POLITECNICO DI TORINO

Corso di Laurea Magistrale in

Ingegneria Gestionale

Tesi di Laurea Magistrale

Analisi e gestione dell'obsolescenza tecnologica:
il caso di Santander Consumer Bank

Relatore
prof. Fulvio Corno

Candidato
Martina Arino

Correlatore
Lorenzo Bulgaron

Anno Accademico 2018/19

Ringraziamenti

Prima di procedere con la trattazione del mio lavoro, tengo a ringraziare le persone che ne hanno reso possibile l'esecuzione.

In primo luogo, quindi, è necessario menzionare il relatore della mia tesi, il professor Fulvio Corno, che mi ha guidato nella stesura di questo lavoro, fornendomi suggerimenti e indicazioni preziosi.

Desidero inoltre ringraziare il correlatore, Lorenzo Bulgaron, che mi ha seguito passo passo nella stesura di questo elaborato e nel lavoro di tutti i giorni; senza il suo supporto, questo lavoro non avrebbe potuto vedere la luce.

Sarebbe impensabile non citare la mia famiglia, senza la quale tutto il mio percorso universitario non sarebbe stato possibile. Tutti, nessuno escluso, sono stati fonte inesuribile di forza e incoraggiamento durante il mio intero percorso di studi, fiduciosi che sarei riuscita a raggiungere il mio obiettivo oltre ogni ostacolo.

Infine, una dedica speciale ai miei amici, che giorno dopo giorno hanno condiviso con me gioie, sacrifici e successi. Il loro affetto e il loro sostegno rendono questo traguardo ancora più prezioso.

Indice

Ringraziamenti 2
Indice 3
Introduzione 5
CAPITOLO 1 – L'Information Technology 8
1.1 L'Information Technology nel settore finanziario 9
1.1.1 Problematiche dell'IT nel settore finanziario 12
1.2 ITIL 13
1.2.1 Concetti di base 13
CAPITOLO 2 – Gli Asset IT 17
2.1 Gli asset nel dettaglio 17
2.1.1 Hardware 18
2.1.2 Software 22
2.2 Mappatura di una rete: come si collocano gli asset nell'infrastruttura 25
2.3 Ciclo di vita di un asset IT 26
2.3.1 Fase di acquisizione 27
2.3.2 Fase di vita 28
2.3.3 Fase di dismissione 33
2.4 Evoluzione di un sistema informatico 34
2.5 Obsolescenza degli asset IT 35
2.5.1 Software versioning 37
2.5.2 Sicurezza informatica 38
CAPITOLO 3 – Gestione degli asset IT e del ciclo di vita 40
3.1 Asset Management 41
3.2 Obsolescence Management 43
3.2.1 Strategie di approccio: Proattivo vs Reattivo 45
3.2.2 Obsolescence management plan 47
3.2.3 Valutazione dell'obsolescenza 49
3.2.4 Monitoraggio dell'obsolescenza 55
3.2.5 Indicatori di performance KPI e di rischio KRI 56
3.3 Il Configuration Management 60
3.3.1 Standard ISO 62

3.4 CMDB: Configuration Management Database 64
3.4.1 Le funzionalità del CMDB per gli apparati di rete 67
3.4.2 Ruolo all'interno di un'organizzazione 72
3.5 Il CMDB nella gestione dell'obsolescenza 72
CAPITOLO 4 – Caso pratico: Santander Consumer Bank 75
4.1 Chi è Santander Consumer Bank 75
4.2 Gestione degli asset IT e dell'obsolescenza prima del CMDB 77
4.2.1 Criticità 78
4.2.2 Le risoluzioni delle criticità 80
4.2.3 Mappa di rete di Santander Consumer Bank 84
4.3 Il CMDB in Santander Consumer Bank 86
4.3.1 Motivazioni della scelta della soluzione 87
CAPITOLO 5 – Alternative possibili e soluzione scelta 94
5.1 Alternativa Alfa 94
5.2 Alternativa Beta 96
5.3 Alternativa Gamma 97
5.4 Il CMDB Alfa in Santander Consumer Bank e la relativa customizzazione 99
5.4.1 Fase 1: installazione del CMDB Alfa 100
5.4.2 Fase 2: data entry 106
5.4.3 Fase 3: personalizzazione del CMDB 108
CAPITOLO 6 – Gestione degli asset IT e dell'obsolescenza dopo il CMDB 115
6.1 Campagna Zero Tolerance 118
6.2 Gli impatti dell'approccio Zero Tolerance 124
6.3 Evidenze 128
6.4 Imprevisti 132
Conclusioni 135
Bibliografia 137
Sitografia 139

Introduzione

La presente trattazione è il frutto del lavoro svolto presso la sede centrale di Santander Consumer Bank (Torino), banca multinazionale leader mondiale del settore, e in particolare nella parte del business legata all'*Information Technology*, in qualità di consulente esterno facente capo ad Alten Italia.
Il periodo trascorso in questa finanziaria mi ha consentito di applicare praticamente le nozioni teoriche acquisite durante il percorso universitario, di lavorare su un progetto avente obiettivi definiti, in un contesto lavorativo, quello dell'*Information Technology*, in rapidissima evoluzione.
Questo incarico mi ha dato la possibilità di condividere conoscenze e competenze derivanti dal lavoro di squadra, in aggiunta a quello individuale, consentendomi di testare le mie abilità organizzative e relazionali; inoltre mi ha fornito l'opportunità di acquisirne di nuove, riguardanti la gestione dei beni aziendali e i progetti aziendali ad essi relativi.

L'obiettivo di questa tesi è la progettazione dell'inserimento di un sistema CMDB (*Configuration Management Data Base*) locale all'interno di un'impresa, nel caso specifico di una finanziaria e, in particolare, il supporto che ne consegue alla gestione dell'obsolescenza degli *asset* IT. Nella pianificazione, quindi la prima fase della vita di un progetto, vengono affrontati sia aspetti tecnologici che organizzativi.

La metodologia proposta per affrontare il problema progettuale viene applicata a un caso di studio concreto, nel quale si trattano i principali *asset* IT, sia Hardware che Software, appartenenti all'infrastruttura informatica della suddetta finanziaria. Gli *asset* IT rientranti nel perimetro considerato sono:

- Hardware:
    - Dispositivi di rete/comunicazione
        - Router
        - Switch
        - Firewall

    - Storage
    - Hypervisor
    - Server
- Software
    - Sistema operativo
    - Motori di Database
    - Web application
    - Applicativi di terze parti

La tesi è strutturata in sei capitoli.

Il primo capitolo di questo elaborato rappresenta una presentazione del mondo dell'*Information Technology* e di come questo si posiziona specificamente nel settore finanziario. Si passa poi alla spiegazione di cos'è l'ITIL e dei concetti fondamentali alla comprensione dell'elaborato.

Il secondo capitolo pone l'attenzione sugli *asset IT* e sulle relative caratteristiche. Si introduce, inoltre, il concetto di obsolescenza, essenziale al raggiungimento dell'obiettivo di questo lavoro.

Il terzo capitolo rappresenta un approfondimento di quanto presentato in precedenza. L'attenzione viene posta sulla gestione degli *asset* e della relativa obsolescenza e sugli strumenti a supporto di tali processi, in questo caso specifico del *Configuration Management Data Base*, un *repository* accurato e affidabile.

Con il quarto capitolo si riporta l'introduzione al caso aziendale di Santander Consumer Bank, in cui si descrive nella pratica tutto ciò che precedentemente era stato presentato in via esclusivamente teorica. In particolare, si pone l'attenzione sulle motivazioni che hanno portato alla scelta di un *Configuration Management Data Base* specifico.

Nel quinto capitolo vengono proposte le possibili alternative e, con una descrizione di dettaglio, la soluzione ritenuta più consona al caso di Santader Consumer Bank. Vengono, inoltre, presentate le fasi relative all'installazione, alla configurazione e all'integrazione dello strumento nell'infrastruttura informatica.

Infine, nel sesto capitolo vengono descritti gli impatti seguenti all'introduzione del *Configuration Management Data Base* e le corrispondenti evidenze, quindi su come

esso sia di supporto alla gestione degli *asset IT* e della relativa obsolescenza, tramite le funzionalità che lo caratterizzano.

Il risultato ottenuto dal lavoro svolto è stato quello desiderato: acquisizione del governo degli *asset*, consapevolezza dello stato attuale degli stessi, pianificazione delle implementazioni/sostituzioni e gestione del budget dedicato maggiormente efficienti. La diretta conseguenza risulta essere l'acquisizione di potere contrattuale nei confronti dei fornitori esterni e di una maggiore sicurezza informatica.
Come evidenza, si analizzano le modalità di gestione utilizzate dall'intermediario finanziario, nonché gli strumenti impiegati dallo stesso: indicatori di performance e le relative criticità, software di censimento e gestione degli *asset*, interfaccia utente, risvolti pratici.
Si ritiene opportuno sottolineare che le evidenze riportate all'interno di questo elaborato sono puramente indicative e i dati parzialmente distorti, dal momento che le informazioni trattate durante il periodo di collaborazione con la suddetta finanziaria sono strettamente confidenziali e rilevanti in termini di *strategical decision making*.

CAPITOLO 1 – L'Information Technology

Secondo la definizione dell'ITIL[1], di cui si parlerà in maniera più approfondita nel paragrafo successivo, l'Information Technology è:

> *l'uso di tecnologia per la memorizzazione, comunicazione o elaborazione di informazioni. La tecnologia tipicamente include computer, telecomunicazioni, Applicazioni ed altro software. Le informazioni possono includere dati aziendali, voce, immagini, video, ecc.. l'Information Technology viene spesso utilizzato per supportare processi aziendali attraverso i Servizi IT.*

Le tecnologie dell'informazione (IT) sono applicate in tutti i settori, con la funzione fondamentale di gestione di informazioni e dati critici. L'elaborazione e la trasmissione dei dati, infatti, avvengono in maniera del tutto automatica. Il fine ultimo dell'*Information Technology* è quello di essere il motore della produttività, non solo nelle imprese di servizi. Tuttavia, solo se applicato strategicamente, esso garantisce il miglioramento in termini di efficienza.
Questo ha cambiato il modo di vivere e di lavorare delle persone, dal momento che si riescono a gestire sempre più attività contemporaneamente, con aggiornamenti in tempo reale, rendendo il processo decisionale più semplice.[2]

Gli ultimi decenni hanno visto una crescita esponenziale degli sviluppi IT, con impatti estremamente rilevanti relativamente al business sul mercato: si parla di nascita e crescita di sistemi sempre più complessi, supportati dalla compresenza di

[1] L'ITIL (*Information Technology Infrastructure Library*) fornisce le linee guida, quindi le *best-practice* per i servizi IT e per i sistemi di gestione della rete, oltre all'allineamento dei processi aziendali. La versione a cui si fa riferimento è: Jan van Bon, Arjen de Jong, Axel Kolthof, Mike Pieper, Ruby Tjassing, Annelies van der Veen, Tieneke Verheijen (2007). *Foundation of IT Service Management – basato su ITIL V3*. Van Haren Publishing, Zaltbommel, www.vanharen.net. Terza edizione, prima stampa, Settembre 2007.

[2] https://www.essaytyping.com/information-technology-banking-industry/#

hardware potenti, software versatili e reti di interconnessione mondiali ultra-veloci. Grazie alle implementazioni suddette, le organizzazioni sono riuscite a sviluppare in misura sempre maggiore i propri prodotti e servizi dipendenti dai dati e dalle informazioni ed inserirli nel mercato in tempi decisamente ridotti.[3]

Nel mondo delle tecnologie dell'informazione è importante considerare che le esigenze aziendali cambiano costantemente, mentre i sistemi rimangono relativamente rigidi. Le implementazioni delle infrastrutture prevedono non solo investimenti iniziali, ma anche il sostenimento di costi in corso d'opera, al fine di garantire agli utenti un utilizzo efficace dei servizi messi a loro disposizione.[4]
In quest'ottica, l'informazione, e di conseguenza l'*Information Technology*, è un elemento sempre più rilevante dei prodotti e dei servizi organizzativi, oltre che la base dei processi aziendali. Ciò fa sì che la relazione tra le tecnologie dell'informazione e i processi organizzativi è imprescindibile: le aziende che sfruttano questo legame ottengono i migliori risultati in termini di prestazioni, generando rendimenti superiori fino al 40% rispetto ai concorrenti.[5]
L'azienda necessita di una logica organizzativa per dati, applicazioni e infrastruttura che sono gestibili in via più semplice tramite la standardizzazione dei primi, un'attività che avviene previa pianificazione e implementazione.[6]

1.1 L'Information Technology nel settore finanziario

L'*Information Technology* ritrova largo impiego anche nel settore bancario, portando numerosi vantaggi sia all'esterno dell'organizzazione, quindi ai clienti,

[3] Come nota 1, Van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., 2007.

[4] Peter Weill, Jeanne W. Ross, IT Governance: How to performers manage IT decision rights for superior results, Harvard Business Press, 6 maggio 2004, Preface, cap 1, cap 2, cap 6.

[5] Ibidem

[6] Ibidem

sia al suo interno, alla banca stessa e agli impiegati nello svolgimento delle attività quotidiane.

Per i primi, primeggia sicuramente l'acquisita autonomia nell'effettuare auto-analisi senza il supporto necessario di un impiegato addetto ai lavori: tra gli esempi lampanti ci sono la possibilità di accedere ai propri dati, effettuare transazioni, recuperare documentazione e gestire i propri conti bancari direttamente da un canale internet o da un'applicazione mobile direttamente dallo *smartphone*. Ciò che può sembrare scontato, come un prelievo di denaro a uno sportello ATM, in realtà nasconde un'infrastruttura informatica che garantisce non solo l'aggiornamento in tempo reale della situazione finanziaria del cliente, ma anche l'irrinunciabile sicurezza relativamente alla gestione dei propri risparmi e dati.

Per i secondi, quindi per l'organizzazione intera, i principali vantaggi si trovano nella contemporanea gestione di un numero di attività sempre crescenti, nell'aggiornamento immediato dei dati dei propri clienti e nella raccolta di informazioni circa il comportamento della clientela. Quest'ultimo può essere ricostruito dalla struttura informatica tramite computer, analisi della frequenza e della tipologia delle transazioni ed è alla base di molte decisioni strategiche.

Oltre che gli aspetti di *business*, è importante considerare anche quelli operativi. Esempio lampante è la generazione di report e rendiconti finanziari, di natura regolamentare, ufficiale o confidenziale, che avviene in via del tutto automatica. L'automazione ha permesso, infatti, un incremento notevole della produttività, dal momento che il personale viene liberato da mansioni meccaniche e che richiedono un impiego di tempo rilevante; basti pensare al bilanciamento automatico dei conti e del calcolo degli interessi, o anche alla stampa automatica di ricevute di deposito, estratti conto e simili. Così facendo, l'impiegato ha modo di prestare maggiore attenzione alle esigenze del cliente e dedicarsi alla risoluzione delle sue richieste.

Oltre alla produttività degli impiegati, l'automazione comporta un incremento della produttività anche nel settore, se applicata in modo strategico. Come anticipato sopra, infatti, il processo decisionale è fortemente semplificato quando le informazioni vengono elaborate automaticamente e i risultati vengono trasmessi a chi di dovere, che sia il *top-management* o il Regolatore. Un altro esempio è la

maggiore semplicità di effettuare operazioni di *marketing* utilizzando gli *smartphone* per la trasmissione di offerte o eventuali modifiche contrattuali.
Tuttavia, è necessario considerare anche quegli aspetti che devono essere oggetto di particolare attenzione nell'impiego della tecnologia nel settore finanziario. In prima linea si trova la sicurezza, messa a dura prova dagli attacchi informatici ai sistemi bancari che hanno portato, in alcuni casi, a trasferimenti di denaro attraverso reti di conti esteri che ne ha reso estremamente difficoltosa la tracciabilità.
Infine, non bisogna tralasciare che l'avvento di una struttura tecnologica sviluppata, e di conseguenza l'automazione di molte attività, ha comportato la perdita di numerosi posti di lavoro o, almeno, una trasformazione delle figure professionali necessarie alla crescita aziendale. Ciò significa che i maggiori benefici sono per la proprietà della banca e non direttamente per l'impiegato.[7]

L'*Information Technology* si può vedere da un punto di vista ancora più vicino all'utente finale. Grazie all'adozione del *mobile banking*[8], le tecnologie coinvolte nei processi informatici del settore bancario sono stati implementate al fine di soddisfare nel migliore dei modi i bisogni e le aspettative dei clienti, oltre che rendere più facile e più efficiente la modalità di condotta del *business*. In particolare, il ruolo dell'*Information Technology* all'interno del settore bancario può essere diviso in due categorie:

1. Comunicazione e connettività
2. Transazioni individuali e aziendali

L'utilizzo delle tecnologie dell'informazione avviene nei modi più disparati e spesso dati per scontati. Rientrano, infatti, i PC (*personal computer*), i dispositivi personali digitali (PDA, *personal digital device*), tablet, smartphone, sportelli automatici di prelievo (ATM, *automatic teller machine*).
Questo perché è necessario fornire ai clienti migliori servizi, considerando anche le lunghe distanze geografiche e mercati diversi.

[7] James Taylor, *Information Technology in the Banking Industry*, 22 febbraio 2018, https://www.essaytyping.com/information-technology-banking-industry/

[8] Cavus, N. & Chingoka, D., N., C. (2015). *Information technology in the banking sector: Review of mobile banking. Global Journal of Information Technology. 5(2), 62-70*

1.1.1 Problematiche dell'IT nel settore finanziario

Di seguito si riporta un elenco delle principali problematiche che possono riscontrarsi nel settore finanziario.

- Sicurezza e Rischio: i clienti possono essere vittime di truffatori. Si possono individuare i casi più disparati, da richieste di invio dei dettagli dei conti bancari, tramite *e-mail* o SMS, al furto dei dispositivi mobili di cui il cliente è proprietario e su cui sono presenti dati sensibili.

- Compatibilità: è necessario che i sistemi informatici siano compatibili con i dispositivi mobili su cui i clienti effettuano le operazioni. Per tale motivo essi possono riscontrare dei limiti nella possibilità di usufruire dei servizi, o di una parte di essi, offerti dal proprio istituto bancario.

- Costo: specialmente in mancanza della compatibilità dei dispositivi, il cliente può dover sostenere dei costi aggiuntivi per implementare la tecnologia in suo possesso o, comunque, per supportare dati e messaggi di testo. I costi devono essere sostenuti anche dall'istituto finanziario, in termini di *software*, per offrire il numero maggiore di servizi possibile.

- Scalabilità e affidabilità: gli istituti finanziari devono garantire l'accesso e le funzionalità dei propri sistemi, affinché i clienti non abbiano problemi di accesso ai servizi in ogni momento e in ogni luogo.

- Disponibilità delle applicazioni: le aspettative dei clienti sono sempre più alte e richiedono aggiornamenti costanti, nonché gli stessi vengano resi disponibili appena sviluppati. Bisogna considerare che l'aggiornamento e l'implementazione dei servizi e delle applicazioni richiede il sostentamento di costi in termini di tempo e risorse non trascurabili.

1.2 ITIL

L'ITIL (*Information Technology Infrastructure Library*) fornisce le linee guida, quindi le *best-practice* per i servizi IT e per i sistemi di gestione della rete, oltre all'allineamento dei processi aziendali.
Esso non è un manuale, né fornisce specifiche a cui bisogna conformarsi, quindi i manager di rete e di sistema adeguano le proprie infrastrutture e i propri processi secondo le indicazioni dell'ITIL.
In questa libreria, infatti, sono definiti molti elementi di gestione relativamente a: disponibilità, capacità, cambiamenti, eventi, sicurezza, livelli di servizio, conoscenze, configurazioni, e tanto altro. È fondamentale, inoltre, considerare che ogni elemento e/o processo è strettamente connesso ad almeno un altro, quindi nessuno è indipendente in assoluto. Un esempio concreto si può ritrovare nella progettazione della capacità delle risorse di rete, dove le informazioni di configurazione sulla rete o sui server sono necessarie per la creazione del modello di base della rete stessa. Pertanto, il processo di gestione della capacità richiede informazioni e dati appartenenti al processo di gestione della configurazione. Nella gestione della disponibilità, poi, si monitora lo stato corrente dei dispositivi di rete. A questo processo di monitoraggio si aggiunge la considerazione che le informazioni sugli eventi, compresi i log di sistema dei router, sono tra le fonti di dati fondamentali per comprendere gli stati dei dispositivi di rete. In generale, nei dispositivi di rete vengono generati una moltitudine di tipi di dati operativi, la cui raccolta e federazione sono le chiavi per gestire l'IT e i sistemi di rete con successo.[9]

1.2.1 Concetti di base

Prima di procedere alla descrizione degli aspetti oggetto della presente tesi, si ritiene necessario introdurre in via preventiva alcuni concetti e definizioni fondamentali alla comprensione della suddetta trattazione.

[9] Hiroshi Yamada, Takeshi Yada, Hiroto Nomura, *Developing network configuration management database system and its application—data federation for network management*, in *Springer Science+Business Media, LLC 2011*, 3 September 2011

1.2.1.1 Good practice

Come già accennato in precedenza, l'ITIL è considerato una *good practice*, che alla lettera significa "metodo corretto". Tale considerazione è valida dal momento che si tratta di un approccio che si è dimostrato un efficace supporto nella pratica per tutte quelle organizzazioni il cui fine è migliorare i propri servizi IT. L'ITIL, infatti, così come altri standard quali, ad esempio, ISO[10], IEC[11], COBIT[12] o CMMI[13], non solo è liberamente accessibile, ma è anche applicabile a una varietà di realtà, contesti e situazioni differenti.

Se tra i benefici rientra non solo l'essere liberamente accessibile, ma anche l'applicabilità a realtà, contesti e situazioni differenti, a cui si aggiunge la facilità di formazione del personale grazie alle proprie caratteristiche, bisogna considerare anche quegli aspetti che rappresentano degli svantaggi. Tra questi ultimi rientra il fatto che una *good practice* è caratterizzata dalla conoscenza esclusiva, la quale è fortemente customizzata alla realtà specifica in cui viene applicata. Tale peculiarità la rende piuttosto complicata da replicare o, addirittura, non efficace nell'utilizzo in un contesto differente.[14]

[10] ISO Sigla di *International Standards Organization*. Persegue lo sviluppo della standardizzazione, stabilendo norme comuni per la costruzione dei manufatti e per le caratteristiche qualitative delle merci, al fine di agevolare gli scambi internazionali di beni e servizi e la mutua cooperazione in campo economico, culturale, scientifico e tecnologico. Esulano dalle sue competenze solo i settori elettrico ed elettronico, che fanno capo all'IEC. http://www.treccani.it/enciclopedia/iso/

[11]IEC Sigla di *International Electrotechnical Commission*, organizzazione fondata nel 1906 per la formulazione e la diffusione di standard di validità internazionale riguardanti le tecnologie elettriche, elettroniche e quelle a esse collegate. http://www.treccani.it/enciclopedia/iec/

[12] Il *Control Objectives for Information and related Technology* (COBIT) è un modello (*framework*) per la gestione della *Information and Communication Technology* (ICT) creato nel 1992 dall'associazione americana degli auditor dei sistemi informativi (*Information Systems Audit and Control Association* - ISACA), e dal *IT Governance Institute* (ITGI). https://it.wikipedia.org/wiki/COBIT

[13] Il *Capability Maturity Model Integration* (CMMI) è un approccio al miglioramento dei processi il cui obiettivo è di aiutare un'organizzazione a migliorare le sue prestazioni. Il CMMI può essere usato per guidare il miglioramento dei processi all'interno di un progetto, una divisione o un'intera organizzazione. https://it.wikipedia.org/wiki/Capability_Maturity_Model

[14] Come nota 1. Van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., 2007. Paragrafo 2.5.

1.2.1.2 Sistemi

Secondo la definizione dell'ITIL, "un **sistema** è un gruppo di componenti interagenti, interconnessi o interdipendenti che costituiscono un insieme unificato e che operano all'unisono per uno scopo comune".[15] È la realizzazione dello scopo specifico ad essere quindi il fine ultimo della nascita del sistema.

Dal momento che ciascun sistema può essere composto da più livelli, ne devono essere delimitati i confini e soprattutto il contesto in cui opera, così da evitare equivoci nell'operatività aziendale. [16]

Infine, bisogna considerare che un sistema è coinvolto nelle interazioni con altri sistemi e con l'ambiente circostante, che però possono considerare processi e punti di vista differenti da quelli adottato nel sistema oggetto d'esame. Questo fa sì che sono necessari strumenti di collegamento e, eventualmente, di traduzione, motivo per cui vengono utilizzate interfacce, procedure predeterminate e servizi esterni. [17]

1.2.1.3 Servizio

Il Servizio viene definito dall'ITIL come "*un mezzo attraverso il quale fornire valore ai clienti facilitando il raggiungimento dei risultati che i clienti vogliono conseguire senza che se ne assumano i relativi costi o rischi*".[18]

Il valore (descritto nel paragrafo successivo) è, quindi, la diretta conseguenza dell'utilizzo del servizio.

Considerando che lo svolgimento delle attività e il raggiungimento di *performance* sono soggetti a numerosi vincoli, si ricorre ai servizi per ridurre questa influenza, così da incrementare le possibilità di raggiungere prestazioni e risultati desiderati.

---

[15] Ibidem

[16] https://sites.google.com/site/systemengineeringitaly/home/system_and_systemengineering/what-is-a-system/cosa-e-un-sistema

[17] Ibidem

[18] Come nota 1. Van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., 2007. Paragrafo 2.5.

1.2.1.4 Valore

Il valore è ciò che spinge all'utilizzo del servizio. Considerando il punto di vista del cliente, esso è costituito da due componenti[19]:

- Utilità: ciò che viene ricevuto dal cliente
- Garanzia: le modalità con cui viene fornito al cliente

[19] Ibidem

CAPITOLO 2 – Gli Asset IT

Con il termine *asset* IT si fa riferimento a un bene aziendale dell'area informatica all'interno dell'organizzazione. È considerato tale qualsiasi componente, *hardware* o *software* che consenta l'utilizzo delle risorse tecnologiche nello svolgimento delle attività operative di ogni funzione aziendale.[20]
Si tratta, quindi, di elementi chiave della strategia aziendale, dal momento che supportano i processi e le informazioni che consentono la prosecuzione della propria attività.
Un *asset IT* è pertanto un qualsiasi elemento che l'organizzazione impiega e di cui può esserne proprietario o semplice fruitore, questo perché il termine include anche i *software* di terze parti e i *software* intesi come servizi.[21] In entrambi i casi si è interessati ad acquisire informazioni circa il relativo ciclo di vita, descritto più avanti.

2.1 Gli asset nel dettaglio

Parlando di *asset IT*, si ritiene necessario fornire un elenco e una breve descrizione almeno di quelli rientranti nel perimetro ristretto di questo lavoro.

Prima di procedere alla descrizione di ognuno, è opportuno andare a definire il concetto di *Configuration Item* (CI, Elemento della configurazione)[22]:

[20] http://www.rfc.it/applicativi/asset-aziendale

[21] Emanuele Gianturco, L'*asset management* e i sistemi automatici, 15 ottobre 2007, https://www.pmi.it/tecnologia/software-e-web/articolo/1542/lasset-management-e-i-sistemi-automatici.html

[22] Jan van Bon, Arjen de Jong, Axel Kolthof, Mike Pieper, Ruby Tjassing, Annelies van der Veen, Tieneke Verheijen (2007). *Foundation of IT Service Management – basato su ITIL V3*. Van Haren Publishing, Zaltbommel, www.vanharen.net. Terza edizione, prima stampa, Settembre 2007.

> *Qualsiasi componente che necessita di essere gestito per poter erogare un servizio IT. Le informazioni su ogni CI vengono registrate in un Configuration Record[23] all'interno del Configuration Management System[24] ed aggiornate per tutto il suo ciclo di vita[25] dal Configuration Management[26]. Tipicamente fra i CI includiamo i servizi IT, hardware, software, edifici, persone, e documentazione formale quale la documentazione del processo e di SLA[27].*

Gli *asset IT* analizzati possono essere suddivisi come riportato di seguito.

2.1.1 Hardware

Quando si parla di *hardware* ci si riferisce alla parte fisica di un computer. Questo significa che si fa riferimento a tutte le componenti che permettono il funzionamento della macchina, quindi le parti elettroniche, elettriche, meccaniche, magnetiche e ottiche.[28] Quando si parla di componenti fisici di un sistema, si considerano inclusi i dati e la documentazione associati[29].

Oltre all'accezione di periferica, si fa riferimento anche a quelle componenti che vanno a formare una struttura di rete. Esempi sono gli apparati di rete, cablaggi e dispositivi.

---

[23] Un *configuration record* è la registrazione di tutti i dettagli di un CI e documenta il relativo Ciclo di Vita.

[24] Un *Configuration Management System* (CMS) è un insieme di strumenti e *database* che semplificano la gestione dei dati di configurazione di ogni CI, includendo qualsiasi tipo di informazione ad esso relativo. Si tratta di uno strumento utilizzato da tutti i processi di gestione dei servizi IT.

[25] Il Ciclo di vita riguarda le varie fasi nella vita di un *asset IT*. Questo argomento verrà approfondito nei paragrafi seguenti.

[26] Il *Configuration Management* è processo responsabile dei CI, delle loro informazioni e soprattutto delle relazioni ad essi relativi. Verrà ampiamente trattato nel capitolo successivo.

[27] SLA, *Service Level Agreement*, Accordo sui livelli di servizio. Si tratta di un accordo tra il fornitore del servizio IT e il cliente. Serve a descrivere il servizio fornito, documentare gli obiettivi dei livelli di servizio e il loro raggiungimento, specificare le responsabilità dei due attori in gioco.

[28] https://it.wikipedia.org/wiki/Hardware

[29] IEC 62402:2007

2.1.1.1 Dispositivi di rete/comunicazione

Si tratta degli elementi informatici che consentono lo scambio di pacchetti[30] tra i sistemi, secondo regole predefinite.

I principali dispositivi sono:

- *Switch*

  Uno *switch* è l'elemento informatico che consente il collegamento tra i dispositivi all'interno di una rete di computer. Tale collegamento avviene mediante la presenza di cavi di rete fisici. Il ruolo dello *switch* all'interno della rete è quello di gestire il flusso di dati, stabilendo le regole di ricezione e destinazione dei pacchetti dati. Tale operazione è semplificata dalla presenza dell'indirizzo MAC[31], che identifica univocamente ogni dispositivo presente sulla rete, ottimizzando così la sicurezza e l'efficienza della stessa.[32]

- *Firewall*

  Un *firewall* è un elemento necessario alla sicurezza informatica. Il suo scopo è fare da filtro al traffico scambiato tra il sistema e l'esterno, controllando quindi gli accessi alle risorse del sistema stesso, sulla base di un insieme di regole prestabilite nelle *policy* aziendali. Il sistema può essere individuato da un singolo computer o da una rete interna[33], che si suppone sia sicura e affidabile. L'ambiente esterno[34], invece, è considerato sconosciuto, insicuro e inaffidabile.[35]

[30] Un pacchetto di dati indica ciascuna sequenza finita e distinta di dati trasmessa su una rete.

[31] MAC *address, Media Access Control*, è un identificativo assegnato dal produttore in modo univoco a ogni singola scheda di rete prodotta.

[32] https://it.wikipedia.org/wiki/Switch

[33] Per rete interna o locale o privata si intende una rete costituita da una moltitudine di computer.

[34] Parallelamente alla rete interna, l'ambiente esterno viene spesso definito anche rete esterna o pubblica.

[35] https://it.wikipedia.org/wiki/Firewall

- *Router*

  Un *router* è un dispositivo elettronico che, in una rete informatica, si occupa di instradare i dati, suddivisi in pacchetti, fra reti diverse.

  L'instradamento può avvenire verso reti direttamente connesse, su interfacce fisiche distinte, oppure verso altre sottoreti non limitrofe che, grazie alle informazioni contenute nelle tabelle di instradamento, siano raggiungibili attraverso altri nodi della rete.

  Esso può essere visto dunque come un dispositivo di interfacciamento tra diverse sottoreti eterogenee e non, permettendone la interoperabilità a livello di indirizzamento.

2.1.1.2 Storage

Gli *storage* sono quei dispositivi *hardware* che consentono la memorizzazione non volatile[36] dei dati. Il loro ruolo nell'infrastruttura è quindi essere da supporto alla memorizzazione e ai *software* dedicati alla stessa.

Lo scopo, quindi, è quello di immagazzinare i dati mantenendoli inalterati per un considerevole lasso di tempo.

2.1.1.3 Hypervisor

Un *hypervisor*, definito anche come *monitor* di macchine virtuali[37] (VMM, *Virtual Machine Monitor*), è un *software*, *firmware*[38] o *hardware* che crea ed esegue macchine virtuali.

Il computer su cui viene eseguita quest'ultima operazione viene definita macchina *host*, mentre ogni macchina virtuale è chiamata *guest machine*.

---

[36] La memoria non volatile è quella che mantiene le informazioni anche quando non viene alimentata da energia elettrica. Si differenzia da quella volatile, tipicamente la RAM (*Random Access Memory*), che necessita invece dell'alimentazione per la conservazione dei dati.

[37] Una macchina virtuale è un *software* che crea un ambiente virtuale che imita il comportamento tipico di una macchina fisica, tramite l'assegnazione di risorse *hardware* condivise, quindi RAM, CPU e spazio disco.

[38] Insieme delle istruzioni e delle applicazioni presenti permanentemente nella memoria di un sistema e che non possono essere modificate dall'utente.

L'*hypervisor* presenta una piattaforma operativa virtuale ai sistemi operativi, gestendone l'esecuzione.
In esso, inoltre, vengono eseguite più istanze delle tipologie di sistemi operativi più disparati (tra i più utilizzati ci sono le istanze Windows®, Linux® e macOS®), i quali condividono le risorse *hardware* virtualizzate.

2.1.1.4 Server e Client

Un *server* è un elemento informatico che fornisce un servizio ad altre componenti, in genere definite *client*. Si tratta di due attori in gioco, il *server* e il *client*, strettamente correlati tra loro: non c'è l'uno senza l'altro e insieme vanno a definire l'architettura logica di rete a livello applicativo, denominata appunto *client-server*.
La fornitura del servizio avviene sia a livello logico che fisico ed è successiva a una richiesta effettuata dalle componenti *client*. Quest'ultima può essere realizzata secondo varie modalità: tramite una rete di computer, all'interno di un sistema informatico o localmente sul computer.
Il server può essere sia *software* che *hardware*, a seconda dei servizi e delle funzionalità offerti agli altri elementi informatici. Parallelamente, anche il *client* può esistere in entrambe le tipologie.
A seconda dell'ambito in cui si sta operando, quindi, con il termine *server* si può fare riferimento a:

- Un computer nell'accezione comune del termine, adoperato per la fornitura di servizi ad altri computer, tralasciando le caratteristiche fisiche;

- Un computer particolare, dotato di alta affidabilità, prestazioni superiori e funzionalità aggiuntive rispetto alla media di mercato;

- Un programma in esecuzione, quindi un processo, che provveda alla fornitura di servizi ad altri processi. Esempio classico è il *Web Server*.

Si potrebbe, quindi, semplificare il discorso considerando:

- *Server* il componente che eroga, tramite un software specifico per ogni caso, un servizio;

- *Client* il componente che fa richiesta del servizio, tramite l'utente finale.

È importante sottolineare come non ci si riferisca a un componente *hardware* specificatamente dal momento che è sempre più utilizzata la virtualizzazione delle macchine.

2.1.2 Software

Con il termine *software* si fa riferimento a programmi, procedure, regole, dati e documentazione associati con aspetti programmabili dei sistemi *hardware* e dell'infrastruttura.[39]

Il *software* è definito come l'insieme di tutti gli elementi logici, che ovviamente non siano *hardware*, necessari per la fornitura di un servizio o di una funzione aziendale. La definizione di *software* generalmente include i seguenti elementi: programmi, moduli di interfaccia, modelli di dati (comprese le informazioni necessarie per garantire la consistenza dei dati e degli indici o delle chiavi di accesso) e i parametri operativi dell'applicazione.

2.1.2.1 Sistema operativo

Si parla di sistema operativo quando si parla di una collezione di programmi che:

- permettono lo svolgimento delle operazioni fondamentali di un computer

- inizializzano il sistema

- assicurano il corretto funzionamento della macchina.

[39] IEC 62402:2007

Per l'esecuzione di qualsiasi altro *software*, quindi, è necessario installare prima il sistema operativo nella memoria del computer (ovviamente si fa riferimento a quella non volatile).
Inoltre, esso svolge numerose funzioni, gestisce le risorse (memoria e processore) nonché le periferiche del computer e l'interfaccia utente, provvede all'esecuzione di *software* e, infine, regola l'accesso alle risorse del computer da diversi utenti e/o programmi.

2.1.2.2 Database

Con il termine *database* (DB) si fa riferimento a un archivio di dati organizzato e sviluppato per agire in tre modi sulle informazioni:

- Memorizzazione
- Recupero e interrogazione efficiente
- Manipolazione ed elaborazione

Parlare di *database*, implica automaticamente il parlare di *Database Management System* (DBMS), nel quale vengono inserite tutte le applicazioni che consentono di soddisfare i compiti richiesti a un *database*.
Il ruolo di un DBMS comprende anche azioni dal punto di vista della sicurezza informatica. Esso infatti provvede alla protezione e al controllo dell'integrità dei dati, la cui condivisione e conservazione è consentita agli utenti finali o ai programmatori delle varie applicazioni.
Tra i *Database Management System* maggiormente utilizzati, sia dall'utente privato che di business, ci sono: Access, MySQL, Oracle e DB2. Le differenze tra questi ultimi sono relativo al linguaggio di programmazione utilizzato nella compilazione del codice.

Fondamentale per un *database* è l'essere progettato razionalmente ed efficientemente, così da rendere maggiormente significativi i dati registrati in esso. Se la base di dati, infatti, è ottimizzata e semplificata, è più semplice sfruttare degli strumenti esterni alla stessa per estrarre ed analizzare le informazioni archiviate. I *tool* a cui si fa riferimento sono quelli che consentono la attività di *reporting*, *intelligence* o ETL (*Extract Transfrom Load*)[40]. Quest'ultimo processo, in particolare, oltre a estrarre i dati da più fonti e renderli disponibili, li ripulisce al fine di renderli conformi alle elaborazioni per il *business*, facendo sì che essi possano essere integrati anche tra più sistemi, tra di loro eterogenei.

2.1.2.3 Web application server

Un *web server* è un'applicazione *software*, installata e in esecuzione su un computer, un *server* per l'appunto, che elabora le richieste di trasferimento di una pagina web, che provengono da un *client* identificato in un *web browser*[41], e genera contenuti in maniera dinamica.
Tra i più diffusi, rientrano sicuramente:

- Apache http Server, sviluppato da Apache Software Foundation®
- IIS, sviluppato da Microsoft®

2.1.2.4 Applicativi di terze parti

Gli applicativi di terze parti sono tutti quei *software* che fungono da servizi elaborati dai server. La caratteristica essenziale, dal punto di vista dell'azienda, è che vengono sviluppati all'esterno dell'organizzazione, quindi quest'ultima non è in possesso del codice. Questi applicativi vengono eseguiti dalle macchine su cui vengono installate senza essere di proprietà del Sistema Operativo.

[40] ETL, Extract Transform Load, indica un processo che estrae, elabora e carica i dati da una moltitudine di sorgenti, ma la cui organizzazione è centralizzata in un unico archivio dati.

[41] Un *web browser* è un applicativo che consente la navigazione di risorse sul web.

2.2 Mappatura di una rete: come si collocano gli asset nell'infrastruttura

Tramite la mappa di rete si può vedere come gli *asset*, nel dettaglio l'*hardware*, siano collegati tra loro. Tuttavia, il loro funzionamento, le loro relazioni e le relative configurazioni avvengono tramite i *software*.

I dispositivi di rete sono necessari, così come gli altri, per giustificare l'inventario e le relazioni esistenti.

Un esempio di rete può essere quello presentato in Figura 1, in cui sono visibili i collegamenti tra gli apparati e la divisione tra ambiente esterno e rete interna all'organizzazione.

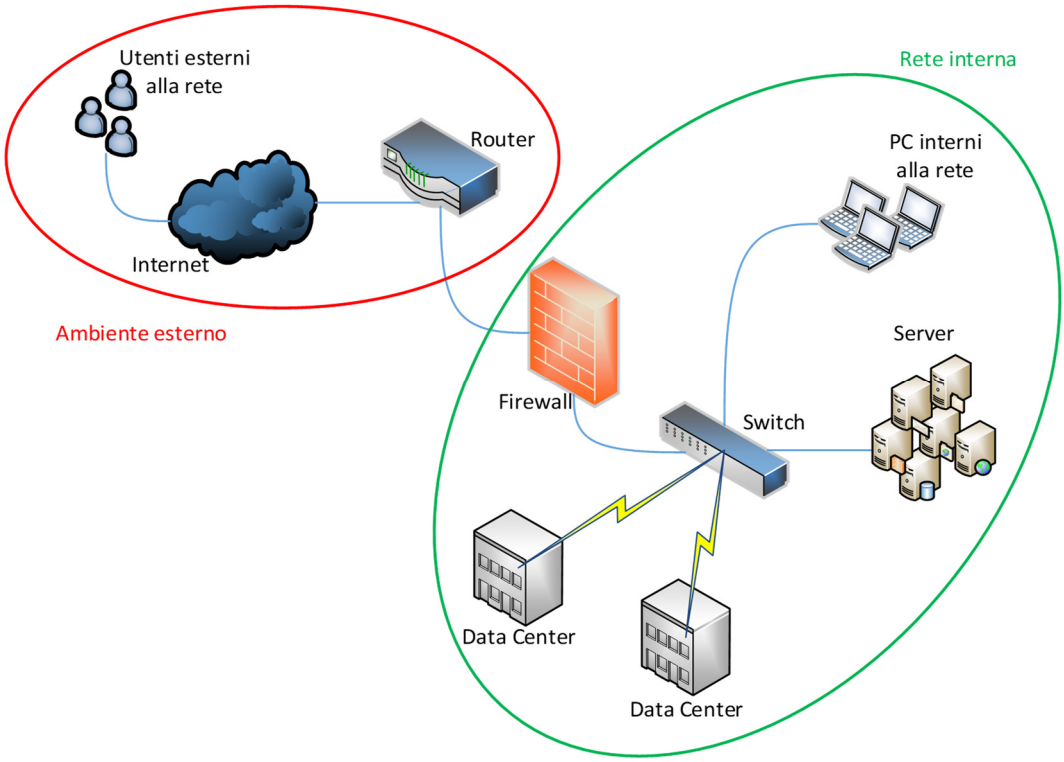

Figura 1 - Esempio di una mappatura di rete

2.3 Ciclo di vita di un asset IT

Con "ciclo di vita" si intende l'insieme delle varie fasi nella vita di un qualsiasi prodotto, servizio o elemento IT. Come indicato dall'ITIL[42], "*il ciclo di vita definisce le Categorie per lo Stato e le transizioni di Stato che sono consentite*".
Con Categoria si indica un insieme di elementi che hanno qualcosa in comune[43].
Con Stato, invece, si fa riferimento alla fase del ciclo di vita in cui versa in un dato momento l'elemento a cui si sta facendo riferimento. Si tratta di un attributo abituale nella descrizione delle caratteristiche di un prodotto o servizio e, infatti, si trova generalmente nelle varie registrazioni o documentazioni ad esso relativi[44].
Il ciclo di vita è, quindi, il periodo che va dalla fase iniziale di progettazione fino a quella di dismissione del componente in esame. A seconda della tipologia di quest'ultimo, tale periodo può avere durata variabile.

[42] Come nota 1, Van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., 2007

[43] Ibidem

[44] Ibidem

Le tre macrofasi che lo caratterizzano, infatti, sono illustrate nella Figura 2.

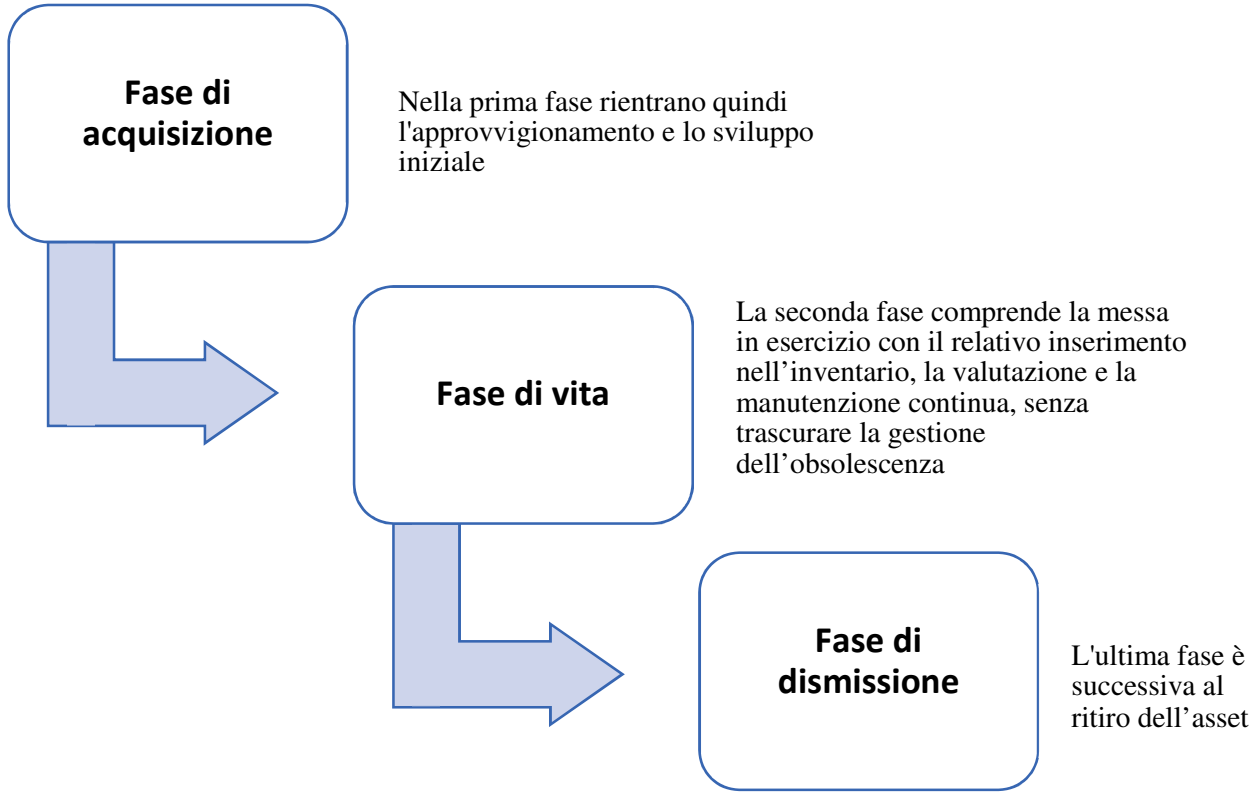

Figura 2 - Fasi del ciclo di vita di un asset IT

Queste fasi sono comuni sia ai dispositivi *hardware* che ai *software*. Le differenze si ritrovano nelle modalità di applicazione, ma nella sostanza sono le medesime.

2.3.1 Fase di acquisizione

La fase di acquisizione è la prima fase del ciclo di vita di un *asset IT*.

Essa comprende varie attività[45]:

- Valutazione delle esigenze di *business*
- Prospetto d'acquisto e valutazione delle alternative

[45] Come nota 24, Gianturco, E., 2007

- Ordine degli elementi necessari all'impostazione dell'infrastruttura

È in questa prima fase che quindi vengono effettuate tutte le valutazioni tecnologiche. In particolare, si valuta:

- La gestione del ciclo di vita dell'*asset* in esame integrato alla progettazione dell'infrastruttura desiderata

- La compatibilità con i sistemi esistenti e con eventuali predecessori

- La garanzia che la tecnologia soddisfi tutte le esigenze richieste

2.3.2 Fase di vita

La fase di vita di un *asset* IT è sicuramente quella che dura maggiormente, andando dalla scelta della tecnologia fino alla sua dismissione.
Essa comprende tre sotto-fasi, profondamente correlate tra loro:

- Redazione degli inventari

- Valutazione e manutenzione

- Gestione dell'obsolescenza

Non appena l'*asset* viene acquisito dall'organizzazione, esso deve essere censito all'interno degli inventari dall'azienda, che si richiede siano continuamente aggiornati.

Il mantenimento appropriato degli inventari dei vari *asset IT* è un processo chiave per ottenere una fotografia completa e aggiornata dei sistemi tecnologici, ma anche per garantire il *Business Continuity Plan* (BCP)[46] e garantire la sicurezza e la

[46] Il *Business Continuity Plan*, BCP, Piano di Continuità operativa, è un piano necessario a garantire la continuità operativa dei processi aziendali in caso di emergenza o disastro. Tali eventi possono includere qualsiasi situazione di condizioni non normali e in cui viene compressa l'operatività

disponibilità delle informazioni. Parallelamente, è necessario considerare che tutti gli *asset* identificati come critici dalla BIA (*Business Impact Analysis*)[47] devono necessariamente avere un piano di emergenza e recupero, definito nel dettaglio e, soprattutto, coerentemente a quando considerato nel TOCP (*Technology and Operational Contingency Plan*)[48].

Il censimento degli *asset*, in particolare, deve rispettare alcune direttive, che ne semplificano l'identificazione e la risoluzione in caso di problematiche pervenute. Tali disposizioni sono customizzate per ogni organizzazione, ma le linee guida sono le seguenti:

- Tutti gli *asset* devono essere inventariati in modo univoco e inequivocabile e le relative informazioni devono essere accessibili attraversi due tipologie di inventario:
    - Un inventario interno, gestito completamente dall'organizzazione
    - Un inventario di terze parti, per i servizi in *outsourcing*[49]

- Tutti gli *asset*, sia *hardware* che *software*, devono essere inventariati per garantire la facilità nella localizzazione, l'identificabilità e l'accessibilità alle proprie informazioni, grazie all'utilizzo dei modelli e dei *tool*[50] a disposizione dell'azienda

aziendale. Nel piano sono quindi considerati vari casi eccezionali che potrebbero verificarsi nella realtà.https://www.techopedia.com/definition/3/business-continuity-plan-bcp

[47] La BIA, *Business Impact Analysis*, è un processo sistematico che consente di determinare e valutare i potenziali effetti di un'interruzione di operazioni critiche al *business*, in caso di disastro, incidente o emergenza.

[48] Il TOCP, *Technology and Operational Contingency Plan*, è una procedura che prevede una sequenza di azioni volte alla ripartenza di tutti i servizi informativi dell'organizzazione. Essa da le indicazioni su come far ripartire l'operatività, specialmente quando sono coinvolti applicativi critici, in caso disastro o emergenza. Esso rappresenta una componente del BCP, già definito in precedenza.

[49] Per i servizi in *outsourcing* si intendono quei servizi esternalizzati, quindi affidati a terze parti, esterne all'organizzazione

[50] I *tool* sono gli strumenti utilizzabili nell'organizzazione tramite *software* o applicativi

- Tutti gli *asset* devono possedere almeno un *Owner* identificato chiaramente, che abbia la responsabilità finale dell'*asset* e un *Administrator*, anch'esso identificato chiaramente, che ne sia invece il responsabile della gestione tecnica (parametrizzazione, configurazione, ecc..), compresa la sicurezza. A causa della molteplicità di tipologie possibili di *asset*, è possibile identificare dei *Co-owner*, in particolare nel caso in cui si tratti di sistemi complessi; questi soggetti possono essere individuati sia in persone singole che in gruppi o funzioni dell'organizzazione. È a questi attori che viene affidato il processo di messa in esercizio dell'*asset* in esame. Nella pratica, bisogna distinguere il caso in cui si tratti di *hardware* o *software*:

    - Nel caso in cui si tratti di *hardware*, la messa in esercizio prevede il prelievo dal magazzino, dove è stato stoccato dall'arrivo in azienda, seguita dall'installazione fisica nella sede a cui è destinato, non appena terminata la configurazione. Quest'ultima deve essere conforme alle *policy* aziendali, in particolare nel rispetto della sicurezza informatica, e soddisfare i requisiti tecnici e tecnologici richiesti dal *business*.

    - Nel caso in cui si tratti di *software*, invece, il processo di messa in esercizio prevede il passaggio dagli ambienti di test/sviluppo, a quelli di collaudo, per poi concludersi con il rilascio in produzione. In particolare, è nella prima transizione che vengono testate le funzionalità del *software* e dei servizi; l'ambiente di collaudo, infatti, emula quasi perfettamente quello di produzione, per cui si ha la garanzia che, una volta rilasciato in produzione, non si abbiano problematiche di tipo sistemistico o di trasmissione dei dati.

È nelle operazioni di configurazione che vengono registrati i dettagli che identificano univocamente ogni *asset* all'interno dell'infrastruttura.[51]

- La responsabilità della gestione degli inventari, e quindi anche del loro aggiornamento, plausibilmente annuale, rientra nelle attività assegnate al CIO (*Chief Information Officier*), il *manager* responsabile della funzione aziendale delle tecnologie dell'informazione e della comunicazione. Egli deve, inoltre, garantire la disponibilità degli stessi, nonché la relativa facilità di accesso

- Tutti gli *asset* devono essere inventariati secondo delle classificazioni appropriate che vanno a considerare i rischi associati e le priorità. Gli aspetti che devono essere considerati sono:
    - Livello di criticità del processo aziendale che supporta e i criteri di disponibilità richiesti
    - Livello di criticità dell'*asset* secondo i requisiti di riservatezza[52], integrità[53] e disponibilità[54] dei dati supportati
    - Il piano di emergenza richiesto per l'attività, in linea con i vari scenari di contingenza

- Fondamentale è avere un efficiente sistema di controllo della versione degli *asset*, al fine di garantirne la consistenza e l'accuratezza. Le informazioni, coerentemente a quanto avviene per l'*asset*, devono essere registrate negli appositi inventari al fine di consentirne una chiara

[51] Come nota 2

[52] La riservatezza informatica è la gestione della sicurezza in modo tale da mitigare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata e ovviamente data privacy.

[53] Con il termine integrità dei dati si intende la garanzia che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.

[54] Per disponibilità dei dati si intende la salvaguardia del patrimonio informativo nella garanzia di accesso, l'usabilità e la confidenzialità dei dati. Da un punto di vista di gestione della sicurezza significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.).

identificazione, comprensiva di dati relativi al produttore e/o al fornitore, nonché l'EOS (*End of support*)[55] e l'EOL (*End of Life*)[56].

- Tutti gli *asset IT* devono essere sottoposti a una valutazione periodica, al fine di identificare tempestivamente criticità e garantire il soddisfacimento delle richieste ed esigenze del *business*, dell'audit e degli enti regolamentari. È nella fase di esercizio, infatti, che avvengono le cosiddette *Change Request*[57] , che comportano delle modifiche nello stato della macchina.[58] I casi che richiedono aggiornamenti o dismissioni devono essere trattati secondo processi specifici (trattati nel paragrafo successivo).

- È necessario un sistema di tracciamento di tutte le relazioni esistenti tra gli *asset*, *hardware* e *software*, nonché le relative dipendenze, al fine di ottenere tutte le informazioni che supportino la comprensione della catena delle relazioni, oltre che l'impatto di una modifica nel sistema può comportare. Tale esigenza viene soddisfatta con l''introduzione di un *Configuration Management Data Base*, CMDB[59], all'interno dell'organizzazione.

[55] L'EOS, *End of Support*, indica il termine del supporto e della manutenzione fornito dal produttore dell'asset in esame. In genere, il termine del supporto manutentivo di una versione coincide con il rilascio di nuove versioni dello stesso prodotto.

[56] L'EOL, *End of Life*, indica che il bene in esame è al termine della sua vita utile e che il fornitore interrompe da quel momento la produzione e, di conseguenza, la commercializzazione dello stesso.

[57] La *Change Request*, richiesta di modifica, è un documento in cui si richiede l'adeguamento di un sistema presente nell'infrastruttura. È fondamentale nel processo di gestione del cambiamento e del progresso tecnologico. Si tratta di una richiesta di modifica dichiarativa, in cui viene indicato ciò che si desidera sia realizzato, ma escludendo le modalità con cui deve avvenire tale modifica.

[58] Come nota 2

[59] CMDB, *Configuration Management Data Base*, è un archivio di informazioni relative agli *asset IT*. Se ne tratterà ampliamente nei capitol successive.

2.3.3 Fase di dismissione

La fase di dismissione è l'ultima del ciclo di vita di un *asset IT* e, generalmente, avviene quando il componente preso in esame risulta essere obsoleto[60], quindi in *End of Life* o, almeno, in *End of Support*, sulla base delle informazioni registrate all'interno degli archivi. In alternativa, la dismissione può avvenire anche perché l'elemento informatico risulta essere danneggiato o non funzionante.

Quest'ultima fase prevede essenzialmente due possibilità: il ritiro e la dismissione vera e propria.[61]

Anche in questo caso bisogna scindere i casi in cui si tratta di dismissione di *hardware* da quelli di *software*.

- Nel caso in cui la dismissione sia relativa ad una macchina fisica, le due alternative sono caratterizzate come di seguito:
  - Il ritiro prevede un ritorno in magazzino, mantenendo quindi la possibilità di una nuova messa in esercizio;
  - La dismissione prevede l'eliminazione dal parco macchine dell'*asset*, seguita dalla rottamazione con cancellazione di eventuali dati memorizzati, che può avvenire a carico dell'organizzazione stessa o del fornitore.

- Nel caso di dismissione di un software, invece, le possibilità diventano:
  - Il ritiro prevede l'interruzione del servizio, prevedendo quindi l'opportunità di riattivazione;
  - La dismissione prevede la disinstallazione dei servizi considerati e la successiva eliminazione dal sistema.

[60] Per la definizione di obsolescenza si rimanda al paragrafo successivo, in cui l'argomento viene ampliamente esplicato.

[61] Come nota 2

2.4 Evoluzione di un sistema informatico

Prima di approfondire il concetto di obsolescenza, nel paragrafo seguente, e la gestione degli *asset* e del loro ciclo di vita, nel capitolo successivo, si ritiene opportuno descrivere cosa si intende con evoluzione di un sistema informatico. Come si può notare dalla Figura 3, si possono definire quindi quattro modalità: l'*update* (*patching*[62]), l'*upgrade*, la *migrate* e il *replace*.[63]

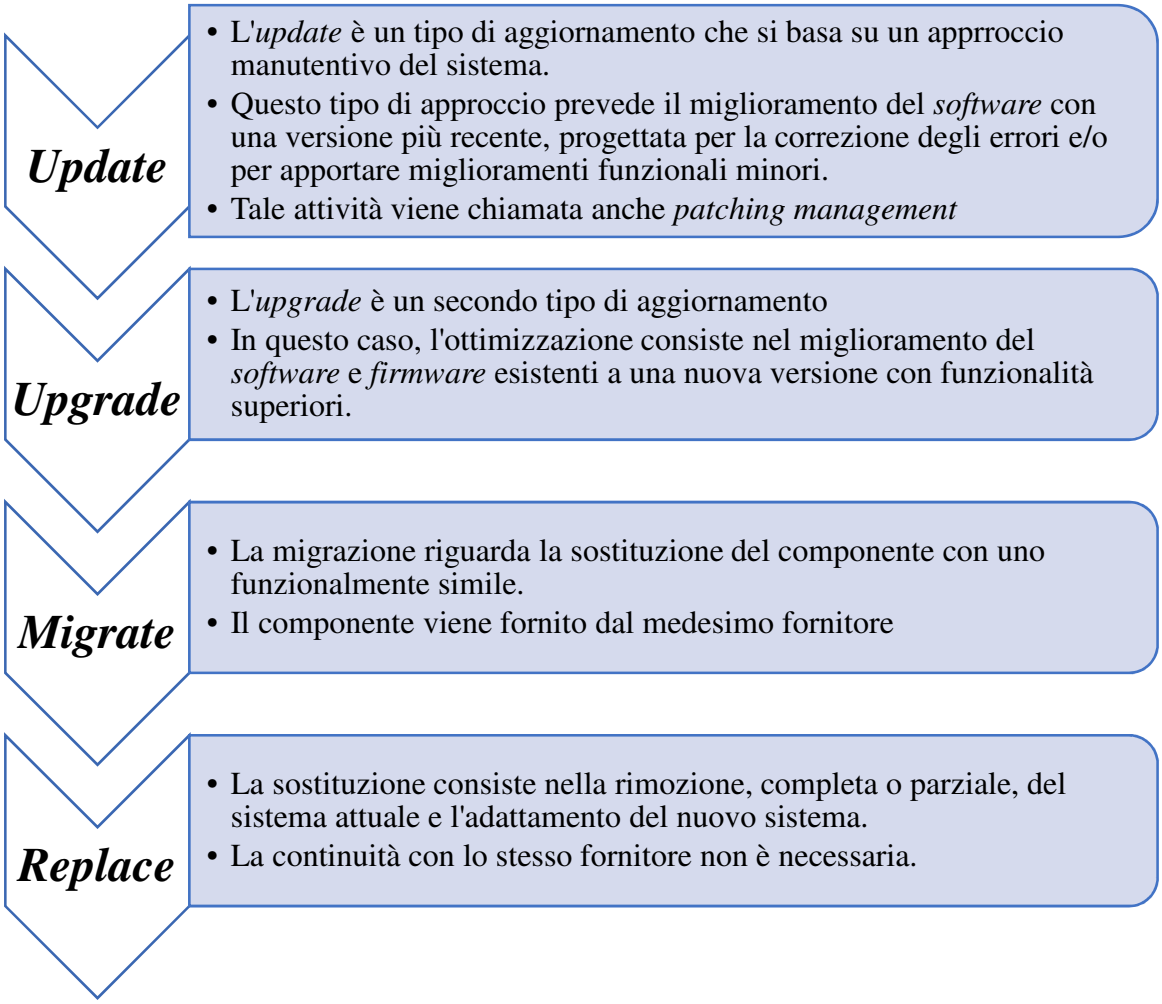

Figura 3 - Evoluzione di un sistema informatico

[62] Con il termine *patching* si indicano degli aggiornamenti del sistema, volti al miglioramento di un programma o alla risoluzione di vulnerabilità di sicurezza e di altri *bug*. Verrà maggiormente trattato nel paragrafo successivo.

[63] IOGP, *Obsolescence and life cycle management for automation system. Recommended practice.*, July 2016, Report 551

2.5 Obsolescenza degli asset IT

Secondo la definizione del vocabolario della lingua italiana, la definizione di obsolescenza è la seguente:

> ***obsolescènza*** *s. f. [der. del lat. obsolescĕre; v. obsoleto]. – In genere, invecchiamento, superamento (di istituzioni, strutture, manufatti e sim.); più specificamente, la perdita di efficienza e di valore economico subiti da un apparecchio, da un impianto, da una tecnologia a causa del progresso tecnologico, ossia dell'immissione sul mercato di nuovi macchinarî che, producendo a costi più bassi, rendono non più competitivi quelli esistenti. Il termine è usato anche con riferimento a beni di consumo (per es., automobili, elettrodomestici o calcolatori) di cui vengono presentati nuove forme o perfezionamenti che inducono ad abbandonare il vecchio modello.*[64]

In presenza di una domanda sempre crescente relativamente all'estensione della vita degli *asset* operativi, il rischio di obsolescenza ha acquisito un'importanza sempre maggiore. L'impatto principale di una tecnologia obsoleta viene percepito nel momento in cui quest'ultima non è più in grado di soddisfare le prestazioni richieste o, ancora di più, quando essa si guasta e non si è più in grado di supportarla, manutenerla o ripararla, a causa dell'indisponibilità delle componenti necessarie.
Una strategia solida di gestione dell'obsolescenza, ossia le attività coordinate per governare l'organizzazione relativamente a quest'ultima[65], deve basarsi su tre azioni principali:

- Prevenire
- Prevedere
- Risolvere

[64] http://www.treccani.it/vocabolario/obsolescenza/

[65] IEC 62402:2007, Obsolescence management – Application guide

Queste tre attività consentono infatti di mitigare i rischi, i costi e gli impatti sulle attività di *business* legati all'obsolescenza di un qualsiasi elemento tecnologico coinvolto nei processi operativi aziendali.
È fondamentale, quindi, ricorrere a un controllo costante dello stato degli *asset* e dei rispettivi cicli di vita, al fine di conservare l'integrità, la disponibilità e costi contenuti dell'infrastruttura informatica. Esempi di *best-practice* che possono essere messe in atto per raggiungere questo scopo sono:

- Introdurre di un processo di una gestione proattiva del ciclo di vita degli *asset*[66];

- Ottimizzare i costi relativi al ciclo di vita, considerando il *Return on investment*, ROI, della tecnologia di riferimento;

- Individuare lo stato degli *asset*, quali hanno un ciclo di vita breve, o comunque quali sono più prossimi alla fase terminale di quest'ultimo, e valutare le alternative che portano alla risoluzione delle problematiche riscontrate;

- Definire delle politiche di interazione con il fornitore al fine di prolungare il supporto alle tecnologie adottate;

- Considerare la compatibilità tra versioni e/o generazioni differenti della stessa tipologia di prodotto;

- Identificare i tempi di utilizzo di determinate componenti all'interno dell'infrastruttura.

[66] Una strategia proattiva è quella che sviluppa e identifica un piano di gestione dell'obsolescenza in anticipo. Si differenzia dalla strategia reattiva che, invece, sviluppa e implementa le soluzioni relativamente all'obsolescenza nel momento in cui le problematiche ad essa relativa si manifestano durante l'attività aziendale. IEC 62402:2007

2.5.1 Software versioning

Avendo illustrato, nel paragrafo precedente, le possibili azioni correttive in caso di funzionalità e sicurezza non aggiornate, si ritiene opportuno dettagliare il concetto di *versioning*, dal momento che le attività di aggiornamento, migrazione e sostituzione sono essenzialmente per combattere l'obsolescenza e rendere i sistemi conformi alle esigenze di *business* e *cyber security*.

Con *versioning* si intende l'esistenza di varie versioni dello stesso *software*, considerando che ognuna è l'implementazione in termini di prestazioni e sicurezza di quella precedente.

Nel dettaglio, l'aggiornamento della versione del *software* è il processo di assegnazione di nomi o numero a uno stato univoco del *software*. In genere l'assegnazione dei numeri avviene in maniera crescente e corrisponde alle implementazioni e ai nuovi sviluppi del *software*.

Parlare di *versioning* ha come diretta conseguenza l'introduzione del concetto di *patching*, che sta a indicare gli aggiornamenti del sistema, volti al miglioramento di un programma o alla risoluzione di vulnerabilità di sicurezza e di altri *bug*.

Le *patch* possono essere di tre tipologie:

- *Patch* di sicurezza: tale aggiornamento ha come scopo la risoluzione di vulnerabilità, andando a effettuare delle correzioni all'interno del *software* stesso. Tendenzialmente, la pubblicazione e, quindi, i rilasci avvengono mensilmente da parte degli sviluppatori.

- *Patch* non ufficiali: lo scopo è simile a quello delle *patch* ufficiali, ma viene rilasciata da terze parti e non dal produttore stesso. Vengono principalmente sviluppate per migliorare la compatibilità dei sistemi, nei casi in cui quelle ufficiali si attardano ad esser rilasciate.

- *Hot patching*: si tratta di un sistema di *patching* che consente l'aggiornamento senza dover riavviare necessariamente il sistema. Generalmente viene applicata ai *software* di servizi che non possono assolutamente essere interrotti.

Sufficientemente chiarificatore può essere prendere ad esempio gli aggiornamenti e le versioni software rilasciate da Microsoft®. Si riportano in Figura 4 le informazioni tipiche che possono trovarsi sul *web*, relativamente al ciclo di vita del software.

Client operating systems	Latest update or service pack	End of mainstream support	End of extended support
Windows XP	Service Pack 3	April 14, 2009	April 8, 2014
Windows Vista	Service Pack 2	April 10, 2012	April 11, 2017
Windows 7 *	Service Pack 1	January 13, 2015	January 14, 2020
Windows 8	Windows 8.1	January 9, 2018	January 10, 2023
Windows 10, released in July 2015 **	N/A	October 13, 2020	October 14, 2025

Figura 4 - Tipiche informazioni del ciclo di vita da Microsoft

Come si può notare dalla Figura 3, la successione numerica dei rilasci degli aggiornamenti di Microsoft avviene in seguito alla definizione di *Service Pack*, pacchetti di aggiornamenti particolarmente corposi.

2.5.2 Sicurezza informatica

Come già detto in precedenza, in un'infrastruttura informatica è fondamentale avere, oltre alle prestazioni e funzionalità ottimizzate, anche i requisiti di sicurezza sempre soddisfatti.

Si ritiene opportuno sottolineare l'importanza dal punto di vista della *Cyber Security*, specialmente considerando che questo lavoro è svolto nel contesto di una finanziaria. La sicurezza informatica diventa un requisito essenziale in un mondo

in cui la tecnologia ha completamente trasformato il settore finanziario, specialmente considerando che i crimini dell'*online banking* sono tra i più diffusi in quelli informatici.[67]

Gli impatti che infatti può avere un attacco *hacker* all'interno di una struttura, in un ambiente di questo tipo, acquisiscono un livello di gravità rilevante e possono essere devastanti e comportare perdite economiche notevoli. A questo punto di vista economico, è necessario aggiungere quello che considera la protezione dei dati trattati, principalmente relativi ai clienti.

Se dovesse crollare il muro di difesa tra i *database* dell'azienda e il mondo esterno, si metterebbe in pericolo l'incolumità del portafoglio dei consumatori, nonché l'esposizione di informazioni di questi ultimi estremamente sensibili.

Gli attacchi informatici che possono presentarsi possono presentarsi sotto varie forme. Esempi sono[68]:

- *Phishing Attack*
- *Pharming Attack*
- *Malware Attack*
- Altri tipi di attacco come:
  - *Virus*
  - *Worms*
  - *Trojan Horse*

[67] Anjali Khurana, *Digitalization in banking: Convenience versus Security Threat*, pag. 1893, *International Conference on Sustainable Computing in Science, Technology & Management*, India, Febbraio 2019.

[68] Paganini, P. (2013). *Modern Online Banking Cyber Crime.* Richiamato da INFOSEC INSTITUTE: https://resources.infosecinstitute.com/modern-online-banking-cyber-crime/

CAPITOLO 3 – Gestione degli asset IT e del ciclo di vita

Il numero di dispositivi di rete, *software* e servizi che devono essere gestiti all'interno di un'organizzazione aumenta continuamente, così come la complessità dei flussi di lavoro ad essi relativi. Ciò rende difficile la gestione dell'infrastruttura se ci si limita agli approcci tradizionali, basati quindi sul monitoraggio umano, i quali non possono garantire le prestazioni desiderate per il funzionamento efficace ed efficiente dell'organizzazione. È quindi necessario definire un appropriato flusso di lavoro di gestione della rete, intesa in senso lato di *hardware* e *software* connessi tra loro, nonché un sistema di gestione della stessa rete che sia più intelligente, sistematico e automatizzato di quello attualmente in uso. La necessità che si presenta è quella di raccogliere grandi set di dati che devono essere aggregati, filtrati e visualizzati al fine di rendere facilmente accessibili le informazioni significative a tutti coloro che devono utilizzarle nello svolgimento delle attività caratterizzanti la loro operatività quotidiana.[69]

L'ITIL (*Information Technology Infrastructure Library*) fornisce le linee guida, quindi le *best-practice* per i servizi IT e per i sistemi di gestione della rete, oltre all'allineamento dei processi aziendali.[70]

La soluzione si ritrova in un CMDB (*Configuration management database*), il quale è un *repository* accurato ed affidabile, la cui trattazione sarà effettuata nel capitolo 3.4.

[69] Come nota 9, Yamada, H., Yada, T., Nomura, H., 2011

[70] Come nota 1, Van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., 2007.

3.1 Asset Management

Il sistema di *asset management* può essere definito come il sistema che pianifica e controlla le attività relative agli *asset* e le loro relazioni, al fine di garantire che le prestazioni incontrino la strategia desiderata dall'organizzazione. Questo sistema ha infatti un potenziale significativo nell'influenzare tutti gli aspetti delle attività relative al ciclo di vita degli *asset*.[71]

Con il termine *asset management* si fa riferimento, quindi, al servizio di gestione di tutti gli apparati presenti all'interno dell'infrastruttura di un'organizzazione.

I compiti di questo mestiere sono molteplici e, generalmente, aumentano con il crescere della piattaforma della società. Essenzialmente, l'*asset management* provvede alla gestione del ciclo di vita degli *asset* e di tutte e informazioni ad essi relative. È per tale motivo che esso diventa sempre più complesso all'affermarsi della piattaforma che lo supporta.[72]

Per una gestione ottimale degli *asset IT*, è consigliabile che la presa in carico del servizio avvenga dalla prima fase del ciclo di vita, specialmente quando il parco cresce nel tempo, così come cresce la sua dinamicità, soprattutto in termini di correlazione tra gli apparati.

L'*asset management* diventa quindi un servizio essenziale per acquisire il pieno controllo dello stato attuale dell'infrastruttura, nonché dei costi ad essa imputati.[73] Esso quindi acquisisce un ruolo chiave nel processo decisionale e nella strategia competitiva.[74]

Elemento fondamentale nell'*asset management* è sicuramente la manutenzione degli apparati, che in genere viene considerata come un "centro di costo" dalle

[71] El-Akruti K., Dwight R., Zhang T., *The strategic role of Engineering Asset Management*, Luglio 2013, Int. J. Production Economics 146 (2013) 227-239, www.elsevier.com/locate/ijpe

[72] Come nota 21, Gianturco, E., 2007

[73] Ibidem

[74] Come nota 3, El-Akruti K., Dwight R., Zhang T., 2013

organizzazioni.[75] In particolare, diversi studi mostrano come essa è spesso trattata all'interno delle organizzazioni come "subordinata alle operazioni"[76] o come un "male necessario"[77].

È stato a lungo riconosciuto che, a causa delle prestazioni degli apparati informatici, le organizzazioni presentano notevoli carenze nella realizzazione della propria strategia. Inoltre, si sostiene che le organizzazioni ad alta intensità di capitale non siano adeguatamente consapevoli delle potenzialità che il ruolo dell'*asset management* può acquisire nella definizione e nell'attuazione delle strategie competitive. Pertanto, si consiglia che le attività di tale sistema siano integrate da tutte le altre caratterizzanti l'organizzazione.[78]

Stabilitane l'importanza nella realtà aziendale, si ritiene opportuno individuare la funzione che organizza le attività dell'*asset management* nell'*IT Governance*. Quest'ultima è definita dall'ITIL[79] come ciò che

> *assicura che le Politiche e le strategie siano effettivamente implementate e che i Processi necessari vengano correttamente eseguiti. Il governo dei sistemi informativi include la definizione dei Ruoli e delle responsabilità, la misurazione ed il reporting; richiede, inoltre, che siano intraprese quelle azioni atte a risolvere ogni problema identificato.*

La figura su cui ricade la responsabilità dell'effettiva applicazione di questo servizio è il CIO, *Chief Information Officier*, cioè il principale responsabile della

[75] Ibidem

[76] Alsyouf, I., 2006. *Measuring maintenance performance using a balanced scorecard approach*. Journal of Quality in Maintenance Engineering 12 (2), 133-149.

[77] Muchiri, P., Pintelon, L., 2008. *Performance measurement using overall equipment effectiveness (OEE): literature review and practical application discussion.* International Journal of Production Research 46 (13), 3517-3535.

[78] Come nota 3, El-Akruti K., Dwight R., Zhang T., 2013

[79] Come nota 1, Van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., 2007.

gestione dell'IT all'interno dell'organizzazione. Egli risponde direttamente al CEO, *Chief Executive Officier*, che ha invece la responsabilità della definizione dei piani strategici e delle politiche stabilite nel Consiglio di Amministrazione.[80]
Un elemento chiave del processo di *IT Governance* è l'allineamento delle attività informatiche a quelle del *business*. In particolare, la misura strategica riconosce che la strategia dell'IT dovrebbe essere articolata in termini di[81]:

- Dominio esterno, quindi come l'organizzazione si posiziona nel mercato
- Dominio interno, cioè come l'infrastruttura deve essere configurata e gestita

Quando l'integrazione è completa e le decisioni tengono conto della condizione totale dell'organizzazione, allora si acquisisce un vantaggio competitivo nei confronti delle imprese concorrenti.[82]

3.2 Obsolescence Management

Nelle realtà aziendali acquisisce sempre maggiore importanza la gestione ottimale degli *asset IT*, del relativo ciclo di vita e, di conseguenza, dell'obsolescenza intrinseca.

Come anticipato nel capitolo precedente, l'obsolescenza è, quindi, la transizione di un apparato, in questo caso specifico, dalla disponibilità del produttore originale alla sua indisponibilità.[83]

[80] De Haes, S., Van Grembergen, W., *IT Governance and its mechanism*, 2004, Information System Control Journal, vol.1.

[81] Ibidem

[82] Ibidem

[83] IEC 62402:2007

L'*obsolescence management* è il processo che coordina le attività per dirigere e controllare un'organizzazione circa l'obsolescenza.[84]

Per scongiurare i rischi legati a dispositivi obsoleti, o comunque obsolescenti[85], è necessario effettuare analisi e considerazioni sugli *asset IT* e sui relativi cicli di vita. Relativamente a questi ultimi, in particolare, è necessario tenere in considerazione che essi variano, anche notevolmente, tra un apparato e l'altro.
Nelle implementazioni e/o sostituzioni è fondamentale tenere conto della progettazione iniziale del sistema, per essere consapevoli dell'effettiva compatibilità dell'infrastruttura con i nuovi elementi che si vanno ad introdurre al suo interno. Le nuove versioni, sia *hardware* che *software*, devono essere compatibili con le precedenti, al fine di evitare disservizi e garantire l'operatività aziendale. Nelle transizioni tra le varie generazioni di rilasci, infatti, viene richiesto che le nuove soluzioni supportino le vecchie interfacce[86].
Per soddisfare questa esigenza, deve essere affrontato un *assessment* di compatibilità e stilata della documentazione a riguardo prima che la vecchia versione diventi obsoleta.
Si può considerare di implementare gradualmente il sistema, evitando di stravolgere completamente l'infrastruttura per rimediare all'obsolescenza degli apparati in essa contenuti e garantire, quindi, la compatibilità. In tal caso, alcune soluzioni possono essere, ad esempio:

- Implementazione parziale, migrazione o sostituzione graduale

- Combinazione tra vecchi e nuovi di:
    - Controlli
    - Input / Output

[84] Ibidem

[85] La differenza tra obsoleto e obsolescente sta nel fatto che il primo risulta già non essere disponibile presso il produttore, di conseguenza i *vendor* non possono garantire la copertura manutentiva globale, mentre il secondo vede annunciata solo la sua data di EOL.

[86] IOGP Instrumentation and Automation Standards Subcommitee (IASSC), *Obsolescence and life cycle management for automation system, Recommended practice*, report 551, July 2016

    - Strumentazione di rete
    - Fornitori potenziali
    - Interfacce ai sistemi di terze parti
    - Strumenti di configurazione
- Conversione degli strumenti
    - In via grafica
    - In via logica

Parallelamente si può pensare anche semplicemente di aggiungere nuove funzionalità, le quali, anch'esse, devono essere analizzate per garantire la compatibilità dei sistemi.

Per la corretta gestione dell'obsolescenza, è fondamentale la pianificazione, il cui *output* si ritrova in un *Obsolescence Management Plan*, di cui si farà un approfondimento nei paragrafi successivi.

3.2.1 Strategie di approccio: Proattivo vs Reattivo

Si ritiene opportuno fare un approfondimento circa le differenze tra le possibili strategie applicabili nell'affrontare i problemi relativi all'obsolescenza.

Assumere un approccio di tipo proattivo significa determinare in anticipo lo stato dell'obsolescenza degli *asset* di cui si ha il governo. Questo significa ridurre i possibili impatti dell'invecchiamento degli apparati, dal momento che è possibile andare a determinare dei piani d'azione per massimizzare la vita degli stessi, nonché per determinare anticipatamente le operazioni di implementazione, migrazione o sostituzione.
Alcune delle azioni che possono essere applicate sono le seguenti:

- Estendere la durata della fornitura attiva presso il fornitore, oppure estendere il supporto post-vendita;

- Stringere accordi di lungo termine per gli apparati maggiormente critici;

- Mantenere competenze e *skill* rilevanti all'interno della propria organizzazione;

- Pianificare l'evoluzione dei sistemi sulla base delle analisi di rischio;
- Prevedere scenari che plausibilmente possono presentarsi e, per ognuno, le relative soluzioni adottabili;

- Scegliere soluzioni tecnologiche in cui la gestione dell'obsolescenza è prevista dalla fase di sviluppo. Un esempio pratico possono essere i sistemi modulari, i cui *standard* prevedono che le interfacce attuali siano completamente compatibili con quelle implementate.

L'approccio proattivo sarebbe il desiderato ideale dalle organizzazioni ben strutturate. Tuttavia, bisogna considerare che richiede costi onerosi in termini di *effort* e risorse, specialmente quando deve essere integrato in un'organizzazione in cui tale documentazione risulta totalmente, o almeno in parte, assente. Per tale motivo, è preferibile iniziare ad applicare tale approccio ai sistemi particolarmente critici per l'organizzazione, per poi estendere tale politica a tutti gli altri *asset*.

L'approccio reattivo, invece, sviluppa e implementa le soluzioni relativamente all'obsolescenza nel momento in cui le problematiche ad essa relativa si manifestano durante l'attività aziendale.

Le azioni che vengono applicate in caso di una strategia reattiva possono essere, ad esempio:

- Iniziare a risolvere una problematica relativa all'obsolescenza solo quando un apparato crea disservizi o smette di funzionare;

- Riparare o rimpiazzare i componenti affidandosi a un terzo fornitore o utilizzando componenti di seconda mano;

- Sostituire completamente il sistema quando esso diventa obsoleto;

- Nel caso in cui si opti per la sostituzione di un componente o di un intero apparato, è importante tenere in considerazione:
  - Verificare la disponibilità dei back-up
  - Verificare che tutti gli *stakeholder* siano informati relativamente alle procedure di *restore* dei sistemi di controllo e di sicurezza
- Avere procedure solide e facilmente accessibili per il rilevamento delle minacce.

È quindi preferibile applicare l'approccio reattivo:

- Quando non si ha il pieno controllo della gestione degli *asset* e, di conseguenza, del relativo ciclo di vita
- Quando i rischi, la probabilità di guasto, l'impatto e i costi associati all'obsolescenza sono bassi

Nel secondo caso, in particolare, un approccio proattivo sarebbe eccessivamente oneroso e non necessario.

3.2.2 Obsolescence management plan

Un piano per la gestione dell'obsolescenza è fondamentale per poter avere il pieno controllo e consapevolezza delle azioni che devono essere applicate.
In particolare, la strategia per gestire l'obsolescenza deve perseguire alcuni obiettivi[87]:

- Deve identificare lo stato di obsolescenza di tutti gli *asset* coinvolti nell'infrastruttura;

- Deve provvedere a una *roadmap*[88] su come gestire l'esposizione all'obsolescenza;

[87] Ibidem

[88] Una roadmap è un piano contenente la sequenza temporale di azioni che devono essere eseguite per raggiungere uno scopo definito in partenza

- Deve identificare dettagliatamente i requisiti di sicurezza e i rischi dati dallo stato di obsolescenza;

- Deve valutare gli impatti dovuti allo stato di obsolescenza degli *asset IT*;

- Deve tenere conto dei vincoli operativi delle risorse a disposizione;

- Deve scindere i casi in cui è preferibile applicare una strategia proattiva e quando, invece, più opportuno affidarsi a una strategia reattiva;

- Deve mantenere i contatti con i *vendor*, al fine di:
  - Essere sempre aggiornati su *End of Support* ed *End of Life*;
  - Essere aggiornati su eventuali estensioni relativamente al supporto e alla manutenzione;
  - Identificare eventuali accordi di estensione dei servizi di supporto, anche se non globali, ma personalizzati sulla base delle esigenze del cliente;
  - Avere ben chiare le soluzioni proposte dal fornitore riguardo la migrazione da una tecnologia obsoleta a una attiva, chiaramente tenendo in considerazione tutti i vincoli di compatibilità descritti in precedenza.

Anche nella pianificazione e nella coordinazione della gestione dell'obsolescenza devono essere considerati dei requisiti essenziali, quali, ad esempio:

- I fornitori devono provvedere alla trasmissione delle informazioni relative alle tecnologie fornite e, in particolare, ai dati riguardanti le fasi post-vendita;

- Ogni componente integrato in un sistema deve avere della documentazione dedicata;

- Ogni sistema deve avere un piano a lungo termine con una visione globale circa la compatibilità dei sistemi e gli impatti che eventuali cambiamenti tecnologici comporterebbero.

Per tale motivo, ci sono una serie di elementi essenziali da considerare all'interno di un piano efficace:

- Diagrammi rappresentanti il ciclo di vita degli *asset* considerati1,
- *Risk assessment*;
- Mappatura e monitoraggio dell'obsolescenza;
- Reportistica relativa alla gestione dell'obsolescenza;
- Ruoli e responsabilità dell'organizzazione relativamente alla gestione dell'obsolescenza.

Particolare evidenza acquisiscono i diagrammi, i quali devono descrivere dettagliatamente le aspettative di durata delle tecnologie adottate, quindi lo stato attuale e quello futuro, prevedendo intervalli temporali di breve, medio e lungo termine.

3.2.3 Valutazione dell'obsolescenza

Per poter avanzare una gestione dell'obsolescenza ottimale, come anticipato in precedenza, è indispensabile effettuare un'analisi della stessa in maniera dettagliata, focalizzando l'attenzione nella fase post-vendita[89].

Per avere una visione completa dello stato effettivo del proprio parco, bisogna seguire due passaggi essenziali, di seguito descritti nel dettaglio.

[89] IOGP Instrumentation and Automation Standards Subcommitee (IASSC), *Obsolescence and life cycle management for automation system, Recommended practice*, report 551, July 2016

1. Creare un inventario completo dei componenti appartenenti all'infrastruttura.
   Ogni apparato deve essere censito con le informazioni relative allo stato di obsolescenza, senza trascurare i dettagli sulle relazioni con gli altri componenti del sistema, così da poter fare delle valutazioni affidabili circa gli impatti di eventuali cambiamenti. Tale documentazione deve essere facilmente accessibile comprensibile da tutti gli attori interessati.

2. Determinare lo stato attuale del ciclo di vita degli *asset*.
   Tale informazione va ad integrare l'inventario descritto al punto 1. Nel caso in cui gli apparati siano coperti dal supporto di un fornitore, tali informazioni possono essere ricavate anche in collaborazione con quest'ultimo.

Una particolare attenzione merita la valutazione dei rischi associati allo stato di obsolescenza delle tecnologie in uso nell'organizzazione, che si preferisce descrivere in un paragrafo dedicato.

3.2.3.1 Analisi dei rischi

Il *risk assessment* è un'attività essenziale per poter effettuare una valutazione completa dell'obsolescenza.

Esso prevede sette fasi[90], presentate in Figura 5:

[90] Ibidem

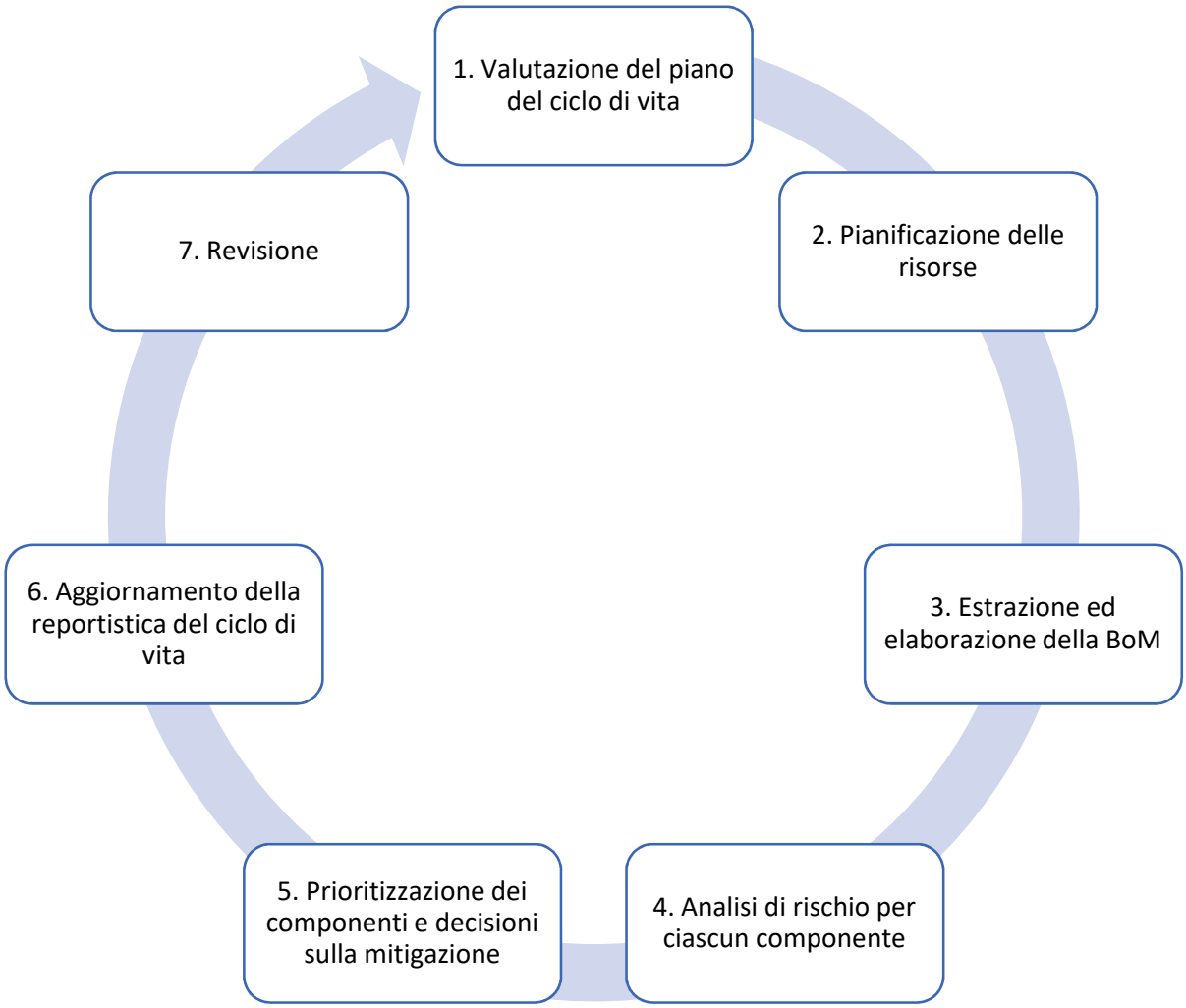

Figura 5 – Ciclo dell'analisi dei rischi

1. Valutazione del piano del ciclo di vita

   Il primo passaggio è relativo alla definizione della situazione attuale dello stato dell'infrastruttura dell'organizzazione. Bisogna tenere in considerazione i tempi per cui la tecnologia è stata in vita ed eventuali piani di implementazione, migrazione o sostituzione dei sottosistemi.

Quest'operazione semplifica l'individuazione dei periodi che devono essere considerati all'interno della *bill of material*.

2. Pianificazione delle risorse

   È necessario assicurarsi di avere sufficienti risorse a disposizione nella gestione dell'obsolescenza. In particolare, le valutazioni vengono fatte su:

   - Persone
   - Strumenti
   - *Budget*

   Per questa fase è necessario che le risorse coinvolte siano tutte allineate circa lo stato attuale della tecnologia e delle strategie che si ha intenzione di applicare.

3. Estrazione ed elaborazione della BoM

   La maggior parte delle problematiche relative all'obsolescenza riguardano singoli componenti degli *asset* impiegati. La *bill of material* consente quindi di avere una panoramica completa di massimo dettaglio di tutti gli elementi dell'infrastruttura.

4. Analisi di rischio per ciascun componente

   Considerando l'obsolescenza, è fondamentale andare a definire gli impatti che una gestione fallimentare di quest'ultima possa avere nell'organizzazione. In particolare, bisogna considerare che, a seconda dell'*asset* che si sta considerando, si avranno conseguenze più o meno gravi. Gli approcci che possono seguirsi possono affidarsi a due scenari differenti.

   A. Il primo metodo considera la disponibilità dei componenti, relazionata al tasso di fallimento del medesimo componente. Per tasso di fallimento si fa riferimento a quello basato sull'esperienza delle risorse coinvolte o, in ogni caso, alle previsioni frutto di analisi analitiche. La rappresentazione grafica si riporta in Figura 6.

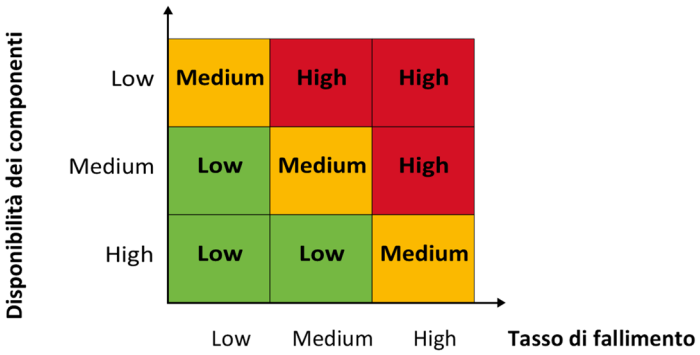

Figura 6 – Rischio dell'obsolescenza come funzione della disponibilità dei componenti

B. Il secondo metodo considera la disponibilità delle competenze delle risorse umane, responsabili del sistema in esame, in funzione della complessità di fallimento o del grado di competenza necessario per sostenere la funzionalità. La rappresentazione grafica si riporta in Figura 7.

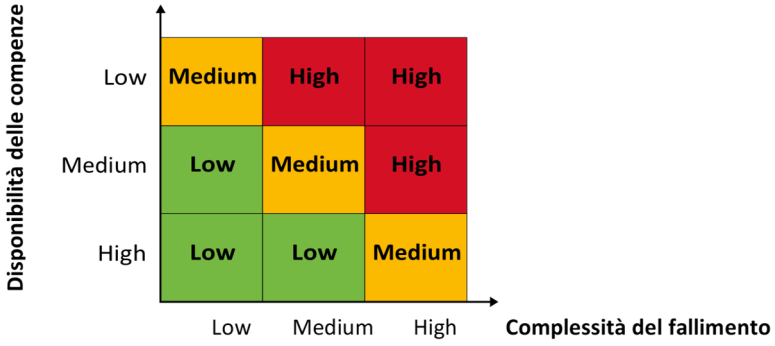

Figura 7 – Rischio dell'obsolescenza come funzione della competenza

5. Prioritizzazione dei componenti e decisioni sulla mitigazione

   È poco realistico pensare di poter risolvere qualsiasi problematica che si presenta immediatamente, sia per motivi di indisponibilità di *budget* che per limiti operativi. Per tale motivo è necessario stabilire delle priorità tra gli *asset* da gestire.

Per poter definire una strategia risolutiva efficace, considerando tutte le conseguenze e gli impatti del caso, è opportuno basarsi sull'analisi dei rischi (descritta nel punto precedente).

Il processo decisionale risulterà essere il seguente:

i. Identificare il rischio di obsolescenza relativo a ciascun componente (*High, Medium, Low*)
ii. Determinare l'esposizione del componente all'interno del sistema, considerando entrambi i casi in cui viene adottato in un singolo punto o in più punti:
    a. Sistema critico
    b. Sistema non critico
iii. Determinare le conseguenze di un guasto, dai punti di vista di:
    a. Sicurezza degli ambienti
    b. Produzione
    c. Reputazione
iv. Identificare la strategia più appropriata, facendo riferimento a quelle presentate nei paragrafi precedenti, quindi un approccio proattivo o reattivo. Le possibili azioni sono quindi:
    a. Accettare il rischio e non fare nulla
    b. Acquistare pezzi di ricambio sicuri o usufruire di competenze attendibili
    c. Sostituire gli elementi danneggiati
    d. Ri-progettare il sistema
    e. Decidere di implementare, migrare o sostituire, interamente o solo parzialmente, il sistema

Chiaramente, non esiste una soluzione ottima. Tutto dipende dalla strategia adottata dall'organizzazione e dalle considerazioni sui vincoli presenti.

6. Aggiornamento della reportistica del ciclo di vita

   Una volta che è stata definita la strategia da adottare, essa deve essere implementata nel sistema. Risolto il problema, quindi, è necessario

apportare le modifiche e gli aggiornamenti nella documentazione relativa alle componenti tecnologiche inventariate.

7. Revisione
   Quest'ultima fase rientra nelle linee guida per una gestione valida ed efficace. Periodicamente, infatti, deve essere previsto di rivedere e, eventualmente, aggiornare l'*assessment*.

3.2.4 Monitoraggio dell'obsolescenza

Definite tutte le modalità con cui deve affrontarsi una possibile problematica relativa all'obsolescenza e le strategie applicabili, bisogna fare in modo che i processi di mappatura e *risk assessment* siano sfruttati correttamente all'interno dell'organizzazioni.
Lo stato dell'obsolescenza e gli impatti dei piani di azioni che si decide mettere in atto devono essere costantemente monitorati. Si ritiene opportuno sottolineare che un approccio di questo tipo è caratteristico di una strategia proattiva.
Per effettuare tale operazioni si possono sfruttare anche strumenti automatizzati, oltre che, ovviamente, basarsi sul lavoro manuale degli addetti all'analisi e al monitoraggio degli *asset*.
Ci sono infatti varie modalità di monitorare lo stato dell'obsolescenza[91]:

- Utilizzo di strumenti automatici di monitoraggio dei componenti
  È la modalità preferita per il monitoraggio dell'obsolescenza. Si tratta dell'utilizzo di soluzioni analitiche, proposte dal fornitore stesso, che consentono di gestire sia le *bill of material* che reportistica in formati differenti, così da semplificare le elaborazioni dei dati messi a disposizione. Tali strumenti sono dotati anche della possibilità di applicare delle query, limitando così le informazioni a un perimetro predeterminato.

[91] Ibidem

- Monitoraggio manuale dei componenti
  Lo stato di obsolescenza, in questo caso, viene definito andando a reperire le informazioni circa le tecnologie in uso sui canali ufficiali o prendendo direttamente i contatti con i fornitori/produttori.

- Monitoraggio effettuato da terze parti, siano essi fornitori o produttori
  In quest'ultimo caso è lo stesso fornitore/produttore a preoccuparsi dello stato di obsolescenza in cui versano i sistemi oggetto d'esame, provvedendo a fornire una documentazione dettagliata dello stato attuale delle cose, secondo termini contrattuali predefiniti. In questi ultimi, infatti, si vanno a definire il livello di dettaglio delle informazioni che deve essere fornito, i responsabili del monitoraggio, come il monitoraggio deve essere condotto, nonché la frequenza con cui deve essere inviata la reportistica.

3.2.5 Indicatori di performance KPI e di rischio KRI

Avendo parlato di prestazioni dei processi aziendali e di analisi di rischio, si ritiene opportuno procedere con una breve descrizione degli indicatori di *performace* e di rischio, utilizzati nei *report*, base per le decisioni strategiche nella gestione dell'obsolescenza.

Per essere efficaci, tali indicatori devono rispondere a cinque requisiti, riassumibili nell'acronimo SMART:

- Specifico (*Specific*)
  Ogni indicatore deve fare riferimento specificatamente al processo che deve essere monitorato

- Misurabile (*Measurable*)
  Gli indicatori devono essere facilmente misurabili, non onerosi e realizzabili facilmente

- Realizzabile (*Achievable*)
  Le soglie definite per ciascun indicatore devono essere realistiche e raggiungibili

- Rilevante (*Relevant*)
  Un indicatore deve essere utile e comprensibile a chi lo esamina: le indicazioni fornite devono essere adeguate a poter definire le strategie e i piani di azione

- Tempestivo (*Timely*)
  Ogni indicatore deve essere utilizzabile in tempi utili.

I *Key Performance Indicator* sono degli indicatori numerici che consentono la valutazione dei processi aziendali, in termini di prestazioni. In questo caso, si considerano le prestazioni dei sistemi e dell'infrastruttura, nonché dei processi di gestione dell'obsolescenza.
Tramite questi indicatori chiave, i *manager* hanno la possibilità di acquisire consapevolezza relativamente al funzionamento dei processi gestiti dal sistema informativo, potendo così implementare un processo di monitoraggio adeguato[92].

Possono inoltre essere individuate tre categorie di *key performance indicator*[93]:

- KPI di efficienza
  La misurazione viene effettuata relazionando le risorse utilizzato e l'output prodotto

[92] Corno, F., Torchiano, M., Sistemi Informativi Aziendali, Appunti per il corso – Capitolo 10, gennaio 2018.

[93] Ibidem

- KPI di qualità
  La misurazione viene effettuata considerando la qualità del prodotto finale come output del processo

- KPI di servizio
  La misurazione è relativa al confronto dell'input, valutando le richieste ricevute, e dell'output, quotando il soddisfacimento della richiesta in termini di prodotto finale, tempi di risposta, comunicazione all'utente.

Nella definizione di un *key performance indicator* è necessario tenere in considerazione:

- Il processo che deve essere monitorato;

- Gli obiettivi che si desidera raggiungere;

- Le caratteristiche SMART;

- Il perimetro di azione.

I *Key Risk Indicator* sono degli indicatori numerici che stimano i potenziali disservizi o guasti delle risorse utilizzate[94].
Si tratta di metriche utilizzate per verificare se l'organizzazione è soggetta, o potrebbe essere soggetta con una certa probabilità, a un rischio superiore alla sua propensione al rischio[95].

[94] KRI, secondo la definizione fornita dall'OECD, *Organisation for Economic Co-operation and Development*.

[95] Per propensione al rischio si intende il livello di rischio accettato dall'organizzazione.

Tali indicatori sono fondamentali per stabilire anche i plausibili impatti che tali eventi, di malfunzionamenti o disservizi, possono avere nell'organizzazione in termini di prestazioni o costi.
In particolare, un monitoraggio costante degli indicatori di rischio può apportare i seguenti benefici:

- Supportare un'azione proattiva nella risoluzione dei fermi operativi, fornendo un avviso tempestivo;

- Fornire una visione retrospettiva, che consente di effettuare analisi e di individuare gli errori, così da formulare dei piani di azioni che scongiurino ulteriori rischi non considerati in passato;

- Fornire indicazioni circa la propensione al rischio dell'organizzazione e del suo stato attuale, fornendo anche indicazioni ai responsabili delle decisioni strategiche.

La differenza essenziale tra le due tipologie di indicatori riportati è[96]:

- I *Key Performance Indicator* forniscono una misurazione ex-post del processo, quindi relativamente al raggiungimento o meno degli obiettivi definiti all'inizio dello stesso

- I *Key Risk Indicator* forniscono una misurazione ex-ante del processo, provando ad anticipare gli eventi che potrebbero avere impatti più o meno notevoli sulle prestazioni aziendali e, di conseguenza, sul raggiungimento degli obiettivi

[96]https://www.softwarequarta.com/risk-based-thinking-kpi-e-indicatori-di-rischio-kri-per-generare-valore/

3.3 Il Configuration Management

Prima di definirne la gestione, bisogna definire cosa si intende per configurazione. Quest'ultima è l'insieme delle caratteristiche fisiche e funzionali di un prodotto, sia esso hardware o software, le quali sono raccolte nella documentazione tecnica stilata durante la creazione dello stesso.[97]
Ciò che deve essere considerato nella configurazione di un apparato sono una serie di criteri, di seguito elencati[98]:

- Requisiti dettati dal Regolatore o dalla Legislazione;
- Requisiti ritenuti critici dal punto di vista della sicurezza e del rischio relativi al prodotto;
- Tecnologie adottate, siano esse nuove o implementazioni di quelle esistenti, progettazione e il conseguente sviluppo;
- Interfacce tra tutti gli elementi di configurazione;
- Condizioni relative all'approvvigionamento degli apparati;
- Manutenzione, supporto e servizi al cliente.

La *configuration management* (la gestione della configurazione) è l'insieme delle attività applicate a tutto il ciclo di vita del prodotto in esame. Grazie alla gestione della configurazione, quindi, si riesce ad acquisire un controllo più efficace e più efficiente dei prodotti e delle specifiche che li caratterizzano.[99]

[97] http://www.humanwareonline.com/project-management/center/configuration-management/ https://it.wikipedia.org/wiki/Configurazione_(informatica)

[98] Ibidem

[99] http://www2.supsi.ch/cms/pmforum/wp-content/uploads/sites/23/2017/07/G2-Configuration-Management-secondo-l%E2%80%99ISO.pdf

In particolare, grazie alla *configuration management*, si riesce a documentare l'intera configurazione del prodotto, garantendone l'accessibilità delle informazioni, in un'ottica di raggiungimento dei requisiti fisici e soprattutto funzionali del prodotto.[100]

Quando si pensa ad approcciarsi alla gestione della configurazione degli apparati, è necessario considerare implementarla tenendo in considerazione le dimensioni dell'organizzazione e il prodotto, sia nella sua natura che nella sua complessità. Questi devono ovviamente prendere in considerazione anche le politiche aziendali, il settore in cui si opera e la struttura dei processi esistenti.[101]

L'implementazione di questo processo si basa sul *Configuration Management Planning*, il cui *output* è la stesura di un *Configuration Management Plan*. La gestione della configurazione, infatti, non è un qualcosa che può essere definito improvvisando, ma ogni decisione deve essere ponderata e ogni conseguenza deve essere considerata. Nel piano, che deve essere ovviamente approvato e controllato, devono essere inserite tutte le procedure da utilizzare necessarie alla gestione e devono essere esplicitati i ruoli e le responsabilità coinvolte nel ciclo di vita del prodotto.[102]

Parlando di pianificazione, non si possono non considerare i *change*, ossia tutti quei cambiamenti che potrebbero essere apportati ai prodotti. Tali modifiche devono chiaramente essere approvate, prima di poter essere applicate ai dispositivi in esame. L'approvazione è il risultato di un'analisi approfondita della *baseline* di configurazione, la documentazione riportante sia lo stato attuale degli apparati che le relative evoluzioni nella configurazione, e degli impatti che questi *change* possono avere nell'infrastruttura, sia dal punto di vista delle prestazioni che della

[100] www.iso.org

[101] Come nota 99

[102] Ibidem

sicurezza. Ciò significa che le valutazioni vengono fatte considerando aspetti sia *hardware* che *software*.[103]

3.3.1 Standard ISO

Il *configuration management* pone le sue basi nella norma ISO 10007, *"Quality management systems — Guidelines for configuration management"* ("Sistemi di gestione per la qualità – linea guida per la gestione della configurazione").[104]

L'ISO (*International Organization Standardization*) è una federazione mondiale composta da enti membri ISO, organismi nazionali di normalizzazione. Tutto il lavoro di preparazione dello standard, che è quindi uno standard internazionale, viene svolto mediante i comitati tecnici specifici. In particolare, ogni organo membro si occupa di un sottoprogetto specifico, per il quale a sua volta è stato convocato un comitato. In collaborazione con ISO, sono presenti anche organizzazioni esterne, sia governative che non, anch'esse internazionali, in particolare con la Commissione Elettrotecnica Internazionale (IEC, International Electrotechnical Commission) per tutto ciò che riguarda le standardizzazioni elettrotecniche.[105]

La ISO 10007 è una norma internazionale che detta le direttive sulla gestione della configurazione all'interno di una qualsiasi organizzazione, sia essa pubblica o privata, piccola impresa o multinazionale.[106]

Anche se applicabile a organizzazioni di ogni tipo, l'implementazione di queste direttive deve essere contestualizzata e adattata al contesto, tenendo in considerazione le caratteristiche dell'impresa in cui si sta operando, oltre che la complessità del prodotto, così da riuscire a ottenere i risultati migliori in termini di ritorni tecnici ed economici.[107]

---

[103] Ibidem

[104] https://it.wikipedia.org/wiki/ISO_10007

[105] https://www.iso.org/obp/ui/#iso:std:iso:10007:ed-3:v1:en

[106] Come nota 104

[107] Come nota 99

La suddetta normativa viene applicata all'intero *life cycle* del prodotto, quindi partendo dalla fase di introduzione, fino ad arrivare a quella di declino, passando ovviamente per quelle di crescita e maturità.[108]
Lo scopo di questo standard internazionale è di migliorare la comprensione comune della materia, di promuovere l'utilizzo della *configuration management*, di assistere le organizzazioni che decidono di applicare questa metodologia, perseguendo il fine di migliorare le proprie prestazioni.[109]
La normativa, inoltre, suggerisce di registrare una documentazione, basata sul database in cui i *configuration item* sono censiti, tale da avere piena visibilità, tracciabilità e gestione dell'evoluzione della configurazione.[110]
In particolare, secondo la ISO 10007, le informazioni ritenute necessarie per definire il prodotto e il relativo utilizzo sono le seguenti:[111]

- Requisiti;
- Specifiche tecniche;
- Disegni costruttivi;
- *Bill of Material*, BOM, ossia la distinta base, anche detta *part list*;
- Documentazione *software*;
- Modalità e specifiche sull'attuazione dei test;

[108] Come nota 99
https://www.logisticaefficiente.it/wiki-logistica/supply-chain/product-life-cycle-ciclo-di-vita-del-prodotto.html
https://www.glossariomarketing.it/significato/ciclo-di-vita-del-prodotto/

[109] Come note 99 e 100

[110] Come nota 99
https://it.wikipedia.org/wiki/Gestione_della_configurazione

[111] Come nota 99

- Manutenzione e supporto;

- Manuali d'uso.

3.4 CMDB: Configuration Management Database

Dalla trattazione fatta in precedenza, è automatico raggiungere la conclusione di come la gestione del ciclo di vita degli *asset* sia di fondamentale rilevanza all'interno di un'organizzazione.
Come accennato nel paragrafo 3.1, *l'asset management* può basarsi su una piattaforma che aggrega i dati e le informazioni di tutti gli *asset* aziendali e delle relazioni che intercorrono tra essi, specialmente nei casi in cui le organizzazioni hanno dimensioni tali da dover gestire un numero notevole di dispositivi.
Una piattaforma valida al supporto dell'*asset management* deve prevedere una base dati centralizzata, in cui possono facilmente ritrovarsi tutte le informazioni relative ad ogni singolo dispositivo configurato nella rete aziendale. [112]

Tale piattaforma si può semplicemente identificare in un CMDB.

CMDB è l'acronimo per *Configuration Management Data Base*[113].
Si tratta dello strumento che supporta la gestione degli elementi di configurazione all'interno di un'organizzazione, dal momento che è un sistema di archiviazione e consultazione ufficiale di tutte, o quasi, le informazioni relative ai sistemi informatici adottati da un'azienda.
L'utilizzo di un CMDB consente di amministrare efficacemente ed efficientemente degli elementi informatici grazie al suo essere un sistema dinamico, stabilmente aggiornato sullo stato dell'*hardware* e del *software*, nonché delle relazioni e delle interdipendenze esistenti tra i due, di proprietà dell'organizzazione.

[112] Come nota 21, gianturco, E., 2007

[113] http://www.cmdbuild.org/it/contenuti/per-saperne-di-piu/cos-e-un-cmdb

L'obiettivo dell'adozione di un CMDB è l'acquisizione del pieno controllo degli *asset IT* utilizzati, grazie alla conoscenza della composizione, della collocazione e delle relazioni funzionali.
Il caso in cui le informazioni nell'archivio non dovessero essere aggiornate rappresenta una mancanza grave per l'organizzazione, la quale si trova ad affrontare costi superflui, operazioni ridondanti, ritardi nella gestione e nella risoluzione delle problematiche, difficoltà nello svolgimento delle attività aziendali.

Gli *asset* gestiti all'interno di un *Configuration Management Data Base* sono tutti gli elementi informatici, proprietari e non, in utilizzo dall'organizzazione.
Le classi standard in cui vengono suddivisi i *configuration item*, così come ampliamente descritti nel capitolo 2 di questo lavoro, sono[114]:

- *Hardware*: *server* (fisici e virtuali), *hypervisor*, *storage*, apparati di rete (*network devices*), PC, postazioni di lavoro, apparati di telefonia;

- *Software*: sistemi operativi, *database*, *web application*, applicativi di terze parti;

- Documentazione: contratti, licenze, *asset* esposti, indicatori di *performance* (KPI), *dashboard*, mappature dei sistemi, mappature della rete;

- Altre risorse: dipendenti, consulenti esterni, stagisti, interinali, fornitori.

Le informazioni presenti sul *Configuration Management Data Base* vanno a soddisfare i quesiti che ci si potrebbe porre in fase di analisi delle risorse, coprendo tutti i dati ad esse relative. Nel censimento degli *asset*, infatti, vengono inserite tutte le informazioni riguardanti gli stessi, con una visione che copre gli aspetti tecnici,

[114] Come nota 1, Van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., 2007.

funzionali, relazionali e in parte anche burocratici. Il CMDB trova risposta agli interrogativi più frequenti su un *configuration item*, quali dubbi sulla locazione (nel caso di *asset* fisici), da chi viene utilizzato, da cosa è composto, dove si colloca nell'infrastruttura dell'organizzazione e quindi le relazioni con gli altri elementi di configurazione, quali sono le licenze ad esso collegato. In particolare, proprio perché nel CMDB sono esplicitate tutte le relazioni tra gli *asset*, è semplificata l'analisi degli impatti dovuti a un'eventuale modifica su un qualsiasi elemento informatico all'interno dell'infrastruttura[115].
Il CMDB può essere utilizzato anche come archivio documentale della storia aziendale, un vero e proprio database storico.

Il *Configuration Management Data Base* è, quindi, la fonte primaria di informazioni relative ai *configuration item* (CI), i componenti appartenenti all'infrastruttura, i cui dati di configurazione sono tra le fonti più importanti per l'ottimizzazione della gestione della rete.
Abbiamo visto che i dati che possono essere archiviati all'interno di un CMDB sono di vario tipo. In particolare, bisogna considerare che le informazioni di ogni dispositivo informatico possono essere statiche o dinamiche[116]: nel primo tipo rientrano quelle relative alla configurazione, mentre nel secondo sono inclusi, ad esempio, i dati di traffico e del sistema di log. Esempi di informazioni memorizzabili in un CMDB sono:

- la configurazione corrente degli elementi informatici presenti nella rete;
- statistiche relative ai dispositivi circa i loro utilizzo e disponibilità;
- specifiche riguardanti i software installati, nonché quelle dell'hardware necessario al loro funzionamento;
- locazione all'interno dell'infrastruttura;
- identità e contatti del responsabile dell'*asset*.

[115] Come nota 113

[116] Come nota 9, Yamada, H., Yada, T., Nomura, H., 2011

Ciò che risulta essere di enorme supporto alla gestione dell'infrastruttura è la possibilità di definire le relazioni tra i vari componenti. Quando si presenta una variazione di alcuni componenti, che sia un semplice aggiornamento applicativo o una sostituzione definitiva dell'elemento informatico, è infatti possibile prevedere come questi cambiamenti possano impattare sugli altri componenti e, in generale, sulla qualità del servizio applicativo.

3.4.1 Le funzionalità del CMDB per gli apparati di rete

Avendo definito a cosa si fa riferimento quando si parla di configurazione e di *Configuration Management Data Base*, si può procedere ad una descrizione di maggior dettaglio su come lo strumento in esame può essere utilizzato nello specifico per gli apparati di rete. Si ritiene opportuno approfondire l'argomento per questa tipologia di *asset* dal momento che sono quelli maggiormente soggetti a modifiche vicine nel tempo, quindi molto dinamiche, mentre gli altri dispositivi possono essere considerati piuttosto statici.

Ci sono 6 funzioni a cui un *Configuration Management Data Base* deve necessarie adempiere.

1) Un CMDB deve per prima cosa essere una fonte affidabile e accurata di informazioni di configurazione relativamente ai *configuration item* (CI), compresi *router*, *switch*, *firewall* e i numerosi server in utilizzo nella rete. La motivazione di tale esigenza va ricercata nel fatto che i dati archiviati all'interno di questo strumento sono indispensabili per analizzare le prestazioni della rete e per progettare la capacità delle risorse della stessa. I *configuration item* infatti, come *switch* e *router*, richiedono una configurazione in cui vengono definiti una serie di parametri e comandi necessari al corretto funzionamento dell'infrastruttura, anche in termini di sicurezza informatica. Le caratteristiche di configurazione che devono essere esplicitate sono:

- *Hostname*, quindi il nome identificativo di un qualsiasi apparato all'interno della rete;

- Indirizzo IP (*Internet Protocol Access*) delle interfacce, che individua univocamente, tramite un'etichetta numerica, un dispositivo all'interno della rete;

- Parametri per il protocollo di *routing*, dove quest'ultimo sta a indicare la strada che percorrono i pacchetti scambiati tra gli apparati della rete, in questo caso non solo quella interna, ma anche quella pubblica;

- SNMP (*Simple Network Management Protocol*), utilizzato, anche questo, per la comunicazione tra gli apparati *hardware* e *software* all'interno di una rete. Tale protocollo supporta l'identificazione dei *device*, monitorando le *performance* e tenendo traccia delle modifiche;

- Comandi per la misurazione del traffico effettuato in ingresso e in uscita;

- Elenchi di accesso alle macchine.

Inoltre, il *Configuration Management Data Base* deve essere in grado di accedere ai dispositivi nella rete così da poter aggiornare in tempo reale i dati di configurazione. Per adempiere a tale scopo si utilizzano anche, ad esempio:

- Il *Lightweight Directory Access Protocol*, LDAP, che è un protocollo standard che consente di interrogare e modificare i servizi di *directory*, ossia un programma, o un insieme di programmi, per l'organizzazione, la gestione e la memorizzazione delle informazioni

centralizzate relative alle risorse aziendali, condivise all'interno di una rete di computer. Un esempio di LDAP è quello in Figura 8:

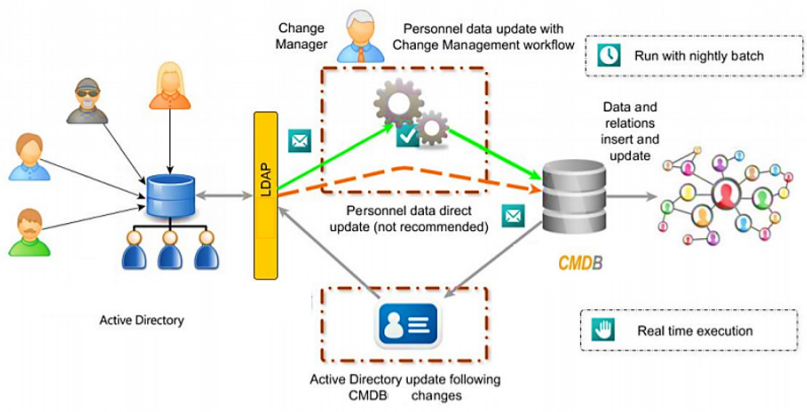

Figura 8 - Esempio di Lightweight Directory Access Protocol

- Il *Source Specific Multicast,* SSM, che specifica il perimetro in cui sono riconosciute le sorgenti e le destinazioni affidabili per la rete;

- Connettori di *software* specifici, come ad esempio con l'infrastruttura virtuale VMWare®. Un esempio è quello riportato in Figura 9:

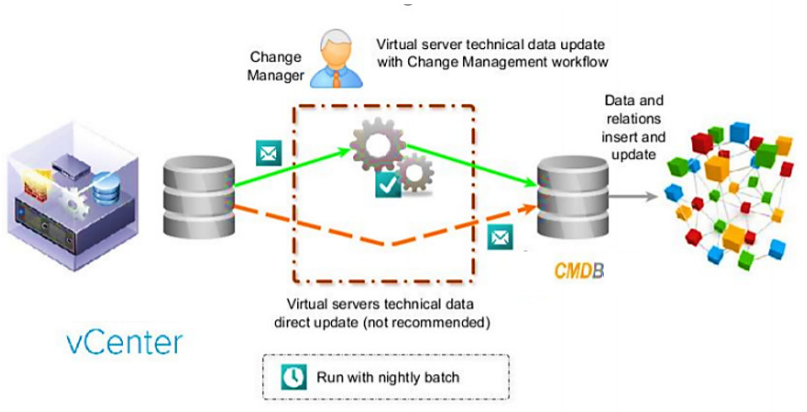

Figura 9 - Esempio di un connettore con un vCenter

- Il *System Center Configuration Manager,* SCCM, di cui Microsoft® ne è proprietario, che è un elenco di *software* installati sui server Windows®.

2) L'archivio di configurazioni memorizzato deve funzionare come una base dati relazionale. Come già spiegato in precedenza, i dispositivi sono fortemente dipendenti l'uno dagli altri, per cui potrebbe essere necessario esaminare le informazioni di elementi correlati nel processo di risoluzione dei problemi all'interno dell'infrastruttura o, semplicemente, nell'ordinario flusso di lavoro di gestione e monitoraggio. Si può considerare come esempio un consueto piano di aggiornamento: il responsabile della rete deve conoscere l'appropriatezza o meno delle versioni dei sistemi operativi nonché della disponibilità di memoria sofficiente a procedere con l'aggiornamento. Ciò è facilmente e velocemente ottenibile tramite *query* al *Configuration Management Data Base*. Sfruttando questo strumento di ricerca, quindi, si riescono a prendere delle decisioni in maniera consapevole e prevedendo gli impatti sia in termini tecnici che di costi.

3) La continua crescita della rete e della sua struttura comporta un incremento del numero di dispositivi coinvolti, quindi un aumento delle configurazioni da governare, le quali subiscono continui cambiamenti che devono essere registrati e gestiti. Il *Configuration Management Data Base* viene quindi utilizzato anche come archivio storico, dal momento che i *manager* possono trovarsi nella posizione di dover confrontare vecchie configurazioni con le nuove. In particolare, è necessario considerare che, essendo gli elementi della rete fortemente correlati tra loro, si potrebbero avere effetti non previsti dovuti ai cambiamenti di configurazione: avendo a disposizione un archivio accurato di informazioni, una vera e propria cronologia delle modifiche, è quasi immediato il ritorno alla situazione precedente l'aggiornamento, risolvendo immediatamente o quasi le problematiche riscontrate e ricominciare dal processo di analisi iniziale.

4) Le informazioni di configurazione archiviate devono poter essere accessibili a tutte le figure coinvolte nella gestione dell'infrastruttura. Tali dati, infatti, possono essere utilizzati per la progettazione della rete, oltre che per la visualizzazione dei diagrammi della stessa. La mappatura della rete, fotografia di quest'ultima in tempo reale, può essere esportata, infatti, ad altri strumenti di gestione, di progettazione o di test. Essa può essere quindi utilizzata come modello di base nel processo di implementazione dell'infrastruttura, avendo così la possibilità di analizzare i vari scenari possibili e confrontare le prestazioni delle alternative realizzabili. Coerentemente con quanto detto in precedenza, la configurazione dello scenario che si decide di concretizzare verrà poi registrata nel CMDB, successivamente all'applicazione dello stesso.

5) Il *Configuration Management Data Base* può essere utilizzato anche nella gestione degli *asset IT*. Le informazioni contenute al suo interno, infatti, includono tutte le informazioni relative a questi ultimi: locazione, identità e contatti del responsabile del dispositivo in esame, numero degli *asset* assegnati dall'organizzazione coerentemente alle regole di gestione degli stessi. Si tratta di informazioni essenziali per la gestione finanziaria e, quindi, per l'organizzazione del budget da destinare alla gestione dell'infrastruttura IT dell'azienda.

6) È necessario che le informazioni contenute nel *Configuration Management Data Base* siano accessibili in modalità "visualizzazione", più facilmente consultabile rispetto alle tradizionali viste topologiche. Queste ultime infatti acquisiscono complessità proporzionalmente al numero sempre crescente di reti e dispositivi da tenere in considerazione. La visualizzazione consente, infatti, al gestore della rete e degli *asset* di avere un quadro completo dell'architettura e della situazione attuale nell'esplorazione dei set di dati archiviati.

3.4.2 Ruolo all'interno di un'organizzazione

Sulla base di quanto trattato in precedenza, è immediato rendersi conto di quanto tale strumento possa essere essenziale nel gestire gli *asset* nella loro totalità.

Il *Configuration Management Data Base* è uno strumento che può essere reso accessibile a qualsiasi utente, con le dovute precauzioni, che sia interessato ad assicurarsi una certa consapevolezza dell'infrastruttura allo stato attuale.

Trattandosi di un archivio completo di qualsiasi tipo di informazione relativo agli apparati, siano essi in utilizzo o già dismessi, diventa la base più attendibile per poter elaborare analisi approfondite sullo stato attuale dei sistemi e sull'evoluzione che essi hanno avuto nel tempo all'interno dell'organizzazione.

Su tali valutazioni, infatti, possono essere stilati *report* indirizzati al Regolatore o al *Bord of Director*, diventando quindi strumento di supporto alle decisioni strategiche e operative dell'azienda. Sono proprio queste decisioni a far sì che essa possa acquisire un vantaggio competitivo nei confronti dei concorrenti e procurarsi una posizione di rilevanza sul mercato.

3.5 Il CMDB nella gestione dell'obsolescenza

Il *Configuration Management Data Base* è uno strumento cardine a supporto della gestione degli *asset* IT, in particolare nel monitoraggio del relativo ciclo di vita e, di conseguenza, nella gestione dell'obsolescenza di tutti gli apparati presenti nell'infrastruttura aziendale.

Tra le informazioni archiviate, infatti, ci sono anche quelle relative allo stato di obsolescenza di ogni dispositivo, all'*End Of Life* e all'*End Of Support,* nonché alle date di acquisto.

Le date indicati in questi campi sono quelle di riferimento per la pianificazione delle implementazioni, migrazioni o sostituzioni. Ciò significa che è sulla base di questi dati che viene stilato anche il *budget*, tra cui quello destinato alla risoluzione delle problematiche relative all'obsolescenza.

Dal momento che si è in precedenza parlato di automatizzazione del sistema relativamente alla gestione dell'obsolescenza, il *Configuration Management Data*

Base è uno strumento che supporta tale attività. Infatti, supporta delle configurazioni software che consentono di gestire operazioni informatiche in autonomia e notificare all'utente responsabile della gestione degli *asset* le informazioni rientranti in un perimetro definito in partenza.
Particolarmente interessante può essere la notifica, tramite ad esempio un'e-mail di *alert*, riguardante lo stato dell'invecchiamento degli *asset* che, chiaramente, devono essere gestiti nella loro interezza.
Tale funzionalità risulta essere particolarmente utile quando ci si trova a gestire infrastrutture di una certa portata e quando i responsabili di questa gestione ricoprono ruoli di responsabilità tali da non poter dedicare completamente il proprio tempo alla sola obsolescenza.

Avendo anche indicazioni circa tutte le relazioni tra i vari apparati, è possibile non solo definire gli impatti sul singolo componente, ma anche quelli che un qualsiasi cambiamento possa avere in un perimetro più ampio. Inoltre, è proprio grazie alla presenza di queste informazioni, che, in caso di malfunzionamenti o disservizi causati dallo stato obsolescente, viene semplificato anche il processo di *troubleshooting*[117].

Tra le informazioni da inserire all'interno del CMDB, come descritto ampliamente nel paragrafo precedente, ce ne sono due essenziali per la gestione dei sistemi complessi:

- Configurazione degli apparati

- Correlazione tra gli *asset*

Si ritiene opportuno sottolineare che l'obsolescenza a livello *hardware* non presuppone quella del *software* installato sullo stesso e viceversa.

[117] Con *troubleshooting* si indica quel processo di risoluzione e comprensione delle problematiche, necessario nello sviluppo e nel mantenimento di sistemi complessi, al fine di trovare la causa origine di disservizi e malfunzionamenti.

Ad esempio, un'*end of life* dell'apparato fisico può non corrispondere allo stato di invecchiamento del *software* ivi installato. Si potrebbe infatti avere un *software* aggiornato all'ultima versione, installato su un *hardware* obsoleto. Parallelamente, si ci si può imbattere in un *hardware* relativamente nuovo, ma su cui è configurato un *software* le cui *versioning* e *patch* installate non sono adeguate al soddisfacimento dei requisiti di sicurezza e *performance* desiderati.

Focalizzando l'attenzione sulla gestione dell'obsolescenza, è fondamentale puntare l'attenzione su alcune componenti caratterizzanti il *Configuration Management Data Base*, in particolare:

- Stesura automatica di *report* su perimetri individuati a priori tramite *query* predefinite

- Utilizzo di *dashboard* che consentono una panoramica globale dello stato attuale degli *asset*

Sono proprio queste le principali informazioni su cui si basano le decisioni strategiche aziendali, dal momento che si tratta dei dati ufficiali relativamente all'infrastruttura informatica dell'intera organizzazione.

CAPITOLO 4 – Caso pratico: Santander Consumer Bank

Nell'ultimo capitolo di questo lavoro, si illustra il caso pratico di Santader Consumer Bank, come applicazione della teoria esplicata nei capitoli precedenti.
Verranno quindi illustrati le modalità di gestione in essere prima dell'acquisizione del *Configuration Management Data Base* e gli impatti che quest'ultimo ha avuto nell'organizzazione.

Si tratterà, quindi, di descrivere i cambiamenti relativamente alla gestione degli *asset* e la riguardante obsolescenza, nel rispetto delle *policy* aziendali.
Si esporranno anche le motivazioni delle scelte effettuate in ottica strategica.
In questo capitolo, si affronteranno anche i temi strettamente operativi che hanno caratterizzato il lavoro di tirocinio e come questo si è evoluto nel tempo.
Si riporteranno, inoltre delle evidenze sui risultati ottenuti dai cambiamenti apportati nella gestione degli *asset*, supportati dall'utilizzo proprio del CMDB.

4.1 Chi è Santander Consumer Bank

Santander Consumer Bank fa parte di un gruppo bancario mondiale che pone le sue origini in Spagna, con sedi disseminate in tutta Europa.

Considerando il territorio italiano, sono presenti 21 filiali fisiche, ciascuna per le principali città, a cui vanno aggiunti i numerosissimi agenti sparsi per tutta la penisola.

Santander Consumer Bank è una finanziaria specializzata in:

- Prestiti personali
- Cessione del Quinto
- Conti Deposito

- Trattamento di fine servizio
- Carte di credito
- Acquisti a rate
- Assicurazioni
- Leasing

In particolare, è in quest'ultima area di mercato che vede il suo *business* maggiore, avendo stipulato accordi di forte rilievo con i colossi dell'*automotive* che l'hanno resa *leader* di settore.

Esaminando l'organizzazione da un punto di vista interno, essa è strutturata in 9 Direzioni, i cui responsabili dipendono direttamente dall'Amministratore Delegato. Ciascuna Direzione è composta da più Servizi, ognuno dei quali suddiviso in uffici indipendenti.
Questo lavoro è frutto della collaborazione realizzata con il Servizio IT, il quale si scompone degli uffici di:

- Architetture IT[118]
- Governance IT[119]
- Demand Management[120]
- Delivery Management[121]

[118] Le Architetture IT sono l'ufficio di riferimento per il governo della struttura del sistema informatico dell'organizzazione, includendo anche le linee guida per la progettazione e l'implementazione dello stesso.

[119] Come già descritto ampiamente nel capitolo 3 di questa trattazione, la Governance IT assicura l'attuazione delle politiche aziendali e la corretta esecuzione dei processi.

[120] L'ufficio di Demand Management è quello che fa da tramite tra le richieste e le esigenze del *business*, lato utente, e l'area tecnico-informatica dell'organizzazione.

[121] Il Delivery Management è l'ufficio preposto agli sviluppi *software* dell'organizzazione e alla messa in produzione nell'ambiente di utilizzo definitivo.

4.2 Gestione degli asset IT e dell'obsolescenza prima del CMDB

La gestione degli *asset IT* all'interno di Santander Consumer Bank doveva basarsi sul rispetto delle *policy* aziendali, che prevedono la contemporanea attenzione alle *policy* di *cyber-security* e *technological risk*. Tuttavia, la tipologia di gestione degli apparati informatici non consentiva il rispetto totale delle politiche dettate dalla Capo Gruppo.

La gestione dell'obsolescenza era un processo completamente manuale che non prevedeva il supporto di alcun *tool* che semplificasse il controllo. Anche gli strumenti di monitoraggio utilizzati, come ad esempio i *software* di monitoraggio della rete, non erano sufficienti per garantire l'automatizzazione del processo, ma erano una semplice strumentazione di base da cui ricavare qualche informazione utile.
Il controllo, infatti, avveniva sfruttando strumentazioni di base come, ad esempio, fogli *Excel*[122] o *database Access*[123]. Si trattava di *file* non sempre aggiornati con informazioni complete e, soprattutto, ogni funzione aziendale gestiva in maniera autonoma la propria documentazione.

Il primo effetto di questo disallineamento era il mancato governo degli *asset IT* e l'inconsapevolezza dello stato degli stessi. A questo si aggiungeva, quindi, l'incapacità di agire proattivamente nei confronti dei fornitori sia degli *asset* che della loro manutenzione, i quali erano soliti presentarsi al termine dei contratti in atto con le offerte di rinnovo per gli anni seguenti. La *Governance IT*, infatti, era costretta spesso ad accettare condizioni contrattuali non ottimali per non rischiare la mancata copertura manutentiva e/o assicurativa dei propri beni.

[122] Excel è un programma sviluppati da Microsoft®, dedicato alla produzione e alla gestione di fogli di calcolo elettronici. https://it.wikipedia.org/wiki/Microsoft_Excel

[123] Access è un'interfaccia software sviluppata da Microsoft® per la gestione di basi di dati di tipo relazionale. https://it.wikipedia.org/wiki/Microsoft_Access

Da un punto di vista prettamente tecnico, l'implementazione e la sostituzione di apparati ormai obsoleti avveniva esclusivamente quando ci si ritrovava ad affrontare *crash* degli stessi e quando, tramite operazioni di *troubleshooting*, si risaliva all'invecchiamento dei dispositivi e dei *software* impiegati come causa dei malfunzionamenti o disservizi e/o blocchi dell'operatività.

4.2.1 Criticità

Descritte le modalità di gestione in uso abitualmente in azienda, è semplice intuire quali possano essere state le criticità più rilevanti.

Il primo problema in cui ci si imbatteva era la carenza di informazioni aggiornate alla situazione reale. Questa mancanza provocava una forte inconsapevolezza relativamente allo stato effettivo dei dispositivi appartenenti all'infrastruttura. La diretta conseguenza era che non ci si poteva approcciare in una maniera proattiva, ma si poteva solo risolvere i malfunzionamenti e i disservizi che improvvisamente si presentavano durante l'operatività normale.
Parallelamente alle carenze lato *hardware* e *software*, si trovavano anche mancanze dal punto di vista degli aggiornamenti lato applicazioni. In molti casi, infatti, l'IT non era al corrente di alcuni applicativi utilizzati dai propri colleghi, quando essi si rapportavano in autonomia ai fornitori esterni per l'acquisizione di *tool* particolari. Tale inconsapevolezza era principalmente dovuta al fatto che non fosse necessario provvedere a cambiamenti infrastrutturali, ma fosse sufficiente una semplice installazione nei sistemi già dedicati a tali uffici.

La seconda conseguenza del mancato allineamento tra gli uffici era l'incoerenza dei dati condivisi con la Sede Centrale di Madrid. Trattandosi di dati ufficiali, questo comportava un susseguirsi di controlli da parte dell'auditoria sia interna che esterna, al fine di chiarire lo stato reale delle cose. L'effetto era l'impiego di tempo e risorse per la correzione delle informazioni scorrette o non aggiornate, aumentando così le attività di ogni ufficio coinvolto.

La terza criticità va individuata nelle difficoltà in cui si imbatteva la *Governance IT*, sia nella gestione dei rapporti con i fornitori, sia nella definizione del *budget* destinato alla gestione dell'obsolescenza e, più in generale, alla gestione degli *asset*:

- Come anticipato nel paragrafo precedente, una questione da tenere in considerazione è l'incapacità nell'eseguire correttamente i processi definiti nelle *policy* aziendali, in questo caso specifico quelle riguardanti la gestione degli *asset*, comportandone quindi il mancato rispetto.

- Nel rapporto con i fornitori, non possedendo un governo totale nella gestione, la *Governance IT*, nella maggioranza dei casi era costretta ad accettare termini contrattuali poco ottimali, al fine di scongiurare i pericoli derivanti da un mancato supporto tecnico e/o manutentivo degli apparati. Questo significava avere un basso potere contrattuale nei confronti dei fornitori esterni, una situazione sicuramente non ideale per una grossa società nella gestione del proprio capitale.

- Diretta conseguenza dei punti precedenti è la difficoltà nella definizione del *budget*. Le previsioni di quest'ultimo, infatti, risultavano falsate e poco giustificabili al *Bord of Director*, che richiedeva un livello di dettaglio e specifiche che non sempre erano raggiungili nell'immediato, ma richiedevano un'analisi da parte delle risorse responsabili degli apparati informatici, il cui lavoro era spesso schedulato per coprire l'elevato numero di richieste da soddisfare, necessarie per l'avanzamento di progetti fondamentali per il *business* aziendale.

Una quarta problematica può trovarsi nella gestione dei malfunzionamenti e dei disservizi. Adottando, infatti, una strategia di tipo reattivo, non si era in grado di prevedere eventi che causassero rallentamenti o blocchi nello svolgimento delle attività cardine dell'azienda.

La diretta conseguenza era un numero enorme di *incident*[124] da gestire. In particolare, vigeva uno stato di emergenza nel caso in cui essi si verificavano, dovendo provvedere alla risoluzione di tali problematiche, parallelamente alle attività già schedulate e con *deadline* incombenti. Una gestione di questo tipo comportava un notevole dispendio di tempi e risorse, sprechi che si sarebbero potuti evitare con una gestione ottimizzata.

Una delle cause principali di queste difficoltà va sicuramente ritrovata nella mancata osservanza delle linee guida dettate dall'ITIL, da cui derivano la gran parte delle *policy* relative alla funzione IT dell'organizzazione.

4.2.2 Le risoluzioni delle criticità

Il primo punto da tenere in considerazione e che genera gran parte delle problematiche riscontrate all'interno dell'organizzazione è la mancanza di conformità con le linee guida dell'ITIL, che definiscono degli standard riconosciuti per la gestione della funzione IT.
Avendo carenze di questo tipo, la strategia pensata dall'azienda per migliorare l'approccio a queste tematiche è stato quello di investire nella formazione delle risorse direttamente coinvolte nella funzione dell'IT, dando la possibilità di seguire il corso per l'acquisizione della certificazione ITIL.
Parallelamente, considerati anche i solleciti da parte dell'auditoria interna e della Sede Centrale di Madrid, era necessario inserire all'interno dell'infrastruttura informatica un *Configuration Management Data Base*, di cui si descriveranno i dettagli nei paragrafi seguenti.

L'esigenza di soddisfare tale richiesta era comunque direttamente legata alle attività di allineamento con le linee guida fornite dall'ITIL. Come teoricamente trattato nei

[124] La definizione di *incident* si riprende dall'ITIL. Si tratta di un'interruzione non pianificata di un Servizio IT o una riduzione della Qualità di un Servizio IT. Anche il guasto su un Elemento della Configurazione (CI) che non ha ancora impattato un Servizio viene considerato un incidente.

capitoli precedenti, infatti, è proprio l'ITIL a richiedere la presenza di un CMDB per la gestione degli *asset* IT.

Il primo passo è stato, quindi, effettuare un *assessment*, al fine di valutare le varie soluzioni adottabili da un punto di vista tecnico, che andassero a sposarsi il più possibile con le esigenze di acquisizione del controllo degli *asset IT* e, contemporaneamente, con i vincoli di budget esistenti.

Per poter effettuare *l'assessment* si è reso necessario raccogliere il maggior numero di informazioni possibili circa gli *asset* di cui la banca era proprietaria o di cui ne usufruiva operativamente, anche se di proprietà di terze parti.
I dati recuperati erano riguardanti sia il numero degli *asset* in utilizzo che tutti i dettagli ad essi relativi.
Il lavoro, in questa prima fase, è stato quindi un lavoro di raccolta che ha visto coinvolti tutti gli uffici di Santander Consumer Bank.

Per collezionare i dati in un tempo più breve possibile, si sono schedulati degli incontri con i responsabili di ciascuna divisione aziendale, evitando la mera condivisione di file, di cui presumibilmente si sarebbero dovuti richiedere chiarimenti.
Prima di procedere al coinvolgimento individuale, si è strutturato un *template* che ha fatto da base per i quesiti da porre ai colleghi che condividevano le informazioni in loro possesso.
La struttura di questo documento prevedeva la richiesta di dati basilari per la definizione della mappatura dei sistemi informatici oggetto d'esame.

La raccolta è stata effettuata su due fronti, ognuno dei quali prevedeva indicazioni richieste differenti:

- Lato applicativi
  Per poter effettuare una raccolta completa degli applicativi, sia proprietari che di terze parti, in utilizzo in Santader Consumer Bank, si è fatto ricorso

alle risorse maggiormente operative di ciascun ufficio. In particolare, si è fatto riferimento agli utenti finali, direttamente coinvolti nell'utilizzo di tali strumenti per lo svolgimento del lavoro normale. A sostegno di questa strategia c'è la considerazione che i dati di dettaglio potevano essere forniti solo dagli utenti finali e, al limite, dai fornitori con cui intrattenevano collaborazioni commerciali.

Le informazioni richieste per questi strumenti sono state le seguenti:

- Nome della soluzione
- Breve descrizione funzionale
- Proprietà dell'applicativo: se di Santander Consumer Bank o di terze parti: questa informazione non sempre si è riusciti ad ottenerla dall'utente finale, ma si è dovuto fare un passaggio tecnico con i sistemisti del *Delivery Management* e uno di business con i referenti del *Demand Management*
- Direzione di riferimento
- Ufficio specifico
- Responsabile commerciale
- Responsabile operativo
- Amministratore di sistema: per questa informazione vale il medesimo discorso fatto per la proprietà dell'applicativo
- Fornitore di riferimento, quando conosciuto
- Se necessario l'accesso tramite le utenze di rete
- Numero di utenti che lo utilizzano
- Necessità di avere delle licenze collegate allo strumento: in questo caso, quando le informazioni non erano reperibili presso gli utenti finali, si è fatto riferimento alla *Governance IT*
- Frequenza di utilizzo della soluzione
- Eventuale utilizzo per elaborazione dati ufficiali
- Intervallo di tempo in cui si potrebbe fare a meno della soluzione in termini operativi

- Percorso per il raggiungimento dell'applicativo (se web, cartella condivisa, applicativo direttamente installato su pc)

- Lato infrastrutturale

  Dal punto di vista *hardware* e *software* ci si è incentrati principalmente nelle funzioni di *Delivery Management*. In particolare, si è lavorato a stretto contatto con l'ufficio *Networking*, tramite cui si sono ricavate tutti i dettagli delle relazioni presenti tra gli apparati informatici presenti nella rete infrastrutturale di Santander. Sulla base delle considerazioni descritte nei capitoli iniziali, è facilmente intuibile come queste informazioni fossero più facilmente ricavabili in questo ufficio, dal momento che è in esso in cui sono presenti i responsabili delle configurazioni degli apparati. Senza il loro lavoro, infatti, sarebbe impossibile utilizzare tali *asset* e avviare le attività da essi dipendenti.

  In questo secondo caso, le informazioni di base richieste sono state:

  - *Hostname*
  - Breve descrizione del sistema
  - Indirizzo IP
  - Ambiente (Test/Sviluppo, Collaudo/Preproduzione, Produzione)
  - Numero di serie
  - Proprietà dell'apparato: se di Santander Consumer Bank o di terze parti
  - Marca
  - Modello
  - Tipologia dell'*asset* (ad esempio *firewall*, *switch*, *server, workstation*)
  - Responsabile dell'*asset*
  - Fornitore
  - Locazione

Sulla base delle informazioni raccolte, si è riusciti quindi a definire un perimetro realistico per poter:

- Avanzare le richieste ai fornitori esterni
- Acquisire consapevolezza del lavoro che effettivamente doveva essere svolto
- Stimare realisticamente tempi e costi
- Effettuare analisi realistiche senza rischiare di dover procedere a revisioni contrattuali per sopperire a eventuali mancanze derivanti dalla prima fase.

4.2.3 Mappa di rete di Santander Consumer Bank

Al fine di semplificare la comprensione dei paragrafi successivi, si ritiene necessario descrivere, anche se in un'ottica di alto livello, l'architettura informatica di Santander Consumer Bank.
Per motivi di privacy non è possibile pubblicare la mappa architetturale, tuttavia possono essere presentate le tipologie di *asset* presenti all'interno dell'infrastruttura.

La classificazione di riferimento per gli apparati informatici, la Sede Centrale di Madrid propone una suddivisione secondo le funzionalità coperte dai vari dispositivi, aggregando così in classi leggermente differenti dallo standard.

Di seguito, il dettaglio:

- *Communication asset*
  In questa categoria rientrano tutti gli elementi di comunicazione presenti all'interno dell'infrastruttura informatica della rete, relativi a tutti gli ambienti di lavoro

- *Hypervisor asset*
  Il nome della categoria è assolutamente esplicativo degli apparati coinvolti. In essa, infatti, viene considerato il numero totale degli *hypervisor*, tenendo in considerazione la natura virtuale degli stessi. Si tratta, per l'appunto, di *virtual server*.

- *High-Ends asset*
  Questa classe fa riferimento ai sistemi *High-Ends*, ossia *iSeries*/AS400, di tutti gli ambienti di lavoro. Il *focus* è sicuramente sui sistemi core del sistema bancario.

- *End-user asset*
  In questa categoria rientrano tutte le tecnologie *end-user*, che, in via molto pratica, possono riassumersi con i computer e *laptop* utilizzati dai dipendenti o forniti come strumentazione ai collaboratori esterni.

- *Storage asset*
  La classe degli *storage*, anche in questo caso piuttosto esplicativa, considera il numero totale delle componenti *storage* integrate nell'architettura informatica di ogni ambiente dell'azienda. Si tratta quindi degli elementi informatici a supporto dell'archiviazione dei dati di qualsiasi tipo, assolutamente fondamentali per una finanziaria.

Le relazioni esistenti tra tutti gli apparati sono perfettamente coerenti con quanto descritto nel secondo capitolo di questo lavoro.

4.3 Il CMDB in Santander Consumer Bank

Come già trattato nel capitolo 2.4, il *Configuration Management Data Base* è la soluzione che consente di semplificare la gestione degli *asset IT* all'interno di un'infrastruttura informatica.
L'esigenza immediata di Santander Consumer Bank di creare un CMDB da zero poteva essere soddisfatta in due modi:

- Con lo sviluppo interno
  Questa soluzione prevedeva, ovviamente, il coinvolgimento del gruppo di sviluppo dell'IT, le cui risorse, però, non potevano sostenere l'*effort* richiesto nei tempi desiderati, a causa della compresenza di altri progetti in essere.

- L'acquisizione da terze parti
  Questa seconda alternativa prevedeva lo stabilire un contratto di collaborazione con un fornitore esterno, che si sarebbe occupato dello sviluppo del *tool*, sulla base delle richieste ed esigenze avanzate da Santander Consumer Bank.
  Si è rivelata la soluzione più veloce, nonostante i tempi necessari per poter effettuare il confronto tra aziende concorrenti e le analisi delle alternative ottenute dalla gara d'appalto, seguite all'*assessment* e al *benchmark* effettuato.

Nel mercato sono presenti numerosi fornitori che offrono ciascuno il proprio prodotto, puntando ognuno a caratteristiche diverse, così da differenziarsi dai concorrenti, e puntando sulla customizzazione dello stesso, sulla base delle esigenze esposte dal cliente.

Nel caso di Santander Consumer Bank si sono esaminate tre proposte. Le aziende, nei termini di rispetto della privacy, verranno identificate con le denominazioni Alfa S.p.A, Beta S.p.A e Gamma S.p.A., con i corrispondenti CMDB Alfa, CMDB

Beta e CMDB Gamma, la cui analisi verrà effettuata nel dettaglio nei paragrafi 4.3.2, 4.3.3, 4.3.4, successivi alle motivazioni della scelta effettuata nel paragrafo 4.3.1.

4.3.1 Motivazioni della scelta della soluzione

Per poter effettuare la scelta dell'alternativa migliore, sono stati considerati sia aspetti tecnici che economici. È stato ovviamente necessario valutare anche la compatibilità dei *software* proposti con le norme di *security* imposte dalla Sede Centrale di Madrid.

4.3.1.1 Aspetti tecnici

Tra gli aspetti tecnici da tenere in considerazione ci sono sicuramente il *software* utilizzato e gli impatti che avrebbe avuto a livello *hardware*.

Relativamente al *software*, di fondamentale importanza era utilizzare programmi e applicativi aggiornati, anche per essere coerenti con le esigenze da cui nasceva tale richiesta. Le versioni del sistema operativo utilizzate dovevano quindi essere non obsolete, o comunque relativamente lontane dalle proprie *End Of Life* e *End Of Support*. Equivalentemente, anche le versioni dei servizi necessari, come ad esempio IIS o SQL, al funzionamento dello strumento dovevano rispettare le medesime condizioni.
Considerando ciò che rientra nel perimetro del *software* da noi considerato, i vincoli imposti sono stati:

- Sistema operativo
    - Caso Windows®: la versione minima accettata sarebbe stata la Windows NT 6.3 (maggiormente conosciuta come Windows 8.1 o Windows Server 2012 R2)
    - Caso Linux®: la versione minima accettata sarebbe stata una pari alla Red Hat 6 o Ubuntu 8.04

- *Database*
  La versione minima accettabile è stata ritenuta una almeno pari al SQL 2016 *Service Pack* 1 o PostgreSQL 9.4.11

- *Web application*
  La versione minima accettabile sarebbe stata una pari all'IIS 7.0 o Tomcat 8.0

Si sono definite delle versioni minime, anche se quasi al termine del loro ciclo di vita, per semplificare la compatibilità tra i sistemi e riuscire a configurare anche funzionalità aggiuntive, non ancora adeguate alle nuove versioni, considerati i tempi estremamente stringenti.

Nel caso in cui le versioni fossero pari alle minime, si sarebbe comunque pensato a una pianificazione per l'implementazione entro le date di *End Of Life* ed *End Of Support*.

Le considerazioni fatte per il *software* hanno avuto ovviamente forti impatti lato *hardware*. Infatti, l'eventuale necessità di avere una macchina dedicata, in questo caso si sarebbe trattato di un *server* virtuale, doveva tenere in considerazione tutte le esigenze di rispetto in termini di obsolescenza, come descritto ampliamente in precedenza, sia per il sistema operativo installato, che per tutti gli eventuali *database* o *web application* configurati.

Una volta definiti *hardware* e *software*, si è dovuto anche considerare gli impatti che determinate installazioni avrebbero avuto nell'infrastruttura, così come anche la compatibilità con i sistemi già in utilizzo.

È bene sottolineare che era indispensabile non trascurare gli aspetti riguardanti le risorse necessarie al funzionamento degli applicativi. Nel caso dell'*hardware*, ad esempio, era imprescindibile considerare i *range* di RAM, CPU e spazio disco richiesti dalla società esterna per soddisfare le richieste di Santander Consumer

Bank, al fine di scongiurare pericoli di insufficienza delle stesse, nonché per verificare che effettivamente si avessero a disposizione tali risorse. La mancanza di queste ultime, infatti, avrebbe generato un fermo del sistema e, di conseguenza, un disservizio per tutti gli uffici della Sede Centrale Italiana.
Medesimo discorso può essere semplicemente riportato anche dal punto di vista *software*.

Un altro elemento tecnico da valutare erano sicuramente alcune funzionalità dello strumento a disposizione. In particolare, avendo l'esigenza di acquisire i controllo totale degli *asset* nella loro totalità, quindi anche dal punto di vista relazionale, era necessario che lo strumento fornisse la possibilità di andare a definire delle relazioni tra le righe delle tabelle di tipo 1:1, 1:n, n:n, a seconda dell'apparato considerato e delle esigenze della classe di appartenenza, delle informazioni disponibili in quel momento, nonché quelle potenzialmente disponibili in futuro.

Un ulteriore aspetto riguardava la possibilità di customizzare lo strumento, sulla base delle esigenze della finanziaria e delle informazioni a disposizione.
In alcuni casi, infatti, si è riusciti a raccogliere più informazioni rispetto alle minime richieste. Per tale motivo, al fine di evitare una perdita notevole e uno spreco dell'*effort* apportato nella fase precedente, era necessario poter implementare il tool come desiderato, valorizzando nuovi campi che si sarebbero aggiunti in fasi successive a quella iniziale di *data entry*.
A sostegno di questa esigenza c'era anche quella di mappare alcune informazioni necessarie alla stesura di reportistica destinata al Regolatore o al *Board of Director*. Avendo un archivio di tutte le informazioni relative agli *asset IT*, infatti, si è ritenuto opportuno considerare la possibilità di inserire anche quelle non prettamente tecniche all'interno delle classi, così da avere una visione globale dell'infrastruttura informatica e dello stato della stessa.

Un elemento tecnico aggiuntivo da non trascurare è stato quello relativo agli accessi effettuabili allo strumento. Era necessario, infatti, che tutti gli attori interessati alla visione dello stato attuale dell'infrastruttura potessero avere libero accesso al *tool*,

al fine di effettuare ciascuno le proprie analisi, mantenere coerenza nei report ufficiali, sfruttando la medesima base dati, evitare un disallineamento tra gli uffici ed evitare che gli uffici lavorassero in via totalmente autonoma nella manipolazione dei dati, col rischio di mancati aggiornamenti e analisi non realistiche.

Parallelamente agli accessi da parte degli utenti, è stato indispensabile considerare l'eventuale possibilità di accesso per il funzionamento di alcuni connettori che consentono l'aggiornamento automatico di alcune informazioni. Esempi a tal proposito possono essere l'SNMP, l'LDAP, l'SCCM, descritti nel capitolo precedente di questo lavoro.

Come ultimo aspetto di cui tenere conto, si è valutata la possibilità di avere una GUI, *Graphical User Interface*, ossia un'interfaccia grafica, di alto livello, basata sulle informazioni presenti all'interno del *database* di *configuration management*, sicuramente maggiormente *user-friendly* rispetto a un applicativo presumibilmente impostato sulla scia dei *database* informatici. Non era elemento indispensabile, ma sicuramente generava un *surplus* e rappresentava un vantaggio rispetto ai concorrenti che invece non inserivano tale possibilità all'interno della propria offerta. La richiesta era dovuta alla possibilità di presentare anche al *Bord of Director* gli avanzamenti e il monitoraggio nella gestione degli *asset IT*, evitando schermate di presentazione eccessivamente tecniche e, quindi, poco chiare a figure di alto livello.

4.3.1.2 Aspetti economici

La prima considerazione da fare relativamente agli aspetti economici riguarda sicuramente il *budget* a disposizione. Esso infatti non era illimitato, ma doveva essere comunque inferiore ai 60k€, cifra entro cui doveva rientrare anche l'eventuale supporto manutentivo successivo alla messa in produzione dello strumento acquistato.

È quindi sulla base della cifra definita dalla *Governance IT* che si è valutato le offerte ricevute dai fornitori partecipanti alla gara d'appalto.

Nel *budget* stabilito bisognava considerare anche la possibilità di ottenere supporto sotto due punti di vista:

- Supporto relativo alle modalità d'uso dello strumento, quindi anche la fornitura di eventuali manuali di utilizzo

- Supporto tecnico per la risoluzione di *bug*, per eventuali modifiche del codice o per l'implementazione delle versioni quando necessario

Inoltre, è stato inevitabile considerare l'eventuale necessità di acquisto di licenze per l'utilizzo dello strumento e degli applicativi in esso installati.

4.3.1.3 Compatibilità con gli standard aziendali

In un'ottica di soddisfacimento delle esigenze presentate dall'organizzazione, nonché dei requisiti necessari all'avanzamento del progetto, elementi assolutamente da non trascurare sono quelli riguardanti:

- Le *policy* definite dalla Sede Centrale di Madrid

- Le *policy* di *cyber-security*

Il presupposto è sicuramente burocratico, perché, se esse non vengono rispettate, gli sviluppi non possono procedere in quanto non autorizzati. Tuttavia, esse hanno degli impatti decisivi dal punto di vista tecnico relativamente a:

- Architettura del sistema da installare

- Configurazione degli apparati

- Grado di obsolescenza degli applicativi installati

- Assegnazione delle responsabilità riguardanti gli *asset* in esame

4.3.1.4 Criteri di benchmark: le valutazioni su costi e benefici

Nella valutazione delle alternative possibili, si è tenuto conto di tre aspetti fondamentali:

- Il perimetro delle attività e gli output attesi da Santander Consumer Bank
- L'approccio, il piano di lavoro e le ipotesi alla base della pianificazione, considerando quindi i relativi tempi di sviluppo
- I costi progettuali

Il primo elemento di valutazione è stata la verifica che tutte le esigenze richieste da Santander Consumer Bank fossero rispettate dal punto di vista tecnico. In particolare, doveva essere chiaro quali attività sarebbero state in carico al fornitore e quali, invece, in carico alle risorse della finanziaria. Tali risorse, presumibilmente, sarebbero state individuate tra i tecnici del *Delivery Management.*

La seconda condizione da considerare era l'esigenza di conformarsi ad una modalità di gestione degli *asset IT* ottimale che doveva assolutamente rispettare la scadenza del 31 Dicembre 2018, relativamente all'introduzione e alla valorizzazione, anche se parziale, del *Configuration Management Data Base* nell'infrastruttura aziendale.
Tale *deadline* è stata stabilita dal *management* di alto livello e condivisa con i referenti della Capo Gruppo.
Dopo tale data, si sarebbe provveduto ad aumentare il livello di dettaglio delle informazioni raccolte, alla customizzazione dello strumento adottato, all'allineamento di quest'ultimo con le esigenze degli utenti di Santander Consumer Bank e alle implementazioni che si sarebbero reputate necessarie.
Per tale motivo, nella quotazione delle proposte di collaborazione presentate, sicuramente hanno avuto un forte impatto nella decisione da prendere i tempi richiesti dai fornitori per gli sviluppi della soluzione proposta.

Come già anticipato negli aspetti economici, il terzo filtro è stato stabilito sull'importo delle offerte ricevute. L'esigenza di provvedere all'introduzione del *Configuration Management Data Base* doveva fare i conti con i vincoli di *budget* definiti dalla *Governance IT*, sulla base della disponibilità di Santander in quel momento. Tale limite, come già accennato in precedenza, è stato fissato a 60k€, comprensivi sia dell'acquisto della soluzione che del supporto manutentivo necessario per poter effettuare modifiche e implementazioni della stessa.

CAPITOLO 5 – Alternative possibili e soluzione scelta

Individuati i criteri di selezione della soluzione più opportuna, si sono valutate tre alternative possibili. Queste ultime sono state confrontate secondo i criteri descritti nel capitolo precedente.

5.1 Alternativa Alfa

La soluzione presentata da Alfa S.p.A presentava le caratteristiche di seguito illustrate.

- Aspetti tecnici
  - Sistema operativo Linux: Ubuntu 16.04
  - *Database*: PostgreSQL, versione 9.4.11
  - *Web Application*: Tomcat, versione 8.0
  - Risorse:
    - RAM: 8 GB
    - CPU: 4
    - Spazio disco: 100GB
  - Relazioni: possibili tutte le relazioni, 1:1, 1:n, n:n
  - Customizzazione possibile grazie alla presenza del doppio modulo, uno per la gestione dei dati, uno come amministratore del sistema. Nel *Data management module* avviene il caricamento degli asset e delle relative informazioni; nell' *Administration module*, invece, è possibile apportare modifiche alla struttura standard del CMDB
  - Reportistica con possibilità di customizzazione e generazione di sistema di e-mail di notifica delle informazioni richieste
  - Numero consentito di abilitazione agli accessi senza limiti

  - Integrazione con i sistemi di Santander Consumer Bank e con sistemi esterni. I connettori previsti sono del tipo LDAP e SCCM. Possibilità di inserimento di ulteriori *web service*.
  - GUI: possibilità di generare un'interfaccia grafica di alto livello

- Ulteriori funzionalità
  - Modellazione del database in forma grafica
  - Interfacce personalizzabili
  - *Import*/*export* dei dati in file in formato standard
  - Possibilità di app mobile
  - Storicizzazione dei dati
  - Schedulatore per task automatici

- Aspetti economici
  - Cifra richiesta per l'acquisto: 53k€
  - Maggiorazione del supporto manutentivo: 5k€

- Tempi di sviluppo
  - Tempi estremamente ridotti grazie a una versione pronta all'utilizzo e alla messa in produzione
  - Prevista una prima fase di test, per la verifica del corretto funzionamento delle configurazioni e dei servizi. In tale fase possono essere definite già le prime modifiche strutturali da apportare.

- Compatibilità con le *policy* aziendali
  - *Policy* di *security* rispettate
  - *Policy* di *technological risk* rispettate

5.2 Alternativa Beta

La soluzione presentata da Beta S.p.A presentava le caratteristiche di seguito illustrate.

- Aspetti tecnici
  - Sistema operativo: Windows NT 6.3
  - *Database*: MySQL, versione 5.5.60
  - *Web Application*: Tomcat, versione 8.0
  - Risorse:
    - RAM: 4GB
    - CPU: 2
    - Spazio disco: 50GB
  - Relazioni: possibili tutte le relazioni, 1:1, 1:n, n:n
  - Customizzazione possibile in via limitata. Necessario l'intervento degli sviluppatori per apportare le modifiche desiderate.
  - Reportistica con possibilità di customizzazione, sempre con supporto degli sviluppatori
  - Numero consentito di abilitazione agli accessi limitato a 50 utenti
  - Integrazione con i sistemi di Santander Consumer Bank. I connettori previsti sono del tipo LDAP per l'autenticazione.
  - GUI: possibilità di generare un'interfaccia grafica di alto livello, di tipo statico. Ciò significa che se vengono effettuati aggiornamenti all'interno del *database*, è necessario il supporto degli sviluppatori per visualizzare le modifiche apportate all'interno della GUI.

- Ulteriori funzionalità
  - Interfacce personalizzabili
  - *Import*/*export* dei dati in file in formato standard
  - Storicizzazione dei dati

- Aspetti economici
  - Cifra richiesta per l'acquisto: 30k€
  - Maggiorazione del supporto manutentivo: 0k€
  - Il supporto tecnico è previsto per il primo anno dalla messa in produzione del software

- Tempi di sviluppo
  - Tempi estremamente ridotti grazie a una versione pronta all'utilizzo e alla messa in produzione
  - Prevista una prima fase di test, per la verifica del corretto funzionamento delle configurazioni e dei servizi. In tale fase possono essere definite già le prime modifiche strutturali da apportare.

- Compatibilità con le *policy* aziendali
  - *Policy* di *security* rispettate
  - *Policy* di *technological risk* rispettate

5.3 Alternativa Gamma

La soluzione presentata da Gamma S.p.A presentava le caratteristiche di seguito illustrate.

- Aspetti tecnici
  - Sistema operativo Linux: Red Hat Enterprise Linux 7
  - *Database*: MySQL, versione 8.0.13-1
  - *Web Application*: nginx 1.12.2-2
  - Risorse:
    - RAM: 16GB
    - CPU: 8
    - Spazio disco: 250GB

  - Relazioni: possibili tutte le relazioni, 1:1, 1:n, n:n
  - Customizzazione possibile grazie alla presenza del doppio modulo, uno per la gestione dei dati, uno come amministratore del sistema. Nel *Data management module* avviene il caricamento degli asset e delle relative informazioni; nell' *Administration module*, invece, è possibile apportare modifiche alla struttura standard del CMDB
  - Reportistica con possibilità di customizzazione e generazione di sistema di e-mail di notifica delle informazioni richieste
  - Numero consentito di abilitazione agli accessi senza limiti
  - Integrazione con i sistemi di Santander Consumer Bank e con sistemi esterni. I connettori previsti sono del tipo LDAP e SCCM. Possibilità di inserimento di ulteriori web service.
  - GUI: possibilità di generare un'interfaccia grafica di alto livello

- Ulteriori funzionalità
  - Modellazione del *database* in forma grafica
  - Interfacce personalizzabili
  - *Import*/*export* dei dati in file in formato standard
  - Possibilità di app mobile
  - Storicizzazione dei dati
  - Schedulatore per *task* automatici
  - Localizzatore GPS
  - Integrazione con i sistemi di monitoraggio dello stato degli apparati
  - Sistema di log
  - Archivio documentale
  - Sistema di *ticketing* integrato
  - Sistema di gestione del personale

- Aspetti economici
  - Cifra richiesta per l'acquisto: 75k€
  - Maggiorazione del supporto manutentivo: 0k€
  - Il supporto tecnico è compreso per 3 anni dalla messa in produzione

- Tempi di sviluppo
  - Tempi relativamente ridotti. Esiste una versione pronta all'utilizzo e alla messa in produzione, ma sono necessari i tempi di integrazione delle varie funzionalità con i sistemi dell'organizzazione acquirente.
  - Prevista una prima fase di test, per la verifica del corretto funzionamento delle configurazioni e dei servizi. In tale fase possono essere definite già le prime modifiche strutturali da apportare.

- Compatibilità con le *policy* aziendali
  - *Policy* di *security* rispettate
  - *Policy* di *technological risk* rispettate

5.4 Il CMDB Alfa in Santander Consumer Bank e la relativa customizzazione

Coerentemente alle considerazioni presentate per le motivazioni che hanno portato a una scelta definitiva tra i concorrenti, la decisione è ricaduta sulla società Alfa S.p.A.

Il CMDB Alfa, infatti, soddisfaceva tutti i requisiti essenziali per il raggiungimento dell'obiettivo proposto.
Si è infatti rivelato essere il *match* giusto tra funzionalità proposte e costi progettuali.

L'alternativa proposta da Beta S.p.A, invece, presentava delle carenze dal punto di vista tecnico, nonostante fosse la proposta più allettante economicamente parlando. Tali carenze, hanno fatto deviare la scelta verso le altre alternative, considerando anche che i requisiti di sistema erano al limite di quelli previsti dalle *policy* di Santander Consumer Bank.

Il CMDB Gamma, all'opposto di quello Beta, avanzava una proposta tecnica di gran lunga superiore alle concorrenti, tuttavia risultava quasi eccessiva rispetto alle esigenze di Santander Consumer Bank. Nonostante le potenzialità estreme dello strumento e il supporto manutentivo costante, si è comunque preferito tralasciare tale offerta essendo assolutamente fuori *budget*. A sostegno di questa decisione ci sono anche le considerazioni riguardanti molte delle funzionalità aggiuntive. Infatti, molte di queste ultime già erano ottimizzati in *tool* differenti, utilizzati indipendentemente dai vari uffici. La centralizzazione di tali strumenti avrebbe generato un allungamento dei tempi di sviluppo, a causa della necessaria integrazione dei sistemi di Santander Consumer Bank.

L'introduzione del CMDB Alfa è stato il *trigger* del processo di inserimento del *tool* all'interno dell'organizzazione.
Tale attività ha visto il susseguirsi di fasi consecutive, in cui ognuna dipendeva da quella precedente. Ciò non ha eliminato, in ogni caso, la possibilità di apportare modifiche al lavoro effettuato e alla pianificazione delle fasi successive. Si è, infatti, ritenuto opportuno acquisire un approccio trasversale all'acquisizione e all'implementazione del *database* di *configuration management*.

5.4.1 Fase 1: installazione del CMDB Alfa

La prima fase ha visto predominanti gli aspetti architetturali e di preparazione all'introduzione del *software*.
Alfa S.p.A. ha infatti richiesto la creazione di un *server* per poter procedere all'installazione dei propri applicativi, necessari al funzionamento dello strumento.
Le risorse desiderate erano:

- Sistema operativo: Linux, Ubuntu 16.04

- *Database*: PostgreSQL, versione 9.4.11
  Questa versione risulta in EOL il 31 dicembre 2019.

Coerentemente al lavoro svolto, si è già preso in carico la risoluzione dello stato obsolescente, pianificazione l'aggiornamento alla versione successiva.

- *Web Application*: Tomcat 8.0
  Questa versione è andata in EOL durante l'avanzamento del progetto.
  Per tale motivo si è provveduto all'aggiornamento della stessa prima del termine del progetto, implementando la versione alla 8.5.

- RAM: 8 GB
- CPU: 4
- Spazio disco: 100 GB

Al termine di tutte le configurazioni, si è avuto accesso al *software* tramite un'interfaccia *web*, da cui era possibile effettuare tutte le lavorazioni desiderate.

Il lavoro che ne è seguito è stato quello di effettuare in maniera proattiva tutte le verifiche di funzionamento dello strumento, andando ad analizzare tutti i casi d'uso in cui ci si poteva imbattere.

Una verifica che si è ritenuto essenziale effettuare, prima di qualsiasi analisi delle funzionalità dello strumento acquistato, è stata quella relativa all'accesso allo stesso. L'accesso, infatti, avviene tramite le utenze di rete personali dei dipendenti di Santander Consumer Bank. Tale verifica ha consentito il corretto funzionamento del protocollo LDAP, che rileva i requisiti d'accesso dai *Domain Controller*[125], tramite l'*Active Directory*[126], dell'azienda.

[125] Il *Domain Controller* è un *server* che gestisce le richieste di autenticazione e organizza la struttura del dominio in esame.

[126] L'*Active Directory* è un insieme di servizi gestiti dal *Domain Controller*, per l'assegnazione delle abilitazioni alle utenze secondo delle *policy* prestabilite.

I casi analizzati hanno riguardato:

- Accesso consentito per le utenze abilitate
  Per la prima fase di test, si è scelto di abilitare un numero limitato di utenze per l'accesso al CMDB. Esse erano corrispondenti al numero di persone operanti negli uffici Architetture IT e *Networking*.
  Inizialmente si sono riscontrate delle incoerenze nel connettore, infatti non tutti gli utenti abilitati riuscivano ad accedere al *tool*.
  Successivamente a un confronto con gli sviluppatori del sistema, si è trovata la risoluzione della problematica, la quale era la scorretta configurazione dell'utente che aveva accesso all'*Active Directory*.

- Verifica degli accessi negati agli utenti non abilitati
  La prova è stata effettuata con alcune utenze appartenenti agli uffici *Governance IT* e *Demand management*.
  Tale requisito è stato soddisfatto dalla prima verifica. Tuttavia, si è ritenuto opportuno ritestare tale funzionalità dopo la correzione della configurazione del servizio che provocava problemi per le utenze abilitate.

La scelta delle utenze da testare è stata basata su motivazioni estremamente pratiche. Lavorando in *open space*, si è preferito coinvolgere le persone che lavorano nello stesso ambiente, al fine di semplificare lo scambio informativo, rendendolo assolutamente informale.

Parallelamente alla verifica del funzionamento dell'LDAP, si è testato anche il funzionamento dei connettori che consentono l'aggiornamento automatico lato *software*, ossia quello con l'SCCM. Tale analisi è stata effettuata in due fasi:

- Fase 1
  La verifica delle informazioni di dettaglio e di configurazione è stata effettuata su ogni riga relativa a sistemi operativi, *database* e *web application*, al fine di scongiurare qualsiasi incorrettezza.

- Fase 2

  Il secondo *check* è stato effettuato al termine delle modifiche apportate dagli sviluppatori del *software*. Si è ritenuto sufficiente effettuare una verifica a campione, selezionando aleatoriamente le informazioni da verificare.

L'ultima attività effettuata relativamente alle connessioni è stato lo scarico delle identità dei dipendenti di Santander Consumer Bank tramite il connettore LDAP.

Il passo successivo è stato quello di andare a testare tutte le funzionalità promesse all'interno dell'offerta tecnico-commerciale.
Si è andati quindi a testare il funzionamento dei moduli di cui è composto lo strumento.
Il CMDB Alfa, infatti, come descritto in precedenza, è costituito da due moduli. Anche su di essi sono state eseguite delle verifiche per valutarne la corrispondenza alle esigenze di Santander Consumer Bank.

- *Data management module*

  Per questo modulo, i test effettuati hanno riguardato principalmente il funzionamento di:

  - Caricamento manuale dei dati
  - Caricamento massivo dei dati

    In una prima fase non è stato utilizzabile per questioni di configurazione in fase di test. Per tale motivo il primo caricamento è stato manuale e solo successivamente la valorizzazione delle classi è avvenuta in modo massivo.
  - Modifiche singole ai dati già inseriti
  - Modifiche multiple ai dati già inseriti
  - Esportazione dei dati di una classe
  - Generazione corretta delle *dashboard*

- Correttezza delle relazioni tra gli *asset*
- Correttezza dei filtri nella barra di ricerca

Nella verifica della struttura del *database* si è reputato utile generare una mappatura delle classi a disposizione e degli attributi in esse contenuti. Il motivo di questa scelta è stato di poter così semplificare l'organizzazione delle informazioni a disposizione e valutarne l'eventuale implementazione.

In figura 10 è riportato, a titolo di esempio, una finestra del modulo di gestione dei dati[127].

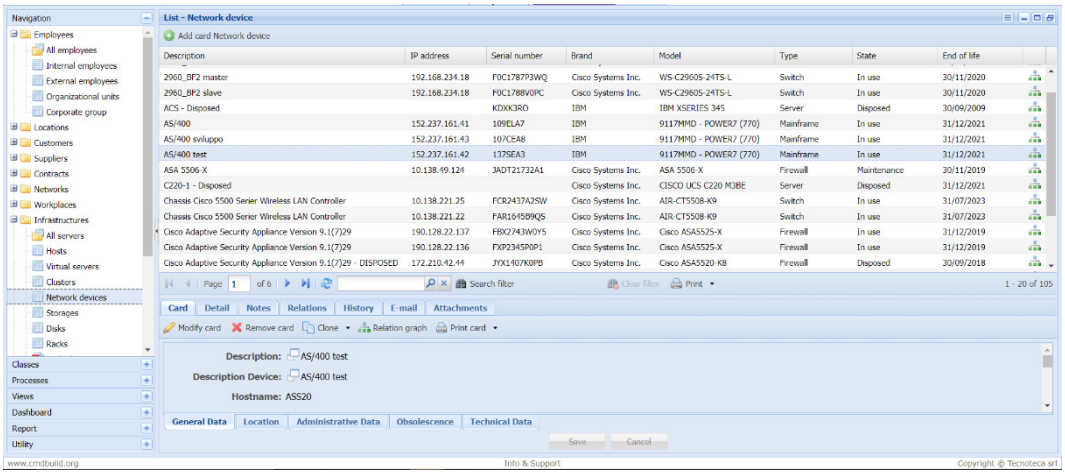

Figura 10- Esempio di Data Management Module

- *Administration module*

  Nel modulo di amministrazione, le verifiche effettuate hanno riguardato principalmente il funzionamento di:

  - Creazione di nuove classi
  - Modifica degli attributi presenti all'interno di una classe
  - Definizione degli attributi da avere nel pannello di controllo riassuntivo

[127] Esempio tratto da www.cmdbuild.org

- Creazione degli elenchi nel caso di generazione di attributi di tipo *lookup*[128]
- Abilitazione all'accesso di utenti o gruppi di utenti

In figura 11 è riportato, a titolo di esempio, una finestra del modulo di amministrazione[129].

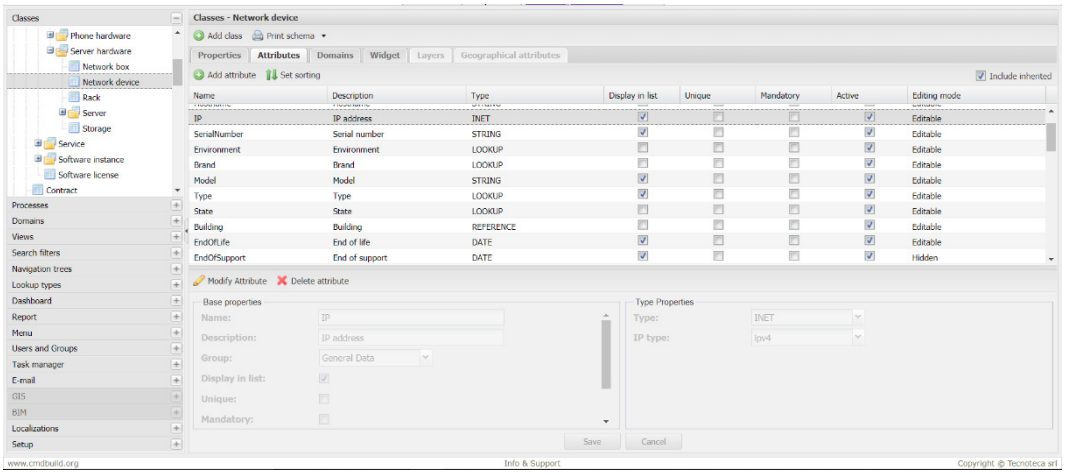

Figura 11- Esempio di Administration Module

Le implementazioni che si è reputato utile apportare sono descritte nel paragrafo seguente, riguardante la personalizzazione del *Configuration Management Data Base*.

Un ulteriore elemento di cui si è testato le funzionalità è stata la *system map*.
Si è ritenuto infatti opportuno verificare che tutte le informazioni prelevate dal CMDB fossero corrette e coerenti con i dati inseriti all'interno del *database*.
Anche in questo caso, si sono riscontrate delle incoerenze che sono state risolte con la collaborazione degli sviluppatori del *software*.

[128] Il tipo *lookup* consente di generare un elenco per la scelta multipla, ma guidata, delle alternative possibili alla valorizzazione dei campi considerati.

[129] Come nota 127

5.4.2 Fase 2: data entry

La seconda fase è stata inizialmente piuttosto meccanica. Si trattava infatti di andare ad inserire all'interno del *database* di *configuration management* tutte le informazioni raccolte durante la fase di *assessment*.

È bene sottolineare che, nel primo caricamento, il perimetro considerato è stato limitato agli *asset* della Sede Centrale italiana. Solo in un secondo momento si è provveduto all'implementazione delle informazioni relative anche alle filiali della finanziaria.

Si è proceduto, quindi, con il caricamento di tutti gli *asset* mappati in fase di *assessment*.
I criteri di caricamento hanno riguardato fondamentalmente l'*hardware*, dal momento che per il *software* esistono i connettori con l'SCCM che garantiscono l'aggiornamento automatico e costante delle informazioni ad esso relative. Tale discorso è valido per le macchine Windows®. Per le macchine Linux®, invece, il caricamento è stato effettuato in maniera manuale.
Per il primo caricamento, si è ritenuto opportuno suddividere lo stesso in più fasi, a seconda degli *asset* considerati, partendo dalle classi meno popolate. La valorizzazione delle classi è avvenuta quindi secondo la sequenza riportata:

1. Locazioni, in cui sono comprese le sottoclassi relative agli edifici, ai piani e alle stanze

2. Fornitori

3. Infrastruttura
   Questa è la classe maggiormente popolata da sottoclassi. In essa, infatti, è presente tutto l'*hardware* nelle varie tipologie descritte nei capitoli precedenti di questa trattazione.

5.4.2.1 Le prime modifiche al Configuration Management Data Base

A differenza di quanto preventivato, però, è stato in questa fase che si è avuto la possibilità di effettuare una valutazione approfondita delle classi standard inserite nello strumento acquistato. A valle delle considerazioni effettuate in questo intervallo temporale, infatti, si è iniziato ad apportare alcune modifiche e personalizzazioni allo strumento, sulla base dei dati che si avevano a disposizione.

La prima aggiunta che si è ritenuto opportuno apportare è stato l'aumento di dettaglio delle informazioni relative alle locazioni. Considerando che Santander Consumer Bank possiede tre Data Center[130], si è ritenuto opportuno aumentare il livello di dettaglio di tale attributo, creando un elenco per l'assegnazione della sala macchina di riferimento. In particolare, si sono aggiunti anche i campi relativi al *rack*[131] e all'unità del *rack* in cui è stato installato l'apparato.

Una seconda aggiunta ritenuta valida ai fini della gestione degli *asset* e della relativa obsolescenza è stata la classe dei contratti. Successivamente alla mappatura degli applicativi e degli *asset* proprietari e non di Santander Consumer Bank, infatti, si è riusciti a ricavare anche il fornitore di questi. I primi attributi inseriti nella suddetta classe sono stati i seguenti:

- Importo del contratto
- Nome del contratto
- Codice di riferimento
- Breve descrizione
- Data di scadenza
- Fornitore
- *Target*, ossia se riferito a *software* o *hardware*

[130] Un *Data Center*, letteralmente un centro dati, è uno spazio fisico compost da tutti i dispositivi informatici (*server*, *storage*, apparati di rete, cablaggi, *rack* e sistemi di condizionamento) che formano l'infrastruttura ICT, a support del *business* aziendale.

[131] Il *rack* è un sistema standard di installazione fisica delle componenti *hardware* di un sistema. Si tratta di una scaffalatura in cui vengono inseriti, in unità definite univocamente, i *configuration item*.

- Condizioni del servizio di supporto/manutenzione (ad esempio se rispetta orario di ufficio, se copre 24 ore su 24)

Al termine della fase di *data entry*, si è ritenuto opportuno effettuare ulteriori controlli a campione, per verificare l'esattezza delle informazioni e delle relazioni tra gli asset.

5.4.3 Fase 3: personalizzazione del CMDB

Questa terza fase è iniziata prima che la precedente fosse conclusa completamente. Grazie al livello di dettaglio raggiunto nella fase di *assessment*, infatti, si è ritenuto opportuno conservare i dati raccolti, evitando il rischio di perderli perché archiviati in strumenti poco controllati e di cui non era garantita la sicurezza in termini di modifiche apportabili e *backup* mancanti.
Sulla base delle informazioni di cui si era in possesso, quindi, si è proceduto alla modifica delle classi e degli attributi in esse contenute, tramite l'*administration module*.
In particolare, la customizzazione è avvenuta secondo i seguenti criteri:

- Implementazione degli attributi contenuti nelle classi, per semplificare l'individuazione della classificazione richiesta dalla Spagna.
  Questa operazione è stata effettuata inserendo un nuovo attributo all'interno di tutte le classi, di tipo *lookup*, in cui gli elementi della lista erano proprio le categorie individuate dalla Sede Centrale di Madrid.

- Aggiunta di attributi se le informazioni raccolte si reputavano essere utili alla generazione di reportistica o nel calcolo degli indicatori di rischio o di *performance*.
  È stata quindi creata un'altra classe relativa ai KPI e KRI per consentire l'archiviazione delle informazioni ad essi relative, così da rendere immediata la generazione di reportistica relativa all'andamento delle prestazioni aziendali.

- Personalizzazione dei *lookup type*, quindi nella definizione delle alternative possibili all'interno di un elenco.

  All'interno degli elenchi si sono inserite le alternative possibili sulla base delle informazioni ottenute in fase di *assessment*. Tuttavia, non è stato fatto un inserimento sconsiderato, ma si è cercato di uniformare i dati a disposizione. Questo perché le informazioni ricevute provenivano dagli utenti finali, ciascuno con la propria percezione, e non sempre in possesso delle informazioni tecnicamente corrette. Prima di procedere alla composizione di tali elenchi, infatti, si è ritenuto opportuno effettuare dei passaggi di verifica con gli uffici di competenza.

  Un esempio semplice può essere l'elenco dei fornitori, la cui denominazione commerciale non sempre era quella conosciuta a livello operativo, vedi il caso di eventuali fusioni societarie avvenute dopo l'acquisizione di applicativi *software* o apparati *hardware*. Tale verifica è stata effettuata in collaborazione con l'ufficio della *Governance IT*.

  Un ulteriore esempio di definizione delle liste di un attributo di tipo *lookup* può essere considerato quello relativo alla proprietà dell'*asset* in esame. In particolare, si sono individuate tre tipologie: "*owned*", "*rented*" e "*leasing*".

- Identificazione della tipologia degli attributi, cioè se fosse meglio, ad esempio, inserire una stringa, un booleano, una data, un *lookup*, o preferire un attributo di tipo *reference*[132], per definire le relazioni tra le righe del *database*.

  La scelta sulla tipologia di attributo da utilizzare è stata fatta sì sulla base delle informazioni di cui si era in possesso, ma anche valutando quelle che si sarebbero potute inserire successivamente, dopo aver aumentato il livello di dettagli dei dati relativi a ogni asset. In particolare, il tipo *reference* è stato fondamentale per decidere di inserire, ad esempio, le relazioni tra:

[132] Un attributo di tipo *reference* è quello che va a mettere una relazione tra più righe di un *database*. In particolare, il campo può essere valorizzato sulla base delle righe presenti in un'altra tabella del *database*.

- Un *asset* e un altro
- Gli apparati e i fornitori
- I fornitori e i contratti
- *L'asset* e il contratto di riferimento
- *L'asset* e il proprio *owner*
- *L'asset* e la relativa locazione
- Il *server* virtuale e lo *storage* su cui opera
- …

- Modifica della classe dei Contratti

  Se nella seconda fase si è ritenuto opportuno inserire dal principio la classe dei contratti, dopo aver preso dimestichezza con gli stessi a cui gli asset sono subordinati, si è considerato appropriato aggiungere anche le informazioni relative ai certificati e alle licenze. Anziché creare una nuova classe, che sarebbe stata praticamente una duplicazione della classe dei contratti, date le informazioni omogenee che le riguardano, si è ritenuto opportuno utilizzare la medesima classe, ma apportando delle modifiche in termini di attributi e relazioni possibili.

  Le variazioni apportate sono state le seguenti:

  - Aggiunta del nuovo attributo "Tipologia"

    Questo campo è stato impostato come *lookup* e le tre alternative possibili sono, quindi, contratto, licenza, certificato.

  - Modifica delle relazioni con gli asset

    La relazione è stata impostata del tipo n:n, coerentemente a quanto descritto successivamente.

- Definizione di quali relazioni dovevano essere stabilite e considerate.

  L'impostazione di partenza era una relazione del tipo 1:1 per tutte le relazioni pensate dallo sviluppatore. Sulla base delle informazioni raccolte

e delle considerazioni da esse derivanti, si è ritenuto opportuno richiedere una modifica di tale configurazione. Successivamente all'implementazione richiesta, le possibili relazioni inseribili all'interno del CMDB coprivano tutti e tre i casi già descritti in precedenza:

- 1:1

  Un caso di questo tipo di relazione potrebbe essere la locazione degli apparati fisici presenti all'interno delle sale macchina dell'organizzazione. Nel caso specifico degli *hypervisor*, ad esempio, ogni *host* viene assegnata a uno slot specifico all'interno del *rack*, il quale viene quindi attribuito univocamente a un singolo componente.

- 1:n

  Esempio di questa tipologia è l'*owner* di un *asset*. Il responsabile di un apparato deve essere univoco, tuttavia non è vero il contrario. Infatti, la stessa persona può essere *owner* di più *asset* contemporaneamente.

- n:n

  Un esempio potrebbe essere quello dell'*asset* con i relativi contratti stipulati con il fornitore. Ogni asset infatti è legato ad almeno un contratto. Si dice almeno uno in quanto, generalmente, a un *asset* sono legati due tipologie di contratti:

  - acquisto/manutenzione *hardware*
  - acquisto/manutenzione *software*

  A queste due tipologie, spesso si aggiunge anche l'eventuale acquisto di licenze per l'utilizzo degli strumenti.

- Personalizzazione delle unità di misura

  Sulla base delle informazioni raccolte, si è ritenuto opportuno ridefinire le unità di misura settate inizialmente, al fine di renderle maggiormente gestibili per i tecnici che necessitano di tali dati. Un semplice esempio può essere la modifica della dimensione degli *storage* da GigaByte a TeraByte.

- Definizione degli attributi da considerare *mandatory*

  Con questa definizione si intendono quei campi obbligatori senza cui non è possibile effettuare l'inserimento all'interno del *database* delle informazioni contribuite. Questa scelta è stata considerata fondamentale per evitare l'eccesso di dati poco utili. I campi ritenuti assolutamente necessari sono:

  - Nome/*Hostname*
  - Descrizione
  - Indirizzo IP

- Unicità degli *asset* censiti

  Al fine di evitare informazioni ridondanti, si è considerato indispensabile trovare il modo di rendere uniche le righe censite.

  Si sono escogitati modi diversi, a seconda della classe considerata:

  - *Hardware* e *software*

    Per tali *asset*, è stato richiesto di introdurre il vincolo di unicità sull'indirizzo IP. Quest'ultimo infatti è univoco per ogni apparato. Il limite che si è richiesto di inserire è stato, quindi, di impedire il salvataggio delle informazioni nel caso in cui l'indirizzo IP inserito fosse già presente all'interno del *database*, restituendo un messaggio di errore che rimanda all'*asset* già censito con tale informazione. Unito al fatto che il campo dell'indirizzo IP è un campo obbligatorio, si è ottenuto il risultato desiderato.

- Contratti

  Nel caso di questo campo, si è considerato utile ritenere come campo univoco il campo del numero dell'offerta. Vale esattamente il medesimo ragionamento seguito per le classi precedenti.

- Definizione del sistema di notifica di *alert*

  Il CMDB Alfa consente l'invio automatico di e-mail di *alert* per notificare alcune notizie di particolare interesse. Nel caso in esame, si è considerato di ricevere reportistica relativamente allo stato di obsolescenza degli *asset* inventariati.

  Nello specifico, le classi che si sono ritenute utili sono state:

  - Contratti
  - *Hardware*
  - *Software*
  - Applicativi

  Le informazioni contenute nei *report* sono state oggetto di continue modifiche, a mano a mano che ci si è resi conto delle informazioni realmente utili ai fini di contrattazione con i fornitori esterni.

  È bene sottolineare che nella prima personalizzazione dello strumento si è ritenuto sufficiente stabilire lo stato di obsolescenza sulla base dei contratti stipulati con i fornitori. Un *asset* era ritenuto obsolescente all'avvicinarsi della data di scadenza del contratto manutentivo proposto dal fornitore.
  Si vedrà successivamente come questo approccio viene modificato e migliorato.

  Nella definizione del sistema di *alerting* si sono dovute fare delle considerazioni dettagliate relativamente a:

- Intervalli temporali di riferimento per inserire gli *asset* nei *report*
  Al fine di generare una pianificazione ottimizzata nella gestione degli *asset*, considerando anche le tempistiche necessarie alla contrattazione con i fornitori e alle eventuali operazioni di *benchmark*, si è ritenuto ragionevole ricevere informazioni circa gli *asset* in scadenza nei sei mesi successivi alla data di ricezione della mail di notifica.

- Tempistiche di ricezione delle e-mail
  Considerando l'intervallo temporale stabilito al punto precedente, si è ritenuto sufficiente stabilire una ricezione mensile delle e-mail di *alert*.

CAPITOLO 6 – Gestione degli asset IT e dell'obsolescenza dopo il CMDB

Il primo risultato raggiunto grazie all'introduzione del *Configuration Management Data Base* nell'infrastruttura di Santander Consumer Bank è stato sicuramente il soddisfacimento delle richieste avanzate dall'organizzazione e dalla Sede Centrale di Madrid, sulla conformità del sistema della finanziaria agli standard desiderati.

Sulla base di questa esigenza di partenza, si è ottenuto un miglioramento sostanziale nella gestione degli *asset IT* e della relativa obsolescenza, da un punto di vista prettamente operativo. Di seguito si illustrano i benefici maggiormente rilevanti ottenuti con l'acquisizione di questo strumento.

1. Consapevolezza della situazione attuale
   Il primo effetto pratico dell'introduzione del *Configuration Management Data Base* è stato decisamente la presa di consapevolezza dello stato reale di tutti gli apparati in gestione di Santander Consumer Bank.
   Le informazioni raccolte, infatti, relative a ogni aspetto dei dispositivi in utilizzo, ha permesso di poter operare con cognizione di causa per il raggiungimento degli obiettivi di *business* e per la pianificazione di tutte le attività con impatti infrastrutturali.
   Inoltre, ha consentito di prendere coscienza anche di tutti quegli applicativi gestiti da terze parti e di cui gli attori principali dell'IT non erano a conoscenza.

2. Governo totale degli *asset* e gestione dell'obsolescenza
   L'acquisizione del governo totale degli *asset IT* è diretta conseguenza del punto precedente. Infatti, la disponibilità di tutte le informazioni relative ad essi ha fatto sì che il *management* fosse completamente autonomo e indipendente nello stabilire le priorità, particolarmente in termini di gestione dell'obsolescenza.

I responsabili degli apparati informatici hanno infatti potuto agire con una panoramica a 360° per definire i vari *action plan*.

L'ottenimento di tale controllo ha, inoltre, permesso di effettuare delle stime realistiche riguardanti il *budget* per l'anno seguente rispetto a quello in corso. La definizione del *budget* 2020, in particolare quello associato all'obsolescenza degli *asset IT*, o alla risoluzione di problematiche da essa derivanti, si è infatti completamente basato sulle informazioni contenute all'interno del *database* di *configuration management*, siano esse relative sia alle date di *End Of Life* o *End Of Support*, che alle configurazioni degli apparati rientranti nel perimetro in esame.

3. Pianificazione ottimizzata di implementazioni e sostituzioni

   Conoscendo tutto ciò che è contenuto nell'*hardware* e nel *software* aziendali, si è potuto pianificare tutte le attività di aggiornamento, implementazione e sostituzione degli *asset IT* che non rispondevano ai requisiti desiderati dalle politiche di governo aziendali.

   Tale pianificazione è stata effettuata tenendo conto dei vincoli di *budget*, di tempo e di risorse a disposizione dell'organizzazione.

   Una funzionalità decisamente strategica per la pianificazione ottimizzata è l'invio automatico di e-mail di *alert*: la possibilità di monitorare costantemente le scadenze relative all'obsolescenza, infatti, ha apportato un decisivo vantaggio per l'organizzazione nella gestione delle risorse, nel rispetto delle *deadline* generate dallo stato di invecchiamento degli apparati e nelle relazioni con i fornitori.

4. Potere contrattuale nei confronti dei fornitori

   La situazione per cui erano gli stessi fornitori a informare Santander Consumer Bank dello stato di obsolescenza degli *asset IT* era decisamente un tasto dolente.

   L'acquisizione della piena consapevolezza dello stato reale dell'infrastruttura e dei sistemi ha consentito di anticipare le richieste

sopraggiunte da parte dei fornitori, nell'eventuale prolungamento degli accordi stipulati.

Ciò ha permesso al *management* di acquisire potere contrattuale nella misura in cui è stata la stessa Santander a richiedere a più società esterne delle proposte per il supporto tecnico e la manutenzione dei propri apparati. La diretta conseguenza è stata la possibilità di effettuare *benchmark* competitivo tra le alternative a disposizione e, quindi, poter scegliere la soluzione ottimale in termini di rapporto costi/benefici.

C'è da considerare che, sapendo le società esterne di essere soggette a valutazione e in competizione con i *competitor* dello stesso settore, le proposte che sono arrivate in Santander erano decisamente più convenienti rispetto a quelle ottenute in precedenza.

5. Accesso all'inventario da parte di tutti gli utenti autorizzati e conseguente collaborazione tra gli uffici

   Come ulteriore punto, c'è da considerare che la possibilità di accedere allo strumento comune ha fatto sì che aumentasse la collaborazione tra gli uffici di Santander Consumer Bank, in particolare tra quelli dell'IT, della *Security*, del *delivery management* e del Rischio.

   Gli accessi, regolati secondo le *policy* di *cyber-security*, hanno consentito la diffusione di informazioni relative allo stato reale degli *asset* e, di conseguenza, l'uniformità dei dati ufficiali condivisi con la Sede Centrale di Madrid.

   Prima di provvedere alla trasmissione di questi ultimi a HQ, infatti, il processo attuale prevede l'allineamento degli uffici di Santader Consumer Bank Italia.

   Tale adeguamento ha permesso anche un costante scambio informativo che ha facilitato l'individuazione di alcune incoerenze e la risoluzione di alcune non-conformità, in termini sia tecnici che di rispetto delle *policy* aziendali.

6. Report e dashboard presentate ai comitati

   Per ultimo, ma non per questo meno importante degli altri, un ulteriore punto di forza acquisito grazie all'introduzione del *Configuration Management Data Base* nell'organizzazione c'è da considerare la reportistica dei dati ufficiali presentati al *Board of Director*. Innanzitutto, come diretta conseguenza della collaborazione tra gli uffici, è bene sottolineare la conformità delle informazioni presentate ai Comitati delle varie Direzioni. Inoltre, grazie alle funzionalità di questo strumento, è stato possibile semplificare la presentazione di tali dati. Il CMDB, infatti, prevede la possibilità di stilare *report* e sfruttare delle *dashboard* che riassumono perfettamente le notizie presenti nel *database*, tramite interfacce estremamente intuitive e comprensibili anche ai non addetti ai lavori.

6.1 Campagna Zero Tolerance

Quasi immediatamente dopo l'introduzione del CMDB in Santander Consumer Bank e all'apprezzamento dei primi benefici da esso portati, dalla Sede Centrale di Madrid è stata promossa una Campagna denominata *Zero Tolerance*.
Tale operazione prevedeva una politica piuttosto rigida, in termini di gestione dell'obsolescenza di quelle risorse IT ritenute particolarmente rilevanti per il funzionamento delle attività della banca dal punto di vista della criticità e dei rischi associati.
In particolare, il desiderato era:

- L'assenza di obsolescenza *software* o *hardware* con ciclo di vita scaduto

- L'assenza di mancate patch di sicurezza critiche attinenti alla *policy* di *cyber-security* e in base agli SLA stabiliti nelle *policy* interne relative all'*IT Asset Management*

- L'assenza di vulnerabilità critiche scadute sempre sulla base delle *policy* di *cyber-security*

I dispositivi a cui si faceva riferimento, quindi rientranti nel perimetro della *Zero Tolerance*, erano identificati secondo una categorizzazione che si rifà a quella descritta nel paragrafo 2.3.2 di questa trattazione.
In particolare, dovevano essere classificati tutti gli *asset* secondo i criteri di Riservatezza, Integrità e Disponibilità dei dati ad essi relativi, oltre che l'impatto che gli stessi hanno sull'operatività aziendale.
Tale classificazione prevedeva l'assegnazione di un punteggio sulla base della criticità di questi, coerentemente ai criteri definiti per l'analisi dei rischi, nel paragrafo 3.2.3.1 di questo lavoro.
A cambiare rispetto a quanto descritto teoricamente in precedenza, sono state le variabili considerate in quella che viene definita come la "Matrice di Rischio degli *asset IT*":

- Sull'asse delle ascisse, si trova la variabile definita *Service Impact*, cioè il grado di criticità dell'*asset* considerato.
  Il grado di criticità può variare in un *range* di valori così definito:
  - Low
  - Medium
  - High

- Sull'asse delle ordinate, invece, si trova il *Security Verification Level*, ossia l'indicatore aggregato della classificazione riguardante le *policy* di *security*, rispetto ai parametri di Riservatezza, Integrità e Disponibilità dei dati.
  Come visibile in figura 12, anche in questo caso la classificazione è del tipo:
  - Low
  - Medium
  - High

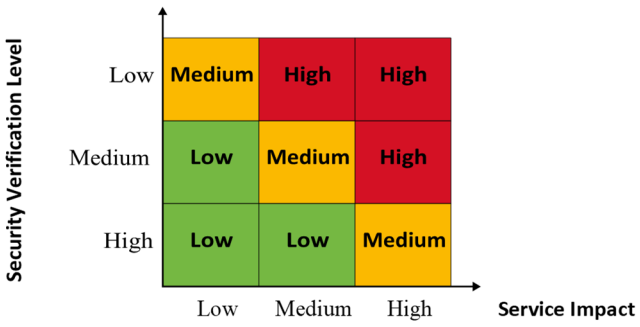

Figura 12 - Matrice di rischio degli asset IT

Gli *asset* rientranti nel perimetro *High* risultavano quelli interessati direttamente dalla Campagna *Zero Tolerance*, per cui era su quelli che premeva la risoluzione di eventuali stati di obsolescenza.

Nel dettaglio, considerando gli *asset IT*, sia *hardware* che *software*, ritenuti critici all'operatività dell'azienda, le richieste erano le seguenti:

- Entro il secondo *quarter*, quindi il 30 giugno 2019, era richiesto che la percentuale di *asset* obsoleti fosse pari o inferiore al 5%.

- Entro il quarto *quarter*, quindi al 31 dicembre 2019, era desiderato che la percentuale fosse pari allo 0%.

Avendo già implementato e customizzato il CMDB Alfa sulla base delle esigenze dell'organizzazione, si è deciso di accogliere tale Campagna come una nuova sfida nell'ottimizzazione della gestione dell'obsolescenza degli *asset IT*.
Il motivo di questa decisione strategica è stato, per l'appunto, quello di puntare all'ottimizzazione dell'infrastruttura informatica della Banca, al fine di:

- Ridurre al minimo i rischi legati all'obsolescenza dei sistemi *software* e *hardware*

- Supportare i processi di *cybersecurity* e *data protection*

- Garantire le prestazioni migliori disponibili sul mercato

Con lo scopo di accettare la sfida proposta da HQ, si è deciso di rispettare la *deadline* del 31 dicembre 2019, senza richiedere la possibilità di estensione dell'intervallo di tempo preventivato.
Per riuscire a rientrare in scadenze così stringenti, è stata pensata una pianificazione annuale che garantisse, considerando anche i vincoli contrattuali e le esigenze di utenti e fornitori, l'implementazione, l'aggiornamento o la sostituzione, dove necessario, di tutti gli asset obsoleti o al termine del loro ciclo di vita inclusi nell'architettura di Santander Consumer Bank.
In particolare, si è diviso il perimetro di azione in due categorie:

- *Hardware*

- *Software*

La pianificazione per ciascuna tipologia ha previsto:

1- Valorizzazione dell'inventario, all'interno del CMDB, di tutti gli *asset* proprietari e non della banca.

2- Individuazione degli *asset* critici e relativo stato di obsolescenza.

3- Piano di azione per gli *asset* critici al fine di ottenere una percentuale di obsolescenza pari al 5% entro il 30 giugno 2019.

4- Piano di azione per gli *asset* critici rimanenti per portare la percentuale allo 0% entro la fine dell'anno.

Si ritiene opportuno sottolineare che non ci si è limitati a rispettare le direttive promosse dalla Sede Centrale di Madrid, relativamente ai soli *asset* critici. A sostegno di questa dichiarazione c'è il fatto che la pianificazione per la riduzione

degli *asset* obsoleti in utilizzo in Santander Consumer Bank è stata effettuata in parallelo sia per gli *asset* rientranti nel perimetro della *Zero Tolerance*, sia per quelli esterni allo stesso, anche se con pressioni decisamente inferiori.

Entrando maggiormente del dettaglio del lavoro svolto, nel mondo *hardware* si è focalizzata l'attenzione sui dispositivi di rete, in quanto quelli a supporto dell'infrastruttura virtuale non presentano carenze di alcun tipo. Tra questi si trovano *switch* e *router*, in particolare quelli appartenenti ad alcune filiali, più datati rispetto agli altri.
Trattandosi di *hardware*, la scelta è stata quella di acquistare nuovi dispositivi per sostituire quelli obsoleti.

Il processo seguito è stato quello di definire in una prima fase gli elementi informatici obsoleti e, quindi, procedere con la raccolta delle offerte da parte dei fornitori. Successivamente si è proseguito con l'analisi delle stesse, con lo scopo di fare *benchmark* e scegliere la soluzione più adatta alle esigenze aziendali, considerando anche i tempi, per il rimpiazzo dei dispositivi, ritenuti opportuni al rispetto delle *deadline* stabilite.
Inoltre, si è anche tenuto in considerazione quanto indicato nelle direttive dettate dalla Sede Centrale di Madrid, coerentemente alle *policy* diffuse, in termini di limiti temporali di utilizzo degli apparati informatici.
L'intervallo di tempo d'uso concesso per l'*hardware* varia, infatti, tra 4 e 7 anni. Nel dettaglio si ha:

- *Storage* meccanici
  Sono considerati idonei fino a 4 anni dalla data di acquisto. È concesso 1 anno per effettuare la sostituzione, dopodiché vengono considerati obsoleti e generano allarmismo in termini di *security*, non rispettandone le *policy*.

- *Hypervisor*
  Valgono le medesime tempistiche che per gli *storage* meccanici

- *Server*
  Anche in questo caso, valgono gli stessi intervalli temporali degli *asset* definiti in precedenza

- *Communication asset*
  Sono considerati idonei fino a 5 anni dalla data di acquisto. Valgono poi le stesse concessioni applicate agli *storage* meccanici, nonché le medesime conseguenze.

- *High-Ends (iSeries/zSeries/AS400)*
  Valgono le stesse considerazioni fatte per i *communication device*

- ATM
  Sono considerati idonei fino a 8 anni dalla data di acquisto. Sono concessi 4 anni per provvedere alla sostituzione, dopodiché sono considerati obsoleti e non conformi alle *policy* di *security* e rischio.
  Si ritiene opportuno sottolineare come questi apparati si aggiungono per completezza, ma non rientrano nel perimetro di nostro interesse, in quanto Santander Consumer Bank non ne possiede sul territorio italiano

Per quanto riguarda il mondo *software*, invece, l'analisi dell'obsolescenza è stata affrontata su tre piani parallelamente:

1- Sistema operativo

2- *Database* (ad esempio: SQL server, MySQL, MariaDB)

3- *Web Application* (ad esempio: IIS, Apache Tomcat)

Si ritiene opportuno sottolineare che l'aggiornamento della *Web Application* è strettamente dipendente dal Sistema Operativo. Infatti, in molte occasioni, si è

dovuto provvedere prima all'aggiornamento della versione di quest'ultimo, per poi procedere all'implementazione della versione del servizio installato sulla macchina. Per tale motivo, per la pianificazione delle attività si è dovuto tenere di un ulteriore elemento di vincolo, rispetto al mondo *hardware*, che provocava un allungamento dei tempi di realizzazione del processo di aggiornamento.

Dal momento che era impensabile cercare di risolvere tutte le problematiche relative all'obsolescenza contemporaneamente, è stato necessario definire delle priorità.

La prima fase ha visto l'applicazione della *Zero Tolerance* agli *asset* critici, secondo la classificazione descritta in precedenza, in modo da poter rispettare la scadenza del secondo *quarter* definita dalla Campagna. Tra questi erano chiaramente presenti quelli rientranti nel perimento del *Business Continuity Plan*.

In una seconda fase, si è poi allargato il perimetro a tutti gli altri applicativi/*hardware*, non ritenuti critici, ma di cui si volevano risolvere le problematiche riguardanti l'obsolescenza, coerentemente alla sfida accolta.

6.2 Gli impatti dell'approccio Zero Tolerance

Successivamente all'accettazione della Campagna proposta dalla Sede Centrale di Madrid, si sono apportate delle modifiche anche all'interno del *Configuration Management Data Base*.
Questo passaggio è stato reputato opportuno alla semplificazione del processo di individuazione degli *asset* rientranti nel perimetro da tenere sotto osservazione nelle varie fasi di svolgimento della suddetta Campagna.
Si è proceduto, quindi, alla creazione di ulteriori attributi nelle classi già esistenti e in parte customizzate dello strumento. In particolare, si sono inseriti i seguenti attributi, prettamente corrispondenti alle caratteristiche richieste dalla Campagna:

- Appartenenza alla *Zero Tolerance*
  Questo attributo è stato inserito per avere l'informazione immediata circa l'appartenenza o meno al perimetro della Campagna.
  Si è ritenuto sufficiente scegliere il tipo booleano per tale campo.

- Per i seguenti attributi, si sono effettuate le medesime considerazioni. Nel dettaglio, si è ritenuto opportuno scegliere il tipo *lookup* al fine di avere un elenco valorizzato con la classificazione richiesta dalla *policy*, quindi inserendo valori quali *low, medium* e *high* all'interno dell'elenco.

  - *Service impact*
  - Riservatezza dei dati
  - Integrità dei dati
  - Disponibilità dei dati
  - *Service verification level*

Parallelamente, si è ritenuto opportuno apportare ulteriori variazioni alle classi del *Configuration Management Data Base*, al fine di uniformarle alle nuove informazioni acquisite e ottenere una visione globale sullo stato degli *asset*.

L'ulteriore customizzazione dello strumento acquisito è stata quindi relativa a:

- Aumento degli attributi in tutte le classi
  Queste aggiunte sono state effettuate su due piani distinti.
  Nel dettaglio, si sono introdotti i seguenti campi:

  - Lato applicativo
    - Presenza di dati confidenziali, tipo booleano Si/No
    - Presenza di dati sensibili dei clienti, tipo booleano Si/No
    - Conformità alle politiche aziendali, tipo booleano Si/No

- Classificazione dell'applicazione, tipo *lookup*, coerentemente alla classificazione *low*, *medium*, *high*
- RTO[133], di tipo *integer*, con unità di misura il numero di ore
- RPO[134], di tipo *integer*, con unità di misura il numero di ore

- Lato infrastrutturale:
  - Stato dell'apparato, tipo *lookup*, con le alternative:
    - *In use*, se in produzione
    - *Disposed*, se dismesso e sostituito da una nuova versione; in particolare, tale attributo ha dato il via all'utilizzo del CMDB anche come archivio storico di ciò che ha fatto parte dell'infrastruttura della finanziaria
    - *Available,* se disponibile, magari a magazzino
    - *Maintenance*, se sotto manutenzione successivamente a un guasto, ma che sarà rimesso in produzione una volta risolte le problematiche associate
  - EOL, calcolata in questo caso come la fine dell'intervallo temporale consentito dalla Spagna, a partire dalla data di acquisto
  - EOS
  - Data di acquisto, rispetto a cui calcolare i termini richiesti dalla Sede Centrale di Madrid per le sostituzioni

- Impostazioni di filtri sugli *asset* per le e-mail di *alerting*

  Avendo aggiunto un grado di dettaglio ulteriore, utilizzando il *Configuration Management Data Base* anche come un archivio storico, è stato necessario definire dei filtri per selezionare gli *asset* di cui ricevere informazioni relativamente allo stato di obsolescenza, dal momento che nel

[133] Il *Recovery Time Objective* è il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo organizzativo. Consiste nella massima durata del *downtime*.

[134] Il *Recovery Point Objective* è il massimo tempo che deve intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso *backup*) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.

database sono presenti anche apparati dismessi e, generalmente, classificati come obsoleti dalle relative *End of Life* ed *End of Support*.
Il filtro principale è stato quindi quello di selezionare gli asset negli stati *in use* e *available*.
Un'ulteriore considerazione è stata fatta sulle date di EOL, EOS e scadenza del contratto: il termine dei sei mesi, infatti, si è ritenuto opportuno stabilirlo sulla più vicina tra le tre date a disposizione.

- Abilitazione all'accesso al *Configuration Management Data Base* da parte di utenti diversi da quelli selezionati nella prima fase
  L'aver accettato la partecipazione alla Campagna *Zero Tolerance* ha avuto impatti non trascurabili in attività da eseguire, al di fuori della mera gestione degli asset obsoleti.
  Secondo le politiche corporative, infatti, tale lavoro doveva svolgersi sotto la supervisione dei Servizi del Rischio e dell'Audit. Per tale motivo, i responsabili operativi per tali attività hanno visto la possibilità di accedere al CMDB e verificare non solo la correttezza delle informazioni inserite, ma anche la coerenza con i dati ufficiali condivisi con la Sede Centrale di Madrid.

- Un ulteriore impatto della Campagna *Zero Tolerance* è stato l'utilizzo incrementale del sistema di *ticketing* in uso in Santander Consumer Bank. Tramite quest'ultimo, infatti, è stato possibile realizzare la pianificazione delle attività alle risorse che avrebbero lavorato operativamente alla risoluzione delle problematiche di obsolescenza e, di conseguenza, all'abbassamento delle percentuali di *asset* obsoleti presenti nell'infrastruttura informatica aziendale.

6.3 Evidenze

Considerato che il perimetro di azione ha coperto alcune migliaia di asset fisici, così come diverse centinaia di server visrtuali, si reputa necessario evidenziare come l'attuazione della campagna Zero Tolerance sarebbe stata irrealizzabile senza la presenza del Configuration Management Data Base.

L'effetto della migliorata gestione dell'obsolescenza degli asset IT è palesemente visibile considerando l'andamento degli indicatori di performance e rischio.

In particolare, soffermandosi sulle classificazioni della Zero Tolerance, si può osservare la variazione dall'inizio del progetto ad oggi, come illustrato nelle figure 13, 14 e 15.

In queste ultime, i valori percentuali inseriti all'interno dei diagrammi rappresentano il numero totale degli asset obsoleti sul numero totale degli asset della medesima tipologia. Inoltre, la suddivisione degli apparati è stata applicata considerando l'appartenenza o meno alla Zero Tolerance, secondo i criteri di Service Impact e Service Verification Level.

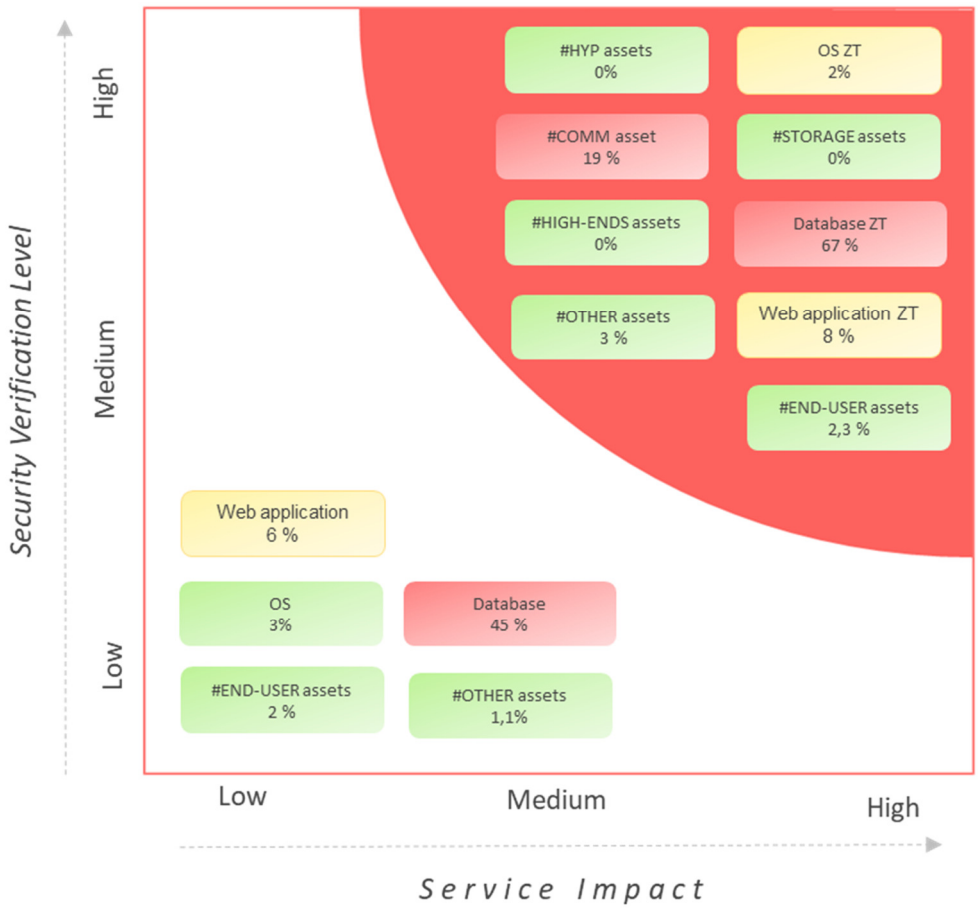

Figura 13 - Situazione al 30 novembre 2018

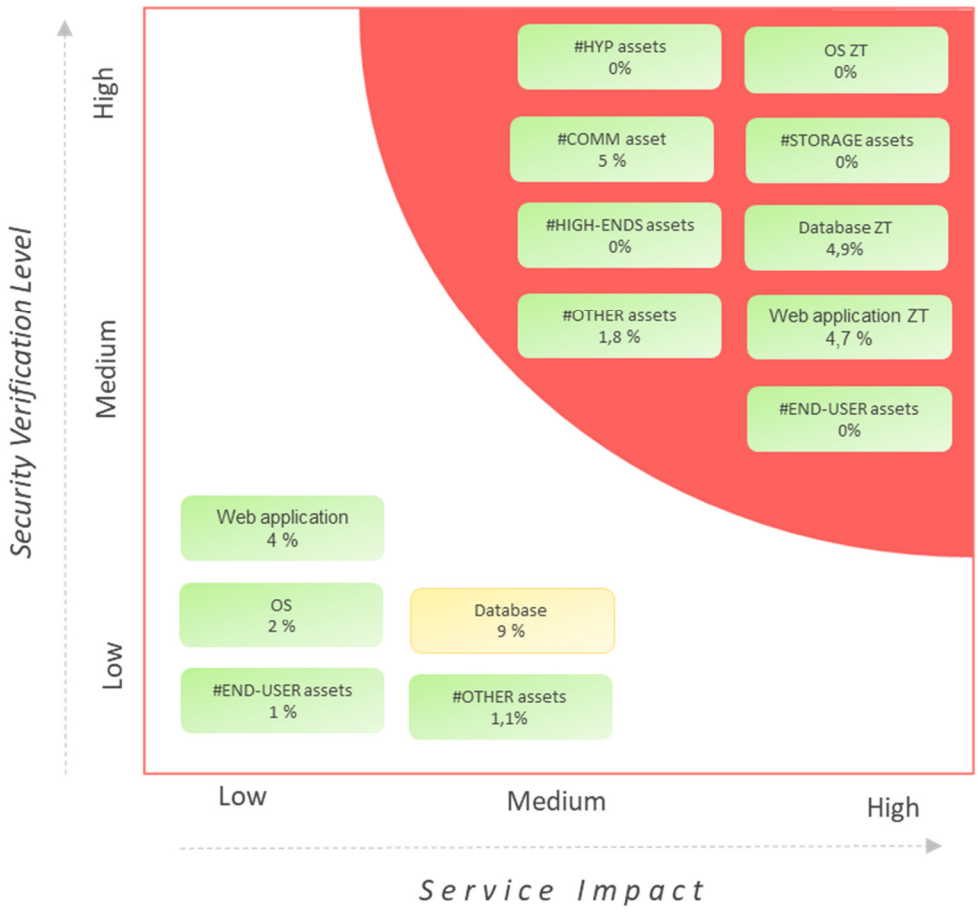

Figura 14 - Situazione al 30 giugno 2019

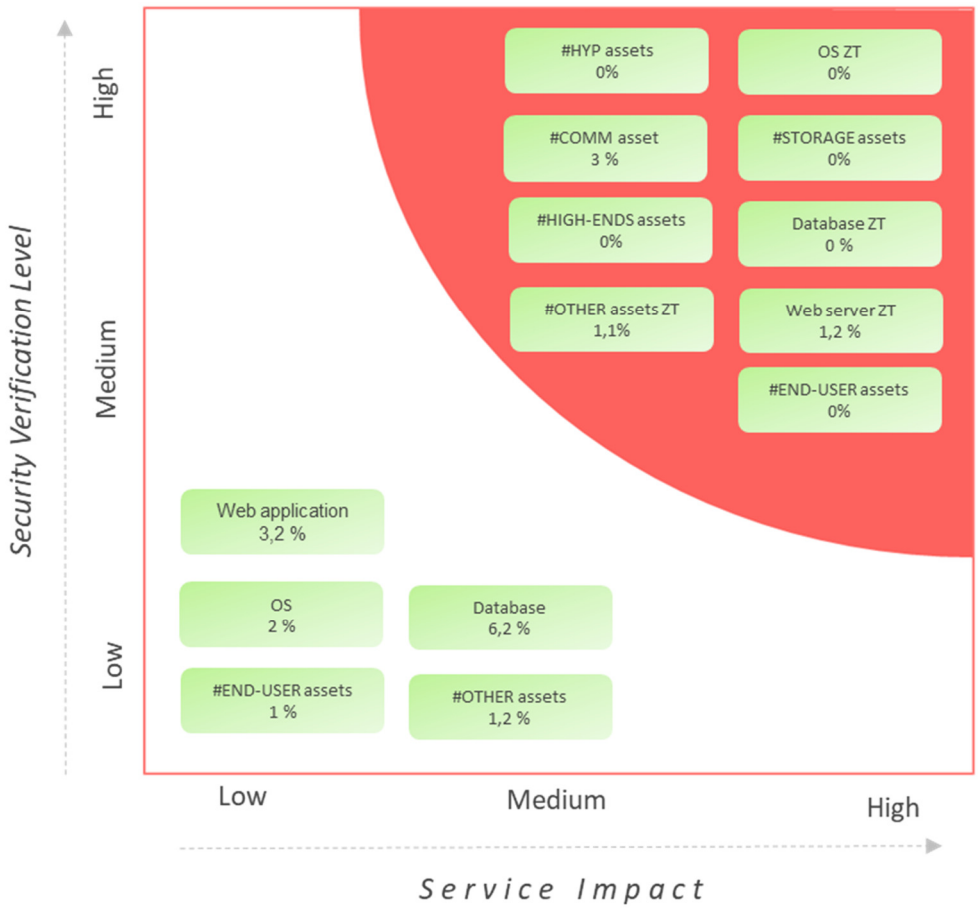

Figura 15 - Situazione al 30 novembre 2019

6.4 Imprevisti

Se lato Architetture IT le attività sono state svolte come previsto, nella realtà aziendale sicuramente non fila tutto liscio come l'olio. Si sono, infatte, presentate delle situazioni inaspettate che è stato necessario gestire, al fine di sfruttare quanto più possibile le potenzialità del *Configuration Management Data Base*.

La prima difficoltà da affrontare è stata la gestione dei *ticket*. Una volta aperte le segnalazioni, infatti, è stato necessario prenderne in carico il monitoraggio, al fine ti controllare non solo che le implementazioni venissero effettuate correttamente, ma anche che il *Delivery Management* avesse tutte le informazioni disponibili quando dovute. In merito proprio a quest'ultimo punto, si è deciso di elaborare dei template per la compilazione delle informazioni di maggior rilievo, da condividere dal primo momento con gli svilippatori.

La seconda difficoltà in cui ci si è imbattuti, una volta definiti i piani di migrazione o implementazione dei sistemi, è stata la gestione dei *failure* di tali operazioni. Di non tutti i server, infatti, è stata possibile una migrazione lineare, così come per non tutti i *database server* o *web server* è stato possibile effettuare un aggiornamento senza problemi. In molti casi, infatti, è stato necessario creare nuove macchine e installare in medesimi applicativi, al fine di rispettare le scadenze stringenti ed effettuare un lavoro decisamente più pulito dal punto di vista informatico. Inoltre, nel caso in cui gli applicativi fossero in gestione a società esterne, è stato necessario coordinare le attività interne ed esterne e, in alcuni casi, la tanta burocrazia presente in alcuni processi, non ha consentito una risoluzione rapida delle problematiche riscontrate. Il medesimo problema si è riscontrato nella gestione delle sostituzioni nel caso di apparati fisici obsoleti manutenuti da contratti di assistenza di società esterne, a cui era in carico la configurazione degli stessi.

Un ulteriore problema di coordinamento si è riscontrato nella collaborazione con gli uffici del Rischio e dell'Audit. Essendo stati coinvolti al termine della fase di inserimento del *Configuration Management Data Base* all'interno

dell'infrastruttura di Santander Consumer Bank, hanno iniziato ad avanzare rischieste sulla verifica del lavoro svolto, dei dati forniti dallo strumento e, di conseguenza, delle informazioni condivisi con la Sede Centrale di Madrid.

Nel dettaglio:

- Rischio

  Per svolgere le proprie attività, l'ufficio del Rischio ha richiesto la fornitura delle situazioni relative a momenti precedenti a quelli presenti. Se vero che il CMDB è stato pensato anche come archivio per tenere traccia di tutti i dispositivi informatici che hanno fatto parte dell'infrastruttura, è pur vero che non si era valutato il mantenimento delle situazioni in determinati momenti dell'anno, in cui vengono riportati dati ufficiali. Per tale motivo si è deciso di risolvere questa esigenza provvedendo all'estrapolazione mensile dei dati in un archivio in condivisione tra i due uffici. Coerentemente, anche il numero di KRI richiesto è aumentato, dal momento che non erano immediati dallo strumento o dalle estrazioni effettuate dallo stesso. Ciò ha significato incaricarsi della corretta pianificazione per il rispetto delle *deadline*. Un esempio di quanto detto può essere la considerazione delle informazioni relative ai soli dispositivi della *Demilitarized Zone*[135], sia relativamente all'*hardware* che al *software*.

- Audit

  Parallelamente a quanto fatto dal Rischio, anche l'ufficio dell'Audit ha avanzato le proprie richieste. Basandosi, infatti, molti report sui dati da noi forniti e avendo a disposizione un numero di informazioni nettamente maggiore rispetto al periodo precedente l'introduzione del CMDB, tale ufficio ha richiesto la fornitura di un numero superiore di indicatori e la

[135]Nell'ambito della sicurezza informatica, una demilitarized zone (DMZ, in italiano zona demilitarizzata), è una sottorete isolata, fisica o logica, che contiene dei servizi informatici offerti da un'azienda, accessibili sia da reti esterne non protette (WAN), che da workstation interne alla stessa azienda (intranet) e il cui scopo è quello di far usufruire questi servizi nella maniera più sicura possibile, senza compromettere la sicurezza della rete aziendale.
https://it.wikipedia.org/wiki/Demilitarized_zone

validazione di quanto dichiarato tramite evidenze. Per queste ultime è stato sufficiente la condivisione di *screenshoot* o di estrazione di alcune classi, ma si è dovuto comunque pianificare periodicamente anche tali attività.

Conclusioni

Questo studio ha cercato di rispondere all'esigenza di acquisire il governo degli asset IT e della relativa obsolescenza. A tal fine è stato seguito un processo che ha visto una prima fase di analisi delle soluzioni alternative a disposizione, una seconda fase di applicazione della soluzione ritenuta maggiormente opportuna e una terza di implementazione.

I risultati che si sono ottenuti con l'acquisizione di un CMDB erano sicuramente quelli desiderati, anche se le perplessità sul rispetto delle deadline erano notevoli. È stato infatti necessario lavorare a ritmo serrato per poter rientrare nei limiti temporali che ci si era imposti, a maggior ragione nel momento in cui si è deciso di estendere l'acquisizione del governo a tutti gli asset di Santander Consumer Bank, senza limitarsi ai soli elementi critici per l'operatività e la strategia aziendale. Un elemento di difficoltà aggiuntivo è stato sicuramente il rispetto della Campagna Zero Tolerance, proposta dalla Sede Centrale di Madrid e accolta in Italia.

Con l'acquisizione del CMDB si è creato un "effetto domino" all'interno dell'organizzazione. I primi impatti si sono sicuramente ritrovati in un rinvenuto potere contrattuale nei confronti dei fornitori esterni, nella piena consapevolezza degli strumenti che si avevano a disposizione. È necessario tenere in considerazione anche il miglioramento dello svolgimento delle attività normali e, soprattutto, l'aumento di collaborazione e di condivisione delle informazioni tra gli uffici coinvolti in tutto il ciclo di vita degli apparati informatici presenti all'interno dell'infrastruttura della finanziaria. Ciò ha fatto sì che iniziasse a diffondersi una maggiore consapevolezza di cosa servisse, da un punto di vista infrastrutturale informatico, al funzionamento di un'organizzazione di questo tipo, facendo sì che, seppur nel piccolo del limitato numero di attori in gioco, ci si approcciasse in maniera più critica nei casi sia di risoluzione delle problematiche, in particolare in termini di sicurezza informatica, che di ideazione di nuovi progetti.

A questo si è aggiunta anche la possibilità di pianificare le implementazioni dei sistemi e le sostituzioni in maniera più dinamica, con una gestione del budget e delle risorse più controllata e meno soggetta alle oscillazioni dovute alle emergenze.

Ciò che è risultato essenziale nello svolgimento di questo lavoro è stata, quindi, la collaborazione con i colleghi di uffici differenti, nonostante le difficoltà organizzative dovute in parte alla logistica degli stessi, in parte alla mole di lavoro che coinvolge tutti gli attori in gioco.

I risultati raggiunti con questo lavoro sono la base per proseguire lungo la strada dell'acquisizione del controllo totale degli asset coinvolti nelle attività di Santander Consumer Bank. Infatti, il passaggio immediatamente successivo prevede l'estensione del modello, applicato in via limitata alla sede centrale di Torino, a tutte le filiali presenti sul territorio italiano, andando a mappare tutti gli elementi hardware e software utilizzati all'esterno del quartier generale.

Bibliografia

Alsyouf, I., 2006. *Measuring maintenance performance using a balanced scorecard approach*. Journal of Quality in Maintenance Engineering 12 (2), 133-149.

Cavus, N. & Chingoka, D., N., C. (2015). *Information technology in the banking sector: Review of mobile banking. Global Journal of Information Technology. 5(2), 62-70.*

Corno, F., Torchiano, M., Sistemi Informativi Aziendali, Appunti per il corso – Capitolo 10, gennaio 2018.

De Haes, S., Van Grembergen, W., *IT Governance and its mechanism*, 2004, Information System Control Journal, vol.1.

El-Akruti K., Dwight R., Zhang T., *The strategic role of Engineering Asset Management*, Luglio 2013, Int. J. Production Economics 146 (2013) 227-239, www.elsevier.com/locate/ijpe

Gianturco, E., L'asset management e i sistemi automatici, 15 ottobre 2007, https://www.pmi.it/tecnologia/software-e-web/articolo/1542/lasset-management-e-i-sistemi-automatici.html

IEC 62402:2007, *Obsolescence management – Application guide*, *International standard*, 2007

IOGP Instrumentation and Automation Standards Subcommitee (IASSC), *Obsolescence and life cycle management for automation system, Recommended practice*, report 551, July 2016

Khurana, A., *Digitalization in banking: Convenience versus Security Threat*, pag. 1893, *International Conference on Sustainable Computing in Science, Technology & Management*, India, Febbraio 2019.

Muchiri, P., Pintelon, L., 2008. *Performance measurement using overall equipment effectiveness (OEE): literature review and practical application discussion.* International Journal of Production Research 46 (13), 3517-3535.

Paganini, P. (2013). *Modern Online Banking Cyber Crime.* Richiamato da INFOSEC INSTITUTE: https://resources.infosecinstitute.com/modern-online-banking-cyber-crime/

Taylor, J., *Information Technology in the Banking Industry*, 22 febbraio 2018, https://www.essaytyping.com/information-technology-banking-industry/

Van Bon, J., de Jong, A., Kolthof, A., Pieper, M., Tjassing, R., van der Veen, A., Verheijen, T., (2007). *Foundation of IT Service Management – basato su ITIL V3*. Van Haren Publishing, Zaltbommel, www.vanharen.net. Terza edizione, prima stampa, Settembre 2007.

Weill, P., W. Ross, J., *IT Governance: How to performers manage IT decision rights for superior results*, Harvard Business Press, 6 maggio 2004, Preface, cap 1, cap 2, cap 6.ù

Yamada, H., Yada, T., Nomura, H., *Developing network configuration management database system and its application—data federation for network management*, in *Springer Science+Business Media, LLC 2011*, 3 September 2011

Sitografia

- http://www.cmdbuild.org/it/contenuti/per-saperne-di-piu/cos-e-un-cmdb
- http://www.humanwareonline.com/project-management/center/configuration-management/
- http://www.rfc.it/applicativi/asset-aziendale
- http://www.treccani.it/enciclopedia/iec/
- http://www.treccani.it/enciclopedia/iso/
- http://www.treccani.it/vocabolario/obsolescenza/
- http://www2.supsi.ch/cms/pmforum/wp-content/uploads/sites/23/2017/07/G2-Configuration-Management-secondo-l%E2%80%99ISO.pdf
- https://it.wikipedia.org/wiki/Capability_Maturity_Model
- https://it.wikipedia.org/wiki/COBIT
- https://it.wikipedia.org/wiki/Configurazione_(informatica)
- https://it.wikipedia.org/wiki/Firewall
- https://it.wikipedia.org/wiki/Gestione_della_configurazione
- https://it.wikipedia.org/wiki/Hardware
- https://it.wikipedia.org/wiki/ISO_10007
- https://it.wikipedia.org/wiki/Microsoft_Access

- https://it.wikipedia.org/wiki/Microsoft_Excel
- https://it.wikipedia.org/wiki/Switch
- https://sites.google.com/site/systemengineeringitaly/home/system_and_systemengineering/what-is-a-system/cosa-e-un-sistema
- https://www.essaytyping.com/information-technology-banking-industry/#
- https://www.glossariomarketing.it/significato/ciclo-di-vita-del-prodotto/
- https://www.iso.org/obp/ui/#iso:std:iso:10007:ed-3:v1:en
- https://www.logisticaefficiente.it/wiki-logistica/supply-chain/product-life-cycle-ciclo-di-vita-del-prodotto.html
- https://www.softwarequarta.com/risk-based-thinking-kpi-e-indicatori-di-rischio-kri-per-generare-valore/
- https://www.techopedia.com/definition/3/business-continuity-plan-bcp
- www.iso.org