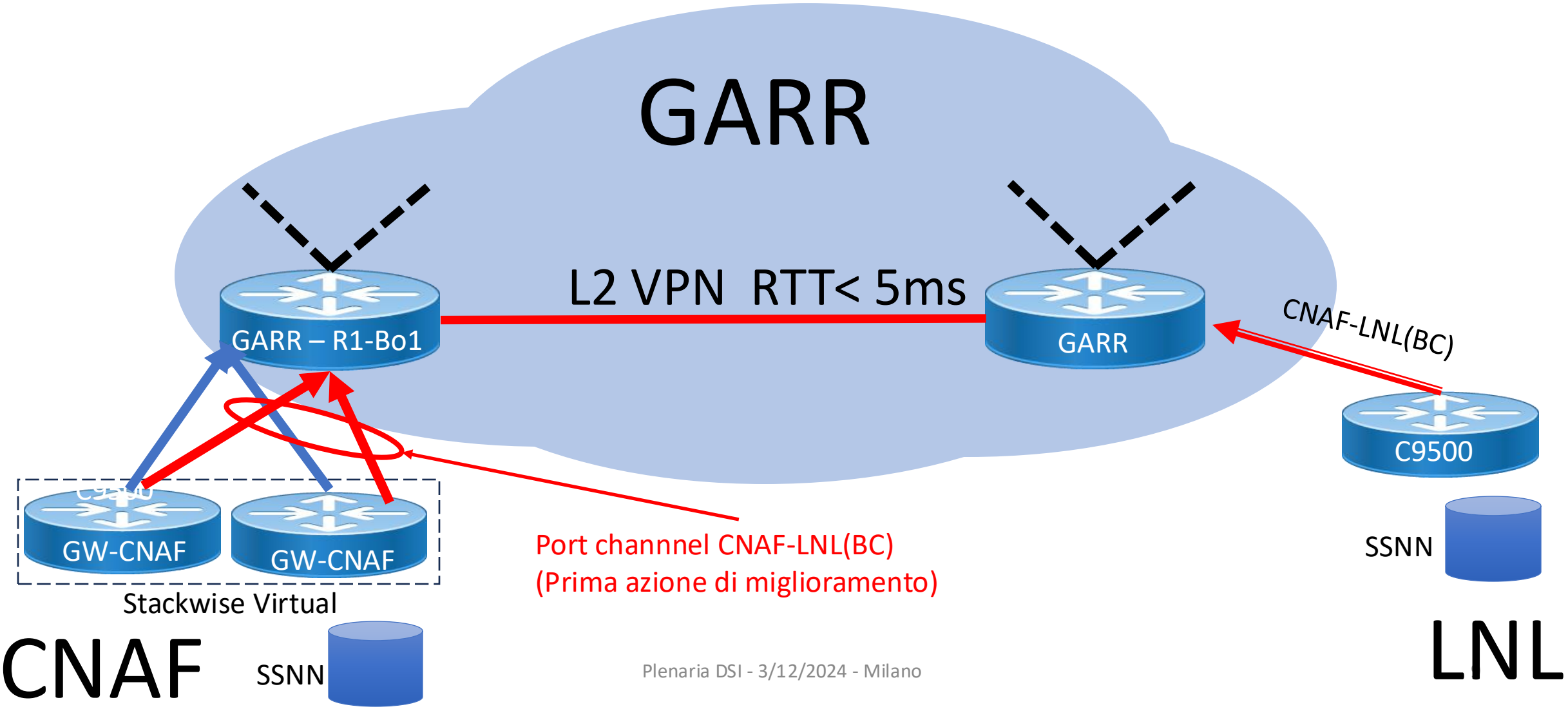
- Sostituzione storage nel 2025 per motivi di eta' (7 anni)
  - 220 TB block, 200 TB NAS
- Durata prevista: 6 anni

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





Situazione attuale



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.

Analisi

- La architettura implementa una HA che e' (quasi) anche DR
- Configurazione complessa
  - Di norma abbiamo spostamenti di VM quando muta lo stato della L2VPN
  - In un caso anche per "problemi di routing" non chiari a GARR
  - Modifiche di connettivita' sovrapposte generano reazioni che allungano i tempi e comportano restart multipli
  - Non sempre possibile correlare eventi consecutivi alle reazioni automatiche
- Il problema principale e' che lo spostamento delle VM non e' trasparente
  - failure nel restart della VM o dei servizi erogati
- I tempi di reazione (brevi) e i tempi di stabilizzazione (lunghi) espongono ad eventi sovrapposti

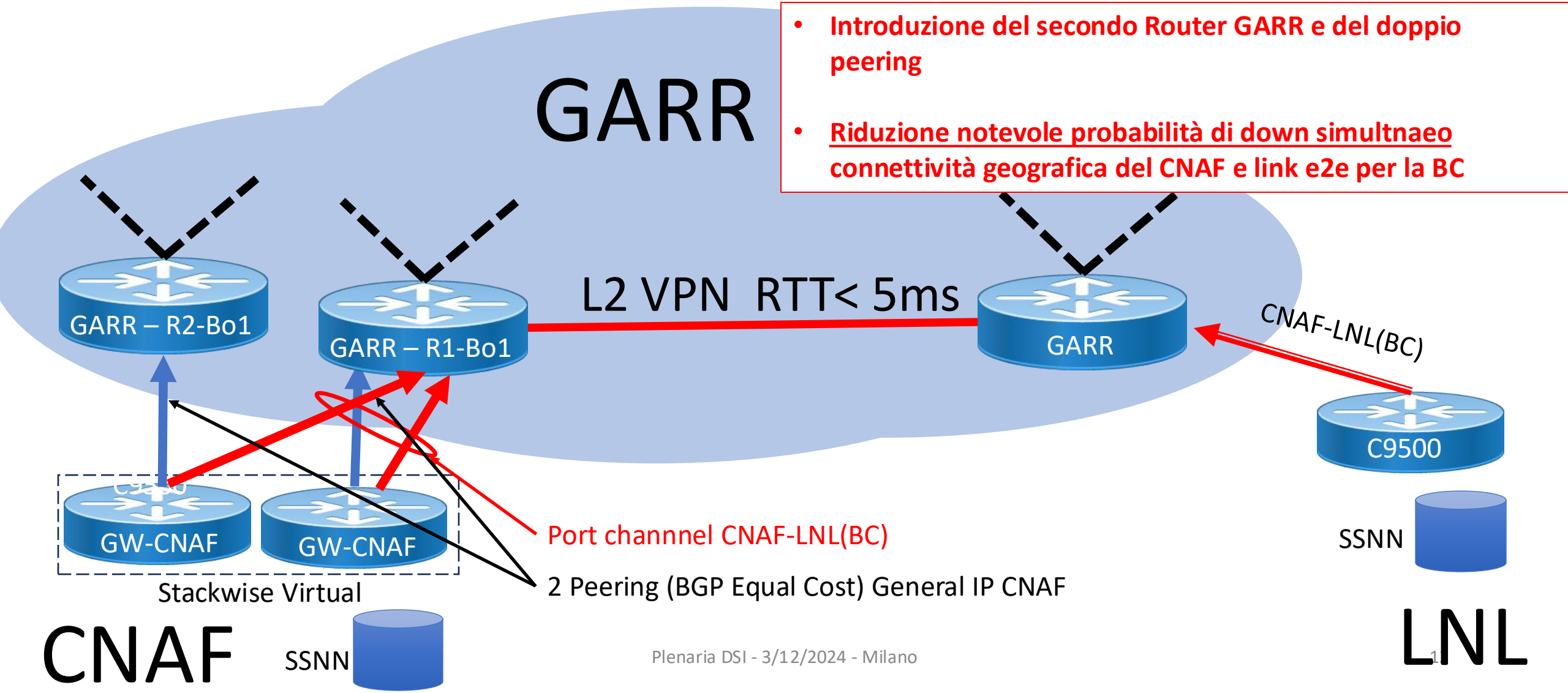
Strategie di mitigazione

- In discussione dopodomani

- Cambiare l'architettura dei siti da active-active a active-stand-by
  - tutto il carico al CNAF
  - spostamento delle VM solo in caso di disconnessione completa del CNAF
    - al netto di problemi di routing GARR non compresi
- Aumentare la ridondanza della connettivita' geografica al CNAF
  - dopo migrazione al tecnopolo (gennaio 2025)
- Valutare con GARR topologie ridondate per la L2VPN
  - questo potra' consentire un ritorno alla active-active

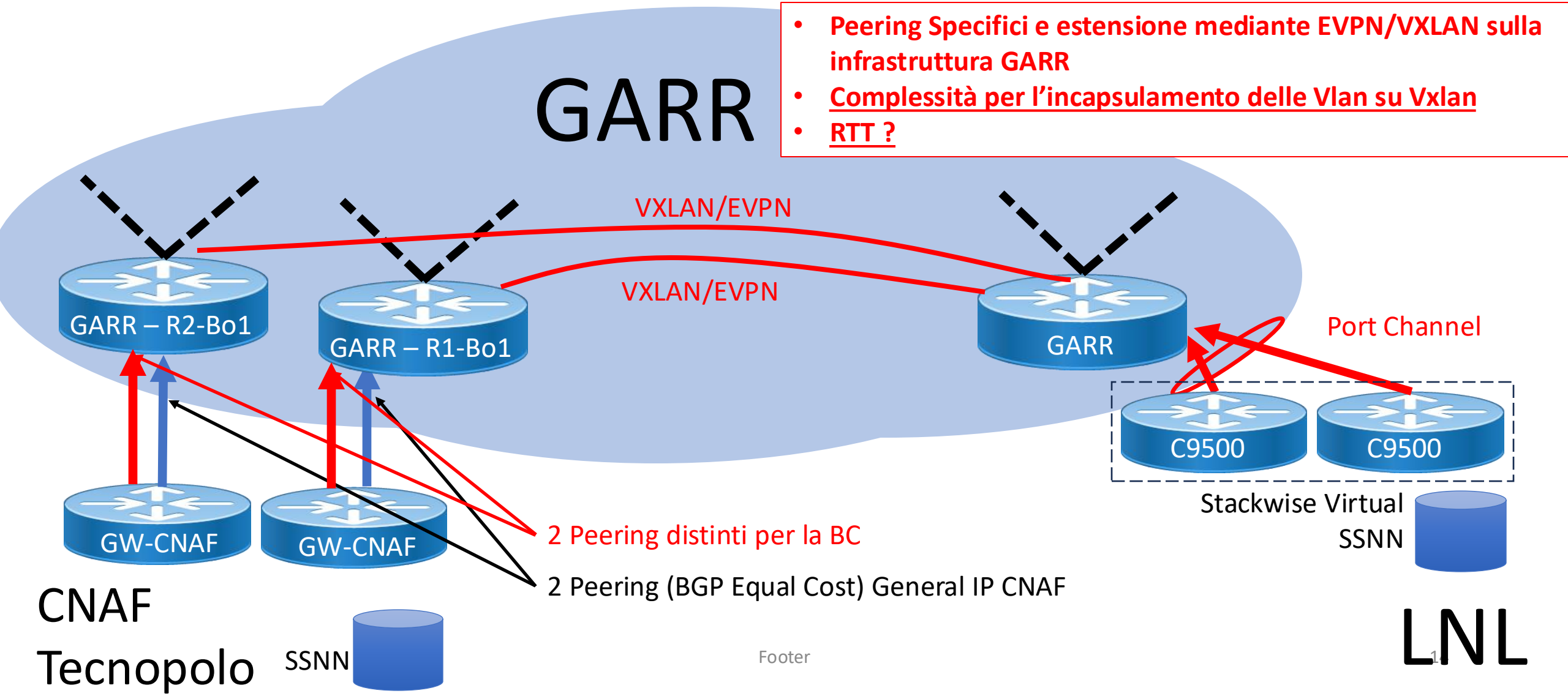
Evoluzione a breve

- **Introduzione del secondo Router GARR e del doppio peering**
- **<u>Riduzione notevole probabilità di down simultnaeo</u> connettività geografica del CNAF e link e2e per la BC**



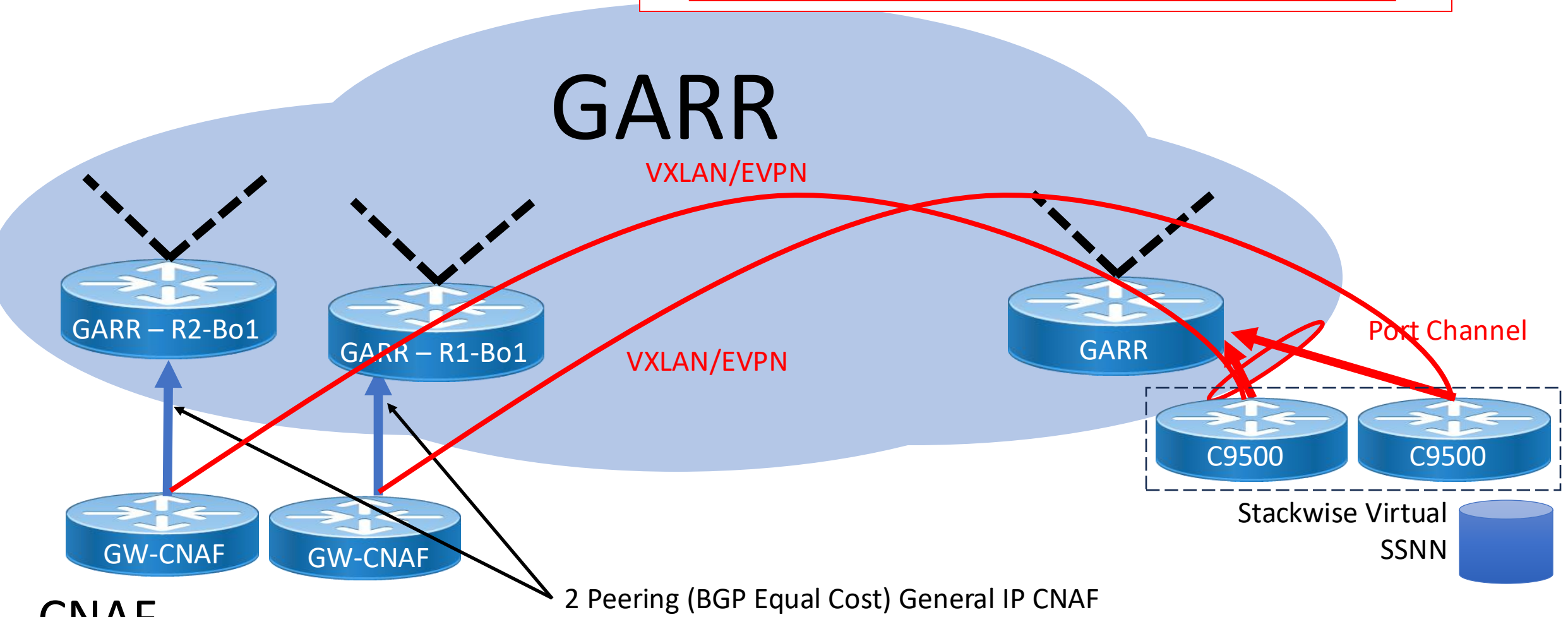
Ipotesi 3 Evoluzione da realizzare per il Tecnopolo (Ancora da discuterte ed approfondire con GARR)

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



Ipotesi 4 Evoluzion
(Ancora da discute

- **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 ?**



- Bilancio
- Infrastruttura
- Disciplinare
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

Disciplinare – dove eravamo...

- In fase di riscrittura il disciplinare di utilizzo delle risorse informatiche dell'Ente
- Struttura:
  - disciplinare piu' snello, con sole definizioni ed elementi di principio
  - riferimenti tecnici e specifici su documenti accessori
    - trattamento log, posta elettronica, cloud esterne, password, retention
  - nuovi elementi
    - categorizzazione dei dati, utenti esterni, BYOD
- Introduzione di nuove figure
  - CCR (non c'e'!)
  - Amministratori di servizio cloud

Cosa abbiamo fatto…

- Giugno: approvazione delega al Direttore Generale in materia di accesso alle risorse informatiche (DataCloud) dell'INFN da parte di utenti esterni
- Luglio: prima discussione bozza: suggerimenti del presidente di CCR
  - introduzione contesti delle risorse IT (Cloud, SSNN, DSI)
  - indicazione di CCR e del NUCS come sorgenti di policy di sicurezza
  - rimozione della figura di "referente delle risorse informatiche"
- Settembre: presentazione in riunione CCR della bozza
  - rimozione della distinzione tra risorse cloud/non cloud
- Ottobre: segnalazione da Ufficio Legale di possibili incompatibilita' con la bozza del nuovo codice di comportamento
- Ottobre: discussione in CCR e indicazioni sui temi aperti (vedi dopo)
- Dicembre: definizione dei gruppi di lavoro per i documenti tecnici allegati
  - BYOD/COPE, utilizzo cloud esterne, trattamento dei dati, use case che richiedono nomine ad amministratori di sistema

Compatibilita’ codice di comportamento

Bozza del codice di comportamento	Bozza del disciplinare
Il personale indicato nell’articolo 2 è tenuto a … utilizzare account istituzionali per i soli fini connessi all’attività lavorativa avendo cura di non compromettere la sicurezza o la reputazione dell’Istituto;	*L'utilizzo delle risorse informatiche per finalità personali è tollerato purché non violi le leggi applicabili, non interferisca negativamente con le infrastrutture e sia compatibile con le norme del presente Disciplinare e delle policy accessorie reperibili in …*

- Gli account sono un tipo di risorsa informatica
  - credenziali, identificativi (e-mail), storage associato, casella PEC, …
  - complesso differenziare l’uso di “account” dall’uso di “altre risorse”
- Deciso di adottare sul codice di comportamento l’interpretazione piu’ permissiva indicata nella bozza di disciplinare.
  - esplicitato nel disciplinare l’aspetto reputazionale.

Amministratore di servizio

	Amministratore di sistema	Amministratore di servizio
Definizione	*Figura professionale dedicata alla gestione e alla manutenzione degli impianti di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza;*	*un amministratore di sistema, che ha i privilegi necessari per la gestione di risorse DataCloud: istanziazione, aggiunta di utilizzatori e amministrazione di servizi;*
Compiti	*mantenere i sistemi al livello di sicurezza appropriato al loro uso; verificare con regolarità l'integrità dei sistemi; controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza; segnalare immediatamente al team responsabile delle risorse informatiche incidenti, sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione; installare e mantenere aggiornati programmi antivirus per i sistemi operativi che lo prevedono; non visionare dati personali o corrispondenza, salvo per necessità tecniche, e in generale considerare sempre tali informazioni strettamente riservate; in caso di interventi di manutenzione, impedire, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati; seguire attività formative in materie tecnico-gestionali, di sicurezza delle reti e di protezione dei dati personali.*	*gli amministratori di servizio devono rispettare le regole indicate nel ToU e AUP e in particolare: potranno dare accesso alle risorse assegnate dopo aver verificato che l'utente rispetti le condizioni indicate nell'articolo Accesso alle risorse informatiche; devono conservare l'associazione tra gli account e le identità degli utenti; non devono condividere l'accesso privilegiato alle risorse assegnate;*

- E' la stessa figura: specificare l'ambito di responsabilita' attraverso il contesto delle risorse amministrate indicato nella nomina ad amministratore di sistema.

Utenti privilegiato

	Utente con password privilegiata sul proprio device	**Utente privilegiato**
Definizione	non definito nel disciplinare	*utente di servizi DataCloud, che, pur non avendo ricevuto la nomina ad amministratore di servizio, ne ha comunque i privilegi, ma solo su risorse per le quali è stata bloccata la inbound connectivity;*
Compiti	*…sono tenuti a prendere visione dei relativi documenti con le Norme d'uso reperibili in …. e a seguirne le indicazioni;*	*I dati trattati dagli utenti privilegiati devono essere di tipo tecnico-scientifico: il trattamento di dati personali non deve essere significativo. Gli utenti privilegiati devono rispettare le restrizioni indicate nelle ToU e AUP e in particolare: non possono dare accesso alle loro risorse ad altri utenti; non devono interferire con il sistema di raccolta dei log; non devono cercare di aggirare le misure di isolamento delle risorse assegnate.*

- E' la stessa figura: si definisce la figura, con gli obblighi

Inoltro automatico della posta elettronica

- Dettaglio tecnico: consentire o non consentire?
- Problemi connessi all'utilizzo del forward
  - SPAM reflector
  - Riservatezza dei documenti e dei contenuti
  - Incompatibilita' con protocolli SPF (risolvibile)
- Problemi connessi alla proibizione del forward
  - reperibilita' del dipendente in quiescenza
  - problemi sociologici (alcuni utenti lo vogliono fortemente)
  - pregresso: da valutare l'attuale diffusione della pratica
- Analisi in corso per il dimensionamento del problema (orizzontale e verticale)
- Orientamento e' non consentire

Documenti accessori

- Citati esplicitamente nella bozza:
  - AUP e TOU per l'uso delle risorse cloud: a cura di DataCloud: gia' disponibili
  - Norme d'utilizzo per i sistemi a uso tecnico-scientifico: gia' disponibili (revisione?)
  - Utilizzo di cloud esterne: a cura di gruppo interno CCR
  - Informativa sul trattamento dei dati acquisiti per l'accesso alle risorse informatiche: a cura del DPO
  - Policy per l'uso dei dispositivi BYOD e COPE: a cura di gruppo interno a CCR
- Non citati esplicitamente
  - Il disciplinare prevede la presenza di altri documenti di policy non esplicitamente citati

Piano approvazione disciplinare

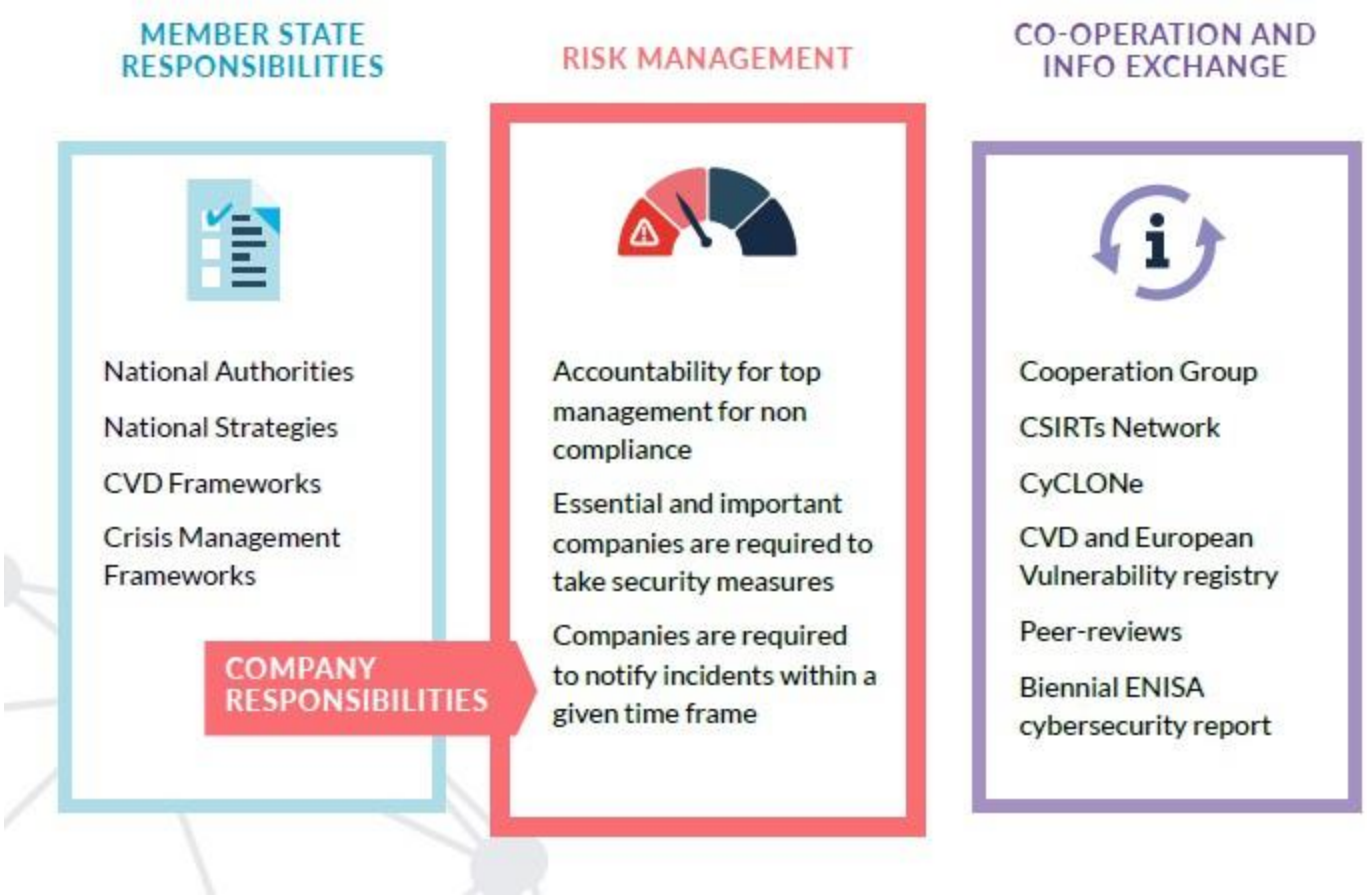
- Meta' gennaio: completamento dei documenti accessori
- Fine gennaio: bozza definitiva approvata in CCR
- Meta' febbraio: presentazione in Giunta Esecutiva
- Fine febbraio: approvazione nuovo disciplinare in CD

  - indeterminazione: +/- 1 mese

- Bilancio
- Infrastruttura
- Disciplinare
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

La NIS2

- This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union; to that end, this Directive lays down:
  - obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);
  - cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;
  - rules and obligations on cybersecurity information sharing;
  - supervisory and enforcement obligations on Member States



Risk Management Measures

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

All measures must:

- be proportionate to risk, size, cost, and impact & severity of incidents
- take into account the state-of-the-art, and where applicable relevant European and international standards

EU can:

- carry out risk assessments of critical ICT services, systems or supply chains
- impose certification obligations
- adopt implementing acts laying down technical requirements

Quasi tutte queste misure sono mappabili su controlli della ISO 27001:2022 (c'è chi l'ha già fatto) o del Cybersecurity framework del NIST: l'occasione è propizia per valutarne l'adozione.

Risk Management Measures nell'INFN

Piano di gestione del rischio informatico (da estendere con tool AGID/ACN – approccio multirischio) – WG Scansioni

INFN CSIRT (TI Listed), WG SOC & EDR

Misure Minime AGID (eventualmente adottando quelle di più alto livello); AUDIT interni

WG Scansioni: Linee guida AGID su SSL/TLS e HTTPS,SSH hardening. ***Crittografia MAIL?***

Dispiegamento 2FA iniziato (WG AAI); NUCS (CSIRT e SOC), DPO. AAI dispongono di canali di comunicazione OOB di emergenza

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

(Significant) incident notification/reporting

Article 23

…

3. An incident shall be considered to be **significant** if:
   a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
   b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Incident reporting nell'INFN

T0: scoperta incidente

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.it

SOC/EDR

CSIRT ITALIA

GARR CERT

EGI CSIRT

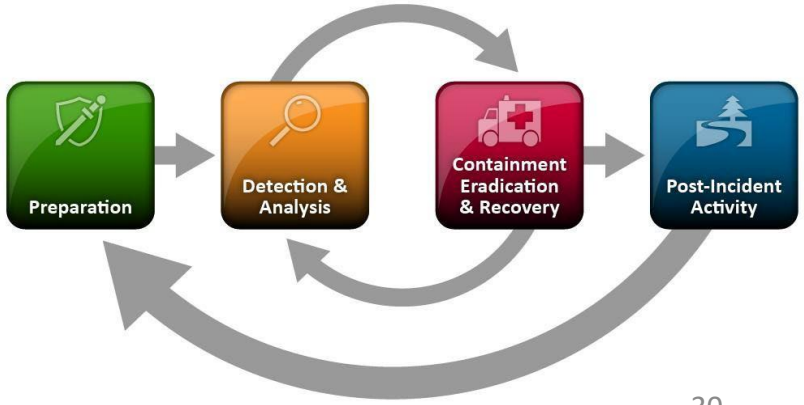
INFN CSIRT
e-mail, PEC, form web, keybase

24/72/1 mese

CSIRT ITALIA ACN (obbligo di risposta e supporto)

T0: ricezione notifica

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



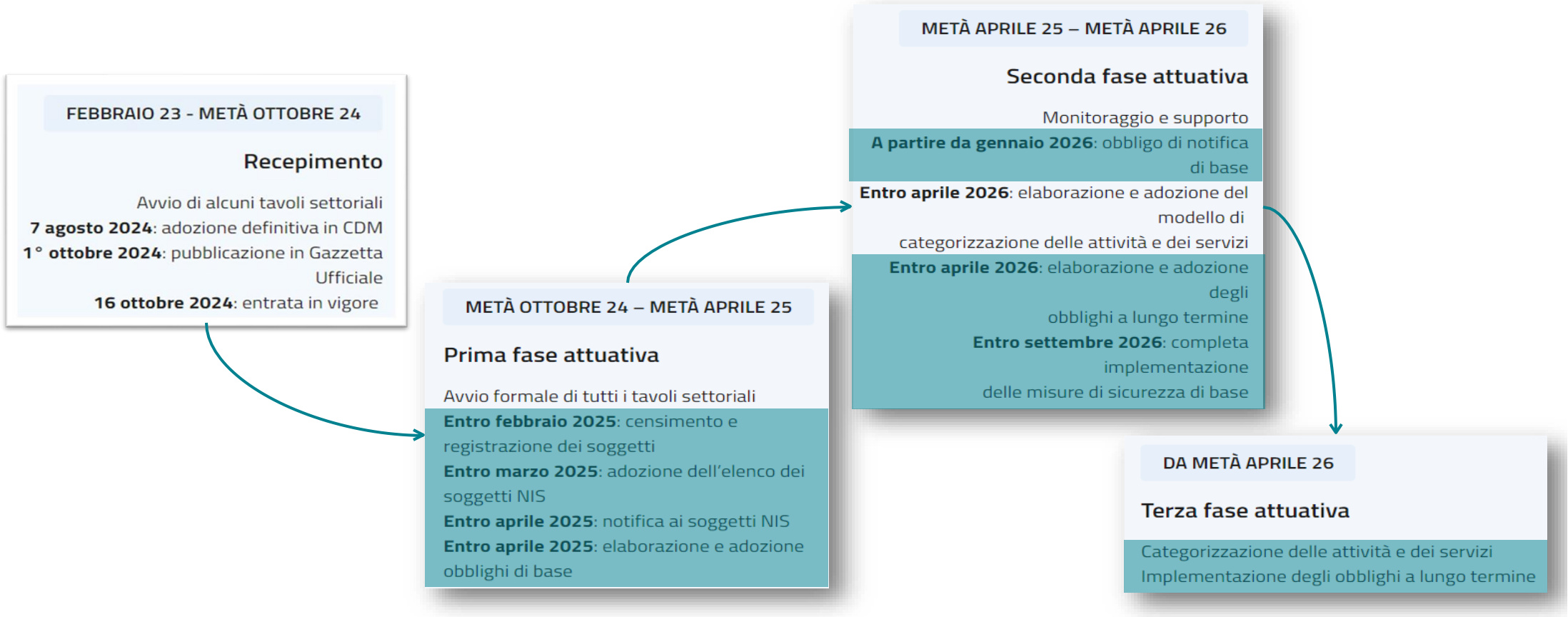
Management responsibilities

NIS2 porta la gestione della sicurezza informatica fuori dall'ambito più strettamente tecnico per farla entrare nella C-suite (CEO, ..) e renderla quindi ***una funzione attiva e strategica*** dell'ente; la formazione specifica in ambito di gestione del rischio per il management diventa un obbligo.

Gli stati membri possono imputare responsabilità personali agli organismi di gestione e, in caso di palesi non conformità in entità essenziali, comminare sanzioni o imporre divieti temporanei all'esercizio delle funzioni dirigenziali.

Possibile scenario: mancata (o ritardata) somministrazione di formazione sulle minacce derivanti dal social engineering in presenza di un rischio conclamato di phishing.

Timeline


FEBBRAIO 23 - METÀ OTTOBRE 24
Recepimento
Avvio di alcuni tavoli settoriali
7 agosto 2024: adozione definitiva in CDM
1° ottobre 2024: pubblicazione in Gazzetta Ufficiale
16 ottobre 2024: entrata in vigore
METÀ OTTOBRE 24 – METÀ APRILE 25
Prima fase attuativa
Avvio formale di tutti i tavoli settoriali
Entro febbraio 2025: censimento e registrazione dei soggetti
Entro marzo 2025: adozione dell'elenco dei soggetti NIS
Entro aprile 2025: notifica ai soggetti NIS
Entro aprile 2025: elaborazione e adozione obblighi di base
METÀ APRILE 25 – METÀ APRILE 26
Seconda fase attuativa
Monitoraggio e supporto
A partire da gennaio 2026: obbligo di notifica di base
Entro aprile 2026: elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
Entro aprile 2026: elaborazione e adozione degli obblighi a lungo termine
Entro settembre 2026: completa implementazione delle misure di sicurezza di base
DA METÀ APRILE 26
Terza fase attuativa
Categorizzazione delle attività e dei servizi
Implementazione degli obblighi a lungo termine

Siamo all'inizio del lavoro

- Governance
  - discussioni avviate con NUCS e RTD, da coinvolgere C3SN, DataCloud, DPO, (DSI)
  - in preparazione la proposta da discutere con il management
  - da definire un piano di formazione per il management
- Referente per la sicurezza informatica presso ACN
  - obbligo di legge (28/6/2024 n. 90)
  - in corso di nomina da parte del presidente
- Policy e procedure
  - nel complesso vengono soddisfatti i requisiti operativi
  - manca una definizione su carta delle procedure e responsabilita'

Attivita' operativa

- CSIRT
  - accreditamento del'INFN CSIRT come listed member del TF-CSIRT (Trusted Introducer)
  - scansioni:
    - aggiunti test specifici per le versioni ssh e protocolli SSL/TLS di web e mail server (vulnerabilita' CMS in corso)
    - sviluppata piattaforma web per la gestione self-service delle vulnerabilità
  - analisi di tool di valutazione del rischio
  - in corso di definizione acquisto servizio di pen-test
  - wishlist: campagna sul phishing

- SOC
  - EDR Microsoft in corso di dispiegamento
  - Attivita' R&D su strumenti (wazuh, ntop, zeek, security onion, ...)

Incidenti

- Il numero di incidenti segnalato allo CSIRT e' contenuto
  - c'e' il dubbio che non sempre si segua la procedura
  - ricordo che c'e' una procedura per gli incidenti informatici (https://www.csirt.infn.it/) ed una in caso di databreach (dpo.infn.it)

	2023	2024
Software piracy	14	6
DDOS/Net scan or probe	1	1
Utenze compromesse	13	7
SPAM/phishing/data breach (credenziali)	10 (3 da INFN)	15 (6 da INFN)
Data breach generico		1

Criticita’

- personale
  - persa una persona rilevante (coordinatore del SOC)
  - insufficiente partecipazione del personale delle sedi alla attivita’ nazionale
  - sovraccarico di impegni: coordinamento, CSIRT, certificazione EPIC, INFN Cloud: sempre le stesse persone

- budget
  - attivita’ finanziata sui fondi ordinari della CCR (qualche contributo dai fondi PNRR)
  - firewall, licenze, servizi, formazione, SOC: richiedono maggiori risorse

- Bilancio
- Infrastruttura
- Disciplinare
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

AAI – 2FA

- 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
- situazione attuale: ~350 utenti abilitati, in lenta crescita
  - rinnoveremo gli avvisi

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

AAI - todo list

- simpleSAMLphp versione2 (90% del lavoro già fatto)
- migrazione dei microservizi su OpenShift 4 (quando pronto)
- Aggiornamento userPortal per cambio password LDAP/Kerberos unificato
- Separazione completa Kerberos da AFS (adeguamento il sistema di gestione ARC)
- Contesti risorse IT ed adeguamento userPortal per la loro gestione
- SPiD Livello2 ed eIDAS
- AAI 2.0

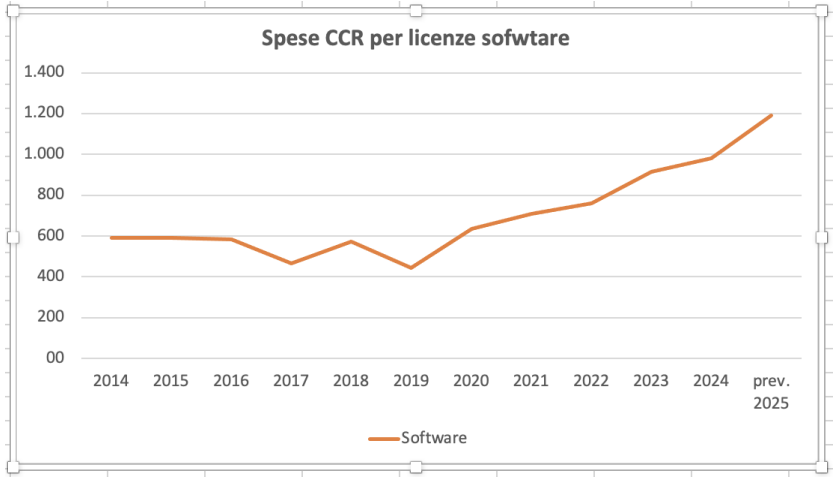
OKD

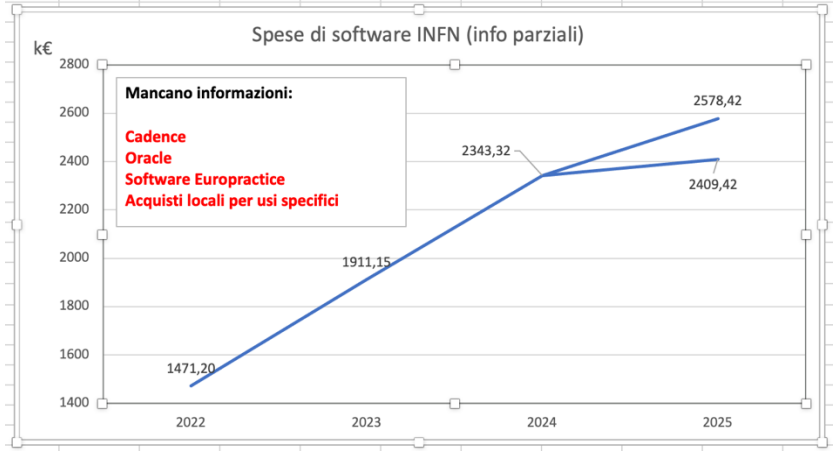
- Attivita completate:
  - preparazione infrastruttura per il deployment di openshift 4 (principalmente network/load balancers/dhcp/dns e servizi a contorno)
  - deployment del primo cluster openshift con automazione ed integrazione con il vCenter
  - test di carico e di funzionalità di autoscaling del cluster
- Attivita' in corso:
  - rifinitura permessi dei service account per interazione con vCenter
  - creazione cluster stage / prod
- Futuro:
  - Valutazione sistema di backup integrato di openshift
  - Migrazione servizi da okd3 a openshift 4
  - Migrazione delle pipeline di deployment

- Bilancio
- Infrastruttura
- Disciplinare
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

Licenze sofwtare

- Spese in costante aumento
- Proposto alla Giunta un processo che permetta un controllo globale
  - acquisti dimensionati il luglio, approvato in settembre nelle CSN e CCR
  - nessuna assegnazione locale ma assegnazione diretta a CCR che si occupa delle contrattazioni
    - risolve il problema degli storni
  - Da implementare anche per gli acquisti delle strutture (progettazioni, etc.)
- Quest'anno prima prova, per ora perfettibile





Software - varie

- Atlassian: acquisto anticipato su fondi 202
  - estensione della scadenza (31/1 ->28/2)
  - aumento licenze JSM (750).

- Alfresco:
  - disponibile da mesi una installazione della versione 7 per l'upgrade: apparentemente lavori fermi
  - disponibile una installazione di Alfresco 23 per test su connettori O365
  - ipotesi: passare direttamente alla versione 23?
    - il salto 7 -23 non dovrebbe essere un problema complesso per Reindex
  - non e' prorogabile all'infinito, se non c'e' intresse a migrare dobbiamo trovare altra soluzione
    - ... breve discussione? …

- VMware: dopo l'acquisizione Broadcom cambia license model
  - da licenze perpetue con manutenzione a licenze a noleggio, a core
  - potenziali incremento insostenibile (ipotesi 30-40 €/core -> da 53 k€ a 290-390 k€)
  - probabile mantenimento solo sulla infrastruttura dei SSNN (~ 75-100 k€)

- Bilancio
- Infrastruttura
- Disciplinare
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

Formazione

- Presentato il piano formativo CCR per il 2025
  - Rinnovo contratto Coursera
  - Attivazione contratto con piattaforma Udemy

- Problema recente su Coursera
  - frontend di accesso alla piattaforma sviluppato con BudiBase
    - versione OpenSource e self hosted
  - recente update del core (nonostante gli update fossero disabilitati)
    - rimosso accesso diretto degli utenti alle app
    - necessaria una richiesta esplicita degli utenti a CCR_Formazione (F. Zani)
    - possibile che a breve vengano imposti altri limiti (numero di utenti < 20)
  - opzioni:
    - acquistare licenza BudiBase (~10-20 k€/anno per 2 sviluppatori)
    - sviluppare internamente
    - commissionare sviluppo all'esterno
  - problema non risolto

- Bilancio
- Infrastruttura
- Disciplinare
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

ASW – siti web

- Attivita' portata avanti da CCR e UC
- www.infn.it quasi completo
  - inserimento entry in Italiano quasi completo (news, newsletter, ...)
  - traduzione in inglese in corso (incaricata una azienda)
  - pubblicazione del nuovo sito prevista per fine dicembre/inizio gennaio
- "declinazioni"
  - laboratori: mockup e grafica completi, installazione sito di test la prossima settimana
  - sezioni: mockup e grafica completi, andiamo in test dopo il lavoro sui laboratori (gennaio)
  - commissione e altre strutture: un po' piu' indietro
    - ma il lavoro su laboratori e sezioni verra' sfruttato
- Criticita': plugin
  - l'azienda ha deciso di fare lo sviluppo di un plugin per il SSO
    - da verificare funzionalita' e solidita'
  - alcuni plugin a pagamento: da capitolato devono darceli licenziati
  - manca un phonebook INFN

- Bilancio
- Infrastruttura
- Disciplinare
- NUCS
- AAI/OKD
- Sofwtare
- Formazione
- ASW

Discussione/Domande