UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria
Corso di Laurea Magistrale in Ingegneria Informatica e dell'Automazione

---

Metodologie di valutazione della sicurezza di servizi Cloud qualificati per la Pubblica Amministrazione

Security assessment methodologies of qualified Cloud services for the Public Administration

Candidato:
Lorenzo Tiseni

Relatore:
Prof. Luca Spalazzi

Correlatore:
Dott. Ivan di Pietro

Anno Accademico 2022-2023

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria
Corso di Laurea Magistrale in Ingegneria Informatica e dell'Automazione

---

Metodologie di valutazione della sicurezza di servizi Cloud qualificati per la Pubblica Amministrazione

Security assessment methodologies of qualified Cloud services for the Public Administration

Candidato:
Lorenzo Tiseni

Relatore:
Prof. Luca Spalazzi

Correlatore:
Dott. Ivan di Pietro

Anno Accademico 2022-2023

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea Magistrale in Ingegneria Informatica e dell'Automazione
Via Brecce Bianche – 60131 Ancona (AN), Italy

If you take a Rook, promote to a Knight, and
fork the King and the Queen, you don't need
to win a chess game for three lifetimes.
You just solved chess

Sommario

La migrazione dei dati e servizi delle Pubbliche Amministrazioni su Cloud potrebbe cambiare il volto del paese, accelerando il processo di transizione verso il digitale e permettendo l'erogazione di servizi migliori ai cittadini. Tuttavia, nonostante gli indubbi vantaggi che si ottengono dall'utilizzo delle tecnologie Cloud, sono emersi nuovi rischi cyber, derivanti dalla migrazione, i quali possono avere importanti ripercussioni sull'economia del paese e sulla *safety* dei cittadini. Per questo motivo, l'Agenzia Nazionale per la Cybersicurezza ha definito dei controlli o requisiti di sicurezza che un fornitore dei servizi Cloud deve rispettare per ospitare dati e servizi delle Pubbliche Amministrazioni. Lo scopo dei controlli è garantire un processo di transizione verso il Cloud sicuro per le Amministrazioni, certificando in maniera adeguata i fornitori attraverso un processo di qualificazione. L'obiettivo di tale processo è quello di verificare che tutti i controlli di sicurezza definiti siano correttamente implementati dal fornitore a cui le Amministrazioni affideranno i loro dati. Tuttavia, operare questa verifica senza un approccio standardizzato, potrebbe allungare i tempi di ispezione e ritardare il processo di transizione verso il digitale per le Amministrazioni. Per fornire un valido aiuto al regolatore nel processo di qualificazione, nell'ambito della tesi presentata, sono state sviluppate metodologie standard di verifica dei controlli di sicurezza elaborati dall'Agenzia. Il processo di sviluppo è stato svolto in maniera da fornire al regolatore un insieme di metodologie adeguabili all'evoluzione delle leggi e del contesto tecnologico, ma allo stesso tempo immediatamente applicabili e adatte per condurre ispezioni accurate. Infatti, alcune metodologie sviluppate sono state subito applicate, ove possibile, per verificare se tre fornitori di servizi Cloud leader nel mercato, come Microsoft Azure, Google Cloud e Amazon Web Services, implementano in maniera corretta i controlli di sicurezza definiti. In più, come caso di studio approfondito, grazie all'intermediazione dell'Agenzia, è stato possibile applicare una particolare metodologia, che richiede una verifica approfondita sui servizi Cloud di Amazon Web Services. La tematica dell'ispezione ha riguardato un aspetto di importante rilevanza strategica per le Pubbliche Amministrazioni, quale la localizzazione dei loro dati e servizi all'interno di infrastrutture digitali situate in Unione Europea. In particolare, è stata effettuata una valutazione degli strumenti messi a disposizione da Amazon Web Services per supportare le Amministrazioni nella localizzazione dei propri dati in Unione Europea. Al termine della valutazione è stato formulato un giudizio globale sugli strumenti individuati, indicandone tratti salienti, pregi e criticità. Il giudizio formulato contribuirà ad accelerare il processo di qualificazione di un grande fornitore di servizi Cloud come AWS, in maniera da

permettere alle Amministrazioni di beneficiare di tutti i vantaggi dei suoi servizi e della sua infrastruttura Cloud, per portare a termine la transizione verso il digitale.

Indice

Elenco delle figure

Elenco delle tabelle

Elenco dei Listati

Introduzione

Nell'ultimo ventennio le organizzazioni come aziende o Amministrazioni Pubbliche hanno sviluppato l'esigenza di poter gestire, utilizzare e immagazzinare una crescente quantità di dati, e l'esigenza di poter erogare i loro servizi a un pubblico sempre più vasto. Tuttavia, molte di queste organizzazioni, specialmente quelle pubbliche, non trovando conveniente o non essendo in grado di sostenere i costi elevati che una soluzione cosiddetta "on-premise" comporta hanno preferito adottare una soluzione Cloud. Infatti una soluzione "on-premise" richiede la presenza all'interno del perimetro dell'organizzazione di un datacenter, i cui costi di realizzazione, di esercizio e di manutenzione sono elevati. A questi costi vanno inoltre aggiunti i costi dovuti alla necessità di avere apposito personale qualificato. Al contrario, affidarsi ad un Cloud Service Provider permette di soddisfare le nuove esigenze che le organizzazioni hanno sviluppato, con facilità e costi contenuti.

Migrando verso un servizio Cloud, le aziende possono offrire i loro servizi a un pubblico sempre più vasto, senza preoccuparsi della gestione dei carichi di lavoro delle macchine, del mantenimento dell'hardware e dei data center e del provisioning delle risorse, che è affidata al provider. Perciò, a fronte del pagamento di una tariffa, un'organizzazione può gestire tutti i suoi servizi occupandosi solo dello strato software, con totale trasparenza rispetto allo strato fisico sottostante che è gestito dal fornitore di servizi Cloud. Per le Pubbliche Amministrazioni, in particolare, il processo di migrazione verso il Cloud di propri servizi è previsto dal principio del *cloud-first* sancito dalla Strategia nazionale sul Cloud computing[7]. I vantaggi offerti dal Cloud hanno permesso lo sviluppo veloce di moltissime aziende che hanno potuto crescere e raggiungere una dimensione che prima non era nemmeno immaginabile. Sfruttare questi vantaggi anche per le Pubbliche Amministrazioni potrebbe contribuire a un miglioramento dei servizi offerti ai cittadini.

La gestione dello strato fisico sottostante ai servizi Cloud, affidata al fornitore di servizi Cloud, non comprende solo aspetti legati al dimensionamento delle risorse e al mantenimento dell'hardware, ma anche aspetti di sicurezza. La migrazione verso un fornitore di servizi Cloud, comporta, per l'organizzazione che la intraprende, anche l'attuazione di una strategia di condivisione del rischio cyber con il provider. Infatti, nella tariffa corrisposta per usufruire dei servizi di un Cloud provider, è incluso anche il costo di gestione di tutti gli aspetti di sicurezza fisica e logica all'interno dei data center. Quindi, a differenza di una gestione on-premise, in cui il rischio

è solo a carico dell'organizzazione, con la migrazione verso un fornitore di servizi Cloud, il rischio è condiviso tra organizzazione e fornitore. Questo aspetto scarica di responsabilità l'organizzazione che migra su Cloud, consentendogli di concentrarsi solo sullo sviluppo e sulla sicurezza delle proprie applicazioni su Cloud.

D'altro canto, la migrazione verso il Cloud di moltissime organizzazioni ha posto nuove implicazioni a livello di sicurezza, specialmente per il fatto che il Cloud lavora con un modello multi-tenant. Quindi, quando si sceglie di usufruire di servizi Cloud, è importante sapere che nelle stesse macchine fisiche potrebbero essere ospitati anche servizi diversi appartenenti ad aziende diverse. Questo comporta che è compito del Cloud Service Provider mantenere un certo livello di isolamento tra i singoli tenant, al fine di non causare incidenti di sicurezza o situazioni inaspettate per i clienti. Lo stesso discorso si può applicare ai dati, in quanto i dati di un'azienda possono essere immagazzinati nello stesso dispositivo di storage in cui sono immagazzinati i dati di un'altra.

Questa caratteristica del Cloud, che per un'azienda privata può avere conseguenze prettamente economiche, per gli enti pubblici rappresenta un problema di sicurezza da non sottovalutare. A differenza di un'azienda privata, un'Amministrazione pubblica, come un'Azienda Sanitaria Regionale o Locale, si trova a gestire dati sensibili appartenenti a cittadini italiani, e quindi deve essere conforme al GDPR. Inoltre, alcune Amministrazioni Pubbliche erogano servizi che sono di importanza strategica per il paese, la cui compromissione potrebbe produrre scenari problematici, che potrebbero sfociare nel blocco di alcune attività fondamentali sia per l'economia che per i cittadini. Ad esempio, se il servizio di gestione della rete elettrica del paese viene compromesso, il risultato potrebbe anche comportare l'assenza di corrente in alcune zone dell'Italia, generando perdite economiche e danni alla *safety* delle persone.

Per questo, la migrazione dei servizi e dati appartenenti a un'Amministrazione Pubblica verso un servizio Cloud è un processo delicato che va condotto in maniera attenta. Non è più sufficiente pensare alla sicurezza in termini tradizionali, valutandola solo al livello di singola applicazione, piattaforma o infrastruttura, ma è necessario cambiare prospettiva e valutare la sicurezza offerta dal modello Cloud e dal fornitore di servizi Cloud. Si rende necessario valutare il livello di sicurezza che si ottiene migrando verso un certo Cloud Service Provider, attraverso un processo di qualificazione del servizio che comprenda anche metodologie di Vulnerability Assessment e Penetration Testing. Lo scopo ultimo del processo citato è quello di stabilire se il fornitore di servizi Cloud permetta a chi migra su Cloud di continuare a offrire i propri servizi, garantendo ai clienti finali la riservatezza, l'integrità e la disponibilità delle informazioni e dei servizi.

Concentrando l'attenzione sulle Amministrazioni Pubbliche, il processo di qualificazione di un Cloud Service Provider e dei servizi da esso offerti non va solamente

definito al livello tecnico. Infatti, è necessario creare un impianto legislativo a supporto degli organi di controllo che si occupano di certificare che un fornitore di servizi Cloud sia adatto per una determinata Amministrazione pubblica. A partire dal 2012 sono stati emanati decreti legge finalizzati a definire un'agenda digitale del Paese e individuare degli organi pubblici a cui demandare la definizione di un regolamento contenente i livelli minimi di sicurezza delle infrastrutture digitali del paese, dei servizi Cloud a cui si possono affidare le Pubbliche Amministrazioni, e il processo di migrazione delle PA verso il Cloud. I decreti legge adottati hanno affidato tale responsabilità, precedentemente a carico dell AgID (Agenzia per l'Italia Digitale), all'Agenzia Nazionale per la Cybersicurezza (ACN) istituita nell'agosto 2021. L'Agenzia ha continuato un lavoro precedentemente iniziato da AgID, modificando il regolamento per i servizi Cloud a cui si fa riferimento nell'articolo 33-septies comma 4 del Decreto Legge 18 Ottobre 2012, n. 179[8].

Tale lavoro è risultato nell'adozione di una determina del direttore generale ACN, la determina n. 307 del 18 gennaio 2022[9], che contiene una serie di allegati recanti *l'aggiornamento degli ulteriori livelli minimi di sicurezza, capacità elaborativa, e affidabilità delle infrastrutture digitali per la pubblica amministrazione e delle ulteriori caratteristiche di qualità, sicurezza, performance e scalabilità dei servizi Cloud per la pubblica amministrazione, nonché i requisiti di qualificazione dei servizi Cloud per la pubblica amministrazione*. Gli allegati nella determina sono stati impostati seguendo la divisione in Funzioni, Categorie e Sottocategorie del Framework Nazionale per la Cybersecurity e la Data Protection[5], includendo solo le Sottocategorie del Framework essenziali per il contesto del Cloud, e aggiungendone alcune per esprimere i requisiti di qualità, performance e scalabilità e interoperabilità. Successivamente per ogni Sottocategoria è stata elaborata una lista di controlli di sicurezza, ovvero dei requisiti veri e propri che i fornitori di servizi Cloud devono rispettare al fine di ottenere la qualificazione.

Tuttavia, la sola definizione di questi requisiti di sicurezza non è sufficiente per aiutare il regolatore nel processo di ispezione presso il fornitore di servizi Cloud, finalizzato al rilascio della qualificazione. Infatti, ogni controllo di sicurezza specificato nella determina indica solo cosa deve implementare o produrre il fornitore di servizi Cloud al fine di ottenere la qualificazione. Al contrario il regolatore che si occupa di verificare l'implementazione di ogni controllo presso il fornitore non ha nessuna indicazione su come svolgere la verifica. Tale aspetto potrebbe complicare molto il processo di qualificazione dei Cloud Provider per la Pubblica Amministrazione, rallentando così il processo di transizione digitale del paese. Per questo, oltre alla definizione dei controlli di sicurezza specificati dalla determina n. 307, occorre individuare metodologie e linee guida per consentire all'autorità preposta di verificare la corretta attuazione di quei controlli. Tali metodologie, prescriveranno all'autorità preposta come condurre la verifica e stabilire se il requisito di sicurezza espresso dal

controllo è correttamente implementato dal fornitore di servizi Cloud.

Lo scopo del lavoro presentato è quello di sviluppare delle metodologie accurate, specifiche ed adeguate, per permettere al regolatore di svolgere delle verifiche celeri e accelerare il processo di qualificazione dei fornitori di servizi Cloud, senza però mettere in secondo piano le implicazioni di sicurezza. Infatti, sarà necessario coniugare, nello sviluppo delle metodologie di verifica, il bisogno di svolgere ispezioni in maniera rapida e standardizzata, con l'esigenza di verificare ogni minimo aspetto di sicurezza citato dai controlli. Al fine di offrire metodologie immediatamente utilizzabili e modificabili nel futuro dal regolatore, lo sviluppo sarà preceduto da una classificazione in categorie dei controlli di sicurezza. Inoltre, parte del lavoro comprenderà anche l'applicazione di alcune metodologie sviluppate, a meno che queste non includano delle verifiche da effettuare nell'ambiente o infrastruttura Cloud del fornitore. Le metodologie saranno applicate per effettuare verifiche su tre grandi Cloud Service Provider leader nel mercato, ovvero Microsoft Azure, Google Cloud e Amazon Web Services. I risultati di tali ispezioni saranno raccolti all'interno di un documento strutturato, riportato in Appendice, che verrà poi fornito all'Agenzia Nazionale per la Cybersicurezza.

Nell'ambito dell'applicazione delle metodologie sviluppate, rientrerà anche la discussione di un caso di studio approfondito, sviluppato in collaborazione con Amazon Web Services (AWS), grazie all'intermediazione di ACN. In particolare, lo scopo della verifica più approfondita, sarà fornire un giudizio sulla validità degli strumenti messi a disposizione da AWS per la localizzazione dei dati delle Amministrazioni in infrastrutture digitali situate in Unione Europea. Il motivo principale che giustifica l'approfondimento della verifica di questo particolare requisito di sicurezza, risiede nel fatto che avere il controllo sulla posizione dei propri dati all'interno dell'infrastruttura di un provider ha grande importanza strategica per l'Amministrazione. Inoltre, avere la possibilità di farlo all'interno di un fornitore di servizi Cloud leader nel mercato come AWS potrebbe essere una grande opportunità per accelerare la transizione verso il Cloud delle Amministrazioni Pubbliche.

L'elaborato prodotto nel corso del lavoro ha una struttura finalizzata ad offrire una piena comprensione del problema e a descrivere come questo è stato affrontato, presentando tutti i risultati raggiunti. Nel Capitolo 1 verrà descritta in breve la tecnologia Cloud e la sua diffusione, al fine di mettere in luce alcuni aspetti di sicurezza rilevanti e comprendere quanto e come le organizzazioni si affidino ai fornitori di servizi Cloud. Il Capitolo 2, presenterà il quadro normativo vigente sulle tecnologie Cloud e sul processo di qualificazione, focalizzandosi su alcuni decreti legislativi e sulla *Strategia Cloud Italia*, che è stata la base per la definizione del processo di qualificazione. Successivamente con il Capitolo 3 si descriveranno tutti i regolamenti e le determine elaborate per la definizione dei requisiti a cui devono aderire i fornitori di servizi Cloud e del processo di qualificazione, descrivendo anche i Framework per la sicurezza da cui prendono spunto.

Terminata la descrizione del contesto al contorno, con il Capitolo 4 si descriverà in dettaglio il processo di sviluppo delle metodologie e il suo risultato finale. In particolare, verranno evidenziate tutte le difficoltà e le criticità incontrate durante il lavoro, presentando anche le relative soluzioni e alcuni esempi sia di metodologie, che di verifiche condotte. Successivamente, il Capitolo 5 presenterà in dettaglio la valutazione degli strumenti per la localizzazione dei dati messi a disposizione da Amazon Web Services. Al fine di permettere una comprensione adeguata delle valutazione finale prodotta, si riporterà anche la descrizione di alcuni aspetti base dell'infrastruttura e dei servizi Cloud AWS, e la descrizione approfondita di ogni strumento individuato per garantire la localizzazione dei dati in UE. Infine, nel Capitolo 6 saranno presentati in maniera sintetica i risultati del lavoro e indicati alcuni sviluppi futuri del lavoro che il regolatore dovrà portare avanti.

Capitolo 1

Il Cloud Computing

1.1 Il cambio di prospettiva portato dal Cloud

L'idea del Cloud Computing nasce e prende piede in Italia e nel mondo per rispondere a delle necessità che si palesavano all'interno di imprese e organizzazioni che sperimentavano un processo di crescita molto rapido, che doveva essere accompagnato da un'analoga crescita in termini di potenza di calcolo e immagazzinamento dati. All'inizio la soluzione più semplice e immediata per rispondere a queste necessità è stata l'acquisto di risorse fisiche con potenza maggiore e capaci di assorbire l'aumento di domanda derivante dalla crescita dell'impresa. Con il tempo, però, moltissime imprese si sono accorte che dotarsi di risorse fisiche on-premise (in sito) ha introdotto un altro problema ancora più complesso, ovvero il dimensionamento delle risorse fisiche atte a soddisfare l'aumento di domanda.

Stabilire quanta potenza di calcolo e/o capacità di immagazzinamento dati deve avere una determinata macchina o hardware non è un problema semplice e sempre risolvibile, in quanto lo stress a cui sono sottoposti i sistemi informatici di un'impresa dipende da moltissimi fattori, e non sempre è possibile stabilire un andamento certo e sicuro delle richieste che arrivano ai sistemi stessi. Ad esempio, nel caso in cui un'impresa compri una risorsa fisica sovradimensionandone in termini di CPU e RAM la capacità computazionale, anche se probabilmente essa sarà in grado di affrontare anche picchi improvvisi di richieste da parte dei suoi clienti, comunque costituirà uno spreco per l'impresa. Infatti, avere una risorsa fisica estremamente potente capace di fronteggiare picchi inaspettati di richieste rappresenta un dispendio enorme in termini economici per l'azienda, che ha immobilizzato una risorsa che, per la maggior parte del tempo, non viene sfruttata in maniera congrua alle sue potenzialità. Al contrario, se si sottodimensiona la capacità computazionale della macchina al momento dell'acquisto, si rischia di creare disagi ai propri clienti nei momenti in cui ci sono dei picchi improvvisi di richieste, nonostante il sistema per tutto il tempo venga sfruttato al massimo delle sue potenzialità.

Il dimensionamento delle risorse fisiche è il maggior problema, ma non l'unico, di un approccio basato sull'uso esclusivo di risorse on-premise per compiere la

transizione digitale. Ad esso si aggiungono altri oneri da considerare, come il costo di mantenimento e gestione delle risorse e del luogo in cui queste sono collocate, ovvero il data center. In più, l'impresa si deve addossare anche tutti i costi legati alla sicurezza delle risorse e delle strutture in cui esse risiedono, nonché tutti i costi legati di formazione e retribuzione del personale che si occupa di sorvegliare e mantenere la struttura. Purtroppo non tutte le imprese possiedono al loro interno le risorse, sia in termini di know-how aziendale, sia in termini di liquidità, per iniziare e completare la realizzazione di una struttura così complessa.

Tutti gli aspetti citati in precedenza hanno portato le aziende che avevano bisogno di servizi ICT più potenti e le aziende che sviluppavano servizi ICT a cambiare prospettiva. Il concetto fondamentale della nuova visione, che si è affermata nel mercato, consiste nel fatto che è più vantaggioso per l'azienda affittare una risorsa fisica, con una potenza dipendente dal carico di lavoro a cui sono sottoposti i propri sistemi informatici e informativi. L'esigenza delle imprese, quindi, è quella di avere una risorsa dimensionata dinamicamente in base alla richiesta verso i propri sistemi informatici, il cui canone dipende dall'utilizzo, secondo un modello pay-per-use. Questa esigenza di flessibilità, scalabilità e misurabilità del servizio, per stabilire un canone da corrispondere, ha incentivato lo sviluppo e la diffusione di un nuovo paradigma di offerta di servizi da parte di imprese ICT, chiamato Cloud Computing.

Spesso con il termine Cloud si tende ad identificare il prodotto fisico, ovvero il servizio Cloud, minimizzando la portata dell'innovazione introdotta. Infatti, quando si parla di Cloud si fa riferimento a una nuova prospettiva di elaborazione, basata su architetture distribuite e non più stand-alone, sull'uso di "commodity hardwares" e caratterizzata da un tipo di sviluppo software e infrastrutturale completamente diverso. Perciò, è fondamentale rimarcare che il termine Cloud Computing porta con sé la definizione di un nuovo modello di elaborazione che supera tutte le problematiche descritte in precedenza. La comprensione del modello di elaborazione Cloud è fondamentale per comprendere il ruolo che questa innovazione ha nell'accelerazione del processo di transizione digitale delle imprese e Pubbliche Amministrazioni.

Per capire cosa rappresenta il paradigma è importante analizzare la definizione che ne viene data dal National Institute of Standards and Technology (NIST) nello standard NIST 800-145:

> *Il Cloud computing è un modello di elaborazione che abilita un accesso in rete, su richiesta, ubiquo e conveniente, a un pool di risorse di calcolo (server, storage, reti, servizi e applicazioni) condivise e configurabili, che possono essere acquisite e rilasciate rapidamente e in modo dinamico, con uno sforzo di gestione minima e con interazione minima con il gestore del servizio. Il modello Cloud è composto di cinque caratteristiche essenziali, tre modelli di servizio, e quattro modelli di implementazione.*[10].

In maniera sintetica, lo standard riporta tutte le caratteristiche principali del nuovo modello di elaborazione introdotto, alcune delle quali sono fondamentali per l'accelerazione della transizione digitale. Partendo dalla definizione presentata è possibile condurre un'analisi approfondita delle principali peculiarità del nuovo modello di elaborazione.

1.2 Caratteristiche principali del Cloud e modelli di servizio

La prima particolarità da menzionare del paradigma Cloud è l'accesso mediante la rete alle risorse su Cloud, cioè la possibilità di accedere a tali servizi indipendentemente dalla loro locazione, a condizione di possedere un'adeguata banda di rete. Tale peculiarità, oltre che un enorme vantaggio, porta con sé anche delle problematiche di sicurezza, legate specialmente alla locazione delle risorse, in quanto non sempre i Cloud Provider permettono di geolocalizzare esattamente la risorsa fisica utilizzata da un client.

Proseguendo, una caratteristica molto importante del Cloud Computing è la possibilità di richiedere e ottenere servizi IT, in base alle richieste ricevute in un certo lasso tempo, senza bisogno di interagire direttamente con il fornitore. L'assenza di interazione, ovvero la possibilità di fare self-service provisioning delle risorse, permette a chi utilizzi un servizio di Cloud di ottenere velocemente tutto quello di cui ha bisogno per erogare i propri servizi, risparmiando tempo e abbattendo i costi. Oltre a questo, un'altra caratteristica fondamentale del modello di elaborazione Cloud è l'elasticità delle risorse che si ottengono da un fornitore di servizi Cloud, che consiste nell'aumentare o diminuire il numero di macchine deputate ad offrire un determinato servizio in base alla richiesta. Quindi, se in un certo periodo un servizio viene richiesto da un numero di utenti superiore alla norma, il fornitore di servizi Cloud garantisce al cliente, l'allocazione e la deallocazione dinamica di risorse per fronteggiare l'aumento o la diminuzione della richiesta. Tale aspetto è gestito interamente dal fornitore di servizi Cloud e rappresenta un grosso vantaggio per un'impresa o Amministrazione Pubblica. Inoltre, la possibilità di avere dei livelli di servizio facilmente misurabili, permette sia all'impresa di sapere a quale servizio sta accedendo, sia al fornitore di stabilire un prezzo di utilizzo dei propri servizi Cloud, secondo un modello pay-per-use.

Invece, il fatto che il Cloud permetta l'accesso a un pool di risorse è una caratteristica del modello di elaborazione che ha conseguenze sia positive che negative. Sicuramente, poter accedere a un vasto pool di risorse, attraverso la rete Internet, permette di offrire un ampio grado di resilienza a chi porta i propri servizi su Cloud, potendo contare su repliche degli stessi e backup dei dati. Però, le risorse a cui accede ogni cliente di un fornitore di servizi Cloud sono condivise con altri clienti e altre imprese che hanno deciso di migrare su Cloud. Questa peculiarità del modello

di elaborazione Cloud deriva dall'implementazione del modello multi-tenant, ovvero si ha un'unica versione del servizio offerto ad ogni cliente, che però viene diviso in più istanze, una per cliente, che possono coesistere all'interno della stessa risorsa fisica. Ad esempio, se un provider offre il software di posta elettronica come servizio sul Cloud, tale applicativo sarà in esecuzione sulla stessa macchina in cui sono eseguiti altri applicativi appartenenti ad altri clienti. Quindi, anche se il codice oggetto dell'applicativo è lo stesso, viene creata un'istanza diversa e teoricamente isolata dalle altre per ogni cliente all'interno della stessa risorsa fisica. Tale aspetto introduce un'importante problema di sicurezza, perché se l'isolamento tra le istanze di software, piattaforme e infrastrutture offerte dal Cloud Provider non è realizzato correttamente, si rischia di permettere a un cliente di accedere ai tenant degli altri. Quindi, il modello multi-tenant, che permette l'uso condiviso e rapido di risorse, crea una problematica di sicurezza, da considerare obbligatoriamente, nello stabilire in che modalità le Pubbliche Amministrazioni dovranno migrare su Cloud.

L'innovazione portata dal modello Cloud non si esaurisce solo con le sue cinque particolarità descritte prima, ma viene espressa anche attraverso la possibilità di offrire diversi modelli di servizio a diversi livelli di astrazione. Nel paradigma Cloud sono disponibili tre principali modelli di servizio che permettono l'acquisizione di risorse a vari livelli di astrazione:

- **Modello Infrastructure as a Service (IaaS)**: comprende l'erogazione di servizi di natura sistemica come macchine virtuali, server virtuali, spazi di salvataggio dati e così via, ovvero tutti ambienti che necessitano di un processo di configurazione iniziale e offrono maggiore libertà.

- **Modello Platform as a Service (PaaS)**: consiste nell'erogazione di servizi di piattaforma, come ambienti preconfigurati per lo sviluppo del software e applicazioni basate sulla tecnologia a *container*, offrendo minore libertà di un ambiente IaaS ma limitando gli aspetti di configurazione.

- **Modello Software as a Service (SaaS)**: riguarda l'erogazione di software ad utenti finali, come servizi di posta elettronica e altro.

Concettualmente ogni livello di servizio introduce un'ulteriore astrazione rispetto al precedente, eliminando degli oneri di gestione che passano dall'ente che migra su Cloud al fornitore di servizi che mette a disposizione l'infrastruttura Cloud. La differenza tra i tre modelli di servizio presentati e la gestione on-premise dei servizi può essere facilmente compresa attraverso la Figura 1.1.

Il modello IaaS rappresenta il livello di astrazione minima tra i tre modelli di servizio, e, comunque, rende trasparente all'utente che lo utilizzo lo strato fisico, detto bare-metal, perché, indipendentemente dal tipo di servizio utilizzato non si ha conoscenza della precisa risorsa fisica in cui è ospitato il servizio stesso. Per

Figura 1.1: Responsabilità di gestione nei modelli di servizio e nell'approccio on-premise

esempio, quando si utilizza una risorsa come una macchina virtuale su Cloud si ha controllo solo su aspetti di livello logico della macchina, come il sistema operativo, lo spazio richiesto su disco e gli applicativi software. Invece, non è noto, o comunque pienamente controllabile, quale macchina fisica, in quale data center stia emulando la macchina virtuale, e quali altri servizi siano presenti sulla macchina. Quindi, adottando un servizio IaaS è a carico di chi usa il servizio la gestione di tutti gli

aspetti logici partendo dal sistema operativo fino alle applicazioni.

Sopra lo IaaS, si trova il modello PaaS, cioè un livello di astrazione intermedio, che predispone un ambiente di piattaforma preconfigurato, tipicamente, per lo sviluppo software. Questo modello di servizio permette all'utente di ottenere un ambiente di sviluppo software preconfigurato, dotato di tutte le librerie necessarie per sviluppare del software sul Cloud in una determinata maniera. A questo livello il cliente che usufruisce del servizio PaaS non ha più l'onere di gestire il sistema operativo, i middleware e l'ambiente di esecuzione in cui verrà eseguito il software sviluppato. Rimane agli sviluppatori solo la gestione dell'applicazione e dei dati che essa dovrà manipolare o fornire.

Infine, il livello di astrazione massima è rappresentato dal modello di servizio SaaS, in cui il cliente coincide con l'utente finale che utilizza un'applicazione. In un servizio SaaS è compito del Cloud Provider fornire un'applicazione direttamente utilizzabile da un utente finale, più o meno formato in ambito IT. Infatti, i servizi SaaS più comuni sono tipicamente i servizi di Posta elettronica e da ufficio, utilizzati anche da utenti non esperti. Nel modello SaaS il cliente si pone come un utilizzatore finale, che non ha nessun onere di gestione e si preoccupa solo di utilizzare il software analogamente a una soluzione COTS(Commercial off-the-shelf).

La possibilità di scegliere tra i tre modelli di servizio descritti offre alle imprese la possibilità di decidere qual è la soluzione più adatta per spostare un proprio servizio su Cloud. Ad esempio, un'azienda con poco personale in campo ICT, nel dotarsi di una nuova soluzione CRM, potrebbe adottare un approccio SaaS e usufruire del software CRM del Cloud Service Provider. Invece, altre aziende con competenze più specializzate in campo IT o che già possiedono un loro CRM, potrebbero decidere di optare per una soluzione PaaS o IaaS sviluppando con più libertà di manovra il loro software CRM personalizzato su Cloud. Per questo, la presenza di più modelli di servizio ha permesso un'ampia diffusione del paradigma di elaborazione basato su Cloud.

1.3 Modelli di implementazione del Cloud

Come accennato nella sezione 1.2, le caratteristiche nel modello di elaborazione Cloud hanno moltissimi vantaggi sia per chi offre i servizi sia per chi ne beneficia, ma allo stesso tempo nascondono delle problematiche di sicurezza. Nel momento in cui un qualsiasi ente migra su Cloud potrebbe avere delle preoccupazioni legate a dove sono salvati i propri dati strategici e quelli dei propri clienti, e sul fatto che possano avvenire degli accessi incontrollati ai propri dati da parte del provider o di altri tenant. A tale scopo, sono definite da parte dei fornitori di servizi Cloud delle policy di sicurezza e degli obiettivi di policy che regolano come può avvenire l'accesso ai dati dei clienti da parte del provider e dove possono essere salvati o replicati i

dati stessi, nonché opportune policy di isolamento dei vari tenant che insistono sulla stessa infrastruttura.

La definizione di queste policy di sicurezza costituisce un primo strumento che permette al cliente di riporre una buona fiducia nel fornitore di servizi Cloud. Comunque molte imprese preferiscono tutelarsi, attraverso clausole e obblighi contrattuali, e stabilire come il provider debba trattare i dati e i servizi dell'azienda che ha migrato sul Cloud. In alcuni casi, specialmente se si parla di dati strategici e dati riguardanti segreti industriali o altre forme di proprietà intellettuali, vista l'architettura multi-tenant intrinseca del Cloud, molte aziende sono restie a portare quella parte della loro infrastruttura su un Cloud. Inoltre, mantenere parte dei propri servizi informatici e dati on-premise contribuisce a non disperdere le competenze e le conoscenze in materia informatica presenti all'interno dell'impresa.

Quindi, le aziende, per necessità, possono mantenere parte dei loro servizi on-premise senza affidarli a un Cloud Provider, avendo, però, l'onere di gestire tali servizi in maniera efficiente ed efficace. In realtà, grazie all'ampia flessibilità del paradigma Cloud, non viene esclusa per un'organizzazione la possibilità di gestire i propri servizi on-premise secondo il modello Cloud, utilizzando un proprio data center, oppure noleggiando il data center di un soggetto terzo. Tale possibilità deriva dal fatto che il modello di deployement del Cloud Computing non è rigido, ma flessibile, concedendo delle libertà non indifferenti a chi sceglie di migrare su Cloud.

Attualmente esistono quattro modelli di implementazione del paradigma Cloud, ognuno con le proprie caratteristiche da tenere in considerazione nel momento in cui un'organizzazione affronta il processo di migrazione. I quattro modelli di implementazione del Cloud sono:

- **Cloud Pubblico**: è il contesto in cui un fornitore di servizi Cloud mette a disposizione la sua infrastruttura, di cui ha il pieno controllo, a degli utenti, aziende ed enti pubblici. Le imprese, dietro il pagamento di un canone, possono accedere all'infrastruttura e alle risorse del Cloud Service Provider, che sono distribuite in tutto il mondo e condivise tra più utenti secondo il modello multi-tenant. Ad esempio, Amazon Web Services, Microsoft Azure e Google Cloud sono degli esempi di Cloud Pubblico, oltre che leader di mercato nel settore.

- **Cloud Privato**: a differenza della soluzione precedente, in questo modello l'ambiente Cloud viene riservato a un singolo utente, impresa o ente pubblico, in maniera esclusiva. Chi usufruisce di un ambiente Cloud Privato può scegliere se gestire l'infrastruttura sottostante all'ambiente Cloud in maniera on-premise, avendo gli oneri di gestione, manutenzione e sicurezza del data center, dei dati e dei servizi. Altrimenti, può usare l'infrastruttura di un soggetto terzo, il quale mette a disposizione del cliente delle risorse dedicate all'interno del proprio

data center, affidando al cliente solo la gestione dell'ambiente Cloud. In questa maniera, da un lato si mantiene controllo sui propri dati e sull'ambiente Cloud, mentre dall'altro si rischia che l'infrastruttura potrebbe non essere in grado di assorbire correttamente picchi improvvisi della domanda.

- **Community Cloud**: non tutte le aziende hanno le risorse finanziarie e umane per permettersi di mantenere un'infrastruttura fisica a supporto di un Cloud Privato. Per questo motivo, si adotta questo modello di implementazione detto Community Cloud, in cui un ristretto gruppo di aziende o organizzazioni, con intenti comuni o nello stesso settore, unisce le proprie risorse finanziarie e umane per costruire un'infrastruttura a supporto di un servizio Cloud. Tale servizio Cloud è di carattere privato, perché ristretto solo ai dipendenti e al personale della comunità di aziende che ha contribuito alla realizzazione del servizio Cloud condiviso. Gli oneri di gestione di questa infrastruttura, messa in piedi dalla comunità di aziende, di solito sono sostenuti o dalle aziende stesse, o da un ente terzo da cui le aziende noleggiano le risorse fisiche per costruirvi poi il loro servizio Cloud condiviso.

- **Cloud Ibrido**: è la combinazione delle due soluzioni precedenti, ovvero l'organizzazione si affida a un Cloud Service Provider che mette a disposizione sia un ambiente Cloud Pubblico interamente gestito, sia delle risorse fisiche on-premise nei propri data center per l'implementazione di un ambiente Cloud Privato, gestito dal cliente. In questo caso si riescono a ottenere sia i vantaggi di alta scalabilità tipici di un Cloud Pubblico, sia i vantaggi di privatezza e controllo del Cloud Privato. Infatti, nel caso in cui le risorse dedicate nel Cloud Privato non siano sufficienti ad assorbire picchi improvvisi di richieste, è possibile attingere alle risorse dell'ambiente pubblico per soddisfare le richieste in eccesso, dato che i due ambienti sono comunicanti.

A questi quattro modelli si aggiungono altri due modelli di implementazione di un servizio Cloud, concepiti in un tempo successivo rispetto agli altri, ma ormai diventati una pratica quasi comune all'interno dei Cloud Service Provider e delle aziende.

Il primo modello aggiuntivo è chiamato Virtual Private Cloud o VPC, nato all'interno dell'ambiente Cloud pubblico e offerto come soluzione da tutti i principali Cloud Provider come AWS, Microsoft Azure e Google Cloud. Il Virtual Private Cloud consiste in un insieme di risorse informatiche configurabili a richiesta in un ambiente Cloud pubblico che fornisce un certo livello di isolamento tra varie organizzazioni che utilizzano queste risorse[11]. In sostanza nel Virtual Private Cloud si crea all'interno di un ambiente pubblico, in cui le risorse fisiche sono condivise, un meccanismo di isolamento al livello logico che permette di accedere determinate risorse solo a una determinata organizzazione. Quindi, esso è molto simile a un Cloud Privato, perché

ne replica la caratteristica single-tenant, però lo fa all'interno però di un ambiente pubblico e multi-tenant. Tipicamente i meccanismi di isolamento utilizzati nei VPC consistono nell'uso di sottoreti IP e meccanismi di comunicazione virtuale, oltre che nell'uso di servizi VPN per l'accesso da remoto.

L'altro modello aggiuntivo, ai quattro descritti in precedenza, è il modello Multi-Cloud, ovvero una soluzione molto simile al Cloud Ibrido, che prevede la possibilità che i due ambienti Cloud, quello Pubblico e quello Privato, siano concessi da fornitori diversi. Mentre nel Cloud Ibrido i due ambienti sono comunicanti, nel Multi-Cloud l'ambiente pubblico e quello privato sono totalmente sconnessi, mantenendo, però, la possibilità di integrare le risorse computazionali a disposizione al livello applicativo.

Ogni modello di deployement del Cloud ha dei vantaggi e degli svantaggi, sia in termini di scalabilità, flessibilità e oneri di gestione, sia in termini di sicurezza e privatezza dei dati e servizi mantenuti all'interno del Cloud. Migrare su un Cloud Pubblico sicuramente è la soluzione migliore per un'impresa in termini di costi, facilità di implementazione, flessibilità e scalabilità del servizio Cloud. Infatti, lo sforzo di gestione è totalmente assente, in quanto chi migra si deve occupare solo di richiedere le risorse virtuali, piattaforme e software ad esso necessari per continuare svolgere il proprio Core Business. Allo stesso tempo, esistono varie problematiche di sicurezza legate alla privatezza dei dati su Cloud e all'architettura multi-tenant del Cloud Pubblico, che rendono tale modello implementativo inadatto per l'immagazzinamento di dati sensibili e strategici di un'organizzazione.

Allo stesso modo il Cloud Privato, anche se garantisce controllo sui dati, sull'infrastruttura sottostante al servizio Cloud e sull'ambiente Cloud, non è una strada sempre percorribile per tutte le aziende. Solo poche grandi organizzazioni sono state in grado nel tempo di costruire un'infrastruttura di Cloud Privato a supporto delle attività dei propri dipendenti, mentre la maggior parte delle aziende di piccola o media grandezza non possiede le risorse sufficienti per costruire e gestire un'infrastruttura così complessa. Anche la scelta di un Community Cloud non è esente da problematiche, in quanto le aziende che si alleano per formare questo Cloud Privato condiviso potrebbero non condividere un'unità d'intenti per un lungo periodo o non riuscire a coordinarsi nella gestione dell'infrastruttura condivisa e dell'ambiente Cloud.

Attualmente le soluzioni migliori che rispondono sia all'esigenza di riservatezza e controllo sui dati sensibili e strategici che hanno alcune organizzazioni, sia alle esigenze di elasticità, scalabilità, flessibilità e facilità di implementazione dell'ambiente Cloud, sono il Cloud Ibrido e il Multi-Cloud. Il Cloud Ibrido infatti, risponde all'esigenza di avere maggior controllo sui dati e sull'ambiente Cloud offerto all'organizzazione, in quanto viene concessa alla stessa l'opportunità di servirsi di risorse fisiche dedicate per implementare il proprio Cloud Privato. Allo stesso tempo con l'Hybrid Cloud sono soddisfatte anche i requisiti di elasticità, flessibilità, scalabilità e self-service

provisioning tipici del Cloud Pubblico. Inoltre, rispetto al Cloud Ibrido, il Multi-Cloud introduce anche la possibilità di affidarsi a più fornitori di servizi Cloud, permettendo all'organizzazione di evitare anche situazioni di *vendor lock-in*, in quanto l'ambiente Cloud Privato e l'ambiente Cloud Pubblico sono erogati da fornitori diversi.

1.4 Utilizzo del Cloud Computing in Italia ed Europa

Attualmente, nel processo di transizione al digitale che stanno attraversando molte imprese italiane ed europee il Cloud Computing sta svolgendo un ruolo chiave, fornendo alle imprese la possibilità di implementare in maniera più veloce e agile i nuovi processi aziendali, ridisegnati per includere le tecnologie digitali. Il vantaggio dell'utilizzo del Cloud Computing, nel processo di trasformazione digitale di un'organizzazione, è quello di dotarsi di strumenti tecnologici flessibili, scalabili e misurabili, secondo un modello pay-per-use, in breve tempo e senza bisogno di interagire direttamente con il fornitore. Molte imprese, non avendo la disponibilità economica necessaria per assumere personale specializzato in campo IT e per costruire un'infrastruttura on-premise, decidono di acquistare servizi da un Cloud Provider, in maniera da ottenere la tecnologia necessaria nel più breve tempo possibile.

Le imprese private hanno iniziato prima della pandemia da COVID-19 il processo di trasformazione digitale, investendo importanti risorse nelle nuove tecnologie emergenti, ridisegnando i loro processi interni per includervi le tecnologie digitali e assumendo personale specializzato in grado di implementare e mantenere nuovi apparati e sistemi. Un esempio vincente di questa trasformazione è l'industria automobilistica, che ha introdotto l'uso dell'automazione per la costruzione dei prodotti, e l'uso degli smart sensor e del machine learning per la manutenzione predittiva e intelligente, riuscendo a sviluppare prodotti sempre più avanzati per venire incontro alle esigenze dei clienti. In questa trasformazione ha avuto un ruolo fondamentale anche il Cloud Computing, che ha permesso alle aziende di memorizzare la grande quantità di dati, proveniente dai sensori installati a bordo dei macchinari nella catena di produzione, e di realizzare su queste dati delle analisi più o meno raffinate, utilizzando soluzioni SaaS di analytics.

Oltre all'esempio dell'industria automobilistica, esistono moltissimi altri esempi e casi di aziende che hanno incluso il Cloud nel loro processo di transizione al digitale. Infatti, l'utilizzo delle tecnologie Cloud all'interno delle imprese italiane ed europee è significativamente cresciuto nel biennio 2020-2021, anche a causa dello scoppio della recente pandemia, che ha spinto le organizzazioni a potenziare i loro servizi IT. L'ultimo report di Eurostat sull'utilizzo del Cloud Computing da parte delle imprese ha evidenziato che la percentuale di aziende che utilizzano il Cloud in tutta Europa è cresciuto del 5% dal 2020 al 2021, mentre nello stesso periodo in Italia l'utilizzo del Cloud da parte delle organizzazioni è rimasto sostanzialmente invariato,

ma comunque diffuso[12]. Una panoramica dell'utilizzo del Cloud in tutti i paesi europei è riportata in Figura 1.2, testimoniando che più della metà delle imprese italiane si sta avvalendo delle tecnologie Cloud.

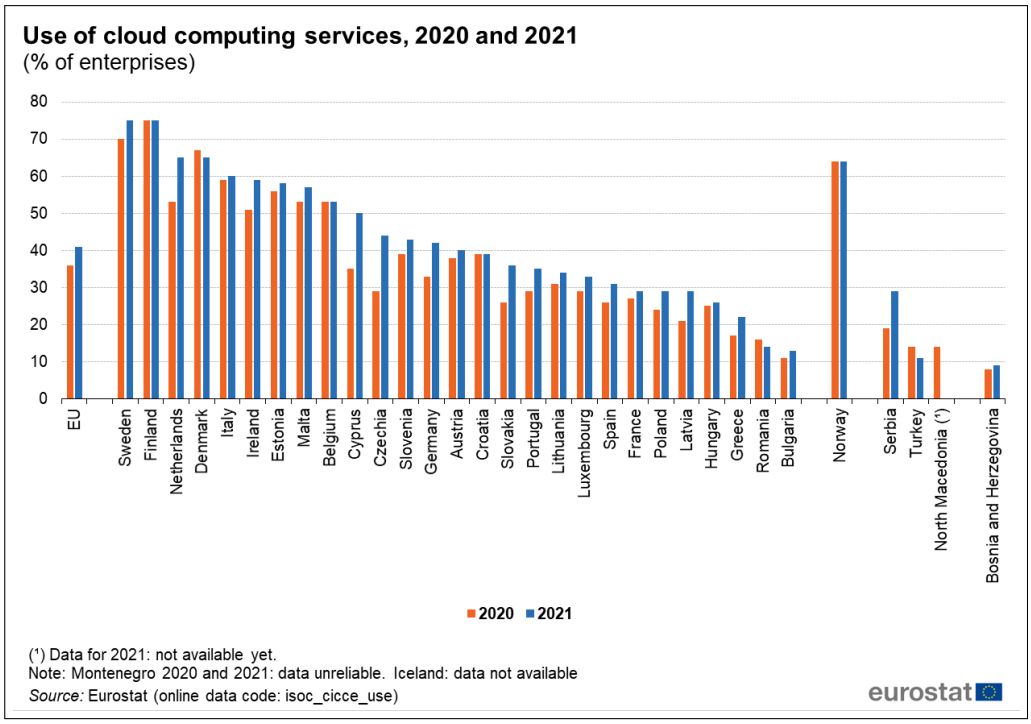

Figura 1.2: Utilizzo del Cloud Computing in Europa nel 2020 e nel 2021[1]

Sempre considerando i dati Eurostat, emerge un altro fattore interessante nell'utilizzo del Cloud fatto dalle imprese in Italia e in Europa. Tra le organizzazioni che utilizzano il Cloud Computing in Europa, la maggior parte di queste, il 79%, ha scelto di avvalersi di una soluzione Cloud per il loro sistemi di posta elettronica, invece di crearne uno proprio interno[12], come riportato nella Figura 1.3. Inoltre, più del 60% delle imprese al livello europeo utilizzano il Cloud per lo storage dei file e per l'Office Software(eg. Microsoft Word, Excel, Google Documenti, Google Fogli etc...), e quasi la metà, il 47%, ospita il proprio database aziendale all'interno di un servizio Cloud. In Italia, a differenza della media europea, si riscontra che quasi tutte le imprese, il 96%, hanno scelto di utilizzare un soluzione SaaS per la gestione della posta elettronica, mentre solo il 39% delle imprese ha migrato il proprio database presso un fornitore di servizi Cloud. Altro aspetto da evidenziare è che, sia in Italia che in Europa, poche aziende utilizzano soluzioni Cloud per lo sviluppo delle proprie applicazioni, e poche aziende utilizzano soluzioni ERP e CRM in Cloud.

Perciò, anche se l'utilizzo del Cloud è già molto diffuso, ancora né in Italia, né in tutti gli altri paesi dell'UE si è raggiunta una piena maturità nell'utilizzo del Cloud e di tutti i suoi vantaggi, ma si utilizzano soluzioni Cloud per riuscire ad abbattere i costi e ottenere delle soluzioni software per l'azienda in maniera rapida e veloce. A

Use of cloud computing services in enterprises, 2021

	Use of cloud computing	E-mail	Storage of files	Office software	Security software applications	Financial or accounting software applications	Hosting the enterprise's database(s)	CRM software applications	Computing power for enterprise's own software	ERP software applications	Platform for application development, testing or deployment
	% enterprises	% enterprises using the cloud									
EU	41	79	66	61	58	47	46	27	24	24	21
Belgium	53	82	81	68	65	50	58	46	40	36	27
Bulgaria	13	80	68	60	44	32	55	21	21	24	21
Czechia	44	81	62	85	78	52	32	17	11	19	7
Denmark	65	86	83	73	80	65	72	38	43	35	40
Germany	42	65	61	55	48	40	33	21	25	18	23
Estonia	58	77	65	68	44	75	26	19	32	19	17
Ireland	59	80	69	73	54	54	40	24	12	13	16
Greece	22	84	67	73	50	34	41	28	36	28	36
Spain	31	82	80	63	62	40	69	38	35	33	28
France	29	67	76	54	51	44	59	30	22	31	25
Croatia	39	88	72	61	65	52	54	20	23	18	22
Italy	60	96	58	58	70	52	39	19	14	20	10
Cyprus	50	83	60	68	71	43	23	20	12	17	8
Latvia	29	79	54	57	41	36	49	17	22	15	17
Lithuania	34	80	58	51	52	46	42	17	33	13	22
Luxembourg	33	81	67	68	61	41	65	33	27	23	29
Hungary	26	72	61	61	45	41	44	21	32	18	17
Malta	57	89	83	80	55	51	55	33	41	22	26
Netherlands	65	82	81	72	64	66	78	49	28	35	30
Austria	40	70	71	52	49	27	26	23	24	16	28
Poland	29	79	41	64	41	30	27	17	10	22	14
Portugal	35	89	71	61	66	41	46	26	35	34	25
Romania	14	80	58	58	52	44	50	27	22	30	22
Slovenia	43	73	66	66	72	38	43	21	28	25	23
Slovakia	36	88	60	65	68	52	39	28	25	16	18
Finland	75	85	76	75	65	64	49	41	20	37	17
Sweden	75	87	84	71	64	73	60	38	43	21	27
Norway	64	88	83	78	67	69	67	38	39	33	32
Serbia	29	77	52	46	34	42	37	14	17	19	14
Turkey	11	72	71	57	46	57	37	27	35	56	29
Bosnia and Herzegovina	9	84	65	62	58	49	55	27	33	28	31

Note: Iceland: 2021 data not available. North Macedonia: 2021 data not available. Montenegro: 2021 data unreliable.

Source: Eurostat (online data code: isoc_cicce_use)

eurostat

Figura 1.3: Utilizzo del Cloud Computing per tipo di serivizio richiesto in Europa nel 2021[2]

testimonianza di questo, l'Osservatorio Cloud Nazionale ha rilevato che quasi due organizzazioni su tre (63%) dichiarano di misurare l'apporto del Cloud al business dell'azienda in base al risparmio sui costi rispetto a una configurazione on-premise. Questo dato è espressione di una cultura organizzativa diffusa: invece di guardare al Cloud come una leva di efficacia nell'accelerare la digitalizzazione e l'innovazione, lo si adotta come mezzo di puro efficientamento, alimentando una narrazione che inibisce la vera trasformazione[13].

In realtà il Cloud può essere uno strumento molto importante per l'accelerazione della transizione digitale non solo per le aziende private, ma anche per le Pubbliche Amministrazioni. Infatti, il Cloud evita all'organizzazione che vuole operare la transizione verso il digitale di gestire tutta una serie di problematiche legate al mantenimento delle infrastrutture fisiche a supporto del Cloud. Inoltre, la possibilità di poter acquistare soluzioni SaaS, PaaS, o IaaS da un fornitore di servizi Cloud accorcia i tempi di inclusione dei servizi IT all'interno dei processi definiti nelle imprese e nelle Pubbliche Amministrazioni. Questo accade perchè un'organizzazione ha sempre la possibilità di operare il self-service provisioning delle risorse ad essa necessarie. Quindi, il Cloud Computing è uno dei pilastri del processo di trasformazione digitale del Paese, finanziato anche dai fondi del Piano Nazionale di Ripresa e Resilienza (PNRR). Le Amministrazioni allo stato attuale non possiedono risorse sufficienti in termini di infrastrutture, data centers e risorse umane per poter sviluppare in

maniera veloce la trasformazione digitale richiesta dall'Unione Europea. Quindi, il Cloud Computing rappresenta uno strumento necessario per permettere alle PA italiane di completare questo processo di transizione digitale, in maniera tale da poter fornire ai cittadini servizi più efficienti, efficaci e resilienti.

La migrazione su Cloud, alla luce delle caratteristiche che ha questo modello di elaborazione, introduce delle problematiche di sicurezza significative per le Pubbliche Amministrazioni Italiane, perché erogano servizi critici e strategici per lo sviluppo economico del Paese e utilizzano dati sensibili e personali appartenenti ai cittadini. Da qui l'esigenza di regolamentare il processo di migrazione su Cloud delle Pubbliche Amministrazioni, in maniera tale che le Amministrazioni Italiane spostino i loro servizi solo presso dei fornitori di servizi Cloud considerati affidabili e supportati da un'infrastruttura resiliente. A tale scopo, sono state emanate delle leggi in materia di sicurezza nazionale al livello IT, e prima l'AgID e poi l'Agenzia per la Cybersicurezza Nazionale (ACN), si sono occupate di creare regolamenti e definire un percorso di qualificazione, per i Cloud Service Provider interessati a ospitare i servizi e dati delle PA italiane.

Capitolo 2

La qualificazione dei Servizi Cloud

2.1 Le Minacce all'Italia e la definizione del PNSC

2.1.1 I Rapporti del Clusit: la situazione Italiana

Il processo di transizione digitale che sta attraversando l'Italia richiede, oltre alla definizione di una strategia con cui guidare questo processo, anche la definizione di aspetti di sicurezza e resilienza che dovranno avere le infrastrutture IT essenziali per il sistema Paese. Infatti, la transizione digitale della Pubblica Amministrazione, oltre a portare con sé dei vantaggi non trascurabili, come un aumento dell'efficienza e dell'efficacia dei servizi offerti ai cittadini e un abbattimento dei costi per le Amministrazioni stesse, può nascondere delle insidie, legate specialmente al contesto della cybersecurity e degli attacchi informatici. Introdurre tecnologie digitali all'interno di un'organizzazione significa anche assicurarsi che le tecnologie introdotte non siano vulnerabili e facilmente attaccabili dai cybercriminali.

La compromissione di un servizio informatico o il furto di dati rappresenta una grande perdita in termini economici per un'organizzazione, sia per il danno di immagine che ne deriva, sia per la diffusione dei dati stessi sul dark web, sia per la perdita dei dati, che potrebbero essere criptati dall'attaccante. Spesso un attacco informatico o un data breach causa un'interruzione del servizio colpito, risultando in problemi per l'azienda e per i suoi clienti. Per una Pubblica Amministrazione o azienda privata, che eroga un servizio di importanza strategica per il Paese, l'impatto è molto più severo e può causare, oltre che seri danni fisici ed economici ai cittadini, anche un blocco dello sviluppo economico dello Stato. Quindi, nel processo di trasformazione digitale che attraverseranno gli enti pubblici e le aziende che erogano servizi critici e strategici per l'Italia, è necessario stabilire dei requisiti di sicurezza più stringenti per le infrastrutture e i servizi IT che saranno realizzati per queste organizzazioni.

La definizione di requisiti di sicurezza più stringenti è necessaria, non solo per il grande impatto che può avere un attacco informatico a un ente pubblico in termini economici e strategici, ma anche per l'incremento delle minacce a cui si è assistito negli ultimi anni. Periodicamente l'Associazione Italiana per la Sicurezza Informatica,

il CLUSIT, pubblica dei rapporti sulla sicurezza delle infrastrutture e beni ICT in Italia, includendo in essi un'analisi degli attacchi avvenuti in un determinato periodo di tempo. I rapporti del CLUSIT sono emessi ogni sei mesi e presentano l'andamento degli attacchi relativi ai cinque anni antecedenti al momento dell'analisi, sia per offrire una panoramica sui trend degli attacchi e altri loro aspetti, sia per confrontare l'andamento dell'ultimo semestre con quello dei precedenti 5 anni.

Accedendo ai rapporti CLUSIT sulla sicurezza ICT in Italia, si può constatare che dal 2018 ad oggi c'è stato un incremento degli attacchi informatici verso organizzazioni italiane, sia per le vulnerabilità di alcuni servizi delle organizzazioni, sia per l'aumento delle minacce causato dall'instabilità del contesto geopolitico negli ultimi due anni. Il rapporto osserva che dal 2018 a giugno 2023, sono stati censiti 505 attacchi noti di particolare gravità che hanno coinvolto realtà italiane, di cui ben 132 (il 26%!) si sono verificati solo nei primi 6 mesi del 2023. Pertanto il dato complessivo 2023 potrebbe non solo confermare la linea di tendenza degli ultimi anni, ma anche superarla nettamente, in continuità con quanto avvenuto nel 2022[14]. Lo scenario, perciò, evidenzia un aumento del numero di attacchi informatici diretti a imprese ed enti italiani, il quale nel futuro non è destinato ad arrestarsi, ma a crescere sempre di più.

Quindi, il processo di trasformazione digitale portato avanti dalle imprese e dalle istituzioni italiane potrebbe avere come effetto collaterale l'aumento della superficie di attacco esposta. Questo potrebbe portare a conseguenze molto negative per il Paese anche alla luce dell'attenzione che il nostro Paese sta ricevendo da parte degli attaccanti di tutto il mondo. Infatti, mentre nel 2018 su tutti gli attacchi informatici condotti a livello globale solo il 2.2% era diretto all'Italia, recentemente si è osservato che la percentuale di attacchi al livello globale diretti all'Italia ammonta al 7.6% nel 2022 e al 9.6% nel primo trimestre del 2023[14]. Oltre al numero di attacchi, è importante analizzare anche le motivazioni e le finalità con cui essi sono condotti al fine di contestualizzare la tendenza di crescita menzionata. Nel primo trimestre del 2023 la maggioranza degli attacchi noti in Italia si riferisce alla categoria "Cybercrime", che rappresenta il 69% del totale, con una quota in significativo calo rispetto all'anno precedente. Crescono invece in modo decisamente rilevante gli attacchi classificati come "Hacktivism", che nel semestre del 2023 si attestano al 30%[14]. Quindi, la crescita di attacchi informatici legati a gruppi di attivisti parastatali è figlia del contesto geopolitico e delle tensioni tra le superpotenze, oltre che del conflitto Russo-Ucraino iniziato nel 2022.

L'analisi del contesto generale suggerisce che anche le Pubbliche Amministrazioni siano state prese di mira dai cybercriminali, specialmente viste le tensioni geopolitiche esistenti tra la NATO e il blocco orientale. Infatti, la crescita generale del numero di attacchi verso le organizzazioni e le realtà italiane non ha risparmiato nemmeno gli enti pubblici che, indipendentemente dalla loro dimensione, sono stati colpiti da pesanti campagne di attacco condotte da cybercriminali e hacktivisti. Il report

del CLUSIT afferma che guardando alla distribuzione delle vittime, ancora una volta il settore per cui si rileva un maggior numero di attacchi è "Government" (23% del totale), seguita a breve distanza da "Manufacturing" (17%)[14]. Questo dato evidenzia come le Pubbliche Amministrazioni siano particolarmente esposte rispetto agli attacchi informatici e alle campagne di attacco, condotte nell'ultimo periodo. Oltre a constatare che il numero di attacchi verso istituzioni pubbliche italiane è aumentato e rappresenta il valore maggiore rispetto a tutti gli altri settori, bisogna sottolineare come la maggior parte di questi attacchi abbia delle conseguenze importanti e critiche. Gli attacchi condotti verso il settore pubblico sono ancora caratterizzati, come l'anno scorso, da una Severity assai maggiore rispetto all'insieme di tutti gli attacchi: ben il 52% è infatti classificato come critico, contro il 40% del dato globale, e il 40% è classificato alto contro il 38% del dato globale.

I dati presentati evidenziano una situazione preoccupante, che potrebbe peggiorare nel momento in cui le Amministrazioni conducessero il loro processo di trasformazione digitale senza tenere conto degli aspetti di sicurezza. Il fatto che gli attacchi all'Italia siano aumentati non deriva solamente dal mutato contesto geopolitico, ma è una conseguenza del fatto che le infrastrutture IT degli enti pubblici del Paese non sono in grado di contrastare la mole di attacchi condotti negli ultimi anni. La debolezza delle infrastrutture IT pubbliche e appartenenti ad aziende private che erogano servizi critici e strategici per il Paese, spinge gli hacker e i cybercriminali a guardare con maggiore interesse verso il nostro Paese. Infatti, gli attacchi condotti contro le organizzazioni italiane hanno una maggiore probabilità di successo e una possibilità concreta di causare danni seri alle istituzioni e ai cittadini, risultando anche in un grande guadagno per gli attaccanti. Tale scenario ha provocato un aumento delle minacce esistenti per le organizzazioni ed enti pubblici italiani che è destinato a causare numerosi problemi ai cittadini e alle organizzazioni stesse.

La compromissione delle infrastrutture digitali e dei servizi erogati dalle Pubbliche Amministrazioni, nonché delle infrastrutture e dei servizi erogati da aziende private che si occupano di fornire beni e servizi essenziali per i cittadini, potrebbe causare seri danni al Paese. Ad esempio, un attacco mirato ai servizi di monitoraggio di un'azienda, anche privata, che si occupa di provvedere alla fornitura di energia elettrica per una serie di province o una regione intera, potrebbe avere impatti anche sulla safety delle persone, portando nei casi più estremi anche a dei decessi, a causa della mancanza di energia elettrica negli ospedali. Quindi, al fine di evitare danni importanti anche per la salute dei cittadini, si è reso necessario definire dei requisiti di sicurezza più stringenti, non solo per gli enti pubblici, ma anche per tutte quelle organizzazioni che si occupano di fornire servizi critici e strategici per il Paese. Ovviamente, la definizione dei requisiti tecnici di sicurezza, che dovranno soddisfare le organizzazioni statali e parastatali, deve essere affiancata anche da un quadro normativo chiaro. Il vigente quadro normativo in materia di cybersicurezza

nazionale è stato definito con l'intento di individuare tutte le organizzazioni obbligate ad adottare standard di sicurezza più elevati e stabilire un insieme di requisiti di sicurezza idonei a garantire un adeguato livello di resilienza.

2.1.2 Il Perimetro Nazionale di Sicurezza Cibernetica

Le problematiche discusse nel paragrafo 2.1.1 hanno portato le autorità legislative, con il Decreto Legge 21 settembre 2019 n. 105, a istituire il Perimetro Nazionale di Sicurezza Cibernetica (PNSC). Esso è uno strumento per raggruppare tutti gli enti pubblici e le aziende private che erogano servizi di importanza critica o strategica per il Paese. Come recita l'articolo 1, comma 1 del decreto:

> *Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, e' istituito il perimetro di sicurezza nazionale cibernetica.*[15]

Il Perimetro Nazionale di Sicurezza Cibernetica, quindi, è un mezzo legislativo che permette di prescrivere, a tutti gli enti che ne fanno parte, il soddisfacimento di requisiti di sicurezza stringenti e definire delle sanzioni amministrative e pecuniarie nel caso in cui le prescrizioni non siano rispettate.

La legge che istituisce il PNSC si occupa anche di definire altri aspetti del perimetro, incluse le caratteristiche degli enti che ne fanno parte, come essi devono agire in determinate situazioni e quali sono le sanzioni per i mancati adempimenti. Innanzitutto, sono inclusi nel PNSC tutti i soggetti o enti che esercitano una funzione essenziale dello Stato, ovvero assicurano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, utilizzando reti, sistemi informativi e servizi informatici[15]. L'individuazione di tutti gli enti che fanno parte del perimetro avviene secondo dei criteri dettagliati all'interno del DPCM 30 luglio 2020 n.131. Per ragioni di sicurezza, l'elenco di tutti i soggetti inclusi nel PNSC non viene pubblicato, ma viene mantenuto riservato, e i soggetti vengono informati, attraverso le modalità appropriate, di essere stati inseriti nel perimetro.

Oltre a definire quali sono i requisiti sull'inclusione nel perimetro, la norma aggiunge una serie di prescrizioni che gli enti inseriti devono soddisfare. Infatti, il decreto legge citato impone a tutti gli enti che fanno parte del PNSC le seguenti azioni:

- la predisposizione, secondo dei criteri definiti dall'ACN, di elenchi di tutti gli asset ICT che possiedono e il trasferimento di tali elenchi all'ACN.

- il rispetto di requisiti di sicurezza definiti dall'Agenzia per la Cybersicurezza Nazionale.

- la notifica di tutti gli incidenti che hanno avuto impatto su asset ICT al CSIRT Italia, che le inoltrerà all'ACN.

Le misure di sicurezza che i soggetti nel perimetro devono implementare, sono definite dal secondo decreto attuattivo del perimetro, ossia il DPCM 81/2021[15]. Lo stesso decreto definisce le procedure secondo cui deve avvenire la notifica degli incidenti di sicurezza al CSIRT Italia, e condurre le ispezioni volte ad accertare che siano soddisfatti tutti i requisiti di sicurezza da parte degli enti nel perimetro.

La legge si occupa anche di definire le modalità con cui devono avvenire le forniture di beni ICT alle Pubbliche Amministrazioni e soggetti privati inclusi nel perimetro nazionale di sicurezza cibernetica. Innanzitutto, i soggetti inclusi nel perimetro che intendano acquisire particolari categorie di beni ICT (definite nel DPCM 15 giugno 2021) da impiegare per l'erogazione di servizi e funzioni essenziali devono comunicarlo al Centro di Valutazione e Certificazione Nazionale (CVCN), allegando anche un documento di analisi del rischio effettuata sull'oggetto della fornitura. Successivamente il CVCN si occupa di valutare la richiesta entro 45 giorni, e se necessario decide di condurre dei test di hardware e software oggetto della fornitura, in collaborazione con l'ente nel perimetro che deve ricevere la fornitura. Se il CVCN dopo 45 giorni non si pronuncia, si procede con la fornitura, altrimenti se sono richieste verifiche aggiuntive si aggiornano i contratti di fornitura, aggiungendo delle clausole di risoluzione legate al superamento delle verifiche e test. Il processo di valutazione del CVCN è definito nel DPR 54/2021. Allo scopo di portare avanti le citate attività di test, il CVCN ha adottato specifiche metodologie di test e può accreditare dei laboratori adatti a portare avanti tali attività. Questi ultimi devono essere accreditati dal CVCN secondo una procedura ben definita all'interno del DPCM 18 maggio 2022 n. 92.

L'impianto legislativo creato risulta essere molto severo e stringente e adatto a contrastare la situazione critica descritta dai rapporti del CLUSIT. Con questo quadro giuridico è stato creato un ecosistema di enti pubblici e soggetti privati che deve obbligatoriamente soddisfare requisiti di sicurezza molto severi, in maniera da garantire un servizio migliore ai cittadini e tutelare la sicurezza nazionale e l'economia del Paese. Il Perimetro Nazionale di Sicurezza Cibernetica definisce delle regole generali che i servizi ICT di tutti gli enti inclusi al suo interno devono rispettare, prescindendo però dal fatto che questi siano servizi ospitati all'interno di risorse on-premise oppure servizi Cloud erogati da un Cloud Service Provider. Come già

descritto nei precedenti paragrafi, il paradigma Cloud introduce un modo di operare differente, e per questo è stato necessario definire delle misure aggiuntive a quelle del PNSC e appropriate per il mondo Cloud.

2.2 La strategia Cloud Italia

2.2.1 Le sfide poste dal Cloud e la Strategia

Il problema più rilevante nell'affrontare la migrazione delle Pubbliche Amministrazioni italiane su Cloud consiste nella debolezza contrattuale verso i fornitori di servizi Cloud. Al livello Europeo esistono dei fornitori di servizi Cloud, ma detengono una quota di mercato irrisoria rispetto ad altre grandi aziende specializzate nel settore. Infatti, la maggior parte delle quote di mercato delle infrastrutture e dei servizi Cloud è detenuta da poche grandi aziende non europee. Come riportato da Gartner, i cinque maggiori Cloud Service Provider in termini di quote di mercato sono Amazon (40%), Microsoft(21.5%), Alibaba Group(7.7%), Google Cloud (7.5%) e Huawei (4.4%), mentre il resto dei fornitori di servizi Cloud, compresi quelli in UE, detengono tutti insieme il 18.9% delle quote di mercato[16]. L'evidente predominio, nel mercato dei servizi e delle infrastrutture Cloud, da parte di aziende non Europee ha posto una serie di sfide e problematiche da trattare e analizzare.

Innanzitutto esiste un problema di **autonomia tecnologica**, in quanto le Pubbliche Amministrazioni, che vogliono portare i loro dati e servizi presso un fornitore di servizi Cloud, sono in una posizione di subordinazione al livello tecnologico (il cosiddetto fenomeno del *lock-in*). Infatti, il Cloud Service Provider potrebbe operare delle modifiche unilaterali dei contratti stabiliti con gli enti pubblici italiani, le quali potrebbero avere conseguenze importanti, come un aumento di costo del servizio o la momentanea interruzione di alcune tipologie di servizio. Conseguenze di questi avvenimenti sono dei disagi importanti non solo per le Amministrazioni stesse, ma anche per i cittadini che usufruiscono dei loro servizi, causando alla lunga danni economici al Paese. Inoltre, poiché i CSP sono tutti non europei, le modifiche unilaterali del contratto potrebbero avvenire anche in ragione di intenti di terzi che vanno contro l'attività strategica del Paese. La sfida che si è posta, quindi, era promuovere il raggiungimento dell'autonomia tecnologica per le infrastrutture del Paese al fine di avere maggior controllo su dati e servizi e facilitare lo sviluppo di un insieme di tecnologie fondamentali per lo sviluppo del Paese.

Altro problema derivante dal predominio nel mercato del Cloud di aziende non europee è quello del **controllo sui dati**. Le aziende non europee sono soggette a leggi e normative in parte diverse rispetto a quelle europee. Questo fatto non influisce solo sui requisiti di qualità, scalabilità e flessibilità che deve soddisfare un Cloud Provider, ma anche su aspetti di carattere geopolitico e strategico per il

Paese. Infatti, se sussistono determinate circostanze, alcune legislazioni prevedono la possibilità di effettuare richieste unilaterali di accesso ai dati gestiti da un Cloud Service Provider. Perciò, potenzialmente, uno Stato Estero, in cui risiede la sede legale dell'azienda che eroga il servizio Cloud, ha la facoltà di accedere ai dati dei clienti del provider, compresi eventuali dati strategici e sensibili appartenenti a una PA italiana che ha migrato su Cloud. Quindi è stato necessario operare una classificazione rigida e precisa dei dati e servizi che potevano essere trasferiti su Cloud, in maniera da distinguere chiaramente dati e servizi che potevano essere affidati a un Cloud Service Provider pubblico anche extraeuropeo, e dati e servizi più sensibili e strategici. Questi ultimi dovevano essere gestiti da un fornitore di servizi Cloud che si impegnasse a soddisfare determinati requisiti di sicurezza e a non fornire i dati dell'Amministrazione a nessun soggetto terzo.

Proseguendo, a prescindere del luogo in cui si trova la sede legale dell'azienda, è necessario considerare anche gli **aspetti di resilienza** che offre un fornitore di servizi Cloud, nel momento in cui un ente pubblico italiano migra verso la sua infrastruttura. Il Cloud Service Provider deve garantire all'Amministrazione, non solo il soddisfacimento di requisiti di sicurezza stringenti, analoghi a quelli stabiliti per i servizi informatici e informativi degli enti nel PNSC, ma anche un certo grado di continuità di servizio e disaster recovery. I requisiti di sicurezza che il provider implementa dipendono anche dalla tipologia di dati e servizi trattati, mentre le funzionalità di disaster recovery devono essere garantite mediante siti geograficamente distribuiti sul territorio europeo. Ovviamente, fare affidamento su delle dichiarazioni di un fornitore di servizi Cloud non è sufficiente per stabilire se i requisiti di sicurezza, interoperabilità e continuità di servizio sono rispettati. Per questo si è resa necessaria la definizione di un *processo di qualificazione dei fornitori di Cloud Pubblico e dei loro servizi*, che si occupasse di valutare aspetti di sicurezza e anche architetturali e organizzativi.

Per rispondere alle sfide descritte e allo scopo di creare le misure aggiuntive citate nel paragrafo precedente, è stata ideata la *Strategia Cloud Italia*. Essa si pone in questo contesto come metodologia implementativa della policy "Cloud-First", pilastro del progetto di digitalizzazione della PA enunciato nel PNRR italiano. Questa policy permetterà di guidare, e favorire l'adozione sicura, controllata e completa delle tecnologie Cloud per la PA, con l'obiettivo, a tendere, che tutti i servizi erogati siano basati su applicazioni "Cloud-native", sviluppate cioè nativamente sulla base dei paradigmi Cloud[7]. La strategia Cloud Italia si basa su tre pilastri fondamentali, o linee di indirizzo strategico, che permettono di definire delle linee guida per l'adozione del Cloud da parte delle Pubbliche Amministrazioni. Nei prossimi paragrafi (2.2.2, 2.2.3, 2.2.4) si illustreranno gli aspetti chiave dei tre pilastri fondamentali della *Strategia Cloud Italia*, aderendo allo schema del documento ufficiale redatto dal Dipartimento per la Transizione Digitale e dall'Agenzia per la Cybersicurezza

Nazionale[7].

2.2.2 Classificazione dei dati e dei servizi

Il primo elemento fondamentale della strategia, che permette di regolamentare il processo di migrazione al Cloud che affronteranno gli enti pubblici, è la **Classificazione dei dati e dei servizi** delle Pubbliche Amministrazioni. Dividere dati utilizzati e servizi erogati dalle Pubbliche Amministrazioni contribuisce a guidare gli enti pubblici nel processo di migrazione verso Cloud, aiutandoli a individuare per i loro dati e servizi un fornitore di servizi Cloud che li gestisca in maniera adeguata e conforme alla loro importanza strategica. A tale scopo, sono state individuate le seguenti classi di dati e servizi:

- **Strategico**: comprende dati e servizi la cui compromissione ha un impatto sulla sicurezza nazionale. Di questa categoria fanno parte, in modo automatico, tutti i dati e i servizi degli enti pubblici e aziende inclusi nel PNSC.
- **Critico**: comprende dati e servizi la cui compromissione determina un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza e il benessere economico e sociale del Paese. Un esempio di dati critici sono i dati sanitari dei cittadini utilizzati da un'ASL. Inoltre, sono automaticamente classificati almeno come critici i dati dei soggetti identificati come Operatori di Servizi Essenziali ai sensi del D.Lgs. 85/2018, che ha recepito nell'ordinamento nazionale la Direttiva europea nota come NIS[17].
- **Ordinario**: comprende dati e servizi la cui compromissione non provoca l'interruzione di servizi dello Stato o, comunque, un pregiudizio per il benessere economico e sociale del Paese. A questa categoria apparterranno, ad esempio, i dati e servizi a portali istituzionali delle Amministrazioni.

Una particolarità importante da sottolineare nella classificazione dei dati stabilita dalla *Strategia Cloud Italia*, è che essa prescinde dalle normative e dai requisiti di sicurezza, classificando i dati e servizi sulla base dell'impatto che risulterebbe, a seguito di una loro compromissione, per il sistema Paese.

2.2.3 Il processo di Qualificazione dei Cloud Providers

Chiaramente, le PA che migrano su Cloud, come avviene per qualsiasi altro bene che acquistano normalmente, devono seguire delle procedure di acquisto ben definite anche nello scegliere un servizio Cloud. Purtroppo, come evidenziato nella *Strategia Cloud Italia* le attuali procedure di acquisto che devono seguire gli enti pubblici non sono abbastanza flessibili per l'acquisizione, in maniera corretta, di un servizio Cloud. Per questo il secondo elemento fondamentale della strategia consiste nella

definizione di un sistema per la *qualificazione dei servizi Cloud*, che ha come obiettivo la semplificazione e la regolamentazione del processo di migrazione di servizi Cloud da parte delle Amministrazioni. Il processo di qualificazione si focalizzerà sull'analisi delle seguenti caratteristiche:

- *gestione operativa* dei servizi Cloud, cioè degli standard tecnico-organizzativi applicati, come l'ISO 27017/27018, l'ISO 22301 e il CSA STAR, e le misure di controllo dei dati.
- *requisiti di sicurezza* implementati nella gestione dei dati ed erogazione dei servizi. Esempi di questi requisiti sono la gestione delle chiavi e i controlli di sicurezza applicati.
- *condizioni contrattuali* applicate all'erogazione del servizio, ovvero i Service-Level Agreement (SLA), e alla rendicontazione. Tra questi si annoverano le garanzie di disponibilità e gli altri strumenti contrattuali a disposizione delle organizzazioni.

Considerando questi tre aspetti di analisi è possibile, guardando all'insieme delle soluzioni tecnologiche e organizzative a disposizione nel mercato dei fornitori di servizi Cloud, individuare a priori la seguente categorizzazione dei servizi Cloud, inclusa nella Strategia Cloud Italia:

- **Servizi di Cloud Pubblico non qualificato (extra UE/UE)**: rappresentano servizi Cloud che non rispondono ai requisiti e criteri tecnico-organizzativi per ospitare servizi delle Pubbliche Amministrazioni.
- **Servizi di Cloud Pubblico qualificato (UE)**: sono servizi Cloud compatibili con le legislazioni rilevanti in materia, come GDPR[18] e NIS[17]. Questi permettono la localizzazione dei dati e dei servizi su territorio europeo e il rispetto degli standard tecnico-organizzativi, attraverso sistemi di cifratura granulare gestiti dal fornitore di servizi Cloud.
- **Servizi di Cloud Criptato (IT)**: essi sono servizi Cloud di tipo pubblico, che però consentono all'Amministrazione di gestire in maniera autonoma i meccanismi di sicurezza. Infatti, il fornitore di servizi Cloud concede all'Amministrazione di gestire autonomamente le chiavi crittografiche per la cifratura dei dati su Cloud Pubblico, utilizzando degli Hardware Security Module (HSM) on-premise.
- **Soluzioni di Cloud Privato e Ibrido**: questo tipo di servizi Cloud consente facilmente la localizzazione dei dati su territorio italiano e l'isolamento dalle "region" pubbliche dei principali fornitori di servizi Cloud. Queste due garanzie sono ottenute perché il servizio Cloud viene erogato da un fornitore sottoposto

a stretto monitoraggio pubblico. Questa tipologia di servizi si implementa in due modi:

- soluzioni basate su tecnologia hyperscaler, in cui uno o più Cloud Service Provider mette a disposizione un ambiente Cloud privato con la possibilità di supportarlo con risorse nel Cloud pubblico. In questo caso si parla di **Cloud privato/ibrido su licenza(IT)**.
- soluzioni basate su tecnologie qualificate attraverso procedure di certificazione tecnologica, denominate **Cloud privato qualificato(IT)**

Definita la qualificazione dei servizi Cloud e i servizi Cloud qualificati, si impongono dei vincoli sulla tipologia di dati e servizi che può ospitare ogni soluzione, visibili anche nella Figura 2.1. A tal proposito, le offerte di Cloud Pubblico Qualificato e

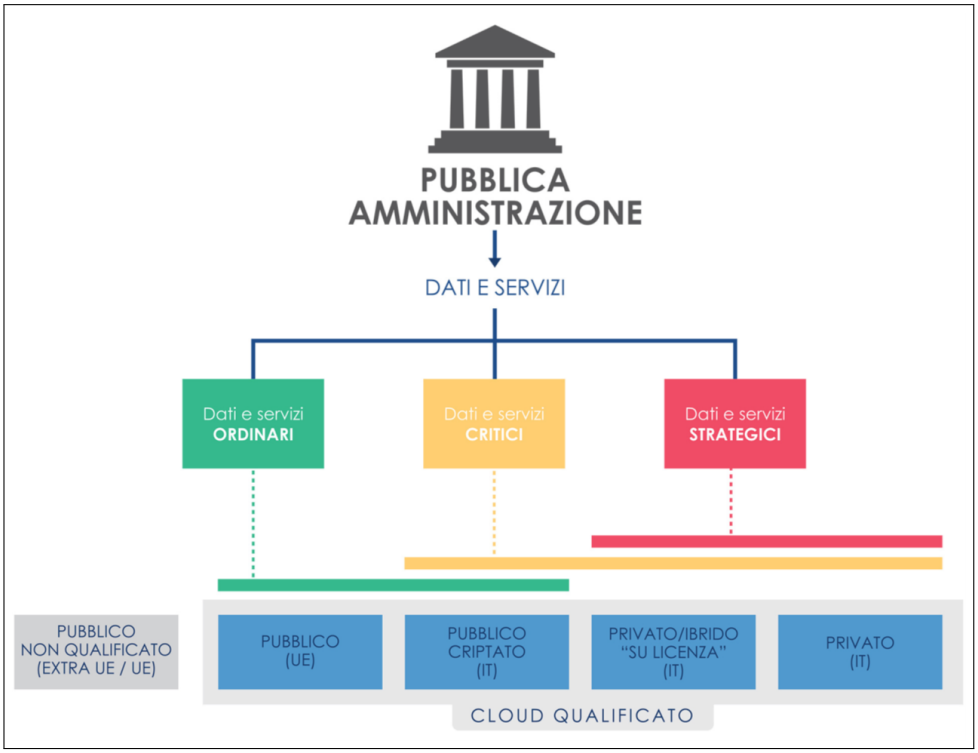

Figura 2.1: Le tipologie di servizi Cloud qualificati e quali dati e servizi possono ospitare[3]

Criptato potranno ospitare dati servizi ordinari, mentre le offerte di Cloud Criptato, Privato/Ibrido su licenza e Privato Qualificato potranno ospitare dati e servizi critici. Infine, le soluzioni di Cloud Privato/Ibrido su licenza e Cloud Privato Qualificato potranno ospitare dati e servizi strategici. In questa maniera, avendo definito ex-ante, un servizio per la qualificazione dei Cloud Provider sarà possibile creare un *mercato elettronico dei servizi Cloud qualificati*, ovvero uno strumento che guiderà tutte gli enti pubblici nella scelta e acquisto del servizio Cloud a loro più idoneo.

2.2.4 Il Polo Strategico Nazionale

I due elementi descritti nei paragrafi precedenti (2.2.2, 2.2.3) permettono di rispondere in parte alle esigenze di autonomia tecnologica e controllo sui dati che si manifestano nella migrazione verso il Cloud delle Pubbliche Amministrazioni. Potrebbe essere un lavoro difficile trovare sul libero mercato delle soluzioni Cloud che soddisfino tutti i requisiti di sicurezza richiesti da dati e servizi strategici delle Pubbliche Amministrazioni. Quindi, il terzo pilastro fondamentale della *Strategia Cloud Italia* consiste nella realizzazione del **Polo Strategico Nazionale (PSN)**, e ha l'obiettivo di dotare la Pubblica Amministrazione di tecnologie e infrastrutture Cloud che garantiscono massima affidabilità, resilienza e indipendenza. Seguendo la progettazione proposta dalla *Strategia Cloud Italia* il PSN è composto da più data center distribuiti sul territorio nazionale, in maniera da garantire la tolleranza ai guasti e la continuità operativa, e viene gestito da un fornitore qualificato sulla base di precisi requisiti tecnico-organizzativi. Inoltre, il PSN deve garantire il rispetto di alcuni requisiti di sicurezza, come ad esempio quelli richiesti dal PNSC e dal NIS[17], e facilitare la migrazione su Cloud da parte degli enti pubblici. Al livello di servizi offerti, il PSN eroga servizi di Cloud Pubblico Criptato (IT), servizi di Cloud Privato/Ibrido su licenza e servizi di Cloud Privato Qualificato (IT).

Attualmente il Polo Strategico Nazionale è in fase di realizzazione, e sono stati già raggiunti alcuni degli obiettivi prefissati dalla progettazione iniziale. Per prima cosa, è stato individuato un fornitore qualificato che si occupi della gestione dell'infrastruttura a supporto delle Pubbliche Amministrazioni, attraverso una gara di appalto europea e la pubblicazione di un bando avvenuta il 28 gennaio 2022. La gara si è conclusa a Giugno 2022, e nell'agosto 2022 è stata firmata ufficialmente la convenzione che affida la gestione del PSN a una società di nuova costituzione partecipata da aziende italiane come TIM, Leonardo Equity e Sogei e dalla Cassa Depositi e Prestiti. Successivamente, sono state individuate le sedi del PSN, cioè sono stati scelti i data center che rappresentano l'infrastruttura a supporto degli enti pubblici. L'infrastruttura Cloud del PSN è ospitata all'interno di 4 Data Center distribuiti sul territorio italiano, allestiti in una configurazione di doppia Region (Nord e Sud, distanti tra loro centinaia di chilometri) in dual-AZ (Availability Zone), cioè una coppia di Data Center in configurazione di business continuity, distanti tra loro diverse decine di chilometri[19]. Precisamente, sono stati individuati due data center nella regione Lazio, ad Acilia e Pomezia, e due nella regione Lombardia, a Rozzano e Santo Stefano Ticino.

L'individuazione dei data center e del fornitore qualificato ha permesso anche la definizione di un processo di migrazione delle Pubbliche Amministrazioni verso i servizi Cloud offerti da Polo Strategico Nazionale. La stipula di un contratto con il PSN e la richiesta di migrazione dei propri dati e servizi critici e strategici su esso

avviene in tre passi:

1. La PA invia al PSN un piano dei fabbisogni, che specifica quali sono i servizi da migrare verso il PSN e quali sono i requisiti di sicurezza di cui questi necessitano.

2. Il PSN, entro 60 giorni dalla ricezione del piano dei fabbisogni, invia alla PA che ha fatto richiesta il progetto per la realizzazione di questo piano e un preventivo riguardo il costo che dovrà sostenere la PA per la migrazione.

3. La PA analizza il progetto ed eventualmente richiede modifiche che sono inserite nel progetto dal PSN. Se la PA approva il progetto si procede con la stipula del contratto.

Con la definizione di un processo di stipula del contratto e conseguente migrazione verso il PSN, prende forma il progetto di un'infrastruttura sicura e resiliente a supporto delle Pubbliche Amministrazioni italiane, descritto nella *Strategia Cloud Italia*. Il PSN rivestirà un ruolo chiave per il supporto nel processo di migrazione verso il Cloud delle Amministrazioni Centrali(e.g. Presidenza del Consiglio dei Ministri, Ministeri, Agenzie Fiscali etc...), delle Amministrazioni Locali (e.g. Regioni, Province, Comuni etc...), e delle Aziende Sanitarie(ASL e AO). A seguito della costituzione e realizzazione dell'infrastruttura, il PSN ha l'obiettivo di portare il 75% delle Amministrazioni italiane ad utilizzare servizi in Cloud entro il 2026[20].

2.3 Altri standard e legislazioni: l'EUCS e il Golden Power

2.3.1 Il decreto Golden Power e la qualificazione del Cloud nelle imprese private

Nelle sezioni 2.1 e 2.2, oltre a descrivere la situazione delle minacce e degli attacchi che possono impattare sulle organizzazioni italiane, si è discusso anche del PNSC e dei fondamenti della *Strategia Cloud Italia*. In particolare quest'ultima, definendo una classificazione dei dati e dei servizi trattati dalle Pubbliche Amministrazioni e un processo di qualificazione dei servizi Cloud che dovranno ospitare dati e servizi delle PA, contribuisce a dare un indirizzo strategico riguardo a come agire con gli enti pubblici. La strategia, infatti, è stata lo spunto fondamentale che ha portato prima all'elaborazione del Regolamento per i Servizi Cloud emanato da AgID e poi agli allegati A2, B2 e C della determina ACN n. 307 del 18 gennaio 2022, che hanno esteso le misure di sicurezza già contenute nel Regolamento Cloud adottato da AgID con Determinazione 628/2021.

Tuttavia, la regolamentazione del processo di qualificazione dei fornitori di servizi Cloud e la definizione di misure minime di sicurezza e organizzative, che essi devono

rispettare per ospitare i servizi e i dati delle Pubbliche Amministrazioni, non sono sufficienti per tutelare completamente la sicurezza nazionale. Come accennato in precedenza, esistono imprese e soggetti privati che erogano servizi essenziali e strategici per il sistema Paese, utilizzando infrastrutture digitali, sistemi informatici e informativi. Queste aziende, come le Pubbliche Amministrazioni, stanno affrontando un processo di trasformazione digitale al loro interno che può includere anche l'adozione di tecnologie e servizi Cloud offerti da un Cloud Service Provider. Poiché anche questi soggetti, come le Pubbliche Amministrazioni, erogano servizi importanti per i cittadini, l'adozione di servizi Cloud in queste aziende ha una rilevanza strategica non indifferente per il Paese.

È apparsa necessaria, dal contesto descritto, la definizione di un sistema legislativo che permettesse di controllare e regolamentare anche il processo di migrazione su Cloud nelle imprese private che fanno parte del tessuto economico del Paese. In particolare, serviva uno strumento normativo che avrebbe permesso al Governo di intervenire nel processo di adozione di servizi Cloud da parte di un'impresa privata, esercitando poteri speciali e straordinari. Questi poteri avrebbero fornito al Governo la possibilità di imporre condizioni e prescrizioni per la migrazione verso determinati servizi Cloud, o in casi estremi, bloccare il processo di migrazione verso un Cloud Service Provider. Per rispondere a questa esigenza, è stato previsto l'ampliamento della portata del DL 15 marzo 2012 n.21, cioè il decreto noto come *Golden Power*[21].

Inizialmente riferito all'esercizio di poteri speciali riguardo i contratti o accordi che avevano come oggetto l'acquisizione di servizi di comunicazione elettronica a banda larga, basati su tecnologie 5G, l'articolo 1-bis del decreto Golden Power è stato ampliato e modificato nel tempo. Infatti, la costante evoluzione tecnologica vissuta negli ultimi anni ha portato a modificare con ulteriori leggi e decreti legge l'articolo per adeguarlo al mutato contesto tecnologico. La modificazione più importante applicata all'art. 1-bis è quella introdotta con l'art. 28 del DL 21 marzo 2022 n.21, convertito in legge con modificazioni dalla Legge 20 maggio 2022 n.51, la quale ha demandato a ulteriori decreti del Presidente del Consiglio dei Ministri l'identificazione di ulteriori beni, servizi, rapporti, attività e tecnologie di rilevanza strategica per il sistema di difesa e sicurezza nazionale del Paese. Di recente, è importante sottolineare che tra le tecnologie di rilevanza strategica per il Paese sono state incluse anche le tecnologie Cloud.

L'art. 1-bis del decreto *golden power*, perciò, stabilisce che i servizi di comunicazione a banda larga basati su 5G, le tecnologie basate su Cloud, e ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica, individuati con altri DPCM, costituiscono attività di rilevanza strategica per i sistemi di difesa e sicurezza nazionale. Inoltre, esso concede al Governo la possibilità di esercitare poteri speciali e straordinari nel caso in cui un'impresa voglia dotarsi di una delle sopracitate tecnologie. Quindi, se un'impresa italiana vuole acquistare un bene, o

servizio, o componente ad alta intensità tecnologica, finalizzato alla realizzazione, alla manutenzione e alla gestione di una delle attività citate, ha l'obbligo di notificare alla Presidenza del Consiglio dei Ministri un piano annuale relativo all'acquisizione degli elementi citati. I contenuti del piano annuale sono ben descritti nel comma 2 all'art. 1-bis del decreto *golden power*, e non si esclude che nel futuro altri decreti del Presidente del Consiglio dei Ministri possano individuare altri contenuti da inserire nel piano stesso. In più, viene anche stabilito che il piano può essere aggiornato dall'impresa con cadenza quadrimestrale e gli aggiornamenti vanno comunicati con le stesse modalità con cui avviene la notifica del piano.

L'esercizio dei poteri speciali conferiti al Governo si traduce nella possibilità di procedere con tre azioni nel momento in cui un'impresa notifica il proprio piano annuale:

- **Imposizione di prescrizioni o condizioni**: è la forma primaria dell'esercizio dei poteri speciali e consiste nel porre delle prescrizioni e condizioni alla realizzazione del piano annuale presentato dall'azienda.

- **Approvazione temporanea del piano**: in alcuni casi non è sufficiente l'imposizione di prescrizioni a condizioni per tutelare gli interessi di difesa e sicurezza nazionale del Paese. Allo stesso tempo, la bocciatura del piano potrebbe rallentare in maniera significativa lo sviluppo tecnologico del Paese creando disagi importanti alle aziende private. Quindi, l'esercizio dei poteri speciali consente anche di approvare il piano, in tutto o in parte, per un periodo limitato di tempo, al termine del quale alcuni beni o servizi vanno sostituiti. Se tale obbligo non viene rispettato dall'impresa allora il Governo impone il veto sul piano.

- **Veto**: il piano annuale viene bocciato completamente.

In più, il comma 3 dell'art. 1-bis stabilisce anche i termini entro cui deve avvenire la revisione del piano e la sua eventuale approvazione da parte della Presidenza del Consiglio dei Ministri.

Proseguendo, l'art. 1-bis sancisce anche come il Governo possa agire nel caso in cui le imprese non assolvano agli obblighi di notifica descritti. Per prima cosa, se l'impresa attiva i contratti contenuti nel piano annuale prima della sua approvazione, il Governo può imporle l'obbligo di ripristinare, a sue spese, la situazione precedente alla loro attivazione. In più, se un'impresa non rispetta gli obblighi di notifica del piano o dei suoi aggiornamenti può essere soggetta a sanzione pecuniaria. Allo stesso modo, se sono attivati contratti che violano le prescrizioni e condizioni imposte dal Governo sul piano, questi sono annullati e l'impresa deve ripristinare, a sue spese, le condizioni precedenti alla loro attivazione. Infine, viene concessa al Governo la

possibilità di avviare il processo di esercizio dei poteri speciali anche in assenza di notifica da parte dell'impresa.

In conclusione, l'articolo già citato istituisce anche un Gruppo di coordinamento e un Comitato di monitoraggio, rispettivamente per curare l'istruttoria delle notifiche e proporre al Governo, se del caso, l'esercizio dei poteri speciali e per la verifica del rispetto delle prescrizioni e condizioni imposte. In dettaglio, il Gruppo di coordinamento si occupa di valutare il piano annuale presentato dalle imprese e di stabilire delle condizioni o delle prescrizioni da imporre per l'attuazione del piano stesso. Il Comitato si occupa, invece, di verificare che l'impresa stia rispettando le prescrizioni e le condizioni imposte e che le misure attuative delle prescrizioni o condizioni siano adeguate al contesto. Inoltre, il Comitato si occupa anche di segnalare al Gruppo di coordinamento il mancato rispetto delle prescrizioni e condizioni imposte. Quest'ultimo, invece, può proporre alla Presidenza del Consiglio dei Ministri di applicare le sanzioni già descritte o di interdire il soggetto dalle attività, funzionali alla progettazione, realizzazione, manutenzione e gestione delle attività descritte in precedenza. La prospettata estensione dell'art. 1-bis del decreto *Golden Power* alle tecnologie Cloud comporterà ulteriori valutazioni. A tal proposito, si rimanda all'analisi svolta in una recente pubblicazione sul tema ([22]), in cui si affrontano gli impatti di tale estensione sulle attività del Gruppo di coordinamento.

Il primo aspetto che il decreto *golden power* lascia a provvedimenti futuri è l'individuazione degli ulteriori beni, servizi, rapporti, attività e tecnologie di rilevanza strategica per il sistema di difesa e sicurezza nazionale. Nel prossimo futuro, sarà compito della Presidenza del Consiglio dei Ministri e dell'ACN stabilire quali tra le nuove tecnologie emergenti avranno impatto sul sistema di difesa e sicurezza nazionale. A tale scopo, come riportato dall'articolo, è possibile fare riferimento all'attuale quadro normativo e ad altre fonti istituzionali. Ad esempio, si potrebbero includere all'interno dell'ambito applicativo del decreto *golden power* sia le categorie di beni e servizi ICT che vanno valutati dal CVCN, se utilizzati per erogare servizi essenziali, sia le Emerging Disruptive Technologies (EDT) elencate all'interno dell'*Agenda di ricerca e innovazione per la cybersicurezza 2023-2026*. In particolare, l'autore dell'articolo indica, tra le EDT individuate dall'Agenda, quelle che potrebbero avere maggiore rilevanza per la sicurezza nazionale, tra cui la Distributed Ledger Technology (DLT), la Hardware-based security, l'Internet of Things (IoT), le tecnologie quantistiche e così via.

Poi, al fine di applicare in maniera efficace i poteri speciali attribuiti al Governo dal decreto *golden power*, è necessario stabilire esattamente qual è l'ambito di applicazione del decreto, ovvero individuare le imprese che possono essere sottoposte ai provvedimenti di esercizio dei poteri speciali. Facendo riferimento alla legislazione vigente, i soggetti privati che rivestono un ruolo di rilevanza strategica per la sicurezza cibernetica del Paese sono:

- le imprese incluse nel Perimetro Nazionale di Sicurezza Cibernetica
- gli Operatori di Servizi Essenziali (OSE), cioè le imprese soggette alla direttiva NIS (direttiva UE 2016/1148).
- gli operatori telco sottoposti alle misure di sicurezza cibernetica di cui al decreto del Ministro dello Sviluppo Economico 12 dicembre 2018.
- i Cloud Service Provider qualificati

Nonostante alcune aziende rientrino in più di una delle categorie elencate, le imprese che potrebbero essere impattate dai provvedimenti, contenuti nell'art. 1-bis del decreto *golden power*, sono nell'ordine delle centinaia. Considerando che ognuna di queste, annualmente, deve notificare il proprio piano di acquisizione, con la possibilità di inviare anche notifiche di aggiornamento del piano con cadenza quadrimestrale, il numero di notifiche prodotte potrebbe sovraccaricare in maniera eccessiva il Gruppo di Coordinamento. L'alto numero di notifiche prodotto potrebbe condizionare il lavoro del Gruppo di Coordinamento portandolo a non poter svolgere un lavoro di revisione del piano e imposizione delle prescrizioni approfondito e minuzioso. Quindi, è necessario individuare alcuni criteri che permettano di limitare il campo di applicazione del decreto. L'autore dell'articolo come possibili soluzioni, relativamente al contesto del Cloud Computing, propone:

- **Tipologia di servizio**: l'obbligo di notifica è imposto solo per i servizi Cloud di tipo IaaS e PaaS, che spesso costituiscono la base attraverso cui si erogano servizi SaaS. Con questa soluzione, si ha il vantaggio di poter valutare profili di rischio che andranno a impattare moltissimi servizi di livello superiore. Allo stesso tempo, lo svantaggio principale è che non si sottopongono a scrutinio servizi SaaS che trattano direttamente dati sensibili appartenenti a soggetti di rilievo per la sicurezza nazionale.
- **Tipologia di dati**: utilizzando la classificazione dei dati e dei servizi, descritta nell'ambito della *Strategia Cloud Italia*, si potrebbe limitare l'obbligo di notifica solo ai servizi Cloud utilizzati per il trattamento di dati critici e strategici e l'erogazione di servizi analoghi. In questa maniera, si ridurrebbe al 20% della quota attuale, la quantità di imprese soggette a notifica.
- **Tipologia di soggetto**: in questo caso si limita l'obbligo di notifica solo a una delle categorie di soggetti citate in precedenza, ad esempio solo alle imprese nel perimetro.

Un ulteriore aspetto che dovrà essere definito riguarda la tipologia di condizioni e prescrizioni che possono essere imposte alle imprese nel processo di approvazione e messa in atto del piano annuale. Il decreto accenna spesso a questo modo di esercitare

i poteri speciali nell'ambito del *golden power*, senza mai indicare esplicitamente o con riferimento ad altre leggi e regolamenti, un modo per definire queste condizioni e prescrizioni. Come sottolineato anche nell'articolo, lo stesso decreto legge fornisce un principio generale di definizione delle condizioni e prescrizioni per la mitigazione dei fattori di rischio, suggerendo di avvalersi dei principi e delle linee guida elaborate a livello internazionale e dall'UE.

Quindi, la definizione di misure idonee per mitigare il rischio connesso all'impiego di un determinato servizio Cloud, deve essere ispirata da standard già collaudati in ambito internazionale. Negli ultimi tempi, però, anche l'Italia ha fatto passi avanti rispetto alla definizione di misure di sicurezza per l'adozione di servizi Cloud, elaborando un impianto di qualificazione per i Cloud Providers valido per le Pubbliche Amministrazioni. Infatti, a livello nazionale prima con la *Strategia Cloud Italia*, successivamente con il Regolamento Cloud per la PA redatto da AgID e poi con la determina n. 307 di ACN, si è definito un impianto di misure e controlli di sicurezza a cui il Gruppo di Coordinamento potrà sicuramente attingere per la definizione delle misure e prescrizioni. In aggiunta, queste misure per la qualificazione di Cloud Service Providers in ambito pubblico sono state definite facendo riferimento a linee guida, framework e norme tecniche internazionali, in ottemperanza a quanto richiesto dal decreto. Inoltre, anche lo schema di certificazione dei servizi Cloud europeo, l'EUCS, potrà essere un valido spunto per il lavoro condotto dal Gruppo di Coordinamento.

Alla luce di questa analisi, il lavoro di definizione di metodologie di verifica delle misure di sicurezza definite in ambito pubblico ha una ripercussione diretta anche sull'ambito del *golden power*. Infatti, le misure di sicurezza per la qualificazione di servizi Cloud in ambito pubblico contribuiscono al lavoro del Gruppo di Coordinamento nell'imposizione di prescrizioni e condizioni per il passaggio al Cloud degli enti privati. Allo stesso tempo, le metodologie sviluppate con questo lavoro di tesi potrebbero essere un valido supporto anche per il comitato che si deve occupare di verificare il soddisfacimento delle condizioni e prescrizioni. Quindi, è fondamentale sviluppare e revisionare continuamente le metodologie proposte, in maniera da costruire anche per il processo di migrazione verso il Cloud delle imprese private, un impianto di verifica delle condizioni e prescrizioni imposte, contribuendo alla sicurezza cibernetica del sistema Paese.

2.3.2 European Cloud Scheme - EUCS

Il bisogno di uno schema di qualificazione per i servizi Cloud non è stato colto solo dagli organismi di governo dei singoli paesi europei, ma anche dalle autorità ed agenzie facenti capo direttamente all'UE. Come testimoniato dai dati presentati nel paragrafo 1.4 l'utilizzo del Cloud Computing in Europa è molto diffuso in tutti i paesi dell'Unione. Allo stesso tempo, i dati evidenziati nel rapporto del CLUSIT,

e discussi nel paragrafo 2.1.1 testimoniano un aumento degli attacchi non solo alle istituzioni italiane, ma anche a quelle europee. Anche in Europa, perciò, il crescente utilizzo del Cloud da parte delle istituzioni unito ad un aumento preoccupante degli attacchi informatici ha spinto le autorità europee ad intervenire. Per questo, l'Unione Europea nel 2019 ha varato il Cybersecurity Act, ovvero un provvedimento per rafforzare l'agenzia europea per la cybersecurity, cioè l'ENISA, e creare un framework di cybersecurity per la certificazione dei prodotti e dei servizi.

In realtà, alcuni paesi dell'Unione Europea hanno già prodotto e stanno producendo degli schemi di certificazione dei prodotti e dei servizi IT al livello nazionale, per gli stessi motivi. Però, la presenza di più schemi al livello nazionale potrebbe causare una serie di problemi, di cui il primo è quello che uno schema creato in un paese dell'UE potrebbe non essere riconosciuto da altri paesi. Quindi, questo significa che un'impresa che desideri operare al livello transnazionale, potrebbe dover certificare i propri prodotti e servizi IT secondo più schemi differenti, sostenendo dei costi di certificazione esagerati, che possono impattare negativamente sulla crescita delle imprese Europee e sull'adozione di nuove tecnologie. Perciò, è evidente la necessità di definire schemi di certificazione dei prodotti e dei servizi IT validi al livello europeo, in maniera tale da facilitare l'adozione di questi prodotti da parte di enti pubblici e imprese nell'Unione, aumentare la fiducia dei consumatori ed abbattere i costi sostenuti dalle imprese che vogliono operare al livello internazionale. Tuttavia il Cybersecurity Act non definisce direttamente gli schemi di certificazione, ma si limita a definire delle regole che stabiliscono quali caratteristiche devono avere questi schemi di certificazione e come devono essere realizzati. In particolare, il provvedimento citato ha affidato all'ENISA il compito di realizzare questi schemi di certificazione, predisponendo dei gruppi di lavoro ad hoc, formati non solo da funzionari dell'agenzia, ma anche da rappresentanti di imprese private operanti nel settore tecnologico per cui si crea lo schema.

Vista l'importanza delle tecnologie Cloud, il Cybersecurity Act le include, all'interno dei prodotti e servizi IT per cui è necessaria la definizione di uno schema di certificazione. Per questo motivo, l'ENISA ha costituito un gruppo di lavoro, composto anche da funzionari di grandi aziende come Amazon e Cisco, che si impegnasse a realizzare uno schema di certificazione dei servizi Cloud. Da questo sforzo congiunto di funzionari dell'ENISA e di alcune aziende private, è nata la prima versione dell'European Cybersecurity Certification Scheme for Cloud Services (EUCS), ovvero uno schema per la qualificazione dei servizi Cloud europeo. I lavori sono tuttora in corso e, una volta finalizzato il testo di EUCS, il nuovo schema dovrà essere adottato attraverso un apposito Atto Esecutivo. Lo schema EUCS presenta alcune differenze fondamentali rispetto all'impianto di qualificazione creato per i servizi Cloud al livello italiano, ed espresso dalla *Strategia Cloud Italia*, dal Regolamento AgID e dagli allegati alla determinazione n.307 di ACN.

Innanzitutto lo schema EUCS è uno schema volontario, cioè attualmente non è necessario ottenere la certificazione secondo lo schema EUCS per fornire servizi Cloud agli enti pubblici dell'Unione Europea e dei paesi membri. Quindi, i fornitori di servizi Cloud per erogare i propri servizi a enti pubblici in un qualsiasi paese europeo, non devono ottenere per forza la qualificazione EUCS, ma devono aderire allo schema di qualificazione ideato e adottato nel paese stesso. Tuttavia, è plausibile che alcuni Stati membri rendano obbligatoria la certificazione EUCS in certi contesti, ovvero i fornitori di servizi Cloud, che vorranno erogare i propri prodotti a enti pubblici e imprese private, considerati essenziali o critici, all'interno dei paesi europei, dovranno ottenere obbligatoriamente la qualificazione EUCS. Quindi, capire quali sono le differenze tra lo schema EUCS e lo schema di qualificazione nazionale è fondamentale per integrare in futuro i due schemi e facilitare l'adozione delle tecnologie Cloud in tutta Europa.

Lo schema di certificazione europeo ha un approccio diverso rispetto a quello nazionale, già accennato tramite la *Strategia Cloud Italia*, e descritto in dettaglio nei paragrafi 3.2.1 e 3.2.2. Per prima cosa lo schema EUCS fa riferimento solamente alla certificazione dei servizi Cloud, elencando una serie di requisiti che devono avere i servizi oggetto della certificazione, tra cui sono inclusi anche quelli a cui deve aderire l'infrastruttura sottostante. Al contrario, lo schema di qualificazione nazionale, espresso dal Regolamento AgID e dalla determina n. 307 di ACN, fa chiara distinzione tra servizio Cloud e infrastruttura sottostante, prevedendo due processi di qualificazione separati e requisiti diversi. Inoltre, lo schema europeo distingue i servizi Cloud sulla base delle *Cloud capabilities type*, ovvero delle risorse impiegate per erogare il servizio Cloud, sconsigliando, invece, l'utilizzo della classificazione per modelli di servizio (IaaS, PaaS, SaaS), propria dello schema di qualificazione italiano. In più, i riferimenti tecnici e gli standard a cui sono ispirati i requisiti contenuti all'interno dello schema EUCS sono diversi da quelli a cui sono ispirati i livelli minimi delle infrastrutture e le caratteristiche dei servizi Cloud, citati nella determina n. 307. Infatti, mentre lo schema europeo si basa principalmente sullo schema tedesco Cloud Computing Compliance Controls Catalog (C5) e sullo schema francese SecNumCloud, lo schema nazionale definisce i requisiti ispirandosi al Framework Nazionale di Cybersecurity e alla CSA Cloud Control Matrix (CCM).

Anche se le differenze appena discusse sono comunque importanti, l'aspetto che allontana lo schema EUCS dallo schema di qualificazione italiano è che questo non si basa sulla classificazione dei dati e dei servizi, che è uno dei pilastri della *Strategia Cloud Italia*. Infatti, lo schema europeo stabilisce quali sono i requisiti a cui devono aderire i servizi Cloud, non sulla base della criticità dei dati e dei servizi che sono offerti mediante quei servizi, ma sulla base dei cosiddetti **livelli di garanzia**. Questi non fanno riferimento al valore o all'impatto derivante dalla compromissione dei dati o servizi migrati sul Cloud, ma fanno riferimento al grado di sicurezza garantito, cioè

quanto devono essere sicuri dati e servizi portati sul Cloud. In particolare, lo schema definisce tre livelli di garanzia:

- **Basic**: comprende tutti i requisiti che coprono tutti i principali aspetti di sicurezza del Cloud.
- **Substantial**: include tutti i requisiti necessari a proteggere la maggior parte dei casi aziendali.
- **High**: è l'insieme dei requisiti finalizzati a proteggere i casi più sensibili di utilizzo del Cloud compresi quelli relativi all'interesse fondamentale per la società, o interessi commerciali molto sensibili.

La differente impostazione dello schema EUCS comporta che anche i metodi di valutazione per l'erogazione della qualificazione siano diversi. Infatti, nello schema EUCS sono definiti due metodi di valutazione, uno per il livello di garanzia Basic e uno per i livelli di garanzia Substantial e High. Al contrario, come si vedrà anche nel capitolo successivo, la determina n. 307 di ACN stabilisce quali tipologie di verifica può effettuare il regolatore, prescindendo però dal livello dei dati e dei servizi.

Chiaramente le differenze evidenziate tra lo schema EUCS e lo schema nazionale non sono un problema che deve affrontare solo l'Italia, ma anche tutti gli altri paesi che hanno un loro schema di qualificazione dei servizi Cloud. Quando lo schema europeo entrerà in vigore, diventando anche obbligatorio, sarà necessario sopprimere o riadattare tutti gli schemi nazionali. Infatti, non è detto che tutti i paesi dell'Unione Europea condividano la modalità con cui è stato realizzato lo schema e i requisiti di sicurezza in esso stabiliti, in quanto alcuni paesi potrebbero giudicarli troppo stringenti e limitanti per il libero mercato, mentre altri potrebbero giudicarli troppo laschi e incapaci di garantire un livello di sicurezza adeguato. Quindi probabilmente, sarà necessario emendare e correggere l'attuale testo dello schema di certificazione europeo fino a raggiungere un punto in cui questo sia condiviso da tutti gli Stati membri. Un'altra soluzione potrebbe essere riadattare gli schemi nazionali, in maniera da configurarli come estensione dello schema EUCS adottato in tutta Europa. In questa maniera, ogni paese può individuare un gruppo di imprese ed enti pubblici per cui sono necessari requisiti di sicurezza più stringenti e imporre che per questi sia utilizzato lo schema nazionale. Così facendo, i fornitori di servizi Cloud, ottenendo una certificazione nazionale, avranno la facoltà di offrire servizi Cloud sia alle istituzioni ritenute particolarmente critiche dal paese in oggetto, sia a tutti gli altri enti pubblici ed imprese private per cui è sufficiente la certificazione europea. Allo stesso modo, se il provider che si certifica a livello nazionale, è già qualificato secondo lo schema EUCS, il processo di verifica al livello nazionale si snellisce, in quanto riguarda solo gli aspetti aggiuntivi rispetto allo schema comunitario.

Capitolo 3

Regolamenti per la qualificazione dei servizi Cloud

3.1 Frameworks per la Cybersecurity

3.1.1 Il Cybersecurity framework del NIST

Nel 2014 il governo degli Stati Uniti d'America, attraverso il Cybersecurity Enhancement Act (CEA)[23], ha affidato al National Institute of Standards and Technology (NIST) il compito di sviluppare dei framework per la cybersecurity. In particolare al NIST venne imposto di identificare un approccio prioritizzato, flessibile, ripetibile, basato sulle performance ed economicamente vantaggioso, che includa misure e controlli per la sicurezza delle informazioni, i quali possano essere volontariamente adottati dai proprietari e gestori delle infrastrutture critiche per aiutarli ad identificare, valutare e gestire i rischi cyber[4]. Il risultato finale è stato, nello stesso anno, la pubblicazione della prima versione del NIST Cybersecurity Framework, cioè uno strumento capace di supportare i gestori e proprietari di infrastrutture critiche nella definizione di processi di gestione del rischio cyber e di programmi di cybersecurity.

Il Cybesecurity Framework sviluppato dal NIST può essere uno strumento molto utile per le organizzazioni che gestiscono infrastrutture critiche e servizi essenziali. Infatti, il Framework fornisce una tassonomia e un meccanismo che supporta le organizzazioni in vari processi:

1. Descrivere la loro postura corrente nei confronti della cybersecurity.
2. Descrivere lo stato "target", in termini di controlli e processi di cybersecurity, che si vuole raggiungere.
3. Identificare e prioritizzare le opportunità per i miglioramenti, in un processo continuo e ripetibile.
4. Valutare i progressi verso lo stato "target".
5. Esporre agli stakeholder interni ed esterni informazioni riguardanti il rischio cyber.

Inoltre, il Framework ideato dal NIST non dipende da una tecnologia implementativa precisa e fa riferimento a numerosi standard, linee guida e best practices che evolvono parallelamente alle tecnologie disponibili. In sostanza, le caratteristiche del Framework lo rendono uno strumento efficace per la gestione del rischio cyber nelle organizzazioni, che però non rallenta le innovazioni e lo sviluppo tecnologico all'interno delle stesse.

La struttura del Framework, come si approfondirà in seguito, è molto schematica e potrebbe sembrare vincolante per certe organizzazioni che hanno bisogni particolari. Tuttavia, come dichiarato anche dal NIST nella pubblicazione omonima[4], il Framework non costituisce un approccio universale per la gestione del rischio cyber per le infrastrutture critiche, in quanto ogni organizzazione è affetta da rischi, minacce e vulnerabilità diverse e allo stesso modo ha anche una sua tolleranza al rischio diversa da quella delle altre. Per questo motivo, il NIST ammette che gli utilizzatori del Framework possano personalizzarne l'implementazione, in maniera che esso possa supportare le organizzazioni ad affrontare anche minacce e rischi specifici. In sintesi, il Framework non nasce come strumento che mira a rimpiazzare le pratiche di gestione del rischio cyber e i programmi di cybersecurity esistenti nelle aziende che possiedono o gestiscono infrastrutture critiche, ma ha l'obiettivo di migliorare questi elementi per abbattere i costi e proteggere le infrastrutture critiche. Il modo in cui utilizzare il Framework è scelto dall'organizzazione in dipendenza dei suoi bisogni e dei propri bisogni in materia di cybersecurity. Tipicamente, nelle organizzazioni che mettono in pratica dei processi di gestione del rischio cyber, il Framework è pensato come un approccio su cui queste possono far leva per identificare delle opportunità e dei modi con cui migliorare la propria gestione del rischio cyber. Invece, nelle organizzazioni che non hanno ancora sviluppato delle pratiche di gestione del rischio cyber e un programma di cybersecurity, il Framework rappresenta un valido aiuto per la gestione di pratiche adatte ad affrontare rischi e minacce cyber.

Il NIST, con la pubblicazione del Cybersecurity Framework, soddisfa le richieste governative e fornisce all'ecosistema delle organizzazioni globali uno strumento altamente flessibile e valido per migliorare la gestione del rischio all'interno delle organizzazioni. La grande flessibilità del Framework si coglie, oltre che negli aspetti già citati, anche dal fatto che può essere utilizzato da organizzazioni che non posseggono o gestiscono infrastrutture critiche e anche da aziende al dì fuori degli Stati Uniti. Infatti, la tassonomia di standard, linee guida e pratiche a cui il Framework fa riferimento è indipendente dallo stato in cui questo viene implementato. Proseguendo, si presenta in dettaglio la struttura del NIST Cybersecurity Framework, che si articola in tre componenti chiave:

- *Framework Core*: costituisce un insieme di attività di cybersecurity comuni a tutti i settori in cui sono utilizzate infrastrutture critiche. Lo scopo di tale

componente è quello di fornire linee guida e standard che permettano di esporre a tutti i livelli dell'organizzazione il programma di cybersecurity e i risultati che esso mira ad ottenere.

- *Framework Imlementation Tiers*: gli Implementation Tiers permettono di descrivere quanto i processi di gestione del rischio cyber all'interno di un'organizzazione aderiscono alle caratteristiche definite nel Framework. É compito di ogni organizzazione selezionare l'Implementation Tier ad essa più adeguato.

- *Framework Profile*: il Profilo rappresenta l'allineamento a determinati standard, linee guida e pratiche definite all'interno della parte Core del Framework, da parte dell'organizzazione. Un Profilo può essere utilizzato o per descrivere lo stato attuale dell'organizzazione, rispetto alle pratiche del Framework Core, oppure per definire uno scenario di aderenza al Framework a cui l'organizzazione vuole arrivare.

Di seguito, si descrivono in maniera più dettagliata le tre componenti chiave del Framework, al fine di mostrare la loro utilità e importanza nel miglioramento dei programmi di cybersecurity delle organizzazioni.

La parte principale, cioè il *Framework Core*, fornisce alle organizzazioni un insieme di attività che permettono di raggiungere dei risultati, oltre che una serie di linee guida e riferimenti informativi che facilitano l'organizzazione nell'ottenimento dei risultati. Il Core si compone di quattro componenti principali, ovvero Funzioni, Categorie, Sottocategorie e Riferimenti Informativi. Le Funzioni provvedono a dare una prima visione di alto livello sulle attività di cybersecurity che vanno condotte all'interno di un'organizzazione. All'interno del Framework esistono cinque funzioni, le cui attività collegate non vanno eseguite in maniera seriale, ma continuamente e in maniera concorrente a quelle delle altre funzioni. Si riporta, la descrizione precisa di ogni funzione e le attività di alto livello che include:

- **Identify**: essa comprende tutte le attività che permettono all'organizzazione di individuare le risorse che supportano le funzioni critiche e il rischio cyber correlato a quelle risorse. Lo scopo delle attività comprese in tale funzione è quello di sviluppare una consapevolezza generale in tutta l'organizzazione, per facilitare le gestione del rischio cyber correlato ai sistemi, agli asset, alle persone e ai dati.

- **Protect**: contiene tutte le attività che permettono di contenere e limitare al minimo gli impatti derivanti dall'accadimento di rischi cyber. Tutte le attività comprese nella funzione contribuiscono a sviluppare e implementare misure di sicurezza per assicurare il funzionamento delle infrastrutture critiche dell'organizzazione.

- **Detect**: tale funzione elenca tutte le attività necessarie a identificare l'accadimento di incidenti informatici ed eventi di cybersecurity. Il fine di questa funzione consiste nello sviluppo di attività appropriate per rilevare eventi che possono essere indice dell'accadimento di un incidente cyber.

- **Respond**: essa ingloba tutte le attività da eseguire al fine di contenere un incidente di sicurezza. Mettendo in pratica tutte le indicazioni contenute in questa funzione è possibile sviluppare e implementare azioni di risposta ad eventuali incidenti di sicurezza.

- **Recovery**: questa funzione indica come ripristinare il normale funzionamento dei sistemi di un'organizzazione in maniera tempestiva a seguito di un incidente di sicurezza. Il risultato dell'implementazione di questa funzione consiste nella costruzione di piani per il ripristino di ogni servizio o funzione organizzativa intaccata da un incidente informatico.

Le funzioni forniscono solo una visione di alto livello sulle attività che un'organizzazione può mettere in pratica per creare o migliorare il processo di gestione del rischio cyber, e per questo ogni funzione viene divisa in **Categorie**. Ogni Categoria del Framework rappresenta una specializzazione della funzione a cui è riferita, dettagliando in maniera più specifica come svolgere determinati attività e processi. Le Categorie danno un'indicazione di alto livello su come un'insieme di processi e attività, compresi all'interno di una funzione e simili per tipologia e risultati desiderati, vanno messi in pratica. Nonostante siano più specifiche, le Categorie non sono comunque sufficienti a dare un'indicazione puntuale e precisa all'organizzazione che utilizza il Framework al fine di metterlo correttamente in pratica. Quindi, ogni Categoria si divide in **Sottocategorie**, che rappresentano un'ulteriore specializzazione e comprendono solo una o più attività, tecnologiche o di gestione, relative alla gestione del rischio cyber. Le Sottocategorie rappresentano la più piccola articolazione del *Framework Core* e rappresentano quello che un'organizzazione deve implementare nel momento in cui applica il Framework. Per facilitare l'implementazione delle Sottocategorie presenti nel Framework il NIST ha allegato ad ognuna di esse una serie di **Riferimenti Informativi**, ovvero una lista di linee guida, pratiche di sicurezza e sezioni di standard, comuni a tutti i settori in cui sono utilizzate infrastrutture critiche. I riferimenti informativi rappresentano una serie di indicazioni su come implementare la sottocategoria associata in maniera corretta, migliorando il processo di gestione del rischio cyber all'interno dell'organizzazione.

Per rendere più chiara la differenza tra funzioni, categorie, sottocategorie e riferimenti informativi si fa riferimento alla Tabella 3.1, in cui è dettagliata la divisione in categorie e sotticategorie della funzione di Identify del *Framework Core*. La funzione di Identify, il cui identificativo è ID, viene suddivisa in delle Categorie, tra

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Governance (ID.GV)**: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1**: Organizational cybersecurity policy is established and communicated	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	**CIS CSC** 1 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**CIS CSC** 12 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

Tabella 3.1: Esempio della divisione in categorie e sottocategorie di una funzione del *Framework Core*[4]

cui quella di "Asset Management" mostrata nell'immagine, che fa riferimento a tutte le attività di gestione degli asset fisici e umani in relazione alla loro importanza e criticità per l'organizzazione. Essa prescrive che tutti gli asset fisici, i dati e le risorse umane dell'organizzazione siano identificati e gestiti a seconda della loro criticità per l'organizzazione. A sua volta la categoria di Asset Management, identificata con ID.AM, è suddivisa in sei Sottocategorie, ognuna identificata da un numero progressivo e relativa solo a un determinato aspetto di quanto indica la Categoria. Ad esempio, la prima Sottocategoria, ID.AM-1, fa riferimento solo ai dispositivi fisici e ai sistemi, imponendo la loro registrazione in un inventario. La sezione sui riferimenti informativi, infine, contiene tutta una serie di riferimenti a sezioni di standard e linee guida, internazionali, che forniscono ulteriori dettagli su come implementare in maniera corretta quanto richiesto dalla Sottocategoria.

Proseguendo, la seconda parte fondamentale del Cybersecurity Framework del NIST sono gli *Implemenation Tiers*, più semplicemente *Tiers*, i quali consentono di stabilire quanto un'organizzazione considera la gestione del rischio cyber e quali processi sono svolti per la gestione del rischio. I *Tiers* rappresentano lo strumento adatto per comprendere quanto il processo di gestione del rischio cyber sia condizionato dagli obiettivi e bisogni di business dell'organizzazione e quanto sia integrato nelle pratiche globali di gestione del rischio all'interno dell'organizzazione. Il Framework definisce quattro *Tiers*, e maggiore è il numero assegnato al *Tier* maggiore è il rigore e la sofisticazione nelle pratiche di gestione del rischio cyber dell'organizzazione. La selezione del *Tier* è un processo svolto dall'organizzazione che utilizza il Framework e in esso si tiene conto di moltissimi fattori, quali le minacce, le normative e le leggi, le pratiche di gestione del rischio cyber e di condivisione dell'informazione dell'organizzazione, i requisiti di sicurezza della "supply chain" e gli altri vincoli interni all'organizzazione. Oltre a selezionare il *Tier* in cui l'organizzazione si identifica, essa deve scegliere anche il *Tier* che desidera, scegliendone uno fattibile, che riduce il rischio cyber e in accordo con i bisogni dell'organizzazione. I *Tiers* devono supportare l'organizzazione nell'impostazione dei processi di gestione del rischio cyber e nel decidere quali unità dell'organizzazione hanno priorità maggiore nell'assegnazione di risorse aggiuntive. Perciò passare da un *Tier* inferiore a uno superiore è un processo che va svolto solo nel caso in cui, a seguito di un'analisi costi-benefici, il passaggio porta a una riduzione fattibile ed economicamente vantaggiosa del rischio cyber.

Nel dettaglio,la definizione dei quattro *Tiers* fornita dal NIST all'interno del Framework, seguendo un ordine crescente dal Tier più debole a quello più forte, è la seguente:

- **Tier 1 (Parziale)**: l'organizzazione nella gestione del rischio non tiene conto in maniera sistematica del rischio cyber e delle minacce circostanti. Spesso la gestione del rischio cyber è svolta in maniera reattiva con processi *ad hoc*

e i membri dell'organizzazione hanno una consapevolezza limitata del rischio. Inoltre, non sono definiti processi di condivisione delle informazioni inerenti alla cybersecurity all'interno e all'esterno dell'organizzazione.

- **Tier 2 (Informato)**: sono definiti processi interni all'organizzazione che tengono conto del rischio cyber anche se non estesi in tutte le sue articolazioni. Il livello di consapevolezza del rischio cyber è sufficiente all'interno dell'ente, però non è accompagnato da processi di gestione che coinvolgono tutti i livelli dell'organizzazione. Lo scambio di informazioni inerenti alla cybersecurity all'interno e all'esterno dell'ente è limitato e tipicamente passivo.

- **Tier 3 (Ripetibile)**: l'organizzazione aggiorna regolarmente le proprie pratiche di cybersecurity sulla base del risultato del processo di gestione del rischio. I processi di gestione del rischio cyber sono adottati a tutti i livelli dell'organizzazione e il personale ha la formazione adeguata per svolgere i ruoli che gli vengono assegnati nella gestione del rischio e risposta agli incidenti. Infine, l'ente scambia informazioni inerenti alla cybersecurity con tutti gli altri attori dello stesso settore in cui opera.

- **Tier 4 (Adattivo)**: le procedure di cybersecurity sono costantemente adattate utilizzando le lezioni apprese e gli indicatori di rischio, fornendo all'organizzazione la capacità di adeguarsi alle minacce in continua evoluzione e rispondere ad attacchi sofisticati. Lo scambio di informazioni inerenti alla cybersecurity con altri attori operanti nello stesso settore avviene in tempo reale.

Concludendo con la descrizione delle componenti del Framework, l'ultima componente chiave definita nel lavoro del NIST è la nozione di Profilo. Il Profilo rappresenta l'allineamento delle Funzioni, Categorie e Sottocategorie con i requisiti di business, la tolleranza al rischio e le risorse di un'organizzazione che utilizza il Framework[4]. Esso costituisce lo strumento che permette di descrivere lo stato attuale di implementazione di determinate attività inerenti alla cybersecurity nell'organizzazione, e/o lo stato desiderato dell'implementazione delle stesse attività. Infatti, esistono due tipi di Profili che un'organizzazione può definire nell'utilizzazione del Framework, cioè il Profilo Corrente e il Profilo Target. Il Profilo Corrente indica lo stato attuale delle attività per la gestione del rischio cyber e i risultati che essi raggiungono. Al contrario, il Profilo Target indica lo stato e i risultati desiderati delle attività di gestione del rischio cyber, e quali attività di gestione del rischio sarebbe desiderabile implementare. In generale, il Profilo è un ottimo strumento sia per esprimere la gestione del rischio cyber in maniera chiara all'interno e all'esterno dell'organizzazione, sia per l'autovalutazione delle stessa gestione internamente all'organizzazione.

La definizione di un Profilo viene svolta dall'organizzazione che utilizza il Framework, la quale deve analizzare tutte le Sottocategorie del Framework, in maniera

da selezionare solo quelle che si adattano al contesto in cui essa opera. Nel caso del Profilo Corrente sono selezionate tutte le Sottocategorie che sono già implementate dall'organizzazione, mentre nel caso del Profilo Target, oltre ad alcune Sottocategorie già implementate, si selezionano anche tutte quelle non implementate che però sono applicabili al settore in cui opera l'organizzazione. La definizione e il confronto dei due profili, Corrente e Target, permette all'organizzazione di valutare quali sono gli aspetti da migliorare nella gestione del rischio cyber, in maniera da poter affrontare meglio le minacce e gestire organicamente il rischio cyber. In sintesi, attraverso il confronto dei profili si possono rilevare delle differenze o gap da colmare, per cui va sviluppato un piano di azione, in maniera da implementare correttamente tutte le Categorie e Sottocategorie mancanti nello stato attuale e presenti in quello desiderato. Operando così, l'organizzazione è in grado di definire una "roadmap" con determinati obiettivi finalizzati alla riduzione del rischio cyber. Inoltre, i Profili sono strumenti molto flessibili, in quanto nel Framework non è imposto l'uso di template predefiniti e allo stesso tempo per un'organizzazione è possibile definire più Profili Correnti o Target, che fanno riferimento a precise componenti della stessa.

3.1.2 Il Framework Nazionale per la Cybersecurity e la Data Protection

La definizione del NIST Cybersecurity Framework ha stimolato una riflessione sullo stato delle infrastrutture critiche e sull'attitudine alla gestione del rischio cyber da parte delle organizzazioni anche in altri stati europei. Infatti, anche le organizzazioni e le piccole e medie imprese italiane hanno cominciato a capire che il problema delle minacce e degli attacchi cyber fosse un problema che le interessava e le interessa anche al giorno d'oggi. Tuttavia, non esisteva una metodologia adatta per guidare le organizzazioni e imprese italiane in un percorso di raggiungimento di un livello minimo di preparazione nella protezione delle informazioni e dei propri asset tecnologici. In quest'ottica nel 2015 è stata creata, da un team composto da personalità impiegate in ambito pubblico e privato, la prima versione del Framework Nazionale per la Cybersecurity[24], cioè uno strumento capace di guidare le imprese e organizzazioni italiane nello sviluppo o revisione delle attività di cybersecurity. Lo sviluppo di uno strumento come il Framework Nazionale di Cybersecurity porta vantaggi a tutte le imprese e organizzazioni italiane, indipendentemente dalla loro dimensione.

La maggioranza delle aziende italiane sono piccole e medie imprese e quasi nessuna di queste ha mai affrontato il problema della sicurezza informatica, in quanto nessuna di loro valuta correttamente il rischio cyber. Inoltre, l'implementazione di misure di sicurezza potrebbe richiedere costi minimi, così come costi elevati che le piccole e medie imprese italiane non sono in grado di sostenere da sole. Inoltre, le PMI italiane, non essendo in grado di individuare soluzioni economicamente vantaggiose e implementabili con il minimo sforzo, che potrebbero diminuire notevolmente il rischio

a cui sono esposte, stimano spesso in maniera errata il costo di messa in sicurezza dei loro dati e asset. Il problema dei costi e la mancanza di competenze per la valutazione del rischio cyber e del costo di messa in sicurezza degli asset spinge le piccole e medie imprese italiane ad accantonare il problema della sicurezza informatica, esponendole a grandi rischi. Con l'introduzione del Framework Nazionale si evita questo problema, in quanto esso individua un insieme di operazioni o controlli minimi di sicurezza, che permettono alle PMI italiane di raggiungere un livello di protezione sufficiente.

Inoltre, il Framework può essere di grande aiuto anche per le grandi imprese italiane che hanno sviluppato al loro interno pratiche, anche complesse, di gestione del rischio, incluso quello cyber. Infatti, come il Framework del NIST, anche il Framework Nazionale è uno strumento che non mira a rimpiazzare pratiche di gestione del rischio cyber già esistenti, ma che può contribuire a un processo di miglioramento e adeguamento di pratiche esistenti all'interno delle organizzazioni. Quindi, le grandi imprese possono utilizzare il Framework Nazionale come una metodologia finalizzata al miglioramento dei processi di gestione del rischio. In più, il Framework Nazionale di Cybersecurity, essendo basato sul Framework del NIST, conserva delle caratteristiche di internazionalità e fa riferimento a standard, pratiche e linee guida globali. L'internazionalità del Framework Nazionale è un grande vantaggio per le grandi imprese, le quali possono utilizzarlo per richiedere determinati livelli di sicurezza a tutti i fornitori che fanno parte della loro supply chain, rendendo più sicuro l'intero ecosistema dell'impresa e minimizzando la superficie di attacco.

Lo sviluppo del Framework nazionale di Cybersecurity, come accennato anche in precedenza, è stato condotto a partire dal NIST Cybersecurity Framework. In sostanza, gli autori hanno analizzato il Cybersecurity Framework sviluppato dall'ente americano e lo hanno integrato con degli elementi aggiuntivi, necessari a rendere il Framework Nazionale facilmente utilizzabile dalle PMI e dalle organizzazioni italiane. Nel 2015 è stata pubblicata la prima versione del Framework, che successivamente è stato aggiornato a seguito di alcuni importanti avvenimenti. Il primo coincide con l'entrata in vigore, nel 2016, del General Data Protection Regulatory (GDPR) che ha stabilito nuovi standard e regole sulla protezione dei dati. Il secondo è avvenuto nel 2018, quando il NIST ha pubblicato la versione 1.1 del Cybersecurity Framework, includendo nuovi elementi per tenere in considerazione alcune problematiche di sicurezza delle supply chain e approfondire la sicurezza dei processi di autenticazione e gestione delle identità. Questi due importanti cambiamenti hanno portato a una revisione del Framework Nazionale per il rilascio della versione 2, attualmente la più aggiornata, in cui oltre ai cambiamenti proposti dal NIST si sono incorporati alcuni elementi sulla data protection. Il risultato è stata la pubblicazione nel 2019 del nuovo Framework Nazionale per la Cybersecurity e la Data Protection[5].

Scendendo nel dettaglio della struttura il Framework Nazionale per la Cybersecurity e la Data Protection ricalca l'organizzazione del Framework del NIST, includendo

come elementi fondamentali le tre componenti del Cybersecurity Framework, descritte nel paragrafo 3.1.1. Infatti, la componente Core ingloba tutte le Funzioni, le Categorie e le Sottocategorie definite nel Framework del NIST, vengono definiti gli stessi *Implementation Tier* ed è introdotta anche la nozione di Profilo. Tuttavia, come prima differenza rispetto al prodotto NIST, si evidenzia che nella componente Core del Framework Nazionale sono state aggiunte nuove Categorie e Sottocategorie riguardanti la protezione dei dati personali. Infatti, con l'entrata in vigore del GDPR, l'Unione Europea ha prescritto il rispetto di alcune pratiche e linee guida per la protezione dei dati personali, che non sono colte però dalle Sottocategorie esistenti nel Framework del NIST. Per questo, gli autori del Framework Nazionale per la Cybersecurity e la Data Protection hanno esteso il Framework originale con delle nuove Categorie e Sottocategorie identificate con il prefisso "DP-", e descritte nella Tabella 3.2.

Gli elementi di novità introdotti dal Framework Italiano non si esauriscono, però, con l'aggiunta di nuove Categorie e Sottocategorie alla componente Core, ma comprendono anche una serie di strumenti e metodologie pensate appositamente per un contesto economico ricco di piccole e medie imprese. Infatti, la più grande differenza tra il Framework del NIST e il Framework Nazionale è che il primo è pensato per le infrastrutture critiche e non per le organizzazioni in generale. Questo comporta che non ci sono livelli intermedi nell'implementazione delle Categorie e delle Sottocategorie del NIST, ovvero non si ammette che una certa Sottocategoria sia implementata in maniera "parziale". Perciò, anche se sono stati definiti in maniera parziale e non automatizzata dei processi che contribuiscono all'implementazione della Sottocategoria in esame, comunque essa nella valutazione delle differenze tra Profilo Corrente e Profilo Target sarà marcata come ancora da implementare. Allo stesso modo, trattando la sicurezza delle infrastrutture critiche, il Cybersecurity Framework non prioritizza una Sottocategoria rispetto all'altra, in quanto tutte quante le Sottocategorie selezionate in un Profilo sono importanti alla stessa maniera per raggiungere i risultati desiderati in termini di sicurezza.

Tutto questo impianto si applica perfettamente al contesto delle infrastrutture critiche, in cui sono necessari livelli di sicurezza elevati, però non è facilmente applicabile allo scenario italiano. Infatti, il panorama italiano è costellato di tantissime piccole e medie imprese che non hanno le risorse economiche e le competenze adatte a realizzare grandi cambiamenti nella gestione del rischio cyber, in breve tempo. Quindi, utilizzare direttamente il Framework del NIST non ha molto senso per le piccole e medie imprese italiane, in quanto il rapporto tra il costo della riduzione del rischio ottenuto implementando il Framework e il beneficio derivante dalla riduzione non è vantaggioso. Allora, per estendere il bacino di utenza del Framework, includendo anche le PMI italiane, gli autori hanno introdotto due nuovi elementi, rispetto al Framework del NIST, che permettono di misurare quanto è urgente implementare

FUNCTION	CATEGORY	SUBCATEGORY
IDENTIFY (ID)	**Asset Management (ID.AM)**: I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**DP-ID.AM-7**: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori,clienti, partner)
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente all'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**DP-ID.RA-7**: Viene effettuata una valutazione di impatto sulla protezione dei dati personali
	Data Management (DP-ID.DM): i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.	**DP-ID.DM-1**: Il ciclo di vita dei dati è definito e documentato
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale
RESPOND (RS)	**Communications (RS.CO)**: Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**DP-RS.CO-6**: Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati

Tabella 3.2: Nuove Categorie e Sottocategorie aggiunte al Framework Nazionale per la Cybersecurity e la Data Protection[5]

una sottocategoria e se questa è implementabile in maniera parziale.

Il primo elemento, che si aggiunge all'impianto della parte Core definita nel Framework del NIST, sono i **livelli di priorità**. Questi rappresentano uno strumento che permette a chi utilizza il Framework di stabilire quali tra le Sottocategorie incluse nel Profilo Target vanno implementate prima di altre, perchè comportano una riduzione del rischio maggiore per l'organizzazione. Attraverso i livelli di priorità, l'organizzazione che implementa il Framework riesce a individuare gli interventi da svolgere immediatamente e inderogabilmente sulle attività legate alla cybersecurity e a gestire meglio il rischio cyber al suo interno. L'assegnazione di un livello di priorità a una data Sottocategoria è un compito svolto dall'organizzazione, sulla base di due criteri fondamentali, ovvero la capacità di ridurre il rischio cyber e la semplicità di implementazione, al livello tecnologico e organizzativo, della Sottocategoria. In particolare, la riduzione del rischio che si ottiene dall'implementazione di una Sottocategoria del Framework si misura stabilendo quanto sono ridotti i tre fattori che concorrono alla determinazione del rischio cyber, ovvero esposizione alla minaccia, probabilità di accadimento e impatto derivante dall'accadimento.

Genericamente nel Framework sono previsti tre diversi livelli di priorità:

- **ALTA**: tale priorità viene assegnata a tutti gli interventi e Sottocategorie, la cui implementazione provoca una importante riduzione di tutti e tre i fattori che concorrono alla determinazione del rischio cyber. In questo caso la Sottocategoria va implementata indipendente dalla sua complessità realizzativa.
- **MEDIA**: il livello caratterizza tutte le Sottocategorie che riducono uno o più fattori che concorrono al calcolo del valore associato al rischio cyber e sono semplici da implementare per un'organizzazione.
- **BASSA**: rientrano in questo livello della scala tutte le Sottocategorie la cui implementazione riduce uno o più fattori chiave del rischio cyber e la complessità realizzativa è molto alta per l'organizzazione.

Tuttavia, la priorità legata a una determinata "subcategory" dipende dalla contestualizzazione adottata nell'uso del Framework e dal contesto specifico dell'organizzazione che lo usa. Per questo motivo, per rendere il Framework uno strumento flessibile e adattabile a tutti i contesti delle organizzazioni che lo utilizzano, viene concessa la possibilità di ridefinire i livelli di priorità esposti prima, per poi assegnarli alle Sottocategorie incluse nel Profilo Target.

Il secondo elemento aggiunto alla struttura del Cybersecurity Framework del NIST sono i **livelli di maturità**, che forniscono una misura della maturità di un processo di sicurezza o dell'attuazione di una tecnologia specifica, oppure una misura delle quantità di risorse adeguate utilizzate nell'implementazione di una Sottocategoria[5]. In sostanza, i livelli di maturità consentono all'organizzazione di misurare quanto è

correttamente implementata una determinata Sottocategoria all'interno di un profilo, facilitando anche il confronto tra Profilo Corrente e Profilo Target. A differenza dei livelli di priorità, non esiste una definizione predefinita dei livelli di maturità, la quale è un compito affidato all'organizzazione o ente che utilizza il Framework. Nella definizione di una scala con i livelli di maturità, l'organizzazione associa ad ogni livello di maturità dei controlli di sicurezza specifici. Maggiore è il livello di maturità e maggiori saranno le pratiche e controlli di sicurezza associati al livello, in quanto ogni livello di maturità deve prevedere controlli incrementali rispetto a quelli inferiori. Per una data Sottocategoria, si può stabilire che viene raggiunto un certo livello di maturità se e solo l'organizzazione implementa tutti i controlli di sicurezza associati al livello di maturità.

3.2 Schemi per la qualificazione dei servizi Cloud

3.2.1 Regolamento AgID per la qualificazione dei servizi Cloud

Con la definizione del Framework Nazionale per la Cybersecurity e la Data Protection è stata aumentata la consapevolezza delle imprese e degli enti pubblici relativamente alla Cybersecurity. Certamente il Framework è un valido strumento per aiutare le piccole e medie imprese italiane nella definizione e miglioramento di processi aziendali per la gestione del rischio cyber, grazie alla sua flessibilità e a tutti gli strumenti e le metodologie che offre. Tuttavia, il Framework Nazionale, oltre che uno strumento di aiuto per le imprese, risulta essere anche uno strumento utile per i regolatori e chi si occupa della definizione di standard e regolamenti. Infatti, utilizzando il Framework come base per la definizione di norme e regolamenti è possibile, non solo agevolare il processo di scrittura dei regolamenti, ma facilitarne l'evoluzione con il tempo, in quanto il Framework evolve parallelamente all'evoluzione delle minacce cyber. Sulla base di queste considerazioni, l'Agenzia per l'Italia Digitale (AgID) ha deciso di utilizzare il Framework Nazionale per la Cybersecurity per la definizione del "Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per le PA e le caratteristiche di qualità, sicurezza, performance e scalabilità e portabilità dei servizi Cloud per la Pubblica Amministrazione, nonché le modalità di qualificazione dei servizi Cloud per la Pubblica Amministazione"[6]. Il regolamento è stato pubblicato il 15 dicembre del 2021 e adottato con la determinazione n. 628/2021.

Il Regolamento AgID è stato il primo provvedimento ufficiale di un ente governativo italiano che ha trattato in maniera approfondita la sicurezza e altri aspetti a cui devono aderire le infrastrutture digitali e le tecnologie Cloud per la Pubblica Amministrazione. In più, il Regolamento prescrive anche le modalità di migrazione delle Amministrazioni verso il Cloud e le modalità di qualificazione delle infrastrutture e servizi Cloud per le

PA. La struttura del Regolamento è molto semplice e lineare. Esso è diviso in cinque capi e quattordici articoli, che trattano nel dettaglio alcuni aspetti fondamentali relativamente all'adozione delle tecnologie Cloud in Italia, escluso il primo Capo che contiene solo le Disposizioni Generali e lo scopo del regolamento.

Di seguito viene riportata una descrizione di alto livello di ognuno dei capi del regolamento successivi al primo:

- **Capo II**: esso impone alle Amministrazioni, indipendentemente dalla loro dimensione, di predisporre un elenco in cui sono caratterizzati e classificati i loro dati e servizi. Poi, si stabilisce che l'ACN deve pubblicare un modello per la predisposizione e l'aggiornamento dell'elenco dei dati e servizi delle Amministrazioni. Infine, sono definite tutte le modalità con cui questo elenco viene trasmesso dall'Amministrazione all'ACN e i termini entro cui ACN deve convalidare, con o senza riserve, o non convalidare la conformità dell'elenco stesso.

- **Capo III**: definisce i criteri da seguire nel processo di definizione dei livelli minimi delle infrastrutture digitali e delle caratteristiche dei servizi Cloud per la Pubblica Amministrazione, quali sono i livelli minimi che devono rispettare le infrastrutture e le caratteristiche che devono avere i servizi Cloud. Inoltre, stabilisce anche i termini entro cui ACN deve aggiornare tali livelli minimi e caratteristiche e quelli entro cui le Amministrazioni si devono adeguare.

- **Capo IV**: in esso si norma come deve avvenire la migrazione delle Pubbliche Amministrazioni verso infrastrutture digitali o servizi Cloud. Si rimarca, inoltre, che è compito dell'Amministrazione definire il piano di migrazione verso il servizio Cloud e trasmetterlo all'AgID e al Dipartimento per la Trasformazione Digitale. Quest'ultimo ha anche il compito di convalidare, eventualmente con prescrizioni, o non convalidare il piano di migrazione.

- **Capo V**: esso stabilisce che è compito dell'ACN definire i criteri per la qualificazione dei servizi Cloud per le PA, specificando come questi vanno definiti, dove vanno resi disponibili e per quali livelli di qualificazione. Inoltre, sono regolate anche le modalità in cui va redatta e trasmessa all'ACN la domanda per la qualificazione di un servizio Cloud e come avviene il processo di qualificazione.

Il Regolamento AgID rappresenta un riferimento molto importante non solo per le Amministrazioni, ma anche per l'Agenzia per la Cybersicurezza Nazionale, in quanto fornisce ad essa indicazioni precise riguardo le funzioni che essa avrà nel processo di migrazione al Cloud svolto dalle Amministrazioni. Sicuramente, anche se le parti inerenti al processo di Qualificazione dei servizi Cloud e alla migrazione verso il Cloud sono comunque fondamentali, l'aspetto più importante trattato dal

regolamento riguarda i livelli minimi delle infrastrutture digitali e le caratteristiche dei servizi Cloud per le PA. Nel Capo III, infatti, si fa riferimento a due allegati al regolamento, ovvero l'**Allegato A** e l'**Allegato B**. In particolare, il primo esprime i livelli minimi di sicurezza e affidabilità, di capacità elaborativa e di risparmio energetico **delle infrastrutture** digitali, e il secondo contiene le caratteristiche di qualità, sicurezza, performance e scalabilità e interoperabilità **dei servizi** Cloud per le PA. La divisione tra infrastrutture e servizi Cloud è fondamentale, non solo per una migliore definizione dei requisiti minimi, ma anche per una facilitazione del processo di qualificazione. Infatti, se un certo servizio Cloud viene erogato attraverso un'infrastruttura non qualificata, si rifiuta subito la domanda di qualificazione, in quanto se l'infrastruttura sottostante non è sicura il servizio Cloud non può essere qualificato.

Entrambi gli allegati hanno una struttura molto semplice, in quanto essi sono strutturati come una tabella che elenca una serie di "requisiti" a cui devono aderire le infrastrutture e i servizi Cloud che utilizzano le Pubbliche Amministrazioni. Ogni requisito elencato negli allegati è caratterizzato da un codice progressivo, un nome del requisito e una specifica del requisito, ovvero una descrizione sintetica di cosa riguarda il requisito. A titolo esemplificativo, la Tabella 3.3 presenta un estratto dell'allegato A del regolamento. L'impostazione degli allegati ricalca molto la divisione in Sottocategorie propria del Framework Nazionale per la Cybersecurity, in quanto i requisiti hanno lo stesso livello di dettaglio e granularità tipico delle Sottocategorie. Infatti, in tutti e due gli allegati, i requisiti di sicurezza sono in realtà un insieme di Sottocategorie estratte dal Framework Nazionale, considerate adeguate per esprimere i livelli di sicurezza delle infrastrutture e le caratteristiche di sicurezza dei Servizi Cloud per la Pubblica Amministrazione. Quanto appena affermato, trova riscontro nel modo in cui sono strutturati i codici progressivi dei requisiti inerenti alla sicurezza sia nell'allegato A che nell'allegato B. Ad esempio, facendo riferimento alla Tabella 3.3, si noti che il primo requisito della tabella è identificato dal codice progressivo `IN-SA-ID.AM-1-01`. Tolte le prime due lettere del codice, che fanno riferimento al fatto che il requisito è legato ai livelli minimi delle infrastrutture, e le seconde due lettere, che indicano che il requisito riguarda la sicurezza, il resto del codice coincide con quello della Sottocategoria uno della Categoria Asset Management della Funzione Identify del Framework Nazionale. Allo stesso modo, la specifica del requisito richiede che sia implementata l'omonima Sottocategoria del Framework Nazionale, confermando che quest'ultimo ha rivestito un ruolo importante nella definizione di schemi di qualificazione per le infrastrutture digitali e i servizi Cloud.

Utilizzare il Framework Nazionale di Cybersecurity ha permesso uno sviluppo più veloce dei livelli minimi di sicurezza delle infrastrutture digitali e delle caratteristiche di sicurezza dei servizi Cloud, in quanto è stato sufficiente riadattare alcune Sottocategorie del Framework. Allo stesso tempo, basare gli schemi di qualificazione

su uno strumento come il Framework Nazionale permette di adattare i requisiti e gli schemi stessi all'evoluzione delle minacce e delle tecnologie. Chiaramente per quanto riguarda le altre tipologie di requisiti è stato necessario utilizzare come base altri riferimenti, standard e linee guida. Ad esempio, per la definizione dei livelli minimi di capacità elaborativa e di risparmio energetico delle infrastrutture digitali e delle caratteristiche di qualità dei servizi Cloud per le PA si è fatto riferimento alle linee guida ISO e alle normative europee. Al contrario, per la definizione di ulteriori requisiti di sicurezza riguardanti i data center, che ospitano le infrastrutture digitali, e le caratteristiche di portabilità e di performance e scalabilità dei servizi Cloud si è fatto riferimento ai corrispondenti standard di settore. Tutti questi contributi hanno portato alla realizzazione di uno schema di requisiti per la qualificazione delle infrastrutture digitali e dei servizi Cloud per la Pubblica Amministrazione che sia

CODICE PROGRESSIVO (ID REQUISITO)	**NOME**	**SPECIFICA REQUISITO**
IN-SA-ID.AM-1-01	**Censimento apparati fisici**	L'Amministrazione implementa la sotto-categoria ID.AM-1 del FCNS.
IN-SA-ID.AM-2-01	**Censimento piattaforme e applicazioni software**	L'Amministrazione implementa la sotto-categoria ID.AM-2 del FCNS.
IN-SA-ID.AM-3-01	**Censimento dei flussi di dati e delle comunicazioni**	L'Amministrazione implementa la sotto-categoria ID.AM-3 del FCNS.
IN-SA-ID.AM-6-01	**Ruoli e responsabilità inerenti alla cybersecurity**	L'Amministrazione implementa la sotto-categoria ID.AM-6 del FCNS.
IN-SA-ID.GV-1-01	**Policy di cybersecurity**	L'Amministrazione deve aver formalmente adottato procedure per la gestione della sicurezza IT, ad esempio ISO 27002 oppure essere certificate ISO 27001.
IN-SA-ID.RA-1-01	**Identificazione delle vulnerabilità**	L'Amministrazione implementa la sotto-categoria ID.RA-1 del FCNS.
IN-SA-ID.RA-5-01	**Valutazione del rischio**	L'Amministrazione implementa la sotto-categoria ID.RA-5 del FCNS.
IN-SA-PR.AC-1-01	**Identity Management**	L'Amministrazione implementa la sotto-categoria PR.AC-1 del FCNS.

Tabella 3.3: Estratto Allegato A del Regolamento AgID per il Cloud[6]

scalabile, comprensibile e facilmente utilizzabile.

3.2.2 I provvedimenti dell'Agenzia per la Cybersicurezza Nazionale

Il Regolamento redatto dall'AgID, oltre a definire un primo schema di requisiti per la qualificazione dei servizi Cloud, affida all'Agenzia Nazionale per la Cybersicurezza alcuni compiti fondamentali per la definizione di un impianto di qualificazione per le infrastrutture digitali e i servizi Cloud per la Pubblica Amministrazione. Per questo, l'ACN ha emanato una serie di provvedimenti atti a soddisfare quanto richiesto dal Regolamento AgID, ovvero le determine n. 306 e n. 307 emanate entrambe il 18 gennaio 2022. Nella determina n. 306[25] viene definito il modello per la predisposizione dell'elenco e della classificazione dei dati e dei servizi della Pubblica Amministrazione, che si basa sulla compilazione di un questionario elaborato dall'ACN, in maniera da facilitare il lavoro delle Amministrazioni. Inoltre, per rendere ancora più semplice la preparazione dell'elenco citato nel Regolamento, l'Agenzia ha creato anche degli elenchi predefiniti, con la relativa classificazione, utilizzabili da Amministrazioni simili per tipologia e dimensioni. Nel caso in cui le Amministrazioni si avvalgano di questi elenchi predefiniti e li trasmettano all'ACN secondo le modalità indicate nel Regolamento, questi sono automaticamente convalidati dall'Agenzia. In aggiunta, è concesso alle PA la possibilità di aggiornare gli elenchi eliminando dati o servizi che non sono trattati, oppure ampliandoli con dati e servizi non inclusi che però sono trattati dall'Amministrazione, e allo stesso tempo di rifiutare gli elenchi stessi. La trasmissione, anche nel caso di aggiornamento o rifiuto avviene secondo le stesse modalità di accettazione dell'elenco, solo che nel caso di rifiuto si deve trasmettere anche la documentazione a supporto del rifiuto stesso.

Tuttavia, il provvedimento di maggiore importanza per la definizione di uno schema di qualificazione per le infrastrutture digitali e i servizi Cloud è la determina n. 307[9] di ACN, in cui i livelli minimi e le caratteristiche rispettivamente dell'allegato A e dell'allegato B del Regolamento sono aggiornati. Oltre ad aggiornare i livelli minimi delle infrastrutture digitali e le caratteristiche dei servizi Cloud, nella determina si indica puntualmente quali infrastrutture e quali servizi Cloud possono ospitare i dati e servizi della Pubblica Amministrazione a seconda che questi siano classificati come ordinari o critici o strategici. Inoltre, il provvedimento introduce il concetto di livelli di qualificazione dei servizi Cloud e delle infrastrutture digitali, introducendo quattro livelli di qualificazione crescenti sia per i servizi Cloud che per le infrastrutture digitali. La Tabella 3.1 riporta la lista dei livelli di qualificazione definiti per servizi e infrastrutture, dal più basso al più alto. L'introduzione dei livelli di qualificazione sia per le infrastrutture che per i servizi permette di esprimere un aspetto importante del processo di qualificazione di un servizio Cloud, ovvero quello di **Catena di qualificazione dei servizi Cloud**. Il principio della Catena di qualificazione dei

Livelli di qualificazione dei servizi	Livelli di qualificazione delle infrastrutture
qualificazione Cloud di livello 1 (QC1)	qualificazione infrastruttura di livello 1 (QI1)
qualificazione Cloud di livello 2 (QC2)	qualificazione infrastruttura di livello 2 (QI2)
qualificazione Cloud di livello 3 (QC3)	qualificazione infrastruttura di livello 3 (QI3)
qualificazione Cloud di livello 4 (QC4)	qualificazione infrastruttura di livello 4 (QI4)

Tabella 3.4: Livelli di qualificazione per servizi Cloud e infrastrutture digitali

servizi Cloud stabilisce che un servizio Cloud erogato secondo un certo modello di servizio (IaaS, PaaS o SaaS) può ottenere un certo livello di qualificazione solo se il servizio o infrastruttura sottostante è qualificato a un livello uguale o superiore. Ad esempio, un servizio PaaS può ottenere un certo livello di qualificazione se e solo se viene erogato attraverso un servizio IaaS qualificato al medesimo livello o superiore, oppure se viene erogato mediante un'infrastruttura digitale qualificata al medesimo livello o superiore.

Tutti i concetti appena accennati sono inseriti nell'Allegato 1 alla determina n. 307 di ACN, la quale però contiene altri tre allegati fondamentali, in cui non solo vengono estesi e aggiornati i livelli minimi delle infrastrutture e le caratteristiche dei servizi Cloud, ma sono definiti anche i requisiti di qualificazione per i servizi Cloud e le infrastrutture digitali per la Pubblica Amministrazione. I primi due allegati sono **l'Allegato A2** e **l'Allegato B2**, i quali definiscono rispettivamente gli ulteriori livelli minimi di sicurezza, capacità elaborativa e risparmio energetico per le infrastrutture digitali e le ulteriori caratteristiche di sicurezza, qualità, performance e scalabilità ed interoperabilità dei servizi Cloud per la Pubblica Amministrazione. Gli allegati A2 e B2 integrano, rispettivamente, gli allegati A e B rel Regolamento AgID. La struttura dei due allegati è molto simile, in quanto le misure sono divise inizialmente a seconda della classe di dati e servizi a cui si riferiscono, ovvero ordinari, critici e strategici. Successivamente ogni sezione che fa riferimento a una certa classe di dati e servizi divide le misure in ulteriori sezioni a seconda dell'aspetto che esse trattano, ovvero qualità, performance e scalabilità, sicurezza, risparmio energetico e così via. Infine, ogni sottosezione riferita a un aspetto particolare trattato dalle misure, è organizzata seguendo lo schema di Categorie e Sottocategorie del Framework, riportando per ogni "Sottocategoria" una breve descrizione.

Tuttavia, il livello di granularità che raggiungono l'allegato A2 per le infrastrutture e l'allegato B2 per i servizi Cloud è più alto rispetto a quello del Framework Nazionale per la Cybersecurity e la Data Protection. Il contesto delle infrastrutture digitali

e dei servizi Cloud è molto più complesso di quello di una singola organizzazione, e per questo l'ACN ha ritenuto opportuno definire, per ogni "Sottocategoria" degli allegati, dei **controlli di sicurezza**. Questi ultimi rappresentano un livello di dettaglio superiore rispetto ai Riferimenti Informativi del Framework Nazionale, perché rappresentano delle prescrizioni esatte e tecnologicamente dettagliate, a cui deve aderire l'infrastruttura digitale o il servizio Cloud oggetto di qualificazione. Lo scopo dei controlli di sicurezza è quello di aiutare il regolatore nel processo di qualificazione delle infrastrutture digitali e dei servizi Cloud, per stabilire se le Sottocategorie sono implementate correttamente e quale livello di qualificazione concedere. Allo stesso tempo, i controlli di sicurezza possono essere anche utili per chi gestisce o possiede infrastrutture digitali o servizi Cloud e vuole ottenere un certo livello di qualificazione per ospitare dati e servizi delle Amministrazioni italiane. In aggiunta, la maggiore granularità raggiunta con la definizione di controlli di sicurezza puntuali per ogni Sottocategoria, permette anche di esprimere le misure di sicurezza da soddisfare per una certa classe di dati e servizi in maniera incrementale rispetto alla classe inferiore. Infatti, in entrambi gli allegati, nella sezione dedicata alle misure di sicurezza da applicare per dati e servizi critici, sono riportati solo Sottocategorie e controlli di sicurezza aggiuntivi rispetto a quelli già presenti per dati e servizi ordinari. La stessa cosa, si verifica anche nel passaggio dalla sezione dedicata ai dati e servizi critici, a quella dedicata a dati e servizi strategici.

Perciò, rispetto agli allegati A e B del regolamento AgID, gli allegati A2 e B2 della determinazione n.307 di ACN introducono non solo delle misure di sicurezza aggiuntive, ma anche una struttura e una schematizzazione diversa che tiene conto della tipologia di dati e servizi trattati. In più, gli allegati alla determina aggiungono per ogni Sottocategoria dei controlli di sicurezza per verificarne la corretta implementazione, a differenza del regolamento che si riferisce ai Riferimenti Informativi del Framework Nazionale. Quindi, con questo nuovo provvedimento si stabilisce che gli allegati A e B del regolamento rappresentano delle misure minime da implementare o per un'infrastruttura digitale o per un servizio Cloud. Al contrario, gli allegati A2 e B2 della determina n. 307 rappresentano le misure di sicurezza che un'infrastruttura digitale o un servizio Cloud deve rispettare per ottenere la qualificazione. Però, il rispetto delle misure aggiuntive dell'allegato A2 per le infrastrutture e dell'allegato B2 per i servizi Cloud è condizione necessaria, ma non sufficiente per ottenere la qualificazione. Infatti, al fine di poter ospitare dati e servizi delle pubbliche amministrazioni le infrastrutture digitali e i servizi Cloud devono soddisfare anche degli ulteriori requisiti inclusi nel terzo e ultimo allegato alla determina n. 307, cioè **l'allegato C**.

L'allegato C alla determina n. 307 contiene l'elenco dei requisiti che devono soddisfare i servizi Cloud per la Pubblica Amministrazione e i requisiti a cui devono aderire le infrastrutture digitali che ospitano servizi Cloud per le PA, per ognuno

dei quattro livelli di qualificazione. Per ogni livello di qualificazione Cloud o livello di qualificazione infrastruttura, l'allegato riporta i requisiti a cui deve aderire e le certificazioni da possedere affinché il servizio Cloud o l'infrastruttura digitale possa ottenere la qualificazione a quel livello. Ovviamente l'allegato C, sia per i servizi Cloud, sia per le infrastrutture, nell'elencare i requisiti necessari per ottenere la qualificazione a un certo livello, fa riferimento alle misure di sicurezza degli allegati A2 e B2 della determina. Tuttavia, per i livelli di qualificazione Cloud e qualificazione infrastruttura più alti, rispettivamente QC4 e QI4, l'allegato introduce ulteriori Sottocategorie e controlli di sicurezza, certificando il fatto che i requisiti espressi negli allegati A2 e B2 sono necessari ma non sufficienti per ottenere la qualificazione.

In conclusione, l'impianto definito con i tre allegati alla determina n. 307 costituisce un valido sistema di misure di sicurezza e requisiti utilizzabili nel processo di qualificazione dei servizi Cloud. Tuttavia, l'aver definito solo dei requisiti, anche se aiuta l'ente regolatore nell'erogazione della qualificazione Cloud a un determinato servizio Cloud, non stabilisce una modalità con cui verificare se un certo servizio Cloud implementa un determinato controllo di sicurezza. Questo può portare a delle verifiche dell'implementazione di un certo controllo non sempre valide, perché persone diverse potrebbero avere metodi di verifica diversi per lo stesso controllo, potendo produrre anche un risultato diverso per l'esito della verifica. Si rende necessaria, quindi, l'individuazione di metodologie di verifica adatte per stabilire la corretta implementazione dei controlli di sicurezza degli allegati.

Capitolo 4

Metodologie di verifica e risultati dell'ispezione

4.1 I controlli di sicurezza dell'allegato B2

Lo sviluppo di metodologie per valutare l'assolvimento ai controlli degli allegati alla determina n. 307 di ACN è un lavoro fondamentale che ha lo scopo di facilitare il compito del regolatore nell'attribuzione di una qualifica a una determinata infrastruttura digitale o servizio Cloud. Chiaramente, i livelli minimi e le caratteristiche richieste, rispettivamente, alle infrastrutture digitali e ai servizi Cloud, che devono ospitare dati e servizi delle Pubbliche Amministrazioni, sono molteplici. All'incirca sia l'allegato A2 che l'allegato B2 elencano in totale sessanta Sottocategorie ciascuno, per ognuna delle quali, in media, sono definiti cinque controlli di sicurezza. L'ambito di analisi della tesi si concentra sui servizi Cloud e mira, pertanto, a definire metodologie di valutazione dell'attuazione delle misure incluse nelle Sottocategorie dell'allegato B2 della determina 307 di ACN.

Il processo di sviluppo delle metodologie non può prescindere però dalla comprensione dei controlli di sicurezza e dalla loro catalogazione in maniera da fornire, oltre al prodotto finale, anche delle indicazioni su come svolgere il processo di sviluppo, utilizzabili per gli altri allegati. Innanzitutto, è importante sottolineare che alcune misure della determina n. 307 sono state emendate con un provvedimento successivo di ACN, la determinazione n. 20610 del 28 luglio 2023, che ha corretto e aggiornato alcuni controlli in alcune Sottocategorie. Attualmente, la forma testuale dell'allegato B2 risulta difficile da utilizzare per lo sviluppo delle metodologie, perché i controlli sono divisi per livello di dati o servizi. Allora, per facilitare il processo di sviluppo delle metodologie richieste, è stato necessario riportare tutti i controlli espressi in maniera testuale, in una forma tabellare più comprensibile e visibile nella Tabella 4.1. Essa richiama la struttura del Framework Nazionale e permette di analizzare i controlli di una Sottocategoria alla volta.

I controlli di sicurezza sviluppati dall'Agenzia Nazionale costituiscono in parte un adattamento, al contesto dei servizi Cloud, dei Riferimenti Informativi del Framework

FCNS - Categoria	ID	FCNS - Sottocategoria	ACN Requisiti - Allegato B2 alla Determinazione ACN n. 307/2022 e ss.mm.ii	LIV
Sicurezza				
ASSET MANAGEMENT ID.AM: I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione	ID.AM-1	Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	1. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto	ORD
			2. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati	ORD
	ID.AM-2	Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	1. Tutte le piattaforme e le applicazioni software installate sono censite ed esiste un elenco di quelle approvate da attori interni al soggetto	ORD
			2. L'installazione delle piattaforme e delle applicazioni software è consentito esclusivamente per quelle approvate	ORD
			3. Esistono politiche che limitino l'aggiunta, rimozione o aggiornamento, nonché la gestione non autorizzata degli asset dell'organizzazione	ORD
	ID.AM-3	I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati	1.Tutti i flussi informativi, inclusi quelli verso l'esterno e relativi al servizio cloud, sono identificati e approvati da attori interni al soggetto	ORD

Tabella 4.1: Estratto della nuova forma dell'allegato B2 alla determina n. 307 di ACN

Nazionale, e in parte sono basati su sezioni di standard e linee guida riguardanti una corretta implementazione dei servizi Cloud. Ogni controllo inquadra un aspetto puntuale e specifico della Sottocategoria a cui si riferisce. Apparentemente, lo sviluppo di metodologie che consentono di stabilire la corretta implementazione di ogni controllo di sicurezza potrebbe sembrare un'opera molto difficile e lunga, e potrebbe non essere così vantaggiosa nel caso in cui i controlli subiscano dei cambiamenti, a causa dell'evoluzione delle minacce e delle tecnologie. Tuttavia, la corretta implementazione di un controllo afferente a una Sottocategoria può essere stabilita utilizzando la metodologia sviluppata per un altro controllo, associato a una Sottocategoria diversa. Infatti, con questo lavoro, si propone anche una suddivisione in tipologie dei controlli di sicurezza sviluppati dall'ACN, la quale ha permesso di elaborare un insieme di metodologie adeguate in un tempo relativamente ristretto. In particolare, i controlli sono stati divisi in più categorie, tenendo conto delle prescrizioni che ognuno di essi impone al fornitore di servizi Cloud:

- **DOC - Controlli che richiedono l'esistenza di documentazione** (e.g. documenti ufficiali, elenchi, verbali, piani ecc...): richiedono che il soggetto produca e metta a disposizione del regolatore uno o più documenti, elenchi, piani e così via.

- **POLICY - Controlli che richiedono la definizione o adozione di policies e/o l'implementazione di processi, procedure e meccanismi**: impongono al soggetto la definizione di politiche di sicurezza e l'implementazione delle procedure, processi e meccanismi per il rispetto delle policies.

- **ACTION - Controlli che richiedono lo svolgimento di azioni periodicamente**: richiedono che il soggetto svolga periodicamente una certa azione o collaudo.

- **TECH - Controlli che richiedono l'implementazione di tecnologie o l'adozione di sistemi afferenti all'ambito della Sottocategoria**: sono imposizioni molto specifiche, che riguardano tecnologie ben precise o altri aspetti collegati all'ambito trattato dalla Sottocategoria.

Purtroppo, la suddivisione individuata non riesce a incasellare tutti i controlli dell'allegato B2. Innanzitutto alcuni controlli di sicurezza sono di tipologia "ibrida", ovvero possono trattare aspetti comuni a più tipologie di controlli. Quindi, per la creazione delle metodologie relative a questi controlli "ibridi", si sono seguite tutte le indicazioni applicabili, tra quelle elaborate, anche se fanno riferimento a tipologie di controlli diversi. Poi, alcuni controlli di sicurezza sono molto particolari e costituiscono un'eccezione rispetto alle categorie individuate in precedenza, e per questo è stata sviluppata per loro una metodologia ad hoc e specializzata. Inoltre,

alcuni controlli di sicurezza che si riferiscono a dati di livello superiore possono imporre ulteriori restrizioni su degli aspetti già menzionati in altri controlli di livello inferiore. Uno scenario ricorrente, ad esempio, consiste nel fatto che per dati e servizi di livello ordinario esiste un controllo che richiede solo che siano definite delle policies riguardanti un certo aspetto, mentre per dati e servizi di livello critico o strategico ne esiste un altro richiede che le stesse policies siano raccolte in un documento ufficiale. In casi come quello appena descritto, allora, è sufficiente riprendere il contenuto della metodologia già individuata per il controllo riguardante dati e servizi di livello ordinario, inserendo in essa dei passi aggiuntivi per la verifica delle prescrizioni aggiuntive.

In aggiunta, la categorizzazione descritta non vale per i controlli che prescrivono come implementare le Sottocategorie legate alle caratteristiche di qualità, performance e scalabilità e interoperabilità. Le prescrizioni legate alle caratteristiche di qualità, performance e scalabilità e interoperabilità richiedono il soddisfacimento di specifiche diverse, legate a degli standard del settore dei servizi Cloud. Per questo, più che tentare di includere questi controlli in una delle tipologie individuate, si è preferito svolgere un lavoro di analisi a parte, cercando, comunque, di individuare delle metodologie che fossero valide per più controlli di sicurezza. Tali indicazioni non sono molto diverse da alcune tra quelle individuate per i controlli di sicurezza, però per correttezza, si è deciso di trattare i controlli legati a queste caratteristiche separatamente. Infatti, a differenza dei controlli di sicurezza, molti di questi controlli richiedono che il soggetto, che fornisce il servizio Cloud all'Amministrazione, offra un servizio di assistenza e delle API, oppure che aderisca a determinati standard di settore o possegga delle certificazioni ben precise. Questa differenza ha inciso anche nello sviluppo delle metodologie di verifica.

La suddivisione in tipologie dei controlli di sicurezza non ha lo scopo di proporre una catalogazione rigida degli stessi, ma è servita nel processo di sviluppo delle metodologie per adottare un approccio sistematico, facilitando uno sviluppo veloce. Infatti, avendo categorizzato i controlli nelle quattro macro-categorie indicate, è stato possibile sviluppare quattro metodologie di verifica ognuna applicabile a un insieme più ampio di controlli. Inoltre, il vantaggio più importante di questo modo di procedere, è quello di fornire all'ACN delle metodologie che possono essere facilmente corrette e revisionate. Infatti, nel momento in cui viene cambiato un controllo di sicurezza o ne viene aggiunto uno nuovo, non bisogna correggere la metodologia, ma è sufficiente individuare la nuova categoria a cui appartiene il controllo e assegnargli poi la metodologia più corretta. Allo stesso modo se il nuovo controllo non appartiene a nessuna delle categorie individuate, lo si tratta come eccezione e quindi sarà sufficiente sviluppare solo una nuova metodologia di verifica ad hoc per il controllo stesso. In più, nel momento in cui, a seguito dell'aggiunta di nuovi controlli, si ritiene che alcuni dei controlli trattati come eccezione, possano essere raggruppati

in una nuova categoria, è sufficiente rivedere le metodologie sviluppate per ognuno e sintetizzarle in unico modo di procedere. Tali vantaggi sono validi specialmente per le metodologie associate ai controlli delle categorie DOC, POLICY e ACTION, mentre per le metodologie della categoria TECH si condurrà un'analisi separata nel paragrafo ad essi dedicato.

La categorizzazione dei controlli, anche se rappresenta un approccio di alto livello che aveva il rischio di portare a uno sviluppo di metodologie non accurate, comunque ha permesso di essere più elastici sia nel processo di sviluppo sia nel processo di revisione a seguito di aggiunta o correzione dei controlli. Oltre a questo, però, lo sviluppo di metodologie, seguendo l'approccio descritto, può essere un valido supporto anche per l'elaborazione delle metodologie di verifica per i controlli dell'allegato A2. Infatti, le stesse categorie di controlli individuate nell'allegato B2, possono essere adeguate anche per alcuni controlli dell'allegato A2, permettendo in questa maniera un processo di sviluppo molto più rapido e collaudato. Perciò, il gruppo di lavoro che si occuperà di sviluppare metodologie di verifica per il contesto delle infrastrutture Cloud, non dovrà partire da zero. Esso potrà utilizzare alcune delle categorie di controlli già individuate per l'allegato B2, aggiungendo poi altre tipologie adatte per tutti i controlli che non rientrano all'interno delle categorie già individuate. Inoltre, procedendo con questo approccio anche nel caso dell'allegato A2, nel caso di aggiunte o cambiamenti nei controlli, sarà facile assegnare metodologie esistenti, o crearne di nuove per i controlli aggiunti o revisionati.

4.2 Metodologie di verifica

Definiti tutti gli elementi preliminari e individuata la suddivisione in tipologie dei controlli, si è proceduto ad elaborare una metodologia di verifica adeguata per ognuna di esse. .

4.2.1 DOC - Controlli che richiedono l'esistenza di documentazione

Per questa tipologia di controlli lo sviluppo di una metodologia di verifica è risultato abbastanza semplice dal punto di vista concettuale. Infatti, è stato sufficiente valutare quali fonti online, anche mantenute dal provider, fossero più adeguate per accedere alla documentazione del controllo. In questa maniera è stato possibile produrre una metodologia semplice e meccanica e facilmente applicabile in un'ispezione. In dettaglio, sono tre i passi da seguire per applicarla:

1. A seconda della descrizione del documento riportata nel controllo si cerca di stabilire se tale documento può essere pubblicato nella documentazione del Cloud Provider, oppure nei portali che espongono alcuni documenti pubblici

come "white papers". Se si ritiene che il documento possa essere pubblico, allora si procede al passo due, altrimenti si procede con il passo tre.

2. Si ricerca nella documentazione dei servizi offerti dal Cloud Provider, o nel portale che rende accessibili white papers e documenti pubblici, il documento richiesto dal controllo, o un insieme di documenti che contengano le informazioni richieste dal controllo stesso. Nel caso in cui la ricerca si concluda con esito positivo, allora o si ritiene il controllo soddisfatto, perché i documenti trovati riportano tutti gli elementi richiesti, oppure si prescrive un'ulteriore interazione con il soggetto, se i documenti ricercati riportano solo una parte degli elementi richiesti dal controllo. Al contrario, se la ricerca ha esito negativo si procede con il passo tre.

3. Si prescrive al regolatore di avviare un'interazione con il Cloud Provider, tramite la quale si richiede ufficialmente una copia del documento descritto nel controllo di sicurezza.

Naturalmente, è importante sottolineare che un corretto svolgimento del processo di ispezione, prescritto dalla metodologia, dipende dallo svolgimento del primo passo, ovvero comprendere la descrizione e il contenuto che il documento deve avere al fine di stabilire se questo sia pubblico o meno. Il rischio che si corre, se non si interpreta correttamente il controllo, è quello di trovare una documentazione non aderente a quanto richiesto e stabilire che il controllo è correttamente implementato dal fornitore, anche se nella realtà non lo è. Allo stesso modo, se non si svolge nessuna analisi preliminare, e si comincia a ricercare per tentativi nella documentazione del Cloud Service Provider, si rischia di perdere una grande quantità di tempo prima di arrivare a trovare il documento desiderato.

4.2.2 POLICY - Controlli che richiedono la definizione o adozione di policies e/o l'implementazione di processi, procedure e meccanismi

Questa tipologia di controllo riguarda spesso elementi che ogni azienda definisce al proprio interno e non rende pubblici all'esterno. Infatti, le politiche e il modo in cui si svolgono procedure e processi e i vari meccanismi implementati per svolgerli possono essere protetti da segreto industriale o riservati. Per questo motivo, la ricerca della documentazione nei portali del fornitore di servizi Cloud non è un'azione proficua. A fare eccezione è il caso delle politiche di sicurezza che vengono adottate all'interno dell'azienda, la cui pubblicazione potrebbe risultare in una maggiore garanzia di sicurezza per i clienti del fornitore di Servizi Cloud. Allo stesso modo, è molto probabile che un fornitore di servizi Cloud pubblichi all'interno delle documentazioni e dei siti web degli accenni alle procedure di distruzione dei dispositivi fisici che trasportano i dati dei clienti. Infatti, pubblicare le procedure di smaltimento i

dispositivi fisici può contribuire all'aumento della fiducia del cliente verso il fornitore di servizi Cloud, poiché si è ragionevolmente sicuri che non ci siano modi non convenzionali di accesso ai loro dati. Tolti questi due casi particolari, negli altri casi molto spesso la definizione di politiche e delle procedure, processi e meccanismi a supporto delle politiche non viene inserita in documenti pubblici. Perciò, la metodologia per questo tipo di controlli prescrive al regolatore di interagire con il Cloud Provider e richiedere la documentazione necessaria per stabilire che le politiche, i processi, le procedure e i meccanismi a supporto siano definiti e implementati correttamente.

4.2.3 ACTION - Controlli che richiedono lo svolgimento di azioni periodicamente

Tipicamente i controlli di sicurezza rientranti in questa tipologia riguardano l'esecuzione periodica di attività di cybersecurity, il collaudo di piani di risposta agli incidenti, l'aggiornamento di documenti ufficiali contenenti politiche, processi o procedure vitali per la sicurezza dell'azienda. Spesso, la verifica dell'esecuzione di azioni periodiche, nel caso in cui non si è un elemento o unità interna all'azienda, non è un processo molto semplice, in quanto il fornitore di servizi Cloud non è tenuto a pubblicare il rendiconto di tutte le attività di sicurezza che sono svolte. Nonostante ciò, nello sviluppo della metodologia di verifica, si è ritenuto opportuno considerare anche i portali che espongono gli white papers e la documentazione in cui sono riportate le informazioni su come il provider protegge i dati salvati su Cloud e assicura la conformità e la sicurezza dei dati e servizi del cliente. Quindi, la metodologia associata al controllo in esame è caratterizzata dai seguenti due passi:

1. Si ricerca tra gli white papers e la documentazione riguardante la conformità e la sicurezza evidenze dello svolgimento delle attività periodiche. Nel caso di aggiornamenti dei piani si ricerca il piano menzionato dal controllo, al fine di visionarlo e controllare se contenga in appendice una cronistoria degli aggiornamenti. Nel caso di attività pratiche, come le attività di penetration testing si ricercano i report relativi alle attività stesse in maniera tale da stabilire quale sia la loro frequenza di esecuzione. Se la ricerca ha esito positivo e i documenti trovati soddisfano le richieste del controllo, allora si stabilisce che il fornitore di servizi Cloud soddisfa i requisiti di sicurezza. Altrimenti, se la ricerca non ha esito positivo si procede con il passo due.

2. Si prescrive al regolatore di interagire con il fornitore di servizi Cloud per richiedere i documenti necessari (e.g. verbali di riunioni, piani, report) per stabilire se il soggetto implementa correttamente il controllo.

La ricerca dei documenti citati non è molto semplice, in quanto non tutti i Cloud Provider pubblicano informazioni riguardanti le attività che compiono e l'aggiornamento dei piani di risposta. A volte, è possibile trovare online dei report delle attività di penetration testing a cui sono stati sottoposti i servizi Cloud di un fornitore, in quanto pubblicare i report dei pentration tests a cui i servizi sono regolarmente sottoposti contribuisce ad aumentare la fiducia del cliente. Tuttavia, specialmente se il team che si occupa di fare attività di penetration testing è interno all'azienda che eroga i servizi Cloud, è molto difficile che questi report siano visualizzabili online.

4.2.4 TECH - Controlli che richiedono l'implementazione di tecnologie o l'adozione di sistemi afferenti all'ambito della Sottocategoria

I controlli di sicurezza che prescrivono l'adozione di tecnologie e sistemi ben precisi da parte del soggetto sono tra quelli per cui è stato più difficile sviluppare la metodologia di verifica. Infatti, il modo in cui i fornitori di servizi Cloud implementano determinate tecnologie a supporto delle attività di cybersecurity e i sistemi di sicurezza che utilizzano non sono necessariamente informazioni di pubblico dominio. Tra tutte le tecnologie e sistemi di sicurezza citati dai controlli, fanno eccezione le tecnologie legate alla crittografia. Queste di solito sono ben documentate da parte dei provider con lo scopo di mettere in mostra le garanzie di sicurezza che essi offrono per i dati dei clienti. Per queste tecnologie allora, la metodologia prescrive una ricerca approfondita sulla documentazione tecnica dei provider, in maniera tale da stabilire se il fornitore garantisce le funzionalità di data protection richieste dal controllo.

Per tutte le altre tecnologie menzionate dai controlli, non avendo accesso a nessuna infrastruttura e ambiente di un Cloud Provider, l'unica prescrizione che si potrebbe imporre sarebbe quella di richiedere al fornitore una relazione sul modo in cui determinate tecnologie e sistemi sono implementati. Tuttavia, questa strada non sembra molto di aiuto per il regolatore, perché rimanda il processo di sviluppo di una metodologia adeguata a un secondo momento. Allora per cercare di fornire maggiore aiuto al regolatore si è deciso di sviluppare una metodologia, ipotizzando, sulla base delle caratteristiche comuni delle infrastrutture Cloud, il modo in cui le tecnologie e i sistemi oggetto del controllo fossero implementati.

L'idea dietro questa scelta, è che, se l'ipotesi di contesto è adeguata, si ottiene una metodologia di alto livello valida per più Cloud Service Provider, che necessita solo di un leggero approfondimento. Al contrario, se l'ipotesi non aderisce al modo in cui determinate tecnologie e sistemi sono utilizzati nell'infrastruttura del provider, comunque rimane valido il modo di procedere indicato in precedenza, che è comunque corretto. Purtroppo, tale scenario di utilizzo del sistema o della tecnologia non è sempre delineabile, poiché la tecnologia o sistema citato nel controllo può essere descritto ad alto livello, senza scendere nel dettaglio implementativo. Ad esempio, se

in alcuni controlli si parla esplicitamente di sistemi SIEM o SDL (System Development Cycle), in altri controlli si parla in maniera più generale di sistema di raccolta dei log. Quindi, in base al numero di dettagli inclusi nei controlli appartenenti a questa tipologia, si può decidere di procedere in uno dei due modi indicati prima.

Ovviamente, poiché la metodologia dei controlli di tipo TECH dipende dalla tecnologia menzionata nel controllo, non è possibile formulare un'unica metodologia valida per tutti i controlli TECH, come avvenuto nel caso degli altri controlli. Tuttavia, a differenza dei controlli catalogati come eccezioni, per questi è stato possibile sviluppare delle indicazioni o linee guida che sono state utilizzate nello sviluppo di ogni metodologia associata a un controllo di questa categoria. Data la possibilità di compiere un ipotesi sul modo in cui tecnologie e sistemi citati dal controllo sono implementati, le indicazioni seguite nello sviluppo sono molto articolate. Esse prevedono delle diramazioni a seconda del carattere più o meno specifico della descrizione delle tecnologia o sistema oggetto del controllo di sicurezza. In particolare, per lo sviluppo di ogni metodologia si è proceduto con i seguenti passaggi:

1. **Analisi della tecnologia o sistema oggetto del controllo**: si caratterizza la tecnologia o il sistema oggetto del controllo. Successivamente, se si è sviluppata una caratterizzazione sufficientemente approfondita della tecnologia si procede con il passo 2, altrimenti si procede con il passo 3.

2. **Ricerca sulla documentazione**: si ricercano nella documentazione del fornitore di servizi Cloud evidenze e dettagli sull'implementazione delle tecnologia o sull'adozione del sistema oggetto del controllo. Nel caso in cui la ricerca ha esito positivo si procede con il passo 2a. Altrimenti si procede con il passo 2b.

2a. **Analisi delle documentazione ricercata**: se la documentazione ricercata all'interno dei portali del fornitore di servizi Cloud riporta tutte le informazioni necessarie a stabilire che la tecnologia è implementata correttamente o il sistema è adottato in maniera aderente al controllo, allora si marca il controllo come soddisfatto. Altrimenti si riporta la documentazione nella metodologia e si prescrive un'ulteriore interazione con il Cloud Service Provider.

2b. **Ipotesi di contesto**: sulla base della conoscenza dell'infrastruttura virtuale del fornitore di servizi Cloud si ipotizza uno scenario di corretta implementazione della tecnologia o di corretta adozione del sistema. La metodologia, a quel punto, prescrive un'ispezione dell'ambiente Cloud gestito dal provider che ha lo scopo di stabilire se la tecnologia o il sistema sono implementati, e se lo sono in maniera aderente allo scenario ipotizzato.

3. **Interazione con il provider**: si prescrive al regolatore di interagire con il provider che ha richiesto la qualificazione per avere maggiori dettagli sull'im-

plementazione della tecnologia o sull'adozione del sistema oggetto del controllo. Lo sviluppo della metodologia è rimandato a un secondo momento.

Seguendo le indicazioni presentate, si sviluppano delle metodologie abbastanza specifiche, con la consapevolezza che però queste vanno comunque revisionate, nel caso in cui l'ipotesi fatta non sia verificata, o sviluppate, nel caso in cui non è stato possibile fare nessuna ipotesi.

4.2.5 Eccezioni e considerazioni finali

Come rimarcato nella sezione 4.1, ci sono controlli di sicurezza che non appartengono in maniera determinata a nessuna delle tipologie individuate, e per questo costituiscono un'eccezione. Per tutti questi controlli non inquadrabili in nessuna delle categorie indicate si è deciso di sviluppare una metodologia ad hoc. Tali metodologie sono riportate in Appendice, mentre in questo capitolo si preferisce riportare solo alcuni esempi di controlli che fanno eccezione. Tra questi sicuramente si annoverano tutti i controlli di sicurezza che fanno riferimento alla Sottocategoria PR.IP-4, che riguarda l'esecuzione e l'amministrazione dei backup delle informazioni. Questi controlli di sicurezza fanno eccezione, rispetto agli altri, perché richiedono un cambio di prospettiva nella scrittura della metodologia stessa. Infatti, a seconda del tipo di backup inteso dal controllo si possono configurare due diversi modi di procedere. Nel caso in cui i backup intesi dal controllo sono quelli relativi a servizi di storage o servizi di DBMS, allora è necessario creare una metodologia per il controllo di sicurezza, seguendo le linee guida già discusse per i controlli di tipo ACTION e descritte in 4.2.3.

Al contrario, se si parla dei backup di servizi e istanze di macchine virtuali su Cloud, di solito i fornitori offrono la gestione di questi backup come un servizio Cloud a parte. Ogni fornitore offre un servizio di carattere SaaS o IaaS che permette al cliente di gestire tutti gli aspetti di sicurezza correlati ai backup delle informazioni. Per questo motivo, dato che il fornitore di servizi Cloud delega la gestione dei backup al cliente, le metodologie per i controlli afferenti a questa Sottocategoria sono state elaborate prescrivendo al regolatore di controllare se l'Amministrazione ha configurato correttamente il servizio offerto dal fornitore. Come per i controlli di carattere TECH, anche in questo caso lo sviluppo di una metodologia di verifica dipende dal tipo di servizio offerto dal fornitore di servizi Cloud considerato. Per questo, si riportano una serie di indicazioni su come sviluppare una metodologia di verifica adeguata:

1. Rintracciare all'interno della documentazione tutte le pagine riguardanti il servizio di backup offerto dal fornitore.

2. Comprendere in maniera approfondita il funzionamento degli aspetti principali del servizio di backup, in maniera da stabilire lo scenario di corretta implementazione in accordo con i controlli.

3. Elaborare le metodologie, prescrivendo l'adozione, da parte dell'Amministrazione, del servizio di backup individuato, e la verifica della sua corretta implementazione.

Allo stesso modo di alcuni controlli di sicurezza, anche i **controlli legati alle caratteristiche di qualità, interoperabilità e performance e scalabilità** rappresentano un'eccezione rispetto alle tipologie individuate. Iniziando dai **controlli di qualità**, si sottolinea che spesso richiedono che il Cloud provider sotto esame aderisca a un preciso requisito o possegga un determinato certificato indicato nel controllo. Quindi, per lo sviluppo di una metodologia di verifica per questa tipologia di controlli è stato sufficiente riutilizzare in parte la metodologia esistente per i controlli di carattere DOC. A differenza di quei controlli però, le fonti in cui ricercare prove o certificati che dimostrano che un fornitore di servizi Cloud aderisce a determinati requisiti di qualità sono diverse. Perciò la metodologia di verifica dei controlli di qualità prescrive di ricercare all'interno del sito web ufficiale del fornitore di servizi Cloud in esame, le informazioni necessarie o i certificati che confermino l'aderenza del provider al requisito di qualità espresso nel controllo. Tuttavia, è importante sottolineare che, allo stato attuale, non è stato possibile applicare la metodologia di verifica proposta per i controlli afferenti alle Sottocategorie della categoria QU.LS. Infatti, i controlli citati riguardano le caratteristiche dei Service Level Agreement (SLA), che sono concordati nel momento in cui avviene la produzione di una bozza del contratto con il fornitore di servizi Cloud. Non avendo a disposizione, perciò, nessun contratto su cui basare le verifiche non è stato possibile utilizzare la metodologia di verifica elaborata e nemmeno svilupparne una adatta. Per questo si è demandato al regolatore lo sviluppo di tale metodologia al momento in cui un'Amministrazione stipula un contratto con un fornitore.

Il modus operandi adottato per i controlli di qualità è lo stesso adottato anche per quelli legati alle caratteristiche di interoperabilità. Per i **controlli di interoperabilità** la metodologia di verifica elaborata prescrive un'analisi delle documentazioni e dei siti web dei fornitori scelti per verificare che fossero fornite tutte le funzionalità di portabilità dei dati e dei servizi richieste nel controllo. Nel caso in cui queste funzionalità non fossero presenti, si prescrive al regolatore di contattare il team di vendita del provider, per richiedere informazioni riguardo gli elementi citati nel controllo. Infine, per tutti i controlli relativi alle caratteristiche di performance e scalabilità, si è proceduto come per i controlli di qualità, ovvero si è adattata la metodologia sviluppata per i controlli di tipo DOC. Infatti, la metodologia di verifica per questi controlli prescrive di ricercare nelle documentazioni, negli white papers e

nei siti web dei fornitori la descrizione delle performance dei servizi offerti. Nel caso in cui questa descrizione non sia presente allora si prescrive una interazione con il team di vendita del provider per acquisire questa informazione

Alla fine del processo di sviluppo delle metodologie si è deciso di applicare quelle associate alle categorie DOC, POLICY e ACTION, quella associata alla categoria TECH per la crittografia e alcune di quelle indicate per i controlli che fanno eccezione. Non potendo coprire un gran numero di fornitori di servizi Cloud, si è ritenuto opportuno applicare le metodologie di verifica sviluppate per tre grandi fornitori di servizi Cloud leader nel mercato, ovvero Microsoft Azure, Amazon Web Services e Google Cloud. La scelta di ispezionare, per quanto possibile, i servizi Cloud offerti da questi tre fornitori, deriva dal fatto che sono molto utilizzati al livello globale e offrono dei servizi Cloud molto potenti e affidabili. Quindi, se uno di questi provider ottenesse la qualificazione per ospitare dati e servizi della Pubblica Amministrazione, si otterrebbe un enorme vantaggio per buona parte degli enti pubblici. Migrare su uno di questi provider, nel caso in cui ottenessero la qualificazione, potrebbe essere un grande passo avanti nel processo di digitalizzazione che stanno attraversando moltissime Pubbliche Amministrazioni Italiane. Lo stesso Polo Strategico Nazionale si avvale di servizi e infrastrutture dei grandi hyperscaler. Il risultato di queste ispezioni è stato raccolto all'interno di un documento strutturato, visibile in Appendice, che contiene anche tutte quelle metodologie specifiche per i controlli della categoria TECH e per quelli che rappresentano un'eccezione. Tali metodologie non sono state riportate in questo capitolo per offrire una visione più di alto livello sul processo di sviluppo e sul suo risultato finale. Inoltre non è stato possibile nemmeno applicare le metodologie associate ai controlli di tipo TECH in un'ispezione, poiché non si è potuto avere accesso nessuna delle infrastrutture dei provider considerati. La struttura del documento è molto comprensibile, in quanto per ogni Sottocategoria viene riportato il codice, la descrizione e poi il risultato dell'ispezione per ogni controllo, o la metodologia di verifica associata ad ogni controllo.

4.3 Esempi di Metodologie sviluppate e ispezioni eseguite

Descritte le metodologie sviluppate per alcune categorie di controlli e le linee guida seguita per sviluppare le metodologie dei controlli TECH, si presentano alcune metodologie e alcuni risultati delle ispezioni condotte e contenute nel documento in Appendice.

4.3.1 Esempio 1: Controllo numero uno Sottocategoria ID.GV-1. (DOC)

Il primo esempio che si discute riguarda il controllo numero uno afferente alla Sottocategoria ID.GV-1, che richiede *l'esistenza di un documento aggiornato che*

descrive le politiche, i processi e le procedure di cybersecurity. Tale controllo appartiene alla prima categoria di controlli individuata, ovvero quella riguardante i controlli che richiedono l'esistenza di determinati documenti. A seguito dell'applicazione della metodologia, si è stabilito il risultato dell'ispezione per ognuno dei tre fornitori di servizi Cloud sotto esame:

MS Azure: Esiste un documento che descrive la politica di cybersecurity di Microsoft, scaricabile a questo link. Tale documento è un documento sintetico. Al contrario un documento più di dettaglio sulla policy di cybersecurity di Microsoft è disponibile qui

Google Cloud: Non esiste un documento pubblico che esprime la policy di cybersecurity di Google, però a questo link, è possibile visionare il white paper che dà una panoramica sulla sicurezza di Google Cloud. In questo documento sono descritti processi e procedure e misure tecnologiche che vengono utilizzate per raggiungere alcuni obiettivi di sicurezza. Per un documento di maggior dettaglio bisogna contattare il team del Cloud Provider.

AWS: AWS non pubblica un documento che descrive le politiche i processi e le procedure di cybersecurity. Per questo tale documento va richiesto al Cloud Provider, verificando che siano descritti le politiche, i processi e le procedure di cybersecurity.

La metodologia appena presentata è funzionale a capire come avviene l'applicazione delle indicazioni discusse in precedenza. Infatti, per tutti e tre i fornitori di servizi Cloud in esame, si è stabilito che un documento, come quello contenente le policies, i processi e le procedure di sicurezza, può essere pubblico, giustificando, perciò, un tentativo di ricerca. Mentre nel caso di Microsoft Azure è stato possibile trovare la documentazione aderente ai requisiti richiesti, per Google Cloud si è trovato solo un documento contente parte degli elementi richiesti dal controllo e per questo si è prescritta una successiva interazione con il provider. Al contrario per AWS non è stato possibile trovare dei documenti che riportino tutti gli elementi richiesti dal controllo e per questo si è prescritta direttamente un'interazione con il provider.

4.3.2 Esempio 2: Controllo numero uno Sottocategoria PR-AC-1 (TECH)

Il secondo esempio riguarda la metodologia associata al controllo numero uno della sottocategoria PR.AC-1, riguardante la gestione delle credenziali del personale aziendale. Il testo esatto del controllo è: *Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.* In questo caso analizzando il testo del controllo, si è subito riscontrata una chiara

definizione dell'ambito, cioè quello della gestione delle identità, che ha permesso di capire quali fossero i sistemi e le tecnologie utilizzabili per la realizzazione del controllo. Per questo, comprendendo che un fornitore di servizi Cloud non rivela come avviene internamente al suo personale la gestione delle identità e delle credenziali, si è deciso di procedere con la definizione di un possibile scenario di implementazione corretta. Tutto il processo di analisi svolto ha portato alla definizione della seguente metodologia:

"Utilizzando le API del servizio di directory utilizzato dal CSP per la gestione delle identità, o accedendo al servizio di directory attraverso il sistema IAM o il sistema PAM, ottenere la lista di credenziali immagazzinate nel Directory Information Base. Successivamente verificare che non ci siano credenziali duplicate per ogni membro del personale del soggetto. Successivamente per ogni entry ottenuta dal servizio di directory interrogato, controllare gli attributi della entry per collegare la entry ai permessi associati alle credenziali. A quel punto, verificare per ogni entry di un nodo del Directory Information Tree, che rappresenta una funzione aziendale, che questa non abbia dei permessi che sono posseduti anche da altre entry di altri nodi dell'albero. In questa maniera se il DIT è conforme all'organigramma del CSP e non ci sono due entry che hanno uno stesso insieme di permessi in due entry differenti, allora viene rispettato il principio di segregazione delle funzioni. Nel caso in cui si acceda alle identità mediante, invece, un sistema di Identity and Access Management o di Priviliged Access Management, allora è necessario verificare che non ci siano credenziali, facenti capo a diverse unità organizzative, che possiedano uno stesso insieme di permessi. Infine, accedere ai log del servizio di directory o a un registro delle attività o del sistema di Identity and Access Management o di Priviliged Access Management e verificare che le credenziali siano state cambiate con una cadenza proporzionata ai privilegi di utenza."

Il contesto di implementazione corretta immaginato per la scrittura della metodologia di questo controllo fa riferimento a uno schema di gestione delle identità standard e adottato da molte aziende in campo IT. Tuttavia, non è detto che il fornitore di servizi Cloud realizzi la gestione delle identità in maniera esattamente aderente allo scenario ipotizzato, in quanto ogni provider è libero di amministrare come meglio crede le credenziali di accesso dei dipendenti. Nonostante ciò, lo schema di gestione delle identità a cui si fa riferimento nella metodologia, è uno schema molto diffuso e standardizzato, e spesso il modo di amministrare le credenziali di accesso all'interno delle imprese può essere ricondotto a questo modello di base, al netto di qualche modifica. Perciò, la metodologia sviluppata risulta comunque valida e costituisce un buon punto di partenza, in quanto nel momento in cui la si applicherà per un fornitore di servizi Cloud specifico, sarà sufficiente adeguare il contesto ipotizzato nella metodologia al modo reale con cui il provider stesso gestisce le identità.

4.3.3 Esempio 3: Controllo numero cinque Sottocategoria PR.DS-1 (TECH)

Un altro controllo appartenente alla categoria TECH è il quinto della Sottocategoria PR.DS-1, la quale riguarda le tecnologie messe in campo dal soggetto per la protezione dei dati, come ad esempio meccanismi crittografici, Hardware Security Modules (HSM) e così via. In particolare il controllo si focalizza sulle chiavi crittografiche richiedendo che *siano presenti processi, procedure e misure tecniche per revocare e rimuovere le chiavi crittografiche prima della fine del loro periodo di validità, quando una chiave è compromessa, o un'entità non fa più parte dell'organizzazione, conformemente a requisiti legali e normativi.* Analizzando il controllo, rispetto al precedente esempio, si rileva subito che le tecnologie e le procedure coinvolte riguardano la crittografia, ovvero un aspetto che di solito è ben documentato dai Cloud providers, in quanto l'approccio di sicurezza per oscurità non è il migliore approccio per le procedure crittografiche. Quindi, si è applicata la metodologia definita per questi particolari controlli TECH ed è stata operata una ricerca sulle documentazioni dei fornitori di servizi Cloud Al termine della ricerca svolta si è concluso che il controllo era soddisfatto da tutti e tre i provider:

MS Azure: Nel caso in cui si sia scelta una soluzione di tipo managed HSM BYOK (Bring Your Own Key) allora è necessario verificare che l'amministrazione preveda i processi per la revoca, prima della fine del periodo di validità, di una chiave compromessa, o nel caso in cui un'entità non faccia più parte dell'organizzazione. Nel caso in cui non si sia scelta la soluzione BYOK, comunque mediante Azure portal o mediante la Azure CLI o mediante le Azure API sono implementate procedure per la revoca delle chiavi. Dalla CLI di Azure usando in successione i comandi seguenti:

```
az keyvault key set-attributes -name <nome_chiave> -enable false
        az keyavult key delete -name <nome_chiave>
            az keyavult key purge -name <nome_chiave>
```

si revoca e si rimuove una chiave dal vault o dall'HSM. Se si utilizzano le REST API di Azure, il processo per cambiare lo stato della chiave è descritto in questa pagina. Per cancellare ed eliminare definitivamente dal vault la chiave si fa riferimento ai comandi descritti nelle seguenti pagine: cancellazione eliminazione

Google Cloud: Nel caso del cloud Google quando una chiave viene rinnovata, viene creata un'altra versione di quella chiave. Quindi, nel momento in cui i dati sono cifrati, si tiene conto della versione della chiave con cui sono stati cifrati. Quindi se si deve sospendere una chiave, perché compromessa o per altri motivi, è necessario creare una nuova versione della chiave, decifrare tutti i dati cifrati

con la precedente versione e ri-cifrarli con la nuova versione. Solo dopo aver compiuto questi passaggi è possibile procedere con l'invalidazione e rimozione della versione compromessa. Ovviamente Google Cloud implementa delle procedure che permettono di fare tutte queste cose, e l'obiettivo è raggiungibile secondo i seguenti passi:

1. Ruotare manualmente la chiave come riportato nel seguente link.
2. Decifrare e ricifrare i dati cifrati con la chiave compromessa con i passaggi esposti in questa pagina.
3. Disabilitare la versione compromessa della chiave nella maniera indicata in questa guida.
4. Distruggere la versione della chiave seguendo le indicazioni riportate qui.

Quindi Google implementa le procedure e le misure tecniche per la revoca anticipata delle chiavi.

AWS: AWS implementa dei processi e delle procedure per revocare e rimuovere le chiavi crittografiche, prima della fine del periodo di validità. Esso permette prima di disabilitare una chiave, in maniera da renderla inutilizzabile, per poi dare la possibilità di schedulare la cancellazione della chiave che al massimo avviene 30 giorni dopo averla programmata. Per disabilitare una chiave sono messe a disposizione le misure tecniche descritte in questa guida. Allo stesso modo per schedulare la cancellazione di una chiave le misure tecniche e le procedure sono descritte in questa pagina. Se si tratta di chiavi multi-regione allora la procedura per la cancellazione è descritta in questa guida, mentre per chiavi importate in AWS KMS dall'utente la procedura di cancellazione è descritta qui. Ovviamente come accade in altri Cloud Provider nel momento in cui si cancella una chiave tutto il materiale cifrato con quella chiave non è più recuperabile e quindi se qualcosa deve essere mantenuto, prima di cancellare la chiave, bisogna decifrare il materiale, e ri-cifrarlo con una nuova chiave.

Per ogni provider, come si evince anche dalla descrizione, è stato possibile trovare tutte le evidenze necessarie per stabilire che il controllo fosse soddisfatto.

Capitolo 5

Case study: Data Localization in AWS

5.1 Scenario

5.1.1 Requisiti di data residency

Tra tutte le verifiche eseguite, mediante l'applicazione delle metodologie sviluppate, è importante descrivere in maniera approfondita il risultato di quella associata alla Sottocategoria `SC-SI-PR.DS-1-01` dell'allegato B alla determina n. 307 di ACN, riguardante la localizzazione dei dati e metadati delle Amministrazioni in Unione Europea. In particolare il testo dell'unico controllo riportato per questa Sottocategoria è il seguente:

> *I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.*

Tale controllo di sicurezza rientra tra quelli della categoria TECH in cui è necessario interagire con il Cloud Service Provider al fine di capire quali strumenti sono messi a disposizione per soddisfare la richiesta del controllo.

Il trattamento dei dati attraverso infrastrutture localizzate sul territorio dell'Unione Europea è un requisito importante, il cui soddisfacimento dipende sia dalla configurazione dell'infrastruttura di rete del provider, sia dalla capacità del fornitore di servizi Cloud di offrire all'Amministrazione adeguati strumenti per la *data localization*. Quindi, la localizzazione dei dati delle Amministrazioni su suolo UE è un requisito che si collega direttamente al concetto di modello a responsabilità di sicurezza condivisa o Shared Security Responsibility Model (SSRM), implementato dalla maggior parte dei fornitori di servizi Cloud. Il modello SSRM distingue in maniera netta il concetto di *sicurezza nel Cloud* dal concetto di *sicurezza del Cloud*. Il primo concetto riguarda la sicurezza dell'ambiente, dell'infrastruttura e dei servizi

che il Cloud Provider offre al cliente. Ad esempio, è compito del fornitore di servizi Cloud configurare la sua infrastruttura di rete in maniera tale che non ci possano essere flussi di dati non ammessi verso data center non situati all'interno dell'Unione Europea. Al contrario, per sicurezza nel Cloud si intende che il cliente, che utilizza i servizi Cloud concessi da un fornitore, deve configurare e operare il provisioning degli stessi in maniera corretta, senza introdurre vulnerabilità o difetti, che possono portare a incidenti di sicurezza. Rimanendo sempre nell'ambito della data localization, è compito del cliente configurare il provisioning delle risorse e utilizzarle in maniera tale da non localizzare dati e servizi in paesi extra-UE. Di solito, per favorire la corretta implementazione di un alto grado di sicurezza nel Cloud è il provider stesso che mette a disposizione degli strumenti a supporto del cliente per la corretta configurazione delle risorse richieste.

I leader di mercato nella fornitura di servizi Cloud organizzano la loro infrastruttura globale secondo un modello a regioni, ovvero raggruppano i loro data center in base alla posizione geografica sul globo. Ogni regione, in inglese region, è isolata dalle altre per aumentare il grado di resilienza dell'infrastruttura, in maniera tale che un fallimento all'interno di una region non influisca sull'operato delle altre. Ogni cliente, nel momento in cui opera il provisioning di servizi Cloud presso un Cloud Provider, ha la possibilità di scegliere in quali region richiedere le risorse di elaborazione o di storage dei dati. Le risorse richieste saranno attivate solo nelle region scelte dal cliente e non in altre, a meno di impostazioni finalizzate a garantire la business continuity e la disaster recovery, che sono segnalate dal provider prima del provisioning del servizio. In aggiunta, se il cliente desidera attivare risorse anche in altre region, può operarne il provisioning anche in un momento successivo alla prima richiesta. Quindi, nell'ambito di una localizzazione dei dati sul suolo europeo, è compito del cliente richiedere risorse nelle region corrette, ed è dovere del fornitore di servizi Cloud garantire che i servizi siano attivati solo nelle region indicate e che i dati transitino e siano salvati solo nelle region selezionate.

Il coinvolgimento, anche parziale, del cliente nell'implementazione di una corretta localizzazione dei dati e dei servizi sul Cloud, comporta che la metodologia di verifica sviluppata per il controllo di sicurezza associato alla Sottocategoria `SC-SI-PR.DS-1-01` richieda una doppia verifica presso il fornitore. Chiaramente se la prima fallisce non si svolge la seconda:

- L'infrastruttura di rete globale del Cloud Service Provider deve essere configurata in maniera tale che non sia possibile instradare i dati dei clienti verso region differenti da quelle richieste dal cliente.

- Tra i servizi offerti dal provider esistono strumenti di sicurezza capaci di impedire all'Amministrazione di operare il provisioning di servizi in region differenti da quelle UE.

Questa doppia verifica rende l'applicazione della metodologia molto interessante e degna di un approfondimento, in quanto con essa non si valuta solo la sicurezza del Cloud che ha un fornitore di servizi Cloud, ma anche gli strumenti che permettono al cliente di incrementare la sicurezza nel Cloud.

Ovviamente, vista l'impossibilità di operare verifiche su un'infrastruttura di un fornitore di servizi Cloud, si è deciso di approfondire la seconda verifica della metodologia, legata agli strumenti di sicurezza offerti dal provider per garantire una corretta localizzazione dei dati e servizi delle Amministrazioni. Tuttavia, non è stato possibile applicare la metodologia per tutti e tre i Cloud Service Provider presi in considerazione, perché il processo di verifica anche solo di uno dei due aspetti della metodologia ha richiesto un tempo non trascurabile. Per questo, anche grazie all'intermediazione di ACN, si è scelto di effettuare la verifica presso un Cloud Service Provider leader nel mercato come Amazon Web Services, valutando se questo offrisse adeguati strumenti alle Amministrazioni per localizzare su territorio europeo i loro dati e carichi di lavoro. Analizzando i prodotti di sicurezza offerti da AWS e le loro documentazioni, si è concluso che ci sono due strumenti utilizzabili con relativa facilità dalle Pubbliche Amministrazioni italiane, cioè le **policy AWS** e **AWS Control Tower**. I servizi individuati possono essere utilizzati sia in maniera esclusiva, sia in combinazione per aumentare il grado di sicurezza nel Cloud per una Pubblica Amministrazione. In seguito verrà offerta una descrizione dettagliata degli strumenti e alcuni esempi di utilizzo degli stessi. Infatti, si è ritenuto opportuno, al fine di operare un'ispezione più approfondita, testare direttamente gli strumenti messi a disposizione, in maniera da evidenziarne eventuali lacune o esaltarne i pregi. Allo stesso modo le configurazioni proposte degli strumenti potranno essere un valido punto di partenza per molte Amministrazioni Pubbliche che hanno intenzione di portare i loro dati e servizi presso il Cloud AWS.

5.1.2 Concetti preliminari su AWS

I grandi fornitori di servizi Cloud organizzano il loro ambiente e la loro infrastruttura secondo le best practices del settore, in maniera da offrire ai loro clienti importanti garanzie di resilienza. Tuttavia, anche se alcune caratteristiche dell'ambiente e delle infrastrutture Cloud sono comuni a più fornitori, ogni provider è libero di personalizzare la propria infrastruttura e il proprio ambiente come meglio crede. La conseguenza naturale di queste personalizzazioni è che la comprensione del funzionamento e delle caratteristiche degli strumenti di sicurezza individuati dipende da una conoscenza preliminare dell'infrastruttura di rete e della divisione dei data center in region del fornitore. Quindi, al fine di offrire una migliore panoramica sul funzionamento delle policy AWS e di AWS Control Tower, si descrivono alcune peculiarità dell'infrastruttura globale creata da AWS nel tempo e dei loro servizi.

Innanzitutto, visto che si approfondisce un argomento delicato come la data residency, è importante descrivere l'organizzazione dei data center di AWS in regioni e zone di disponibilità. Infatti, il modo in cui i data center sono localizzati in tutto il globo e connessi tra loro influisce in maniera importante sulla velocità, sulla resilienza e sulla disponibilità dei servizi offerti dal provider. In particolare AWS organizza la sua infrastruttura Cloud attorno a tre elementi fondamentali:

- **Data Center**: è il luogo fisico che ospita e gestisce i server veri e propri e l'infrastruttura informatica;
- **Zone di disponibilità (Availability Zones)**: rappresentano dei cluster di almeno tre data center connessi tra loro e fisicamente isolati dagli altri in altre zone di disponibilità;
- **Regioni AWS**: sono sedi fisiche, distribuite su tutto il globo e isolate fisicamente l'una dall'altra, che raggruppano almeno tre zone di disponibilità.

Questo tipo di organizzazione rappresenta una prima importante differenza tra AWS e gli altri fornitori di servizi Cloud, i quali identificano la region con il singolo data center. Avere più data center all'interno di una stessa region, organizzati in più zone di disponibilità, permette al cliente di beneficiare di un'infrastruttura con elevati livelli di disponibilità e resilienza, anche localizzando i propri dati e servizi in una singola region AWS. Infatti, ogni zona di disponibilità all'interno di una region AWS è collegata alle altre mediante collegamenti a bassa latenza, però essa è fisicamente indipendente dalle altre. Ciò significa che un fallimento di uno o più data center all'interno di una zona di disponibilità, non ha impatto sulle altre zone e sulla disponibilità dei servizi in quelle zone. Questo, unito all'isolamento reciproco tra le region, e alla progettazione dei data center secondo i migliori standard di settore contribuisce all'alta disponibilità e tolleranza ai guasti dell'infrastruttura.

La suddivisione delle region in zone di disponibilità non è l'unica caratteristica importante dell'infrastruttura AWS, in quanto le regioni AWS si possono suddividere tra loro in due gruppi. Il primo gruppo è quello delle *default regions*, ovvero tutte quelle introdotte nell'infrastruttura AWS prima del 20 marzo 2019. Originariamente AWS rendeva disponibili ai clienti tutte le regioni appartenenti alla sua infrastruttura globale, in maniera da permettergli di creare, richiedere e gestire risorse in una qualsiasi di questi raggruppamenti di data center. Tuttavia, avendo ormai trentadue regioni distribuite in tutto il globo, AWS ha deciso di non renderle disponibili subito. Infatti, nel momento in cui viene resa operativa una nuova regione AWS essa non viene subito abilitata per i clienti, ma rimane disattivata, e non è possibile richiedere e gestire risorse al suo interno. Queste regioni, introdotte dopo il marzo 2019, sono definite *regioni opt-in*. Se un cliente desidera utilizzare servizi o salvare dati all'interno dei data center di una di queste region, deve richiederne l'abilitazione dal suo account.

Attualmente fanno parte delle *regioni opt-in* tutte quelle elencate nella Tabella 5.1 Chiaramente l'attivazione di una region opt-in non è immediata, in quanto prima di

Nome della regione	Codice
Africa (Cape Town)	`af-south-1`
Asia Pacific (Hong Kong)	`ap-east-1`
Asia Pacific (Hyderabad)	`ap-south-2`
Asia Pacific (Jakarta)	`ap-southeast-3`
Asia Pacific (Melbourne)	`ap-southeast-4`
Europe (Milan)	`eu-south-1`
Europe (Spain)	`eu-south-2`
Europe (Zurich)	`eu-central-2`
Israel (Tel Aviv)	`il-central-1`
Middle East (Barhain)	`me-south-1`
Middle East (UAE)	`me-central-1`

Tabella 5.1: Regioni AWS disabilitate per impostazione predefinita

poter creare e gestire risorse all'interno della nuova region, AWS deve eseguire delle azioni necessarie per fornire pieno accesso all'infrastruttura a chi ha richiesto una nuova region. Allo stesso modo anche la disattivazione di una region opt-in non è immediata, perché AWS deve disabilitare l'accesso alla console di gestione e quello programmatico nella regione.

La divisione dell'infrastruttura Cloud di AWS in regioni, però, non ha effetti solo sulla disponibilità e sulla resilienza dei servizi, ma anche sulla strutturazione dei servizi stessi. Una delle peculiarità di AWS è la separazione tra *control plane* e *data plane* nei propri servizi. Il *control plane* rappresenta tutte le funzionalità per creare, leggere, descrivere, aggiornare, cancellare ed elencare le risorse associate a un certo servizio. Al contrario, il *data plane* rappresenta la funzione primaria del servizio, ovvero la lettura e scrittura su un bucket di Simple Storage Service (S3), oppure l'esecuzione di una macchina virtuale EC2. La separazione tra questi due aspetti dei servizi AWS permette di classificarli in tre categorie che si distinguono per il grado di distribuzione del loro *data plane*. Infatti, nel Cloud AWS esistono **servizi zonali**, **servizi regionali** e **servizi globali**.

I **servizi zonali** sono caratterizzati dall'avere un *data plane* indipendente in ogni zona di disponibilità in cui si può accedere al servizio. Questo significa che è possibile specificare in quale zona di disponibilità sono distribuite le risorse associate al servizio e che i servizi zonali funzionano in maniera indipendente in ogni zona di disponibilità in cui sono accessibili. Quindi, un fallimento del servizio in una zona di disponibilità non intacca il funzionamento del servizio in un'altra zona di disponibilità. Inoltre, alcuni servizi zonali replicano in ogni zona di disponibilità non solo il *data plane* ma anche il *control plane*, per permettere di compiere operazioni riferite a una sola zona di disponibilità. Ad esempio, Elastic Compute Cloud (EC2) è un servizio zonale di

AWS che ha un *control plane* in ogni zona di disponibilità per permettere all'utente di lanciare un'istanza di EC2 nella stessa zona. Tuttavia, AWS per tutti i servizi zonali mette a disposizione anche un unico endpoint di accesso al *control plane* del servizio al livello regionale sia per facilitare l'interazione con il servizio, sia per fornire la possibilità di eseguire operazioni aggregate sulle risorse al livello regionale.

Proseguendo i **servizi regionali** si differenziano per il maggior grado di distribuzione del *data plane* rispetto ai servizi zonali. Infatti, nei servizi regionali non esiste un *data plane* indipendente per ogni zona di disponibilità, ma si ha un unico *data plane* regionale distribuito su più zone di disponibilità. Questo comporta che nell'utilizzo di servizi regionali il cliente non deve entrare nel merito della zona di disponibilità utilizzata e ha una visione più astratta indipendente dalla divisione in zone di disponibilità. I servizi regionali, come alcuni servizi zonali, hanno poi un unico endpoint di accesso al *control plane* al livello regionale. Un esempio di servizio regionale è Amazon Dynamo DB, in cui il cliente non deve gestire il meccanismo di replicazione delle copie nelle singole zone di disponibilità. Infatti, è il servizio stesso che, sfruttando l'indipendenza delle singole zone di disponibilità, si occupa di ridondare i dati per aumentare la resilienza e minimizzare il rischio di indisponibilità dei dati.

L'ultima categoria è quella dei **servizi globali**, ovvero quell'insieme ristretto di servizi AWS le cui risorse non sono specifiche di una singola regione o zona di disponibilità. I servizi globali, come per altre due categorie, mantengono la separazione tra *control plane* e *data plane*, però il *data plane* è è distribuito al livello globale, e il *control plane*, per la maggior parte di essi, è ospitato in una sola region AWS. Ad esempio, il servizio di Identity and Access Management (IAM) di AWS è un servizio globale, con un unico endpoint di accesso al *control plane* situato nella region AWS situata in North Virginia (`us-east-1`), e data plane distribuito globalmente. La distinzione in categorie dei servizi AWS, appena illustrata, è fondamentale per soddisfare i requisiti di data residency. Infatti, anche se per localizzare correttamente dati in Unione Europea è necessario interdire l'accesso a region non ammesse, bisogna tenere conto dell'esistenza dei servizi globali, in maniera da non bloccare l'accesso al loro *control plane* e causare problemi di utilizzo del Cloud.

Per concludere, l'ultimo aspetto importante da sottolineare per una piena comprensione degli strumenti e della struttura del Cloud AWS è il concetto di account AWS. Nel Cloud Amazon un account è inteso come un contenitore di risorse e utenti isolato rispetto ad altri account, anche se appartenenti alla stessa organizzazione, introducendo un primo livello di sicurezza nel Cloud. Quindi, la definizione di account AWS permette anche di sottolineare la distinzione tra due concetti che apparentemente potrebbero risultare identici, ovvero quello di account e di utente. Infatti, un utente AWS è un'identità creata all'interno di un account attraverso il servizio di Identity and Access Management di AWS, e un account AWS può contenere più

utenti AWS. Tra gli utenti contenuti all'interno dell'account AWS è sempre presente il **root user**, ovvero l'utente privilegiato di default con cui si accede all'account, dopo il login. La distinzione tra utente e account apre a due possibilità di strutturazione e configurazione delle identità all'interno del Cloud AWS, cioè l'ambiente a singolo account e l'ambiente multi-account. Nell'ambiente a singolo account si utilizza un unico account AWS per tutta l'organizzazione, e si creano gli utenti, gruppi e ruoli necessari a riprodurre nel servizio di IAM l'organigramma. Al contrario, nell'ambiente multi-account esistono più account AWS raggruppati all'interno di una singola organizzazione, e ognuno di questi è isolato rispetto agli altri. Come si vedrà nei prossimi paragrafi, mentre con le policy AWS si può utilizzare anche un ambiente a singolo account, invece utilizzando AWS Control Tower è necessario impostare un ambiente multi-account.

5.2 Strumenti AWS per la localizzazione dei dati

5.2.1 AWS Policies

AWS IAM è un servizio centralizzato di creazione e gestione delle identità e dei permessi per l'accesso degli utenti alle singole risorse implementate nel proprio Cloud. Esso permette di gestire l'accesso degli utenti, dei gruppi e dei ruoli alle risorse nel Cloud mediante la creazione e l'assegnazione di policy sia alle risorse che alle identità. Un utente IAM è un'identità creata all'interno di account AWS che dispone di determinate autorizzazioni che gli permettono di compiere azioni sulle risorse nel Cloud. Tipicamente le identità degli utenti sono associate a delle persone specifiche o dipendenti dell'organizzazione e possono avere associate sia credenziali temporanee che credenziali a lungo termine.

Tuttavia, le sole identità non sono sufficienti per una gestione accurata delle autorizzazioni, perché è a volte un utente potrebbe aver bisogno di compiere azioni per cui i permessi sono tra loro incongruenti. Allora il sistema IAM di AWS definisce anche il concetto di ruolo, ovvero un'identità che dispone di autorizzazioni specifiche, ma non è associata a una persona o dipendente specifico. In questa maniera, ogni utente può avere assegnati ruoli diversi per compiere operazioni diverse anche se i permessi associati ai ruoli sono tra loro incongruenti. Inoltre, non è necessario assegnare in maniera permanente i ruoli agli utenti, ma è possibile per un utente assumere il ruolo con i permessi sufficienti per svolgere le azioni richieste e mantenerlo per un periodo di tempo limitato. Allo stesso modo, IAM consente di gestire utenti simili in maniera aggregata specificando le autorizzazioni per tutti gli utenti una sola volta per tutti. Infatti, in IAM esiste anche il concetto di gruppo di utenti, ovvero un entità IAM che raggruppa un insieme di utenti simili, a cui è possibile assegnare delle policy che conteranno i permessi da associare a tutti gli utenti del gruppo. È

importante sottolineare che a differenza di utenti e ruoli, i gruppi non sono delle identità con cui è possibile effettuare l'accesso ai servizi AWS, ma uno strumento finalizzato alla gestione simultanea di più identità.

I concetti di gruppo, di ruolo e di utente permettono di ricreare, all'interno del servizio di Identity and Access Management, la struttura organizzativa della Pubblica Amministrazione che migra su Cloud, e ad AWS di fornire meccanismi di autenticazione. Il sistema IAM di AWS a queste funzionalità aggiunge anche la gestione delle autorizzazioni che viene effettuata attraverso le *policy AWS*. Una *policy AWS* è un oggetto che quando viene associato a una identità o gruppo o una risorsa ne definisce le autorizzazioni. Quando un utente o ruolo IAM richiede l'accesso a una risorsa, sono controllate le autorizzazioni espresse nelle policy assegnate all'utente o ruolo e alle risorse stesse, e sulla base di quelle l'accesso è consentito o negato. Tipicamente, le *policy AWS* sono archiviate nel Cloud come documenti in formato JSON, e si dividono in due macro-tipologie. Una tipologia è rappresentata dalle policy gestite (*policy managed*), ovvero delle policy che esistono come oggetti indipendenti rispetto ai principali a cui sono attaccate. Esse si distinguono in:

- **AWS Managed Policies**: sono policy definite da AWS secondo le migliori pratiche di sicurezza e immediatamente pronte per essere attaccate a dei principali.
- **Customer Managed Policies**: sono le policy gestite dal cliente, definite dall'utilizzatore dei servizi Cloud AWS, attraverso un editor testuale o il generatore di policy AWS.

L'altra tipologia è quella delle *policy inline*, che non esistono come oggetto singolo, ma hanno una relazione uno a uno con il principale per cui sono state definite. Infatti, nel momento in cui il principale a cui è associata una *inline policy* viene eliminato, anche la policy associata viene cancellata.

Gli elementi fondanti di una policy AWS che può essere assegnata a un utente, ruolo o risorsa all'interno del Cloud sono i cosiddetti *statements*, ovvero degli oggetti strutturati, ognuno dei quali contiene delle informazioni riguardanti un permesso che la policy nega o concede. Ogni policy è composta da uno o più *statements* che sono posti in OR logico tra loro e sono preceduti, opzionalmente, da un'informazione sulla versione della policy. Ogni *statement* contiene più informazioni, alcune delle quali vanno specificate obbligatoriamente, mentre altre sono opzionali. Di seguito si elencano tutti campi che contiene uno *statement*, dove tutti i campi obbligatori sono quelli sottolineati:

- `Sid`: è un campo stringa contenente l'ID univoco associato allo statement
- `Effect`: può assumere come valori solo `Allow`, nel caso in cui lo statement consenta l'accesso, o `Deny`, nel caso in cui lo neghi. Dato che in AWS, per

garantire una maggiore sicurezza, tutte le azioni sono negate di default, a meno che non ci sia una policy che lo consenta esplicitamente, di solito in questo campo si utilizza il valore `Allow`.

- `Principal`: tale campo è obbligatorio in tutte le policy assegnate alle risorse e indica l'account, l'utente, il ruolo o il gruppo a cui si consente o nega l'accesso alla risorsa.

- `Action`: è una lista di una o più azioni che lo statement della policy AWS consente o nega.

- `Resource`: è un campo obbligatorio in tutte le policy assegnate alle identità o ai gruppi. Esso indica l'insieme di risorse su cui sono consentite o bloccate le azioni espresse nello statement.

- `Condition`: indica le circostanze che devono verificarsi affinché lo statement conceda i permessi specificati

Chiaramente, anche se la struttura di base è identica per tutte le policy definite all'interno dell'ambiente AWS, comunque queste si differenziano in vari tipi o a seconda dell'oggetto a cui sono assegnate, o in base al modo in cui sono combinate con altre policy. In particolare, ai fini della localizzazione dei dati sul territorio dell'Unione Europea è stato importante approfondire i quattro seguenti tipi di policy AWS:

- **Identity-based policies**: esse sono assegnabili solo a identità IAM e stabiliscono quali azioni possono essere compiute su una certa risorsa da una certa identità (utente, ruolo o gruppo di utenti). Le policy basate su identità possono essere sia policy gestite sia policy inline.

- **Resource-based policies**: stabiliscono quali permessi ha un certo utente, ruolo o gruppo di utenti su una certa risorsa. Queste policy possono essere definite solo come policy inline attaccate a una risorsa, e nel momento in cui si fa il deprovisioning della risorsa, la policy smette di esistere.

- **Permission boundaries**: definiscono un limite ai permessi che le policy di tipo identity-based possono concedere a un'identità IAM.

- **Service Control Policies (SCPs)**: Esse si applicano per gli account membri di un'organizzazione, creata con il servizio AWS Organizations, oppure per gli account membri di una singola unità organizzativa. Tali policies stabiliscono un limite ai permessi che una policy identity-based o resource-based può concedere alle identità definite nell'account dell'organizzazione o dell'unità organizzativa.

Mentre i primi due tipi di policy sono molto semplici da comprendere, è necessario evidenziare altre proprietà dei Permission boundaries e delle Service Control Policies, vista anche la loro utilità per implementare una corretta localizzazione dei dati.

Iniziando dai permission boundaries, è bene sottolineare che queste non sono policy che concedono dei permessi in maniera esplicita, ma restringono l'insieme dei permessi effettivi concessi ad un utente o ruolo attraverso le policy identity-based. Si supponga che una policy basata su identità conceda a un utente accesso in lettura e scrittura a un bucket S3 e che all'identità sia assegnata un'altra policy, come permission boundary, che permette l'utilizzo di istanze EC2 e la lettura degli oggetti nello stesso bucket di S3. Anche se la policy basata su identità permette la scrittura sul bucket S3 all'utente, comunque l'azione verrà bloccata perché nel Permission boundary assegnatogli non è consentito esplicitamente di scrivere sul bucket. Quindi, all'atto pratico, i reali permessi concessi a un'identità su AWS sono l'intersezione dei permessi concessi da tutte le identity-based policy assegnate e dai permission boundary ad essa associate, come indicato nella Figura 5.1. Tale situazione rimane

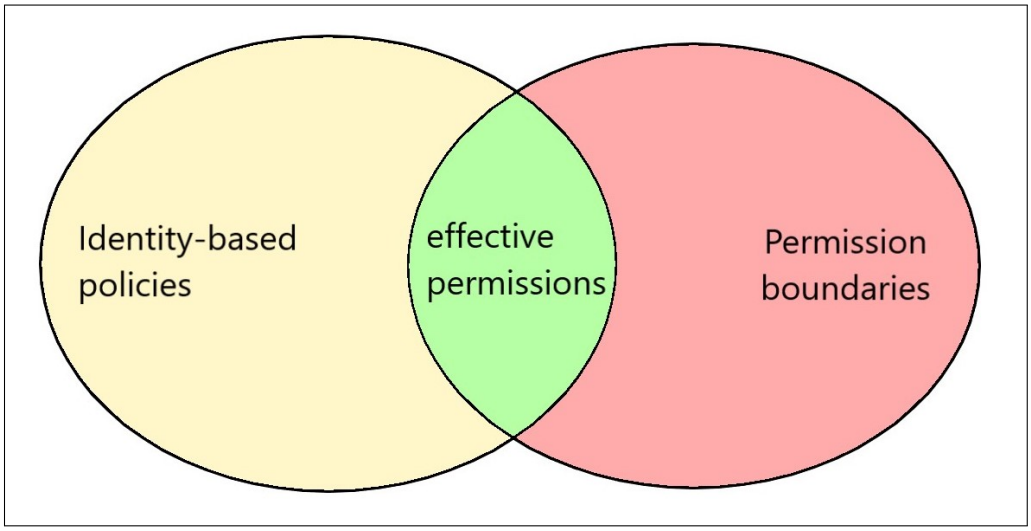

Figura 5.1: Insieme di permessi effettivi in presenza di permission boundaries e policy identity-based

valida nel momento in cui non sono definite delle resource-based policies sulle risorse su cui un principale vuole compiere un'azione. Infatti, durante la valutazione dei permessi, in presenza di policy inline sulle risorse, ai permessi effettivi indicati prima si aggiungono tutti i permessi concessi al principale, che ha effettuato la richiesta, nella policy basata su risorse.

L'evoluzione del Permission boundary è rappresentata dalla Service Control Policy, che però ha un effetto più vasto, dato che è applicata anche a più account AWS all'interno di una stessa organizzazione. Come i Permission Boundaries, anche le Service Control Policies non concedono direttamente dei permessi agli utenti e ruoli

definiti negli account target, ma limitano il numero di permessi concessi alle identità. I permessi effettivi vanno concessi agli utenti utilizzando sempre le identity-based o le resource-based policy. Tuttavia, Le SCPs, a differenza dei Permission boundaries, hanno impatto anche sulle resource-based policies definite nelle risorse interne agli account dell'organizzazione o dell'unità organizzativa a cui sono associate. Ad esempio, si ponga che in un *account A* sia definita una policy basata su risorse, che permette a tutti gli utenti l'accesso in lettura a un bucket di S3, creato all'interno dello stesso account. Contemporaneamente, si ponga che l'*account A* faccia parte di un'organizzazione per cui è definita una SCP che impedisce le azioni di lettura dirette sui bucket di S3. Allora, qualsiasi utente richieda di compiere un'azione di lettura del bucket, vedrà la sua richiesta negata per effetto della SCP. Al contrario,

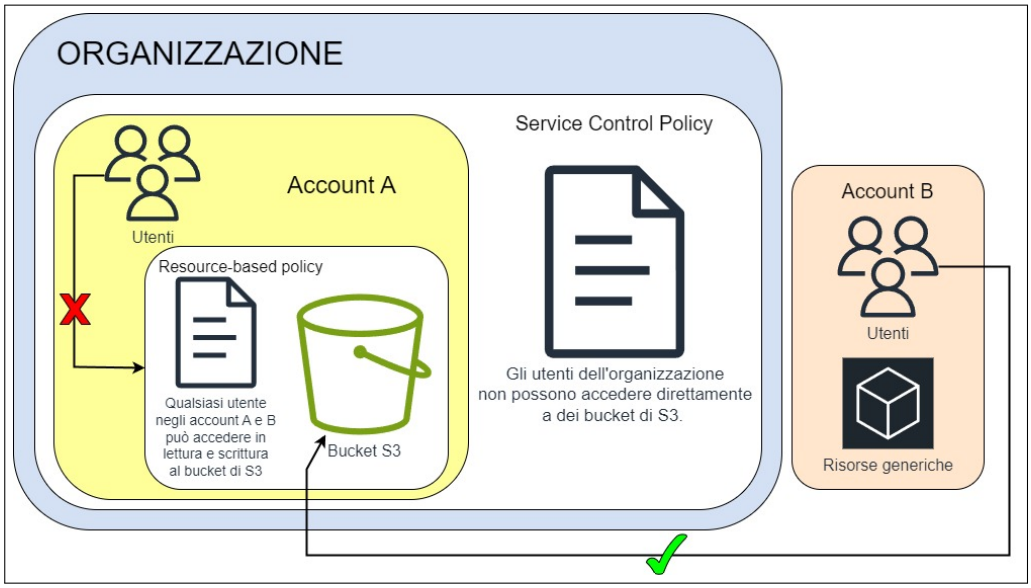

Figura 5.2: Funzionamento di una SCP rispetto a una resource-based policy

se la policy basata su risorse concede l'accesso a un bucket definito nell'*account A* agli utenti creati in *account B*, che è esterno all'organizzazione, allora per loro sarà possibile portare a termine le richieste di lettura del bucket. Tale esempio, esplicato anche dalla Figura 5.2, evidenzia anche che le Service Control Policies non hanno valenza al di fuori dell'organizzazione o dell'unità organizzativa a cui sono applicate. Inoltre, gli effetti della Service Control Policy sono validi anche per l'utente root dell'account e non solo per i normali utenti IAM.

In aggiunta è possibile applicare contemporaneamente più Service Control Policies a ogni livello dell'organizzazione. Infatti, è possibile assegnare una SCP a tutta l'organizzazione, indicando un limite ai permessi di tutti gli account, e assegnare una SCP a una singola unità organizzativa, per restringere ulteriormente il numero massimo di permessi concesso agli account in essa contenuti. In sostanza, nel momento in cui un utente IAM all'interno di un account vuole compiere un'azione, questa

deve essere permessa sia dalla policy identity-based assegnatagli, sia da tutte le Service Control Policies definite a ai livelli superiori. Quindi, se una certa azione è esplicitamente bloccata, o non è esplicitamente permessa, in una qualsiasi delle Service Control Policies a livelli superiori rispetto a quello degli utenti dell'account, allora, anche se l'azione è permessa dalla policy basata su identità, essa viene bloccata. Inoltre, è possibile combinare l'utilizzo delle Service Control Policies con l'utilizzo di Permission Boundaries, al fine di avere un controllo ancora più granulare sul numero massimo di permessi concessi a un utente o ruolo IAM. Nello scenario più completo, in cui sono utilizzate policy basate su identità, Service Control Policies e Permission Boundaries, se viene richiesta un'azione da un utente IAM, questa deve essere esplicitamente permessa (o non esplicitamente negata) da tutte e tre le policy.

Le Service Control Policy e i Permission Boundaries, rappresentano un ottimo strumento per implementare la corretta localizzazione dei dati su territorio UE, specialmente per il modo in cui definiscono i permessi effettivi associati a un'identità. Infatti, in un ambiente a singolo account, i permission boundaries e le policy basate su identità, sono già uno strumento sufficiente per restringere l'insieme delle region in cui è possibile fare il provisioning di risorse, per tutti gli utenti di un account, privilegiati e non. Le policy basate su identità sono definite in maniera tale da impedire lo svolgimento di tutte le azioni, correlate a un largo insieme servizi AWS, in tutte le regioni che non si trovano in Unione Europea, e l'attivazione di nuove regioni extra-UE. Queste policy saranno poi assegnate a tutti gli utenti compresi quelli privilegiati. Successivamente, per permettere agli utenti IAM con privilegi di amministratore di poter svolgere le loro mansioni, come ad esempio la definizione delle policy IAM per gli utenti ordinari, evitando che questi possano assegnarsi privilegi eccessivi e utilizzare risorse in regioni non ammesse, si definiscono dei Permission Boundaries. In particolare, si nega qualsiasi azione di cambio delle policy assegnate agli utenti con privilegi, compresi se stessi. Definendo, le policy basate su identità e i Permission Boundaries, nella maniera indicata è possibile forzare la localizzazione dei dati e il provisioning dei servizi nelle region AWS europee, senza però creare problemi di utilizzabilità dei servizi Cloud agli utenti dell'Amministrazione.

Allo stesso modo in un ambiente multi-account è possibile raggiungere lo stesso obiettivo utilizzando, oltre a policy basate su identità e Permission boundaries, le Service Control Policies. L'utilità delle SCPs, risiede nel fatto che esse possono essere applicate sia al livello di una singola unità organizzativa che contiene più account e più utenti, sia al livello dell'intera organizzazione. Quindi, con la definizione di una Service Control Policy adeguata è possibile consentire a tutti gli account dell'organizzazione l'accesso ai servizi AWS solo nelle region localizzate all'interno dell'Unione Europea. In questa maniera, se in un certo account un utente si attribuisce, attraverso una identity-based policy, un insieme di privilegi troppo largo, che consente il provisioning di risorse in una region esterna all'UE, comunque ogni azione in una regione extra-

UE viene bloccata dalla SCP. Inoltre, è possibile combinare l'azione di Permission Boundary e Service Control Policies per implementare ulteriori restrizioni, che vincolino solo determinati utenti, o interi account, a utilizzare servizi e localizzare i dati solo nelle regioni all'interno della propria nazione. La garanzia di sicurezza che offrono Permission boundaries e Service Control Policies per la localizzazione dei dati, unita alla loro capacità di non creare problemi di utilizzo del Cloud nelle attività quotidiane di un'organizzazione, le rendono degli strumenti adatti per forzare la localizzazione dei dati in UE.

5.2.2 AWS Control Tower

La configurazione di un ambiente multi-account da zero sul Cloud AWS richiede la conoscenza approfondita di molti servizi AWS, tra cui AWS Organizations, e una certa maturità di utilizzo del Cloud da parte dei dipendenti dell'Amministrazione. Lo sforzo iniziale da compiere per la configurazione corretta di questo ambiente potrebbe essere rilevante, senza il supporto di servizi di consulenza, specialmente per quelle Amministrazioni Pubbliche che non hanno mai utilizzato servizi Cloud per le loro attività quotidiane. Inoltre, la gestione corretta e sicura di un ambiente multi-account richiede l'implementazione di molte best practices attraverso vari strumenti AWS, come Config, CloudFormation e le stesse Service Control Policies. Per evitare che un'Amministrazione, nell'ipotesi in cui riesca a configurare un ambiente multi-account, lo renda non sicuro, esponendosi ad attacchi o incidenti di sicurezza, è consigliabile che la configurazione di un ambiente multi-account sia svolta attraverso il servizio **AWS Control Tower**.

AWS Control Tower è un servizio gestito di AWS che permette la costruzione di un ambiente multi-account o *landing zone* che aderisce alle migliori pratiche di sicurezza, definite nei più importanti framework di cybersecurity. Esso, utilizzando altri servizi AWS come Organizations, Service Catalog e IAM Identity Center, permette di costruire una *landing zone* in breve tempo, e applicare controlli di sicurezza mutuati dai migliori framework per mantenerla sicura. Oltre a fornire dei controlli di sicurezza, Control Tower mette a disposizione anche tutta una serie di funzionalità di gestione dell'organizzazione e degli account nel Cloud AWS. Infatti, AWS Control Tower mette a disposizione tutte le funzionalità già presenti in AWS Organizations, come la possibilità di creare nuovi account AWS e nuove unità organizzative, per riprodurre al meglio l'organigramma dell'organizzazione. Inoltre, è possibile collegare Control Tower con un servizio di gestione delle identità esistente, anche presso altri Cloud Provider, per integrare lo strumento con i servizi preesistenti nella propria organizzazione. Altrimenti, nel caso in cui non si abbia già un proprio identity provider, Control Tower è in grado, attraverso il servizio AWS IAM Identity Center, di creare e configurare autonomamente un servizio di directory su AWS.

Il deploy di Control Tower e di tutte le risorse chiave necessarie per il suo corretto funzionamento avviene all'interno di una singola region AWS, denominata *home region*. Essa viene scelta durante il processo guidato di set up della *landing zone* e non può essere cambiata in seguito, motivo per il quale va scelta in maniera aderente ai requisiti normativi. Definita la *home region* è consigliabile anche selezionare, sempre in aderenza alle normative, anche altre region aggiuntive, per estendere anche lì la governance di Control Tower e aumentare sia la sicurezza che la resilienza del proprio ambiente. Al momento della creazione della *landing zone* all'interno delle region scelte, Control Tower configura anche una struttura organizzativa di default, composta da due unità organizzative.

La prima unità organizzativa, chiamata **Security**, contiene due account condivisi utilizzati per tracciare e monitorare lo stato dell'organizzazione:

- **Log Archive Account**: in esso viene definito un bucket di S3 che contiene i log delle attività e delle configurazioni delle risorse in tutti gli account della *landing zone*.

- **Audit Account**: esso deve essere accessibile solo al team di sicurezza dell'organizzazione, in quanto ha assegnati dei permessi di accesso a tutti gli account della *landing zone*. Infatti, è possibile accedervi in lettura per raccogliere delle informazioni con cui condurre audit di sicurezza, o con permessi di amministratore, attraverso precisi strumenti AWS, per rimediare a configurazioni errate e potenzialmente vulnerabili.

Inoltre, alla mail associata all'account di Audit sono inviate anche delle notifiche di sicurezza, riguardanti eventuali configurazioni potenzialmente vulnerabili delle risorse all'interno degli account della *landing zone*. La seconda unità organizzativa creata è quella che ospiterà gli account dell'organizzazione, e il nome assegnatogli di default è **Sandbox**. Infine, all'interno dell'organizzazione viene compreso anche l'account AWS che ha lanciato il deploy della *landing zone* di Control Tower. Tale account viene definito come *Management Account* ed è quello a cui sono assegnati tutti i permessi di gestione e di amministrazione sull'ambiente gestito da Control Tower. Esso ha la facoltà di creare nuove unità organizzative e nuovi account sotto la governance di Control Tower e di abilitare sulle unità organizzative i controlli di sicurezza già predisposti da Control Tower.

Terminato il processo di configurazione iniziale della *landing zone* dall'account di gestione di Control Tower è possibile visualizzare la dashboard dello strumento che presenta una situazione riassuntiva sulla struttura dell'organizzazione e sulle risorse attivate. Essa è molto utile per fornire all'amministratore di Control Tower una visione di insieme per comprendere quali risorse in quali account sono state configurate in maniera potenzialmente vulnerabile e quanti controlli di sicurezza

sono attivati. Dalla dashboard è possibile accedere al cuore dello strumento, ovvero la libreria contenente tutti i controlli di sicurezza predefiniti di Control Tower, applicabili a una o più unità organizzative all'interno dell'organizzazione. I controlli sono categorizzati secondo moltissimi aspetti, come il servizio AWS a cui si applicano, l'obiettivo di sicurezza, la tipologia di controllo, il framework da cui sono tratti e così via. Utilizzando questa categorizzazione è possibile ricercare i controlli in maniera efficiente per esaminarli e decidere quali attivare.

Ogni controllo ha associata una scheda descrittiva che ne elenca in maniera dettagliata tutte le caratteristiche. In particolare, è fondamentale sottolineare che la scheda di ogni controllo riporta una descrizione di alto livello, senza dettagliarne l'implementazione. Tale aspetto è molto vantaggioso perché permette di selezionare il controllo sulla base di aspetti di alto livello, senza per forza dover comprendere fino in fondo lo strumento AWS che lo implementa nel Cloud. Per chiarire meglio questo aspetto si consideri la Figura 5.3, che riporta la scheda descrittiva di un controllo di Control Tower. Nella scheda del controllo, alla voce "Framework" sono riportati

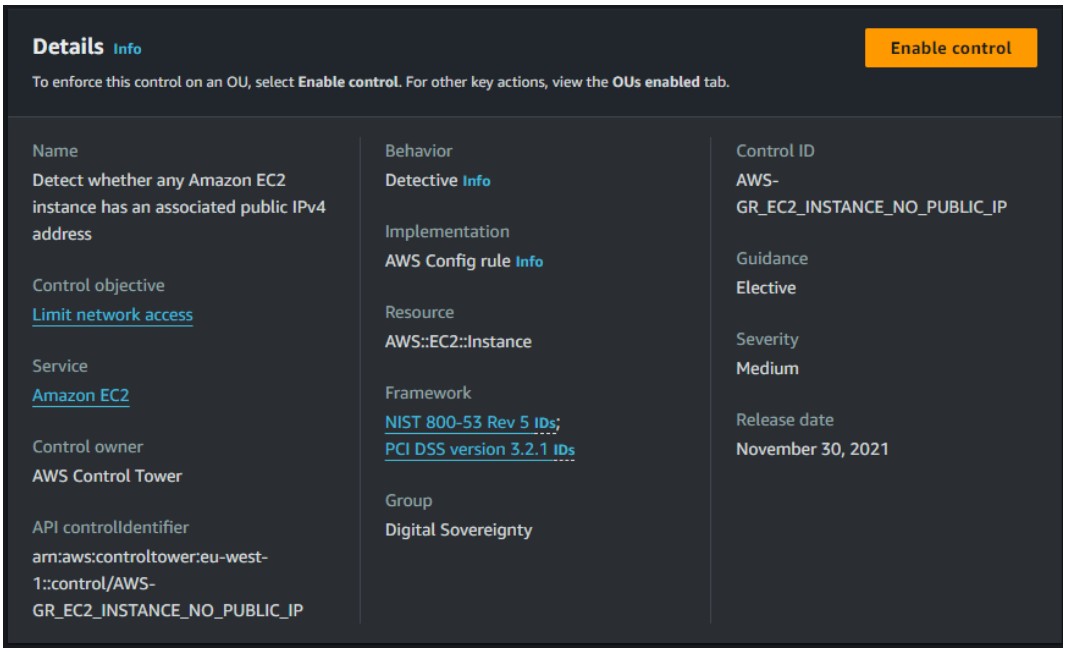

Figura 5.3: Scheda descrittiva di un controllo di sicurezza

gli standard e i framework di sicurezza presi come riferimento per lo sviluppo del controllo di Control Tower. In particolare, cliccando su `IDs` è possibile visualizzare tutti controlli del framework o dello standard di sicurezza utilizzato come riferimento. Questo aspetto facilita la scelta dei controlli da attivare nella propria *landing zone*, perché permette all'Amministratore di selezionarli sulla base del framework a cui sono riferiti e dei controlli del framework implementati. Tale caratteristica è molto utile nei settori regolati in cui l'aderenza a determinati framework e standard è un

requisito normativo.

Nonostante siano varie le caratteristiche interessanti dei controlli in AWS Control Tower, le due peculiarità più importanti di ogni controllo sono il *behavior*, ovvero come agisce il controllo, la *guidance*, ovvero quanto è consigliato attivarlo. Iniziando dalla seconda caratteristica, Control Tower permette di distinguere controlli in **obbligatori**, **raccomandati**, **opzionali**. I controlli obbligatori sono quelli che vengono sempre attivati all'interno della *landing zone* governata da Control Tower. Tali controlli sono applicati a tutte le unità organizzative già dal momento in cui viene effettuato per la prima volta il deploy della *landing zone* e non possono essere disattivati dall'amministratore di Control Tower. Al contrario, i controlli opzionali possono essere attivati o disattivati in qualsiasi unità organizzativa e di solito consentono di rilevare o bloccare delle azioni che di solito non sono consentite in un Cloud AWS. A metà tra queste due tipologie si collocano i controlli raccomandati, ovvero controlli non obbligatori, che però servono per l'implementazione di best practices comuni e richieste in ambienti multi-account. Passando al *behavior*, Control Tower cataloga i controlli in tre categorie: **controlli di rilevamento**, **controlli proattivi** e **controlli preventivi**. Ogni tipologia di controllo viene implementata da Control Tower orchestrando le funzionalità di un altro servizio dell'ecosistema Cloud di AWS.

I **controlli di rilevamento** permettono di rilevare configurazione errate o non sicure delle risorse AWS all'interno degli account sotto la governance di Control Tower. Ogni controllo definisce una corretta configurazione di un aspetto di una qualsiasi risorsa nel Cloud AWS. Se viene rilevata una risorsa AWS la cui configurazione si discosta da quella corretta, la risorsa viene marcata come *Noncompliant* e viene inviato un alert sia alla dashboard di Control Tower, sia all'indirizzo mail associato all'account di Audit. La maggior parte dei controlli appartenenti a questa tipologia riguarda singole risorse, anche se ultimamente sono stati aggiunti anche controlli che rilevano configurazioni errate di gruppi di risorse. Per implementare questa tipologia di controlli, AWS Control Tower si avvale delle regole del servizio AWS Config, ovvero un servizio Cloud che fornisce una panoramica dettagliata su tutte le risorse AWS presenti all'interno di un account. Esso consente di monitorare la configurazione delle risorse richieste all'interno di un account AWS, e di impostare delle regole che specificano qual è la corretta configurazione delle stesse e generano un alert qualora una risorsa sia configurata in maniera non corretta. Nel momento in cui si attiva un controllo di rilevamento su una certa unità organizzativa, Control Tower attiva AWS Config in tutti gli account all'interno dell'unità e attiva la regola di Config che implementa il controllo attivato. In questa maniera, non solo viene inviato l'alert all'amministratore sulla dashboard di Control Tower, ma viene inviata una notifica sulla dashboard di AWS Config anche ai membri dell'account che hanno richiesto la risorsa. Anche se non prevengono l'implementazione errata di risorse nel Cloud, i controlli di rilevamento sono un ottimo strumento per facilitare tempestive

azioni di correzione delle risorse, anche automatizzate.

I **controlli proattivi** impediscono il provisioning di un insieme di risorse con determinate caratteristiche, nel momento in cui queste non aderiscono a specifici requisiti di sicurezza. A differenza dei controlli di rilevamento, i controlli proattivi bloccano il deploy di risorse configurate in maniera potenzialmente non sicura. Tali controlli però non si applicano a singole risorse ma a gruppi di risorse che nel Cloud AWS sono definiti stack. Infatti, AWS, per le organizzazioni che hanno bisogno di effettuare il provisioning di una grande quantità di risorse in tempi brevi, mette a disposizione uno strumento molto potente chiamato CloudFormation. CloudFormation è un servizio gestito di AWS che permette di effettuare il provisioning di più risorse contemporaneamente, solo specificandone le caratteristiche. Infatti, attraverso la definizione di un template, ovvero un file JSON in cui si descrivono gli attributi delle istanze di cui dovrà essere fatto il deploy, CloudFormation è in grado di provvedere autonomamente al deploy e alla configurazione delle risorse desiderate. Inoltre, a seguito dell'implementazione, le risorse possono essere gestite tutte insieme, poiché sono raccolte in un'unica unità chiamata stack, che facilita la gestione aggregata di grandi insiemi di risorse.

I controlli proattivi hanno il compito di bloccare il deploy di uno stack, nel momento in cui esso contiene una risorsa che non è configurata correttamente in aderenza al controllo stesso. Infatti, ogni controllo proattivo viene implementato attraverso una regola, detta *CloudFormationRule*, che verifica prima del deploy di uno stack se le risorse coinvolte aderiscono a una configurazione corretta definita nel controllo stesso. Nel caso in cui le risorse nello stack rispettano la configurazione corretta definita nel controllo, la *CloudFormationRule* permette il provisioning delle risorse, altrimenti lo blocca. L'utilità di questi controlli risiede nel fatto che il provisioning viene bloccato direttamente, senza bisogno dell'intervento diretto dell'amministratore di Control Tower, oppure dell'utente che ha richiesto il deploy di un template di CloudFormation. Tuttavia, il principale svantaggio di questa tipologia di controlli è che non hanno alcun effetto sulle richieste di risorse effettuate attraverso un servizio diverso da CloudFormation. In quel caso è necessario integrare il controllo proattivo attivando un opportuno controllo di rilevamento che controlla la stessa tipologia di risorse.

Infine, i **controlli preventivi** servono per garantire che gli account appartenenti alle unità organizzative su cui sono attivati rimangano in uno stato sicuro, ovvero che mantengano la conformità rispetto a determinate regole di sicurezza. Questa tipologia di controlli si occupa, quindi, di bloccare tutte le azioni che determinano una violazione di precise regole di sicurezza che sono espresse attraverso delle policy. In particolare, i controlli preventivi sono implementati attraverso delle **Service Control Policies**, il cui funzionamento è già stato descritto nel paragrafo 5.2.1. Quando si attiva un controllo preventivo su una unità organizzativa gestita di Control

Tower, il risultato che si ottiene è che viene assegnata all'unità stessa la Service Control Policy definita nel controllo. In questa maniera, nel caso in cui un utente qualsiasi, creato in un account appartenente all'unità, abbia attribuiti dei permessi per compiere un'azione che viola il controllo preventivo, l'azione della Service Control Policy limita i permessi dell'utente, impedendo qualsiasi azione che danneggi la conformità dell'account.

Dalla descrizione delle loro caratteristiche e del loro funzionamento i controlli messi a disposizione da AWS Control Tower, sono uno strumento fondamentale anche per forzare la localizzazione dei dati e dei servizi delle Amministrazioni in UE. Control Tower mette a disposizione più di cinquecento controlli di sicurezza mutuati da framework e standard noti in tutto il mondo, e di questi più di duecento sono controlli che contribuiscono alla *sovranità digitale* dell'organizzazione che utilizza il Cloud, ovvero al controllo degli asset digitali sul Cloud. Tra questi controlli sono presenti anche controlli specifici che permettono di aumentare il controllo dell'Amministrazione sulla localizzazione dei propri dati e servizi migrati all'interno del Cloud AWS. Questi controlli definiti in AWS con il nome di ***Data residency controls***, sono un insieme di circa venti controlli di sicurezza che permettono di rilevare situazioni che possono portare a una errata localizzazione dei dati e generare dei flussi di dati non ammessi verso altre regioni AWS situate in territori extra-UE.

I due *Data residency controls* più importanti sono quelli che impediscono l'accesso a qualsiasi servizio AWS al di fuori delle region controllate da Control Tower, ovvero i cosiddetti *Region Deny controls*. Questi due controlli appartengono alla categoria dei controlli preventivi, e si distinguono per il livello dell'organizzazione a cui sono applicati. Il primo, ovvero quello con ID `AWS-GR_REGION_DENY` si applica al livello dell'intera landing zone, impedendo a tutti gli account all'interno dell'organizzazione gestita da Control Tower di accedere ai servizi AWS in una qualsiasi region non governata da Control Tower. Il secondo, con ID `CT.MULTISERVICE.PV.1`, si applica a una singola unità organizzativa e applica gli stessi divieti del primo solo agli account che ne fanno parte. Questi due controlli sono già un primo strumento che fornisce un grande aiuto alle Amministrazioni per localizzare i dati solo all'interno dell'Unione Europea. Infatti, già abilitando uno di questi controlli di sicurezza, a seconda del livello a cui si vuole agire, si riesce ad avere la certezza che i dipendenti dell'Amministrazione non siano in grado, nemmeno per errore, di richiedere risorse in region extra-UE. Tuttavia, non basta attivare solo uno di questi due controlli non dà l'assoluta certezza che i dati delle Amministrazioni rimangano in UE, perché i due controlli non impediscono flussi di dati non ammessi verso internet. Quindi, come si discuterà in seguito nel paragrafo 5.3.2, sarà necessario attivare ulteriori controlli per avere una maggiore sicurezza che i dati e i servizi delle Amministrazioni rimangano confinati all'interno dell'UE.

5.3 Implementazione degli strumenti di Data Residency

5.3.1 Policy IAM per la data localization

L'analisi delle policy AWS, effettuata nel paragrafo 5.1.2, stabilisce che queste sono uno strumento adatto per garantire la localizzazione dei dati e servizi delle Amministrazioni in Unione Europea, proponendo anche un possibile modo di utilizzo. Tuttavia, per formulare una valutazione più completa sullo strumento messo a disposizione da AWS è necessario implementare l'idea proposta in precedenza per analizzarne eventuali criticità e metterne in risalto i punti di forza. Per cui, si è deciso di formulare delle policy AWS capaci di riprodurre lo scenario proposto in precedenza. Analizzando lo scenario descritto nel paragrafo 5.2.1, si deduce che le policies da definire devono soddisfare quattro requisiti fondamentali:

- Impedire l'accesso ai servizi AWS in tutte le regioni extra-UE.
- Garantire l'accesso ai servizi globali di AWS anche in regioni extra-UE.
- Impedire l'attivazione di regioni opt-in non situate all'interno dell'Unione Europea.
- Impedire a tutti gli utenti amministratori che hanno accesso al servizio di Identity & Access Management, di cambiare le policy assegnate a tutti gli utenti con privilegi.

Il secondo requisito, anche se apparentemente sembra violare i requisiti di data residency richiesti alle Amministrazioni, è necessario per impedire problemi di utilizzabilità del Cloud AWS. Infatti, limitare l'accesso anche per tutti i servizi globali risulterebbe nell'impossibilità, da parte dell'Amministrazione, di utilizzare quei servizi, dato che hanno un unico endpoint di accesso non per forza collocato in una region UE. In merito, si rimanda a ulteriori approfondimenti nelle valutazioni finali.

I primi due requisiti possono essere soddisfatti con un'unica policy AWS, riportata in Listato 5.1., utilizzando in maniera intelligente una proprietà messa a disposizione dell'ambiente AWS, ovvero `NotAction`. Analizzando in dettaglio la policy formulata, si nota che essa contiene uno statement con effetto `Deny`, che normalmente impedisce una serie di azioni. Tuttavia, la proprietà `Action` è stata sostituita con la proprietà complementare `NotAction`, alla quale si associa una lista di azioni eseguibili nel Cloud AWS. Inoltre, nella policy si associa al campo `Resource` la wildcard `*` per indicare la policy ha effetto su tutti i tipi di risorse in AWS. La conseguenza principale di questa combinazione è che **sono impedite tutte le azioni su risorse AWS ad eccezione di quelle indicate nella clausola `NotAction`**. Chiaramente, nel campo `NotAction`, sono riportate, per ogni servizio globale che utilizza l'organizzazione, tutte le azioni che si possono compiere in quei servizi, attraverso la sintassi `Nome_Servizio:*`, dove

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideRequestedRegions",
            "Effect": "Deny",
            "NotAction": [
                "iam:*",
                "access-analyzer:*",
                "sts:*",
                "organizations:*",
                "globalaccelerator:*",
                "waf:*",
                "importexport:*",
                "cloudfront:*",
                "route53:*",
                "route53domains:*",
                "support:*",
                "account:*",
                "payments:*",
                "freetier:*",
                "invoicing:*",
                "tax:*",
                "consolidatedbilling:*",
                "purchase-orders:*",
                "sustainability:*",
                "pricing:*",
                "budgets:*",
                "ce:*",
                "billing:*",
                "bcm-data-exports:*",
                "cur:*",
                "cost-optimization-hub:*",
                "savingsplans:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-south-1",
                        "eu-west-1",
                        "eu-west-3"
                    ]
                }
            }
        }
    ]
}
```

Listato 5.1: **DenyAllOutsideRequestedRegions**, policy per negare l'accesso a servizi AWS in region extra-UE

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableDisableEURegionOnly",
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "account:TargetRegion": [
                        "eu-south-1"
                    ]
                }
            }
        },
        {
            "Sid": "ViewConsole",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Listato 5.2: **EnableDisableEURegionsOnly**, policy per consentire l'attivazione solo di region opt-in in UE

`*` è la wildcard per indicare tutte le azioni. Comunque, solo con questi elementi, la policy bloccherebbe qualsiasi azione sul Cloud, ad eccezione di quelle sui servizi globali. Per questo, si aggiunge la proprietà `Condition`, la quale permette di affermare, con la sintassi indicata sopra, che la policy si applica solo quando si richiede di fare un'azione su una risorsa in una region tra quelle non elencate nella policy. Utilizzando questa proprietà e specificando tra le region nella policy solo quelle locate in Unione Europea si soddisfano i primi due requisiti elencati sopra.

Tuttavia, bloccare l'accesso ai servizi AWS in region extra-UE non è sufficiente, perché un utente con privilegi è ancora in grado di attivare region opt-in che non si trovano in UE, creando potenzialmente degli scenari in cui i dati possano fluire in region non europee. Quindi, è necessario definire un'altra policy che impedisca l'attivazione di region opt-in diverse da quelle localizzate all'interno dell'Unione Europea. A tale scopo si utilizza la policy descritta in Listato 5.2, che contiene due statements. Il primo permette esplicitamente (`Allow`) le azioni di abilitazione e

disabilitazione di una region solo a condizione che si richieda di attivare o disattivare quella con codice `eu-south-1`. Tale regione AWS, al momento di realizzazione della verifica, è l'unica region opt-in localizzata in UE. Il secondo statement, invece, si occupa di permettere esplicitamente l'azione di elencazione delle region selezionabili, in maniera tale da permettere al cliente di cambiare region e sceglierne una tra quelle ammesse.

Infine, l'ultima policy che si definisce ha lo scopo di soddisfare l'ultimo requisito, ovvero quello di impedire a qualsiasi utente privilegiato di cambiare le policy ad esso assegnate, e compiere delle azioni che potrebbero portare dati e servizi dell'Amministrazione al di fuori delle region UE. Tale policy dipende dalla struttura organizzativa riprodotta dall'Amministrazione nel servizio di Identity and Access Management di AWS. Per questo, al fine di sviluppare questa policy e poi applicare tutte le altre per testarne il funzionamento è stato necessario creare degli utenti e dei gruppi IAM. Nella creazione di utenti e gruppi si è supposto che l'Amministrazione, la quale utilizza le policy IAM per implementare una corretta localizzazione in UE dei propri dati e servizi, avesse raggiunto un livello di maturità nell'utilizzo del Cloud non molto elevato. Infatti, si è ipotizzata la configurazione di uno scenario a singolo account con la struttura riportata nella Figura 5.4. L'Amministrazione, in questo

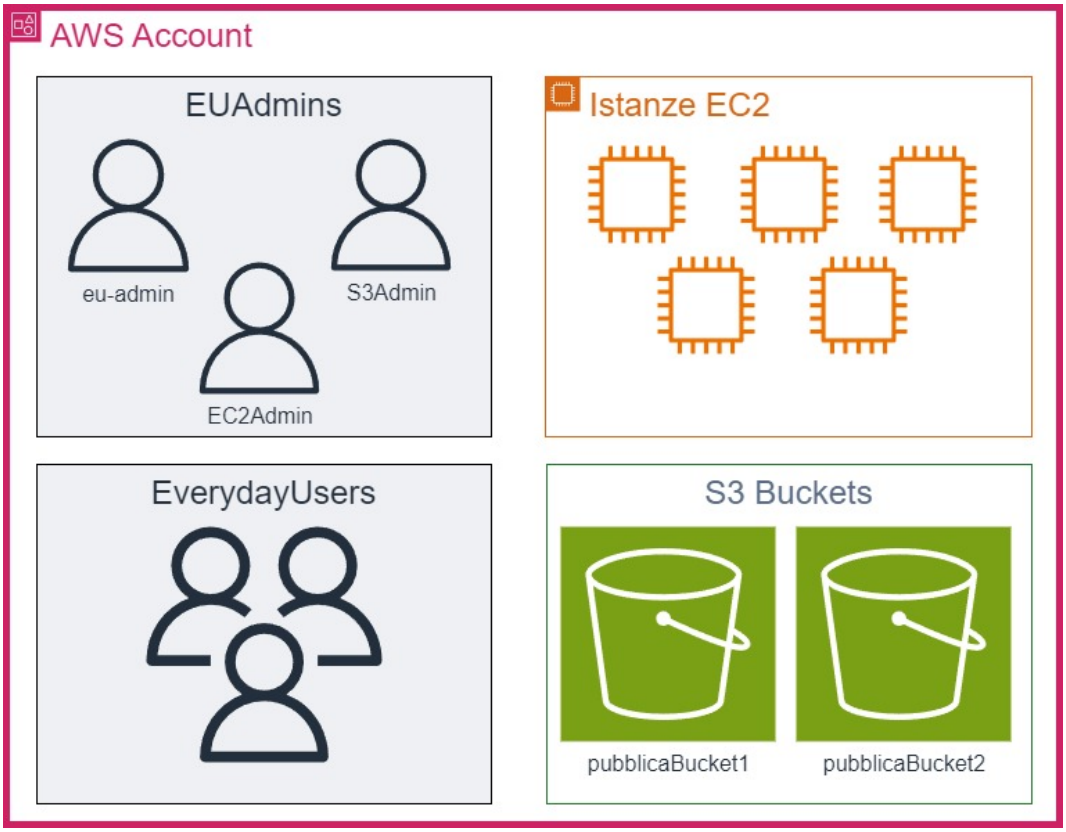

Figura 5.4: Struttura organizzativa ambiente a singolo account

caso, utilizza il Cloud solo per accedere ai servizi AWS Elastic Compute Cloud (EC2) e Simple Storage Service (S3), e possiede solamente tre utenti privilegiati, ad ognuno dei quali è assegnata una policy gestita da AWS:

- `eu-admin`: è l'amministratore dell'ambiente AWS e può accedere a qualsiasi servizio. Ad esso viene assegnata l'identity-based policy denominata *AWSAdministratorAccess*
- `EC2Admin`: è colui che si occupa di effettuare il provisioning di macchine virtuali per l'organizzazione, grazie ai permessi concessi dalla policy assegnatagli, ovvero *AmazonEC2FullAccess*.
- `S3Admin`: è l'utente che gestisce i bucket di S3, dato che gli viene assegnata la policy *AmazonS3FullAccess*.

Oltre a questi utenti privilegiati sono stati definiti degli utenti ordinari raccolti nel gruppo IAM `EverydayUsers`, per cui è stata definita una policy basata su identità concede un insieme limitato di permessi sulle risorse create nell'account. Allo stesso modo anche gli utenti privilegiati sono stati raccolti all'interno del gruppo `EUAdmins`, in quanto raccogliere gli utenti in gruppi faciliterà la successiva assegnazione delle policy.

Dalla descrizione della struttura organizzativa ipotizzata è evidente che l'utente `eu-admin` ha potenzialmente dei privilegi adeguati per accedere al servizio di Identity and Access Management e cambiare o rimuovere qualsiasi policy gli venga assegnata, comprese quelle per forzare la data residency in UE. Per questo sarà necessario definire la policy riportata in Listato 5.3 per impedire che questo accada. Senza scendere nel dettaglio e commentare ogni azione elencata nella policy, la sua conseguenza principale è quella di impedire la maggior parte delle azioni di aggiunta, rimozione e aggiornamento delle policy assegnate sia agli utenti amministratori, sia al gruppo `EUAdmins`. Con quest'ultima policy si ottiene l'ultimo strumento capace di implementare il quarto requisito descritto in precedenza.

A questo punto, al fine di valutare l'effettiva capacità delle policy presentate di garantire una corretta collocazione di dati e servizi all'interno di region UE e un corretto utilizzo del Cloud, è stato necessario decidere come assegnare le policy ai vari utenti e gruppi definiti. Innanzitutto a tutti e due i gruppi presenti, `EUAdmins` e `EverydayUsers`, è stata assegnata la DenyAllOutsideRequestedRegions policy, per impedire a tutti gli utenti dell'Amministrazione di accedere a servizi in region extra-UE. Successivamente si è assegnata solo al gruppo `EUAdmins` la policy EnableDisableEURegionsOnly, per impedire l'attivazione da parte degli amministratori di region non ammesse. Tale policy non è stata assegnata anche al gruppo degli utenti ordinari, perché la policy definita per loro non gli concede il permesso di accedere alla funzionalità di abilitazione e disabilitazione delle region. Infine è stata impostata

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SetMaximumAllowedActions",
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "",
            "Action": [
                "iam:DeletePolicy",
                "iam:AttachUserPolicy",
                "iam:DeleteUserPolicy",
                "iam:DetachUserPolicy",
                "iam:PutUserPolicy",
                "iam:SetDefaultPolicyVersion",
                "iam:CreatePolicyVersion",
                "iam:DeleteUserPermissionsBoundary",
                "iam:PutUserPermissionsBoundary",
                "iam:DeactivateMFADevice",
                "iam:UpdateAccountPasswordPolicy",
                "iam:DeleteAccountPasswordPolicy"
            ],
            "Effect": "Deny",
            "Resource": [
                "arn:aws:iam::ID:user/eu-admin",
                "arn:aws:iam::ID:user/EC2Admin",
                "arn:aws:iam::ID:user/S3Admin"
            ]
        },
        {
            "Sid": "",
            "Action": [
                "iam:AddUserToGroup",
                "iam:AttachGroupPolicy",
                "iam:RemoveUserFromGroup",
                "iam:DeleteGroup",
                "iam:DeleteGroupPolicy",
                "iam:DetachGroupPolicy",
                "iam:PutGroupPolicy"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:iam::ID:group/EUAdmins"
        }
    ]
}
```

Listato 5.3: **EU-Admin-Not-Change-Own-Policy**, policy per impedire la modifica dei privilegi degli amministratori

la policy EU-Admin-Not-Change-Own-Policy come permission boundary per l'utente `eu-admin`. La scelta di utilizzare il permission boundary e non la policy basata su identità è legata al fatto che al livello logico, si devono restringere i permessi dell'amministratore. Quindi, l'amministratore non deve vedersi negate esplicitamente determinate azioni, ma nel caso in cui provi a fare azioni che eccedono i limiti stabiliti deve essere bloccato. Per questo, è più coerente utilizzare lo strumento del permission boundary rispetto alla policy basata su identità.

5.3.2 Implementazione della landing zone di Control Tower

Il processo di configurazione di una landing zone di Control Tower è relativamente semplice per un utilizzatore finale che abbia delle conoscenze anche non troppo avanzate delle tecnologie Cloud. L'intera configurazione della landing zone è un processo guidato in cui chi utilizza lo strumento deve solo scegliere in quali region abilitare la governance di Control Tower. Per garantire una corretta localizzazione dei dati all'interno dell'UE l'Amministrazione, durante il processo di configurazione deve essenzialmente fare tre operazioni:

1. Scegliere come *home region* una delle region UE. Allo stato attuale è conveniente scegliere come *home region* una di quelle attivate di default, in maniera tale da essere sicuri di poter beneficiare di tutte le funzionalità di Control Tower. Tra queste attualmente in Unione Europea ci sono `eu-west-1` (Irlanda), `eu-central-1` (Francoforte), `eu-west-3` (Parigi) e `eu-north-1` (Stoccolma).

2. Scegliere come region addizionali da inserire sotto la governance tutte le region in Unione Europea al fine di garantire una maggiore resilienza del Cloud. Oltre, a quelle indicate nel punto precedente, si aggiunge la region `eu-south-1` (Milano).

3. Abilitare il *region deny setting*, ovvero il controllo `AWS-GR_REGION_DENY`, sull'intera landing zone. Esso è realizzato con una Service Control Policy molto simile alla policy DenyAllOutsideRequestedRegions.

Con questa configurazione iniziale si impedisce a tutti gli account che verranno aggiunti sotto la governance di Control Tower di accedere ai servizi AWS in region extra-UE, in maniera tale da garantire la localizzazione dei dati delle Amministrazioni in Unione Europea.

Ovviamente, il *region deny setting* da solo non è sufficiente per ridurre a zero la probabilità che o delle configurazioni errate delle risorse o azioni sbagliate dei dipendenti dell'Amministrazione, possano provocare il trasferimento di dati dell'Amministrazione verso altre region extra-UE. Per questo motivo è necessario attivare anche altri controlli di data residency, messi a disposizione da Control Tower, per

aumentare il grado di sicurezza dell'infrastruttura e chiudere eventuali canali di transito dei dati imprevisti e indesiderati. Tra i venti controlli di *dat residency*, a cui si era accennato prima nel paragrafo 5.2.2, ce ne sono alcuni molto specifici. Ognuno di questi controlli fa riferimento a un diverso servizio AWS, e ha lo scopo di evitare che si generino flussi di dati, associati a quel servizio, verso region non ammesse. Quindi, a seconda dei servizi utilizzati, ogni Amministrazione deve scegliere quali controlli di *data residency* abilitare, in quanto non ha nessun senso abilitare un controllo su un'unità organizzativa, se questo fa riferimento a un servizio non utilizzato dagli account in essa contenuti. Tuttavia, alcuni dei controlli di *data residency* vanno attivati indipendentemente dai servizi utilizzati dall'Amministrazione, perché hanno il compito di garantire che non ci siano flussi di dati non ammessi, nel trasferimento dei dati delle Amministrazioni dalle loro infrastrutture on-premise al Cloud AWS. Di seguito si analizzeranno due di questi controlli di *data residency* generali, e altri due controlli, ognuno legato a un servizio AWS differente.

Il primo controllo che ogni Amministrazione deve attivare, per favorire la corretta localizzazione dei dati in UE è `AWS-GR_DISALLOW_VPC_INTERNET_ACCESS`, ovvero un controllo preventivo che non permette il collegamento a internet da e verso tutti i Virtual Private Cloud (VPC) creati dagli account appartenenti a Control Tower. Lo scopo del controllo è quello di ridurre la superficie di attacco, evitando che i dati dell'Amministrazione passino attraverso la normale rete internet e possano essere per errore trasferiti, o transitare, verso o altre region, o dispositivi, o infrastrutture, non situate in UE. Abilitando questo controllo è possibile creare un VPC solo con sotto-reti private accessibili all'interno della zona di disponibilità in cui avviene la creazione, ma non accessibili dalla rete globale internet. Anche se questo controllo potrebbe limitare in qualche modo la normale operatività di un'organizzazione, comunque, AWS mette a disposizione due eleganti soluzioni per connettere un VPC privato con la propria infrastruttura on-premise in maniera sicura:

- **AWS DirectConnect**: è una soluzione altamente sicura, che consente di connettere la propria infrastruttura on-premise con una particolare region del provider, attraverso una connessione in fibra ottica dedicata, ad alta velocità. In questa maniera, è possibile collegare il proprio ambiente locale all'ambiente Cloud tramite linee dedicate e punti di presenza di Amazon ed evitando che i propri dati possano finire in paesi extra-UE.

- **AWS site-to-site VPN**: è una soluzione più economica della precedente, che però fornisce un livello di sicurezza adeguato. In sostanza, si connette la propria infrastruttura on-premise con un endpoint AWS attraverso una VPN. In questa maniera, è noto qual è il tunnel cifrato che attraverseranno i dati per andare dalla propria infrastruttura alle region AWS scelte.

L'altro controllo preventivo che è consigliabile attivare al fine di prevenire flussi di dati non ammessi è `AWS-GR_DISALLOW_CROSS_REGION_NETWORKING`. Lo scopo di questo controllo è principalmente quello di impedire la connessione (*peering*) tra due Virtual Private Cloud creati all'interno di region diverse. In questa maniera, si impedisce che un VPC, anche privato, situato in una region UE, possa comunicare con qualsiasi altro VPC situato in una region extra-UE, azzerando qualsiasi possibilità che i dati dell'Amministrazione possano uscire dalle region sotto la governance di Control Tower. Impedire la connessione tra due VPC in region diverse introduce anche un ottimo livello di isolamento tra le region gestite da Control Tower e non genera problemi di utilizzabilità del Cloud. Infatti, se l'Amministrazione progetta in maniera corretta il proprio ambiente Cloud su AWS, non ha bisogno di far comunicare risorse in region diverse attraverso due VPC, ma può mantenere le risorse in ogni region isolate per aumentare il livello di resilienza dei propri servizi attraverso meccanismi di replicazione.

Poi, ci sono altri due controlli che ogni Amministrazione deve attivare, in maniera da localizzare i dati solo all'interno delle region gestite da Control Tower, ovvero `AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP`, specifico per il servizio Elastic Compute Cloud, e `AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC`, specifico per il servizio S3. Il primo è un controllo di rilevamento, che segnala se viene creata una macchina virtuale EC2 con indirizzo IP pubblico e serve per permettere al team di sicurezza che controlla l'account di Audit di rilevare eventuali punti di ingresso pubblici dentro l'ambiente Cloud dell'Amministrazione ed eliminarli nel più breve tempo possibile. Infatti, rendere una macchina virtuale EC2 dell'Amministrazione raggiungibile da internet, mediante un IP pubblico, potrebbe creare canali collaterali attraverso i quali i dati dell'Amministrazione possono transitare verso altre region o altre macchine nella rete internet situate in territorio non europeo. Allo stesso modo anche il secondo controllo evita che si crei un punto di contatto con la rete pubblica, perché serve per individuare in maniera tempestiva la creazione di un bucket di S3 con accesso pubblico da qualsiasi punto della rete. Rendere pubblico un bucket di S3, significa esporre i dati dell'Amministrazione ad accessi incontrollati, aumentando il rischio di diffusione dei dati in paesi non europei. Rilevare al più presto questo genere di configurazioni potenzialmente vulnerabili è essenziale per rispettare tutti i requisti di *data residency* imposti.

L'attivazione di tutti i controlli descritti consente a un'Amministrazione anche strutturata di creare un ambiente sicuro in cui i dati e i servizi sono confinati nelle sole region AWS localizzate in Unione Europea. Chiaramente i controlli aggiuntivi al *region deny setting* vanno attivati in tutte le unità organizzative create all'interno di Control Tower, in maniera da sottoporre tutti gli account creati dall'Amministrazione a una rigida sorveglianza. Tuttavia, i controlli descritti sono sufficienti in un ambiente in cui l'Amministrazione utilizza solo EC2 e S3, e non nei casi in cui essa arrivi a un

livello di maturità nell'utilizzo del Cloud più avanzato. Nel caso di Amministrazioni che utilizzano più servizi AWS diversi è necessario ricercare, all'interno della documentazione AWS e nella libreria di Control Tower, tutti i controlli di *data residency* specifici per i loro servizi e applicarli a tutte le unità organizzative. Solo così è possibile ottenere una garanzia adeguata che i dati dell'Amministrazione rimangano all'interno dell'UE, grazie all'utilizzo di AWS Control Tower.

5.4 Valutazioni finali

L'analisi delle caratteristiche dei servizi Cloud AWS e degli strumenti messi a disposizione per la localizzazione dei dati, anche attraverso una loro implementazione di prova, è stata sufficiente per formulare un giudizio finale sulla loro validità e capacità di soddisfare i requisiti di *data residency*. Ognuno dei due strumenti ha dei vantaggi importanti che permettono all'Amministrazione di mantenere i propri dati e servizi in UE, ma evidenzia anche delle criticità che è necessario approfondire al fine di permetterne un corretto utilizzo e una valutazione trasparente.

5.4.1 Valutazioni sulle policy IAM

Le policy IAM sono uno strumento adeguato per implementare la localizzazione dei dati all'interno di una determinata area geografica. Innanzitutto IAM è uno strumento totalmente gratuito, ovvero non genera costi aggiuntivi per l'Amministrazione, rispetto a quelli sostenuti per implementare i propri carichi di lavoro. Allo stesso tempo, le policy definite nell'ambito di questo lavoro possono essere mantenute direttamente dal regolatore, che le può fornire alle Amministrazioni, insieme a delle indicazioni su come assegnarle ai vari utenti. In questa maniera lo sforzo di gestione da parte delle Amministrazioni, nell'utilizzo dello strumento per localizzare i dati e i servizi su territorio UE, è minimo. Infatti, ogni Amministrazione che utilizza un ambiente a singolo account si deve occupare solo di creare gli utenti e di assegnare, ed eventualmente definire, le policy a loro necessarie per svolgere la mansione designata. Al contrario, le policy di *data residency* saranno fornite dal regolatore che indicherà quali sono le tipologie di utenti a cui ognuna delle policy definite nel paragrafo 5.3.1 vanno assegnate.

Questo scenario risulta particolarmente adatto per Amministrazioni Pubbliche che non hanno raggiunto un livello di maturità sufficiente nell'utilizzo del Cloud. Nell'ipotesi in cui l'Amministrazione utilizzi poche tipologie e istanze di servizi Cloud per scopi come lo storage e l'elaborazione, **le policy IAM sono uno strumento sufficiente per garantire la localizzazione di dati e servizi in UE**. Esse permettono all'Amministrazione di mantenere un pieno controllo sui propri dati e servizi nel Cloud, senza creare problemi di utilizzabilità dell'ambiente e caricarle di

oneri di gestione troppo pesanti. Al contrario, nel caso di amministrazioni strutturate che hanno raggiunto un livello di maturità nell'utilizzo del Cloud avanzato, utilizzando più servizi AWS e creando centinaia di istanze, l'approccio basato su singolo account e sulle policy non è più sufficiente. Per quel genere di Amministrazioni è **consigliabile utilizzare altri strumenti come Control Tower**, in maniera da creare un livello di isolamento aggiuntivo con la creazione di più account AWS e mantenere pieno controllo sulla landing zone.

Comunque, il fatto che esso è adatto solo per Amministrazioni non strutturate e con pochi carichi di lavoro non è l'unica criticità delle policy IAM. Infatti, come riportato nella policy DenyAllOutsideRequestedRegions, è consentito l'accesso in region esterne all'Unione Europea per tutti quei servizi AWS classificati come servizi globali. Il rischio che si può correre in questo caso è che se tramite i servizi globali sono trattati direttamente dati delle Amministrazioni Pubbliche, in realtà si va incontro a una violazione dei requisiti di *data residency* imposti dal controllo della Sottocategoria `SC-SI-PR.DS-1-01`. Infatti, trattare i dati delle Amministrazioni attraverso un servizio globale comporta, per come è strutturata l'infrastruttura AWS, che i dati siano replicati in tutte le region AWS del mondo, a causa della distribuzione del *data plane* di questi servizi. Quindi, al fine di evitare una violazione, e formulare una valutazione corretta si sono analizzati alcuni dei servizi globali che l'Amministrazione deve utilizzare per forza quando migra sul Cloud AWS.

I servizi globali riportati nella policy DenyAllOutsideRequestedRegions sono classificabili in tre macro-categorie:

- **Servizi di gestione e reportistica dei costi**: ovvero tutti quesi servizi AWS che permettono all'Amministrazione di gestire i costi, le fatture e genera dei report di utilizzo dei servizi AWS.
- **Servizi di rete**: tutti i servizi che consentono di impostare la rete all'interno del Cloud, compresi i firewall.
- **Servizi di gestione dell'organizzazione su Cloud**: tutti i servizi che consentono di gestire gli utenti e gli account e di monitorarne le loro attività.

Considerando la prima macro-categoria, gli unici dati dell'Amministrazione che sono trattati da questi servizi globali sono le informazioni relative ai metodi di pagamento e agli estremi di fatturazione dell'Amministrazione stessa. Tuttavia, queste informazioni sono utilizzate dall'Amministrazione anche in altri contesti e condivisi anche con altri enti privati e pubblici. Quindi, il fatto che siano replicati al livello globale non crea un problema. Allo stesso modo, i dati trattati dai servizi appartenenti alla seconda macro-categoria sono dati relativi a come è impostata la rete virtuale dell'Amministrazione all'interno Cloud, non coinvolgendo direttamente dati dell'Amministrazioni. Quindi, almeno per queste tipologie di servizi globali, i

dati trattati sono classificabili tra i metadati, secondo la definizione che ne dà la determina n.307 di ACN. Per questo insieme di dati non è necessaria la localizzazione all'interno dell'Unione Europea.

Per quanto riguarda i servizi di gestione delle identità e delle organizzazioni, potenzialmente questi possono trattare dati personali dei dipendenti delle Amministrazioni Pubbliche. Quindi, utilizzando servizi globali come IAM, per la gestione degli utenti dell'Amministrazione potrebbe comportare una violazione dei requisiti di *data residency* richiesti. Tuttavia, è possibile aggirare questo problema, in maniera tale da non compromettere l'utilizzo dei servizi AWS per le Amministrazioni Pubbliche e bloccare la loro transizione digitale. Infatti, piuttosto che creare gli utenti per i dipendenti dell'Amministrazione, sulla base della loro identità, conviene crearli in base alla mansione svolta, compatibilmente con i vincoli e i requisiti derivanti dall'impianto normativo dei procedimenti amministrativi. In questa maniera, è possibile evitare di inserire dati personali dei dipendenti all'interno del Cloud AWS e non violare i requisiti imposti. Inoltre, la gestione delle identità sul Cloud basata sulle mansioni del dipendente facilita anche la gestione stessa degli utenti, perché quando un dipendente termina il rapporto di lavoro con l'Amministrazione è sufficiente solo cambiargli la password, e non modificare tutte le sue credenziali.

Un'altra soluzione, più elegante della precedente, è quella della federazione delle identità. È molto probabile che le Amministrazioni pubbliche abbiano già un loro provider di identità, in cui sono raccolte tutte le identità digitali dei dipendenti dell'Amministrazione. Quindi, l'idea migliore per non esporre direttamente dati dei dipendenti dell'Amministrazione è quella di federare il proprio identity provider con AWS IAM. Infatti, utilizzando protocolli come SAML e OpenID Connect, è possibile far assumere a ogni utente registrato nel proprio identity provider, un ruolo AWS, a cui poi sono associati tutti i permessi che deve avere all'interno del Cloud AWS l'utente che assume quel ruolo. In questa maniera è possibile non esporre i dati degli utenti all'interno del Cloud AWS e riutilizzare le policy definite in 5.3.2 assegnandole ai ruoli che assumeranno gli utenti una volta che accederanno ad AWS con l'identità federata. Così si continua a forzare la localizzazione dei dati in UE senza esporre alla diffusione globale i dati dei dipendenti dell'Amministrazione.

Alla luce delle criticità analizzate e dei vantaggi evidenziati, la valutazione su IAM è sicuramente positiva, in quanto concede tutte le funzionalità per implementare una corretta localizzazione dei dati in Unione Europea. Tuttavia, vista l'esistenza dei servizi globali, prima di stabilire che con IAM non c'è nessun rischio che i dati dell'Amministrazione finiscano in region extra-UE, è necessaria un'analisi di ogni servizio globale di cui ha bisogno l'Amministrazione. Lo scopo di questa ulteriore verifica, rimandata a sviluppi futuri del presente lavoro, è quello di valutare se il servizio globale possa trattare anche solo in parte dell'Amministrazione. Nel caso in cui i dati dell'Amministrazione non siano accessibili a tale servizio, si può autorizzare

l'utilizzo dello strumento, altrimenti è necessario stabilire se l'Amministrazione può fare a meno del servizio oggetto di verifica. Nel caso in cui il servizio sia indispensabile per un corretto utilizzo del Cloud AWS, è necessario interagire con AWS e capire se è possibile aggirare questo problema solo per le Amministrazioni italiane. Infine, è necessario sottolineare che nel caso in cui IAM alla fine ottenga una valutazione pienamente positiva, comunque esso può essere utilizzato solo per dati e servizi di natura ordinaria. Infatti, secondo le disposizioni attualmente vigenti, per dati e servizi critici o strategici anche eventuali metadati dell'Amministrazione devono essere trattati attraverso infrastrutture localizzate in UE.

5.4.2 Valutazione su Control Tower

Control Tower rappresenta lo strumento migliore, messo a disposizione da AWS, per garantire una corretta localizzazione dei dati in Unione Europea, in quanto può essere utilizzato anche da Amministrazioni strutturate che hanno raggiunto un livello di maturità alto nell'utilizzo del Cloud. La semplicità con cui è possibile configurare la *landing zone* e l'astrazione che offre Control Tower, rispetto allo strumento AWS con cui sono implementati i controlli di sicurezza attivabili, sono i principali vantaggi del servizio. Infatti, la configurazione e la gestione degli account e delle unità organizzative di Control Tower è relativamente semplice e ben documentata. Allo stesso tempo, quando l'amministratore deve scegliere se attivare un controllo, non deve per forza approfondirne la tecnologia di implementazione, ma può semplicemente fare riferimento all'obiettivo del controllo e ai framework da cui esso proviene. Questo facilita il lavoro dell'amministratore di Control Tower, velocizzando il processo di attivazione del controllo. Tuttavia, viene lasciata la possibilità all'amministratore di visionare la tecnologia implementativa del controllo, al fine di non precludere una valutazione più approfondita dello stesso.

La dashboard di Control Tower offre una visione d'insieme all'Amministratore, segnalando lo stato dell'organizzazione e il rilevamento di eventuali risorse che non rispettano determinati controlli di sicurezza. Allo scopo di segnalare tempestivamente la presenza di risorse con configurazioni potenzialmente vulnerabili, è importante anche la presenza dell'account di Audit. Esso, rispetto al caso a singolo account, permette un monitoraggio più stretto delle risorse implementate sul Cloud e anche un intervento più tempestivo nel caso in cui ci sia bisogno di svolgere azioni di correzione. In più i dati relativi al monitoraggio e alle azioni dei vari account, utilizzati dall'account di Audit, sono salvate all'interno della *home region* di Control Tower, localizzando così eventuali metadati dell'Amministrazione in Unione Europea. Allo stesso modo Control Tower, per la gestione degli account appartenenti all'Amministrazione, configura il servizio di gestione delle identità AWS, IAM Identity Center, solo all'interno della *home region* della *landing zone*. Questo aspetto permette di

superare una delle criticità evidenziate nel paragrafo 5.4.1, ovvero il fatto che dati di dipendenti dell'Amministrazione vengano esposti globalmente. Infatti, avendo IAM Identity Center configurato in una region UE tutti i dati degli account relativi a Control Tower sono mantenuti in data center europei, rendendo soddisfatti i requisiti di *data residency* richiesti.

Proseguendo e focalizzandosi su tutti i controlli offerti da Control Tower per implementare i requisiti di localizzazione dei dati richiesti, si può affermare che questi rendono Control Tower uno strumento assolutamente completo. Infatti, i controlli di *data residency* e più in generale i controlli appartenenti alla categoria *digital sovereignity* coprono in maniera minuziosa ogni aspetto potenzialmente vulnerabile nelle configurazioni dei servizi AWS più utilizzati dalle organizzazioni. In questa maniera, se un'Amministrazione desidera abilitare un nuovo servizio AWS per migliorare la qualità dei servizi offerti ai cittadini, può operare una valutazione più rapida del rischio correlata all'attivazione. Infatti, poichè i controlli sono catalogati anche per il tipo di servizio a cui sono riferiti, l'Amministrazione può visionare tutti i controlli di *data residency* correlati al servizio e valutarli, per capire se l'abilitazione del nuovo servizio impatta negativamente sulla localizzazione dei dati in UE. Allo stesso modo, il fatto che molti controlli siano specifici per il particolare servizio, consente all'amministratore di attivare solo i controlli necessari all'ente pubblico. In questo modo, le notifiche di sicurezza sulla dashboard e sulla email associata all'account di Audit saranno selezionate e specifiche per il servizio, favorendo la tempestività di qualsiasi azione correttiva.

I grandi vantaggi di Control Tower però non lo rendono uno strumento privo di criticità che vanno analizzate attentamente e possibilmente risolte. Innanzitutto, Control Tower è uno strumento che ha degli oneri sia economici che di gestione. Infatti, l'utilizzo di altri strumenti come AWS Config e CloudFormation ha un prezzo non trascurabile in termini economici, specialmente quando gli account sono molti. Inoltre, anche se la gestione di Control Tower è relativamente semplice, comunque è necessario avere un team di almeno qualche persona che si occupa non solo di valutare l'attivazione dei controlli, ma anche del monitoraggio e delle azioni correttive configurabili attraverso l'account di Audit. Quindi, anche al livello gestionale Control Tower richiede l'impiego di alcune persone, al fine di essere utilizzato al pieno delle sue potenzialità, che rappresentano un costo per l'Amministrazione. Quindi, è consigliabile utilizzare Control Tower solo in scenari complessi con molti dipendenti e carichi di lavoro, in maniera che il beneficio che si ottiene superi i costi di gestione. Altrimenti, è bene utilizzare le policy IAM per non introdurre ulteriori costi economici e di gestione per l'Amministrazione.

Proseguendo, anche se avere dei controlli già predisposti può essere molto utile per accelerare la configurazione e mettere subito in sicurezza la *landing zone*, comunque una criticità importante è data dalla rigidità di alcuni controlli di sicurezza. Infatti,

se per un certo servizio non esistono controlli adatti a implementare la localizzazione dei dati come è richiesto per l'Amministrazione, oppure ci sono dei controlli, ma sono troppo restrittivi o troppo laschi, solo utilizzando Control Tower non c'è modo di risolvere questo problema. Quindi non è possibile personalizzare tutti i controlli messi a disposizione da Control Tower, creando una rigidità che può complicare il passaggio al Cloud delle Amministrazioni. Per risolvere questa criticità, è necessario utilizzare direttamente gli strumenti orchestrati da Control Tower, ovvero AWS Config, CloudFormation e le SCPs, configurando poi meccanismi di logging adeguati con AWS CloudWatch. Ovviamente questo scenario si proporrà specialmente in futuro quando alcune Amministrazioni avranno raggiunto un livello di maturità nell'utilizzo del Cloud molto alto. In un orizzonte temporale più stretto i controlli di Control Tower sono sufficienti per garantire la localizzazione dei dati in UE.

Un'altra criticità dello strumento è rappresentata dal fatto che tra i controlli di rilevamento, ce ne sono alcuni che sono collegati ad un altro strumento AWS per la sicurezza, ovvero AWS Security Hub. Tale aspetto è importante perchè AWS Security Hub non è attualmente disponibile in tutte le region AWS. In particolare, nella region `eu-south-1` (Milano), non è possibile accedere a tutte le funzionalità offerte da questo strumento. Ciò significa che, se si tenta di attivare un controllo di rilevamento legato a Security Hub, in una *landing zone* che include, o come *home region* o come region addizionale, la region `eu-south-1`, il controllo non viene attivato. In sostanza, tutti i controlli correlati a AWS Security Hub non possono essere utilizzati in tutte le region UE. Questo rappresenta un problema, perché tra questi controlli correlati a Security Hub si trovano anche alcuni controlli di *data residency* che possono essere utili all'Amministrazione. Attualmente l'unico modo per risolvere questo problema è eliminare dalla *landing zone* tutte le region in cui Security Hub non è disponibile, anche se questo rappresenta una limitazione per il cliente che migra su Cloud AWS. Tuttavia, nel futuro la situazione potrebbe cambiare, dato che AWS lavora continuamente per rendere disponibili tutti le funzionalità dei propri servizi in tutte le sue region.

Tra tutti i controlli di *data residency*, il più importante è il *region deny setting*, che blocca l'accesso alle region AWS non governate da Control Tower. Tuttavia, anche questo controllo possiede un piccolo difetto risolvibile solo integrando Control Tower con le policy IAM. Infatti, il controllo in questione non impedisce comunque agli account che fanno parte dell'organizzazione di attivare region AWS esterne alla landing zone. Anche se potenzialmente l'accesso a molti servizi AWS viene bloccato in quelle region, comunque al fine di evitare qualsiasi possibilità che qualche dato finisca in region non UE, sarebbe bene evitare questo scenario. Per risolvere questo problema risulta molto utile il fatto che Control Tower si interfaccia AWS Organizations. Infatti, è possibile riadattare la policy EnableDisableEURegionsOnly come indicato in Listato 5.4, in maniera da renderla una Service Control Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableDisableEURegionOnly",
            "Effect": "Deny",
            "Action": [
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "account:TargetRegion": [
                        "eu-south-1"
                    ]
                }
            }
        },
        {
            "Sid": "ViewConsole",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Listato 5.4: **EnableDisableEURegionsOnlySCP**, Service Control Policy per consentire l'attivazione solo di region opt-in in UE

utilizzabile in AWS Organizations per limitare l'attivazione di region non europee in tutti gli account dell'organizzazione. Il modo di risolvere questa criticità, può chiaramente essere applicato anche nel caso in cui l'Amministrazione abbia bisogno di definire dei controlli preventivi personalizzati.

Combinare Control Tower con le policy IAM e le Service Control Policy in realtà è una buona prassi quando si hanno dei requisiti diversi per diverse unità organizzative dell'Amministrazione. Infatti, nell'implementazione dello strumento, si è osservato che il *region deny setting* può essere troppo vincolante nel caso in cui ci siano unità organizzative dell'Amministrazione a cui si applicano requisiti diversi. Ad esempio, se i dati utilizzati da una certa unità organizzativa sono talmente sensibili, da essere mantenuti solo su territorio nazionale, con il singolo *region deny setting* non è possibile venire incontro a questo bisogno. Infatti, l'unica soluzione possibile sarebbe limitare l'intera *landing zone* alla sola region italiana, creando però un ambiente Cloud troppo rigido. Allora, per evitare di restringere troppo la *landing*

zone e venire incontro alla particolare esigenza dell'unità organizzativa è conveniente implementare in tutti gli account in essa contenuti le policy descritte nel paragrafo 5.3.1. In particolare è sufficiente modificare solo il campo `Condition` della policy DenyAllOutsideRequestedRegions, come indicato nel Listato 5.5

```
{
    "Condition": {
        "StringNotEquals": {
            "aws:RequestedRegion": [
                "eu-south-1",
            ]
        }
    }
}
```

Listato 5.5: **DenyAllOutsideItalyRegions**, policy per negare l'accesso a servizi AWS in region fuori dall'Italia

La combinazione dei due strumenti è una possibilità sempre da considerare, specialmente quando bisogna venire incontro a bisogni di *data residency* specifici per le Amministrazioni.

L'analisi svolta ha permesso di stabilire che Control Tower è certamente lo strumento migliore messo a disposizione da AWS per implementare i requisiti di *data residency* richiesti dalla determina n.307 di ACN. Esso tratta tutti i dati e anche i metadati relativi al monitoraggio utilizzando solo region incluse nella *landing zone*. Inoltre, l'ampia gamma di controlli che mette a disposizione è in continuo aggiornamento, testimoniando che in futuro sarà possibile impostare limitazioni ancora più stringenti sulla localizzazione dei dati. Oltretutto, le criticità evidenziate possono essere risolte in maniera abbastanza semplice, rendendo lo strumento molto sicuro e adatto per tutte le Amministrazioni pubbliche, specialmente quelle più strutturate. Tuttavia, anche qui esistono due aspetti negativi che non è stato possibile arginare grazie all'utilizzo di altre tecnologie e servizi AWS. Infatti, sarà necessario aspettare prima che i controlli di rilevamento di Security Hub diventino disponibili in tutte le Region AWS. In aggiunta, analizzando la Service Control Policy con cui è implementato il *region deny setting* di Control Tower, si evidenzia che essa concede l'accesso anche ad altri servizi globali oltre a quelli inclusi nella policy DenyAllOutsideRequestedRegions. Anche se questi servizi globali, non dovrebbero trattare direttamente dati delle Amministrazioni, ma solo metadati, è essenziale analizzarli approfonditamente, al fine di permettere alle Amministrazioni di usare questo strumento in totale sicurezza. Tale analisi, sarà cruciale anche per stabilire se Control Tower può essere adottato non solo da Amministrazioni che trattano dati e servizi di livello ordinario, ma anche dati e servizi di livello critico.

Capitolo 6

Conclusioni e Sviluppi Futuri

Il processo di qualificazione dei servizi Cloud è essenziale per garantire una transizione verso il Cloud sicura per tutte le Amministrazioni Pubbliche tenuto conto dei dati e servizi che trattano e di come essi sono classificati da un punto di vista della sicurezza. Tuttavia, i controlli aggiunti con gli allegati A2, B2 e C alla determina n.307 di ACN, seppur necessari, sono tanti e una verifica di tutti potrebbe rendere il processo estremamente lungo e dispendioso per il regolatore e rallentare la transizione digitale. Quindi lo sviluppo di metodologie di verifica serve proprio per fornire al regolatore un modo standardizzato di procedere in maniera da accelerare il processo di qualificazione dei servizi Cloud e delle Infrastrutture, per favorire la migrazione delle Amministrazioni verso il Cloud. Nel presente lavoro ci si è focalizzati sull'allegato B2, contenente requisiti specifici per i servizi Cloud rispetto ai quattro livelli di qualificazione, data anche l'importanza che hanno i servizi Cloud e l'impossibilità di condurre determinate verifiche sulle infrastrutture.

Infatti, oltre a sviluppare delle metodologie adeguate per condurre verifiche standard e ispezioni presso i fornitori di servizi Cloud, è stato richiesto, ove possibile, di mettere in pratica le metodologie sviluppate su tre grandi provider come Azure, AWS e Google Cloud. L'idea dietro queste verifiche, consiste nel fatto che se uno di questi tre provider richiede di qualificarsi per ospitare dati e servizi delle Amministrazioni Pubbliche, si potrebbe avere una grande accelerazione del processo di transizione digitale iniziato nel paese. Servirsi delle grandi tecnologie hyperscaler e di servizi resilienti, messi a disposizione da uno dei tre provider leader nel mercato, potrebbe facilitare la digitalizzazione della Pubblica Amministrazione, migliorando i servizi offerti ai cittadini. Quindi, avere la certezza che questi provider abbiano tutti i requisiti per ospitare almeno i dati e servizi delle Amministrazioni classificati come ordinari, potrebbe essere un passo in avanti importante.

Lo sviluppo di metodologie non è stato un problema solo di carattere tecnico, ma ha richiesto anche una comprensione importante della normativa vigente in materia di Cloud Computing. Infatti, lo studio e la comprensione di alcuni pilastri della strategia Cloud Italia, oltre che delle leggi e delle determine ACN, è stato fondamentale per sviluppare metodologie capaci di soddisfare i requisiti imposti dal regolatore.

Tuttavia, avere alle spalle una conoscenza approfondita del Cybersecurity Framework del NIST e del Framework Nazionale per la Cybersecurity e la Data Protection, è stato essenziale per comprendere la struttura dell'allegato B2, e capire cosa richiede ogni controllo di sicurezza. Acquisite tutte queste conoscenze preliminari, è stato subito evidente che sviluppare una metodologia di *assessment* per ogni singolo controllo non era la cosa migliore da fare, sia per l'eccessiva lunghezza del processo di sviluppo, sia per la scarsa versatilità del prodotto finale. Per questo si è deciso di spendere tempo nella comprensione approfondita dei controlli, al fine di sviluppare una loro categorizzazione che fosse utile per sviluppare metodologie facilmente revisionabili e adattabili, anche in maniera rapida.

Dall'analisi svolta è stata individuata una categorizzazione dei controlli molto soddisfacente che ha permesso di sviluppare metodologie di verifica applicabili in maniera semplice e rapida. In particolare sono state individuate quattro categorie, marcate con i tag DOC, POLICY, ACTION e TECH. Il risultato è stato fornire al regolatore, per la maggior parte dei controlli, metodologie immediatamente applicabili e utilizzabili anche su grandi fornitori di servizi Cloud. Infatti, per tutti i controlli che rientrano nelle classi indicate con ACTION, POLICY e DOC sono state sviluppate immediatamente metodologie valide per un largo insieme di controlli, le quali permettono di condurre verifiche accurate sul fornitore di servizi Cloud. Invece, per i controlli di categoria TECH sono state prima elaborate delle linee guida di alto livello su come sviluppare delle metodologie, perché questi sono molto legati alla particolare tecnologia o sistema a cui fanno riferimento. L'idea di sviluppare queste linee guida, è sembrata da subito molto utile, perché permette al regolatore di avere delle indicazioni da utilizzare su come sviluppare in futuro nuove metodologie per nuovi controlli di sicurezza che potranno essere inseriti nella categoria TECH. Applicando queste linee guida è stato possibile fornire all'Agenzia per la Cybersicurezza Nazionale, ente al quale compete il processo di qualificazione dei servizi cloud e promotore del presente lavoro di tesi, delle metodologie sufficientemente specializzate e adatte per una verifica potenzialmente su qualsiasi fornitore di servizi Cloud esistente.

In più, la categorizzazione individuata non è rigida, perché è previsto il fatto che alcuni controlli potrebbero non rientrare in nessuna delle categorie individuate. In quel caso è stato sufficiente adottare un approccio ad hoc, in quanto il numero di controlli da trattare in maniera specifica si era ormai ridotto notevolmente. La classificazione determinata per i controlli dell'allegato B2 ha il vantaggio di essere utilizzabile anche per i controlli degli altri allegati, perché alcune tipologie di controlli sono presenti anche negli altri allegati. Inoltre, l'aggiunta o il cambiamento di nuovi controlli non rende necessario una riscrittura delle metodologie, perché grazie alla categorizzazione sviluppata è sufficiente individuare la categoria a cui appartiene il controllo aggiunto o modificato. In sostanza, grazie alla categorizzazione dei controlli

è stato possibile offrire all'Agenzia per la Cybersicurezza Nazionale un prodotto finale di alta qualità ampiamente modificabile e mantenibile nel tempo.

Aver sviluppato le metodologie in maniera adeguata, ha facilitato enormemente la loro applicazione. I processi di ispezione condotti nell'ambito di questo lavoro, presso i tre grandi fornitori indicati prima. Infatti è stato possibile verificare quasi un terzo dei controlli di sicurezza dell'allegato senza la conoscenza diretta dell'infrastruttura e dell'ambiente Cloud del provider, in maniera accurata. Le ispezioni condotte mediante l'applicazione delle metodologie sviluppate hanno messo in evidenza che i tre leader di mercato nel mondo della fornitura dei servizi Cloud, potrebbero essere potenziali fornitori di servizi per le Pubbliche Amministrazioni. Tuttavia, ogni giudizio finale è rimandato al momento in cui sarà possibile svolgere tutte le verifiche anche sulle infrastrutture e sugli ambienti Cloud dei tre provider, verificando che anche questi rispettino i controlli indicati all'interno degli allegati A2 e B2.

Molte delle ispezioni condotte sono state lineari e hanno richiesto un'opera di verifica all'interno delle documentazioni dei Cloud Service Provider, che fossero soddisfatti determinati requisiti. Tuttavia, nell'ambito di questo lavoro, rientra una verifica molto interessante che riguarda un aspetto critico per tutte le Amministrazioni Pubbliche italiane, ovvero la localizzazione dei dati dell'amministrazione su territorio UE. Grazie all'intermediazione di ACN, è stato possibile sviluppare una caso di studio sui servizi Cloud di Amazon Web Services, in maniera tale da individuare e valutare gli strumenti messi a disposizione per forzare la localizzazione dei dati in Unione Europea. A seguito di un'interazione con il provider e di un approfondito studio sulla documentazione nonché la simulazione di due diversi scenari d'impiego, sono stati individuati due servizi che potevano rispondere a questa esigenza, ovvero le policy IAM e AWS Control Tower. Entrambi gli strumenti sono stati analizzati a fondo al fine di evidenziarne pregi e difetti e stabilire se fossero adatti a soddisfare il requisito imposto.

Dall'analisi condotta, il giudizio finale che si può formulare su entrambi gli strumenti è che possiedono le funzionalità giuste per favorire la corretta localizzazione dei dati su territorio Europeo. In particolare, le policy IAM risultano adatte per Amministrazioni con pochi carichi di lavoro da gestire e di dimensioni ridotte, mentre Control Tower è più adatto per Amministrazioni più strutturate che utilizzano una grande varietà di servizi AWS. Rispetto a IAM, AWS Control Tower ha dei vantaggi aggiuntivi, in quanto è uno strumento completamente gestito che garantisce anche il salvataggio di alcuni metadati dell'Amministrazione all'interno delle Region UE. Al contrario, le policy IAM sono uno strumento che necessita di un lavoro di sviluppo maggiore e legato ai dettagli implementativi delle policy AWS, mentre Control Tower rende lo strumento utilizzato per implementare i controlli di sicurezza, completamente trasparente al suo amministratore. Tuttavia, Control Tower risulta essere meno personalizzabile delle policy IAM, poiché i suoi controlli di sicurezza sono già definiti

da AWS, e soprattutto comporta un costo maggiore rispetto alle policy che sono totalmente gratuite.

Entrambi gli strumenti hanno determinati vantaggi e determinati svantaggi, che però possono essere mitigati, come già indicato nel capitolo dedicato. Inoltre, è possibile combinare l'azione dei due strumenti, in maniera da utilizzare i lati positivi che hanno entrambi e sviluppare degli ambienti in Cloud in cui si ha una garanzia sufficiente di localizzare i propri dati in Unione Europea. L'unico elemento degno di approfondimenti specifici che è stato possibile individuare riguarda l'accesso che essi danno ai servizi globali di AWS. Sia con Control Tower, che con le policy IAM è necessario mantenere l'accesso a servizi AWS globali, in determinate region extra-UE per non creare problemi di utilizzabilità del Cloud. Questo comporta che è necessario stabilire con certezza che questi servizi globali non trattino dati delle Amministrazioni, ma al massimo solo metadati, in maniera che i servizi AWS possano essere utilizzati almeno da Amministrazioni che gestiscono dati di livello ordinario. Da una prima analisi preliminare, si evidenzia che tutti i servizi globali necessari per un corretto funzionamento dei servizi Cloud AWS, gestiscono al massimo metadati delle Amministrazioni, rendendo gli strumenti adatti almeno per tutte le Amministrazioni che gestiscono dati e servizi di livello ordinario.

In conclusione, il lavoro di sviluppo delle metodologie e il caso di studio sui servizi AWS hanno contribuito in maniera importante al processo di qualificazione dei servizi Cloud per la Pubblica Amministrazione italiana. Tuttavia, il lavoro condotto apre a una serie di interessanti sviluppi futuri e di ulteriori verifiche da effettuare riguardo i due strumenti AWS valutati, nonché ad analoghi strumenti offerti dagli altri provider. Per quanto riguarda le metodologie, il prossimo passo sarà quello di rendere ancora più specifiche le metodologie della categoria TECH, dividendo i controlli associati, se necessario, in più sotto-tipologie, e associandogli metodologie ancora più dettagliate di quelle proposte. Allo stesso modo l'evoluzione della classificazione iniziale proposta in questo lavoro sarà fondamentale anche nel momento in cui si aggiungeranno nuovi controlli di sicurezza agli allegati della determina n.307. Magari, una serie di controlli attualmente indicati come eccezione, potrà in futuro formare una nuova categoria insieme ad altri controlli che saranno aggiunti. Oltre all'allargamento della categorizzazione, un altro passo importante da compiere sarà quello di specializzare alcune delle metodologie TECH in dipendenza dell'infrastruttura del fornitore di servizi Cloud, in maniera da rendere il processo di verifica ancora più rapido e accurato.

Nell'ambito del case study, in futuro sarà necessaria un'ispezione approfondita di tutti i servizi globali AWS. Infatti, comprendere il loro funzionamento, anche mediante delle prove implementative, è l'unico modo attraverso cui si può stabilire in maniera definitiva se gli strumenti individuati nel Cloud AWS sono adatti per garantire una corretta localizzazione dei dati in UE. In particolare, una prova imple-

mentativa potrebbe essere indispensabile per capire anche la tipologia di metadati delle Amministrazioni trattati da questi servizi. Inoltre, relativamente a Control Tower, sarà necessario continuare ad ispezionare e valutare in controlli di *data residency* messi a disposizione, in maniera da valutare costantemente l'aggiornamento dello strumento rispetto all'allargamento dell'offerta AWS e all'aumento delle minacce. Infine, sicuramente, sarà necessario provare ad implementare uno o entrambi gli strumenti presso una vera Amministrazione Pubblica, per valutare effettivamente come questi impattano sull'ambiente Cloud AWS che l'Amministrazione ha creato e sui processi dell'Amministrazione stessa.

Bibliografia

[1] Eurostat. File:Use of cloud computing services, 2020 and 2021 (% of enterprises) v2.png — ec.europa.eu, 2021. Disponibile qui.

[2] Eurostat. File:Use of cloud computing services in enterprises, 2021 v2.png — ec.europa.eu, 2021. Disponibile qui.

[3] DIPARTIMENTO PER LA TRANSIZIONE DIGITALE-AGENZIA PER LA CYBERSICUREZZA NAZIONALE. File: 4.2.png, 2021. Disponibile qui].

[4] Matthew P. Barret. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, 2018. NIST Cybersecurity Framework, [online], `https://doi.org/10.6028/NIST.CSWP.04162018`, `https://www.nist.gov/cyberframework`.

[5] Framework Nazionale per la Cybersecurity e la Data Protection, Febbraio 2019. Distribuito Online – `http://www.cybersecurityframework.it`.

[6] Determinazione n. 628/2021 del 15 dicembre 2021 - Adozione del "regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione".

[7] DIPARTIMENTO PER LA TRANSIZIONE DIGITALE-AGENZIA PER LA CYBERSICUREZZA NAZIONALE. *Strategia Cloud Italia.* Roma, 2021. Disponibile qui.

[8] Art. 33-septies comma 4, D.L. n. 179 del 18 ottobre 2012, *Ulteriori misure urgenti per la crescita del Paese.*, aggiornato con Legge n. 233 29 dicembre 2021. [Accessed 01-12-2023].

[9] AGENZIA PER LA CYBERSICUREZZA NAZIONALE. Determinazione n. 307 del 18 gennaio 2022. `https://assets.innovazione.gov.it/1642694131-det_307_cloud_ulteriorilerqc_20220118.pdf`, 2022.

[10] Peter M. Mell and Timothy Grance. The NIST Definition of Cloud Computing. NIST Special Publications (SP) 800-145, National Institute of Standards and Technology, Gaithersburg, MD, 2011. https://doi.org/10.6028/NIST.SP.800-145.

[11] Wikipedia. Virtual private cloud — wikipedia, l'enciclopedia libera, 2023. [Online; in data 29-novembre-2023].

[12] Eurostat. Cloud computing - statistics on the use by enterprises — ec.europa.eu. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises, 2021. [Accessed 30-11-2023].

[13] Osservatorio Cloud Transformation. Mercato Cloud Computing in Italia in crescita del 19% — osservatori.net. https://www.osservatori.net/it/ricerche/comunicati-stampa/cloud-italia-mercato, 05/10/2023. [Accessed 27-11-2023].

[14] Luca Bechelli, Lorenzo Beliusse, Giancarlo Butti, Giorgia Cesarone, Mauro Cicognini, Alfredo Di Gennaro, Aldo Di Mattia, Giorgia Dragoni, Gabriele Faggioli, Ivano Gabrielli, Paola Girdinio, Paolo Giudice, Corrado Giustozzi, Pier Paolo Glave, Lorenzo Ivaldi, Federica Maria Rita Livelli, Luca Livrieri Nilo, Giuseppe Massa, Carlo Maucelli, Alessio L.R. Pennasilico, Pierluigi Rotondo, Leonardo Sartore, Sofia Scozzari, Gaspare A. Silvestri, Claudio Telmon, Enzo Maria Tieghi, Anna Vaccarelli, and Andrea Manzoni Zapparoli. Rapporto clusit 2023 sulla sicurezza italiana ict - aggiornato fino a ottobre 2023. https://clusit.it/rapporto-clusit/, 2023. [Accessed 30-11-2023].

[15] Art. 1, D.L. n. 105 del 21 settembre 2019, *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*, aggiornato con Legge n. 142 21 settembre 2022. [Accessed 01-12-2023].

[16] Gartner. Gartner Says Worldwide IaaS Public Cloud Services Revenue Grew 30% in 2022, Exceeding $100 Billion for the First Time. Link all'articolo. [Accessed 04-12-2023].

[17] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union, July 2016.

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive

95/46/EC (General Data Protection Regulation) (Text with EEA relevance), May 2016.

[19] Polo Strategico Nazionale. Sicurezza — polostrategiconazionale.it. `https://www.polostrategiconazionale.it/chi-siamo/sicurezza/`. [Accessed 05-12-2023].

[20] Polo Strategico Nazionale. Polo Strategico Nazionale — polostrategiconazionale.it. `https://www.polostrategiconazionale.it/chi-siamo/polo-strategico-nazionale/`. [Accessed 05-12-2023].

[21] D.L. n. 21 del 15 marzo 2019, *Ulteriori misure urgenti per la crescita del Paese.*, aggiornato con Legge n. 108 5 agosto 2022. [Accessed 01-12-2023].

[22] Ivan Di Pietro. Il *cloud* e gli ulteriori servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica. In *Golden Power*, chapter 15, pages 333–350. La Tribuna, Il Foro Italiano, Novembre 2023.

[23] See 15 u.s.c. § 272(e)(1)(a)(i). the cybersecurity enhancement act of 2014 (s.1353) became public law 113-274 on december 18, 2014 and may be found at: `https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.`

[24] Roberto Baldoni and Luca Montanari. Un Framework Nazionale per la Cyber Security. Italian Cybersecurity Report, CIS Sapienza, 2015.

[25] AGENZIA PER LA CYBERSICUREZZA NAZIONALE. Determinazione n. 306 del 18 gennaio 2022. `https://assets.innovazione.gov.it/1642693979-det_306_cloud_modclass_20220118.pdf`, 2022.

Ringraziamenti

Chiudo un altro percorso di studi con la consapevolezza di aver acquisito competenze e conoscenze rilevanti nella materia di mio maggior interesse, ovvero la Cybersecurity. Attraverso le opportunità offerte dall'Università ho potuto formarmi e partecipare ad esperienze interessanti e sfidanti che mi hanno fatto crescere sia come futuro ingegnere che come persona. Tuttavia portare a termine un percorso di laurea magistrale e un progetto di tesi così faticosi non sarebbe stato possibile senza l'ausilio di tante persone intorno a me.

Innanzitutto, ringrazio il mio relatore, il Prof. Luca Spalazzi che mi ha sempre incoraggiato e supportato nella mia formazione e mi ha permesso di svolgere esperienze davvero formative come la Cyberchallenge e questo progetto di tesi sulla sicurezza del Cloud Computing. Spero che la fine di questo percorso dia inizio a una serie di collaborazioni future.

Un ringraziamento particolare va anche al mio correlatore il Dott. Ivan di Pietro e all'Agenzia per la Cybersicurezza Nazionale che mi ha permesso di approfondire una tematica innovativa come la sicurezza all'interno del Cloud. Grazie a loro ho potuto approfondire un tema nuovo e sicuramente attuale, oltre che collaborare con gli ingegneri di Amazon Web Services, nello sviluppo di un case study davvero interessante e di assoluta utilità per le Pubbliche Amministrazioni del paese.

Inoltre, non posso che spendere due parole per tutti gli altri tesisti, dottorandi, assegnisti di ricerca e tecnici che ho conosciuto negli ultimi mesi di lavoro all'interno del DAISY Lab e nel Laboratorio di Cybersecurity. Vi ringrazio per aver alleggerito le giornate più difficili, per avermi ascoltato quando parlavo con voi del mio lavoro, e di avermi parlato del vostro. È sempre un piacere per me stare con voi.

Tuttavia, non avrei potuto portare a termine questa esperienza senza l'ausilio della mia famiglia. Un ringraziamento in particolare va ai miei genitori. A mio papà che mi ha sempre spronato a continuare a lavorare senza mai buttarmi giù, anche quando davanti non vedevo futuro per me. A mia mamma che non ha smesso mai di farmi sentire il suo supporto e il suo amore in ogni gesto quotidiano che faceva per me. Ad entrambi, che mi avete consolato e rallegrato nei momenti più difficili e mi avete sempre lasciato libero di fare quello che desideravo. Senza di voi non ce l'avrei mai fatta. Ringrazio i miei fratelli Andrea e Luca, e le loro fidanzate, Marcella e Viola. Siete e sarete sempre per me un modello da seguire sia nella vita lavorativa che nella vita personale. Vi ringrazio tanto per avermi ispirato e aiutato in questo breve ma

intenso percorso di studi. Ringrazio anche la mia nipotina, la piccola Eleonora, la nuova arrivata nella famiglia, che ha rallegrato sempre tutti noi con i suoi bellissimi sorrisi. Ringrazio tutti i miei zii. Zia Eugenia che, nonostante le difficoltà, non mi ha fatto mai mancare il suo sostegno, Zio Gianmario, Zia Elisabetta, Zio Gianni, Zia Ida e Daiana. Avete sempre creduto in me. Ringrazio anche tutti i miei cugini Michela, Stefano, Francesco, Paola e Fabio. A tutti voi, so che anche se non abbiamo spesso occasione di incontrarci, siete sempre dalla mia parte.

Non posso non menzionare anche i miei compagni di squadra del Porto United. Grazie a voi per avermi accompagnato in questi due anni. A tutte le partite insieme, le risate alle cene, le innumerevoli storie che ho ascoltato da voi con piacere e tutte le altre cose che vivremo in futuro.

Un altro grande ringraziamento va a tutti i miei amici di sempre a Porto Recanati. Che dire ... siamo cresciuti insieme, ognuno di noi sta trovando la sua strada, però ognuno di voi mi ha sempre aiutato durante questi anni. Vi ringrazio tanto, per tutti i momenti in cui ero giù e avete sempre trovato il modo di tirarmi su con leggerezza. Spero di poter vivere con voi tante altre serate insieme in piazza, aste del fantacalcio, grigliate, feste di compleanno e qualunque altro traguardo importante.

Sei rimasta solo tu, Mimmi. Non so che dire. Mi sei sempre stata vicino, mi hai sempre ricordato quali fossero le mie capacità anche quando io stesso dubitavo di essere all'altezza di qualsiasi sfida ho affrontato. Mi hai sempre supportato nelle mie decisioni e affrontato con me tutti i momenti difficili. Spero di poter condividere con te ancora tanto tempo insieme. Sei unica per me. Grazie.

Ancona, Febbraio 2024

Lorenzo Tiseni

Appendice: Documento integrale contenente le metodologie sviluppate e i risultati delle verifiche condotte per Agenzia Nazionale della Cybersicurezza

Metodologie per la verifica dei controlli riportati nell'allegato B2 alla determina ACN n. 307 del 18 gennaio 2022, ed esiti delle ispezioni condotte

Descrizione delle metodologie di verifica specifiche e dei risultati delle loro applicazioni

Autore:
Lorenzo Tiseni

Supervisori:
Ivan Di Pietro
Alessandro Greco
Alessia Galli

Indice

Capitolo 1

Qualità

1.1 QU.SE-1

Sono adottati sistemi per la gestione del servizio IT e della qualità conformemente agli standard di settore

Risultati dell'ispezione

1. **MS Azure:** Tale controllo è soddisfatto per questo provider in quanto viene pubblicato il certificato[1] ufficiale che attesta che Azure e gli altri servizi online Microsoft aderiscono allo standard ISO 9001:2015.

   Google Cloud: Il controllo risulta soddisfatto per questo soggetto in quanto è pubblico a questo link[2] il certificato che attesta che i servizi di Google Cloud sono certificati ISO 9001:2015.

   AWS: Anche il provider in oggetto soddisfa il controllo, perché è pubblica la certificazione[3] che attesta che i servizi cloud AWS aderiscono allo standard ISO 9001:2015

2. **MS Azure:** Tale controllo è soddisfatto dato che Microsoft ha pubblicato la certificazione[4] ufficiale che attesta la conformità dei loro servizi cloud allo standard ISO/IEC 20000-1:2018

   Google Cloud: Analizzando la documentazione online[5], si evidenzia che Google Cloud non ha pubblicato un certificato di aderenza allo standard ISO/IEC 20000-1:2018. Interagire con il Cloud Service Provider per richiedere se posseggono una certificazione equivalente ed approfondire questo aspetto.

   AWS: Il controllo viene soddisfatto visto che AWS ha pubblicato il certificato[6] ufficiale che attesta l'aderenza allo standard ISO/IEC 20000-1:2018 dei suoi servizi cloud.

1.2 QU.SE-2

Viene fornito un adeguato servizio di assistenza e supporto

Risultati dell'ispezione

1. **MS Azure:** Il controllo è soddisfatto, in quanto la Microsoft si impegna ad offrire un servizio di supporto tecnico per Azure, come constatibile consultando il suo sito web[7].

Google Cloud: Il controllo è soddisfatto, in quanto Google Cloud offre la possibilità di avere assistenza tecnica, potendo scegliere anche tra vari livelli a diversi prezzi, come riportato nella documentazione[8]

AWS: Anche il Cloud provider in esame soddisfa il controllo in oggetto, in quanto offre la possibilità di avere assistenza tecnica, potendo scegliere anche qui tra diversi piani come riportato nel sito web[9].

2. **MS Azure:** Da quanto dichiarato sul sito internet della Microsoft si può dire che parte del controllo è soddisfatto in quanto si dice che *Microsoft offre supporto tecnico in nove lingue: inglese, spagnolo, francese, tedesco, italiano, portoghese, cinese tradizionale, coreano e giapponese. Il supporto è disponibile 24 ore su 24, 7 giorni su 7, in lingua inglese per tutti i livelli di gravità e in lingua giapponese solo per la gravità A. Per tutte le altre lingue supportate, il supporto è disponibile solo durante gli orari di ufficio locali. Il supporto al di fuori degli orari di ufficio verrà fornito in lingua inglese, con servizi di traduzione inclusi, se necessario. In alternativa, puoi attendere fino al giorno lavorativo successivo per ottenere il supporto nella tua lingua.*[10]. La dichiarazione riportata testimonia che il servizio in lingua inglese è fornito 24/7 tutto l'anno. Ovviamente questo tipo di supporto viene garantito se si sottoscrive con Azure un piano di supporto "Standard" o "Professional Direct". Invece, per il supporto in lingua italiana fuori dall'orario di lavoro, da quanto riportato anche prima, esso non è disponibile, anche se però sono disponibili dei servizi di traduzione. Chiaramente, per verificare la disponibilità di Microsoft a fornire questo tipo di supporto all'Amministrazione è necessario interloquire con il team di vendite del provider e valutarne la disponibilità.

   Google Cloud: Google Cloud, sottoscrivendo un accordo di assistenza di tipo Avanzato o Premium si impegna ad offrire supporto in lingua inglese 24/7, come riportato anche nella documentazione[11]. Non viene menzionato nulla sul supporto continuativo in lingua italiana in tutti i giorni dell'anno e in qualsiasi orario. Quindi, al fine di approfondire la questione e verificare il controllo, è necessario contattare il team di vendita e valutare che sia possibile ottenere assistenza in lingua italiana.

   AWS: Il controllo viene soddisfatto in pieno da questo Cloud Provider. Innanzitutto, consultando la pagina di confronto[9] dei piani di supporto, si deduce che viene fornita assistenza in lingua inglese 24/7 e in tutti i giorni dell'anno sottoscrivendo un piano di supporto almeno di livello business. In più se si vuole supporto in lingua italiana in tutti i giorni dell'anno e in qualsiasi orario è necessario sottoscrivere un piano di livello Enterprise. Infatti, viene dichiarato che *Se disponi di un piano di supporto AWS Enterprise, avrai a disposizione account manager tecnici che possono parlare e interagire nella lingua locale cinese, inglese, francese, tedesco, italiano, giapponese, coreano, portoghese, spagnolo, tailandese e altro ancora. Per sapere se possiamo interagire nella tua lingua, contatta il tuo team di gestione dell'account o contatta il supporto vendite di AWS per ulteriori informazioni.*[12]. Quindi, il cloud provider si rende disponibile a erogare il servizio di assistenza in lingua italiana.

2. **MS Azure:** Solo per Amministrazioni che erogano servizi di livello almeno critico, è necessario contattare il team di vendita del provider e richiedere se è possibile avere un supporto in lingua italiano dedicato, accessibile in tutti i giorni dell'anno e in qualsiasi orario.

   Google Cloud: Solo per Amministrazioni che erogano servizi di livello almeno critico, è necessario contattare il team di vendita del provider e richiedere se è possibile avere un supporto in lingua italiano dedicato, accessibile in tutti i giorni dell'anno e in qualsiasi orario.

   AWS: Il controllo è verificato perché, come riportato nella metodologia precedente, sottoscrivendo un piano di supporto Enterprise si accede a un supporto di assistenza che può essere erogato anche in lingua italiana.

3. **MS Azure:** Come riportato anche nella descrizione sintetica dei piani di supporto di Azure, consultabile in questa pagina[13], se si sottoscrive un piano di supporto "Standard" o "Professional Direct" è possibile ottenere, previa creazione di un ticket di supporto, il servizio di assistenza tramite telefono o posta elettronica.

   Google Cloud: Seguendo quanto affermato nella documentazione[14] di Google Cloud Customer Care, si rileva che il servizio di assistenza è contattabile sicuramente per via telefonica, mentre l'assistenza via email è rimpiazzata da un contatto via chat con un operatore.

   AWS: Il controllo è soddisfatto perché, osservando la descrizione sintetica[9] dei piani di supporto, si rileva che sottoscrivendo almeno un piano di supporto di livello business si ottiene la possibilità di contattare l'assistenza clienti sia via telefono, che via chat.

4. **MS Azure:** Nel momento in cui l'Amministrazione acquista un piano di assistenza Professional Direct il controllo viene soddisfatto perchè, come riportato sulla documentazione[13], è possibile per essa creare e gestire ticket di supporto tecnico di Azure in modo programmatico

   Google Cloud: Acquistando un piano di assistenza che sia almeno di tipo "Assistenza Avanzata" il controllo è soddisfatto, perché viene offerta all'Amministrazione la possibilità di utilizzare la Cloud Support API per gestire in maniera programmatica i ticket. Qui[8] il riferimento alla documentazione

   AWS: Con AWS, acquistando un piano di supporto almeno di livello "Business", come riportato nella pagina di confronto[9] dei piani, è possibile usufruire di API AWS Support per la gestione programmatica dei casi.

1.3 QU.SE-3

Il soggetto dichiara la frequenza di aggiornamento del servizio

Risultati dell'ispezione

MS Azure: Azure pubblica tutti gli aggiornamenti, le nuove funzionalità e il rilascio di nuovi servizi all'interno del proprio servizio cloud in questa pagina[15].

Qui è possibile consultare tutti i nuovi aggiornamenti e nuove release dei prodotti in microsoft Azure, potendo anche impostare dei filtri opportuni.

Google Cloud: Google pubblica tutti gli aggiornamenti, nuove funzionalità e rilascio di nuovi servizi all'interno del suo sistema cloud nella sua documentazione[16]. Gli aggiornamenti pubblicati nella documentazione principale sono i più rilevanti negli ultimi sessanta giorni, mentre se si vuole avere una lista comprensiva di tutti gli aggiornamenti è necessario consultare la seguente pagina[17].

AWS: Il controllo è soddisfatto per il provider in oggetto, in quanto tutte le nuove funzionalità e aggiornamenti dei servizi all'interno dell'ecosistema cloud di AWS sono pubblicati in questa pagina web[18].

1.4 QU.SE-4

Linee guida e raccomandazioni sull'uso sicuro di soluzioni cloud

Risultati dell'ispezione

MS Azure: Il provider soddisfa il controllo in quanto è fornita una robusta documentazione che copre tutti gli aspetti del controllo in esame. Di seguito si indicano i riferimenti:

a. Microsoft Cloud Security Benchmark[19]
b. Microsoft Cloud Security Benchmark[19]
c. Monitoraggio in Azure[20]
d. Documentazione sull'autenticazione Azure[21]
e. Microsoft Entra ID[22]
f. Microsoft Cloud Security Benchmark[19]
g. Tutte le linee guida sono mantenute in maniera attenta e assidua facendo parte della documentazione ufficiale del prodotto.

Google Cloud: Il controllo è soddisfatto in quanto la documentazione del provider assolve a tutti gli aspetti previsti dal controllo. Di seguito si indicano i riferimenti:

a. Cloud Architecture Framework[23]
b. Google Cloud security bulletins[24]
c. Monitoring[25] e Error Handling[26]
d. Meccanismi di autenticazione[27]
e. Identity and Access Management[28]
f. Cloud Architecture Framework[23]
g. Tutte le linee guida sono mantenute in maniera attenta e assidua facendo parte della documentazione ufficiale del prodotto.

AWS: Consultando tutti i riferimenti presentati di seguito si può constatare che il Cloud Provider soddisfa il controllo in esame.

a. AWS well-architected framework[29]
b. AWS security bulletins[30]
c. Amazon Cloud Watch[31]
d. Meccanismi di autenticazione[32]
e. AWS IAM[33]
f. AWS well-architected framework[29]
g. Tutte le linee guida sono mantenute in maniera attenta e assidua facendo parte della documentazione ufficiale del prodotto.

1.5 QU.PR-1

Tracciamento, reportistica e trasparenza dei costi e della loro elaborazione

Risultati dell'ispezione

1. **MS Azure:** Il Cloud Service Provider soddisfa il controllo, in quanto rende disponibile una dashboard con tutte le funzionalità richieste, le quali sono ben documentate all'interno della documentazione[34].

   Google Cloud: Google soddisfa il controllo perché è disponibile un servizio di gestione della fatturazione e dei costi e di una dashboard con tutte le funzionalità richieste, le quali sono descritte nella documentazione[35].

   AWS: Il controllo viene soddisfatto data la disponibilità per i clienti di un servizio di gestione della fatturazione dei costi e di una dashboard che permette di assolvere alle richieste del controllo. Tale servizio è documentato in questa pagina[36]

2. Per tutti e tre i Cloud Provider in esame, analizzando le documentazione che tramite l'utilizzo delle API e degli strumenti di cost management messi a disposizione, l'Amministrazione è in grado di creare dei report con il dettaglio dei costi per ogni account o prodotto in uso acquistato dal Cloud Service Provider. L'aggiornamento e il tracciamento delle informazioni di costo viene lasciato all'Amministrazione.

1.6 QU.PR-2

Notifica e monitoraggio dei costi

Risultati dell'ispezione

MS Azure: Il controllo è soddisfatto in quanto il sistema di gestione dei costi di Azure[34], oltre a fornire anche altre funzionalità di monitoraggio, reportistica e analisi dei costi, consente anche di impostare degli alert o delle email predefinite nel momento in cui l'utilizzo del servizio cloud produce un costo superiore a un budget preimpostato.

Google Cloud: Il provider offre uno strumento con moltissime funzionalità di monitoraggio dei costi chiamato Cloud Billing[35], che ha anche la funzionalità di impostare degli alert o email automatiche che avvertono determinati membri dell'organizzazione nel momento in cui l'utilizzo dei servizi cloud causa lo sforamento da un budget preimpostato. Il modo di impostare gli alert è documentato in questa pagina[37]

AWS: Amazon permette al cliente di avere un proprio strumento per la gestione e il monitoraggio dei costi chiamato AWS Cost Management[38], che contiene anche la funzionalità di inviare a determinate persone degli alert o delle email nel momento in cui si supera una certa soglia di utilizzo o di costo nel servizio cloud. Tale funzionalità è descritta nella documentazione AWS[39]

1.7 QU.PR-3

Requisiti minimi per il capitolato dei prezzi

Risultati dell'ispezione

1. Contattare il team di vendita del CSP e richiedere, impegnandosi a non divulgarlo, un documento che descriva il metodo e il processo di determinazione dei prezzi del servizio cloud. Valutare, poi, che questo modello offra flessibilità commerciale, supportando scalabilità e crescita.

2. Richiedere al soggetto la disponibilità nel fornire a una qualsiasi Amministrazione che voglia migrare verso il suo servizio cloud, di fornire alla stessa i documenti citati nel controllo due della sottocategoria in esame.

1.8 QU.LS-1

È garantito il rispetto degli indicatori di servizio obbligatori, sono rese note le modalità di condivisione dei livelli di disponibilità dei servizi e le eventuali penali compensative

Metodo di verifica

La creazione di metodologie per la verifica dei controlli associati a questa sottocategoria necessita di avere dei riferimenti contrattuali. Si rimanda lo sviluppo di tali metodologie al momento in cui viene sottoscritto un contratto con un fornitore di servizi Cloud.

1.9 QU.LS-2

Esistono limitazioni per i Service Level Agreement (SLA) per prevenire impatti sugli ambienti dell'Amministrazione

Metodo di verifica

La creazione di metodologie per la verifica dei controlli associati a questa sottocategoria necessita di avere dei riferimenti contrattuali. Si rimanda lo sviluppo di tali metodologie al momento in cui viene sottoscritto un contratto con un fornitore di servizi Cloud.

1.10 QU.LS-3

Esistono contenuti e caratteristiche minimi per i Service Level Agreement

Metodo di verifica

La creazione di metodologie per la verifica dei controlli associati a questa sottocategoria necessita di avere dei riferimenti contrattuali. Si rimanda lo sviluppo di tali metodologie al momento in cui viene sottoscritto un contratto con un fornitore di servizi Cloud.

1.11 QU.LS-4

È disponibile un servizio di monitoraggio (allarmi e parametri) e sono rese note eventuali integrazioni native con soluzioni leader di mercato

Metodo di verifica

La creazione di metodologie per la verifica dei controlli associati a questa sottocategoria necessita di avere dei riferimenti contrattuali. Si rimanda lo sviluppo di tali metodologie al momento in cui viene sottoscritto un contratto con un fornitore di servizi Cloud.

Capitolo 2

Sicurezza

2.1 ID.AM-1

Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione

Metodo di verifica

Non esiste un white paper in cui Microsoft, Google o AWS, affermano di censire tutti i sistemi e gli apparati fisici. Inoltre, non esiste un white paper in cui si accenna al censimento dei dispositivi collegati alla rete e all'accesso solo a quelli approvati. Per questo è necessario interagire con il Cloud Provider per ottenere questo elenco e verificare i controlli

2.2 ID.AM-2

Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione

Metodo di verifica

Non esiste un white paper in cui Microsoft, Google o AWS, censiscono tutte le piattaforme e le applicazioni software installate nei loro data center. Nel caso in cui si voglia avere questo elenco è necessario richiederlo al Cloud Provider prima di autorizzare la migrazione.

2.3 ID.AM-3

I flussi di dati e comunicazioni inerenti all'organizzazione sono identificati

Metodo di verifica

É necessario richiedere al Cloud Provider il documento che descrive tutti i flussi informativi sia verso l'interno che verso l'esterno del servizio cloud.

2.4 ID.AM-6

Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)

Metodo di verifica

La verifica di questa sottocategoria del framework viene operata seguendo dei passaggi:

1. Verificare che le articolazioni competenti del Cloud Provider conoscano l'organizzazione di cybersecurity, conoscendo ruoli e responsabilità sia di attori interni al soggetto sia di terze parti.

2. Verificare che sia stato nominato un incaricato, e un suo sostituto, competenti nell'ambito di cybersecurity, che si occupino di attuare le disposizioni del Regolamento e assicurarne l'efficace implementazione, all'interno del del Cloud Provider.

3. Verificare che sia stato nominato un referente tecnico e un suo sostituto, con competenze tecnico-specialistiche in materia di cybersecurity, che si occupino di interfacciarsi con il CSIRT Italia per la gestione di incidenti che hanno avuto impatto sul servizio cloud.

4. Verificare che esistano documenti e processi standardizzati che testimonino che il referente tecnico e l'incaricato operino in sinergia.

5. Solo per servizi e dati delle PA classificati come di livello critico, ACN deve verificare che il soggetto gli abbia comunicato ufficialmente i nominativi dell'incaricato e del referente tecnico, al momento della verifica.

6. Solo per servizi e dati delle PA classificati come di livello critico, verificare che esista un elenco completo di personale, interno ed esterno, con ruoli di responsabilità nei processi di cybersecurity.

7. Solo per servizi e dati delle PA classificati come di livello critico, verificare l'esistenza dell'elenco delle figure analoghe sia all'incaricato che al referente tecnico, presso terze parti, in relazione alle dipendenze esterne, e presso il soggetto in relazione alle dipendenze interne. Successivamente, richiedere al soggetto, come prova, un documento in cui sia contenuta la valutazione delle competenze dell'incaricato e del referente tecnico, in funzione della tipologia di dipendenza.Infine, contattare tutte le articolazioni competenti del soggetto, per controllare che abbiano una copia dell'elenco contenente tali figure analoghe.

8. Solo per servizi e dati delle PA classificati come di livello critic, verificare che l'incaricato abbia firmato un documento in cui garantisce la collaborazione con l'agenzia per le attività riportate nel DL 105/2019 e quelle riportate nel DL 82/2021.

2.5 ID.GV-1

È identificata e resa nota una policy di cybersecurity

Metodo di verifica e ispezione

1. **MS Azure:** Esiste un documento che descrive la politica di cybersecurity di Microsoft, scaricabile a questo link[40]. Tale documento è un documento sintetico. Al contrario un documento più di dettaglio sulla policy di cybersecurity di Microsoft è disponibile qui[41]

   Google Cloud: Non esiste un documento pubblico che esprime la policy di cybersecurity di Google, però a questo link[42], è possibile visionare il white paper che dà una panoramica sulla sicurezza di Google Cloud. In questo documento sono descritti processi e procedure e misure tecnologiche che vengono utilizzate per raggiungere alcuni obiettivi di sicurezza. Per un documento di maggior dettaglio bisogna contattare il team del Cloud Provider.

   AWS: AWS non pubblica un documento che descrive le politiche i processi e le procedure di cybersecurity. Per questo tale documento va richiesto al Cloud Provider, verificando che siano descritti le politiche, i processi e le procedure di cybersecurity.

2. **MS Azure:** I documenti citati al punto uno contengono al loro interno o una cronistoria che indica tutte le revisioni che sono state effettuate, che sono annuali, oppure la dichiarazione che vengono revisionati annualmente o in un periodo di tempo prestabilito.

   Google Cloud: Ovviamente il documento al punto uno è un white paper e questo comporta che non è detto che sia aggiornato costantemente. Per questo quando si richiede il documento contenente la policy è necessario verificare che questo sia approvato dal CSP e aggiornato.

   AWS: Una volta richiesto il documento citato al punto uno è necessario verificare che sia aggiornato almeno annualmente, controllando che esistano prove dell'aggiornamento.

3. Solo per servizi e dati delle PA classificati come di livello critico, verificare che esista una procedura di identificazione e gestione, all'interno del CSP, con un processo di governance strutturato, che si attiva se viene rilevato uno scostamento dai livelli minimi di sicurezza definiti al punto uno.

4. Solo per servizi e dati delle PA classificati come di livello critico, verificare che esista, nel CSP, un documento che regola la pianificazione quali siano i ruoli, i processi di implementazione, operazione, valutazione e miglioramento dei programmi di cybersecurity.

2.6 ID.GV-4

La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity

Metodo di verifica e ispezione

1. Richiedere al Cloud Service Provider il documento che descrive i processi di gestione del rischio, verificando che contempli i rischi legati alla cybersecurity.

2. **MS Azure:** Come riportato in questo documento[43], per l'ERM viene utilizzato il framework basato su Committee of Sponsoring Organizations of the Threadway Commission(COSO). Il processo di ERM, quindi, è definito in maniera formale e si allinea allo standard ISO 31000:2009. Nonostante ciò, non viene pubblicato in maniera integrale un programma di Enterprise Risk Management da parte di Microsoft. Per questo motivo per un controllo più approfondito è comunque necessario, e va richiesto un documento che descriva il programma formale di ERM, verificando l'inclusione di tutti gli elementi riportati nel controllo omonimo.

   Google Cloud: Richiedere un documento che descriva il programma formale di ERM, verificando l'inclusione di tutti gli elementi riportati nel controllo omonimo.

   AWS: Richiedere un documento che descriva il programma formale di ERM, verificando l'inclusione di tutti gli elementi riportati nel controllo omonimo.

2.7 ID.RA-1

Le vulnerabiltà delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate

Metodo di verifica e ispezione

1. Richiedere al Cloud Provider il piano aggiornato di verifica e test di sicurezza, per controllarne l'esistenza e per verificare quali sono le attività per la valutazione del livello di sicurezza cibernetica, l'efficacia delle misure di sicurezza tecniche e procedurali e la periodicità e modalità di esecuzione dei test.

2. Richiedere al Cloud Provider un documento che descriva le procedure per la gestione dei rischi associati a variazioni nell'ambito di asset organizzativi. Verificare, poi, che questo documento sia aggiornato almeno su base annuale, controllando che ne esista una cronistoria allegata.

3. **MS Azure:** Sono pubblicati dei report sul processo di vulnerability assessment e penetration testing sull'infrastruttura di Azure, che contengono tutti i punti indicati nel controllo omonimo. Infatti come visibile in questo documento[44], le relazioni periodiche dei penetration test condotti sul servizio contengono tutti gli elementi riportati nel controllo omonimo.

   Google Cloud: Google conduce autonomamente i test di penetrazione sulla sua infrastruttura cloud, e quindi non pubblica dei report relativi a questi test. Per questo se si vogliono avere dei report sul processo di vulnerability assessment e pentesting sull'infrastruttura Google cloud è necessario richiederli direttamente al team per la sicurezza di Google cloud.

   AWS: AWS non pubblica report sui penetration test che conduce sulla sua infrastruttura, per questo è necessario richiedere al cloud provider i report sul processo di vulnerability assessment e pentesting.

4. Richiedere al Cloud Provider la documentazione sulla correzione delle vulnerabilità.

2.8 ID.RA-5

La misura richiede che le minacce, le vulnerabilità e le relative probabilità di accadimento e i conseguenti impatti sono utilizzati per determinare il rischio.

Metodo di verifica

1. Richiedere una relazione che esplicita come è stata condotta l'analisi del rischio dal CSP, per verificare che sia stata eseguita tenendo conto di minacce, vulnerabilità, e relative probabilità di accadimento e impatti.
2. Nell'analisi della relazione, verificare che nel processo di analisi del rischio siano tenute in considerazione dipendenze esterne e interne.
3. Nell'analisi della relazione, verificare che siano individuati tutti i fattori di rischio, e poi verificare che sia stato eseguito correttamente il processo di ponderazione.
4. Solo per servizi e dati di livello critico, verificare che esista il documento aggiornato di valutazione del rischio con:
   a. Identificazione di minacce interne ed esterne e delle probabilità di accadimento.
   b. Le vulnerabilità.
   c. Gli impatti, descritti e valutati, sul servizio cloud.
   d. Identificazione, analisi e ponderazione del rischio.

2.9 ID.SC-1

I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione.

Metodo di verifica e ispezione

1. Richiedere il documento in cui sono descritti i processi di risk management al CSP e verificare che siano definiti i processi di gestione per la catena di approvvigionamento cyber.
2. Verificare che nel documento al punto uno sia certificato che i processi sono stati approvati dal vertice del soggetto.
3. Solo per Amministrazioni che erogano servizi di livello critico, verificare che nel documento siano presenti politiche e procedure finalizzate all'implementazione e l'applicazione del modello SSRM. Verificare che queste politiche e procedure siano riviste almeno su base annuale, controllando che esista una cronistoria del documento.

4. Solo per i servizi e dati di livello critico, verificare che il modello SSRM sia applicato in tutta la catena di approvigionamento cyber. Di solito questo viene garantito se ci si rivolge maggiori CSP come riportato in questo articolo[45]

5. Nel momento in cui si sceglie un CSP come Azure, Google Cloud o AWS, questo controllo viene automaticamente soddisfatto. I riferimenti sono i seguenti: AWS[46] Azure[47] Google Cloud[48]

6. Solo per servizi e dati di livello strategico verificare l'esistenza del documento che contenga i processi del punto uno e del punto due.

2.10 ID.SC-2

I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber

Metodo di verifica e ispezione

1. Solo per servizi, sistemi e dati di livello critico, verificare che siano adottate le seguenti misure di sicurezza per la catena di approvigionamento cyber:
   a. Controllare che esista una prova reale del fatto che l'organizzazione di cybersecurity del Cloud Provider e l'incaricato, di cui alla sottocategoria ID.AM-6, siano stati coinvolti nel processo di fornitura.
   b. Controllare che il CSP rispetti il requisito di fungibilità e abbia individuato altri fornitori nel caso in cui tale requisito non sia soddisfatto entro la scadenza.
   c. **MS Azure:** Scaricando la lista di tutti i subprocessor di microsoft, che è disponibile qui[49] si evidenzia che Microsoft differenzia molto i fornitori del servizio Cloud, raggiungendo un ottimo grado di resilienza. Come si vede ogni funzione viene affidata a un fornitore diverso e non si affida sempre allo stesso fornitore.

      Google Cloud: Anche Google Cloud ha una vasta lista di subappaltatori e fornitori da cui prende dei servizi, come visibile in questa pagina[50]. Qui si vede che Google ha moltissimi fornitori tendendo a differenziare molto.

      AWS: Relativamente a questo CSP la lista di tutti i subprocessor che forniscono servizi al cloud provider è visibile qui[51]. AWS tende a mantenere la propria infrastruttura "in casa" senza ricorrere moltissimo a dei fornitori esterni.
   d. Richiedere al cloud provider una relazione contenente una valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi. Nella valutazione controllare che siano stati considerati la qualità dei prodotti e delle pratiche di sicurezza del fornitore, verificando il controllo che essi hanno sulla loro catena di approvvigionamento cyber e la priorità che danno agli aspetti di sicurezza. Inoltre, deve essere valutata la capacità del fornitore

di Servizi Cloud e dei suoi partner terzi di garantire l'approvvigionamento delle risorse e allo stesso tempo assistenza e manutenzione.

2. **MS Azure:** La lista di tutti i fornitori, aggiornata al 2023, è disponibile qui[49]. Per quanto riguarda la documentazione relativa al processo di valutazione questa va richiesta al Cloud Service Provider.

   Google Cloud: Anche qui la lista di tutti i fornitori aggiornata al 2023 è visibile a questa pagina[50]. Richiedere poi al CSP una relazione del processo di valutazione dei fornitori.

   AWS: La lista di tutti i fornitori aggiornata al 2023 è disponibile qui[51]. Richiedere poi al CSP una relazione del processo di valutazione dei fornitori.

3. Solo per Amministrazioni che erogano servizi di livello strategico procedere con queste azioni:
   - Controllare, analizzando la relazione menzionata al punto uno lettera d, che il CSP abbia valutato l'affidabilità tecnica dei fornitori tenendo conto di:
     i. disponibilità del fornitore a condividere il codice sorgente
     ii. certificazioni o evidenze che permettano di valutare la qualità del processo di sviluppo software del produttore
     iii. adozione da parte del produttore di procedure e strumenti tecnici per garantire l'autenticità e integrità del o software o firmware installato nei beni ICT
     iv. adozione da parte del produttore di procedure o strumenti tecnici per garantire corrispondenza univoca tra codice sorgente e codice oggetto installato ed eseguito
   - Richiedere al CSP una relazione in cui siano descritti tutti i processi e strumenti tecnici adottati per:
     – valutare la sicurezza e la qualità del codice sorgente, ad esempio analizzatori statici di codice, oppure test di penetrazione.
     – acquisire il codice oggetto dai beni ICT.
     – verificare la corrispondenza univoca tra codice sorgente e codice oggetto, attraverso meccanismi di firma digitale del codice.

     In seguito richiedere una prova concreta al Cloud Provider, che permetta di stabilire che questi processi siano adottati effettivamente.

2.11 ID.SC-3

I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber

Metodo di verifica

Verificare che sia le misure di sicurezza implementate dal CSP in relazione a dipendenze interne, sia le misure di sicurezza implementate da terzi affidatari di servizi esterni, sono coerenti con le misure di sicurezza applicate al servizio Cloud. Verificare che contratti e accordi siano aggiornati di conseguenza.

2.12 ID.SC-4

Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali

Metodo di verifica

1. Richiedere al CSP il documento aggiornato che descrive il processo, le modalità e la cadenza delle valutazioni per fornitori e partner terzi.
2. Richiedere al CSP il documento contenente la pianificazione aggiornata di audit e verifiche, nonché la documentazione relativa e i registri di quelli effettuati.
3. Richiedere al CSP una relazione che descriva il processo di Audit Management che permetta valutazioni indipendenti e di garanzia, almeno su base annuale, e che tenga conto del rischio
4. Richiedere al CSP, per verificarne l'esistenza, documenti ufficiali che stabiliscano le politiche e procedure di audit, e documenti ufficiali o verbali di riunioni che testimoniano che le politiche siano riviste almeno annualmente.
5. Richiedere al CSP un documento ufficiale approvato in cui è definito un piano di Remediation.

2.13 PR.AC-1

Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza

Metodo di verifica

1. Utilizzando le API del servizio di directory utilizzato dal CSP per la gestione delle identità, o accedendo al servizio di directory attraverso il sistema IAM o il sistema PAM, ottenere la lista di credenziali immagazzinate nel Directory Information Base. Successivamente verificare che non ci siano credenziali duplicate per ogni membro del personale del soggetto. Successivamente per ogni entry ottenuta dal servizio di directory interrogato, controllare gli attributi della entry per collegare la entry ai permessi associati alle credenziali. A quel punto, verificare per ogni entry di un nodo del Directory Information Tree, che rappresenta una funzione aziendale, che questa non abbia dei permessi che sono posseduti anche da altre entry di altri nodi dell'albero. In questa maniera se il DIT è conforme all'organigramma del CSP e non ci sono due entry che hanno uno stesso insieme di permessi in due entry differenti, allora viene

rispettato il principio di segregazione delle funzioni. Nel caso in cui si acceda alle identità mediante, invece, un sistema di Identity and Access Management o di Priviliged Access Management, allora è necessario verificare che non ci siano credenziali, facenti capo a diverse unità organizzative, che possiedano uno stesso insieme di permessi. Infine, accedere ai log del servizio di directory o a un registro delle attività o del sistema di Identity and Access Management o di Priviliged Access Management e verificare che le credenziali siano state cambiate con una cadenza proporzionata ai privilegi di utenza.

2. Richiedere al CSP un documento che descriva le politiche e le procedure per la gestione delle credenziali e verificare che esista una cronistoria del documento contenente tali politiche che certifichi il loro aggiornamento su base annuale. Infine controllare che il CSP abbia fornito, a seguito di accordo precedente, la possibilità di visionare queste politiche all'Amministrazione che migra su Cloud.

3. Richiedere al fornitore di servizi Cloud una relazione tecnica dettagliata che descriva i meccanismi di gestione, memorizzazione e revisione delle informazioni in maeria di credenziali, identità di sistema e livello di accesso.

4. Guadagnare l'accesso al sistema di Identity Access Management del CSP, e verificare che tra gli attributi delle identità, o credenziali sia presente una indicazione sul tempo di vita delle credenziali. Nel caso in cui il tempo di vita delle credenziali non sia riportato, allora il controllo non è superato. Se, invece, esiste tale indicazione, verificare che le credenziali abbiano un tempo di vita inferiore a quello massimo consentito e successivamente verificare che il sistema IAM in uso dal CSP configuri un meccanismo di rotazione tale per cui sia possibile aggiornare o invalidare delle credenziali a seguito di una variazione di utenza.

5. In questo caso è sufficiente verificare che il sistema di Priviliged Access Management del CSP permette alle utenze privilegiate di accedere al portale di gestione delle identità, oppure tramite le API del servizio di directory al Directory Information Base, fornendo un certificato digitale, tramite smart card o altro supporto, o utilizzando una tecnica alternativa di pari livello di sicurezza. Se ogni dipendente privilegiato non utilizza un certificato proprio per accedere al sistema di PAM o alle menzionate API, allora il controllo non è superato.

6. Richiedere al CSP un documento che descriva la pianificazione aggiornata degli audit di sicurezza delle identità digitali e che esista un registro che riporti tutti gli audit effettuati, e la relativa documentazione.

7. Solo per sistemi e dati di livello critico verificare l'esistenza di un documento aggiornato che contenga tutte le cose menzionate nella sotto-categoria in esame.

2.14 PR.AC-3

L'accesso remoto alle risorse è amministrato.

Metodo di verifica

1. Il monitoraggio degli accessi da remoto di solito viene svolto attraverso il controllo dei log di sistema emessi dalle risorse accedute. Ogni log emesso testimonia un evento che accade nella macchina, e un accesso viene considerato come un evento. Allora, per soddisfare questa sottocategoria, è necessario che l'organizzazione di cybersecurity abbia installato un sistema SIEM, a cui si inviati tutti i log delle risorse, in maniera tale che esso possa correlarli e analizzarli al fine di segnalare gli accessi da remoto che vengono fatti su tali macchine.

2. Per verificare l'implementazione di un sistema di controllo degli accessi e di un sistema di autenticazione, è necessario operare un penetration testing sull'infrastruttura del CSP. Per verificare che sia previsto un meccanismo di controllo accessi è necessario assicurarsi che:

   - I permessi di accesso a qualsiasi risorsa siano controllati ad ogni richiesta.
   - Le richieste siano negate a meno che non sia soddisfatta una certa regola tra quelle previste.
   - Impedire che un fallimento di un controllo di autorizzazione comporti l'accesso alla risorsa.

   Per verificare l'esistenza di sistemi di autenticazione è sufficiente operare delle richieste alle risorse del CSP e successivamente controllare se ci sono vie per accedere a quelle risorse senza essere passati per un meccanismo di autenticazione noto. Nel caso in cui esistano modi o tecniche per accedere a una risorsa senza previa autenticazione il controllo non è superato. Per verificare che ci sia una contabilizzazione e registrazione degli accessi è sufficiente verificare che il sistema di PAM del cloud provider abbia questa funzionalità, o che sia implementato un sistema ad hoc per soddisfare questo task.

3. Verificare che il Cloud Service Provider utilizzi per la gestione delle identità dei suoi dipendenti processi e applicazioni o un sistema di Active Directory, o un sistema di Identity and Accessa Management (IAM). Inoltre, verificare che le utenze privilegiate siano gestite attraverso un sistema di Priviliged Access Management

4. Verificare che il CSP mantenga in una o più macchine a sua disposizione, un log di tutti gli accessi da remoto operati su macchine del CSP stesso che vengono utilizzate dai clienti.

5. Solo per servizi, dati e sistemi di livello critico, verificare che esista il documento aggiornato di dettaglio contenente le politiche di sicurezza per la definizione delle attività consentite tramite l'accesso remoto e le misure di sicurezza adottate e i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

6. Solo per servizi, dati e sistemi di livello strategico, verificare che esistano dei verbali o un archivio che riporta tutte le modifiche alle politiche e alle procedure di sicurezza. Verificare che queste politiche e procedure siano revisionate su base annuale.

7. Solo per servizi, dati e sistemi di livello strategico, richiedere al CSP una relazione tecnica in cui si descrive il meccanismo di autorizzazione congiunta con l'Amministrazione che è stato implementato nel caso in cui ci siano accessi ai dati dell'Amministrazione mantenuti dal fornitore di servizi Cloud. Altrimenti nel caso in cui non fosse possibile per il soggetto mettere in piedi e implementare questo meccanismo di autorizzazione congiunta con l'Amministrazione, verificare che esistano dei processi o dei mezzi attraverso cui il soggetto può contattare l'Amministrazione nel più breve tempo possibile.

8. Solo per servizi, dati e sistemi di livello strategico, richiedere al Cloud Service Provider una relazione tecnica dettagliata in cui sia descritta la gestione di tutte le operazioni che prevedono l'accesso ai dati che l'Amministrazione affida al soggetto. Verificare che la gestione di queste operazioni avvenga in ottemperanza con i criteri di user management e logging delle utenze privilegiate.

2.15 PR.AC-4

I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.

Metodo di verifica

1. Verificare che siano state definite per iscritto in un documento ufficiale:
    a. Le risorse censite a cui è necessario accedere, per quali funzioni e quali autorizzazioni.
    b. i gruppi di utenti e i loro privilegi rispetto alle risorse a cui possono accedere e con quali autorizzazioni.
    c. L'assegnazione degli utenti ai gruppi.

2. Tale controllo va verificato attraverso un processo di penetration testing. Per prima cosa, una volta guadagnato l'accesso al sistema informativo con delle credenziali legittime o in altri modi è necessario verificare alcune cose:
    - Non ci sono modi di guadagnare accesso a dati o servizi non necessari per lo svolgimento delle funzioni associate a determinate credenziali, rispettando il principio del privilegio minimo. Non devono essere possibili, perciò, SQLi o altri meccanismi di accesso inusuale ai dati, che permettano di accedere a dati altrimenti non accessibili. Inoltre, non deve essere possibile rubare cookie di sessione o token, tramite XSS, per accedere a servizi non necessari per svolgere la propria mansione.
    - Nello svolgimento di una transazione qualsiasi come la validazione di un accesso, il salvataggio di dati in uno o più storage, il rollback di codice etc... la pipeline della transazione deve prevedere che ogni passaggio sia gestito da un entità diversa. Per verificare tale cosa è sufficiente, nel momento in cui parte una transazione, assicurarsi che un singolo dipendente associato a delle credenziali non sia in grado di portarla a termine da solo anche attraverso meccanismi non convenzionali.

3. Se il cloud Service Provider utilizza un sistema di Privileged Access Management per la gestione delle identità e dei ruoli di accesso privilegiato, verificare per ognuna delle identità e dei ruoli definiti nel sistema di PAM, che questo non possieda più di un elemento tra i tre citati nel controllo omonimo. Nel momento in cui, ad esempio, un ruolo o identità ha la capacità di effettuare un accesso amministrativo ai dati e contemporaneamente è in grado di esercitare delle funzioni crittografiche, allora il controllo non è soddisfatto.

4. Solo per sistemi, servizi e dati di livello critico, verificare l'esistenza del documento che descrive i processi al punto uno.

5. Richiedere al Cloud Service Provider di mantenere un registro dedicato, accessibile dall'Amministrazione, in cui siano documentati tutti i tentativi di accesso ai dati dell'Amministrazione da parte del personale del soggetto e da terze parti. Verificare che tra tutti i tentativi di accesso solo quelli autorizzati dall'organizzazione di cybersecurity del soggetto possano andare a buon fine. Inoltre, verificare che sia concessa la possibilità di contestare l'accesso nel caso in cui non fosse essenziale l'accesso ai dati, per erogare le funzionalità necessarie all'Amministrazione e che servono ad essa per erogare il servizio.

2.16 PR.AC-5

L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)

Metodo di verifica

1. Verificare che esistano documenti scritti che riportino le politiche e le procedure per la sicurezza delle infrastrutture di rete su cloud. Verificare, inoltre, che esistano dei documenti che provino che le politiche e le procedure sono revisionate e aggiornate su base annuale.

2. Verificare che esista una pianificazione scritta per il monitoraggio della disponibilità, qualità e capacità delle risorse di rete di fornire le prestazioni richieste.

3. Solo per Amministrazioni che erogano servizi di livello strategico verificare che esista un documento di dettaglio contenente:
   a. le politiche di sicurezza adottate per la segmentazione o segregazione delle reti;
   b. la descrizione delle reti segregate/segmentate;
   c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza;
   d. le modalita con cui porte di rete, protocolli e servizi in use sono limitati e/o monitorati

2.17 PR.AC-7

Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti del soggetto, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)

Metodo di verifica e ispezione

1. Richiedere al CSP una relazione che documenti le politiche e le procedure per l'accesso ai sistemi. Per verificare l'implementazione di queste politiche e procedure, è sufficiente cercare di accedere a uno dei sistemi o macchine del CSP, che vengono messe a disposizione dei clienti e verificare che siano implementati i meccanismi di autenticazione descritti. Inoltre quando si tenta di accedere a servizi privilegiati, come i servizi di PAM, o ai dati, verificare che sia necessaria una procedura di autenticazione a più fattori.

2. **MS Azure:** Utilizzando Azure e Microsoft Entra ID è possibile sempre attivare l'autenticazione a più fattori per l'accesso alle applicazioni, infrastrutture o piattaforme sul cloud microsoft, in quanto è sufficiente definire una Conditional Access Policy secondo quanto specificato dal seguente tutorial[52]. In più nella documentazione di Azure sono chiari e trasparenti i modi utilizzati per implementare l'autenticazione a due fattori

   Google Cloud: Dalla documentazione di Google Cloud, si deduce che se si utilizza Cloud Identity è sempre possibile attivare il processo di autenticazione a più fattori per delle risorse dell'organizzazione. Inoltre a questa pagina[53] sono disponibili e documentati tutti i metodi di autenticazione a due fattori disponibili in Google Cloud.

   AWS: Dalla documentazione di AWS, utilizzando IAM Identity Center si deduce che è sempre possibile per l'Amministrazione attivare l'autenticazione a più fattori. Le modalità di autenticazione a due fattori disponibili in AWS sono documenatate al seguente link[54].

3. Solo per Amministrazioni che erogano servizi di livello strategico, verificare che esista il documento aggiornato che contenga sia le modalità di autenticazione disponibili, sia la loro assegnazione alle categorie di transazione.

2.18 PR.AT-1

Il personale del soggetto è informato e addestrato

Metodo di verifica

1. Richiedere al Cloud Provider il documento di dettaglio e aggiornato con i contenuti dell'addestramento e le modalità di verifica dell'acquisizione dei contenuti.

2. Controllare, nell'analisi del documento al punto uno, che l'addestramento e la formazione forniti agli utenti del soggetto, in relazione ai ruoli, prevedano tutte le cose riportate nel controllo omonimo.

3. Solo per amministrazioni che erogano servizi critici, verificare che per ogni membro del personale del Cloud provider esista un registro aggiornato, comprensivo delle istruzioni ricevute.

2.19 PR.AT-2

Gli utenti con privilegi(es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità

Metodo di verifica

1. Richiedere al CSP una relazione che definisce i contenuti dell'istruzione fornita al personale e le modalità di verifica dell'acquisizione dei contenuti.

2. Richiedere al CSP un documento in cui siano certificati per ogni membro del personale del soggetto i privilegi e le istruzioni ricevute.

3. Solo per amministrazioni che erogano servizi di livello strategico verificare che esistano nel Cloud Provider documenti di dettaglio e aggiornati che riportino le cose espresse nei due punti precedenti.

2.20 SC-SI-PR.DS-1-01

I dati delle pubbliche amministrazioni, ivi incluse quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.

Metodo di verifica

La localizzazione dei dati all'interno delle region o delle zone di disponibilità messe a disposizione da un Cloud Service Provider è un aspetto la cui responsabilità è in parte in carico al cliente. Ogni cliente di un CSP può scegliere in quale regione richiedere il provisioning di un servizio di elaborazione o storage. D'altra parte il Cloud Provider assicura che i dati salvati o elaborati mediante quei servizi siano custoditi e replicati solo all'interno della region indicata, e che questi, nel tragitto dai sistemi dell'Ammininstrazione ai data center del fornitore, non siano instradati prima verso altre region. Da cui per verificare questo aspetto sono necessarie due azioni:

- Richiedere al fornitore di servizi Cloud un'ampia descrizione degli endpoint e delle regole di instradamento nella sua rete globale, al fine di verificare come i dati sono instradati verso le region dei data center.

- Studiare la documentazione del Cloud Service Provider in maniera tale da individuare strumenti adatti che permettano all'Amministrazione e ai suoi dipendenti di operare il provisioning di servizi e risorse, e di salvare dati sono nelle region europee.

2.21 PR.DS-1

I dati memorizzati sono protetti

Metodo di verifica e ispezione

1. **MS Azure:** Azure definisce chiaramente quali sono le politiche, processi, metodologie e tecnologie per la sicurezza dei dati memorizzati su cloud come riportato nel white paper sulla sicurezza di Azure scaricabile al seguente link[55]. In particolare nel capitolo sulla Data Protection sono riportati modalità e riferimenti alle politiche di sicurezza e alle procedure e tecnologie per implementarle.

   Google Cloud: Anche Google definisce quali sono le politiche, processi, metodologie e tecnologie per la sicurezza dei dati memorizzati su cloud come indicato nel white paper sulla sicurezza di Google Cloud scaricabile al seguente link[56]. Qui nel capitolo due nelle sezioni dalla 2.1 alla 2.4 sono citati i meccanismi uilizzati per la protezione dei dati in transito e sul cloud, oltre che le politiche di data governance e di data residency.

   AWS: Il white paper sulla sicurezza di Amazon elenca quali sono le politiche di sicurezza di AWS in accordo al GDPR e agli standard di sicurezza. Inoltre tale documento contiene anche la descrizione di tutti gli strumenti di controllo di accesso ai dati e protezione dei dati che servono a implementare le politiche di sicurezza. Tale documento è scaricabile al seguente link[57].

2. Molti Cloud Provider, per facilitare l'utilizzo all'utente finale, astraggono dai metadati e non dichiarano pubblicamente nelle documentazioni dove questi vengono salvati. Per questo è necessaria un'interlocuzione con i Cloud Provider per capire come gestiscono i metadati, e se scelgono o di salvarli nella stessa region in cui è collocata la risorsa, oppure in una region differente anche abbastanza lontana da quella in cui è salvata la risorsa. A seconda della policy adottata, per ogni risorsa utilizzata dall'Amministrazione è necessario ispezionare la formattazione dei metadati, per stabilire se questi contengano informazioni legate all'Amministrazione.

4. **MS Azure:** Per quanto riguarda la crittografia dei dati e la gestione delle chiavi nella documentazione Azure alcuni dettagli relativi alle procedure e alla gestione delle chiavi sono riportati nei seguenti link: procedure[58] gestione delle chiavi[58]. Andando nello specifico delle chiavi ulteriori informazioni si trovano a questo link[59] e anche in questa pagina[60]. Per quanto riguarda gli auditing e la verifica periodica delle politiche procedure e processi di crittografia, è necessario interfacciarsi con Azure, in quanto tale aspetto non è menzionato nella documentazione. Infine,

relativamente all'uso delle librerie crittografiche per la generazione delle chiavi e all'indicazione degli algoritmi utilizzati e anche ai generatori di numeri casuali consultare il seguente link[61]

Google Cloud: La documentazione di Google Cloud, in materia di crittografia, fornisce un documento aggiornato che reca la descrizione delle procedure di crittografia e la gestione delle chiavi. Per la cosiddetta crittografia dei dati at rest si consideri il seguente documento[62], mentre per la crittografia dei dati in transito si consideri la seguente pagina[63]. Per quanto riguarda la gestione e l'aggiornamento di chiavi gestite dal cliente si rimanda al seguente documento[64], con la possibilità di interagire con il CSP per ricevere ulteriori informazioni. Per quanto riguarda la verifica periodica dei sistemi non sembra essere disponibile online e quindi è necessario contattare Google Cloud e chiedere delucidazioni. Invece, relativamente alla generazione di chiavi sono utilizzate le librerie crittografiche citate nei white paper allegati prima, cioè Tink e Boring Crypto. Tink, che è la libreria comune di Google ha una documentazione open-source e accessibile al seguente link[65], in particolare la sezione design di Tink. Boring Crypto è documentata invece al seguente link[66].

AWS: Le procedure di crittografia, gestione delle chiavi sono descritte sempre nel whitepaper sulla sicurezza di AWS. Ad alto livello le procedure di crittografia per la protezione dei dati sono descritte nel white paper allegato al controllo numero uno. Invece, per avere una panoramica su come vengono gestite le chiavi bisogna considerare un altro white paper scaricabile al seguente link[67]. Inoltre in questo white paper al paragrafo "Cryptographic primitives" sono descritte le primitive crittografiche utilizzate, non solo per la cifratura simmetrica e asimmetrica, ma anche per la generazione di numeri casuali e la generazione delle chiavi stesse. Inoltre altre informazioni sulle chiavi crittografiche e la loro gestione sono riportate nel seguente documento[68]. Allo stesso modo degli altri due provider per sapere come avviene la verifica periodica dei sistemi e l'auditing e la revisione delle procedure è necessario contattare AWS per chiedere delucidazioni.

4bis. **MS Azure:** Come riportato al seguente link[69] è possibile nel cloud di Azure per l'amministrazione gestire in maniera autonoma le chiavi crittografiche, utilizzando delle soluzioni di key vault come Azure Managed HSM o Azure Dedicated HSM o Azure Payment HSM. Inoltre con queste soluzioni c'è anche la possibilità di generare le chiavi all'interno dei propri HSM on-premise, per poi trasferirle in Azure Managed HSM. Per quanto riguarda la privatezza e la segretezza delle chiavi, questi due requisiti viene raggiunta perché, come descritto in questa pagina[70] e in questa pagina[71], l'accesso al key vault e alle chiavi è autenticato grazie a Microsoft Entra ID. In più è possibile configurare una politica di access control sia per tutto il key vault, sia per le singole chiavi all'interno del key vault per la gestione.

Google Cloud: É garantita la possibilità di gestione autonoma delle chiavi da parte dell'Amministrazione attraverso il servizio di Cloud Key Management di Google. Infatti come riportato nella pagina di overview del

prodotto, qui[72], le soluzioni Cloud KMS keys, Cloud HSM keys e Cloud EKM keys, a vari livelli di sicurezza danno la possibilità all'Amministrazione di gestire le proprie chiavi crittografiche. Inoltre, ogni chiave crittografica ha un attirbuto specifico purpose che consente di specificare lo scopo che ha quella chiave, e tale attributo non può essere cambiato dopo la creazione della chiave. In più, le chiavi sono mantenute private e segrete attraverso i livelli di protezione della chiave, che è un altro attributo della chiave non modificabile dopo la creazione, e attraverso le KEK e la crittografia envelope.

AWS: Anche Amazon ha una soluzione di gestione delle chiavi crittografiche. AWS KMS permette all'amministrazione di gestire autonomamente le chiavi crittografiche utilizzate per la cifratura dei dati dell'amministrazione stessa. Inoltre, tra gli attributi le chiavi possiedono un attributo KeyUsage che chiarifica qual è lo scopo della chiave, se la cifratura, la decifratura, o la firma digitale. Per quanto riguarda la privatezza delle chiavi, le metodologie con cui sono protette e rese private le chiavi sono descritte al seguente link[73].

5. **MS Azure:** Nel caso in cui si sia scelta una soluzione di tipo managed HSM BYOK(Bring Your Own Key) allora è necessario verificare che l'amministrazione preveda i processi per la revoca, prima della fine del periodo di validità, di una chiave compromesa, o nel caso in cui un'entità non fa più parte dell'organizzazione. Nel caso in cui non si sia scelta la soluzione BYOK, comunque mediante Azure portal o mediante la azure CLI o mediante le Azure API sono implementate procedure per la revoca delle chiavi. Dalla CLI di azure usando in successione i comandi seguenti:

```
az keyvault key set-attributes -name <nome_chiave> -enable
                  false
     az keyavult key delete -name <nome_chiave>
         az keyavult key purge -name <nome_chiave>
```

si revoca e si rimuove una chiave dal vault o dall'HSM. Se si utilizzano le REST API di Azure, il processo per cambiare lo stato della chiave è descritto in questa pagina[74]. Per cancellare ed eliminare definitivamente dal vault la chiave si fa riferimento ai comandi descritti nelle seguenti pagine: cancellazione[75] eliminazione[76]

Google Cloud: Nel caso del cloud Google quando una chiave viene rinnovata, viene creata un'altra versione di quella chiave. Quindi, nel momento in cui i dati sono cifrati, si tiene conto della versione della chiave con cui sono stati cifrati. Quindi se si deve sospendere una chiave, perché compromessa o per altri motivi, è necessario creare una nuova versione della chiave, decifrare tutti i dati cifrati con la precedente versione e ri-cifrarli con la nuova versione. Solo dopo aver compiuto questi passaggi è possibile procedere con l'invalidazione e rimozione della versione compromessa. Ovviamente Google Cloud implementa delle procedure che permettono di fare tutte queste cose, e l'obiettivo è raggiungibile secondo i seguenti passi:

a) Ruotare manualmente la chiave come riportato nel seguente link[77].

b) Decifrare e ricifrare i dati cifrati con la chiave compromessa con i passaggi esposti in questa pagina[78].

c) Disabilitare la versione compromessa della chiave nella maniera indicata in questa guida[79].

d) Distruggere la versione della chiave seguendo le indicazioni riportate qui[80].

Quindi Google implementa le procedure e le misure tecniche per la revoca anticipata delle chiavi.

AWS: AWS implementa dei processi e delle procedure per revocare e rimuovere le chiavi crittografiche, prima della fine del periodo di validità. Esso permette prima di disabilitare una chiave, in maniera da renderla inutilizzabile, per poi dare la possibilità di schedulare la cancellazione della chiave che al massimo avviene 30 giorni dopo averla programmata. Per disabilitare una chiave sono messe a disposizione le misure tecniche descritte in questa guida[81]. Allo stesso modo per schedulare la cancellazione di una chiave le misure tecniche e le procedure sono descritte in questa pagina[82]. Se si tratta di chiavi multi-regione allora la procedura per la cancellazione è descritta in questa guida[83], mentre per chiavi importate in AWS KMS dall'utente la procedura di cancellazione è descritta qui[84]. Ovviamente come accade in altri Cloud Provider nel momento in cui si cancella una chiave tutto il materiale cifrato con quella chiave non è più recuperabile e quindi se qualcosa deve essere mantenuto, prima di cancellare la chiave, bisogna decifrare il materiale, e ri-cifrarlo con una nuova chiave.

6. **MS Azure:** Per il periodo di aggiornamento delle chiavi è necessario controllare che chi ha migrato su Cloud abbia configurato correttamente la Key Rotation Policy come indicato in questa guida[85]. Grazie alla key rotation policy, configurabile attraverso o il portale di Azure o la Azure CLI o altre interfacce è possibile prevedere delle procedure per la disattivazione e la creazione di nuove chiavi al momento della scadenza delle vecchie. Inoltre grazie alla console di Azure e alle REST API sono implementati una serie di metodi predefiniti per la gestione delle chiavi e per la loro sospensione. Alcuni metodi per la CLI e le API sono riportati nei seguenti link: CLI[86] API[87]

   Google Cloud: Nel cloud Google esistono delle procedure che permettono di creare una nuova chiave o versione di una chiave all'interno di Cloud Key Management Service. La procedura per la creazione di una chiave, simmetrica o asimmetrica è descritta nel seguente documento[88]. Allo stesso modo esistono delle procedure per la sospensione delle chiavi prima della scadenza. Infatti, è possibile configurare la rotazione delle versioni di una chiave seguendo le guide esposte di seguito: Configurare la rotazione automatica di una chiave[89], Decifrare e ri-cifrare i dati e schedulare la distruzione della chiave[78], Disabilitare la chiave[79], Eliminare una versione disabilitata[80]. Le ultime due guide vanno seguite nel caso in cui non si sia schedulata la distruzione della versione.

AWS: AWS implementa dei processi per la creazione delle chiavi gestite dall'utente, come riportato in questa pagina[90], dove sono indicati i riferimenti alle guide passo per la creazione di ogni tipo di chiave creabili in AWS KMS. Inoltre come descritto in questa guida[91], AWS permette di configurare la rotazione automatica delle chiavi in maniera tale da poter generare una nuova chiave al momento della scadenza. Chiaramente per la cancellazione della chiave e la sua disattivazione è necessario agire come riportato nelle guide allegate al controllo numero 5

6bis. Garantito nella stessa maniera di come riportato nel punto 4bis.

7. Si applica la metodologia di verifica espressa per il controllo numero cinque.

8. Verificabile allo stesso modo del controllo numero 1, anche per le Amministrazioni che erogano servizi critici.

9. **MS Azure:** Utilizzando le soluzioni Managed HSM, Dedicated HSM e Payment HSM Azure supporta il meccanismo di Bring Your Own Key, ovvero concede la possibilità all'amministrazione di generare autonomamente qualsiasi chiave, anche la Root Key, attraverso un suo HSM ospitato direttamente nella sua infrastruttura. Al contrario, se si vuole usufruire di un'infrastruttura messa a disposizione solo dell'Amministrazione che migra su Cloud si deve sempre scegliere una delle soluzioni indicate. Tutti i riferimenti sono riportati nelle seguenti pagine: scelta dell'HSM[69], Managed HSM[92], Dedicated HSM[93], Payment HSM[94]

   Google Cloud: Nel Cloud Google sono garantite delle soluzioni di tipo Bring Your Own Key, ovvero Cloud EKM, che consente all'amministrazione di generare le proprie chiavi crittografiche presso un key manager supportato da google. Tali key manager supportati da Google sono Fortanix, Futurex, Thales e Virtru, e lo stesso servizio Cloud EKM è disponibile per tutti i servizi Google riportati in questa pagina[95]. Quindi è possibile per l'amministrazione generare le chiavi presso un HSM di una terza parte compatibile. Altrimenti utilizzando la soluzione "Hosted Private HSM", descritta al seguente link[96], è permesso all'Amministrazione di ospitare un proprio HSM con determinati requisiti all'interno delle strutture e dei datacenter di Google. In questa maniera si riesce a gestire, con un proprio HSM dedicato, a cui Google non ha accesso logico, la generazione delle chiavi. Infine, è anche data la possibilità all'amministrazione di avere una propria infrastruttura HSM, importando poi in maniera sicura le chiavi all'interno di Cloud Key Management Service come riportato in questa guida[97].

   AWS: Sono supportate anche in questo cloud provider soluzioni di tipo Bring Your Own Key che permettono all'amministrazione di generare le chiavi non in un HSM di Amazon ma anche in un loro HSM. Infatti viene data la possibilità all'amministrazione di utilizzare un custom keystore che può essere di due tipi. Il primo tipo è il cloud HSM keystore, ovvero un HSM ospitato nei cluster di AWS e dedicato al cliente che lo utilizza, come riportato nella documentazione del prodotto, visibile qui[98]. Altrimenti è possibile anche implementare una soluzione BYOK, che fa riferimento

a un HSM esterno come riportato nella documentazione di external key store[99], ovvero una soluzione che permette di gestire le chiavi all'interno di un HSM presso l'infrastruttura dell'Amministrazione o l'infrastruttura di un soggetto terzo.

10. **MS Azure:** Come descritto in questa pagina[100] la procedura di importazioni delle chiavi è sicura e viene messa a disposizione ed è ben documentata nel link indicato in precedenza.

    Google Cloud: Anche Google mette a disposizione una funzionalità di importazione sicura delle chiavi all'interno dello spazio di Cloud Key Management Service. Gli algoritmi crittografici con cui importare la chiave all'interno del Cloud sono descritte in questa pagina[101]. Invece il modo in cui formattare la chiave per l'importazione sicura è descritto qui[102], mentre la procedura di importazione manuale della chiave è descritta nelle pagine seguenti: Configurazione OpenSSL[103], Wrapping chiave[104]. Infine, la guida per l'importazione della chiave cifrata è consultabile a questo link[97].

    AWS: Anche questo Provider mette a disposizione una soluzione di importazione sicura delle chiavi all'interno di un custom key store. Infatti, seguendo i 4 step visualizzabili nella seguente guida[105], è possibile importare il materiale crittografico per la chiave, cifrandolo con una chiave pubblica scaricabile dal sito di AWS, per poi poterlo trasferire, insieme a un import token, che serve a rafforzare la sicurezza del processo di importazione.

11. Si applica la metodologia di verifica espressa per il controllo numero cinque.

12. In questo caso come riportato al punto uno sono state riportate le pagine della documentazione ufficiale dei vari provider. Se si vuole richiedere un documento di maggior dettaglio bisogna interfacciarsi direttamente con il Cloud Provider.

12bis. **MS Azure:** Le entità extra-UE che possono accedere ai dati, secondo il white paper sulla sicurezza di Microsoft, possono essere solo il Cloud Provider stesso, i governi quando fanno una richiesta di accesso secondo delle leggi e le ditte a cui Microsoft subappalta alcuni servizi. Per quanto riguarda i subappaltatori come riportato in questo documento[106], anche se questi hanno un accesso potenziale ai dati, comunque o non li accedono per svolgere le loro mansioni, oppure li accedono anonimizzati. Nel caso remoto in cui li accedano comunque sono tenuti per legge a non divulgarli e allo stesso tempo li accedono solo nel momento in cui l'accesso si rende necessario per erogare i servizi che sono richiesti dai clienti. Per quanto riguarda i governi, a seconda di quanto riportato nei punti precedenti viene dichiarato che:

    - *Microsoft non fornirà dati dei clienti ospitati nei data center Azure a un governo straniero o a un organo di legge, a meno che l'Amministrazione non sia d'accordo, o Microsoft non sia costretta a causa di leggi. Quindi, Microsoft non concede a nessuna terza parte, inclusi governi o organi di legge, l'accesso diretto e senza rrestrizioni ai dati dei clienti.*

- *Microsoft prova sempre a riportare e rimandare tutte le richieste di dati provenienti da terze parti al cliente.*
- *Se Microsoft è obbligata dalla legge a fornire dati appartenenti all'Amministrazione, essa riceverà una notifica immediata e una copia della richiesta formale di accesso ai dati. Tale cosa non accade solo nel caso estremo in cui a Microsoft viene esplicitamente proibito dalla legge, per ragioni di sicurezza estreme, di notificare la richiesta al cliente. Microsoft si impegna anche a fornire solo i dati richiesti dall'ordine giudiziario.*

Quindi, sulla base di quanto riportato nei documenti indicati sono segnalate le richieste di accesso ai dati da parte di entità extra-UE e tutte queste richieste sono sempre reindirizzate al cliente, ovvero l'Amministrazione.

Google Cloud: Anche Google quando riceve una richiesta di accesso ai dati dell'Amministrazione, da parte di un governo straniero, implementa una policy che soddisfa il controllo. Infatti, nel momento in cui un governo o entità extra-UE richiede l'accesso ai dati salvati nel cloud di Google, l'azienda segue questi quattro passi:

- Google richiede al governo o entità che ha fatto la richiesta di rivolgersi direttamente all'amministrazione.
- I legali di Google valutano se la richiesta è a norma di legge, proporzionata e soddisfa le policy interne. Inoltre tutte le richieste di accesso ai dati dei clienti sono prima revisionate dai legali di Google, e solo se sono approvate vengono lasciate proseguire.
- Google, a meno che non sia impossibilitata, perché potrebbero essere lesi in maniera seria individui, si impegna a notificare al cliente la richiesta di accesso che ha ricevuto.
- Google terrà in considerazione eventuali ricorsi dei propri clienti nelle sedi opportune. Nel caso in cui il ricorso viene notificato a Google correttamente Google non fornirà i dati.

Il processo in maniera estesa è descritto sul white paper per le richieste provenienti dai governi scaricabile al seguente link[107]. Comunque la policy espressa da Google rispetta i requisiti richiesti dal controllo omonimo

AWS: Il comportamento di AWS di fronte alle richieste da parte di autorità extra-UE e governi extra-UE è descritto alla seguente pagina. In essa viene affermato che Amazon segnala al cliente quando ci sono richieste di accesso ai loro dati da parte di autorità di qualsiasi parte del globo e che allo stesso tempo a meno che non sia obbligato per legge non concede l'accesso ai dati.

13. **MS Azure:** Nella documentazione di Azure non esiste un documento aggiornato che elenchi tutti i data center di Azure. Però Microsoft mette a disposizione lo strumento localizzato in questa pagina web[108], il quale permette di controllare da quali data center può essere erogato uno dei loro prodotti o Servizio cloud.

Google Cloud: Nella documentazione di Google Cloud non esiste un documento che elenca tutti i Data Center. La lista di tutti i Data Center offerti da Google è disponibile al seguente link[109]. Per maggiori informazioni anche sui servizi disponibili nei vari data center si consideri la seguente pagina[109].

AWS: AWS dà un elenco di tutte le regioni e data center disponibili nel mondo alla seguente pagina[110]. Infatti, cliccando su List View sono mostrate tutte le regioni e la locazione dei vari edge

2.22 PR.DS-2

I dati sono protetti durante la trasmissione

Risultati dell'ispezione

MS Azure: Nella seguente pagina[111] sono descritti i meccanismi di cifratura dei dati in transito indipendentemente dal fatto che siano legati a servizi, storage e applicazioni. Viene segnalato che sono usati vari standard di sicurezza nel trasferimento dei dati, come gli IEEE 802.1AE MAC Security Standards, TLS, HTTPS per le chiamate alle API di AZURE, la cifratura SMB per le reti virtuali di Azure, e altri meccanismi come SSH per l'interazione con le macchine virtuali. Per quanto riguarda la migrazione di App, servizi e server sul cloud, lo strumento incorporato di Azure, Azure Migrate, offre la possibilità di utilizzare vari strumenti di sicurezza durante la migrazione. Come riportato nella security baseline[112] del prodotto sono presenti dei meccanismi di cifratura dei dati in transito e anche dei meccanismi di encryption at rest.

Google Cloud: Anche qui sono implementati di default, e anche in maniera configurabile dall'utente dei meccanismi di cifratura dei dati in transito. Infatti, nella documentazione di Google, precisamente in questa pagina[63] sono descritti tutti i protocolli, di dominio pubblico e mantenuti da Google, che sono utilizzati per la cifratura dei dati in transito verso il cloud Google. Per quanto riguarda la migrazione delle applicazioni e dei server su Google Cloud nella documentazione del tool di migrazione non sono citati i meccanismi di sicurezza utilizzati per il trasferimento. Probabilmente sono gli stessi descritti nella pagina precedente che spiega come avviene la cifratura dei dati in transito.

AWS: Per i dati in transito, la descrizione di come avviene la cifratura si trova nel white paper[57] sulla sicurezza nella sezione Encrypt Data in Transit. In questa sezione viene menzionato che sono utilizzati TLS e HTTPS, per i dati in transito che sono veicolati utilizzando le API di AWS. Inoltre, si aggiunge che è possibile utilizzare l'Amazon Virtual Private Cloud (VPC) come un'estensione dei propri data center, connettendo questi due endpoint in maniera sicura attraverso una VPN, implementabile in più modi. Infine, come riportato nella documentazione, in questa pagina[113], la migrazione delle applicazioni su Cloud AWS, tramite il servizio AWS Application Migration Service, segue determinati standard di sicurezza come la cifratura dei dati in transito attraverso TLS. Inoltre, la documentazione riportata prescrive alcuni dettami di

sicurezza che vanno seguiti durante il processo di migrazione verso il Cloud AWS delle applicazioni. Lo stesso vale anche per altri tipi di migrazione.

2.23 PR.DS-3

Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale

Metodo di verifica e ispezione

1. **MS Azure:** Microsoft definisce le politiche per il trasferimento dei device e più in generale degli asset, oltre che delle politiche per la distruzione, con poi i relativi processi, metodologie e tecnologie implementate per soddisfare le politiche. In questa pagina[114] sono descritti politiche, processi e metodologie per il trasferimento degli asset. Invece, in questo documento[115], sono riportati tutti i processi, con tutti i riferimenti necessari, finalizzati alla distruzione di dispositivi che avevano prima incorporati dei dati. Per quanto riguarda le politiche quest'ultimo documento dice che sono definite ma non dove. Perciò se si vuole avere una relazione che descriva le policy e gli obiettivi di policy è necessario contattare il Cloud Provider. Però, al livello tecnologico per la distruzione, inoltre, si afferma che sono seguite le prescrizioni del NIST 800-88[116], come riportato qui[117].

   Google Cloud: Dalla documentazione di Google Cloud non sembra essere esplicitata la policy di trasferimento e distruzione dei dispositivi di memorizzazione. Invece, i processi, le metodologie e le tecnologie per l'eliminazione e il trasferimento, degli asset e dei supporti di memorizzazione, sono esplicitati qui[118]. Nel documento citato si afferma che Google Cloud monitora la posizione e lo stato dei supporti, e sono descritte le procedure di distruzione dei supporti, affermando che queste sono in accordo con lo standard NIST 800-88[116]. Per ulteriori informazioni sulle policy adottate è necessario richiedere una relazione che le descrive in maniera dettagliata al Cloud Provider direttamente.

   AWS: Anche AWS non sembra riportare le policy, i processi e i meccanismi con cui si gestiscono i trasferimenti fisici e le rimozioni dei device. Per questo è necessario richiedere ad AWS una relazione di dettaglio che descriva politiche, processi e meccanismi atti al tracciamento degli asset. Al contrario, per quanto riguarda la distruzione dei supporti di memorizzazione, come riportato in questa pagina[119], si afferma che sono utilizzate tecniche convalidate e approvate dallo standard NIST 800-88[116] per lo smaltimento degli hard drive, che contenevano i dati dei clienti.

2. In generale, tutti e tre i Cloud Service Provider sotto esame offrono una documentazione molto approfondita di ogni servizio SaaS offerto. Quindi, solo per dati e servizi di livello critico, per verificare il controllo, è necessario richiedere all'Amministrazione l'elenco di tutti i servizi SaaS acquistati dal Cloud Service Provider, per poi studiare la documentazione del servizio e verificare che

siano abilitate capcità di geo-localizzazione remota per tutti i dispositivi mobili gestiti. Nel caso in cui la documentazione non sia pubblicata e disponibili online, richiedere al Cloud Service Provider la documentazione dei prodotti SaaS acquistati dall'Amministrazione e procedere come indicato nel periodo precedente.

3. Per ogni servizio SaaS acquistato dall'Amministrazione, nel caso in cui sia disponibile una documentazione pubblica, studiare la documentazione del servizio e verificare che siano definite e implementate tecniche di cancellazione dei dati dell'Amministrazione da remoto. Nel caso in cui non sia disponibile una documentazione pubblica del servizio SaaS, richiedere al fornitore di servizi Cloud la documentazione e procedere come indicato in precedenza. La metodologia si applica solo per dati e servizi di livello almeno critico.

4. Solo per dati e servizi di livello strategico, richiedere formalmente il documento di dettaglio citato nel controllo omonimo al CSP.

2.24 PR.DS-5

Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)

Metodo di verifica e ispezione

1. **MS Azure:** Le politiche, i processi, le metodologie e le tecnologie per il rispetto delle politiche stesse, per quanto riguarda l'accesso ai dati sono descritte nel seguente documento[120]. Qui viene fornita una panoramica di come Microsoft gestisce i dati sul Cloud, specificando anche qualche metodologia di offuscamento dei dati per limitarne l'accesso, come la pseudonimizzazione dei dati. Allo stesso modo, come dichiarato nel white paper sulla sicurezza[55], si parla di isolamento logico dei tenant per impedire ad altri clienti l'accesso ai propri dati.

   Google Cloud: Al livello di accesso ai dati, Google Cloud esprime le policy, le metodologie e i processi di controllo degli accessi ai dati, a vari livelli nel suo white paper[42] sulla sicurezza, segnalando come agisce per impedire, ad entità non autorizzate, l'accesso ai dati.

   AWS: Alcune delle politiche di accesso ai dati relativamente ai servizi AWS sono descritti nell'addendum[121] sulla protezione dei dati. In tale documento sono descritte alcune, non tutte, le politiche sull'accesso ai dati da parte del personale AWS e dei sub-appaltatori, oltre che dei governi esteri, come anche descritto in questo documento[122].

   Per tutti e tre i Cloud Provider, nel caso in cui siano necessarie informazioni aggiuntive sulle policy di accesso ai dati e sui processi e meccanismi, che permettono l'enforcement delle politiche stesse, è necessario richiedere al CSP una relazione di dettaglio contenente tali informazioni.

2. **MS Azure:** Per quanto riguarda le policy di data loss di Microsoft, non è pubblicato un documento che le definisce, nella documentazione online

accessibile al pubblico. Allo stesso tempo però viene concessa l'opportunità a ogni cliente che migra su Cloud di poter definire una propria Data Loss Policy nello strumento Microsoft Purview. Infatti, consultando la guida[123] dello strumento, si trovano riportati vari template di Data Loss Prevention policy, classificati per categoria e divisi. Quindi, Microsoft definisce delle policy di Data Loss Prevention che l'utente può adottare in Microsoft Purview per impedire che alcuni dati sensibili appartenenti all'organizzazione siano soggetti a oversharing. Allo stesso tempo, però, se è necessario conoscere quali siano le policy adottate da chi gestisce il servizio cloud riguardo la data loss, è necessario richiedere una relazione che le descriva al team di sicurezza di Azure.

Google Cloud: Non esistono documenti pubblici in cui sono esplicitate le policy interne a Google Cloud per la Data Loss Prevention. Però, Google Cloud mette a disposizione dei suoi clienti uno strumento chiamato Sensitive Data Protection, che permette al cliente di, implementare delle proprie politiche per prevenire la data loss, oppure utilizzare delle politiche predefinite per impedire l'esfiltrazione o perdita di dati sensibili. La documentazione del prodotto, con i riferimenti alle policy predefinite è riportata qui[124].

AWS: Non sono esplicitate, in nessun documento pubblico, le policy per la Data Loss Prevention interne ad AWS. Nonostante ciò, Amazon ha lanciato, di recente, Amazon Macie, cioè uno strumento che aiuta l'organizzazione a proteggere i propri dati sensibili, individuandoli e pseudonimizzandoli in maniera da prevenire una perdita dei dati stessi. Chiaramente qui sono configurabili delle policy ed esistono policy predefinite per prevenire l'esfiltrazione di dati.

3. Richiedere al Cloud Provider il documento contenente tutti gli elementi elencati al controllo numero uno della sottocategoria per valutarne l'esistenza. Infatti, tutti i documenti citati nella metodologia di verifica del controllo uno contengono una descrizione sintetica delle policy, e non di dettaglio. Per questo motivo è necessaria un'interlocuzione diretta con il Cloud Provider, in cui si richiede formalmente il documento.

2.25 PR.DS-6

Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni

Metodo di verifica

1. Richiedere al CSP una relazione di dettaglio che definisca i seguenti aspetti:
   a. l'elenco dei meccanismi di controllo dell'integrità per verificare l'autenticità di osftware, firmware e informazioni.
   b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa.

c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

2. Solo per Amministrazioni che erogano servizi di carattere strategico richiedere al CSP una prova che tutti gli elementi descritti nella relazione al controllo numero uno siano anche contenuti all'interno di un documento ufficiale di dettaglio del Cloud Provider. Se necessario per indagini approfondite richiedere il documento al Cloud Provider.

2.26 PR.DS-7

Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione

Metodo di verifica

1. Richiedere al CSP una relazione di dettaglio che definisca i seguenti aspetti:
   a. l'architettura di massima per cui gli ambienti sono separati e, negli eventuali punti di contatto, come la separazione è realizzata.
   b. le politiche di sicurezza adottate per garantire la separazione dell'ambiente di sviluppo e test da quello di produzione.
   c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza

2. Solo per Amministrazioni che erogano servizi di carattere strategico richiedere al CSP una prova che tutti gli elementi descritti nella relazione al controllo numero uno siano riportati all'interno di un documento di dettaglio del Cloud Provider. Se necessario per indagini approfondite richiedere il documento al Cloud Provider.

2.27 PR.IP-1

Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)

Metodo di verifica

1. Richiedere al Cloud Service Provider una relazione in cui siano descritte le politiche e procedure che supportano la pianificazione realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni. Richiedere al CSP anche un documento una cronistoria o dei verbali di riunioni che possano permettere di certificare che queste politiche e procedure siano riviste e aggiornate su base annuale.

2. Solo per Amministrazioni che erogano servizi di livello almeno critico, richiedere al Cloud Provider, al fine di ispezionarlo, il documento aggiornato di dettaglio che contenga:

a. le politiche di sicurezza adottate per lo sviluppo di configurazioni di sistemi IT e il dispiegamento delle sole configurazioni adottate

b. l'elenco delle configurazioni dei sistemi IT e impiegate e il riferimento alle relative pratiche di riferimento

c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

3. Tutti e tre i Cloud service provider hanno una documentazione esaustiva dei loro servizi e applicazioni in cui sono descritti ed esposti anche tutti i requisiti di sicurezza che vi si applicano. Comunque, per avere un quadro di maggior dettaglio, richiedere, magari per modello di servizio, una relazione tecnica in cui sono definiti e documentati tutti i requisiti di sicurezza delle diverse applicazioni e servizi Cloud. Questa metodologia si applica solo per dati e servizi critici delle Amministrazioni.

4. Solo per dati e servizi critici delle Amministrazioni, richiedere al fornitore di servizi Cloud una relazione tecnica in cui sono descritte le metriche tecniche e operative. Verificare , successivamente che le metriche tecniche e operative siano in linea con i requisiti di sicurezza e gli obblighi di conformità.

5. Solo per Amministrazioni che erogano servizi di livello almeno critico, richiedere al CSP una relazione che documenti il processo di mitigazione e ripristino per la sicurezza delle applicazioni, al fine di valutare se viene anche implementato, ove possibile, un processo di mitigazione automatizzato delle vulnerabilità.

6. Solo per Amministrazioni che erogano servizi di livello critico, richiedere al CSP una relazione che descriva il processo di convalida che permette di stabilire se un certo dispositivo è in grado di ospitare un determinato sistema operativo o applicazione

7. Solo per Amministrazioni che trattano dati o erogano servizi di livello almeno critico richiedere al fornitori di servizi Cloud una relazione tecnica dettagliata che descriva il sistema di gestione delle variazioni, in termini di sistema operativo, patching e/o applicazioni.

2.28 PR.IP-2

Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle)

Risultati dell'ispezione

MS Azure: Vengono definite in questa pagina[125] alcune delle pratiche tipiche dell'SDLC seguito in Microsoft. Chiaramente, le pratiche indicate non sono esaustive e ogni team all'interno dell'azienda potrebbe prevedere fasi aggiuntive nell'SDLC, che non sono documentate. Allo stesso modo, alcune fasi dell'SDLC di Microsoft sono documentate in questa pagina[126]. Chiaramente anche se le fasi dell'SDLC riportate nel documento precedente, non sono esattamente le stesse riportate nelle linee guida OWASP, comunque è possibile

ricondurre il processo seguito in Microsoft al processo OWASP, testimoniando l'aderenza alle linee guida. Per quanto riguarda i report sui test OWASP condotti, è necessario richiederli formalmente al CSP, perché attualmente non sono pubblicati nelle documentazioni ufficiali.

Google Cloud: Google, per lo sviluppo sicuro del servizio Cloud e delle sue componenti, definisce L'SLSA framework, cioè un framework pensato per lo sviluppo sicuro del software. Tale framework non è direttamente riferibile ad OWASP, perciò è necessario un'analisi comparata dei controlli OWASP e dell'SLSA per capire se quest'ultimo aderisce alle linee guida OWASP. Inoltre, i report sui test di aderenza ai controlli OWASP sono da richiedere al CSP, perchè non pubblicati online.

AWS: AWS non pubblica dettagli sul processo di SDLC, ma pubblica una guida che spiega come è possibile sfruttare l'SDLC nello sviluppo di codice su AWS per mettere al sicuro le proprie applicazioni. Per questo motivo si ritiene necessaria un'interlocuzione con il Cloud Provider al fine di, richiedere una relazione che permetta di comprendere a fondo il ciclo di SDLC messo in pratica, e il relativo report sui test di aderenza ai controlli OWASP

2.29 PR.IP-3

Sono attivi processi di controllo della modifica delle configurazioni

Metodo di verifica

1. Richiedere al CSP un documento ufficiale che certifichi la definizione per iscritto di:
   a. le politiche di sicurezza adottate per l'aggiornamento delle configurazioni di sistemi IT e di controllo e per il controllo della modifica delle configurazioni in uso rispetto a quelle previste.
   b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.
2. Richiedere al CSP una relazione che documenti la procedura di gestione delle eccezioni ed emergenze nei processi di modifica e configurazione. Successivamente richiedere l'accesso a un ambiente attraverso i cui i dipendenti del Cloud Provider possono modificare le configurazioni dei sistemi o delle applicazioni utilizzate nei data center, e verificare la corretta implementazione della procedura così come è descritta.
3. Richiedere al Cloud Provider i documenti ufficiali che descrivono i piani di ripristino degli stati precedenti a seguito di errori o problemi di sicurezza. Successivamente accedere ai sistemi del Cloud Provider e verificare che questi piani siano stati implementati correttamente così come descritti.
4. Solo per Amministrazioni che erogano servizi di livello strategico, richiedere al soggetto il documento aggiornato e di dettaglio che contiene e descrive i processi e le politiche citati nel controllo numero uno.

2.30 PR.IP-4

I backup delle informazioni sono eseguiti, amministrati e verificati

Metodo di verifica e ispezione

1. Richiedere al CSP una relazione in cui sono definite le politiche di sicurezza per il backup delle informazioni e i processi, le metodologie e le tecnologie impiegate per il rispetto delle politiche stesse.

2. **MS Azure:** Utilizzando il Cloud Microsoft quando si parla di servizi IaaS, SaaS e PaaS teoricamente è responsabilità del cliente la gestione dei backup. Microsoft non gestisce per l'Amministrazione i backup, ma dà la possibilità all'Amministrazione stessa di gestire i backup dei propri dati autonomamente. Quindi, all'Amministrazione è data la possibilità di scegliere dove replicare i dati e le soluzioni di replicazione che possono essere adottate. L'Amministrazione che migra su Cloud deve utilizzare e configurare correttamente il servizio Azure Backup, impostandolo in maniera da tale da effettuare i backup periodicamente, secondo un periodo di tempo che l'Amministrazione stessa decide e che sia adatto ai dati trattati. Inoltre, affinché sia rispettata l'integrità dei dati sottoposti a backup, è necessario che l'Amministrazione configuri tutti i backup che produce tramite Azure Backup come dei "backup o vault irreversibili", come consigliato in questa pagina[127]. In questa maniera, i backup che si ottengono sono integri, perché non è possibile cancellare o modificare i recovery point del backup stesso. Per quanto riguarda la riservatezza è necessario utilizzare dei meccanismi di encryoption at rest che sono disponibili sul Cloud Microsoft, come spiegato anche in questa pagina[128] della documentazione.

   Google Cloud: Nel cloud di Google è responsabilità del cliente configurare le proprie procedure di backup. Quindi, Google delega la responsabilità di gestire i backup all'Amministrazione stessa, predisponendo un servizio apposito chiamato "Backup and DR", che permette anche di scegliere la modalità di replicazione e la "region" in cui il backup è salvato. Perciò, l'amministrazione che migra su cloud, deve configurare opportunamente il servizio "Backup and DR", occupandosi di configurare dei backup periodici, secondo un periodo di tempo deciso dall'Amministrazione stessa e opportuno per i dati trattati. Per mantenere l'integrità dei backup, Google cloud permette di configurare una policy di backup, in cui, settando il parametro "Enforced Retention", è possibile specificare il numero di giorni in cui il backup deve rimanere immutabile, proteggendone così l'integrità, come riportato in questa pagina[129]. Per garantire, invece, la riservatezza dei backup, bisogna utilizzare i permessi IAM, ovvero configurare per i backup creati i permessi corretti di accesso, in maniera tale che solo chi è autorizzato possa accedere ai dati.

   AWS: Anche AWS delega all'utente la gestione dei backup dei dati e dei servizi, tramite il servizio AWS backup, che permette di gestire autonomamente i backup delle risorse e delle applicazioni in AWS. Tale servizio permette

all'Amministrazione di decidere quale sia la soluzioni di replicazione a lei più congeniale, schedulare il tempo che intercorre tra due backup e scegliere il luogo o la region in cui il backup viene salvato. Quindi, è responsabilità dell'Amministrazione eseguire periodicamente dei backup o schedulare dei backup dei suoi dati salvati nel cloud. Oltretutto, AWS implementa automaticamente dei meccanismi che consentano di mantenere l'integrità dei backup come riportato in questa pagina[130] della documentazione. Invece, la riservatezza dei backup viene mantenuta, dando la possibilità di implementare dei meccanismi di autorizzazione e autenticazione per accedere ai backup, come riportato nella documentazione[131].

3. **MS Azure:** Seguendo quanto dichiarato in questa pagina[132] della documentazione, i backup effettuati con Azure Backup sono protetti di default con crittografia utilizzando chiavi gestite dalla piattaforma. Però, Azure concede anche la possibilità di proteggere i backup attraverso algoritmi crittografici che si servono chiavi gestite dall'Amministrazione. Inoltre, come dichiarato nel documento riportato, tutti i dati che fluiscono dallo storage di Azure e il vault che contiene i backup sono protetti mediante protocollo HTTPS. In conclusione, le opzioni di backup fornite da Azure backup, descritte nella documentazione[133], consentono di archiviare i backup in siti remoti e la connessione con questi siti avviene mediante HTTPS.

   Google Cloud: Come dichiarato in questa pagina [62] della documentazione di Google Cloud, tutti i dati, compresi quelli di backup, sono cifrati utilizzando meccanismi di encryption at rest forti. Le procedure crittografiche descritte nella documentazione si applicano per tutte le copie di backup comprese quelle archiviate in siti remoti. Allo stesso modo, considerando la pagina[63] della documentazione che illustra i meccanismi di cifratura dei dati in transito, si afferma che tutti i dati in transito sono protetti un meccanismo di crittografia forte come TLS, indipendentemente dal punto di partenza dei dati, dal punto di arrivo e dal servizio coinvolto.

   AWS: Vengono implementate delle procedure di cifratura per i backup descritte nella documentazione[134]. La cifratura usa come algorirtmo AES-256 e, a seconda del servizio o dati che sono cifrati, possono essere usate o solo chiavi gestite dalla piattaforma AWS oppure sia chiavi gestite dalla piattaforma sia chiavi gestite dall'amministrazione che migra su cloud. Inoltre, ai dati in transito si applicano i meccanismi di cifratura descritti negli white papers sulla sicurezza AWS, già citati nel controllo numero uno della sottocategoria PR.DS-1. Infatti, tutte le chiamate alle API di AWS Backup sono protette utilizzando TLS e HTTPS, mentre i dati in transito tra un sito e l'altro all'interno della rete AWS sono protetti utilizzando sempre meccanismi crittografici descritti negli white papers.

4. Dato che il backup è gestito direttamente dall'Amministrazione, essa si deve occupare di gestire i test di restore. Quindi, è necessario verificare che l'Amministrazione stessa abbia eseguito dei test di restore periodici su cloud, utilizzando le funzionalità dei vari CSP.

5. Richiedere al CSP un documento che indica quali sono le politiche di sicurezza adottate per il backup delle informazioni e i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.

6. Verificare che esista un documento aggiornato contenente i processi che sono descritti al controllo numero uno.

2.31 PR.IP-9

Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro

Metodo di verifica

1. Richiedere al CSP una relazione in cui viene descritto come viene stimato l'impatto derivante da delle interruzioni di business.

2. Richiedere al CSP il documento aggiornato di dettaglio che contiene i piani di continuità operativa e risposta agli incidenti e comprende le cose indicate nel controllo omonimo.

3. Richiedere al Cloud Provider il documento aggiornato contenente l'elenco delle attività di istruzione e formazione del personale e delle esercitazioni svolte.

4. Richiedere al Cloud Provider una relazione o una prova ufficiale che testimoni il collaudo dei piani di business continuity. Richiedere, inoltre, che sia tracciata la comunicazione dei piani alle parti interessate fornendo un adeguato documento di riscontro.

5. Verificare che l'Amministrazione abbia potuto accedere la documentazione descritta al controllo numero due contattando la stessa. Verificare, successivamente, che la documentazione, citata al controllo numero due, abbia una cronistoria e un versioning che testimoniano la sua revisione periodica.

6. Solo nel caso in cui l'Amministrazione eroghi servizi critici, richiedere al CSP il documento che descriva i livelli di servizio attesi del servizio cloud.

7. Solo nel caso in cui l'Amministrazione eroghi servizi critici, verificare l'esistenza di un documento del CSP contenente i piani di risposta e recupero dagli incidenti e disaster recovery e che comprende tutti gli elementi del controllo omonimo.

8. Richiedere al Cloud Provider il documento aggiornato contenente l'elenco delle attività di istruzione e formazione e delle esercitazioni svolte. Tale metodologia si applica solo se il Cloud Provider serve Amministrazioni che erogano servizi e trattano dati di livello almeno critico.

9. Richiedere al Cloud provider un report del collaudo delle strategie di disaster recovery, e il documento di gestione delle comunicazioni che testimoni che tutte le parti interessate siano state informate della strategia. Tale metodologia si

applica solo se il Cloud Provider serve Amministrazioni che erogano servizi e trattano dati di livello almeno critico.

10. Richiedere al fornitore di servizi Cloud una lista di tutti i dispositivi, fisici e virtuali, critici per il funzionamento del servizio Cloud o dei servizi Cloud acquistati dall'Amministrazione, con allegato per ognuna dei dispositivi una misura che ne esprime il livello di criticità per il funzionamento dei servizi. Successivamente richiedere al Cloud Service Provider un documento in cui per ogni dispositivo o applicazione sono elencate le sue copie e il luogo in cui sono collocate o eseguite. Infine, valutare, in merito alla criticità del dispositivo, se i dispositivi o appplicazioni critiche per il funzionamento del servizio Cloud sono ridondate correttamente, utilizzando dei meccanismi come il Multi-Region Deployement, il Multi-Availability Zone Deployement, il Failover Automatico e così via. Per un singolo dispositivo possono essere adottate anche più best practice a seconda del livello di criticità che essi hanno. Tale metodologia si applica solo se il Cloud Provider serve Amministrazioni che erogano servizi e trattano dati di livello almeno critico.

2.32 PR.IP-12

Viene sviluppato e implementato un piano di gestione delle vulnerabilità

Metodo di verifica

1. Richiedere al CSP il documento aggiornato di dettaglio che contiene le politiche di sicurezza che si usano per gestire le vulnerabilità e i processi, le metodologie e le tecnologie che permettono il rispetto delle politiche di sicurezza.

2. Richiedere al CSP una relazione che definisca le procedure e le misure tecniche per l'aggiornamento degli strumenti di rilevamento e delle threat signatures. Per verificare l'implementazione di queste procedure è necessario accedere ai firewall o eventuali Intrusion Detection System utilizzati dal CSP, per verificare che le procedure relazionate siano messe in pratica e concorrano all'aggiornamento dei firewall e degli IDS. Infine, è necessario controllare i log degli strumenti di rilevamento per capire se l'aggiornamento delle firme è avvenuto di frequente o su base settimanale.

3. Solo per Amministrazioni che erogano servizi di livello critico, richiedere al CSP una relazione che definisca le misure tecniche per l'identificazione degli aggiornamenti per le applicazioni che usano librerie di terze parti. Per verificarne l'implementazione è necessario accedere all'infrastruttura virtuale del Cloud Provider e verificare che tutte le macchine in un determinato data center con i software che usano librerie di terze parti implementino le misure contenute nella relazione. Tale controllo andrebbe eseguito su tutti i data center.

4. Richiedere al CSP una cronistoria del documento al punto uno, per controllare che sia stato aggiornato almeno una volta ogni sei mesi.

2.33 PR.MA-1

La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati

Metodo di verifica

1. Richiedere al CSP una relazione in cui siano descritte le politiche per la registrazione della manutenzione e riparazione dei sistemi, e tutte le procedure, metodologie e tecnologie per il rispetto delle politiche stesse.

2. Solo per Amministrazioni che erogano servizi di livello critico verificare che il CSP documenti le politiche e i processi al punto uno in un documento ufficiale di dettaglio.

3. Solo per Amministrazioni che trattano dati o erogno servizi di livello almeno critico, durante l'analisi della relazione menzionata nella metodologia al punto uno, controllare che essa includa anche la verifica degli aspetti di sicurezza.

4. Richiedere al Cloud Provider una relazione in cui sono elencate le fonti approvate da cui vengono scaricati gli aggiornamenti per le macchine residenti nei datacenter che il CSP utilizza per erogare il servizio. Successivamente richiedere al CSP anche una prova concreta che tutte le macchine nei data center abbiano installato gli aggiornamenti solo da quelle fonti. Alternativamente richiedere l'accesso al software o sistema che utilizza il CSP per gestire in maniera coordinata i log che provengono dallo loro infrastruttura di rete, filtrare i messaggi di log che riguardano gli aggiornamenti e verificare con uno strumento automatico che gli aggiornamenti siano stati scaricati solo da fonti contenute nella lista fornita dal CSP.

5. Tale metodologia si applica solo per Amministrazioni che erogano servizi critici. Per prima cosa, è necessario accedere ai sistemi del CSP e verificare che il sistema o applicazione che gestisce in maniera coordinata i log delle attività di aggiornamento e manutenzione provenienti dalle macchine installate nei data center del CSP, abbia la parte di elaborazione e i relativi client non ospitati nelle macchine oggetto della sorveglianza. Successivamente, utilizzando uno strumento di sniffing del traffico internet come tcpdump o wireshark è necessario accertarsi che esistano pacchetti, contenenti i log prodotti da queste macchine, che viaggino sulla rete protetta del CSP e siano inviati a delle macchine diverse da quelle oggetto di manutenzione. Infine, una volta individuate le macchine adibite allo storage dei log e ad ospitare il sistema di gestione dei log, è necessario verificare che l'accesso a queste macchine sia ristretto solo agli utenti che ne hanno il diritto. Quindi, è necessario accedere al sistema di PAM del CSP e verificare che le utenze che hanno i permessi per svolgere la manutenzione non abbiano anche i permessi per accedere alle macchine in cui i log della manutenzione e degli aggiornamenti sono salvati.

6. Solo per Amministrazioni che erogano servizi di livello critico richiedere al Cloud Provider un documento aggiornato che descrive e documenta gli strumenti tecnici che permettono di soddisfare i controlli numero tre, quattro e cinque.

7. Solo per Amministrazioni che erogano servizi di livello strategico richiedere al CSP un registro in cui si tiene conto delle attività manutenzione e riparazioni eseguite.

8. Richiedere al Cloud Service Provider un registro, cartaceo o elettronico, in cui siano elencati tutti gli aggiornamenti dei software ritenuti critici, e, successivamente richiedere anche una lista di tutte le patch dei software sperimentate in ambiente di test. Dal confronto tra i due registri stabilire se tutti gli aggiornamenti dei software critici siano presenti anche nel registro delle patch sperimentate in ambiente di test. Nel caso in cui un aggiornamento di un software critico non sia presente all'interno del registro, richiedere al fornitore di servizi Cloud la motivazione del deploy istantaneo della patch e stabilire se il deploy è stato effettuato per soddisfare esigenze di tempestività relative alla sicurezza.

9. Solo per Amministrazioni che erogano servizi di livello strategico, richiedere al Cloud Service Provider di mantenere il codice oggetto utilizzato per ogni aggiornamento, citato al controllo numero tre, per almeno 24 mesi dall'aggiornamento stesso. Al fine di verificare che tale codice sia effettivamente salvato, richiedere al Cloud Service Provider l'accesso alle macchine o storage individuati per mantenere il codice oggetto, al fine di verificare, con controlli periodici, che sia mantenuto per 24 mesi.

2.34 PR.MA-2

La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati.

Metodo di verifica

1. Richiedere al Cloud Provider una relazione che descriva il processo di manutenzione da remoto delle risorse e dei sistemi. Successivamente ispezionare il documento e verificare che il processo rispetti le misure riportate nella sottocategoria PR.AC-3.

2. Richiedere al fornitore di servizi Cloud un registro di tutti gli accessi eseguiti da remoto da personale di terze parti. Successivamente richiedere dei verbali o dei documenti ufficiali che provino che gli accessi elencati nel registro siano stati approvati dall'organizzazione di cybersecurity. Infine, per ogni accesso, controllare la motivazione per cui questo è stato effettuato e valutare attraverso questa se l'accesso era necessario ed essenziale.

3. Richiedere al Cloud Service Provider una relazione in cui sono descritti tutti i meccanismi di protezione per l'autenticazione, l'identificazione e per il tracciamento degli eventi. Successivamente accedere ai sistemi del Cloud Provider e verificare che siano implementati i meccanismi così come descritti sulla relazione, verificando che questi impediscano a chi sta utilizzando il servizio Cloud o a un ente non autorizzato del soggetto stesso di disabilitare o compromettere i meccanismi citati in precedenza.

4. É necessario che il Cloud Provider abbia implementato un sistema di Privileged Access Management o Priviliged Identity Management, che permetta di supervisionare le utenze privilegiate. Infatti, attraverso un sistema come quello, è possibile per il CSP creare delle identità privilegiate ad hoc specializzate per determinate funzionalità amministrative e con i permessi concessi per un dato limite di tempo. In questa maniera, il CSP riesce ad avere pieno controllo di tutto quello che le utenze privilegiate riescono a fare. In sintesi il sistema PIM o PAM utilizzato dal Cloud Provider deve possedere la funzionalità di impostare, ogni volta che si crea un'utenza privilegiata, i permessi dell'utenza e il limite di tempo per cui i permessi sono concessi all'utenza creata.

5. Il controllo in questione viene verificato se sono soddisfatte due condizioni:
   - Viene soddisfatto il controllo numero cinque della sottocategoria PR.MA-1.
   - Accedendo all'infrastruttura virtuale del CSP, si riesce a constatare, utilizzando degli strumenti di sniffing del traffico, come wireshark o tcpdump, che esistono pacchetti contenenti i log relativi ad attività di aggiornamento o manutenzione da remoto, e che siano inviati a macchine differenti da quelle che sono oggetto di manutenzione. Una volta individuate le macchine verificare, accedendo alle stesse che i log siano effettivamente salvati lì. Infine, accedendo al sistema PAM del Cloud Provider, controllare che i privilegi concessi alle utenze che si occupino di fare attività di manutenzione e aggiornamento da remoto non comprendano anche possibilità di accesso alle macchine in cui sono immagazzinati i log.

6. Solo per Amminstrazioni che erogano servizi di livello strategico, richiedere al Cloud Service Provider un documento aggiornato e di dettaglio contenente una descrizione dei processi e degli strumenti tecnici che si utilizzano per soddisfare i controlli numero due, tre, quattro e cinque.

2.35 PR.PT-1

Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi

Metodo di verifica

1. Accedere all'infrastruttura virtuale del Cloud Provider e successivamente individuare la macchina, o le macchine nel caso in cui i log siano gestiti in maniera distribuita, in cui sono conservati i log. Richiedere l'accesso alla macchina individuata al Cloud Provider e accedere al registro dei log. Successivamente, anche a seconda di come sono organizzati e conservati i log, con uno strumento automatico, verificare che ci siano log che risalgono ad aventi accaduti almeno 24 mesi del momento della verifica. Se tali log sono presenti il controllo è superato. Altrimenti, se i log non sono presenti il controllo si ritiene non superato, a meno che la produzione degli stessi non sia cominciata da meno di 24 mesi.

2. Richiedere al CSP una relazione che descriva in maniera dettagliata le policy di sicurezza e gli obiettivi di policy adottati per la gestione dei log esistenti,

e tutti i processi, metodologie e tecnologie impiegate per forzare il rispetto delle policy di sicurezza. Analizzando la relazione è necessario verificare che siano dettagliate in maniera particolarmente accurata le policy di integrità e disponibilità per i log.

3. Solo per Amministrazioni che erogano servizi di livello strategico, richiedere al Cloud Service Provider o una prova di esistenza di un documento aggiornato e di dettaglio che descriva processi e politiche menzionati nel controllo numero due, oppure il documento stesso.

2.36 PR.PT-4

Le reti di comunicazione e controllo sono protette

Metodo di verifica

Tutti le metodologie di verifica riportate per la sottocategoria in esame vanno applicate solo nel caso di Amministrazioni che erogano servizi di livello strategico.

1. Richiedere l'accesso all'infrastruttura di rete, reale o virtuale, del provider, tramite VPN o altri meccanismi, e individuare quali sono i firewall installati e in quali macchine sono stati installati, considerando tutti i firewall hardware e software e a qualsiasi livello della pila ISO/OSI. Successivamente per ognuno dei firewall individuati:
   - Controllare la versione installata e i log dello strumento, se presenti, per determinare se gli aggiornamenti sono stati svolti con continuità e non sono in uso versioni non aggiornate o non sicure.
   - Controllare i log dello strumento al fine di verificare tutte le operazioni di mantenimento operate sul firewall, come riavvii, cambio delle interfacce monitorate, cambio delle regole, etc... al fine di stabilire se il personale del soggetto mantiene costantemente lo strumento.
   - Analizzare le regole configurate sul firewall, anche alla luce della tipologia di firewall, verificando se queste sono ben scritte e permettono di assolvere alle funzioni di sicurezza.

   Infine, svolta l'analisi delle regole di ogni firewall singolarmente, eseguire un'analisi comparata delle regole di firewall lavorano a livelli diversi della pila ISO/OSI o di firewall installati su macchine che comunicano tra loro, in maniera da verificare se i controlli di sicurezza che impediscono una certa azione malevola siano implementati o ad entrambi i livelli o in entrambe le macchine.

2. Richiedere l'accesso alla rete del provider, tramite VPN o altri meccanismi, e individuare quali sono gli Intrusion Prevention System installati e in quali macchine sono stati installati. Successivamente per ognuno degli IPS individuati:
   - Controllare la versione installata e i log dello strumento, se presenti, per determinare se gli aggiornamenti sono stati svolti con continuità e non sono in uso versioni non aggiornate o non sicure.

- Controllare i log dello strumento al fine di verificare tutte le operazioni di mantenimento operate sull'IPS, come riavvii, cambio delle regole, caricamento di un nuovo modello di rilevamento etc.. al fine di stabilire se il personale del soggetto mantiene costantemente lo strumento.
- Analizzare il modello utilizzato dall'IPS, stabilendo se è un modello basato su regole, su anomaly detection oppure su misuse case. Successivamente nel caso di modelli che si avvalgono di algoritmi di machine learning richiedere informazioni su come è avvenuto il loro addestramento. Nel caso di modello basato su regole ispezionare le regole di rilevamento al fine di stabilire se includono tutti i casi e permettano di assolvere alle funzioni di sicurezza dello strumento. Nel caso di modelli ibridi è necessaria un'analisi più complessa.
- Verificata la parte di rilevamento, procedere alla verifica delle eventuali azioni impostate per il blocco di azioni malevole. Verificare che le azioni siano adeguate per prevenire incidenti informatici o compromissione degli asset, ma allo stesso tempo valutare che non siano troppo restrittive, in maniera che non permettano facili attacchi di Denial of Service.

3. Eseguire un'analisi delle policy esposte nelle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS, e stabilire se tutti gli strumenti tecnici menzionati nei controlli uno e due e le regole in essi configurate permettono il rispetto delle suddette.

4. Per prima cosa è necessario recuperare tutti i log degli strumenti tecnici menzionati nei controlli uno e due, e i log relativi alle operazioni di aggiornamento e manutenzione, menzionati nelle categorie PR.MA, filtrando solo quelli relativi agli strumenti. Successivamente analizzare i log e stabilire se gli aggiornamenti e le attività di manutenzione eseguite sugli strumenti tecnici citai nei controlli precedenti, soddisfano le policy espresse nelle categorie PR.AC, PR.DS, PR.IP e PR.MA.

5. Verificare che gli strumenti tecnici menzionati ai controlli numero uno e due siano gli stessi utilizzati dall'organizzazione anche per assolvere al soddisfacimento dei controlli indicati per le sottocategorie della funzione di Detect.

6. Richiedere al CSP il documento aggiornato che descrive i processi e gli strumenti tecnici che sono impiegati per soddisfare i controlli numero uno, due, tre e quattro, in maniera da valutare la sua esistenza.

2.37 PR.PT-5

Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse

Metodo di verifica e ispezione

1. Considerando Microsoft e Google, entrambe dichiarano che nei loro data center sono implementate delle topologie CLOS, ovvero delle topologie di rete parti-

colarmente efficienti che permettono di ottenere un buon grado di resilienza, ridondando connessioni e dispositivi di rete. I riferimenti relativamente a quanto dichiarato dai vari provider nella documentazione sono riportati di seguito: Infrastruttura Azure[135], Rete di Produzione Azure[136], Infrastruttura Jupiter di Google Cloud[137]. Al contrario dalla documentazione di AWS non risulta nessun dettaglio tecnico sulle architetture ridondate di rete e di connettività adottate nei data center e nell'infrastruttura globale di Amazon. In ogni caso, dato che le documentazioni non sono un'evidenza sufficiente per concludere l'adozione di architetture ridondate di rete, di connettività e applicative, è necessario richiedere prima al CSP una relazione che descriva sinteticamente l'architettura di rete che si adotta nei data center, e come avviene la replicazione delle istanze applicative dei servizi cloud forniti all'amministrazione. Nel caso delle architetture di rete potrebbe essere anche necessaria un'ispezione di qualche data center nell'unione europea per constatare l'adozione di tali architetture. Successivamente, poichè agendo nella maniera indicata si è verificata solo la parte infrastrutturale, è necessario controllare la rete di produzione. Quindi, per verificare che, anche per la rete di produzione, siano adottate architetture ridondate di rete, di connettività e applicative è necessario richiedere al Cloud Service Provider una relazione tecnica che descriva la struttura della rete di produzione. Dalla relazione verificare se le architetture di rete e di connettività siano adeguate.

2. Il controllo va revisionato da chi lo ha ideato. Non è stato possibile sviluppare una metodologia.

3. Richiedere al soggetto una relazione in cui siano dettagliate le politiche di sicurezza adotatte in relazione ai controllo numero uno e due, e anche i processi, le metodologie e le tecnologie che concorrono al rispetto delle politiche.

1bis. Solo per Amministrazioni che erogano un servizio di livello almeno critico, oltre a procedere come riportato nella metodologia per il controllo numero uno, richiedere al soggetto di indicare dove sono locati tutti i siti di disaster recovery che sono predisposti dal Cloud Provider stesso.

4. Solo per Amministrazioni che erogano servizi almeno di livello strategico, richiedere al CSP, al fine di verificarne l'esistenza, un documento aggiornato di dettaglio in cui sono riportate le politiche e le procedure descritte al controllo numero due.

2.38 DE.DP-1

Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability

Metodo di verifica e ispezione

1. Verificare, richiedendo al soggetto tale documento, che le nomine indicate nella sottocategoria ID.AM-6 siano pubblicate in un documento o in una pagina web dell'organizzazione accessibile a tutto il personale del Cloud Service Provider.

2. Verificare che il soggetto abbia redatto un documento o un organigramma in cui sono definiti formalmente i ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sul servizio cloud. Successivamente verificare che tale documento o organigramma sia accessibile e noto da tutte le articolazioni competenti del soggetto.

3. Richiedere al Cloud Provider l'accesso al documento di dettaglio aggiornato, che indica i ruoli, i processi e le responsabilità citate al controllo due e le procedure per la diffusione delle nomine, dei ruoli e dei processi citati al controllo numero due, al fine di verificare l'esistenza del documento stesso.

4. Tutti e tre i Cloud Service Provider presi in esame definiscono e implementano un sistema che si occupa di notificare all'Amministrazione eventuali eventi anomali che compromettono le applicazioni in uso dalla stessa. Infatti, ogni Cloud Service Provider possiede un suo sistema di Service Health che permette all'amministrazione di sapere lo stato delle applicazioni e delle risorse cloud da essa create, e, nel caso in cui ci siano, quali sono gli eventi anomali che le hanno coinvolte. Ognuno di questi tre servizi va configurato dall'Amministrazione seguendo le pratiche che sono riportate nelle documentazioni. Di seguito sono riportati i link alle documentazioni dei prodotti descritti: Azure Service Health[138], Google Cloud Personalized Service Health[139], AWS Health[140]. Allo stesso modo, tutti e tre i CSP non descrivono nelle loro documentazioni dei sistemi che permettono di notificare all'Amministrazione di notificare eventi anomali che coinvolgono l'infrastruttura sottostante al servizio Cloud. Quindi, è necessario richiedere ad ogni Cloud Provider una relazione che descriva il sistema che viene utilizzato per notificare ai clienti gli eventi anomali che possono affliggere l'infrastruttura utilizzata dal fornitore di servizi Cloud. Successivamente, bisogna verificare l'implementazione di tale sistema accedendo all'infrastruttura che collega i data center utilizzati dal cloud Provider, per verificare che questo sistema sia in funzione e svolga effettivamente il compito richiesto.

2.39 DE.AE-3

Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple

Metodo di verifica

1. Procedere con le seguenti verifiche:
    a. Per prima cosa censire tutte le potenziali sorgenti di informazioni e i sensori nella rete del Cloud Provider che possono essere utili a raccogliere informazioni rilevanti. Successivamente verificare che almeno per un certo numero di sorgenti o sensori sia implementato un sistema di comunicazione con una macchina adibita alla raccolta di tali informazioni per un'analisi successiva. Infine, constatare se il modello di comunicazione implementato sia di tipo push, cioè è il sensore o la sorgente che invia le informazioni alla macchina, o di tipo pull, ovvero è la macchina che preleva periodicamente le informazioni dai sensori o dalle sorgenti.

   b. Constatare che ci sia del personale adibito, o un processo dedicato, a raccogliere informazioni sulla sicurezza del servizio Cloud rese note dal CSIRT Italia, da fonti interne o esterne al soggetto.
   c. Verificare che sia stato implementato un processo di analisi delle informazioni, citate nei punti a e b, svolto da un team di sicurezza dedicato. Altrimenti, verificare che nella rete del Cloud Provider, tutte le informazioni raccolte siano fatte pervenire a un sistema SIEM, che si occupa di analizzare e correlare le informazioni in maniera automatica per rilevare eventuali minacce o eventi di interesse.

2. Nel caso in cui le attività di correlazione siano svolte da un team di sicurezza dedicato, richiedere al team stesso la documentazione relativa alle attività di correlazione per verificarne il monitoraggio e la registrazione. Altrimenti, se l'attività di correlazione viene svolta in maniera automatica attraverso un sistema SIEM, controllare che il Cloud Provider abbia definito un processo di registrazione di tutti gli alert emessi dal SIEM e che ci sia un team apposito che si occupa della gestione e del monitoraggio del SIEM. Successivamente verificare che il team citato produca una documentazione sintetica o dei report, anche tramite il SIEM, che testimonino lo svolgimento del monitoraggio e della registrazione dell'attività di analisi e correlazione svolta. Infine, individuare la macchina o storage in cui sono conservati tutti i report e i documenti, relativi a queste attività, e verificare che siano conservati fino a 24 mesi prima.

3. Richiedere al soggetto una relazione in cui siano descritti e definiti i seguenti aspetti:
   a. le politiche applicate per individuare i sensori e le sorgenti citate nel controllo uno alla lettera a).
   b. le procedure e gli strumenti tecnici per ottenere le informazioni di cui al controllo numero uno lettere a) e b).
   c. le politiche, i processi e gli strumenti tecnici per l'analisi e la correlazione di cui al controllo numero uno, lettera c).
   d. i processi e gli strumenti tecnici per il monitoraggio e la registrazione di cui al controllo numero due.

4. Richiedere al CSP una relazione che espliciti le politiche e procedure di logging, monitoraggio, sicurezza e conservazione dei registri di accesso. Richiedere in calce alla relazione che sia riportata una cronistoria delle policy, in maniera da poterla analizzare e verificare se le politiche e le procedure siano state riviste e revisionate almeno una volta ogni anno.

5. Richiedere al provider i verbali relativi al processo di auditing per il rilevamento di informazioni inerenti alla sicurezza, il monitoraggio degli accessi, modifiche o cancellazioni non autorizzate di dati o metadati. Successivamente ispezionare i documenti forniti per valutare il processo di auditing e se effettivamente esso è implementato. Nel caso in cui il provider non fornisca tali verbali il controllo è non superato.

6. Richiedere al soggetto una relazione in cui siano descritti i processi, le procedure e le misure tecniche per la segnalazione di anomalie e guasti del sistema

di monitoraggio. Poi, valutare se tra questi elementi sia inserito un processo, procedura o misura tecnica finalizzata alla notifica immediata di guasti e anomalie al soggetto responsabile. Infine, richiedere al provider i verbali prodotti a seguito del processo di valutazione dei processi, procedure e misure tecniche menzionate, per revisionarli e determinare effettivamente se la valutazione è avvenuta e in maniera corretta.

7. Richiedere al fornitore di servizi Cloud se sono stati definiti e implementati degli strumenti che permettano all'Amministrazione di gestire gli errori e il logging. Successivamente controllare che questi strumenti permettan o la definizione del periodo di custodia desiderato e che permettano di avere informazioni sullo stato di sicurezza del servizio Cloud che l'Amministrazione ha comprato. Infine, controllare che le informazioni fornite siano adatte per la verifica dei due aspetti riportati nel controllo omonimo.

8. Richiedere al fornitore di servizi Cloud se per tutti i servizi Cloud acquistati da un'amministrazione sia possibile integrare i log dei servizi all'interno del sistema SIEM di gestione e e monitoraggio dell'Amministrazione. Successivamente, richiedere al fornitore di servizi Cloud una relazione dettagliata o dei riferimenti nella documentazione dei servizi, che spieghino come esportare i log dei servizi.

9. Solo per Amministrazioni che erogano servizi di livello almeno critico, richiedere al CSP l'accesso alla propria rete o infrastruttura virtuale, in maniera tale da individuare la macchina che viene adibita a repository centralizzato dei log di accesso degli utenti del soggetto alle varie risorse del soggetto. Successivamente, accedendo al sistema di PAM del soggetto verificare che le utenze privilegiate di questo repository siano riconducibili solo a personale interno al Cloud Provider. Infine, controllare che la macchina o storage, reale o virtuale che contiene il repository centralizzato siano all'interno di una sottorete isolata da tutte le altre macchine reali o virtuali utilizzate da terze parti, oppure sia l'unica macchina virtuale emulata su una certa macchina server del data center, che non deve essere utilizzata da nessun altro.

10. Solo per Amministrazioni che erogano servizi di livello almeno strategico, richiedere al Cloud Service Provider il documento aggiornato di dettaglio contenente i processi e le politiche espressi nel controllo numero 3, lettere a, b, c e d, al fine di ispezionarlo.

2.40 DE.CM-1

Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity

Metodo di verifica

1. Richiedere al Cloud Service Provider, un accesso privilegiato alla rete virtuale che gestiscono, per poi individuare tutte le macchine nella rete che non possono essere usate da terze parti, perché ospitano strumenti sensibili per il logging o

il monitoraggio. Successivamente verificare se in qualcuna di queste macchine siano presenti Intrusion Detection System, accedendovi e controllando tutti i software che sono installati su quelle macchine. Alternativamente, richiedere al CSP una relazione dettagliata, che ci si impegna a non divulgare, nella quale siano descritti gli IDS utilizzati e su quale macchine sono installati.

2. Richiedere al Cloud Service Provider una relazione dettagliata che descriva quali sono i processi di monitoraggio degli eventi che riguardano la sicurezza e l'infrastruttura sottostante. Successivamente accedere all'infrastruttura del CSP e verificare che questi processi siano effettivamente messi in atto così come documentato, verificando che esistano applicativi, interfacce o SIEM, che si occupano di raccogliere i log degli eventi citati permettendone così l'analisi e il monitoraggio.

3. Accedere all'infrastruttura del Cloud Service Provider e individuare la macchina, o le macchine, in cui è ospitato il sistema di monitoraggio degli accessi citato nel controllo. Valutare come questo sistema produce log e allarmi relativi alle attività classificate come sospette e quali sono i criteri che permettono al sistema di stabilire che un'attività è sospetta(regole, modelli di Machine Learning e così via). Infine, stabilire se e come il provider ha definito, per ogni tipologia di attività sospetta rilevata, un processo che permette di adottare azioni tempestive e appropriate per le anomalie rilevate.

5. Solo per Amministrazioni che erogano servizi almeno di livello critico, accedere alla rete virtuale del CSP e verificare che tutti i sistemi perimetrali, quali routers e firewalls, inviino tutti i loro log ed alert verso un unico storage, o un insieme di storage, che alimenta un SIEM. Controllare, inoltre, che tutti i log degli eventi amministrativi di rilievo e degli accessi alle risorse di rete o postazioni terminali, siano sempre inviati verso lo stesso "pozzo" che alimenta il sistema SIEM. Infine, constatare che nel SIEM siano previste regole di alerting, monitoraggio e correllazione di tutti gli eventi raccolti, al fine che sia possibile per il team di cybersecurity identificare tempestivamente tutti gli eventi di cybersecurity.

6. Solo per Amministrazioni che erogano servizi almeno di livello critico, accedere all'infrastruttura del CSP e stilare una di tutti gli strumenti tecnici presenti nell'infrastruttura che permettono di soddisfare i controlli numero uno, tre, quattro e cinque. Successivamente per ognuno di questi strumenti recuperare:
   - La versione installata, al fine di controllare che non sia una versione vulnerabile o troppo obsoleta.
   - I log di gestione dello strumento, al fine di poter revisionare tutte le attività di manutenzione e aggiornamento.
   - I file di configurazione degli strumenti per poterne analizzare la configurazione.

   Una volta recuperate tutte le informazioni necessarie, strumento per strumento, controllare che le configurazioni, gli aggiornamenti e le attività di manutenzione siano state condotte nel rispetto delle policy stabilite alle categorie

PR.AC, PR.DS, PR.IP, PR.MA. Infine, verificare che tutte queste attività siano state condotte al fine di forzare il rispetto delle policy definite alle categorie ID.AM, ID.GV, ID.SC, PR.AC, PR.DS.

7. Solo per Amministrazioni che erogano servizi almeno di livello critico, verificare che gli strumenti tecnici utilizzati per soddisfare i controlli numero uno, tre, quattro e cinque siano gli stessi strumenti utilizzati per soddisfare sottocategorie e controlli della categoria DE.AE.

8. Solo per Amministrazioni che erogano servizi almeno di livello critico, richiedere al CSP, impegnandosi a non diffonderne il contenuto, un documento aggiornato che descriva le politiche di sicurezza adottate in relazione ai controlli numero uno, tre, quattro e cinque, e i processi, le metodologie e le tecnologie impiegate per il rispetto delle politiche stesse.

2.41 DE.CM-4

Il codice malevolo viene rilevato

Metodo di verifica

1. Accedere all'infrastruttura del Cloud Service Provider e verificare che nelle macchine nevralgiche o nelle macchine utilizzate dai clienti siano presenti delle sonde, cioè dei sensori, che inviino dati a un'altra macchina con installato sopra un software antivirus e antimalware, capace di rilevare e bloccare sul nascere l'operato del codice malevolo. Successivamente, controllare che il CSP abbia adottato una Endpoint Protection Platform in maniera tale da poter avere un unico punto centrale da cui monitorare proteggere tutte le postazioni terminali presenti nella rete delle macchine presenti nei vari data center. Alternativamente verificare che siano adottati almeno nei punti più importanti e nevralgici dell'infrastruttura del CSP, delle soluzioni di Endpoint Protection Systems.

2. Richiedere al CSP una relazione in cui siano descritte tutte le politiche antimalware che sono adottate all'interno del provider. Richiedere, in allegato al documento, anche una cronistoria o dei verbali di riunioni, che permattano di stabilire se tali policies siano state riviste almeno una volta ogni anno.

4. Accedere all'infrastruttura del Cloud Provider e censire tutti i dispositivi presenti. Successivamente, verificare che in ogni dispositivo sia installato un software firewall adatto e che sia stato configurato in maniera da funzionare correttamente. Per quest'ultimo aspetto, verificare qual è la versione del firewall installato sul dispositivo e successivamente accedere al file di configurazione per verificarne la correttezza. Tale metodologia si applica solo nel caos in cui siano coinvolte Amministrazioni che erogano servizi almeno di livello critico.

5. Accedere all'infrastruttura o rete virtuale del Cloud Service Provider e verificare che tutti i computer dei dipendenti abbiano configurato un antivirus che analizzi i file che sono scaricati o che sono introdotti all'interno del filesystem attraverso un dispositivo removibile. Inoltre, se necessario, verificare che sia

attivata la funzionalità di Sandbox nel sistema operativo della macchina, verificando che i file scaricati passino per AppContainer, nel caso di una macchina con installato Windows, per AppSandbox, nel caso di una macchina con installato MacOS, oppure per seccomp, nel caso di una macchina con installato linux. Nel caso in cui il dipendente utilizzi un dispositivo mobile, verificare che sia configurato l'ambiente di sandboxing predefinito per Android, oppure che sia attivo AppSandbox nel caso di un dispositivo IoS. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

6. Una volta ottenuto un accesso privilegiato alla rete interna del Cloud Service Provider, stilare una lista di tutti gli strumenti tecnici che sono utilizzati per soddisfare i controlli numero uno, quattro e cinque. Quindi, censiti tutti gli strumenti recuperare le seguenti informazioni:
   - La versione installata, al fine di controllare che non sia una versione vulnerabile o troppo obsoleta.
   - I log di gestione dello strumento, al fine di poter revisionare tutte le attività di manutenzione e aggiornamento.
   - I file di configurazione degli strumenti per poterne analizzare la configurazione.
   - Il database delle firme dell'antivirus o dell'antimalware nel caso in cui sia uno strumento basato su firme. Altrimenti, nel caso in cui l'antimalware abbia incorporato un modello di intelligenza artificiale, richiedere al team di sicurezza i dataset con cui è stato eseguito l'ultimo addestramento del modello, il tipo di algoritmo utilizzato e i parametri dell'algoritmo.

   Ottenute tutte queste informazioni analizzarle, strumento per strumento, e stabilire se la configurazione e gli interventi di aggiornamento e manutenzione soddisfano le politiche espresse nella categorie PR.AC, PR.DS, PR.IP e PR.MA e garantiscono il rispetto delle politiche espresse nelle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS. Tale metodologia si applica solo per Amministrazioni che erogano un servizio di livello almeno critico.

7. Solo per Amministrazioni che erogano servizi almeno di livello critico, richiedere al Cloud Service Provider il documento aggiornato e di dettaglio recante la descrizione delle politiche di sicurezza adottate in relazione ai controlli numero uno, due e tre, e tutti i processi, metodologie e tecnologie impiegate per rispettare le politiche di sicurezza.

2.42 DE.CM-7

Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati

Metodo di verifica e ispezione

Tutte le metodologie espresse di seguito si applicano solo per Amministrazioni che erogano servizi di livello almeno critico.

1. Per quanto riguarda l'accesso fisico alle risorse e ai data center tutti i Cloud Provider in analisi, ovvero Azure, Google Cloud e AWS, implementano delle misure di sicurezza molto stringenti che permettono facilmente di rilevare l'accesso fisico di personale non autorizzato. Infatti, nelle seguenti pagine della documentazione è presente una lista di tutti i controlli messi in piedi dai tre provider per rendere sicuri i loro data center: Azure[141], Google Cloud[142], AWS[143]. Nel caso in cui tale metodologia si applichi per un altro Cloud Service Provider, è necessario richiedere una visita presso uno dei data center utilizzati dal CSP e verificare che siano implementati dei sistemi di sorveglianza come accesso multifattore con dati biometrici e badge, processi di revoca dei privilegi di accesso, sistemi di sorveglianza a circuito chiuso e così via, prendendo anche come riferimento quello che fanno i maggiori CSP. Per quanto riguarda gli accessi da remoto, è necessario richiedere l'accesso alla rete virtuale del provider e verificare che il sistema di Priviliged Access Management emetta dei log ad ogni tentativo di accesso che possano essere usati come sorgente di un SIEM che permette di sorvegliare accessi remoti non autorizzati.

2. Accedere all'infrastruttura del Cloud Service Provider o alla sua rete virtuale e verificare che ci sia un sistema di rilevamento di connessioni non autorizzate e un meccanismo che permetta solo a dispositivi appartenenti a personale autenticato e con delle credenziali valide di connettersi alla rete. Infatti, è necessario verificare che siano presenti dei sistemi di controllo degli accessi alle reti come EAP o PEAP, che permettono solo a dispositivi autenticati e registrati di connettersi alla rete del CSP.

3. Accedere all'infrastruttura del CSP e stilare una lista di tutti gli strumenti tecnici che sono utilizzati per soddisfare i controlli numero uno e due. Successivamente per tutti gli strumenti utilizzati per la sicurezza e il controllo degli accessi fisici, richiedere al CSP una relazione in cui siano descritti tutti gli interventi di manutenzione e di aggiornamento del firmware degli stessi. Successivamente per gli strumenti per controllare l'accesso da remoto alle risorse, e per quelli che permettono di controllare l'accesso alla rete del CSP, verificare che siano emessi in qualche storage o macchina dei log consultabili che elenchino tutte le attività di manutenzione e aggiornamento, e che siano accessibili i file di configurazione degli stessi. A questo punto, ottenute tutte le informazioni necessarie, analizzare quanto raccolto al fine di stabilire se sono rispettate le politiche espresse nelle categorie PR.AC, PR.DS, PR.IP e PR.MA, e se gli strumenti configurati permettono di far rispettare le policies espresse nelle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.

4. Richiedere al Cloud Service Provider il documento aggiornato e di dettaglio che descriva le politiche di sicurezza adottate relativamente al controllo numero uno e al controllo numero due e i processi, le metodologie e le tecnologie che sono impiegate per il rispetto delle policy.

5. Accedere all'infrastruttura del Cloud Service Provider, da utente privilegiato, e verificare che nella rete sia presente un sistema di rilevamento di software non approvati che abbia sonde in tutte le macchine della rete, le quali devono inviare, ogni qualvolta viene installato un software su quelle macchine, tutti

i dati relativi al software installato. Tale sistema deve essere anche in grado, ricevuti questi dati, di classificare il software come autorizzato o non autorizzato secondo una policy configurata dal Cloud Service Provider. Infine, deve fornire una funzionalità di interrogazione dei dati e di un suo archivio che permetta agli amministratori di sicurezza di recuperare la lista dei software non approvati e capire in quale macchina e d quale dipendente sono stati installati. Tale metodologia si applica solo per Amministrazioni che erogano servizi di livello almeno strategico.

6. Una volta ottenuto l'accesso all'infrastruttura di rete del Cloud Provider, verificare che nei router della rete sia presente un'interfaccia di amministrazione che permetta di vedere quali dispositivi sono connessi a quel router. Successivamente, verificare che esista un sistema centralizzato capace di ottenere la lista di tutti i dispositivi connessi a un router, per ogni router della rete. Tale dispositivo, poi, una volta ottenute tutte le liste, deve produrre una lista sintetica di dispositivi connessi alla rete, eliminando i duplicati e dispositivi perimetrali. Infine, esso deve potersi interfacciare con un database di tutti i dispositivi autorizzati a connettersi alla rete, in maniera tale da poter emettere degli allarmi nel momento in cui, tra i dispositivi connessi, ne risulta uno non autorizzato.

7. Accedere all'infrastruttura del CSP e stilare una lista di tutti gli strumenti tecnici che sono utilizzati per soddisfare i controlli numero cinque e sei. Successivamente, recuperare i log di gestione sia del sistema di rilevamento dei software non approvati sia del sistema di rilevamento delle connessioni non approvate, oltre che i file di configurazione dei suddetti sistemi. A questo punto, analizzare le informazioni raccolte, strumento per strumento, al fine di stabilire se sono rispettate le politiche espresse nelle categorie PR.AC, PR.DS, PR.IP e PR.MA, e se gli strumenti configurati permettono di far rispettare le policies espresse nelle categorie ID.AM, ID.GV, ID.SC, PR.AC e PR.DS.

8. Richiedere al CSP il documento aggiornato e di dettaglio che descrive le politiche di sicurezza adottate relativamente ai controlli numero cinque e sei, e le procedure, metodologie e tecnologie implementate che servono a far rispettare le politiche di sicurezza.

2.43 DE.CM-8

Vengono svolte scansioni per l'identificazione di vulnerabilità

Metodo di verifica e ispezione

Tutte le metodologie elencate di seguito si applicano solo per Amministrazioni che erogano servizi almeno di livello critico.

1. Per verificare l'esecuzione del processo di vulnerability assessment e penetration testing di un applicativo software prima della messa in esercizio dello stesso è necessario richiedere al Cloud Provider il report tecnico che è stato scritto prima della messa in esercizio del prodotto. Verificare che il report

riporti una data anteriore alla messa in esercizio del progetto e che sia sufficientemente dettagliato. Nel caso in cui il CSP non fornisca tale documento il controllo è da ritenersi non superato.

2. **MS Azure:** Azure pubblica periodicamente i report dei penetration test che sono condotti da parte di aziende esterne ingaggiate da Microsoft a tale scopo. Quindi, Azure si sottopone regolarmente a penetration tests e a un processo di vulnerability assessment & penetration testing. L'ultimo dei report pubblicati da Microsoft è visibile consultando il seguente documento[44], le relazioni periodiche dei penetration test condotti sul servizio contengono tutti gli elementi riportati nel controllo omonimo. Inoltre, come dichiarato in questa pagina[144] della documentazione, nel contesto della preparazione alla risposta agli incidenti di sicurezza viene condotta regolarmente un'opera di vulnerability assessment & penetration testing.

   Google Cloud: Google Cloud, come riportato in questa pagina[145], mantiene un team permanente di sicurezza che si occupa, tra le altre cose, di portare avanti un processo continuo di vulnerability assessment e pentesting. Essi utilizzano strumenti automatici per ricercare le minacce, e conducono autonomamente dei test di penetrazione su tutta l'infrastruttra di Google Cloud.

   AWS: AWS non accenna nulla nella sua documentazione riguardo il processo di vulnerability assessment & penetration testing condotto. Quindi, è necessario richiedere al team di sicurezza del Cloud Provider, la documentazione che riporta ogni quanto sono stati eseguiti il processo di vulnerability assessment e di penetration testing sull'infrastruttura AWS. Quindi, è necessario richiedere al CSP una cronistoria che riporta tutte le sessioni di vulnerability assessment & penetration testing condotte. Allo stesso modo richiedere anche i report di queste sessioni, per capire quanto dettagliato fosse il processo. Tale metodologia di procedere è valida per qualsiasi altro provider.

3. Richiedere al Cloud Service Provider il documento aggiornato che riporta le tipologie di penetration tests e vulnerability assessment previsti.

4. Richiedere al CSP il registro aggiornato che contiene la lista di tutti i penetration tests eseguiti e tutta la doccumentazione ad essa associato, compresa la reportistica.

2.44 RS.RP-1

Esiste un piano di risposta(response plan) e questo viene eseguito durante o dopo l'incidente

Metodo di verifica e ispezione

1. **MS Azure:** Nel piano di risposta agli incidenti, come riportato in questa pagina[146], viene riportato che non appena viene conclusa la fase di

escalation, ovvero la fase in cui si determina e si segue l'evoluzione dell'incidente, si procede con la formazione di un "vteam", ovvero un team più ampio del team di sicurezza di Azure che si occupa della gestione dell'incidente. Quindi, la comunicazione verso le altre articolazioni competenti del soggetto, tra cui il team di risposta agli incidenti, il team di comunicazione degli incidenti e vari team di servizio, avviene quasi subito dopo una prima valutazione dell'incidente. Perciò, il controllo può considerarsi soddisfatto, in quanto, seguendo quanto dice la documentazione prima citata, non appena un SIEM che attinge da un sistema di log centralizzato rileva qualche anomalia, il team di sicurezza valuta il possibile incidente subito, determinandone il livello di gravità. Inoltre, subito dopo una veloce valutazione della gravità dell'incidente sono avvertite tutte le articolazioni competenti del soggetto, compreso il team di comunicazione che nella successiva fase di ripristino si dovrà occupare di notificare all'Amministrazione l'incidente. Non si parla nella documentazione di eventuali notifiche al CSIRT Italia.

Google Cloud: Nella documentazione[147] viene riportato che, a seguito della fase di identificazione, in cui strumenti automatici e manuali producono un primo report sulla natura dell'incidente, avvalendosi di log, IDS basati su anomaly detection e così via, si procede subito con la fase di valutazione dell'incidente che viene effettuata da un "oncall responder". L'oncall responder rivaluta l'incidente in maniera rapida e passa la sua gestione a un "incident Commander", che si occupa di coinvolgere subito tutte le articolazioni competenti del soggetto per la risposta all'incidente, compreso il team di comunicazione che si dovrà occupare nella fase successiva della notifica ai clienti coinvolti nell'incidente, tra cui anche l'Amministrazione. Non si afferma esplicitamente se anche al CSIRT Italia arriva una notifica dell'incidente. In sintesi, si può stabilire che per come viene descritto il processo di risposta all'incidente il controllo risulta soddisfatto.

AWS: Relativamente a questo Cloud Service Provider non sono riportati dettagli sul piano di risposta all'incidente. Si ritiene necessario allo scopo di verificare il controllo, richiedere al CSP il piano di risposta agli incidenti per verificare se prevede una tempestiva analisi e valutazione degli eventi rilevati. Inoltre, bisogna controllare che il piano preveda di informare tutte le articolazioni competenti del soggetto necessarie a rispondere all'incidente, compreso il team di comunicazione dell'incidente, che si dovrà occupare di notificare l'incidente all'Amministrazione e al CSIRT Italia.

2. Solo per Amministrazioni che erogano servizi di livello almeno critico, richiedere al provider una relazione contenente la lista di tutti gli incontri o riunioni che hanno avuto come oggetto la rivalutazione delle politiche e procedure di sicurezza per la gestione degli incidenti. Stabilire poi se la revisione avviene almeno annualmente.

3. **MS Azure:** Seguendo quanto riportato nella documentazione[146] del provider, il piano di risposta coinvolge tutti i dipartimenti interessati dall'incidente e tutte le figure professionali necessarie per la risposta. Comunque, non essendo tale documento ufficiale, se si vuole avere una prova ufficiale

del coinvolgimento sia dei dipartimenti critici del soggetto, sia dell'Amministrazione stessa e di tutte le terze parti interessate, è necessario richiedere il piano di risposta agli incidenti e una relazione che riporti le politiche citate nel controllo due al CSP e valutare se gli enti citati sono coinvolti.

Google Cloud: Dalla documentazione[147] non si ha una chiara evidenza di chi viene coinvolto, ma semplicemente viene assicurato che l'incident Commander si occupa di coinvolgere tutto il personale necessario per rispondere all'incidente. Per questo si ritiene necessario richiedere il piano di risposta e una relazione che riporti le politiche citate nel controllo due al Cloud Provider per valutare se viene previsto il coinvolgimento dei dipartimenti critici del soggetto, dell'Amministrazione e di tutte le terze parti interessate.

AWS: Richiedere al Cloud Service Provider il piano di risposta agli incidenti e una relazione in cui sono descritte le politiche citate al controllo numero due, al fine di valutare se entrambi prevedano il coinvolgimento nel piano dei dipartimenti critici, dell'Amministrazione e di tutte le terze parti interessate

Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

4. Richiedere al provider una relazione in cui si elenchino in ordine cronologico tutte le variazioni e revisioni subite dal piano di risposta agli incidenti, opportunamente motivate. Verificare che tali variazioni o revisioni siano state effettuate periodicamente o in seguito a cambiamenti organizzativi o ambientali significativi, osservando la motivazione degli stessi. Infine, richiedere al soggetto un documento che registri tutti i collaudi del piano di risposta agli incidenti, in maniera tale da valutare che questi siano stati effettuati in maniera periodica e con cadenza adeguata. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

5. Sia Microsoft che Google nelle loro documentazioni riportano alcune metriche considerate durante il processo di stima del livello di severità dell'incidente, come visibile consultando i link nel controllo numero uno e numero due. Chiaramente se si vuole avere una definizione di maggior dettaglio è necessario procedere come si farebbe, invece, per AWS che non riporta nulla sul suo piano di risposta agli incidenti. Quindi, è necessario richiedere al Cloud Service Provider una relazione di dettaglio in cui sono definite tutte le metriche degli incidenti rilevanti in materia di cybersecurity. Infine, è necessario confrontare la relazione con il piano di risposta agli incidenti per stabilire se le metriche fornite sono tutte monitorate durante il processo di risposta. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

6. Richiedere al CSP una relazione che descriva tutti i processi, procedure e misure di supporto ai processi aziendali per il triage degli eventi legati alla sicurezza. Successivamente richiedere al soggetto la documentazione relativa alle esercitazioni e al collaudo dei piani di risposta per verificare che questi

processi, procedure e misure di supporto siano effettivamente implementate. Infine, se da quanto visionato non si è sicuri dell'effettiva implementazione richiedere al provider la possibilità di assistere a un collaudo del piano di risposta agli incidenti. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

7. Visitare la sede del Cloud Provider, per verificare che sia implementato un CERT per coordinare la fase di risoluzione degli incidenti aderendo allo standard ISO/IEC 27035-2. Inoltre, si valuti la disponibilità del Cloud Service Provider a coinvolgere periodicamente l'Amministrazione nella condivisione, revisione e risoluzione degli incidenti. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

2.45 RS.CO-1

Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta a un incidente

Metodo di verifica

1. Il controllo va revisionato da chi lo ha ideato. Non è stato possibile sviluppare una metodologia.

2. Richiedere al provider un registro in cui sono annotate tutte le attività di esercitazione condotte, al fine di verificare la loro periodicità e di stabilire se sono eseguite abbastanza spesso.

3. Il controllo va revisionato da chi lo ha ideato. Non è stato possibile sviluppare una metodologia.

4. Richiedere al provider il registro in cui sono annotate tutte le attività di esercitazione svolte, controllando che per ognuna delle esercitazioni siano riportate le lezioni apprese. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

5. Richiedere al Cloud Service Provider una relazione dettagliata che descriva le politiche e le procedure per la gestione degli incidenti e i processi di E-Discovery & Cloud Forensics. Inoltre, richiedere anche un documento ufficiale contenente la lista di tutte le revisioni apportate alle procedure e alle politiche, in maniera da verificare che avvengano revisioni almeno su base annuale. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

6. Richiedere al Cloud Service Provider una relazione in cui sono descritti i processi, le procedure e le misure tecniche per notificare le violazioni di sicurezza, sia all'interno dell'organizzazione del CSP, sia all'Amministrazione. Successivamente richiedere al fornitore di servizi Cloud una prova che testimoni l'implementazione di questi processi, procedure o misure tecniche. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

7. Richiedere al Cloud Service Provider una relazione in cui viene descritto in maniera dettagliata il meccanismo di segnalazione di ogni violazione di sicurezza. Assicurarsi che tale meccanismo comprenda le violazioni che riguardano la supply chain e che avvengano nel rispetto di SLA, leggi e regolamenti.

8. Richiedere al Cloud Service Provider il piano delle comunicazioni che si applica nel momento in cui avvengono le attività di risposta all'incidente. Verificare che all'interno del piano si affermi che sia obbligatorio informare delle attività di risposta tutte le parti interessate interne ed esterne al soggetto, compresi i dirigenti e i vertici. Inoltre, verificare che sia presente nel piano la prescrizione di informare tutte le articolazioni competenti del soggetto riguardo tutte le attività di risposta. Per verificare la messa in atto del piano così come viene analizzato, richiedere la documentazione dell'attività postincidente, per valutare se le comunicazioni sono state effettuate correttamente. Tale metodologia si applica solo per Amministrazioni che erogano servizi almeno di livello critico.

2.46 RS.CO-3

Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione

Metodo di verifica

Solo per Amministrazioni che erogano un servizio di livello almeno critico, richiedere al provider il piano delle comunicazioni che si applica nel momento in cui avvengono le attività di ripristino dall'incidente. Successivamente constatare che il piano contenga la prescrizione di informare delle attività di ripristino dall'incidente tutte le parti interessate sia interne che esterne al soggetto.

2.47 RS.CO-5

É attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)

Metodo di verifica

1. Richiedere al servizio di assistenza del Cloud Provider una lista di tutti i gruppi di interesse legati al Cloud e altre entità con cui il CSP mantiene dei contatti. Successivamente richiedere anche una relazione in cui siano descritti i tipi di contatti con questi gruppi ed entità e tutte le iniziative messe in pratica con esse, al fine di valutare se i contatti sono mantenuti.

2. Richiedere al provider una lista dettagliata di tutti i punti di contatto con autorità di regolamentazione applicabili, forze dell'ordine e autorità giurisdizionali. Successivamente, per verificare che questi contatti siano mantenuti richiedere al soggetto una relazione che documenti tutti le iniziative, i contatti avuti con questi enti, certificando anche qual era il fine dell'interazione.

2.48 RS.AN-5

Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)

Metodo di verifica

1. Accedere all'infrastruttura di rete virtuale, impersonando il ruolo di uno dei dipendenti del Cloud Provider e verificare che sia accessibile una pagina web, un'applicazione web o directory condivisa, in cui siano memorizzati tutti gli esiti delle valutazioni citati nella sottocategoria DE.AE-3 e gli esiti dei pentests e vulnerability assessment citati nella sottocategoria DE.CM-8. Verificare che indipendentemente dal team a cui appartiene e dal tipo di dipendente si riesca sempre ad accedere a questi documenti.

2. Richiedere al Cloud Service Provider un report di monitoraggio di tutti i canali di comunicazione citati nel controllo omonimo, al fine di valutare se il monitoraggio viene effettuato in maniera corretta.

3. Richiedere al soggetto il documento aggiornato che descrive gli elementi indicati nel punto a. e nel punto b. del controllo omonimo.

2.49 RS.MI-3

Le nuove vulnerabilità sono mitigate o documentate come rischio accettato

Metodo di verifica

Tutte le metodologie esposte di seguito si applicano per Amministrazioni che erogano servizi almeno di livello critico.

1. Richiedere al Cloud Service Provider una relazione che descriva tutte le misure di mitigazione che sono riportate nel piano di gestione delle vulnerabilità, per poi verificarne l'effettiva implementazione accedendo all'infrastruttura del Cloud Provider. Successivamente richiedere al CSP una relazione in cui sia documentato, per ogni vulnerabilità mitigata, il rischio residuo e la motivazione dell'accettazione di quel rischio.

2. Richiedere al soggetto una relazione che definisca, per ogni vulnerabilità riportata e identificata nella relazione di cui al punto due, le procedure e misure tecniche che consentono di mettere in atto azioni di risposta derivate dallo sfruttamento della vulnerabilità. Successivamente richiedere al Cloud Service Provider la possibilità di condurre un'ispezione delle parti di infrastruttura virtuale o delle macchine in cui sono state rilevate delle vulnerabilità per poi valutare l'effettiva implementazione.

2.50 RC.RP-1

Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity

Metodo di verifica

Le seguenti metodologie si applicano solo per Amministrazioni che erogano servizi almeno di livello critico.

1. Richiedere al soggetto il piano di ripristino, per poi analizzarlo e stabilire se prevede tutti i processi e le procedure necessarie al ripristino del normale funzionamento dei servizi Cloud.

2. Richiedere al provider un registro di tutti i test del piano di recovery dei servizi cloud condotti fino al momento della verificare. Successivamente controllare che nel registro siano riportati almeno due esercitazioni di collaudo del piano di ripristino.

2.51 RC.IM-2

Le strategie di recupero sono aggiornate

Metodo di verifica

Solo per Amministrazioni che erogano servizi di carattere almeno strategico, richiedere al soggetto un documento ufficiale che contenga la lista di tutte le revisioni che ha subito il piano di ripristino e dei cambiamenti operati a seguito della revisione, per verificare che esso sia mantenuto aggiornato. Successivamente richiedere anche il registro delle lezioni apprese a seguito di ogni attività di ripristino effettuata documentata e controllare che tutti gli aggiornamenti subiti dal piano siano stati guidati dalle lezioni apprese.

Capitolo 3

Performance e Scalabilità

3.1 PS.CA-1

Il servizio cloud presenta le caratteristiche tipiche ed è conforme agli standard di settore

Risultati dell'ispezione

Il requisito è soddisfatto per tutti e tre i Cloud Provider. Analizzando le documentazioni di tutti e tre i soggetti si riesce facilmente a stabilire che è molto facile per l'Amministrazione che migra verso uno di questi Cloud operare da sola il provisioning delle risorse ad essa necessarie e senza necessità di approvazione da parte del CSP. Allo stesso modo sono molteplici le soluzioni di accesso alla rete, dato che sono implementate, oltre al normale accesso internet, anche soluzioni VPN e VPC. Infine, i provider garantiscono meccanismi di scalabilità verticale e orizzontale, come riportato anche nella documentazione dei servizi cloud di ognuno di loro.

3.2 PS.SC-1

Trasparenza sulle modalità e meccanismi di scalabilità

Metodo di verifica

Verificare che il soggetto al momento della stipula del contratto per la migrazione dei servizi dell'Amministrazione su Cloud sia disponibile a comunicare all'Amministrazione tutti gli elementi riportati nel controllo omonimo.

Capitolo 4

Interoperabilità

4.1 IP.GR-1

Sono disponibili API per la gestione remota del ciclo di vita del servizio

Risultati dell'ispezione

1. Il controllo risulta soddisfatto da tutti e tre i Cloud Provider, in quanto espongono delle REST API utilizzabili per gestire i servizi che l'Amministrazione migra su Cloud. Queste API consentono di eseguire operazioni, anche privilegiate se la richiesta viene fatta con le giuste credenziali. Quindi, esse permettono di implementare degli strumenti per la gestione del ciclo di vita del servizio cloud.

2. Tutti e tre i Cloud Provider soddisfano il controllo in quanto documentano in maniera molto dettagliata tutte le REST API. Le API Azure[148] sono documentate tutte in un'unica pagina, mentre Google Cloud e AWS documentano le API di ogni prodotto nella pagina di documentazione del prodotto stesso. Per quanto riguarda gli endpoint delle API, è necessario richiedere ad ogni Cloud Provider una lista degli endpoint da cui loro forniscono le API, in quanto questi non sono documentati.

4.2 IP.IN-1

Sono disponibili API per funzionalità applicative

Risultati dell'ispezione

In tutti e tre i Cloud Service Provider trattati tutti i servizi SaaS messi a disposizione sono corredati di API per l'interazione programmatica. Mentre Microsoft documenta queste API in un'unica pagina per tutti i servizi (API Azure[148]), invece Google Cloud e AWS documentano le API di ogni servizio nella pagina di documentazione del servizio. Per quanto riguarda gli endpoint delle API, è necessario richiedere ad ogni Cloud Provider una lista degli endpoint da cui loro forniscono le API, in quanto questi non sono documentati.

4.3 IP.PO-1

Sono disponibili funzionalità/API per import/export dei dati

Risultati dell'ispezione

Nelle documentazioni dei tre Cloud Service Provider sono disponibili degli strumenti per l'esecuzione della migrazione da un Cloud Provider all'altro. Ad esempio, AWS offre la possibilità di utilizzare Cloud Migration per importare dati e carichi di lavoro dal Cloud Microsoft e Google in maniera guidata. Allo stesso modo anche Azure, con Azure Migrate offre una soluzione simile e lo stesso vale per Google Clooud che offre strumenti specifici a seconda del carico di lavoro. Tuttavia, non esiste evidenza nella documentazione dei tre provider che esistano funzionalità o API che dichiaratamente facilitino la migrazione verso altri Cloud Service Provider. Quindi, è necessario contattare il team di vendita del fornitore di servizi Cloud e richiedere informazioni riguardo gli strumenti di migrazione e import/export dei dati messi a disposizione dal provider.

4.4 IP.PO-2

L'interoperabilità e la portabilità dei dati sono gestite mediante procedure e politiche regolarmente aggiornate. La portabilità dei dati prevede l'applicazione di protocolli di rete sicuri e l'accesso ai dati al termine dei rapporti contrattuali è gestito mediante accordi specifici.

Risultati dell'ispezione

1. Richiedere al soggetto una relazione in cui sono descritte tutte le politiche e le procedure per l'interoperabilità e la portabilità dei dati. Successivamente richiedere al CSP un documento che certifichi la revisione annuale delle politiche e procedure almeno annualmente, e verificare che la relazione citata contenga anche i requisiti per tutti gli elementi riportati nel controllo.

2. **MS Azure:** Seguendo quanto riporta la documentazione[111] del provider per la cifratura dei dati in transito, si rileva che sono utilizzati protocolli di rete sicuri per la maggior parte dei servizi cloud di Azure. Allo stesso modo consultando la documentazione delle API di Azure, si osserva che tutte le chiamate alle API sono protette secondo protocollo HTTPS. Quindi, il soggetto soddisfa il controllo.

   Google Cloud: In questa pagina[63] della documentazione di Google Cloud viene offerta una panoramica di tutti i meccanismi di cifratura in transito che si applicano anche quando avviene l'import e l'export dei dati. Infatti, vengono descritti vari casi di interazione possibili che prescindono dal tipo di operazione che viene fatta, ma riguardano solo chi comunica. In tutti questi sono utilizzati protocolli sicuri e standardizzati, così come nel caso dell'import ed export dei dati attraverso le API, per cui si usa sempre protocollo HTTPS.

   AWS: Amazon pubblica un breve estratto[149] su come cifra i dati in transito, indipendentemente dal fatto che questi siano importati o esportati. In tale estratto si dichiara che per tutte le comunicazioni tra i client e gli endpoint di AWS, compresi quelli delle API, si utilizzano i protocolli HTTPS e TLS

che permettono una cifratura dei dati rendendo il trasferimento sicuro e il controllo omonimo soddisfatto.

3. Richiedere al CSP gli accordi citati nel controllo e verificare che questi comprendano tutti gli elementi riportati nel controllo.

Bibliografia

[1] https://univpm-my.sharepoint.com/:b:/g/personal/s1107327_studenti_univpm_it/EeSYNqsqqf5ChensUYftSM4BUME_0ysdVAOqD2aIUAAfnA?e=ojnZCz.

[2] https://services.google.com/fh/files/misc/winter2023_iso_9001_certificate.pdf.

[3] https://d1.awsstatic.com/certifications/iso_9001_certification.pdf.

[4] https://univpm-my.sharepoint.com/:b:/g/personal/s1107327_studenti_univpm_it/ES-gksrNmJNPm1QCzoWrR3kBuHymojcxaLe5iIBqMDtv0w?e=phpXoV.

[5] https://cloud.google.com/security/compliance/offerings?hl=it#/countries=Global.

[6] https://d1.awsstatic.com/certifications/AWS_Certificate_ISO_20000_Global_Fall2022.pdf.

[7] https://azure.microsoft.com/it-it/support/#layout-container-uidfa83.

[8] https://cloud.google.com/support/docs?hl=it.

[9] https://aws.amazon.com/it/premiumsupport/plans/.

[10] https://azure.microsoft.com/it-it/support/legal/faq/#areaheading-oc6003.

[11] https://cloud.google.com/support/docs/language-working-hours?_ga=2.117485001.-11833560.1674832006&hl=it.

[12] https://aws.amazon.com/it/premiumsupport/faqs/.

[13] https://azure.microsoft.com/it-it/support/plans/.

[14] https://cloud.google.com/support/docs/customer-care-procedures?hl=it#contact_customer_care.

[15] https://azure.microsoft.com/en-us/updates/?

[16] https://cloud.google.com/release-notes.

[17] https://cloud.google.com/release-notes/all.

[18] https://aws.amazon.com/it/new/?whats-new-content-all.sort-by=item.additionalFields.postDateTime&whats-new-content-all.sort-order=desc&awsf.whats-new-categories=*all.

[19] https://learn.microsoft.com/en-us/security/benchmark/azure/introduction.

[20] https://learn.microsoft.com/en-us/azure/app-service/overview-monitoring.

[21] https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods.

[22] https://learn.microsoft.com/en-us/entra/fundamentals/whatis.

[23] https://cloud.google.com/architecture/framework/security.

[24] https://cloud.google.com/support/bulletins.

[25] https://cloud.google.com/monitoring/docs/monitoring-overview.

[26] https://cloud.google.com/error-reporting/docs/grouping-errors.

[27] https://cloud.google.com/docs/authentication.

[28] https://cloud.google.com/iam/docs/overview.

[29] https://docs.aws.amazon.com/wellarchitected/latest/framework/welcome.html.

[30] https://aws.amazon.com/security/security-bulletins/?nc1=h_ls&card-body.sort-by=item.additionalFields.bulletinId&card-body.sort-order=desc&awsf.bulletins-flag=*all&awsf.bulletins-year=*all.

[31] https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html.

[32] https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html#intro-structure-authentication.

[33] https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html.

[34] https://learn.microsoft.com/en-us/azure/cost-management-billing/cost-management-billing-overview.

[35] https://cloud.google.com/billing/docs/concepts.

[36] https://docs.aws.amazon.com/it_it/awsaccountbilling/latest/aboutv2/billing-what-is.html.

[37] https://cloud.google.com/billing/docs/how-to/budgets#budget-actions.

[38] https://docs.aws.amazon.com/cost-management/latest/userguide/what-is-costmanagement.html.

[39] https://docs.aws.amazon.com/cost-management/latest/userguide/budgets-controls.html.

[40] https://univpm-my.sharepoint.com/:b:/g/personal/s1107327_studenti_univpm_it/EWmZOMFoA6BJgeQNL42SbI0BqMGr31S1dVYqlTWCmU5dIQ?e=T5PtDA.

[41] https://univpm-my.sharepoint.com/:b:/g/personal/s1107327_studenti_univpm_it/EabGySD2iYVGqXwHQIdluaYBuALdnvMkf6Xh3gZmXRj-Eg?e=iYODQs.

[42] https://univpm-my.sharepoint.com/:b:/g/personal/s1107327_studenti_univpm_it/ER8S7u7uJ_NNlnkQYB4W-r0BfVTHDccz96by0WBrQ8Wjsg?e=OQdAaA.

[43] https://univpm-my.sharepoint.com/:b:/g/personal/s1107327_studenti_univpm_it/EfnX_0RJLO9HozlmCLecmrkBcOs430J19SHFd_6QmJ5HMg?e=XcR3z3.

[44] https://univpm-my.sharepoint.com/:b:/g/personal/s1107327_studenti_univpm_it/EUK6SBYsYwNBn37OJmCEYssBiWZwIk2YUJYkCfd89aYTzQ?e=r2HekK.

[45] https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/.

[46] https://aws.amazon.com/compliance/shared-responsibility-model/?nc1=h_ls.

[47] https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.

[48] https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fat.

[49] https://univpm-my.sharepoint.com/:b:/g/personal/s1107327_studenti_univpm_it/EZUK4VYKJgJLte1IxRtJouMB9Omvzv9cWxep-JLyDg5Ecw?e=Lgv2Fw.

[50] https://cloud.google.com/terms/subprocessors.

[51] https://aws.amazon.com/it/compliance/sub-processors/archived/sub-processors_10262023/.

[52] https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa.

[53] https://cloud.google.com/identity/solutions/enforce-mfa?hl=it.

[54] https://aws.amazon.com/it/iam/features/mfa/?audit=2019q1.

[55] https://download.microsoft.com/download/1/6/0/160216AA-8445-480B-B60F-5C8EC8067FCA/WindowsAzure-SecurityPrivacyCompliance.pdf.

[56] https://services.google.com/fh/files/misc/072022_google_cloud_trust_whitepaper.pdf?hl=it.

[57] https://docs.aws.amazon.com/pdfs/whitepapers/latest/navigating-gdpr-compliance/navigating-gdpr-compliance.pdf.

[58] https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview.

[59] https://learn.microsoft.com/en-us/azure/key-vault/keys/about-keys.

[60] https://learn.microsoft.com/en-us/azure/key-vault/keys/about-keys-details.

[61] https://learn.microsoft.com/en-us/azure/key-vault/keys/about-keys-details.

[62] https://cloud.google.com/docs/security/encryption/default-encryption?hl=it.

[63] https://cloud.google.com/docs/security/encryption-in-transit?hl=it.

[64] https://cloud.google.com/docs/security/encryption/customer-supplied-encryption-keys?hl=it.

[65] https://developers.google.com/tink?hl=it.

[66] https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3678.

[67] https://docs.aws.amazon.com/pdfs/kms/latest/cryptographic-details/kms-crypto-details.pdf.

[68] https://docs.aws.amazon.com/pdfs/kms/latest/developerguide/kms-dg.pdf.

[69] https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management-choose.

[70] https://learn.microsoft.com/en-us/azure/key-vault/general/security-features#key-vault-authentication-options.

[71] https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/key-vault-security-baseline?context=%2Fazure%2Fkey-vault%2Fgeneral%2Fcontext%2Fcontext.

[72] https://cloud.google.com/kms/docs/key-management-service.

[73] https://docs.aws.amazon.com/kms/latest/developerguide/data-protection.html#encryption-key-mgmt.

[74] https://learn.microsoft.com/en-us/rest/api/keyvault/keys/update-key/update-key?view=rest-keyvault-keys-7.4&tabs=HTTP.

[75] https://learn.microsoft.com/en-us/rest/api/keyvault/keys/delete-key/delete-key?view=rest-keyvault-keys-7.4&tabs=HTTP.

[76] https://learn.microsoft.com/en-us/rest/api/keyvault/keys/purge-deleted-key/purge-deleted-key?view=rest-keyvault-keys-7.4&tabs=HTTP.

[77] https://cloud.google.com/kms/docs/rotate-key#manual.

[78] https://cloud.google.com/kms/docs/re-encrypt-data.

[79] https://cloud.google.com/kms/docs/enable-disable#disable.

[80] https://cloud.google.com/kms/docs/destroy-restore#destroy.

[81] https://docs.aws.amazon.com/kms/latest/developerguide/enabling-keys.html.

[82] https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys-scheduling-key-deletion.html.

[83] https://docs.aws.amazon.com/kms/latest/developerguide/multi-region-keys-delete.html.

[84] https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-managing.html#importing-keys-delete-key-material.

[85] https://learn.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation.

[86] https://learn.microsoft.com/en-us/cli/azure/keyvault/key?view=azure-cli-latest.

[87] https://learn.microsoft.com/en-us/rest/api/keyvault/keys/operation-groups?view=rest-keyvault-keys-7.4.

[88] https://cloud.google.com/kms/docs/create-key.

[89] https://cloud.google.com/kms/docs/rotate-key#automatic.

[90] https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html.

[91] https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html.

[92] https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/.

[93] https://learn.microsoft.com/en-us/azure/dedicated-hsm.

[94] https://learn.microsoft.com/en-us/azure/payment-hsm/.

[95] https://cloud.google.com/kms/docs/ekm#supported_services.

[96] https://cloud.google.com/kms/docs/hosted-private-hsm.

[97] https://cloud.google.com/kms/docs/key-import.

[98] https://docs.aws.amazon.com/kms/latest/developerguide/keystore-cloudhsm.html.

[99] https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html.

[100] https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/hsm-protected-keys-byok.

[101] https://cloud.google.com/kms/docs/key-wrapping.

[102] https://cloud.google.com/kms/docs/formatting-keys-for-import.

[103] https://cloud.google.com/kms/docs/configuring-openssl-for-manual-key-wrapping.

[104] https://cloud.google.com/kms/docs/wrapping-a-key.

[105] https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-create-cmk.html.

[106] https://go.microsoft.com/fwlink/p/?LinkID=2162834&clcid=0x409&culture=en-us&country=us.

[107] https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf?hl=it.

[108] https://azure.microsoft.com/en-us/explore/global-infrastructure/products-by-region/?regions=all&products=all.

[109] https://www.google.com/intl/it/about/datacenters/locations/.

[110] https://aws.amazon.com/it/about-aws/global-infrastructure/.

[111] https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview#encryption-of-data-in-transit.

[112] https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-migrate-security-baseline?context=%2Fazure%2Fmigrate%2Fcontext%2Fmigrate-context.

[113] https://docs.aws.amazon.com/mgn/latest/ug/infrastructure-security.html.

[114] https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-asset-management#media-transport.

[115] https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction.

[116] https://csrc.nist.gov/pubs/sp/800/88/r1/final.

[117] https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security#data-bearing-devices.

[118] https://cloud.google.com/docs/security/deletion?hl=it#ensuring_safe_and_secure_media_sanitization.

[119] https://aws.amazon.com/it/compliance/data-center/controls/.

[120] https://go.microsoft.com/fwlink/p/?LinkID=2162834&clcid=0x409&culture=en-us&country=us.

[121] https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.

[122] https://aws.amazon.com/it/compliance/amazon-information-requests/.

[123] https://learn.microsoft.com/en-us/purview/dlp-policy-reference#data-loss-prevention-policy-reference.

[124] https://cloud.google.com/dlp/docs/inspect-sensitive-text-api.

[125] https://www.microsoft.com/en-us/securityengineering/sdl/practices.

[126] https://learn.microsoft.com/en-us/azure/security/develop/secure-dev-overview.

[127] https://learn.microsoft.com/en-us/azure/backup/backup-azure-immutable-vault-concept?tabs=recovery-services-vault.

[128] https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest.

[129] https://cloud.google.com/backup-disaster-recovery/docs/create-plan/policy-settings.

[130] https://docs.aws.amazon.com/aws-backup/latest/devguide/backup-integrity.html.

[131] https://docs.aws.amazon.com/aws-backup/latest/devguide/backup-iam.html.

[132] https://learn.microsoft.com/en-us/azure/backup/security-overview.

[133] https://learn.microsoft.com/en-us/azure/backup/backup-overview#why-use-azure-backup.

[134] https://docs.aws.amazon.com/aws-backup/latest/devguide/encryption.html.

[135] https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-network.

[136] https://learn.microsoft.com/en-us/azure/security/fundamentals/production-network.

[137] https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43837.pdf.

[138] https://learn.microsoft.com/en-us/azure/service-health/overview.

[139] https://cloud.google.com/service-health/docs/overview.

[140] https://docs.aws.amazon.com/health/latest/ug/what-is-aws-health.html.

[141] https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security#physical-security.

[142] https://cloud.google.com/docs/security/physical-to-logical-space.

[143] https://aws.amazon.com/it/compliance/data-center/controls/.

[144] https://learn.microsoft.com/en-us/compliance/assurance/assurance-sim-preparation#penetration-testing--assessment.

[145] https://cloud.google.com/docs/security/overview/whitepaper#our_dedicated_security_team.

[146] https://learn.microsoft.com/en-us/compliance/assurance/assurance-sim-detection-analysis.

[147] https://cloud.google.com/docs/security/incident-response.

[148] https://learn.microsoft.com/en-us/rest/api/azure/.

[149] https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/encrypt-data-in-transit.html.