Regione Campania

Tech Strategy Regionale sulla Cybersecurity

fonte: http://burc.regione.campania.it

Sommario

1 Premessa

1.1 Data Center Regionale

Il potenziamento del Data Center "Don Bosco" della Regione Campania rappresenta un passo fondamentale nel percorso di trasformazione digitale delle Pubbliche Amministrazioni (PA), con l'obiettivo di migliorare i servizi offerti a cittadini, imprese ed enti locali. Questo percorso si inserisce nel contesto degli obiettivi fissati dalla normativa europea e nazionale e recepiti dalla Strategia Digitale della Regione Campania, approvata con Delibera di Giunta regionale n. 226 del 27 Aprile 2023, con l'obiettivo di supportare il processo di crescita dell'intero ecosistema digitale regionale verso più elevati standard qualitativi e di promuovere l'adozione di più efficienti modelli organizzativi dell'amministrazione regionale.

Il Data Center di una PA, come quello della Regione Campania, rappresenta il cuore pulsante della trasformazione digitale, poiché garantisce la continuità operativa, la gestione sicura dei dati, e la disponibilità di risorse critiche per l'erogazione di servizi. Un'infrastruttura moderna, sicura, affidabile e sostenibile è essenziale per:

- Gestire i dati e i servizi digitali in modo efficiente;
- Offrire servizi avanzati ai cittadini e alle imprese (sanità digitale, trasporti, lavoro);
- Garantire la sicurezza dei dati,

Il contesto normativo gioca un ruolo chiave nell'evoluzione del Data Center regionale, con obblighi derivanti da normative europee e nazionali che stabiliscono i requisiti minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità. Tra le normative più rilevanti:

- NIS 2 Directive (Network and Information Security 2) che impone standard più elevati di sicurezza informatica per le infrastrutture critiche, comprese quelle gestite dalle PA, rendendo obbligatorio un maggiore coordinamento e condivisione delle informazioni sulle minacce.
- Cybersecurity Act (Regolamento UE 2019/881), che istituisce un quadro comune di certificazione della sicurezza informatica per i servizi e i prodotti digitali in Europa, contribuendo ad aumentare la fiducia nella cybersicurezza delle infrastrutture pubbliche.
- Legge 28 giugno 2024, n. 90, che aggiorna il quadro normativo in materia di sicurezza informatica e protezione dei dati, allineandosi ai più recenti sviluppi europei.
- AGID - ACN: stabiliscono i requisiti minimi per la sicurezza, la capacità elaborativa e l'affidabilità delle infrastrutture digitali della PA nonché per la qualificazione delle infrastrutture come cloud per la PA, con particolare attenzione ai dati ordinari e critici.

L'iniziativa di riqualificazione del Data Center della Regione Campania è un processo strutturato che ha avuto inizio nel novembre 2021, attraverso l'istituzione dell'Ufficio Speciale per la crescita e la transizione digitale con l'inserimento di nuovo personale specializzato. Questo percorso, descritto nel progetto "Modello Data Center 2.0", ha posto le basi per la modernizzazione dell'infrastruttura IT secondo standard europei e nazionali, puntando su sicurezza, efficienza energetica, sostenibilità economica e affidabilità.
Di seguito alcune delle principali attività svolte:

- Censimento completo delle infrastrutture, inclusi impianti elettrici, dispositivi di rete, sistemi di monitoraggio, server fisici e applicativi;
- Implementazione di un sito di Disaster Recovery a Fisciano, "gemello digitale" del sito primario di via Don Bosco dotato di 1320 TB di storage e supporta il backup di 1700 V;
- Aumento delle risorse tecnologiche: da 50 a 300 server fisici, da 500 terabyte a 3000 TB di spazio dati e da 1000 a 2000 sistemi;

- Introduzione di soluzioni avanzate per la sicurezza informatica, tra cui politiche di autenticazione multifattoriale, backup sicuro tramite strumenti Backup & Replication, e soluzioni di backup immutabile per Office 365;
- Creazione di una rete metropolitana regionale con fibra a 100 Gbps e progetti WiFi su tecnologia di ultima generazione (WiFi 7);

l progetto "Modello Data Center 2.0" prevede quattro aree di intervento per l'evoluzione del Data Center:

1. Area Applicativa: aggiornamento del parco applicativo della Regione.
2. Area Sicurezza: prevenzione e contrasto delle minacce cyber.
3. Area Infrastrutturale: potenziamento ed evoluzione della struttura fisica del Data Center.
4. Area Governance e Organizzazione: gestione flessibile e agile del Data Center per una gestione efficiente.

In particolare, la cybersicurezza è un pilastro cruciale per il Data Center della Regione Campania, in considerazione del grado di criticità e sensibilità dei dati trattati (sanità, lavoro, trasporti, cultura). Il percorso di trasformazione relativo all'Area Sicurezza prevede:

- Protezione delle infrastrutture IT da attacchi informatici sempre più sofisticati, attraverso sistemi avanzati di monitoraggio e rilevamento delle minacce;
- Implementazione di politiche di autenticazione multifattoriale e accessi condizionati per ridurre i rischi legati all'identità digitale;
- Piani di backup sicuro e immutabile per garantire la protezione e il recupero dei dati in caso di incidenti o attacchi;
- Piani di Disaster Recovery con un'infrastruttura di Data Center "gemello digitale" a Fisciano, per garantire la continuità operativa anche in caso di eventi critici.

Le certificazioni ISO 9001, ISO/IEC 27001, ISO 27017 e ISO 27108 recentemente ottenute dal Data Center sono un riconoscimento della conformità ai più alti standard di gestione della qualità e della sicurezza delle informazioni. Inoltre, l'infrastruttura cloud ibrida in via di qualificazione sarà conforme ai requisiti del Regolamento, adottato da ACN con Decreto Direttoriale n. 21007/24 del 27 giugno 2024 e applicabile dal 1 agosto 2024, garantendo la gestione sicura sia dei dati ordinari che di quelli critici.
L'evoluzione del Data Center regionale verso un'architettura iper-convergente e integrata con un Software Defined Data Center (SDDC) e un'infrastruttura cloud ibrida, rappresenta una strategia avanzata per garantire l'efficienza, la sostenibilità e la sicurezza informatica. Questo processo si allinea pienamente con le normative europee e nazionali, e posiziona la Regione Campania come un modello per le altre PA italiane, nel percorso verso una digitalizzazione sicura e avanzata.

1.2 CSIRT/SOC Regionale

Il ruolo del CSIRT (Computer Security Incident Response Team) all'interno della Pubblica Amministrazione (PA) diventa sempre più centrale, soprattutto in un contesto caratterizzato da crescenti minacce informatiche e da un quadro normativo sempre più stringente. Le recenti disposizioni europee, come la Direttiva NIS2 e normative italiane, impongono obblighi precisi sulla sicurezza delle reti, dei sistemi informativi e sulla protezione dei dati, obbligando le amministrazioni a dotarsi di strumenti adeguati alla prevenzione, gestione e risposta agli incidenti informatici.
Il CSIRT svolge un ruolo chiave nella difesa della PA, attraverso una serie di compiti fondamentali:

1. **Prevenzione e mitigazione del rischio**: analizza costantemente i dati relativi alle minacce emergenti, supportando le amministrazioni locali nell'implementazione di processi di gestione della sicurezza e di prevenzione degli attacchi.
2. **Gestione degli incidenti informatici**: il CSIRT interviene nella risoluzione di crisi cibernetiche, fornendo un supporto immediato per la mitigazione degli effetti di attacchi cyber, minimizzando l'interruzione dei servizi pubblici essenziali.
3. **Diffusione tempestiva di informazioni**: è in prima linea nella condivisione di informazioni riguardanti nuove minacce, attacchi in corso e tendenze relative ai fenomeni cyber, garantendo che le Pubbliche Amministrazioni locali siano costantemente aggiornate su come fronteggiare i nuovi rischi.
4. **Conformità alle normative**: il CSIRT aiuta le PA a rispettare le normative vigenti, come la NIS2 e il perimetro di sicurezza nazionale cibernetica, che prevedono obblighi di notifica e l'adozione di misure di sicurezza da parte degli operatori classificati come essenziali o importanti.
5. **Collaborazione e coordinamento**: agisce come punto di contatto tra le amministrazioni locali e gli organismi nazionali e internazionali (come l'ACN e il CSIRT Italia), potenziando la cooperazione nella difesa cibernetica.
6. **Formazione e sensibilizzazione**: promuove l'innalzamento delle competenze tecniche degli addetti alla sicurezza informatica, migliorando la capacità delle PA di gestire minacce complesse e di sensibilizzare il personale sull'importanza della cyber-resilienza.

Con l'incremento degli attacchi informatici rivolti a infrastrutture critiche, come la sanità e i trasporti, il CSIRT regionale diventa uno strumento strategico per garantire la continuità operativa dei servizi pubblici, proteggere i dati e difendere l'integrità dei sistemi IT. La creazione e il potenziamento dei CSIRT regionali, come sottolineato dal PNRR e dalla Strategia Nazionale di Cybersicurezza, rappresentano dunque un tassello imprescindibile per una trasformazione digitale sicura e resiliente delle Pubbliche Amministrazioni.

L'Agenzia per la Cybersicurezza Nazionale, che ospita il CSIRT Italia, ha adottato le "Linee Guida per la realizzazione di CSIRT", prot. n. 21392 del 07/08/2023, aggiornate il 24 luglio 2024, rivolte alle organizzazioni che intendono istituire o potenziare un Cyber Security Incident Response Team (CSIRT), seguendo le migliori prassi e standard internazionali. Le linee guida definiscono i requisiti per squadre di pronto intervento informatico, dedicate al rilevamento, all'analisi, alla risposta agli incidenti di sicurezza informatica e allo svolgimento di attività di prevenzione e mitigazione del rischio cyber.

La Regione Campania ha implementato un sistema di sicurezza informatica per proteggere i propri sistemi informativi e, contestualmente, ha integrato all'interno dell'Ufficio Speciale per la Crescita e la Transizione al Digitale personale con competenze specifiche nella gestione digitale dei sistemi informativi. Con il Decreto Dirigenziale n. 139 del 12/10/2022, è stato istituito il Security Operation Center (SOC), composto da personale interno con esperienza nel campo della sicurezza informatica. L'obiettivo del SOC è rafforzare la resilienza cibernetica dei servizi critici offerti ai cittadini, in particolare nei settori dei trasporti e della sanità, attraverso la protezione degli asset, delle infrastrutture IT e dei sistemi che supportano tali servizi da minacce cyber.

In linea con la Strategia Nazionale di Cybersicurezza 2022-2026 e il Piano Operativo per la Digitalizzazione della Regione Campania 2023-2025, l'Amministrazione regionale ha l'intenzione di istituire CSIRT/SOC Regionale Federato, che faciliti la cooperazione tra diverse regioni o enti locali, con il ruolo di coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo cyber nell'ambito del dominio costituito dalle Pubbliche Amministrazioni Locali (PAL);

In particolare, le attività critiche dei CSIRT regionali comprendono, limitatamente alle proprie constituency, una serie di servizi, tra cui:

- fornire supporto nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
- agevolare la diffusione di informazioni tempestive su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cyber indirizzati a specifici settori e possibili impatti per le PAL e la loro utenza;
- incentivare a livello locale l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite a livello nazionale;
- facilitare le attività di prevenzione e monitoraggio sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale, mediante azioni di aggregazione dei servizi per le PAL;
- collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle PAL in materia di cyber security;
- accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi.
- aiutare le PAL a conformarsi alle normative vigenti in materia di sicurezza informatica, come la direttiva europea NIS e NIS2 e il decreto italiano sul perimetro di sicurezza nazionale cibernetica, che prevedono l'obbligo di notifica e di adozione di misure di sicurezza per gli operatori classificati come essenziali o importanti.

2 Obiettivi del documento

Questo documento ho lo scopo di delineare le linee guida strategiche di Regione Campania per le architetture ICT delle organizzazioni regionali, in termini di cyber security. La guida mira a determinare un modello comune ed integrato di sviluppo per le principali organizzazioni pubbliche regionali, basato sulle normative nazionali e comunitarie, best practices, armonico con gli investimenti correnti e futuri, basati sulle pianificazioni di spesa dei fondi europei Regionali e PNRR nei prossimi tre anni.
Tale guida si rende opportuna affinché la spesa sia:

- efficiente in relazione alle possibili sinergie che si possono conseguire tra la strategia tecnologica della regione e quella delle singole organizzazioni ad essa collegate;
- efficace in relazione al conseguimento di un livello di livello minimo comune di maturità della cyber security di tutte le organizzazioni coinvolte ed in relazione all'adozione di best practices utili alla riduzione del rischio di adozione delle tecnologie.
- conforme alle raccomandazioni di legge e a quelle dei principali istituti di indirizzo interazionale.

Per modelli strategici basati sulle normative a cui più spesso si fa riferimento, si rimanda al paragrafo 5.2

3 Modelli Strategici per la cyber security

Di seguito sono descritti i modelli a cui fare riferimento in relazione alle tre principali sfide che si prospettano nel prossimo futuro.

3.1 Modello per la resilienza e la sicurezza di servizi multi-cloud

L'adozione di tecnologie cloud in Italia si attesta nel 2023 al 19% per un valore totale di 5,51ML€. (Osservatori Digitali Politecnico di Milano) e promette ulteriore aumento in relazione alla strategia nazionale basata sul PSN. Questa crescita attesta e consolida i benefici dell'utilizzo del cloud nelle sue molteplici declinazioni. Tuttavia, l'adozione di servizi cloud, anche se minimali, necessita di grande attenzione principalmente in relazione all'organizzazione dei processi e alle tematiche di sicurezza. L'ultimo report di IBM Ponemon Institute, relativo al costo dei data breach, asserisce che l'82% delle violazioni sui dati impatta quelli immagazzinati in cloud. In particolare, ciò accade nel caso in cui l'organizzazione oggetto dell'attacco adotta strategie IT multi-cloud ed hybrid cloud. Per definire una strategia nel caso di adozione di architetture cloud occorre fare riferimento al modello di responsabilità condivisa rappresentato in Figura 1. Questo modello determina le responsabilità relative alle funzioni di sicurezza in dipendenza del modello di servizi cloud che si intende adottare.

Figura 1 Modello di responsabilità condivisa

L'adozione di un servizio cloud implica che le responsabilità concernenti la sicurezza e la resilienza del sistema siano condivise tra utente e fornitore del servizio. Come conseguenza, l'organizzazione che usufruisce del servizio deve avere consapevolezza del proprio dominio di responsabilità e delle responsabilità del fornitore nell'ottica più generale della sicurezza della supply chain. (*La "sicurezza della supply chain" si riferisce all'insieme di pratiche, politiche e tecnologie finalizzate a proteggere l'integrità, la confidenzialità e la disponibilità dei componenti, dei materiali e delle informazioni che compongono la catena di approvvigionamento di un'organizzazione. Una supply chain comprende tutte le fasi coinvolte nel processo di produzione e distribuzione di beni o servizi, dalla selezione dei fornitori fino alla consegna ai clienti finali.)*
Risulta quindi evidente che in tali scenari, infrastrutture, dati e applicazioni sono gestite in parte dall'organizzazione, on premise ed in cloud, ed in parte sono gestite dal/dai fornitore/fornitori di servizi cloud, complicando implementazione una strategia di sicurezza organica, integrata e soprattutto coerente.

Quindi, **Errore. L'origine riferimento non è stata trovata.**si espongono i seguenti casi di allocazione delle responsabilità.

- in caso di servizi SaaS a carico dell'ente, al cliente resta la responsabilità relativa alle informazioni trattate, ai device utilizzati dagli account e alle identità.
- In caso di servizi IaaS e PaaS, il cliente del servizio cloud acquisisce una infrastruttura virtuale, ne consegue che il fornitore del servizio cloud ha responsabilità che vanno dalla componente fisica fino alle piattaforme di virtualizzazione. Tutto il resto: dati, network, applicazioni, identità è piena responsabilità dell'utente del servizio, il quale, deve farsi carico di integrare le soluzioni di sicurezza in cloud con quelle on premise.

Statisticamente, a trascinare la crescita del cloud in Italia sono in particolare i servizi infrastrutturali (IaaS), che raggiungono in Italia, i 1,511 miliardi di euro (+29% sul 2022), arrivando a parimerito con la quota rappresentata dai servizi Software (SaaS), storicamente più diffusi (Osservatori Digitali Politecnico di Milano). Il caso IaaS risulta essere anche il più complesso in termini di architettura per l'organizzazione che sceglie di andare in cloud ma al contempo polarizza le responsabilità proprio sull'organizzazione che riceve il servizio, risulta quindi il meno complesso in termini di supply chain.
Lo sviluppo delle infrastrutture verso modelli multi-cloud sarà caratterizzato dalla presenza di uno o tutti i seguenti elementi:

- Cloud pubblici, come PSN, AWS, Azure, Google, che forniscono servizi Platform-as-a-Service (PaaS) o Infrastructure-as- a-Service (IaaS).
- Cloud pubblici (PSN) e privati, che ospitano applicazioni SaaS (Software-as-a-Service).
- Cloud ibridi che combinano data center on-premise con cloud pubblico o privato.

3.1.1 Modelli per la pubblica amministrazione e funzioni di sicurezza.

Per quanto attiene alla pubblica amministrazione italiana, con l'attivazione del Polo Strategico Nazionale, il governo, con le misure PNRR Missione 1, componente 1, investimento 1.1 (Cloud PA/Polo Strategico Nazionale) congiuntamente all'iniziativa 1.2 (Abilitazione e facilitazione migrazione al cloud), si è posto l'obiettivo di portare il 75% delle amministrazioni italiane ad utilizzare servizi in cloud entro il 2026. Il Polo ospiterà i dati ed i servizi critici e strategici di tutte le amministrazioni centrali (circa 200), delle Aziende Sanitarie Locali (ASL) e delle principali amministrazioni locali (Regioni, città metropolitane, comuni con più di 250 mila abitanti).
Al contempo, diversi enti regionali e società in-house si stanno attrezzando per certificare i propri datacenter nell'ottica di ospitare servizi in modalità cloud per le amministrazioni locali secondo come mostrato in Figura 2.

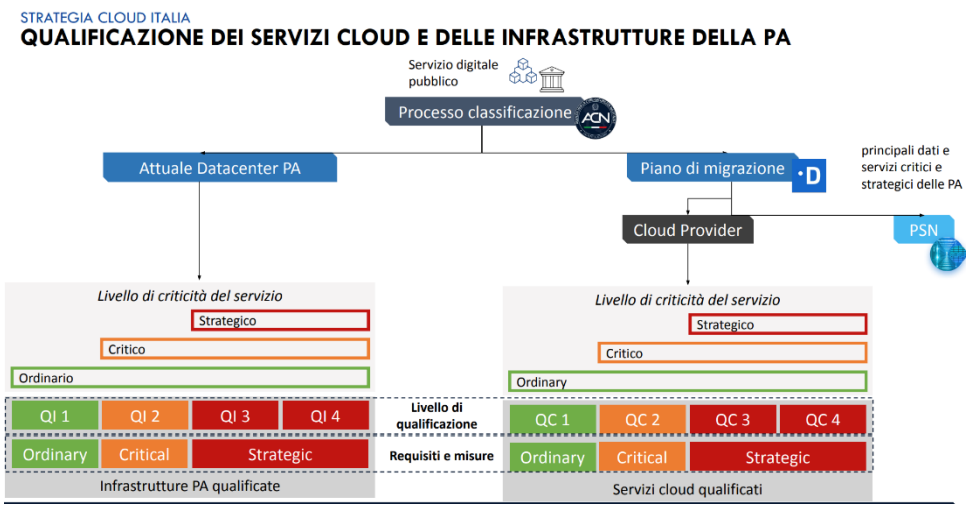


Figura 2: Destinazione uso datacenter certificati - (Dipartimento Trasformazione Digitale)

Nello scenario più articolato, una pubblica amministrazione può trovarsi in una situazione ibrida, in cui dati e applicazioni sono distribuiti tra datacenter on-premise, datacenter regionali e PSN/cloud pubblici. Ciò determina la necessità di avere il controllo sulla sicurezza su una infrastruttura distribuita e non omogenea.
In questa situazione ci sono degli elementi essenziali di sicurezza da affrontare, elementi che diventano critici per tutte quelle organizzazioni che ricadono nel perimento nazionale di sicurezza poiché soggetti alla normativa NIS2, e dal nuovo regolamento per la sicurezza degli elettromedicali MDR per le organizzazioni sanitarie.
In particolare, occorre affrontare le seguenti macro-sfide:

- **Espansione della superficie di attacco**: la migrazione verso il cloud espande la superficie di attacco e introduce complessità nella specificatamente in termini di supply chain; architetture estese come quelle determinate da ambienti multi-cloud ne complicano ulteriormente lo scenario di difesa.
- **Scarsa visibilità**: la distribuzione di dati ed applicazioni in modalità multi-cloud complica la visibilità delle operazioni; infatti, ogni infrastruttura cloud può assicurare la visibilità relativamente al servizio erogato; pertanto, si ha crea la necessità di mettere insieme le informazioni di ogni servizio cloud per ottenere la visione unificata delle operazioni e quindi delle minacce per valutarne immediatamente l'impatto sugli asset dell'organizzazione.
- **Mancanza di coordinamento**: L'assenza di integrazione tra le funzioni di sicurezza dei servizi cloud crea la necessità di una orchestrazione centralizzata al fine di determinare la possibilità di organizzare una risposta coordinata per mitigare l'impatto di minacce.

Ne consegue che, in un contesto complesso come questo che può derivare dall'adozione di servizi in modalità multi-cloud, è essenziale ridurre la complessità delle soluzioni impiegate e centralizzare il controllo delle policies di sicurezza e del monitoraggio degli eventi e delle attività
A conferma di ciò, l'analisi del 2023 di IBM Ponemon Institute, al fine di ridurre rischio ed impatti di un data breach, suggerisce di semplificazione le infrastrutture di sicurezza, consolidando ed integrando le tecnologie utilizzate, in modo da ridurre la complessità di gestione e abilitare l'automazione delle operazioni. In particolare, l'automazione e l'utilizzo degli strumenti di analisi come l'intelligenza artificiale.

3.1.2 Linee guida per la sicurezza delle infrastrutture cloud.

Affrontare le sfide di un ambiente multi-cloud richiede un approccio olistico che armonizzi la gestione della sicurezza tra elementi in cloud e con quella della sicurezza interna alla struttura aziendale, integri la valutazione del rischio con il rischio dovuto alla gestione degli elementi di sicurezza di responsabilità dei provider di servizi cloud (supply chain security). L'assunto è: **il cloud non è intrinsecamente sicuro, anzi il contrario, e deve essere protetto con gli stessi standard utilizzati all'interno delle infrastrutture on premise**.
Ciò che serve è una suite completa di strumenti di prevenzione, rilevamento e mitigazione delle minacce che si integri con tutti i principali servizi cloud e che possa essere gestita all'interno dell'azienda da un unico pannello di controllo.
Al fine di rappresentare le linee guida per affrontare il problema della sicurezza informatica in cloud, si fa riferimento alla matrice di responsabilità, Figura 3, condivisa come bussola per orientare le azioni più opportune alla riduzione dei rischi.

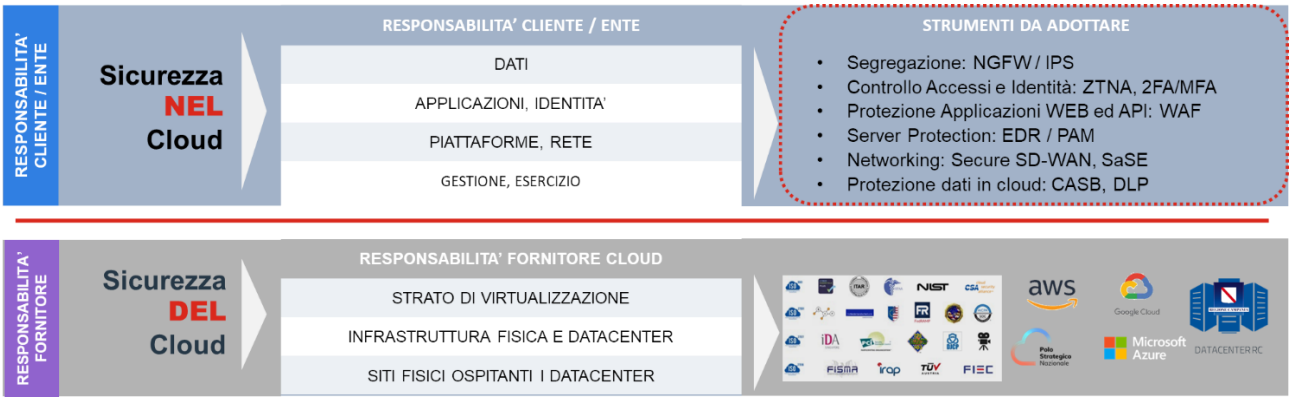


Figura 3 Modello di responsabilità condivisa: normative applicate dai provider e strumenti di sicurezza a carico del cliente

In questo modello di responsabilità condivisa l'ente che usufruisce di servizi in cloud è responsabile della sicurezza di quanto è ospitato in cloud e il fornitore del servizio lo è per l'infrastruttura ospitante. Quanto di responsabilità dell'ente può essere quindi protetto declinando quanto proposto in Figura 3 come mostrato in Figura 4, considerando la divisione verticale sul livello di servizio proposto dal modello di responsabilità condivisa.

Figura 4 Schema tecnologie di sicurezza applicabili per tipologia di servizio

Si individuano quindi, per livelli di servizio scelti, i componenti di sicurezza necessari come di seguito descritto:

3.1.3 Servizi SaaS

I servizi SaaS richiedono all'organizzazione che li adotta di gestire in modo centralizzato i seguenti elementi essenziali:

- **La gestione dell'identità degli utenti secondo il modello Zero Trust, integrato con i sistemi di accesso del SaaS provider**
  Spesso i servizi SaaS permettono il censimento e la profilazione degli utenti mettendo a disposizione dei connettori (sincroni o asincroni) per raccogliere le informazioni degli accedenti dai sistemi di "directory" dei propri clienti, come ad esempio dall'Active Directory. Integrare l'autenticazione degli accedenti al servizio con la profilazione dei dispositivi utilizzati e l'analisi delle connessioni consente, in base alle policy aziendali, di negare o autorizzare l'accesso alle risorse; questo approccio è più comunemente citato come "approccio zero trust (appendice ZTNA)" nel quale appunto non ci si fida né dell'utente, né del device che utilizza, né della singola connessione verso le risorse/servizi. Nessun utente, nessun device, nessuna connessione viene autorizzata se rispettivamente non risponde correttamente a tutte le "challenge" (quali per esempio coppia utente/password complessa, doppia autenticazione con segreto "one time" eventuale terzo segreto biometrico o su dispositivo inviolabile fisico), non si utilizza un dispositivo gestito dall'organizzazione o che ha superato con successo le regole di profilazione, non si concede l'utilizzo di una risorsa web se il certificato client utilizzato per chiudere ad esempio una connessione SSL non è stato emesso da una CA riconosciuta dallo ZTNA gateway.
- **La visibilità delle attività attraverso soluzioni CASB e adozione di meccanismi di DLP (Data Leak Prevention).**
  I servizi SaaS, per loro natura, sono erogati tramite connessioni pubbliche e possono essere acceduti da ovunque nel mondo (si pensi per esempio a One Drive o Microsoft Office 365) rendendo indispensabile utilizzare appunto un servizio CASB (Cloud Access Security Broker). In sostanza un CASB è una soluzione di sicurezza che protegge l'accesso ai servizi cloud mettendo a disposizione, tramite accordi tra fornitori di servizi e fornitori di sicurezza e chiamate API, strumenti di sicurezza quali il controllo degli accessi, il monitoraggio delle attività effettuate identificando comportamenti anomali o sospette violazioni della sicurezza generando report periodici e di compliance agli standard di sicurezza, protezione dei dati consentendo di individuare eventuali malware, protezione dal Data Leak impedendo l'esfiltrazione e divulgazione non autorizzata di informazioni. In sostanza, un CASB agisce come intermediario tra gli utenti e i servizi cloud, garantendo un controllo granulare e una sicurezza avanzata per le risorse e i dati gestiti attraverso piattaforme SaaS.
- **Protezione dei dati, tramite backup (Data Loss Prevention)**
  I dati presenti nei servizi SaaS devono comunque essere sottoposti a backup continui e questi ultimi devono essere a loro volta revisionati e verificati periodicamente. In primis è necessario valutare se le misure messe a disposizione dal fornitore del servizio SaaS sul backup dei dati sono sufficienti a soddisfare i requisiti dell'ente ed integrare queste misure con eventuali strumenti esterni che consentano di: verificare i backup, esportare i backup verso altre destinazioni (altri cloud oppure on premise), cifrare i dati presenti nel backup, ripristinare o "montare dal vivo" i backup a scopo di verifica.

3.1.4 Servizi IaaS e PaaS

Quanto considerato per i servizi SaaS resta valido anche per i servizi IaaS/PaaS ed on Prem. Come esposto nel modello di responsabilità condivisa. Internalizzando le infrastrutture ci si deve far carico anche di specializzare ed estendere la sicurezza, sobbarcandosi la necessità di adottare ulteriori strumenti, di orchestrarli e di manutenerli. Le esigenze sono molti simili per IaaS/PaaS ed on Prem fatte salve le opportune varianti messe a disposizione o dai fornitori di infrastruttura o da eventuali terzi: spesso un unico servizio, prendiamo ad esempio quello di "protezione applicazioni tramite web application firewall", potrebbe essere per datacenter on-premise erogato tramite apposite apparecchiature fisiche, ma su una piattaforma condivisa (es. PSN) non è sempre possibile o opportuno utilizzare appliance fisiche; è

conveniente dotarsi della stessa funzionalità ma erogata tramite "appliance virtuale o VM". Infine, per i cloud provider che lo consentono o che mettono a disposizione strumenti nativi di "protezione applicazioni" tramite le proprie piattaforme native (o di terze parti), resta sempre valido il meccanismo di adozione scegliendo la forma erogazione più opportuna. Il punto è quindi dotarsi della funzionalità di protezione nella forma più agile e pratica per l'infrastruttura che si deve gestire. Fatta questa dovuta precisazione si andranno ora ad elencare le funzionalità/strumenti minimi che sarebbe necessario predisporre e che integrano quelli proposti per i SaaS.

Per i servizi IaaS/PaaS ed on Prem:

- **Network Security**

  Spostando l'asticella della responsabilità verso il basso si deve affrontare la componente fondamentale della sicurezza: la rete. Trattandosi in ogni caso di argomento vasto e complesso si cercherà di schematizzare e semplificare utilizzando alcune macroaree di intervento.

  Per infrastrutture di tipo on-premise risulta necessario innanzitutto segmentare in opportune VLAN (Virtual Lan) il livello 2 (Rif. pila OSI) sia per il contesto del datacenter o dei datacenter degli enti. A questo primo livello di segmentazione deve poi, per consentire visibilità e conseguente protezione dei flussi di traffico, aggiunto un livello di segregazione. La segmentazione viene implementata su switch di rete mentre la segregazione viene implementata su Next Generation Firewall (NGFW). Utilizzando invece un PaaS, in cui spesso non è esposto al cliente/ente il livello 2 dell'infrastruttura di rete, se non in maniere "virtuale", è possibile e necessario comunque dotarsi di NGFW, erogati tramite appliance virtuale o servizio o container, per realizzare gli stessi meccanismi di visibilità e segregazione delle direttrici di traffico da e verso i servizi. Gli NGFW mettono a disposizione varie modalità operative di protezione, e a seconda dei casi, possono essere configurati anche per agire come IPS (Intrusion Prevention System), fondamentali per assicurare elevati livelli di sicurezza di rete.

  Spostando invece lo sguardo verso le direttrici di traffico che invece viene generato dagli utenti ospitati all'interno delle sedi degli enti, ancora una volta i Next Generation Firewall trovano loro utilizzo in modalità operativa di Secure Web Gateway. Gli utenti finali ed il loro traffico sia verso servizi pubblici che in datacenter devono essere quindi protetti con un SWG allo scopo di gestire i rischi associati alla navigazione web, inclusi attacchi malware, phishing e accesso a contenuti non sicuri o non conformi alle politiche aziendali.

  In questo dominio, quello del livello di accesso degli utenti alla rete dell'organizzazione, inoltre risulta di cruciale importanza l'adozione di sistemi di **Network Access Control (NAC)**: gestire l'accesso al livello 2 delle infrastrutture degli enti, con uno strumento che consenta la visibilità e conceda l'utilizzo della risorsa di rete primaria solo agli utenti censiti, agli ospiti autorizzati, ai consulenti con ancora contratti validi ed i cui device rispettino le norme di sicurezza stabilite dalle politiche dell'ente.

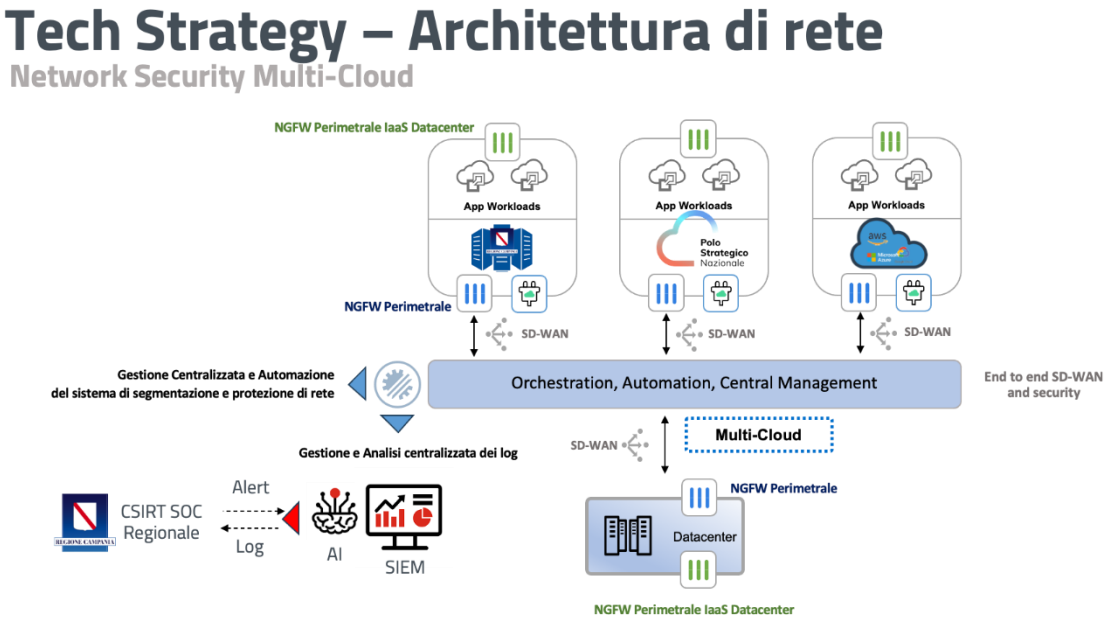


Figura 5 Sicurezza di rete per le architetture multi-cloud

- **Connettività sicura e resiliente**

  La sicurezza di una infrastruttura di rete non si limita e confina solo agli ambiti di datacenter e rete locale ma deve essere anche estesa alle reti geografiche: per sicurezza si intende anche la gestione intelligente della banda a disposizione, dei molteplici collegamenti tra le varie infrastrutture, la riconfigurazione dinamica ed automatica delle politiche di instradamento del traffico verso servizi richiesti in base alle condizioni effettive di utilizzo della rete da parte degli utenti. La tecnologia che è ormai largamente riconosciuta e adottata per assicurare si servizi resilienza, sicurezza e agilità è l'SD-Wan.

  Si rimanda al capitolo 3.2 che analizza tutte le implicazioni del caso ed esplicita molti degli scenari possibili con relative soluzioni di sicurezza minime da adottare.

- **Sicurezza delle applicazioni WEB: WAF e API security**

  Moltissime applicazioni vengono ormai erogate tramite web, tramite protocollo http/https sul quale spesso vengono rese disponibili chiamate ad API. Questa esposizione di dati, servizi e chiamate API risulta essere un punto di vulnerabilità molto sfruttato dagli attaccanti in relazione alle debolezze quasi fisiologiche del software: dotarsi di strumenti specifici per proteggere tali applicazioni diventa elemento fondamentale di difesa. L'adozione di un WAF contribuisce in maniera sensibile a ridurre il rischio di violazioni della sicurezza e a proteggere l'integrità e la disponibilità delle applicazioni erogate in datacenter on-premise o in IaaS/PaaS. Le minime caratteristiche di un WAF moderno, escluse quelle intrinseche di essere poter erogato dal produttore in forma di appliance fisica, virtuale o come servizio, possono essere: abilità di analizzare e filtrare i dati di input provenienti dagli utenti per individuare e bloccare tentativi di inserire codice dannoso o sfruttare vulnerabilità nelle applicazioni web; abilità a riconoscere e prevenire attacchi SQL injection, che cercano di manipolare le query del database, e attacchi XSS, che mirano a eseguire script lato client non autorizzati nei browser degli utenti; implementare controlli avanzati per gestire l'accesso alle applicazioni web, autenticare gli utenti e prevenire accessi non autorizzati (integrazione con ZTNA, si veda requisito 1); mitigare attacchi di tipo Cross-Site Request Forgery (CSRF), che cercano di eseguire azioni non autorizzate a nome degli utenti, e attacchi di tipo Distributed Denial of Service Applicativo; utilizzare tecniche di rilevamento delle minacce e analisi del comportamento per identificare attività sospette o modelli anomali di

traffico che potrebbero indicare un attacco; registrare dettagliatamente gli eventi di sicurezza, consentendo il monitoraggio in tempo reale e la generazione di report per l'analisi degli incidenti; mantenere costantemente aggiornate le firme e le regole di sicurezza per rilevare nuove minacce e vulnerabilità; collaborare con altri componenti della sicurezza informatica, come firewall di rete (cfr. requisiti NGFW) e sistemi di prevenzione delle intrusioni (cfr. requisiti IPS), per fornire una protezione olistica.

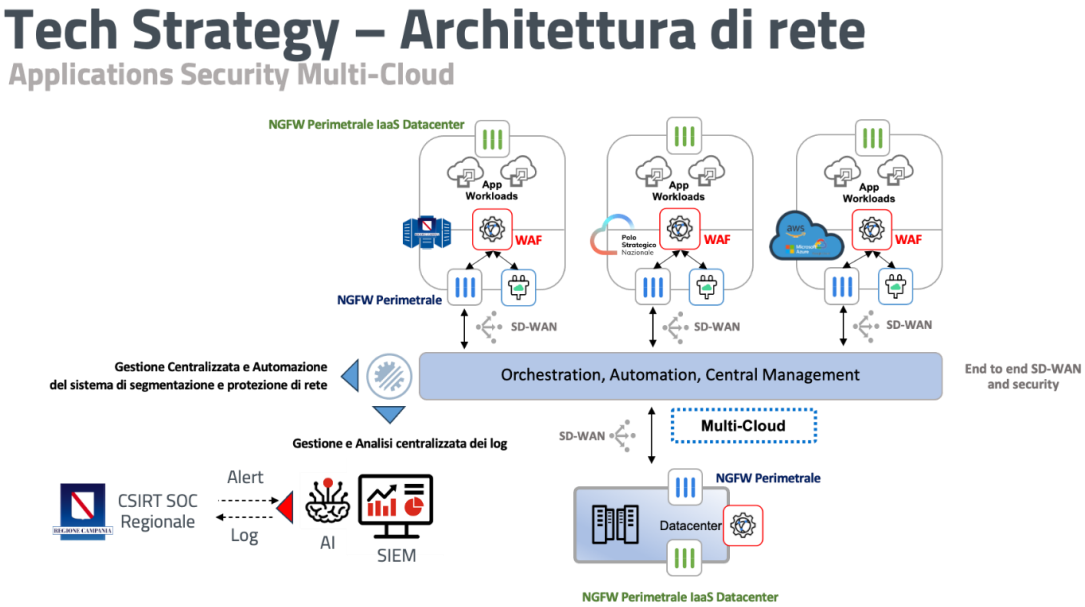


Figura 6 Sicurezza Applicazioni ed API per le architetture multi-cloud

- **Edge Protection (EDR)**
  Gli End point sono spesso l'anello debole di tutta la catena di protezione di un qualsiasi sistema informativo per un semplice motivo: sono utilizzati dagli umani che per errore, dolo o omissione sono il primo punto debole che i malintenzionati tendono a sfruttare. Il primo click su un link contenuto in un allegato o nel testo di una e-mail, la propagazione di un malware attraverso una penna usb, o semplicemente il click su una pagina che ci invita a riscuotere un premio sono quanto di più comune accade in qualsiasi ente ed è spesso la causa principale di incidenti di sicurezza anche molto gravi.
  Inserire strumenti di protezione delle workstation moderni ed intelligenti quali un **EDR (Endpoint Detection and Response)** risulta di cruciale importanza. L'utilizzo di strumenti di protezione quali semplici antivirus basati su database di firme virali non è una sufficiente contromisura verso gli attuali attacchi; un normale antivirus risulta cieco e non riesce ad essere aggiornato in tempo reale contro, per esempio, le versioni "Zero- day" (si veda appendice) o attacchi che non utilizzano normale codice ma script shell o attacchi in-memory. L'approccio di protezione basato su machine learning ed intelligenza artificiale è quanto necessario per contrastare questo tipo di minacce e centrare l'obiettivo minimo di protezione adeguato delle workstation. Le organizzazioni che hanno adottato un EDR riescono anche a "rispondere" agli attacchi sugli endpoint (dispositivi come computer desktop o portatili, server, laptop, dispositivi mobili) e ad individuarli in tempi ragionevoli e contemporaneamente riescono a mettere a disposizione degli amministratori di rete o dei team di sicurezza una quantità di informazioni necessarie all'investigazione forense in caso di incidente informatico.

- **Business Continuity / Disaster recovery / ADC / GSLB**

L'utilizzo di sistemi multi-cloud e/o architetture ibride consente di implementare meccanismi di resilienza dei servizi. Tipicamente un'analisi dei requisiti del parco applicativo determina i requisiti di resilienza in termini di Recovery Time Objective (RTO, tempo interruzione massimo ammissibile) e il Recovery Point Objective (RPO, perdita ammissibile dei dati), da cui deriva una categorizzazione delle applicazioni e dei servizi.
Applicazioni che richiedono tempi di recupero nulli o quasi vengono definiti di business continuity. Per implementare architetture di business continuity si usano bilanciatori di traffico prodotto dai client verso i servizi in maniera intelligente. L'architettura di bilanciamento è consapevole di quanti e quali server/componenti costituiscono un servizio e indirizza le richieste dei client verso le infrastrutture al momento disponibili o che risultino più idonee ad erogare i servizi richiesti. I bilanciatori devono essere disposti in maniera intelligente sia sulle infrastrutture on-premise che su quelle in cloud, e devono essere in grado di integrare le funzioni erogate con le risorse esposte da provider di servizi IaaS/PaaS. A questo proposito si parla di GSLB (rif. appendice) quando appunto un servizio erogato da più punti di una infrastruttura multi-cloud risulta resiliente al malfunzionamento o alla completa caduta/disconnessione di uno dei suoi componenti: utilizzare Load Balancer e Global Server Load Balancing (GSLB) consente di abbassare i tempi di RTO fino ad annullarli.

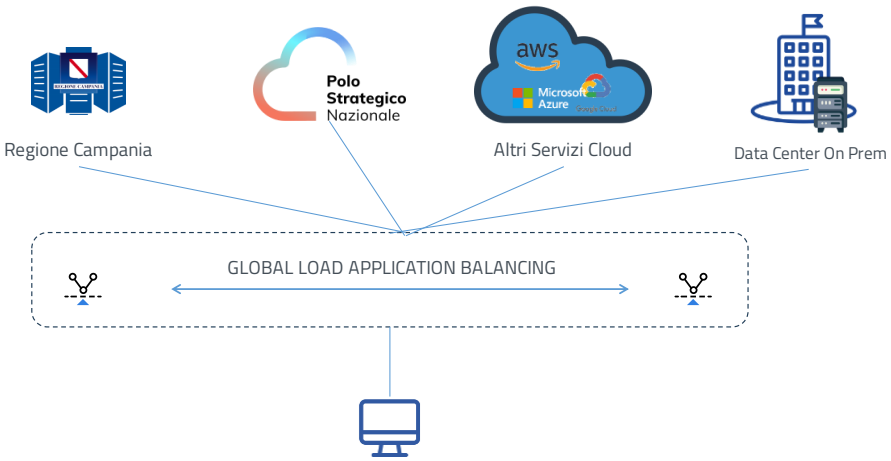


Figura 7 Architettura di servizio basata su GSLB

3.1.5 Requisiti trasversali SecOps

Nel far evolvere il proprio sistema informativo verso una qualsivoglia infrastruttura IaaS/PaaS/SaaS/On-Prem non può prescindere da una serie di requisiti comuni individuabili, tra cui possiamo sicuramente citare come minimi ed assolutamente necessari:

- **Sistema centralizzato di Policy Management** e processo di change management security in place
  Avere un framework di riferimento, una chiara indicazione di standard operativi, una definizione esaustiva delle politiche di sicurezza fisica, logica è fondamentale per implementare e mettere in piedi un processo di gestione della sicurezza informatica a tutti i livelli. Quindi partire da un framework o uno standard e muoversi verso l'integrazione di esso nei processi dell'ente consentirà avere la completa governance del sistema di sicurezza. Di cruciale importanza è l'adozione di un processo di change management strutturato e autorizzato a più livelli che operi all'interno di un

security policy package definito e verificato: le politiche di sicurezza devono essere implementate, manutenute e modificate in maniera omogenea su tutta l'infrastruttura sotto il proprio governo nello scenario multi-cloud. Disporre di un sistema centralizzato per memorizzazione ed implementazione delle politiche di sicurezza è la base di un sistema di governance affidabile. Questo determina, inoltre, la riduzione del rischio di errori umani e semplifica i processi operativi.

- **Monitoring and detection – SIEM / SOAR - AI**
  Gli incidenti di sicurezza informatica accadono, e accadono ad un tasso sempre più elevato e la loro magnitudo risulta sempre in crescita. Con l'avvento della direttiva NIS prima e la sua seconda versione NIS2 si sta sempre di più allargando il perimetro di aziende/enti per il quale è obbligatorio adottare misure di sicurezza atte a innanzitutto a individuare gli incidenti pena la sanzione. Per raccogliere e correlare tutte le evidenze che vengono generate da un perimetro frastagliato di infrastrutture multi-cloud è necessario dotarsi di SIEM (cfr. Appendice). Che tipo di SIEM adottare è una scelta ponderata su molteplici fattori; innanzitutto va valutato se l'ente abbia le capacità in termini di personale e di competenze per gestire in autonomia un servizio SIEM: qui vengono in soccorso le versioni di SIEM federati o addirittura SaaS. I SIEM federati sono di solito ospitati presso le infrastrutture cliente/ente e vengono gestiti da enti terzi mediante connettori implementati su reti crittografate: in sostanza la raccolta degli eventi di sicurezza avviene sugli ambienti multi-cloud, un primo consolidamento e correlazione degli eventi avviene all'interno del SIEM federato e poi le risultanze vengono collegate e correlate in un super-SIEM ospitato in un SOC (cfr. appendice) esterno all'organizzazione. L'ente / cliente conserva una vista in lettura per avere accesso alle informazioni in fase di notifica degli incidenti e per la fase di rimedio.
  Nei SOC avanzati, come quelli federati, spesso vengono utilizzati anche sistemi SOAR (cfr. appendice) che consentono l'automazione e l'orchestrazione dei processi di operativi e di risposta agli incidenti. Avvalendosi di meccanismi di machine learning ed intelligenza artificiale i SOC federati aumentano la quantità di informazioni che riescono a correlare, la quantità di eventi che riescono a gestire, la qualità della individuazioni (detection) di eventi multipli e diluiti nel tempo, e velocizzano il triage degli incidenti: a valle di questo processo di detection automatizzato e condiviso su più enti/clienti, valutato l'impatto di un incidente, il SOAR usando sia l'AI che le competenze degli operatori, può attuare una serie di playbook automatici che possono operare automaticamente o suggerire azioni per la fase di rimedio all'incidente. Nel campo della sicurezza informatica, la collaborazione e la condivisone delle informazioni tra enti è fondamentale per ridurre i tempi necessari ad individuare e risolvere un attacco.

- **Preparazione e notifica degli incidenti**
  Affidare la detection, la gestione e la risposta agli incidenti non è esaustivo rispetto ad altre due azioni che sono cruciali: essere preparati come ente a gestire un incidente e notificare in maniera corretta questi ultimi alle autorità competenti. Si potrebbe pensare che una volta affidato il servizio SOC ad un ente terzo ci si sia completamente liberati di tutte le responsabilità: anche sapere cosa fare dal momento che viene identificato un incidente, nelle prime ore, è fondamentale così come lo è essere preparati al notificare al pubblico, alle autorità di pubblica sicurezza e alle autorità competenti in materia di privacy (leggasi Garante, ACN, PS, etc..). Essere preparati richiede formazione di tutto il personale coinvolto e che utilizza il sistema informativo e per quelli che lo gestiscono è necessaria una preparazione specifica su come comportarsi in caso di incidente. Lo stesso è valido per chi dirige e che dovrà comunicare con tutti gli attori coinvolti e coordinare le attività di risposta. È opportuno quindi acquisire le competenze descritte mediante corsi specifici, esercizi, simulazioni ed è consigliabile impostare questa attività di formazione in guisa di programmi duraturi e su archi temporali più lunghi rispetto a semplici progetti formativi una tantum.

- Particolare attenzione va data alla gestione della **sicurezza della supply chain** (appendice), infatti, se il fornitore del servizio non rispetta le buone pratiche e le normative riguardanti la cyber security, il rischio di ricevere attacchi tramite il fornitore stesso o disservizi possono essere elevati.

In generale un approccio architetturale basato su standard e protocolli aperti, che integri diversi dispositivi di sicurezza in un unico sistema che si estenda all'intera rete multi-cloud risulta il modo migliore di progettare un'infrastruttura di sicurezza, adeguata a proteggere le minacce in un ambiente cloud distribuito. Questo approccio deriva dalla necessità di ridurre la complessità dei sistemi di sicurezza e di renderli, di conseguenza, efficienti e gestibili.

4 Modello per la resilienza e la sicurezza della connettività

La rete rappresenta un sistema critico nell'insieme degli elementi che concorrono ad erogare qualsiasi tipo di servizio. Adottando una strategia multi-cloud, man mano che vengono coinvolti più fornitori di servizi Cloud, l'architettura di rete deve evolvere per adottare un modello semplificato ed efficace che possa offrire:

- Una connessione efficiente tra le varie applicazioni e una distribuzione dei carichi di lavoro sulle varie connettività in modo da migliorare l'esperienza applicativa per gli utenti.
- L'ottimizzazione dell'esercizio e dei costi mediante l'automazione.
- L'aumento della visibilità dei modelli di traffico e la possibilità di applicare efficacemente controlli coerenti per ridurre i rischi di sicurezza informatica.
- La resilienza richiesta dalla criticità dei servizi erogati.

Ecco, pertanto, quattro requisiti fondamentali, per la rete, che bisogna adottare quando si distribuiscono applicazioni su più cloud:

- **Policy comune di rete e sicurezza e framework di applicazione**: una delle sfide principali delle distribuzioni multi-cloud è rappresentata dal fatto che i Cloud provider hanno diverse architetture proprietarie costruite su framework, API e set di strumenti specifici per ciascuna di esse. La giusta soluzione multi-cloud è quella in grado di mettere a disposizione un'architettura di rete e sicurezza che si estende fin dentro questi cloud, ne sfrutta le caratteristiche e le funzioni native di ciascuno astraendo tali funzionalità con le API gestendo tali connessioni in modo dinamico utilizzando l'automazione.
- **Rete *application-aware* per una migliore esperienza dell'utente**: un'altra sfida importante con le attuali tecnologie di rete che collegano più cloud è rappresentata dalla mancanza di conoscenza dei diversi tipi di applicazioni da parte del trasporto sottostante. È importante che la rete riconosca le applicazioni per ottimizzare l'uso delle risorse disponibili, delle condizioni e della capacità di rete. Il traffico non importante deve essere controllato per migliorare l'esperienza dell'utente finale al fine di fornire prestazioni coerenti per le applicazioni critiche dell'organizzazione
- **Architettura di rete e sicurezza integrata per l'efficacia e l'efficienza**: integrare la sicurezza con la connettività è un elemento basilare per assicurare un sistema resiliente. Il controllo dell'accesso degli utenti e delle applicazioni, l'ispezione del traffico di rete e la segregazione del traffico geografico sono funzioni importantissime per potenziare il controllo, difesa e visibilità,

oltre che assicurare il contenimento di attacchi, confinandoli in segmenti logici di rete qualora questi avessero successo.

4.1 Piano Sanità Connessa

Nell'ambito del progetto nazionale gestito da Infratel e denominato Sanità Connessa, la Regione Campania ha in piano di realizzare un anello in fibra ottica utilizzato come infrastruttura di comunicazione avanzata per collegare ai datacenter regionali le principali sedi delle organizzazioni sanitarie della regione Campania. L'anello in fibra ottica come rete regionale è stato scelto al fine di garantire una solida infrastruttura di comunicazione, agile, altamente affidabile, e ad alta capacità di trasmissione. Il progetto non prevede accessi ad internet attraverso l'anello. Ogni organizzazione manterrà il proprio accesso alla Internet attraverso Sanità Connessa e/o altro operatore di telecomunicazioni.

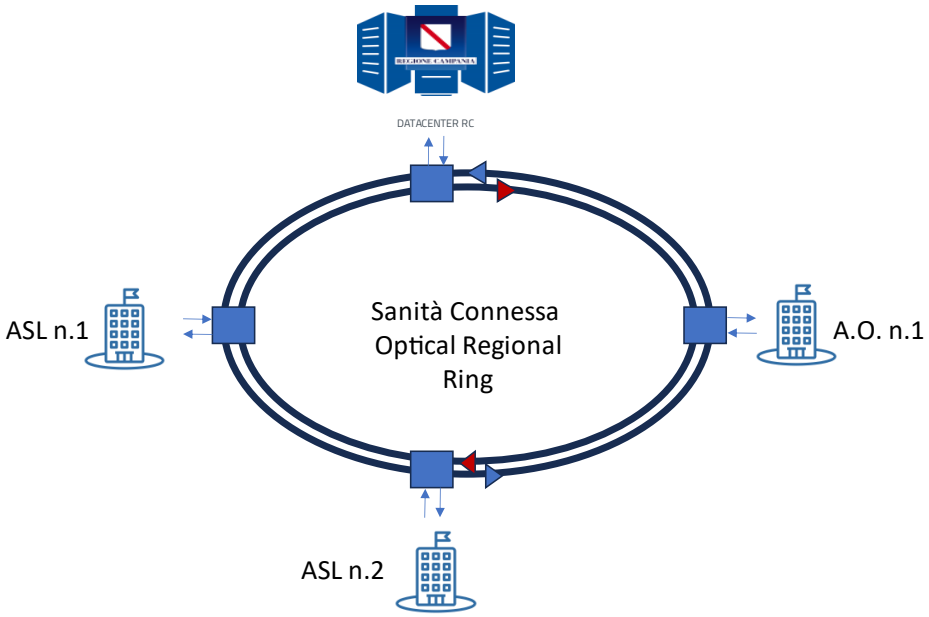


Figura 8 Architettura di backbone Regionale Sanità Connessa

La descrizione dell'architettura di backbone regionale è la premessa alla raccomandazione di architettura di rete resiliente e sicura.
Nel contesto del progetto di Sanità Connessa e del modello di erogazione dei servizi multi-cloud, la raccomandazione è sicuramente quella di utilizzare una tecnologia di rete SD-WAN (Software-Defined Wide-Area Networking) per raggiungere gli obiettivi precedentemente elencati.
Inoltre, l'adozione di un'infrastruttura SD-WAN integrata con la componente di sicurezza offre un approccio sicuro, resiliente ed efficace per i servizi multi-cloud aziendali. La visibilità, il controllo, e la gestione centralizzata di funzionalità di rete e sicurezza proteggono il traffico cloud e instradano le sessioni in modo intelligente in base alle esigenze dell'applicazione specifica, migliorandone le prestazioni e riducendo la dipendenza di collegamenti più costosi come quelli MPLS.

Prendendo a riferimento la configurazione geografica di una Azienda Sanitaria Locale tipo, il modello di riferimento si articola su tre livelli gerarchici, come descritto di seguito.

- **Sedi secondarie**. Con esse si intendono uffici, Ospedali, Presidi e altre sedi dislocate sul territorio. Queste sedi sono collegate alla sede principale attraverso almeno due operatori di

telecomunicazioni differenti, uno dei quali è Infratel Sanità Connessa. Le sedi secondarie accedono ad Internet e all'anello regionale di Sanità Connessa attraverso la sede primaria.

- **Sede Primaria**. Con essa si intende la sede principale dove è collocato l'accesso ad internet e la connessione all'anello regionale di Infratel Sanità Connessa. Questa sede si collega alle sedi secondarie mediante gli Infratel Sanità Connessa e uno o più ulteriori operatori di telecomunicazioni.

Le varie connettività presenti tra le sedi dell'Azienda Ospedaliera e presso i Datacenter che ospitano i servizi cloud sono governate da una infrastruttura overlay SD-WAN che, in maniera centralizzata:

- Assicura la resilienza del servizio di connettività.
- Assicura i livelli di servizio di connettività alle applicazioni.
- Gestisce l'accesso alle risorse di rete e la crittografia dei flussi di traffico.
- Controlla le prestazioni dell'infrastruttura nel suo complesso in tempo reale ed in modo granulare.
- Controlla tutti i flussi di traffico garantendo l'accesso sicuro alle risorse mediante opportuna segregazione in coerenza con la policy di sicurezza aziendali.

La Figura 9 illustra il modello di riferimento architetturale dell'infrastruttura di rete di una organizzazione sanitaria o regionale.

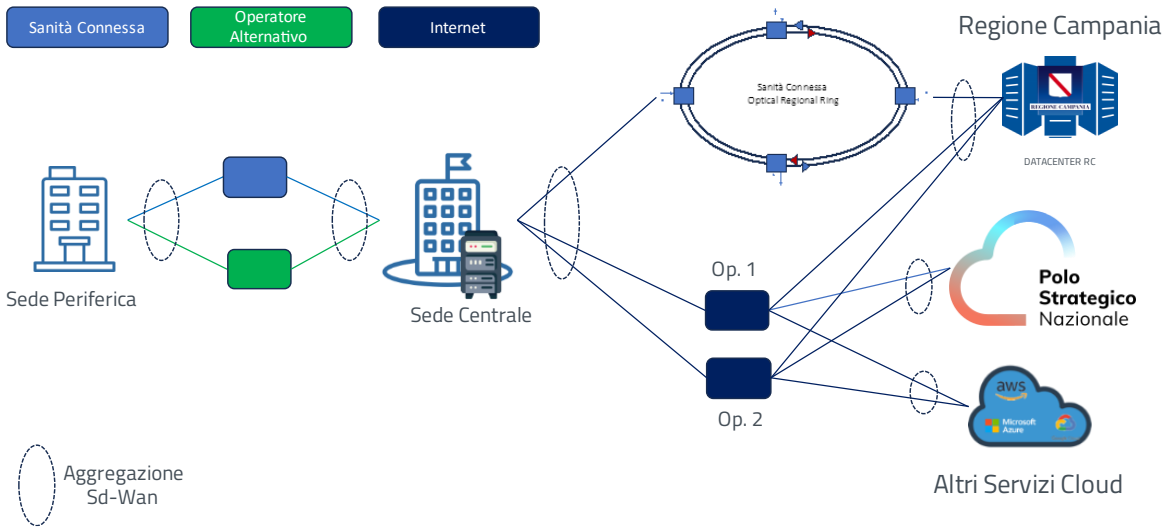


Figura 9: Architettura di connettività e sicurezza SD-Wan end-to-end, modello con sedi gerarchiche

L'adozione di una infrastruttura SD-WAN integrata con la componente di sicurezza abilita anche l'adozione di un modello di connettività alternativo dove anche le sedi secondarie possano accedere direttamente alla rete internet eliminando il concetto di gerarchia. Secondo questo modello, tutte le sedi della azienda sanitaria hanno diretto accesso alla rete internet (Internet Breakout) garantendo lo stesso livello di sicurezza. Il modello è descritto dalla Figura 10: sfruttando la rete Overlay, la connettività Internet può rappresentare di per sé anche una seconda via diversificata per usufruire dei servizi applicativi erogati internamente alla intranet dell'amministrazione. Qualora l'accesso ad internet sia erogato anche da operatore diverso da quello Infratel si può anche valutare di eliminare il secondo operatore di rete MPLS garantendo lo stesso livello di affidabilità. Ancora più importante, l'accesso ad

internet da ogni sede della ASL consente di accedere direttamente ai servizi cloud, ottimizzando/semplificando i flussi di traffico, senza controindicazioni in termini di sicurezza

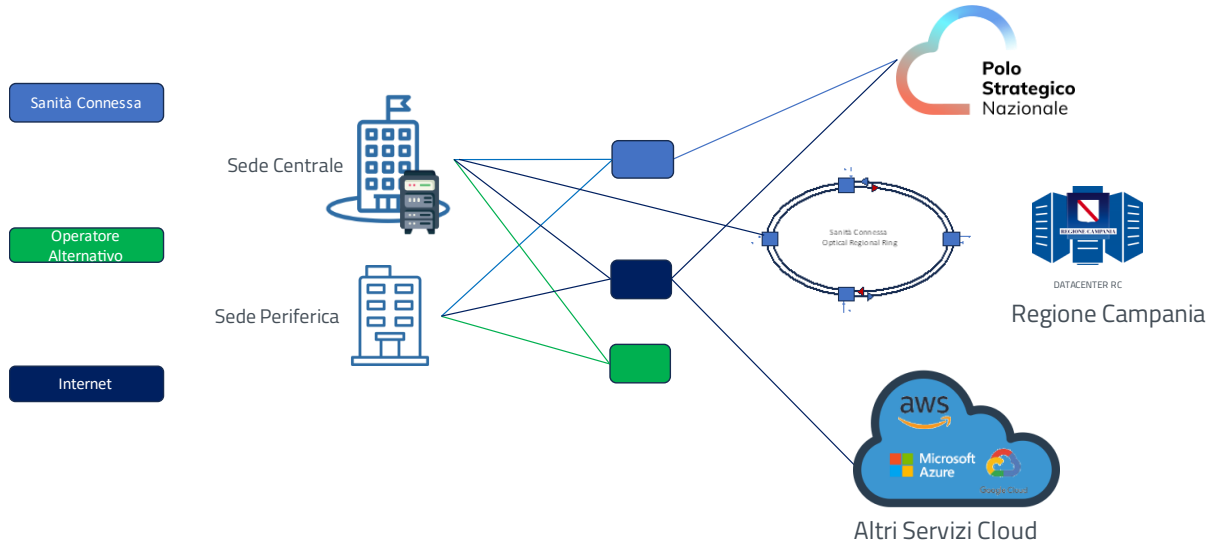


Figura 10: Architettura di connettività e sicurezza Sd-Wan end-to-end, modello piatto

4.1.1 Secure-SD-WAN Use Case

Una rete Secure SD-WAN consente di utilizzare più connettività (Internet/MPLS) in un'interfaccia unica di tipo SD-WAN e distribuire il traffico basandosi su algoritmi di bilanciamento (volume, sessioni, spillover, IP Sorgente, IP Destinazione). Consente di monitorare lo stato dei link in base a latenza e jitter e parametri di perdita di pacchetti ed effettua una distribuzione dinamica del traffico, basata sulle informazioni sullo stato dei collegamenti e su regole configurabili.

Le regole SD-WAN consentono di definire flussi di traffico specifici in base a indirizzi IP, porte, applicazioni o servizi Internet e selezionano i link migliori attraverso i quali verranno inoltrati i vari flusso di traffico. Inoltre, una Secure SD-WAN offre funzionalità per fornire diversi livelli di sicurezza al traffico come per le comunicazioni dirette a Internet o la comunicazione multi-cloud. Il livello di sicurezza deve essere configurabile a partire da funzioni predefinite come firewall e controllo delle applicazioni fino al raggiungimento di funzionalità di sicurezza avanzate come IPS, Web filter, Antimalware, protezione contro minacce avanzate e soluzioni come ZTNA. Tutto l'insieme di policy di instradamento del traffico e sicurezza nonché il monitoraggio di rete e di tutti gli eventi di sicurezza viene orchestrato e gestito centralmente su un'unica piattaforma.

4.1.1.1 Comunicazione da sede remota a sede principale

Questo è uno dei casi più comuni per una rete Secure SD-WAN che soddisfa la necessità di creare connettività tra le varie sedi di un'amministrazione. In questo caso, tutti i siti remoti si collegano ad una sede centrale (Hub) mediante una rete Overlay costituita da Tunnel IPSEC creati sui vari link fisici a disposizione per usufruire delle applicazioni dell'azienda.

Il caso d'uso da sede remota ad hub costituisce la base per una distribuzione Secure SD-WAN a cui si affiancano anche altri scenari che lo completano e che verranno descritti nei prossimi paragrafi: accesso diretto a Internet da tutte le sedi, comunicazione con carichi di lavoro verso ambienti cloud o connettività diretta tra sedi remote.

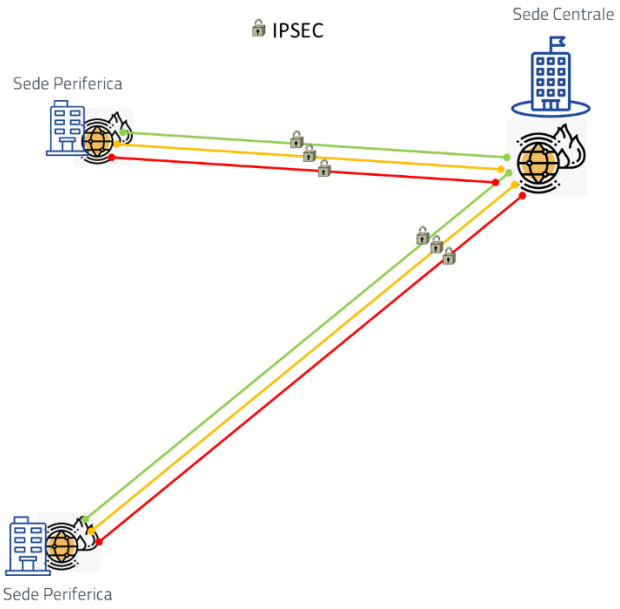


Figura 6: Connettività sito remoto verso sede Centrale

4.1.1.2 Comunicazione tra sedi remote

Questo caso d'uso rende possibile una comunicazione diretta tra le sedi remote nel caso in cui ci siano applicazioni o servizi (esempio traffico VoIP) distribuiti su più siti.

Una soluzione Secure SD-WAN deve consentire la creazione di tunnel IPSEC dinamici on demand tra le sedi remote nel momento in cui ci sia traffico diretto tra le sedi. Questo scenario fornisce la possibilità di creare una comunicazione diretta tra tutte le sedi tipica di una rete mesh completa pur tuttavia continuando a fornire la semplicità di una topologia a stella. Per questo motivo, questo scenario si adatta facilmente a reti con un numero elevato di siti e rende una soluzione Secure SD-WAN molto scalabile.

La possibilità di utilizzare più collegamenti rimane valida anche in questo caso se ci sono più link disponibili, verranno generati più tunnel IPSEC dinamici (uno per ogni connettività) per la comunicazione tra le varie sedi. Ciò consente di aumentare la resilienza ai guasti, oltre a contribuire a migliorare l'esperienza degli utenti, in quanto consente di scegliere il collegamento con la massima qualità o addirittura bilanciare il traffico tra diversi collegamenti

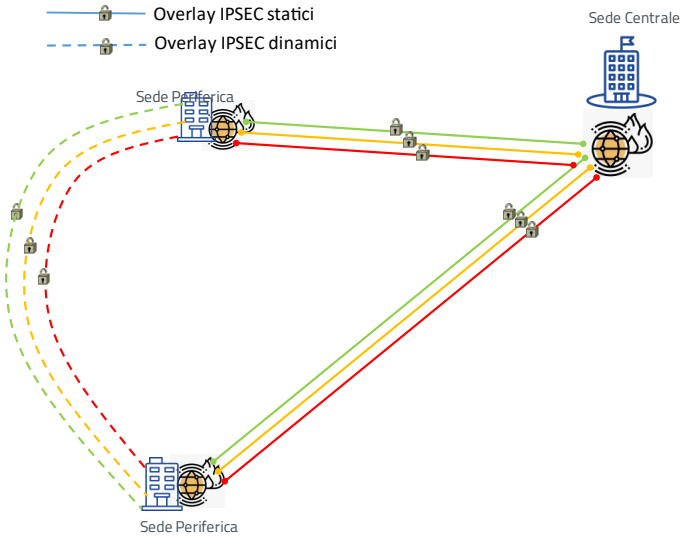


Figura 7: Connettività diretta tra siti remoti

4.1.1.3 Local internet Breakout

Il caso d'uso 'Local Internet Breakout' è utile ogni qualvolta le dinamiche di rete includono una grande percentuale del traffico verso Internet. Una rete Secure SD-WAN rende sicuro l'accesso ad Internet direttamente da ciascuna sede remota dotata di connettività internet grazie all'utilizzo delle funzionalità di sicurezza che devono essere integrate negli apparati di rete.
La possibilità di effettuare un breakout diretto verso Internet sfruttando la connettività locale offre numerosi vantaggi:

- Migliora l'esperienza dei propri utenti che accedono ad Internet dalle filiali, perché con un accesso diretto si evita la latenza caratteristica di un accesso attraverso un punto centrale.
- Evita la congestione nell'accesso ad Internet del sito centrale, perché in questo modo ogni filiale utilizza il proprio accesso.
- Oltre a offrire i vantaggi della user experience, le funzionalità di sicurezza della soluzione migliorano la sicurezza in modo da proteggere tutti gli utenti e il loro traffico durante la navigazione in Internet.
- Insieme alla protezione, inoltre, una soluzione Secure SD-WAN garantisce la visibilità del traffico gli utenti che navigano
- Grazie all'utilizzo di Policy di sicurezza orchestrate centralmente, la loro applicazione su tutte le sedi risulta agevole e distribuita in modo omogeneo.

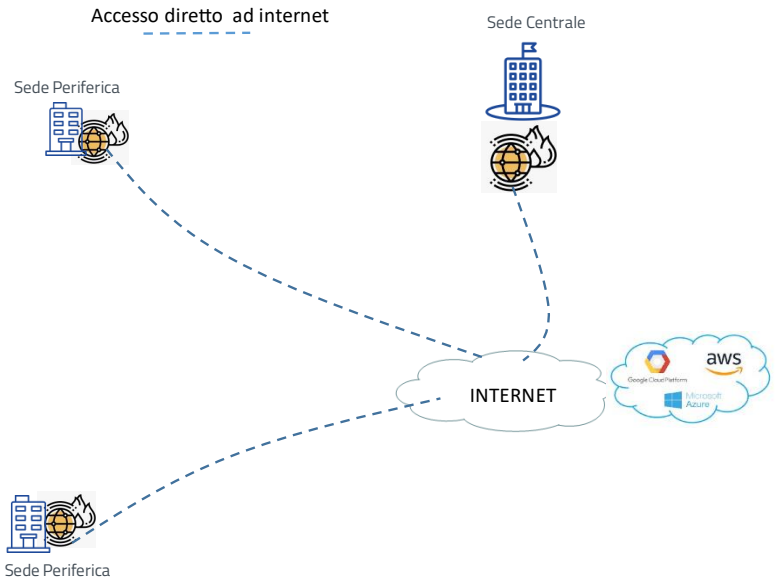


Figura 8: Connettività diretta verso Internet dalle sedi remote

Data la flessibilità della soluzione Secure SD-WAN, in caso di fault della connettività Internet locale è possibile reinstradare il traffico Internet della sede attraverso la rete Overlay IPSEC verso una sede remota senza arrecare alcun disservizio alla sede oggetto di fault:

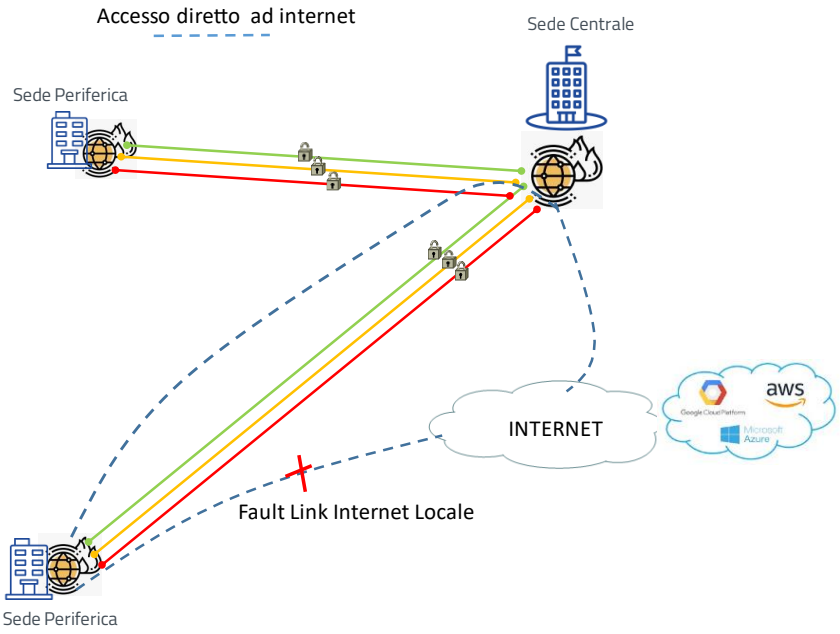


Figura 9: Connettività SD-WAN verso Internet in caso di fault

4.1.1.4 Connettività verso Cloud

Una Secure SD-WAN va oltre un'evoluzione della WAN tradizionale consentendo la connessione verso i servizi Cloud, in modo che possano accedervi come se accedessero ad un'altra delle proprie sedi.

Questo use case è utile nel caso in cui vi siano carichi di lavoro verso un cloud pubblico o in generale verso un servizio Cloud remoto. Nel cloud remoto può essere creata un'istanza dell'apparato Edge della soluzione Secure SD-WAN che si configura come un altro sito della propria rete gestita e orchestrata centralmente dalla stessa piattaforma che gestisce tutte le sedi.

In questo modo si beneficia di una migliore connettività verso il cloud, supportata da tutte le funzionalità di monitoraggio, automazione e gestione ottimizzata dei flussi di traffico tipici della Secure SD-WAN. Il vantaggio è anche nella sicurezza poiché la comunicazione utilizzando canali pubblici viene protetta e crittografata.

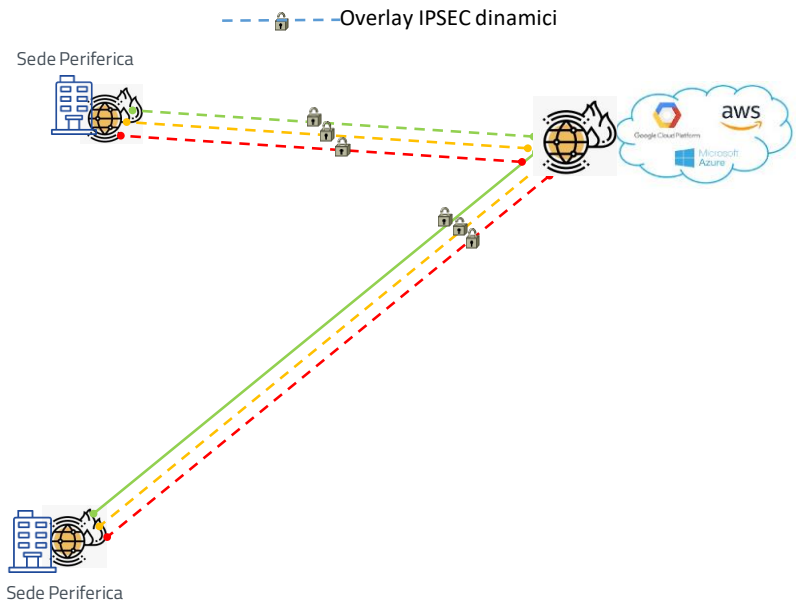


Figura 10: Connettività SD-WAN verso Cloud

4.1.1.5 Connettività Muti-cloud

Il caso d'uso verso multi-cloud estende il caso d'uso verso un singolo cloud nel momento in cui i carichi di lavoro sono distribuiti su più servizi cloud e/o sul DC privati del cliente interconnessi tra loro. In tutti i cloud remoti coinvolti potrà essere creata un'istanza dell'apparato edge della soluzione Secure SD-WAN che si configura come un altro sito della propria rete gestita e orchestrata centralmente dalla stessa piattaforma che gestisce tutte le sedi.

In questo modo si beneficia di una migliore connettività verso il cloud, supportata da tutte le funzionalità di monitoraggio, automazione e gestione ottimizzata dei flussi di traffico tipici della Secure SD-WAN. Il vantaggio è anche nella sicurezza poiché la comunicazione utilizzando canali pubblici viene protetta e crittografata.

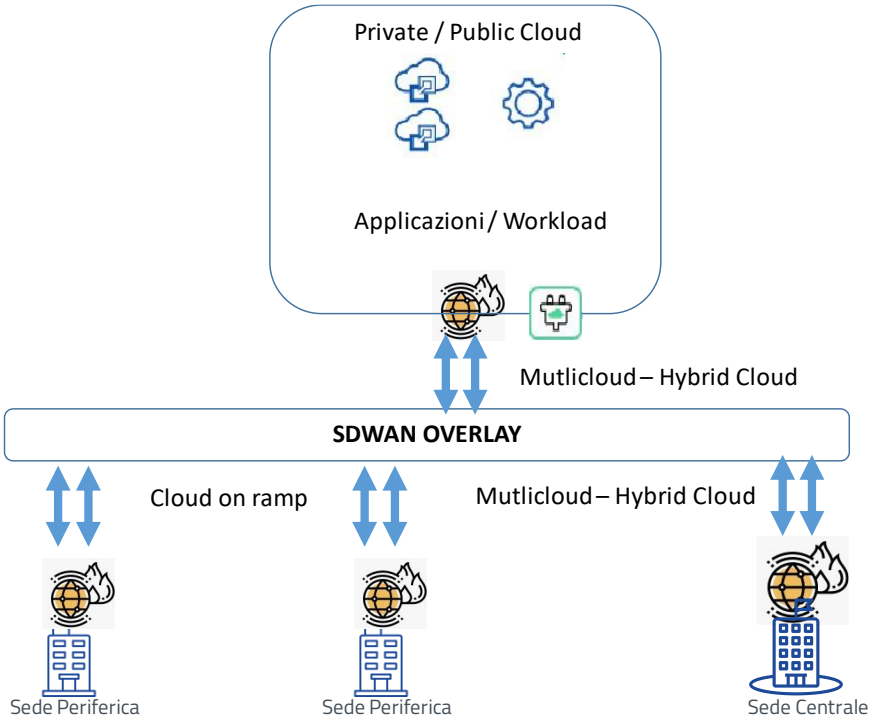


Figura 11: Connettività SD-WAN verso Multi-Hybrid Cloud

4.2 Modello per resilienza e la sicurezza per le Operation Technologies

Le tecnologie cosiddette "Operational Technologies", definite da Gartner come "l'insieme di hardware e software che rileva o causa cambiamenti attraverso il monitoraggio o il controllo diretto di dispositivi fisici, processi ed eventi di un'impresa" rappresentano uno dei settori di maggiore attenzione per quanto attiene alla sicurezza cibernetica. Di questo settore tecnologico fanno parte, ad esempio, i sistemi di automazione SCADA/ICS e sistemi elettromedicali.
In accordo con il percorso di attuazione della normativa NIS2 ed MDR sono illustrati di seguito i modelli di riferimento ai fini della cyber resilienza:

La normativa NIS 2, che sarà obbligatoria per una serie di Enti e Aziende nazionali a partire dal recepimento dello stato italiano della direttiva europea, introduce rigorose misure di sicurezza in relazione alla gestione del rischio di sicurezza informatica, tra cui la catena di approvvigionamento, gli obblighi di segnalazione, gli obblighi di vigilanza e di esecuzione, comprese le ispezioni in loco e le revisioni di audit.

Alcuni esempi di soluzioni che possono andare ad indirizzare la compliance con la direttiva NIS2 e che sarà necessario implementare sono:

- **Asset Management**: La gestione delle risorse viene utilizzata nel contesto della NIS2 per identificare le risorse e i sistemi critici. Questo aiuta le aziende a stabilire la visibilità, comprendere le reti informatiche ed industriali e fornire informazioni preziose durante la risposta agli incidenti. Alcune tecnologie utili per soddisfare questo aspetto della direttiva sono: NGFW, NAC, SIEM, SOAR, ZTNA, NDR.

- **Access Control**: Il controllo degli accessi fornisce un monitoraggio continuo delle persone o dei ruoli che operano, gestiscono e controllano tutte le reti informatiche (OT, IT, IoT, IoMT). Alcune

tecnologie utili per soddisfare questo aspetto della direttiva sono: Autenticazione Federata, Autenticazione a fattore multiplo, NAC, PAM, ZTNA, WAF.

- **Network Segmentation**: La direttiva NIS 2 prevede di implementare logiche di segmentazione della rete interna in base alla criticità degli asset derivata dall'analisi del rischio dell'asset aziendale. Alcune tecnologie utili per soddisfare questo aspetto della direttiva sono: NGFW, NAC, EDR, WAF, ADC, ZTNA, PAM.

- **Logging & Monitoring**: La direttiva NIS 2 prevede specifiche procedure e tempi relativamente alla gestione e alla notifica degli incidenti informatici. Sistemi di logging, analisi ed incident management sono fondamentali per la creazione di servizi CSIRT e per la notifica agli stessi degli eventi da parte degli enti. Alcune tecnologie utili per soddisfare questo aspetto della direttiva sono: Log Management, SIEM, SOAR.

- **Risk Management**: Le valutazioni del rischio devono considerare come le risorse critiche possono essere attaccate e compromesse e, soprattutto, quali saranno gli impatti fisici, ambientali e finanziari di eventuali indicenti. Queste informazioni possono portare a una migliore determinazione delle risorse e dei sistemi critici, nonché alla definizione delle priorità dei controlli di sicurezza per mitigare i rischi potenziali o le vulnerabilità note. Alcune tecnologie utili per soddisfare questo aspetto della direttiva sono: Vulnerability Management, Valutazione del rischio Digitale, Penetration Test, NDR, Network Asset visibility and control.

4.2.1 Operational Technology

Normative di riferimento

La normativa NIS 2 fa riferimento sia al mondo IT che al mondo OT ed Industrial IoT, le direttive e le eventuali sanzioni sono applicabili ad entrambi i mondi. Le infrastrutture OT ed Industrial IoT si dovranno adeguare andando ad implementare logiche di protezione che siano adeguate a rispettare gli standard definiti nella direttiva.
A differenza di IEC 62443, modello Purdue, Framework NIST, che sono tutte linee guida per l'implementazione di una corretta postura di sicurezza all'interno del mondo industriale, la direttiva NIS 2 implicherà sanzioni e richiederà la definizione di procedure atte a raggiungere il rispetto delle procedure e delle direttive definite nella stessa.

Le best practices di riferimento per la protezione in ambito OT fanno riferimento allo standard ISA/IEC 62443 per la sicurezza informatica dei sistemi IACS (Industrial Automation Control Systems) e in particolare definiscono le norme di conformità tecnica agli standard di sicurezza informatica dei singoli endpoint quali PLC, sensori, attuatori, ecc.
IEC 62443 separa un'organizzazione ICS in zone di sicurezza in base alla valutazione dei rischi. Lo standard fornisce indicazioni su come selezionare le zone e assegnare il livello di sicurezza (SL). Per soddisfare ogni livello sono necessari determinati controlli. Un'organizzazione deve valutare le lacune tra i controlli di sicurezza esistenti e la definizione dello standard del livello assegnato. A queste zone vengono quindi assegnati SL che vanno da 1 a 4.
Quando un'organizzazione separa i propri ambienti ICS in più zone, non esiste mai un perfetto isolamento del rischio tra tutte le zone perché una zona indebolita può influenzare le zone circostanti in due modi. In primo luogo, un'interruzione dei servizi o delle operazioni all'interno della zona indebolita può

ripercuotersi a cascata in altre zone, in secondo luogo, una compromissione di zona avvicina una minaccia ad altre zone.

Figura 112: IEC 62443 Protection Levels

Per determinare i requisiti all'interno di ciascuna area di sicurezza, lo standard classifica sette requisiti fondamentali (FR), ampliati in una serie di requisiti di sistema (SR) e di requisiti migliorativi (RE) per migliorare postura di sicurezza.
Per facilitare la definizione di ogni SL, lo standard fornisce una definizione di minaccia per ogni livello e un grafico per mappare SR e RE ai livelli di sicurezza FR 1-4.

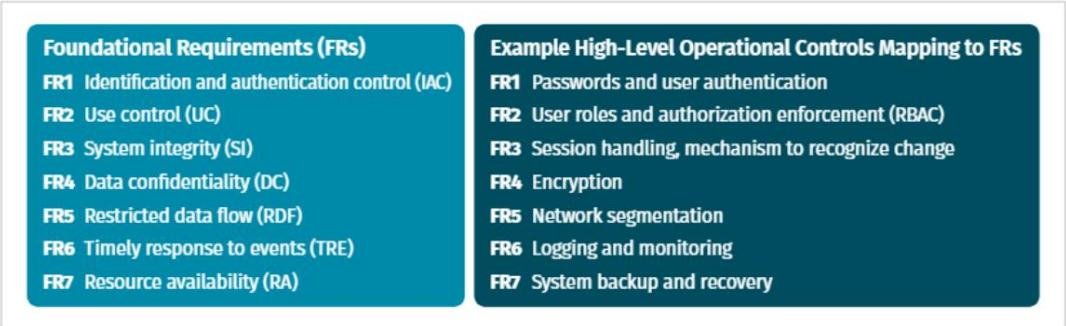


Figura 13: Foundational Requirements e Operational Controls

Sebbene si tratti di definizioni solide e di un buon punto di partenza, le linee guida vanno poi applicate in modo specifico in relazione alla postura di protezione di ognuno degli enti che usano sistemi industriali di controllo e automazione per andare a costruire un Sistema di Gestione della Sicurezza Informatica atto a proteggere i vari livelli di un sistema basato su tecnologia industriale:

- **Fase di Analisi:** Network Access Control, Vulnerability Scan, Network Asset Visibility and Control, Next Generation Firewall, consentono di andare a costruire un modello che verifica lo stato attuale della postura di sicurezza, individui le vulnerabilità presenti e definisca correttamente i vari livelli di protezione ed isolamento secondo le logiche del Purdue Model e dello standard IEC 62443.

- **Fase di Implementazione:** A vari livelli ogni tecnologia è parte del sistema di protezione industriale: le logiche di segmentazione e controllo degli accessi, così come di monitoraggio attraverso sonde comportamentali e protezione dell'asset con tecnologie IPS presente nei dispositivi NGFW e WAF sono alla base di un sistema di protezione del mondo industriale. Nei livelli più vicini al mondo IT del sistema è sicuramente necessario inserire prodotti e soluzioni come EDR, PAM, ZTNA e Multi Factor Authentication per andare a controllare chi accede e limitare le possibilità dei rischi dati dalle operazioni di manutenzione.

- **Fase di Mantenimento:** Tecnologie come Log Management, SIEM in integrazione con tutti i sistemi di sicurezza inseriti nella fase di implementazione consentono una veloce costruzione di cruscotti per il riconoscimento di attività malevole per andare ad implementare un corretto monitoraggio e una corretta gestione del sistema di sicurezza definito nelle fasi precedenti.

Piu in dettaglio nel modello Purdue (ISA-62443) le zone principali di sicurezza vengono definite in questo modo:

- **Zona di sicurezza fisica**: Include i dispositivi e i sensori sul campo, come sensori di temperatura, pressione e altri elementi di monitoraggio.
- **Zona di controllo del processo**: In questa zona, avvengono i processi di controllo in tempo reale. Comprende controllori logici programmabili (PLC), unità remote di input/output e altri dispositivi di controllo.
- **Zona di supervisore**: Qui sono presenti i sistemi di supervisione, come i sistemi SCADA (Supervisory Control and Data Acquisition), che monitorano e controllano l'intero processo.
- **Zona di azienda**: Quest'area è dedicata alle attività di gestione e amministrazione dell'azienda, come sistemi ERP (Enterprise Resource Planning) e altre applicazioni aziendali.

L'obiettivo della norma IEC 62443 è quello di fornire un quadro completo per la sicurezza dei sistemi di controllo industriale, coprendo aspetti come l'identificazione delle vulnerabilità, la gestione dei rischi, la protezione dell'accesso e la gestione degli eventi di sicurezza. L'implementazione di queste linee guida aiuta a mitigare i rischi di attacchi informatici nei settori industriali, proteggendo i sistemi di automazione da minacce interne ed esterne: una possibile mappatura tra sistemi di sicurezza da adottare per ogni "zona" del Purdue model può essere schematizzata come in figura:

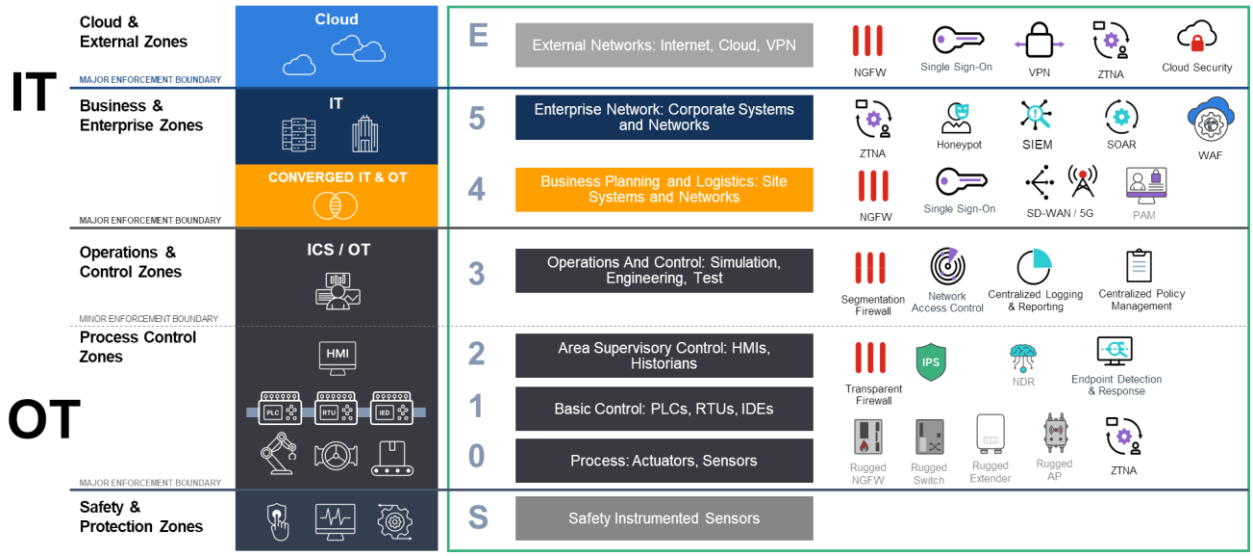


Figura 14: Purdue Model e distribuzione strumenti di sicurezza

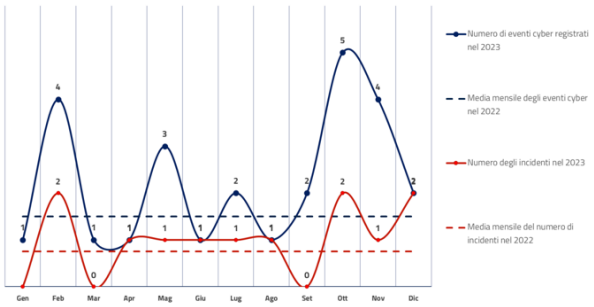
Si noti come ad esempio medesime tecnologie possono e devono essere usate su più livelli: una su tutte i NGFW. Data la loro versatilità possono essere configurati in maniera differente a seconda dello scopo di protezione che devono perseguire per il diverso livello in cui vengono installati.
Esistono invece altri strumenti che tipicamente vengono impiegati solo in alcune zone quali per esempio i componenti industriali (rugged) date le loro caratteristiche fisiche che sopportano l'operatività in ambienti critici.

4.2.2 Settore Sanitario

Attualmente il settore sanitario oggetto di una profonda trasformazione digitale ed al contempo rappresenta uno dei principali target del crimine informatico per il valore dei dati che vengono trattati e per la criticità dei servizi erogati. Pertanto, si è ritenuto opportuno produrre l'approfondimento riportato nei paragrafi a seguire.

4.2.2.1 Breve sintesi dello stato della cyber security nel settore sanitario in Italia.

Sulla base dei dati prodotti da ACN nel mese di ottobre 2024 è possibile affermare che gli attacchi nel settore sono in crescita dal 2022 ad oggi; nello specifico nel 2023 sono stati rilevati 45 casi di eventi cyber con un aumento del 50% rispetto all'anno precedente. Il 47% di questi eventi sono stati confermati come incidenti.



La maggior parte di eventi ed incidenti sono stati provocati di Ransomware. Particolare rilevanza ha la diffusione di informazioni intenzionale o accidentale. Seguono la diffusione di Malware tramite e-mail, così come la sottrazione di credenziali e lo sfruttamento delle vulnerabilità.

Nei primi otto mesi del 2024 si conferma un trend in crescita sia di eventi sia di incidenti di cyber, dove la sottrazione di credenziali riveste questa volta un ruolo primario nei meccanismi di attacco.
Nell'analisi ACN riporta tre principali categorie di minacce che possano costituire le cause principali di questi incidenti: dispositivi esposti incautamente, servizi con vulnerabilità obsolete, configurazioni errate non conformi alle best practices. Un approfondimento sul tema delle dei dispositivi elettromedicali segue al paragrafo successivo. L'ACN riporta anche le Bad Practices, ossia i comportamenti non virtuosi, che sono: gestione decentralizzata dei sistemi, dispositivi obsoleti, carenza di personale. In particolare, un controllo centralizzato delle configurazioni e delle policy, quanto una integrazione spinta tra i sistemi di difesa al punto di consentire processi automatici di prevenzione e contenimento delle minacce sono elementi primari nel disegno di un'architettura di sicurezza. Per quanto attiene alle best practice, ACN ribadisce nella sostanza quanto già descritto ai capitoli precedenti.

4.2.2.2 Dispositivi Elettromedicali e regolamento MDR

Approfondendo il tema dei dispositivi vulnerabili esposti incautamente menzionato al paragrafo precedente, il documento MDCG 2019-16 rev. 1, parte del regolamento MDR, rappresenta la guida per gestire il ciclo di vita dei sistemi elettromedicali per quanto attiene alla sicurezza informatica.
Occorre premettere che il documento si fonda sui requisiti afferenti alla sicurezza informatica, sicurezza fisica delle persone e al funzionamento efficiente dei dispositivi medici. Inoltre, è necessario sottolineare come la soddisfazione dei requisiti passa attraverso il concetto di responsabilità condivisa tra tutti gli attori convolti nell'erogazione del servizio: produttori dei dispositivi, integratori, operatori del servizio sanitario inclusi medici e pazienti.
La guida si fonda sulla gestione del rischio e, restringendo il campo al modello di implementazione, sono stati in essa individuati alcuni requisiti per l'ambiente operativo dove i dispositivi vengono utilizzati e per il loro monitoraggio. I requisiti rilavanti ai nostri scopi sono sintetizzati di seguito come estratto delle misure NIS2:

Requisiti generali per gli ambienti operativi (dove sono presenti elettromedicali):

- Strumenti, politiche e meccanismi per la sicurezza dei sistemi IT:
  - Firewall / NGFW
  - Network segmentation
  - Meccanismi di partizionamento e segregazione del traffico di rete
  - Application safelist e blocklist
  - Utilizzo di filtraggio del traffico con hardware/software
  - Crittografia
  - Processo di Patch management
- Gestione delle identità e degli accessi:
  - Gestione degli accessi utente (credenziali uniche per accedere a software e device, politiche di accesso chiare e definite, etc.).
  - Tenere un inventario di tutti i dispositivi medici, monitorare e tenere traccia dei cambiamenti all'inventario.
  - Implementare appropriate misure di sicurezza per i lavoratori remoti.
- Monitoraggio:
  - Monitorare la corretta funzionalità degli apparati.
  - Investigare e rispondere agli incidenti.

Sulla base delle prescrizioni elencate viene definito il modello architetturale sintetizzato di seguito

- Identity and access management: fare riferimento ad un modello di accesso Zero Trust Network Access, secondo il quale l'accesso alla rete avviene in base al contesto e all'identità del dispositivo e della persona che lo utilizza. Particolarmente importante per i dispositivi medici sono le applicazioni di Network Access Control per il controllo continuo dell'accesso, IAM (Identity Access Management) / PAM (Privileged Access Management), integrate con sistemi di Multifactor Authentication (MFA) per la gestione delle identità e delle password. Considerato che molti dispositivi elettromedicali non hanno utenza, l'identificazione del dispositivo attraverso tecniche di fingerprinting sono essenziali da mettere in atto attraverso sistemi NAC e/o sonde di analisi del traffico
- IT Security Architecture: fare riferimento ad un modello di segregazione e compartimentazione del traffico di rete locale e geografica, filtraggio del traffico su base applicazione/utente, filtraggio del traffico in funzione delle application safe listing attraverso l'utilizzo di Firewall.
- Monitoring e detection: fare riferimento ad un modello di analisi dei log attraverso sistemi SIEM e di database verticali per i dispositivi elettromedicali. Inoltre, con il fine di controllare che anche il traffico generato dal dispositivo sia coerente con la sua funzione è auspicabile l'utilizzo di soluzioni di analisi del comportamento dei sistemi tipo NDR ed UEBA, aggiungendo

Il modello è illustrato dalla Figura 15.

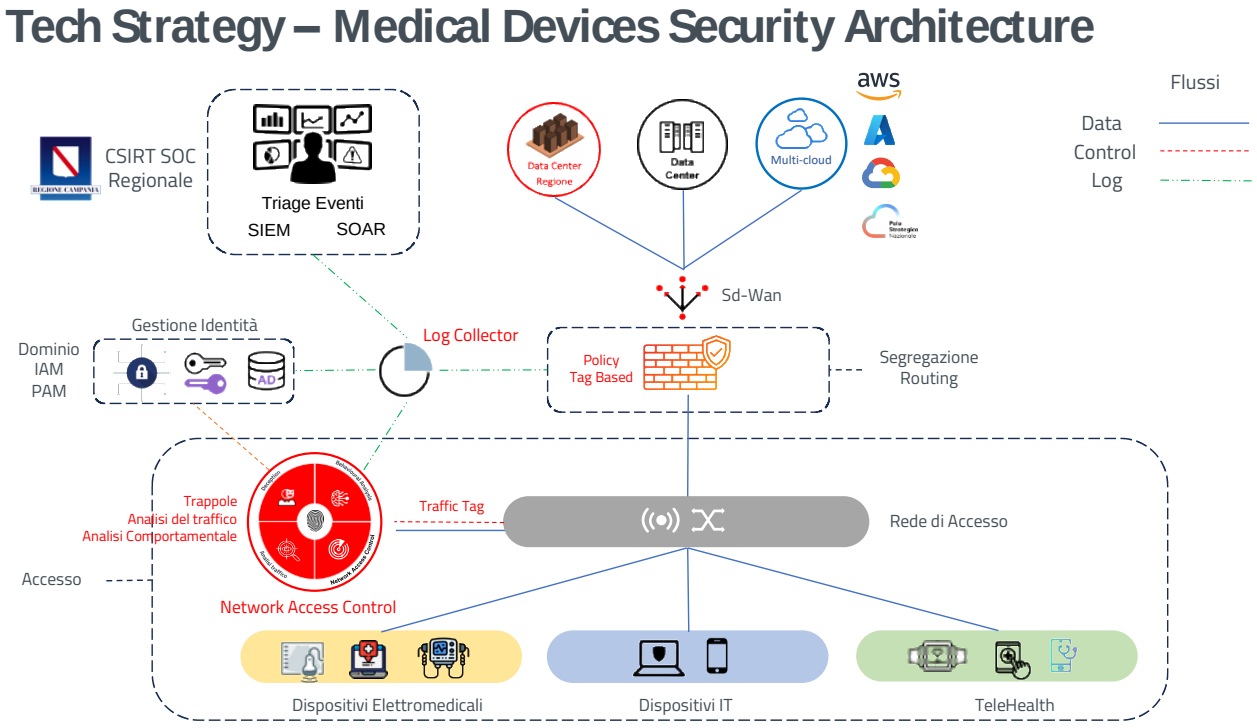


Figura 15: Architettura protezione Elettromedicali

Fondamentale implementare azioni di automazione tra applicazione delle politiche di sicurezza e monitoraggio delle operazioni attraverso soluzioni di piattaforma integrate (Gartner Cybersecurity Mesh Architecture (CSMA)). L'integrazione di supporti di Intelligenza Artificiale è un ulteriore elemento aggiuntivo utile alla riduzione dei tempi di rilevamento e contenimento delle minacce.

5 Best practices Supply Chain e Cyber security.

La "sicurezza della supply chain" si riferisce all'insieme di pratiche, politiche e tecnologie finalizzate a proteggere l'integrità, la confidenzialità e la disponibilità dei componenti, dei materiali e delle informazioni che compongono la catena di approvvigionamento di un'organizzazione. Una supply chain comprende tutte le fasi coinvolte nel processo di produzione e distribuzione di beni o servizi, dalla selezione dei fornitori fino alla consegna utenti finali.
Il tema della protezione della Supply Chain ai fini della resilienza informatica ha acquisto una importanza primaria nei processi di difesa, diventando rilevante per la NIS2. Il sistema dei fornitori e dei partner è un mezzo per condurre attacchi come è ben evidenziato nell'ultimo report sulla sicurezza della supply chain di ENISA(https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity), la quale, ha condotto una sondaggio presso i principali soggetti alla normativa con le seguenti evidenze:

- Sebbene le organizzazioni comprendano l'importanza della sicurezza della supply chain, non allocano le risorse necessarie.
- Anche quando investono in progetti di sicurezza informatica della supply chain, la maggioranza delle organizzazioni non utilizza una struttura chiara di gestione con la conseguente impossibilità di determinare il rapporto tra costi e benefici
- Le organizzazioni con procedure aziendali formalizzate di sicurezza della supply chain sono la minoranza, il settore bancario è quello con le politiche di sicurezza più consolidate e con un budget dedicato.
- La mancanza di criteri di gestione della sicurezza della supply chain crea problemi nel classificare e riportare gli incidenti.
- Le certificazioni rappresentano il modo preferito dalle organizzazioni per seguire le pratiche di sicurezza della supply chain anche se queste rappresentano costi elevati soprattutto per i fornitori non rilevanti allo scopo.
- Le organizzazioni intervistate concordano sul fatto che sarebbe vantaggioso definire requisiti comuni di sicurezza informatica per prodotti e servizi.
- La maggior parte delle organizzazioni intervistate non dispone di un sistema di gestione delle vulnerabilità che li copra tutti asset organizzativi, la gestione delle vulnerabilità e i test dei prodotti contribuiscono a migliorare la posizione di sicurezza informatica della supply chain ICT/OT.

Emergono alcune criticità in relazione al problema della sicurezza della supply chain. In particolare, emerge la mancanza di una governance aziendale e di politiche formalizzate per la gestione dei rapporti con i fornitori, approcci non coordinati alla qualità dei fornitori di prodotti/servizi e modalità ad hoc per la gestione delle vulnerabilità. Sulla base di questi risultati e sulla base delle disposizioni dell'articolo 21 della direttiva NIS2, vengono proposte alcune best practice per le cinque aree di interesse.

5.1 Approccio Strategico

Le organizzazioni soggette a NIS2 dovrebbero avere un approccio strategico alla sicurezza della supply chain, garantendo alcuni elementi fondamentali, quali:

- Le pratiche per la sicurezza informatica della supply chain ICT/OT sono stabilite, seguite, mantenute e documentate.
- Politiche aggiornate o altre direttive organizzative definiscono i requisiti per le attività della supply chain ICT/OT.
- Vengono fornite risorse adeguate (persone, finanziamenti e strumenti) per supportare la sicurezza informatica della catena di fornitura ICT/OT attività.

- I gruppi responsabili del rischio della catena di fornitura che includano dirigenti di tutta l'organizzazione (ad es. cyber, sicurezza, appalti, legale, privacy, gestione del rischio aziendale, ecc.) (NISTIR 8276 24). Il personale che svolge attività rilevanti per la sicurezza informatica della supply chain ICT/OT deve avere le competenze e conoscenze necessarie per svolgere le responsabilità assegnate.
- Responsabilità e autorità per lo svolgimento di attività rilevanti per la sicurezza informatica della supply chain ICT/OT sono assegnati al personale. Ruoli, strutture e processi collaborativi espliciti per la supply chain, vengono create funzioni di sicurezza informatica, sicurezza del prodotto e sicurezza fisica (NISTIR 8276).
- Il Consiglio di Amministrazione è sempre coinvolto nella sicurezza informatica della supply chain ICT/OT attraverso la valutazione del rischio e misure di performance (NISTIR 8276).

Coerentemente con l'approccio basato sulla valutazione del rischio, proprio della NIS2, è raccomandato si valutare con attenzione gli aspetti:

- La gestione del rischio derivante dalla supply chain risk;
- Le relazioni con I principali fornitori di servizi e prodotti.
- La gestione delle vulnerabilità dei prodotti e delle loro componenti;
- La qualità dei prodotti e le pratiche in termini di cybersecurity dei fornitori.

Questi elementi possono essere strutturati in un piano di azione (PDCA) tipo ciclo di miglioramento ISO 9001.

Figura 12: Ciclo per il miglioramento del rischio cyber della supply chain

I punti essenziali del processo sono di seguito descritti:

- Risk Assesment (Rif ISO 31000:2018). Il processo di risk assesment ha lo scopo di identificare e documentare la filiera dei fornitori di servizi e prodotti. Tale filiera deve essere corredata da una valutazione del rischio per l'organizzazione e per i servizi che essa eroga in caso di compromissione di componenti della filiera identificata.
- Supplier relationship management (ISO/IEC 27002:2022, capitoli 5.19–5.23). Il processo di gestione delle relazioni con i fornitori è essenziale per introdurre accordi, politiche e procedure che regolano le attività e le relazioni tra i soggetti, con lo scopo di ridurre i rischi di cybersecurity derivanti dalla filiera. Queta operazione è strettamente correlata all'analisi al punto precedente e deve essere supportata dal monitoraggio delle prestazioni dei fornitori e delle pratiche dei processi di Change Management.

- Vulnerability Handling (Rif ISO/IEC 27002:2022, Paragrafi 5.19 – 5.22 per utilizzatori, IEC 62443-4-1:20186 per produttori, IEC TR 62443-2-3:2015 Patch Management). Il processo di gestione delle vulnerabilità determina come l'organizzazione intende affrontarle. In relazione ai rischi che queste determinano per i propri asset, che devono essere misurati, l'organizzazione deve dotarsi di processi di mitigazione e politiche di manutenzione e monitoraggio. Le principali indicazioni per la gestione delle vulnerabilità sono declinate in tre categorie: per operatori IT e infrastrutture operative, produttori di dispositivi e/o componenti, system integrator
- Quality of product and services. Un elemento fondamentale per la sicurezza della supply chain è la qualità dei prodotti e dei servizi utilizzati. Ciò comporta che gli attori della catena del valore abbiano in campo processi di cyber security, utilizzino infrastrutture protette e misure tecniche che aumentino il livello di sicurezza dei prodotti e dei servizi erogati. La qualità deve essere Misurata e migliorata in modo continuativo, ed è fondamentale che le aziende facenti parte della supply chain siano trasparenti sulle pratiche di cybersecurity adottate per la propria produzione di prodotti e servizi.

Le pratiche elencate dovrebbero essere attuate in conformità a quanto richiesto dalla NIS2 da tutte le organizzazioni definite come essenziali ed importanti per le proprie filiere. Va notato che queste organizzazioni sono, al contempo, organizzazioni essenziali/importanti e fornitori di servizi e prodotti. Questo tipo di organizzazioni possono attuare buone pratiche per quattro categorie di fornitori: produttori di componenti e prodotti finiti, system integrator, managed security service provider e provider di servizi digitali.
Si rimanda al documento di ENISA per i dettagli relativi alle buone pratiche per le categorie elencate ((https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity). Questo documento risposta in maniera tabellare le indicazioni de seguire per ognuna delle categorie di organizzazioni elencate precedentemente. Piu specificatamente, per determinare una architettura di buone pratiche più granulare e correlata al rischio si rimanda alla raccomandazione NIST SP 800-161 Rev. 1 (https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf)

5.1.1 Aree di interesse

In maniera sintetica è possibile elencare alcune aree di interesse, alle quali occorre prestare particolare attenzione, sui cui si focalizza principalmente la sicurezza della supply chain, tra queste:

- **Integrità dei Prodotti:**
  Garantire che i prodotti o i componenti non siano alterati o compromessi durante il trasporto o la produzione, prevenendo la contraffazione e assicurando che siano conformi agli standard di qualità.
- **Sicurezza Fisica:**
  Proteggere gli elementi fisici della catena di approvvigionamento, come gli impianti di produzione, i magazzini e i mezzi di trasporto, da minacce come furti, danneggiamenti o atti terroristici.
- **Gestione dei Fornitori:**
  Valutare e monitorare la sicurezza dei fornitori per garantire che seguano le migliori pratiche e standard di sicurezza, riducendo il rischio di forniture da fonti non affidabili. Questo può avvenire anche, ma non solo, attraverso le certificazioni conseguite dai fornitori.
- **Protezione delle Informazioni:**
  Assicurare la confidenzialità delle informazioni sensibili all'interno della catena di approvvigionamento, come dati finanziari, progetti di produzione e informazioni strategiche, per evitare furti di dati o spionaggio industriale.
- **Resilienza e Continuità Operativa:**

Pianificare e implementare misure per affrontare interruzioni nella catena di approvvigionamento, garantendo la continuità operativa anche in situazioni di emergenza o crisi.

- **Conformità Normativa:**
  Rispettare le normative e gli standard di sicurezza specifici del settore o geografici per evitare sanzioni legali e garantire che la catena di approvvigionamento sia in linea con le regolamentazioni applicabili.
- **Monitoraggio e Tracciabilità:**
  Implementare sistemi di monitoraggio e tracciabilità per identificare rapidamente eventuali anomalie o problemi nella catena di approvvigionamento e rispondere tempestivamente.

5.2 Raccomandazioni e report

- NIST SP 800-160 Vol. 2 Rev. 1: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
- NIST Special Publication (SP) 800-160: Systems Security Engineering—Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy; and NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations.
- NIST Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security
- NIST SP 800-207A. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments
- NIST SP 800-210: General Access Control Guidance for Cloud Systems
- ISO/IEC/IEEE 15288:2015, Systems and software engineering—Systems life cycle processes.
- IEC 62443. International series of standards that address cybersecurity for operational technology in automation and control systems.
- MDCG 2019-16 - Guidance on Cybersecurity for medical devices.
- Framework Nazionale per la Cybersecurity e la Data Protection
- https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
- https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf
- LA MINACCIA CIBERNETICA AL SETTORE SANITARIO, Analisi e raccomandazioni, ACN, ottobre 2024

5.3 Legislazione

- DECRETO LEGISLATIVO 18 maggio 2018, n. 6: Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
  - Art. 12. Obblighi in materia di sicurezza e notifica degli incidenti
    1. Gli operatori di servizi essenziali adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente. 2. Gli operatori di servizi essenziali adottano misure adeguate a prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei

sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi. 3. Nell'adozione delle misure di cui ai commi 1 e 2, gli operatori di servizi essenziali tengono conto delle linee guida predisposte dal gruppo di cooperazione di cui all'articolo 10, nonché delle linee guida di cui al comma 7. 4. Fatto salvo quanto previsto dai commi 1, 2 e 3, le autorità competenti NIS possono, se necessario, definire specifiche misure, sentiti gli operatori di servizi essenziali. 5. Gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti. 6. Il CSI

- Art. 14. Obblighi in materia di sicurezza e notifica degli incidenti 1. I fornitori di servizi digitali identificano e adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relativi alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dell'offerta di servizi di cui all'allegato III all'interno dell'Unione europea. 2. Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente e tengono conto dei seguenti elementi: a) la sicurezza dei sistemi e degli impianti; b) trattamento degli incidenti; c) gestione della continuità operativa; d) monitoraggio, audit e test; e) conformità con le norme internazionali. 3. I fornitori di servizi digitali adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali sui servizi di cui all'allegato III offerti all'interno dell'Unione europea, al fine di assicurare la continuità di tali servizi.

- DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 14 aprile 2021, n. 81.
- DECRETO LEGISLATIVO 18 maggio 2018, n. 65 Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. (18G00092) (GU Serie Generale n.132 del 09-06-2018)
- Medical Device Regulation: Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE

5.4 Classi datacenter

SERVIZI CLOUD: REQUISITI DI QUALIFICAZIONE

- Certificazione richiesta
- Dichiarazione di conformità allo schema richiesta

	Requisiti (incrementali)	Requisiti principali (sovranità)	Certificazioni richieste
ORDINARIO	QC1 — 40 Sicurezza 17 Qualità, Performance, Interoperabilità	• **Infrastruttura e dati localizzati in EU** (no vincoli sui metadati) • Richieste accesso ai dati della PA da entità extra-EU **notificate ad ACN e alla PA.** • **Nessun accesso è accordato** senza l'autorizzazione della PA	• ISO 27001 (est. 27017/18 o CSA STAR L2) • ISO 9001 (Qualità)
CRITICO	QC2 — + 8 Sicurezza (48) [+23 estesi]	• **Localizzazione in EU anche per i metadati** • **Funzionalità Bring-Your-Own-Key (BYOK) fornite dal provider** (inclusi requisiti specifici sugli HSM, e su generazione e gestione delle root keys)	• ISO 27001 (est. 27017/18 o CSA STAR L2) • ISO 9001 (Qualità) • ISO 20000 (IT Service Management) • ISO 22301 (Business Continuity)
STRATEGICO	QC3 — + 2 Sicurezza (50) [+ 21 estesi]	• **Controllo delle attività** privilegiate (inclusi aggiornamenti e accessi ai dati della PA) **esteso al personale del CSP** • Aggiornamenti verificati in ambiente di test, anche ai fini di sicurezza • **Informazioni su sedi e infrastrutture da cui è erogato il servizio cloud** rese disponibili alla PA	• ISO 27001 (with 27017/018*) • CSA STAR L2 • ISO 9001 (Qualità) • ISO 20000 (IT Service Management) • ISO 22301 (Business Continuity)
	QC4 — +1 Sicurezza (51) [+ 2 estesi]	• **Funzionalità Hold-Your-Own-Key (HYOK) fornite dal provider** (inclusi requisiti specifici di gestione autonoma PA degli HSM e generazione e gestione delle chiavi) • **Flussi** dati da/verso esterno **soggetti a procedure di approvazione,** monitoraggio e controllo **concordate con la PA** • **Autonomia operative: il CSP deve essere** autonomo nella fornitura del servizio cloud e nella gestione dell'infrastruttura fisica e logica sottostante. Terze parti solo se assicurata la fungibilità	• ISO 27001 (with 27017/018*) • CSA STAR L2 • ISO 9001 (Qualità) • ISO 20000 (IT Service Management) • ISO 22301 (Business Continuity)

5.5 Appendice termini di sicurezza ed acronimi

Si lascia una descrizione breve per molti degli acronimi utilizzati nel documento

- **Next Generation Firewall (NGFW)**: Firewall che vadano a segmentare e controllare l'accesso all'interno di tutti gli ambienti, che questi siano on premise o in cloud remoti. Il ruolo del next generation firewall sarà sia proteggere il livello Edge per il controllo del traffico da e verso internet su tutti gli ambienti che sono parte della rete dell'ente, sia quello di segmentare e controllare il traffico tra le varie strutture. Il controllo e la segmentazione dell'infrastruttura, che sia essa ospitata in un cloud pubblico o privato, dovrà seguire la stessa logica essendo le minacce del tutto simili indipendentemente dal tipo di ambiente utilizzato.

- **Web Application Firewall (WAF)**: L'esposizione di servizi Web, che siano essi interni o pubblici, richiede una protezione verticale attraverso prodotti che siano in grado di utilizzare in modo spinto le funzionalità di machine learning/intelligenza artificiale e offrano un pannello di gestione singolo con le altre funzionalità di sicurezza, in particolar modo con i Next Generation Firewall che andranno a gestire lo stesso traffico che verrà protetto dai Web Application firewall. È importante proteggere anche i servizi acceduti internamente dagli utenti aziendali attraverso un WAF, perché le minacce possono provenire anche dall'interno, internet non è l'unico vettore di attacco per i servizi web aziendali.

- **Network Access Control (NAC)**: In un mondo in cui le reti contengono sempre più apparati IoT e IoMT occorre gestire e controllare l'accesso per andare ad applicare logiche di segmentazione spinte così da sfruttare le funzionalità di sicurezza dei Next Generation Firewall per la protezione di tutti i dispositivi vulnerabili presenti all'interno delle reti. Per gestire tale complessità è necessario applicare logiche di Network Access Control per andare ad automatizzare l'accesso alla rete e renderla autoadattante alla operatività giornaliera che gli utenti e gli oggetti necessitano.

- **Multi-Factor Authentication (2FA/NAC)**: Abilitare tecniche di autenticazione forte, basate su tecnologie multi-fattore, che vadano a gestire sia gli accessi ai dispositivi di rete (ad. es. VPN), sia l'accesso alle applicazioni attraverso concetti di federazioni basati su protocolli standard quali SAML, OAUTH2, OIDC, RADIUS, ecc.

- **Zero Trust Network Access (ZTNA)**: Gestire l'accesso a risorse, dati e servizi attraverso l'abbinamento di tecnologie per l'autenticazione forte a una verifica posturale del dispositivo utilizzato per accedere agli stessi. Certificare utenti e dispositivi e persino le singole connessioni alle risorse esposte in modo da garantire che l'accesso sia autorizzato solo a dispositivi che rispettino le regole di compliance e siano conosciuti e censiti tra gli asset aziendali.

- **Application Delivery Controller (ADC / GSLB)**: La resilienza dei servizi distribuiti su più datacenter e la corretta gestione dell'accesso agli stessi attraverso una catena che includa sistemi di protezione (IPS, WAF, ZTNA, ecc.), richiede la presenza di funzionalità che vengono erogate da bilanciatori di carico. Quest'ultimi possono garantire l'accesso ai servizi, alle risorse, alle singole reti o a qualsiasi elemento dell'infrastruttura multi-cloud in maniera intelligente mediante l'applicazione di politiche di global server load balancing, di bilanciamento dei servizi di backend e di verifica dello stato operativo consentendo di avere una rete resiliente a qualsiasi interruzione di servizio. Inoltre, la pubblicazione dei servizi attraverso il livello di astrazione dato dal bilanciatore di carico consente di semplificare le politiche di sicurezza e di inibire l'accesso diretto ai sistemi da parte degli utenti finali.

- **Endpoint Detection and Response (EDR)**: La protezione delle postazioni di lavoro aziendali dagli attacchi di nuova generazione richiede di utilizzare tecnologiche che si basino sull'analisi comportamentale; un normale antivirus non è più sufficiente data l'enorme e continua evoluzione delle tecniche di attacco. La soluzione di Endpoint Detection and Response (EDR) abilita un livello di protezione completamente basato sull'analisi comportamentale ed in grado di proteggere dagli attacchi di nuova generazione, quali: Ransomware, Fileless Attack, Privilege Escalation, Persistence, Evasion, ecc. La soluzione EDR deve integrarsi nativamente con il resto delle tecnologie di sicurezza, quali: Next Generation Firewall, Network Access Control, ecc., per automatizzare il più possibile le risposte agli eventi di sicurezza rilevati. Stessa considerazione, fatte le dovute eccezioni, può essere applicata per proteggere anche i server.

- **E-mail Security (MS)**: La posta elettronica è il maggior vettore di infezione andando a colpire la parte più debole del perimetro dell'ente: l'utente finale. L'utilizzo di servizi cloud non garantisce una protezione completa contro gli attacchi evoluti, è necessario implementare tecniche di analisi del traffico di posta che includano sistemi evoluti di protezione dallo spam e soprattutto sistemi di sandboxing che garantiscano l'analisi statica e dinamica dei contenuti prima che questi possano arrivare agli utenti finali.

- **Sandboxing (SANDBOX)**: Proteggere le infrastrutture richiede abilitare controlli per ciò che viene scaricato e ricevuto secondo vari vettori dagli utenti ed i servizi. Il sistema di Sandboxing si deve integrare con posta elettronica, next generation firewall, web application firewall e application delivery controller così da poter proteggere sia gli utenti finali che i servizi esposti da eventuali tentativi di invio di malware e zero day da parte degli attaccanti.

- **Log Management (SIEM)**: Infrastruttura centralizzata di Log Management che offra una console di gestione univoca per l'archiviazione, il monitoraggio e la reportistica dei log prodotti da tutte le

tecnologie di sicurezza implementate. L'unificazione della gestione rende molto più facile le operazioni di verifica ed analisi da parte degli operatori, console separate con dati eterogenei rendono il lavoro degli operatori complesso e con enormi difficoltà nel correlare evidenze prodotte da tecnologie diverse.

- **Network Behavioral (NDR)**: Conoscere è fondamentale per capire che qualcosa sta accadendo all'interno dell'infrastruttura, tecnologie quali Deception, Network Detection and Response, Network Asset Visibility and Control e User Entity Behavioral Analytics', consentono agli amministratori di capire in anticipo che all'interno delle reti avvengono comportamenti non autorizzati e potenzialmente pericolosi. In particolar modo la tecnologia di deception consente di andare a capire che all'interno della rete stanno avvenendo movimenti laterali senza rischi di falsi positivi. L'interazione del sistema di deception con gli apparati di network access control e next generation firewall consente l'immediato isolamento della minaccia.

- **Vulnerability Management – Digital Risk Protection (VA/PT, DRP)**: Effettuare in modo periodico ed approfondito attività di vulnerability management e penetration test è fondamentale per capire come configurare correttamente gli apparati di sicurezza e come intervenire per contenere o risolvere le vulnerabilità presenti nei servizi erogati. Inoltre, risulta fondamentale conoscere e gestire l'esposizione digitale della propria organizzazione, conoscere se ci sono interessi verso la stessa da parte di gruppi hacker e criminali, se nel deep web si scambiano informazioni sui dati ed utenti della propria struttura e se ci sono tentativi di costruire informazioni falsificate per tentare di ingannare gli utenti che accedono ai servizi erogati dall'ente.

- **Privileged Access Management (PAM)**: Isolare il perimetro di gestione dell'infrastruttura dagli utenti che accedono per i servizi di manutenzione e gestione è fondamentale per impedire accessi non controllati alla parte più delicata dell'infrastruttura aziendale e per impedire che eventuali vulnerabilità possano essere sfruttare per ottenere accessi amministrativi ai sistemi aziendali. Il sistema di privileged access management è fondamentale per controllare e limitare gli accessi, impedire movimenti non autorizzati e loggare le attività di manutenzione effettuate dal personale interno ed esterno che interagisce con i sistemi dell'ente.

- **Security Information and Event Management (SIEM)**: Implementare un SIEM è il tassello fondamentale per costruire un primo livello di Security Operation Center, questo primo livello dovrà controllare gli eventi catturati dai vari sistemi di sicurezza e gestire i log dei sistemi aziendali compresi i dispositivi di rete. L'infrastruttura SIEM dovrà essere centralizzata, multitenant e gerarchica, andando a costituire la base dei servizi CSIRT regionali. Ogni ente dovrebbe avere la possibilità di gestirsi il proprio SIEM o utilizzare un tenant del servizio centralizzato erogato dalla regione; la regione gestirà centralmente gli eventi importanti in modo da costruire la base di un SOC ed aggregherà gli incidenti in modo da aiutare gli enti nelle fasi di riconoscimento e risposta degli incidenti di sicurezza.

- **Security Orchestration, Automation and Response (SOAR)**: Un servizio SOC evoluto richiederà l'implementazione di un sistema SOAR che vada ad automatizzare la risposta agli incidenti di sicurezza andando a scremare il rumore di fondo e consentendo alla squadra di Incident Response della regione di utilizzare le funzionalità del sistema per analizzare, gestire e mitigare eventuali eventi realmente importanti. Funzionalità di automazione, di arricchimento delle informazioni, di War Room e gestione del flusso di lavoro sono fondamentali per ottimizzare e velocizzare la risposta agli incidenti. Il sistema dovrà implementare ed essere parte dei flussi di lavoro che

verranno definiti dagli operatori SOC e dal gruppo di Incident Response. Con una gestione centralizzata della sicurezza si può ottenere un'analisi completa degli incidenti e un quadro chiaro della postura di Sicurezza dell'ente.

- **DLP** è l'acronimo di Data Loss Prevention, che in italiano può essere tradotto come "Prevenzione della Perdita di Dati". Il DLP è una strategia e un insieme di tecnologie progettate per proteggere i dati sensibili da perdite non autorizzate o dalla divulgazione accidentale. L'obiettivo principale del DLP è garantire che le informazioni critiche di un'organizzazione siano gestite e condivise in modo sicuro, prevenendo la fuga di dati riservati.

- **CASB** Acronimo di Cloud Access Security Broker, è una soluzione di sicurezza informatica progettata per proteggere l'accesso ai servizi cloud all'interno di un'organizzazione. In sostanza, un CASB agisce come intermediario tra gli utenti e i servizi cloud, garantendo un controllo granulare e una sicurezza avanzata per le risorse e i dati gestiti attraverso piattaforme cloud.

- **ZERO DAY** Il termine "0day" o "zero day" si riferisce a una vulnerabilità informatica che è stata appena scoperta o divulgata, ma per la quale non esiste ancora un fix o una patch ufficiale da parte del produttore del software. In altre parole, è una vulnerabilità "zero-day" perché gli sviluppatori non hanno avuto alcun tempo, o zero giorni, per risolvere il problema prima che diventasse di dominio pubblico o venisse sfruttato da malintenzionati.