ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA
SCUOLA DI INGEGNERIA E ARCHITETTURA

CORSO DI LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

TITOLO DELLA TESI

PROGETTO DI INTEGRAZIONE DI STRUMENTI PER L'ASSET MANAGEMENT IN FUNZIONE DI PRIVACY E SICUREZZA

Tesi in

SISTEMI MULTI-AGENTE

Relatore

Chiar.mo Prof. Andrea Omicini

Presentata da

Enrico Gualandi

Sessione III

Anno Accademico 2012/2013

Introduzione

In questi ultimi anni l'informatica è diventata sempre più diffusa in tutte le aziende, indipendentemente dalla loro dimensione. La gestione IT deve quindi amministrare e mantenere una mole superiore di macchine client e server, ognuna delle quali ha determinati software da installare e aggiornare, nonché un incremento di chiamate di assistenza per guasti e problemi.
Tutto questo deve essere conforme ai vincoli di legge presenti nel D.lgs. 196/2003 (Testo unico sulla privacy) riguardo l'accesso ai dati privati dell'utente, nel D.lgs. 231/2001 (Responsabilità di Impresa, Codice Etico e Responsabilità delle persone Giuridiche) riguardo la responsabilità aziendale relativa alla presenza di software illecito installato dagli utenti o ad azioni intraprese dagli stessi per compiere illeciti, nello Standard UNI CEI ISO/IEC 27001:2006 che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni. Sono quindi necessari nuovi strumenti per avere una gestione coerente delle macchine, degli utenti e dei software.
Una gestione "a polling" delle informazioni sulle varie macchine non è percorribile, sia per le difficoltà tecniche sia per il monte ore necessario a svolgere tali attività, né si può fare affidamento a una trasposizione e aggiornamento manuale da parte degli operatori che intervengono sulla rete a causa di possibili dimenticanze o errori di trasposizione. Si necessita pertanto di utilizzare prodotti che s'interfaccino con le macchine e gli utenti, tipicamente attraverso agenti installati sulle macchine e sui server, e che permettano di recuperare le varie informazioni in modo rapido ed efficiente. Strumenti che compiono questo lavoro esistono già, ma lavorano in modo indipendente l'uno dall'altro, creando alcune difficoltà di gestione degli apparati da parte dei tecnici IT.

Alya S.r.l. è un'azienda informatica presente sul territorio da quasi venti anni, che si occupa di integrazione e sviluppo di tecnologie informatiche. Supporta aziende nel territorio e non solo nelle fasi di pianificazione strategica, progettazione, sviluppo, implementazione e supporto. La certificazione Microsoft Gold Certified Partner porta l'azienda comunque a valutare e proporre prodotti Microsoft, integrando con software di terze parti dove questi non siano adeguati alle esigenze dei clienti.
La collaborazione con la suddetta azienda ha permesso di poter avere uno spaccato sulla situazione delle aziende di varie dimensioni.

In questo elaborato viene progettato, basandosi sull'esperienza acquisita durante il periodo lavorativo presso l'azienda Alya S.r.l., uno strumento per gestire in modo centralizzato gli asset aziendali, integrando tra loro strumenti già esistenti, permettendo un controllo più veloce e agile dello stato della rete e degli utenti in modo da rispettare gli standard di legge in materia di privacy e di software non licenziati, con forti risparmi di tempo e denaro.

L'elaborato è organizzato come segue.
Nel primo capitolo viene presentata la gestione degli asset allo stato attuale, attraverso la descrizione degli asset stessi e alcuni degli strumenti utilizzati per la loro gestione a campione.
Nel secondo capitolo vengono presentati gli obblighi di legge e le necessità operative che hanno portato alla stesura del progetto in esame; nonché i processi che l'azienda deve controllare attraverso di esso.
Nel terzo capitolo vengono analizzati i vincoli e le possibili problematiche inerenti la progettazione e lo sviluppo del progetto in essere, fornendo poi l'architettura logica del sistema.

Nel quarto capitolo viene presentato il progetto del sistema, con un particolare accento sui processi richiesti dalle aziende e alle parti atte a svolgere l'integrazione tra le parti.

Indice

Capitolo 1

La gestione asset

All'interno di un'azienda la gestione degli asset aziendali prevede la raccolta informazioni e la gestione riguardo alcuni aspetti:

1. monitoraggio server;
2. call tracking;
3. gestione inventario client;
4. gestione permessi utenti.

Ognuno di questi aspetti è gestito con strumenti di varia natura e prodotti da aziende differenti, rendendo di fatto ardua l'integrazione tra di essi. Le informazioni prodotte dai vari sistemi risultano essere pertanto ridondanti e di non facile consultazione. Le collezioni di informazioni utili sono pertanto fatte a mano dagli amministratori IT recuperandole dai vari report generati dagli strumenti indicati e inserendole in fogli di calcolo che spesso risultano essere di difficile gestione per la quantità di informazione contenuta, oltre a essere ad altro rischio di incoerenza con la realtà presente in azienda.

1.1 Gli asset

Ogni asset ha una vita all'interno del processo aziendale che deve essere registrata in ogni sua variazione, per poter avere in ogni momento una visione chiara e coerente dello stato dell'azienda.
Abbiamo classificato 4 tipi di asset aziendali principali:

- Utenti;
- Documenti;
- Macchine;
- Software.

I primi sono gli utenti dell'azienda stessa, che vengono registrati nel momento dell'assunzione e che devono essere collegati agli altri asset come documenti e macchine che li riguardano.
I documenti sono intesi tutti i contratti legati ad altri asset, come i contratti di assunzione o la dichiarazione di visione di norme sulla privacy legate agli utenti, oppure i contratti di garanzia legati a una particolare macchina.
Le macchine sono tutti i client e i server presenti in azienda, che devono essere monitorati e censiti.
Il software rappresenta invece, come asset indipendente, il prodotto licenziato e utilizzato in azienda. Se invece inserito in un collegamento con una particolare macchina rappresenta l'installazione specifica.
Di seguito sono descritti nel dettaglio.

1.1.1 Utenti

L'utente rappresenta un dipendente o collaboratore dell'azienda. Come tale è legato a un utente di dominio e a un indirizzo e-mail aziendale. Possiede diritti specifici di accesso alle varie informazioni definite in base alle sue mansioni aziendali e alle aree di competenza.

Un asset utente è di norma descritto dai seguenti parametri:

Parametro	**Descrizione**
IDAsset	Campo identificativo univoco dell'utente. Corrisponde solitamente al nome utente di dominio, essendo per definizione univoco.
Cognome	Cognome dell'utente.
Nome	Nome dell'utente.
Area	Indica l'area aziendale in cui è inquadrato l'utente.
Incarico	Indica il livello di permesso di accesso ai dati

	aziendali. Possono essere molteplici, es. Responsabile marketing e Responsabile Amministrazione.
Contatti	Indica tutti i contatti a cui è possibile rintracciare l'utente.

1.1.2 Documenti

I documenti rappresentano i contratti che riguardano altri asset quali contratti firmati dall'utente riguardo presa in carico delle macchine, piuttosto che i contratti di garanzia di una macchina o eventuali manuali legati al software. Dato importante per la gestione documentale è la data di scadenza del documento stesso che permette di stabilire il rinnovo dello stesso, es un contratto di manutenzione su una certa macchina.

I documenti sono rappresentati dai seguenti parametri:

Nome Dato	**Descrizione**
IDAsset	Campo identificativo univoco del documento.
Titolo	Il titolo del documento.
Asset correlato	Identifica l'asset al quale il documento è collegato, tipicamente l'identificativo.
Localizzazione	La posizione dove il documento è archiviato.
Scadenza	Scadenza del documento.

1.1.3 Macchine

Le macchine rappresentano i dispositivi presenti in azienda. Ogni client (sia computer sia device portatile) è preparato e assegnato a un utente, possiede alcune installazioni software che devono essere censite e licenziate. Ogni server invece deve esse-

re registrato e messo sotto monitoraggio. Tutte le macchine devono essere mantenute, in altre parole tenute aggiornate e in efficienza, perché non rappresentino buchi nella sicurezza.

Le macchine sono rappresentate dai seguenti parametri:

Nome Dato	**Descrizione**
IDAsset	Campo identificativo univoco dell'asset, tipicamente il nome FQDN, univoco per definizione.
Produttore	Indica il produttore.
Modello	Indica il modello della macchina.
Sistema Operativo	Indica il sistema operativo installato.
Software installati	Riporta i software installati sulla macchina.
Utente principale	Identifica chi è l'utente principale che opera sulla macchina.
Fine Garanzia	Indica quando la garanzia della macchina scade, per valutarne se possibile un'estensione, o la sostituzione della stessa.
Fornitore	Indica il fornitore presso il quale si è acquistato il prodotto e presso il quale richiedere assistenza hardware.

1.1.4 Software

L'asset Software non rappresenta l'installazione del software in oggetto su una particolare macchina, ma dell'entità generale in quanto presente in azienda. Devono esserne verificate le compatibilità con le macchine presenti in azienda e la loro vita utile, sia per quanto riguarda la licenza che per quanto concerne il supporto da parte del produttore. Inoltre rappresenta software in fase di valutazione per l'utilizzo effettivo in azienda.

I software sono rappresentati dai seguenti parametri:

Nome Dato	**Descrizione**
IDAsset	Campo identificativo univoco dell'asset.
Produttore	Indica il produttore.
Nome	Nome del software.
Versione	Versione del software
Sistema Operativo Compatibile	(Opzionale) Indica il sistema operativo su cui può essere installato.
Termine Supporto	Indica quando il produttore terminerà il supporto al software.

1.2 Gli strumenti attuali

Visioniamo di seguito i vari software attualmente utilizzati e proposti per la gestione degli asset.

1.2.1 SCCM

System Center Configuration Manager è lo strumento utilizzato per il deploy delle macchine client e il loro inventario. Una volta generato il modello di installazione, composto dai driver relativi alla macchina e ai software da installare, si possono preparare svariate macchine in serie, pronte da consegnare all'utente e terminare le ultime configurazioni personali, es. la casella di posta elettronica in Outlook. Il prodotto installa un agente su ogni macchina che periodicamente (tipicamente una volta al giorno) fa l'inventario del software presente, permettendo di verificare variazioni eseguite dagli utenti alle installazioni effettuate. Se si inserisce il numero di licenze in possesso per ogni software segnala anche la presenza di installazioni in eccedenza e quindi non correttamente licenziato.

1.2.2 SHAREPOINT

Sharepoint è lo strumento utilizzato per la repository documentale. Gestisce gli accessi ai vari documenti attraverso gruppi di sicurezza che possono essere collegati ai gruppi di Active Directory. Prevede sia una gestione attraverso le cartelle di sistema, che una gestione attraverso un sito web, attraverso il quale sono visionabili direttamente on line i file generati con i prodotti Office. Inoltre se pubblicato permette il recupero dei documenti anche dall'esterno con lo stesso standard di sicurezza dell'accesso.

1.2.3 MAAS

Monitoring As A Service è un prodotto studiato per il monitoraggio delle macchine aziendali, principalmente server. Esso permette un controllo attivo dei vari dati della macchina attraverso l'installazione di un agent. L'architettura del sistema prevede che i singoli agenti comunichino con un server proxy presente sulla rete e questi si mantiene in comunicazione con il server di monitoraggio che risiede all'esterno dell'azienda, presso una farm terza.
Tipici utilizzi del prodotto sono il monitoraggio eventi di sistema, lo stato di riempimento dei dischi, il carico della CPU, la raggiungibilità delle macchine attraverso la rete, la disponibilità di siti web pubblicati.
Il sistema presenta in una dashboard lo stato delle macchine, indicando le varie anomalie in base alla loro gravità, e inviando le e-mail per errori gravi o critici, in modo da poter intervenire tempestivamente su un problema presente sulla macchina e dare il minor disservizio possibile agli utenti.

1.2.4 CRM

Microsoft Dynamics Customer Relationship Management è il prodotto utilizzato per la gestione delle chiamate di assistenza verso gli utenti. Altamente personalizzabile, permette appunto di visionare le chiamate aperte, le chiamate relative a un particolare utente, ecc..., inoltre ha una serie di campi utili a descrivere una chiamata sotto tutti gli aspetti: stato della chiamata, scadenza della chiamata, ecc….
A seconda del tipo di evento generato (es. apertura caso) il sistema invia mail ai gruppi di utenti designati, per permettere una gestione più efficiente delle chiamate in essere, senza che sia il tecnico IT a controllare periodicamente il prodotto per verificare se sono state aperte chiamate, quali sono chiuse, ecc...

1.3 Stato attuale della gestione.

Attualmente i prodotti indicati non sono strutturati per sincronizzarsi tra loro. Le informazioni trasversali, come per esempio quale utente è proprietario della macchina A, sono registrate a mano dai tecnici, normalmente su fogli di calcolo. Inoltre su tali documenti sono riportate in modo ridondante informazioni di utilizzo più frequente relative agli utenti e alle macchine stesse per rendere più rapido il recupero delle stesse, causando però problemi di coerenza dei dati che potrebbero cambiare nei sistemi principali e non essere riportati su tutti i documenti correlati.
La gestione documentale non prevede nessun collegamento con i relativi asset. I documenti sono archiviati e organizzati non secondo gli asset, ma secondo il tipo di documento.
Nel caso di documenti a scadenza (come le garanzie e i contratti a tempo determinato) si deve creare uno scadenzario compilato a

mano e che deve essere prontamente aggiornato in base alle modifiche ai vari documenti.
La gestione risulta quindi frammentaria e con perdite di tempo sensibili per il reperimento delle informazioni richieste a seconda delle esigenze.
I software difficilmente sono tracciati in quanto entità e spesso viene creata solo una documentazione per l'analisi dei requisiti e una guida per l'installazione.

Capitolo 2

Rinnovo della gestione asset aziendale

L'aumento dei volumi di asset da gestire mantenendo il rispetto delle norme giuridiche impone un rinnovo della gestione degli stessi, sia tecnologicamente sia organizzativamente rinnovandone i processi.

2.1 Obblighi di legge

Le norme che regolano la gestione dei dati e delle informazioni, nonché la gestione della rete stessa sono il D.lgs. 196/2003 (Testo unico sulla privacy), il D.lgs. 231/2001 (Responsabilità di Impresa, Codice Etico e Responsabilità delle persone Giuridiche) e lo Standard UNI CEI ISO/IEC 27001:2006.

2.1.1 D.lgs. 196/2003 (Testo unico sulla privacy)

Il D.lgs. 196/2003, in particolare nell'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza), indica le "modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici".
Nei primi 10 articoli specifica come sia necessaria l'identificazione univoca degli incaricati al trattamento dei dati sensibili, attraverso un username univoco associato in via definitiva all'utente e una password o caratteristica biometrica. La password deve essere conosciuta unicamente dall'utente al quale viene associata. Ogni utente può possedere più credenziali per eseguire l'accesso. Le credenziali di accesso non devono essere

divulgate e si rende necessario sensibilizzare gli utenti su questo aspetto.
Sono indicate anche le caratteristiche minime della password: lunghezza di 8 caratteri o, in caso di strumenti elettronici come le smartcard, il numero massimo di caratteri consentiti. Essa non deve contenere riferimenti facilmente riconducibili all'incaricato e deve essere modificata dall'utente al primo accesso e dopo ricorsivamente ogni 6 mesi, o 3 in caso di trattamento di dati sensibili e giudiziari.
Tali credenziali devono poi essere disattivate per interruzione dell'incarico che ne permetteva l'utilizzo o il relativo inutilizzo di 6 mesi. Le credenziali di gestione tecnica non sono sottoposte a questo vincolo.
È ribadito più volte di istruire gli utenti a come conservare le proprie credenziali in modo sicuro e non renderle accessibili a terzi. Indica inoltre che "in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema" il titolare può fornire le proprie credenziali, secondo accordi e modalità presi in precedenza. "In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato."
Nei successivi 3 articoli esplicita che nel caso di creazione di profili comuni di autorizzazioni, tipicamente i gruppi AD, i gruppi devono essere predisposti in precedenza "in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento" e che "periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione".

2.1.2 D.lgs. 231/2001 (Responsabilità di Impresa, Codice Etico e Responsabilità delle persone Giuridiche)

Il D.lgs. 231/2001 estende alle persone giuridiche la responsabilità per reati commessi in Italia e all'estero da persone fisiche che operano per la società.
In aggiunta alla responsabilità della persona fisica che realizza l'eventuale fatto illecito la normativa ha introdotto la responsabilità in sede penale degli Enti per alcuni reati commessi nell'interesse o a vantaggio degli stessi, da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua organizzazione dotata di autonomia finanziaria o funzionale e da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.
Elenca inoltre le situazioni per cui la società non risulta responsabile quali l'adozione da parte dell'organo dirigente di modelli di organizzazione e gestione idonei a prevenire i reati commessi, l'affidamento a organismi terzi dotati di poteri autonomi, l'elusione fraudolenta da parte delle persone che hanno compiuto l'illecito dei modelli di organizzazione.
L'organo dirigente deve quindi preparare dei modelli organizzativi che devono rispondere alle seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi reati;

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;

d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;

e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

La norma dispone infine che l'efficace attuazione del modello consiste in una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività.

Tali adempimenti devono poter essere svolti senza danneggiare l'attività aziendale per cui è necessario l'utilizzo di strumenti che permettano di raggiungere il risultato senza gravare in modo eccessivo sui processi aziendali riducendo al contempo il costo correlato agli adempimenti stessi.

2.1.3 Standard UNI CEI ISO/IEC 27001:2006

Lo Standard UNI CEI ISO/IEC 27001:2006 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) è una norma internazionale che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.

In particolare indica che i documenti dello SGSI (Sistema di Gestione della Sicurezza delle Informazioni) devono essere protetti e controllati e deve essere impostata una procedura documentata per :

a) approvare documenti per adeguamenti preventivi;
b) rivedere e aggiornare documenti quando necessario e riapprovare documenti;
c) garantire che i cambiamenti e lo stato di revisione attuale dei documenti rilevanti siano identificati;

d) garantire che le versioni più recenti dei documenti di maggiore importanza siano disponibili agli utenti;
e) garantire che i documenti rimangano leggibili e prontamente identificabili;
f) garantire che i documenti siano disponibili a chi ne ha bisogno e siano trasmessi, memorizzati e infine dismessi nel rispetto delle procedure applicabili alla loro classificazione;
g) garantire che i documenti di origine esterna siano identificati;
h) garantire che la distribuzione dei documenti sia controllata;
i) prevenire l'uso incorretto di documenti obsoleti;
j) applicare degli identificativi appropriati ai documenti obsoleti se è necessaria la loro conservazione per un qualche scopo.

Sottolinea che l'organizzazione deve garantire che tutto il personale a cui vengano assegnate responsabilità definite nello SGSI sia in grado di svolgere i compiti richiesti:

a) determinando le competenze del personale necessarie ad effettuare lavori collegati all'SGSI;
b) fornendo una formazione o intraprendendo altre azioni (es. impiegando personale competente) per soddisfare tali necessità;
c) valutando l'efficacia delle azioni intraprese;
d) mantenendo annotazioni su educazione, formazione, abilità, esperienza e qualifiche.

L'organizzazione deve inoltre garantire che tutto il personale interessato sia cosciente della rilevanza e dell'importanza delle sue attività collegate alla sicurezza delle informazioni e di come contribuire al raggiungimento degli obiettivi dell'SGSI.

Tutto l'SGSI deve essere revisionata periodicamente dalla direzione almeno una volta l'anno per garantirne la conformità, l'adeguatezza e l'efficacia.
La norma ne indica anche le modalità e i punti da revisionare.
All'interno dell'Allegato A vengono indicati gli obiettivi e i controlli da effettuare, in particolare relativamente alla gestione degli asset afferma che:

- Tutti gli asset devono essere chiaramente identificati e deve essere creato e mantenuto un inventario di tutti gli asset importanti. (Inventario degli asset)
- Tutte le informazioni e gli asset associati con le strutture di elaborazione delle informazioni devono essere "detenute" da una parte designata dell'organizzazione. (Detenzione degli asset)
- Le regole per un uso accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate ed implementate. (Uso accettabile degli asset)

2.2 Necessità tecniche

Il reparto di gestione IT e la direzione hanno bisogno di avere un unico punto di accesso per la consultazione delle informazioni, senza dover accedere ai singoli prodotti destinati alla gestione operativa degli asset. Inoltre devono essere standardizzati i processi relativi agli stessi, quali l'inserimento di un nuovo asset o la sua rimozione, per facilitarne il controllo e l'esecuzione.

2.3 Processi richiesti

La direzione ha segnalato i processi chiave che devono essere rivisti e standardizzati:

- Provisioning
- Deprovisioning
- Gestione ordinaria
- Gestione straordinaria
- Conformità legale

Il provisioning riguarda l'ingresso nel processo aziendale di un nuovo asset, che deve essere censito e registrato opportunamente all'interno dei sistemi.
Il deprovisioning è l'operazione inversa, in altre parole l'uscita dell'asset dal processo aziendale.
La gestione ordinaria prevede la manutenzione dell'asset, dagli aggiornamenti software per un asset macchina al rinnovo delle credenziali per un asset utente. All'interno di questa gestione rientra anche il rinnovo delle licenze e dei vari contratti.
All'interno della gestione straordinaria rientrano tutti i guasti e le modifiche agli asset non previsti durante la manutenzione ordinaria.
La conformità legale viene indicata come il processo di aggiornamento e verifica degli altri processi che siano conformi alle normative vigenti, nonché la segnalazione agli utenti di eventuali variazioni delle procedure da adottare.

Capitolo 3

Analisi

Tenendo conto di tutti gli obblighi legali e le richieste della direzione è stata svolta un'intensa attività d'analisi, che affronta gli aspetti chiave dei sotto problemi che il sistema presenta nella sua complessità.

3.1 Analisi del problema

Il problema è molto complesso data l'eterogeneità dei dati e degli strumenti. Possiamo però suddividerlo in sotto problemi per poterne analizzare meglio i vari aspetti. Inoltre bisogna allineare i dati attualmente archiviati con la nuova organizzazione e le nuove procedure.

3.1.1 Acquisizione nuovi dati

I dati vengono generati da varie sorgenti e la natura stessa degli asset è profondamente diversa. Una macchina fisica ha dati identificativi e descrittivi diversi da un utente, nonché da un software o da un documento.
Inoltre ogni utente ha un modo diverso di scrivere e di memorizzare i dati. Questo comporta la memorizzazione di dati incoerenti sintatticamente, anche se non semanticamente, che causa problemi in fase di ricerca e analisi dei dati stessi creando, di fatto, duplicati non necessari.
L'utilizzo di automatismi informatici riduce sensibilmente il rischio, creando template diversi a seconda dell'asset e delle sue caratterizzazioni che andranno applicati agli asset in fase di inse-

rimento e modifica. Inoltre bisogna definire pattern per la nomenclatura in modo da unificare l'inserimento dei dati manuali. Ogni asset presenta pertanto informazioni generate automaticamente dal sistema e altri manualmente. Di seguito indichiamo i parametri identificativi e descrittivi, specificando come debbano essere generati e compilati.

a) Utenti

Parametro	**Descrizione**	**Generazione**
IDAsset	Campo identificativo dell'utente.	Generato automaticamente dal sistema. Deve essere univoco rispetto a tutti gli asset.
Cognome	Cognome dell'utente	Generato manualmente. Deve essere creato seguendo il pattern di nomenclatura utente.
Nome	Nome dell'utente	Generato manualmente. Deve essere creato seguendo il pattern di nomenclatura utente.
Area	Indica l'area aziendale in cui è inquadrato l'utente.	Selezionato da un elenco precostituito di modelli. Possono esserne selezionati più di uno.
Incarico	Indica il livello di permesso di accesso ai dati aziendali.	Selezionato da un elenco precostituito di modelli. Avrà effetto anche sui permessi di accesso ai dati all'interno dell'azienda. Possono esserne selezionati più di uno.

Contatti	Indica tutti i contatti a cui è possibile rintracciare l'utente.	L'e-mail aziendale è generata dal sistema in automatico in base ad un pattern deciso precedentemente. Altri contatti sono inseriti manualmente secondo il pattern nomenclatura utente.

b) Documenti

Parametro	**Descrizione**	**Generazione**
IDAsset	Campo identificativo del documento.	Generato automaticamente dal sistema. Deve essere univoco rispetto a tutti gli asset.
Titolo	Titolo del documento	Generato manualmente. Deve essere creato seguendo il pattern di nomenclatura documento.
Asset di riferimento	Identifica l'asset al quale il documento è collegato.	Selezionato dall'elenco degli asset, dall'operatore o dal sistema. Possono essere più di uno.
Localizzazione	La posizione dove il documento è archiviato digitalmente.	Generato in automatico dal sistema.
Scadenza	Scadenza del documento	Generato manualmente secondo un pattern prestabilito.

c) Macchine

Parametro	**Descrizione**	**Generazione**
IDAsset	Campo identificativo della macchina.	Generato automaticamente dal sistema. Deve essere univoco rispetto a tutti gli asset.
Produttore	Indica il produttore	Generato automaticamente dal sistema prelevandolo dal registro.
Modello	Indica il modello della macchina.	Generato automaticamente dal sistema prelevandolo dal registro.
Sistema Operativo	Indica il sistema operativo installato.	Generato automaticamente dal sistema prelevandolo dal registro.
Software installati	Riporta i software installati sulla macchina.	Generato automaticamente dal sistema prelevandolo dal registro. Possono essere più di uno.
Utente principale	Identifica chi è l'utente principale che opera sulla macchina.	Selezionato dall'elenco Asset Utenti.
Fine Garanzia	Indica quando la garanzia della macchina scade, per valutarne se possibile un'estensione, o la sostituzione della stessa.	Generato manualmente secondo un pattern prestabilito.
Fornitore	Indica il fornitore	Selezionato da un elen-

	presso il quale si è acquistato il prodotto e presso il quale richiedere assistenza hardware.	co precostituito.

d) Software

Parametro	**Descrizione**	**Generazione**
IDAsset	Campo identificativo del software.	Generato automaticamente dal sistema. Deve essere univoco rispetto a tutti gli asset.
Produttore	Indica il produttore.	Generato automaticamente dal sistema prelevandolo dal registro.
Nome	Nome del software.	Generato automaticamente dal sistema prelevandolo dal registro.
Versione	Versione del software	Generato automaticamente dal sistema prelevandolo dal registro.
Tipo	Identifica se il software è un sistema operativo.	Generato automaticamente dal sistema prelevandolo dal registro.
Sistema Operativo Compatibile	Indica il sistema operativo su cui può essere installato.	Selezionato dall'elenco Asset Software di tipo OS. Possono esserne selezionati più di uno.
Termine Supporto	Indica quando il produttore terminerà il supporto al software.	Selezionato da un elenco precostituito.

Ogni elenco precostituito indicato deve essere compilato secondo specifici pattern; tutti i pattern devono poi essere approvati dalla direzione, poiché costituiscono parte integrante delle procedure.

3.1.2 Memorizzazione dei dati

Il principale problema di avere più fonti di dati è la replica incoerente dei dati stessi. È necessario pertanto prevedere una sincronizzazione tra le fonti primarie in modo che tali dati siano coerenti a meno di un ciclo di aggiornamento.

3.1.3 Rimozione dei dati

La dismissione di un asset non è di immediata soluzione. Bisogna, infatti, rimuovere l'accesso ai dati dell'asset dismesso, ma al contempo bisogna archiviarli in modo da conservarli per eventuali necessità di recupero dei dati. L'archiviazione deve avvenire in un ambiente separato e protetto da password.

3.1.4 Accesso ai dati

Esistono figure diverse all'interno del sistema con autorizzazioni diverse di accesso ai dati. Tali distinzioni sono da mantenere per rispetto della privacy sui vari dati.

Ruolo	**Accessi**
Operatore	Completo a tutto il sistema, ad eccezione delle autorizzazioni.
Responsabile	Accesso completo al sistema.
Utente	Consultazione parziale, riferita solo a lui. Possibilità di generare chiamate.

Deve essere garantita la sicurezza attraverso l'utilizzo di password complesse e con rinnovo ciclico (ottimi 90 giorni). Inoltre gli utenti amministrativi non devono avere nomi di facile individuazione, per evitare di facilitare attacchi al sistema. Anche eventuali utenti di sistema devono avere nomi significativi ma non di facile deduzione per lo stesso motivo.

3.1.5 Scadenzario

Rientra tra i problemi primari di un'azienda la programmabilità degli interventi da effettuare per il mantenimento della propria infrastruttura distribuendo i costi lungo un periodo di tempo prefissato. Si rende pertanto necessaria la progettazione di uno scadenzario che presente con anticipo quando devono essere fatti gli interventi manutentivi ordinari degli asset, le scadenze di licenze e garanzie, il termine del supporto per certi prodotti.

3.1.6 Processi ulteriori

Rispetto ai processi individuati dalla direzione, sono stati individuati ulteriori processi, in particolare sono stati suddivisi i processi di Gestione Ordinaria e di Gestione Straordinaria.
Il primo è stato suddiviso nei processi di Gestione Manutenzione, Gestione Eventi e Gestione Scadenze.
Il secondo in Gestione Guasti, Gestione Installazioni e Gestione Infezioni.
La Gestione Manutenzioni riguarda le operazioni cicliche di manutenzione degli asset macchina, quali l'installazione di aggiornamenti, la verifica dello stato dei dischi e l'analisi del registro eventi.
La Gestione Eventi tratta le procedure da seguire a seguito della segnalazione dei sistemi di monitoraggio di un errore, grave o critico, su di un asset.

La Gestione Scadenze è inerente alla gestione dello scadenzario, es. per rinnovi ed estensioni di garanzia.
La Gestione Guasti disciplina invece l'apertura di una chiamata per un guasto a un asset e la sua riparazione.
La Gestione Installazioni tiene monitorate le installazioni sugli asset: se viene rilevato un nuovo software viene segnalato ai tecnici IT che devono verificare la presenza della relativa autorizzazione.
La Gestione Infezioni infine esplicita la procedura per far fronte a un'eventuale rilevazione di virus all'interno del gruppo degli asset e alla loro rimozione.

3.2 Architettura logica

Viene presentata di seguito l'architettura logica del sistema nei suoi tre aspetti cardine: struttura, comportamento e interazioni.

3.2.1 Struttura

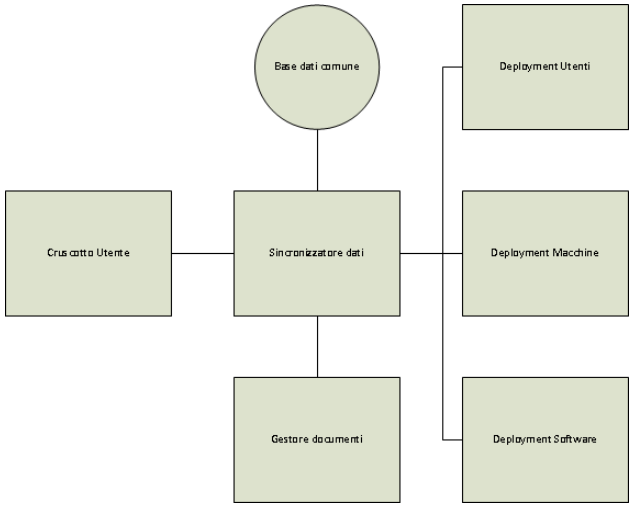

Figura 1 – Sistema – struttura logica

Dall'analisi effettuata risulta quindi la struttura logica di cui sotto. Esistono i tre strumenti principali per la gestione operativa dei vari tipi di asset. Tutti sono connessi al Sincronizzatore Dati che esegue la raccolta dati e la loro sincronizzazione. Gestisce anche l'accesso ai documenti e a tutte le informazioni. Il cruscotto utente è l'interfaccia attraverso cui gli utenti interagiscono con il sistema.

3.2.2 Comportamento

Di seguito sono presentati i modelli di comportamento del sistema per ogni processo individuato.

a) Provisioning

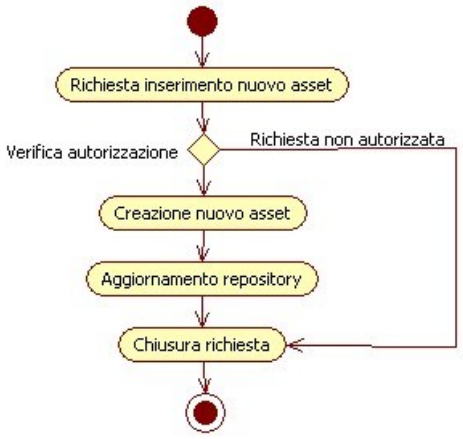

Figura 2 - Provisioning – comportamento

b) Deprovisioning

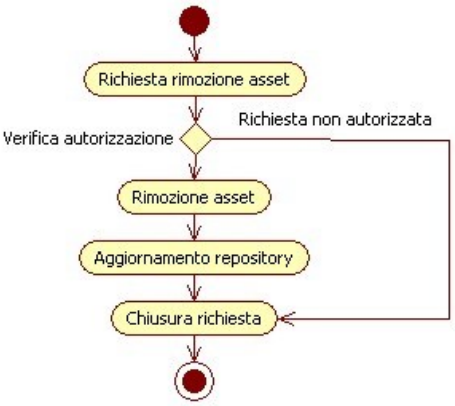

Figura 3 - Deprovisioning – comportamento

c) Gestione ordinaria degli asset
   a. Gestione manutenzioni

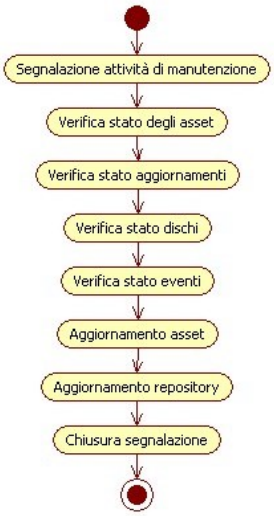

Figura 4 - Gestione manutenzione – comportamento

b. Gestione scadenze

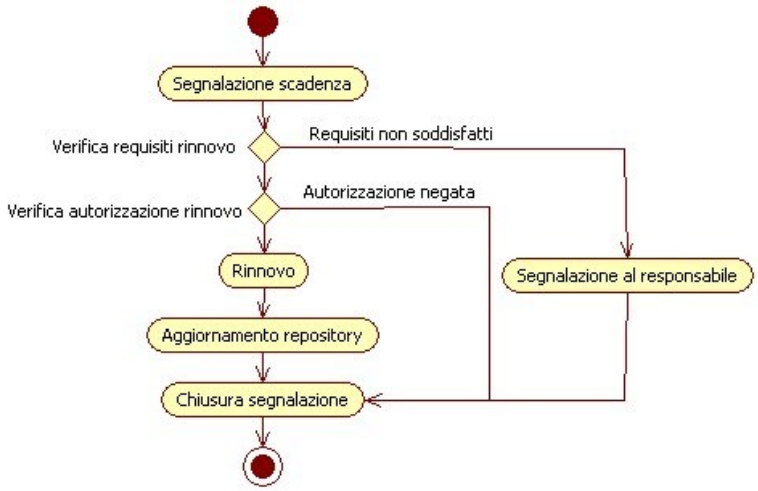

Figura 5 - Gestione scadenze – comportamento

c. Gestione eventi

Figura 6 - Gestione eventi – comportamento

d) Gestione straordinaria degli asset
    a. Gestione guasti

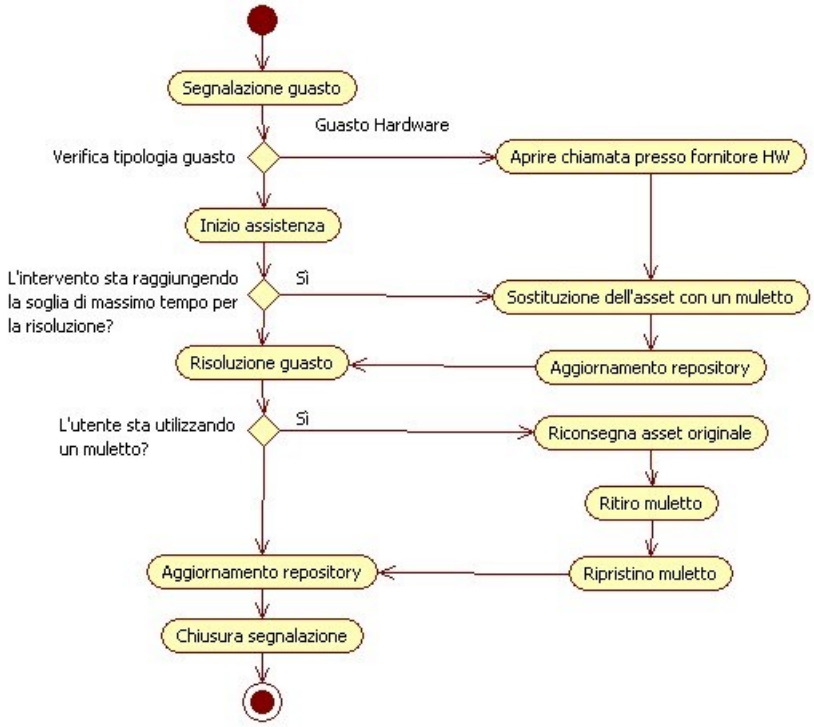

Figura 7 - Gestione guasti – comportamento

b. Gestione installazioni

Figura 8 - Gestione installazioni – comportamento

c. Gestione infezioni

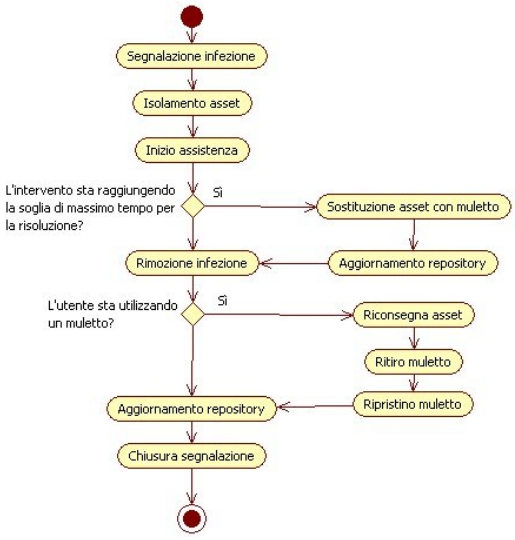

Figura 9 - Gestione infezioni – comportamento

e) Conformità legale

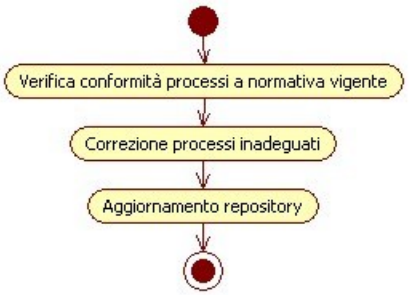

Figura 10 - Conformità legale – comportamento

3.2.3 Interazioni

Nei seguenti schemi di interazioni tra le varie parti del sistema, oltre a quelle già indicate all'interno della struttura, compaiono le figure di "Utente", "Responsabile" e "Operatore" che corrispondono alla componente umana che interagisce ordinariamente con il sistema. Viene aggiunta anche la figura di "Asset" che rappresenta l'asset su cui bisogna intervenire secondo le situazioni.
Non viene presentato il Cruscotto Utente poiché si considera rappresentato dalle tre figure soprascritte, portando quindi a un inutile appesantimento degli schemi riportati.
Si segue la stessa divisione del paragrafo precedente riportando anche tutte le combinazioni di interazioni significative.
Non vengono presentate interazioni per il processo di "Conformità Legale" perché non ne possiede.

a) Provisioning

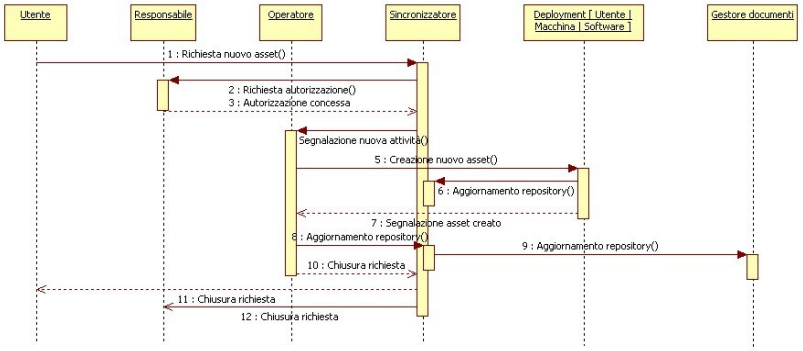

Figura 11 - Richiesta nuovo asset – richiesta autorizzata – interazione

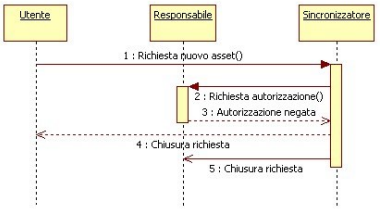

Figura 12 - Richiesta nuovo asset – richiesta non autorizzata – interazione

b) Deprovisioning

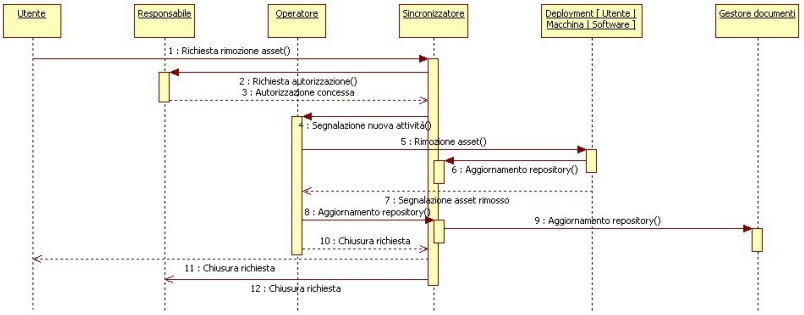

Figura 13 - Richiesta rimozione asset – richiesta autorizzata – interazione

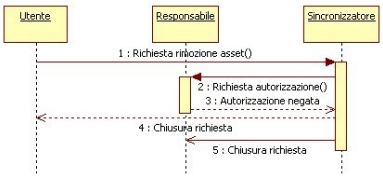

Figura 14 - Richiesta rimozione asset – richiesta non autorizzata – interazione

c) Gestione ordinaria degli asset

a. Gestione manutenzioni

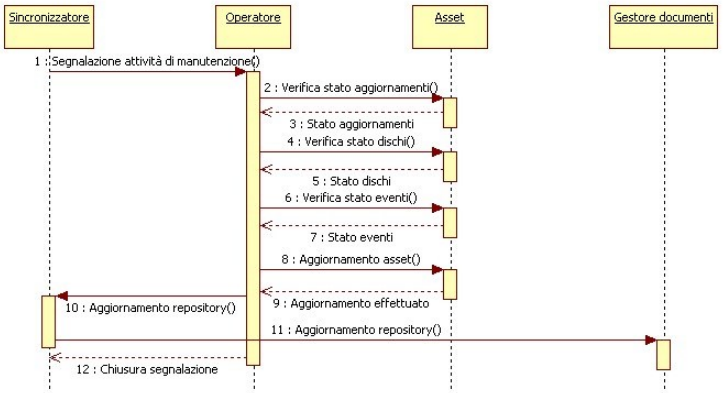

Figura 15 - Gestione manutenzioni – interazione

b. Gestione scadenze

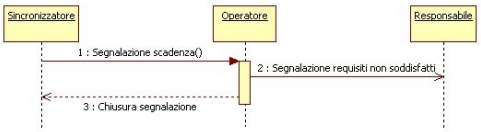

Figura 16 - Gestione scadenze – requisiti non soddisfatti – interazione

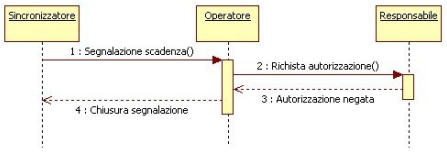

Figura 17 - Gestione scadenze – autorizzazione negata – interazione

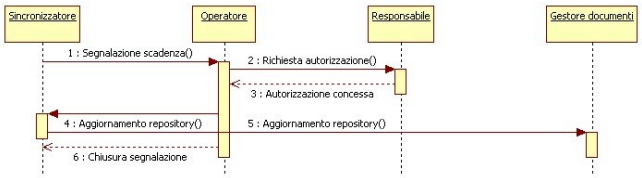

Figura 18 - Gestione scadenze – rinnovo autorizzato – interazione

c. Gestione eventi

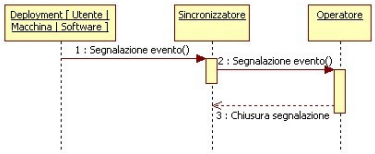

Figura 19 - Gestione eventi – falso allarme – interazioni

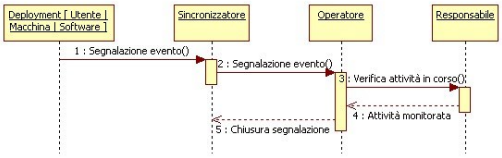

Figura 20 - Gestione eventi – attività monitorata – interazione

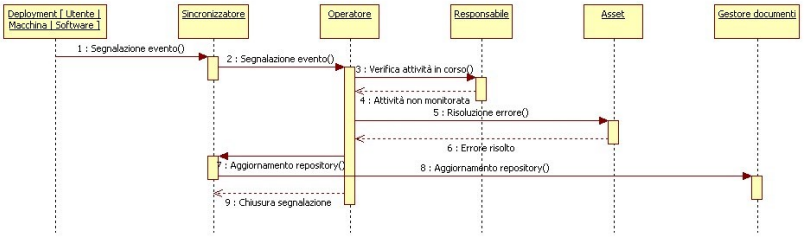

Figura 21 - Gestione eventi – errori non previsti – interazione

d) Gestione straordinaria degli asset
    a. Gestione guasti

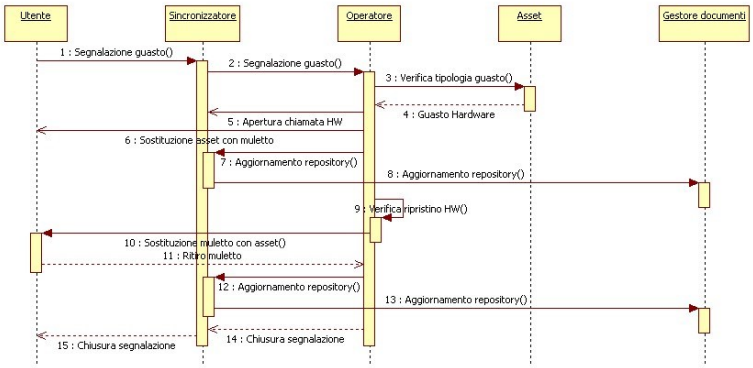

Figura 22 - Gestione guasti – guasto hardware - interazione

Figura 23 - Gestione guasti – guasto software – interazione

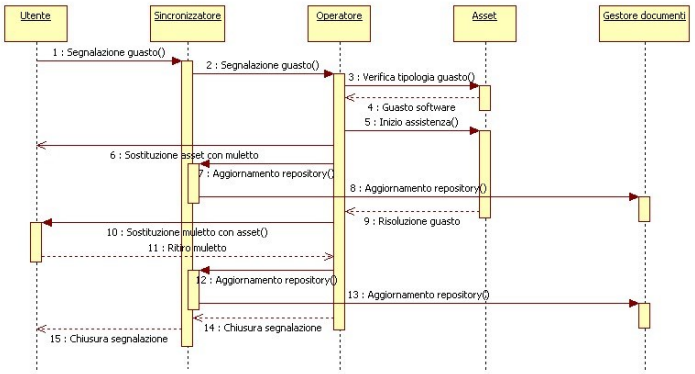

Figura 24 - Gestione guasti – guasto software con muletto – interazione

b. Gestione installazioni

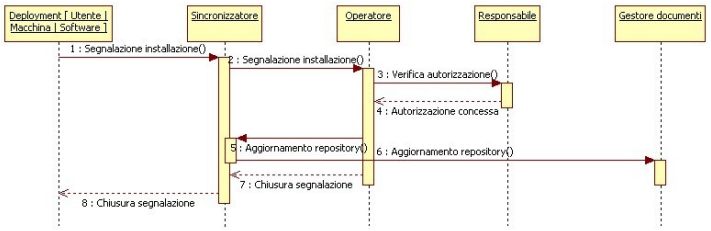

Figura 25 - Gestione installazioni – installazione autorizzata – interazione

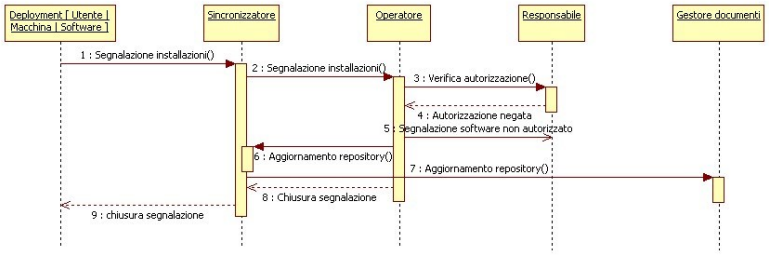

Figura 26 - Gestione installazioni – installazione non autorizzata – interazione

c. Gestione infezioni

Figura 27- Gestione infezioni – rimozione infezione – interazione

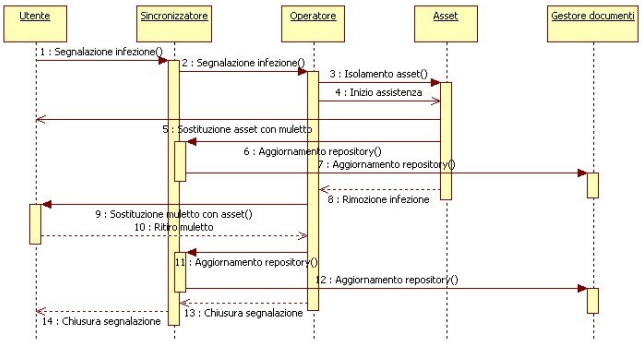

Figura 28 - Gestione infezioni – rimozione infezione con muletto – interazione

Capitolo 4

Progetto

Il sistema è progettato sfruttando gli strumenti già presenti in azienda, integrandoli con alcuni connettori ai quali è affidata la sincronizzazione dei dati per permettere una consultazione degli stessi più rapida. Il cruscotto utente è l'interfaccia principale del sistema, attraverso la quale gli utenti e i responsabili interagiscono con esso. Come si evince dai processi gli operatori lo utilizzano come unico punto di accesso per la visione dello stato degli asset, per poi intervenire direttamente sugli stessi, curandosi poi di aggiornare la documentazione che non è generata automaticamente dal sistema.

4.1 Scelte progettuali

Si preferisce utilizzare alcuni strumenti commerciali già a disposizione da integrare poi tra di loro per ottenere un buon compromesso tra efficienza e modifica alla struttura preesistente.
I principali prodotti utilizzati sono:

- Microsoft Dynamics Customer Relationship Management (CMR)
- Microsoft System Center Configuration Manager (SCCM)
- Monitoring As A Service (MAAS)
- Microsoft Sharepoint (SP)

CRM gestirà la base dati comune e il cruscotto utente.
Sharepoint sarà il repository documentale di tutto il sistema.
SCCM è lo strumento per il deployment delle macchine client e il loro inventario software.
MAAS infine gestirà la segnalazione eventi delle macchine.

Si utilizzerà una farm in Cloud dove inserire la gestione core dell'applicazione, come il server CRM, lasciando presso l'azienda solo il server SCCM e il Proxy MAAS. Questo permette di avere accesso al sistema anche in caso di problemi alla rete intranet aziendale e di gestire anche questo tipo di chiamate.
Saranno inseriti connettori che eseguiranno la sincronizzazione tra i vari strumenti, creando in questo modo l'integrazione degli stessi. I connettori avranno anche il compito di aprire segnalazioni in modo proattivo in caso di eventi non previsti.

4.2 Architettura

Il sistema presenta una distribuzione dei vari componenti su diverse macchine, dislocate in almeno due aree separate, la rete interna aziendale e in Cloud. Oltre agli strumenti già presenti in azienda, vengono creati alcuni connettori ai quali è affidata la sincronizzazione dei dati e la gestione di situazioni monitorate dagli strumenti.
Il connettore SCCM-CRM, da installare sul server SCCM, permette di trasmettere i dati delle macchine presenti in azienda alla base dati comune, sincronizzando tra loro i due database. Oltre al caricamento dei dati nel momento del deploy di una nuova macchina, esegue con frequenza giornaliera la sincronizzazione dell'inventario, verificando eventuali modifiche e segnalandole aprendo i casi relativi sul CRM.
Il connettore MAAS-CRM, da installare sul server MAAS, si occupa di aprire casi sul CRM in base agli eventi rilevati nel sistema, se questi non sono già stati aperti.
Il connettore AD-CRM, invece, è da utilizzare per creare i nuovi utenti all'interno del dominio aziendale per cui dovrà essere installato sul Domain Controller primario del dominio. Oltre a creare fisicamente gli utenti sull'interno di Active Directory in

conformità a dei modelli precostituiti sulle politiche aziendali, crea gli asset utenti direttamente sul CRM.

4.2.1 Struttura

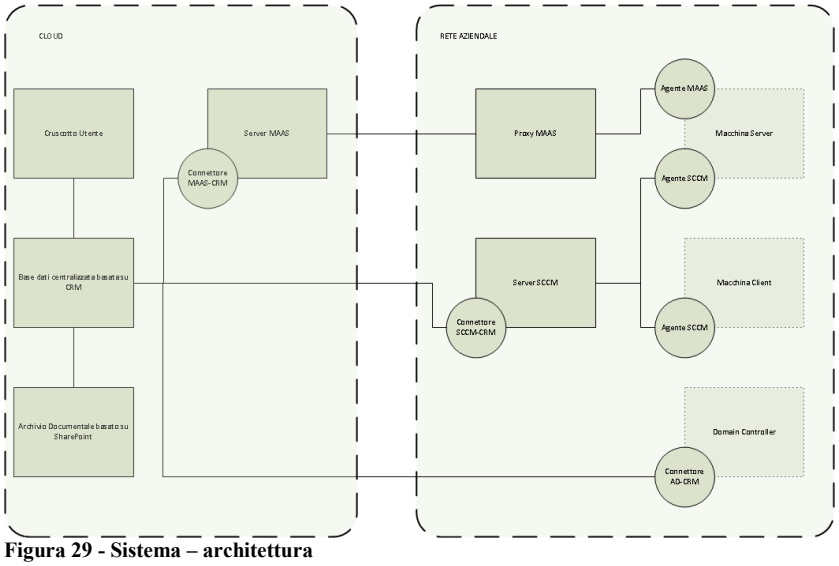

Figura 29 - Sistema – architettura

Lo schema evidenzia anche la dislocazione spaziale delle singole parti. I server SCCM e il Proxy MAAS devono restare in azienda per vincoli tecnici, mentre il server MAAS deve essere al di fuori della rete. Il server SCCM deve risiedere nella rete per poter eseguire il deploy completo delle macchine client eseguendo anche l'inserimento a dominio delle stesse. Il Proxy MAAS e il server MAAS, risiedendo rispettivamente all'interno e all'esterno della rete, permettono di individuare anche un problema alla connettività internet dell'azienda, oltre agli errori ed eventi che si possono verificare dalle varie macchine.

4.2.2 Comportamento

a) Provisioning

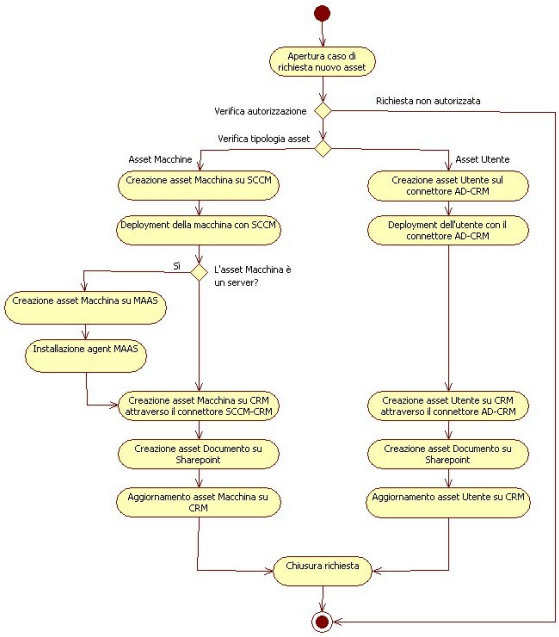

Figura 30 - Richiesta nuovo asset – comportamento

b) Deprovisioning

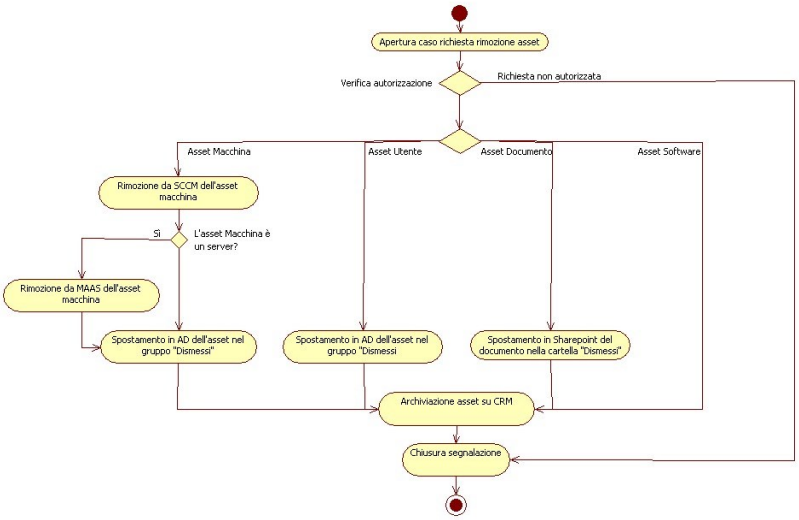

Figura 31 - Richiesta rimozione asset – comportamento

Il deprovisioning non prevede una cancellazione definitiva dei dati relativi ma la semplice archiviazione dei dati, raggiungibili nuovamente solo da un amministratore del sistema.

Al decorrere dei tempi di conservazione determinati dalla direzione aziendale, tali oggetti verranno definitivamente cancellati.

c) Gestione ordinaria degli asset
    a. Gestione manutenzioni

Figura 32 - Gestione manutenzioni – comportamento

La segnalazione viene generata dallo scadenzario su CRM.

    b. Gestione scadenze

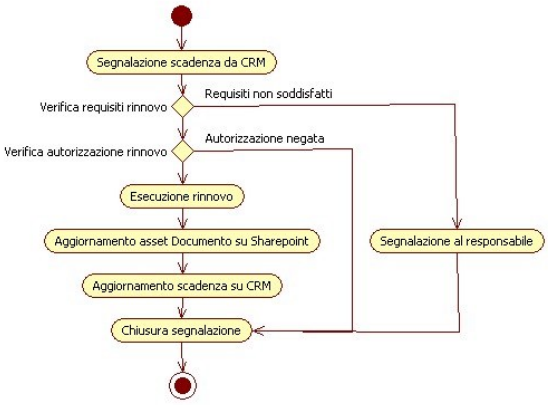

Figura 33 - Gestione scadenze – comportamento

La segnalazione viene generata dallo scadenzario su CRM.

c. Gestione eventi

Figura 34 - Gestione eventi – comportamento

Il connettore MAAS-CRM riceve una segnalazione di evento da parte del Proxy MAAS e quindi dall'agente MAAS installato sulla macchina, e apre il caso una volta verificato che lo stesso non fosse già aperto e in corso.

Si segnalano sempre anche i falsi positivi, per tenere traccia di cosa viene rilevato dal sistema. Se l'evento segnalato risulta essere indicato anche dai produttori come evento ignorabile, lo si potrà escludere dal monitoraggio all'interno di MAAS per cui non verrà più segnalato.

d) Gestione straordinaria degli asset
    a. Gestione guasti

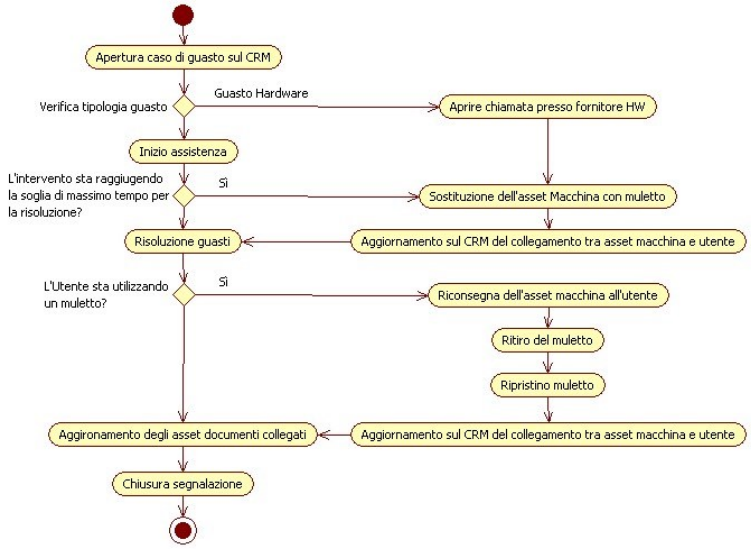

Figura 35 - Gestione guasti – comportamento

La gestione guasti riguarda i client, perché i guasti server sono già contemplati all'interno della gestione eventi. Pertanto il guasto in oggetto deve essere segnalato dagli utenti.

Se il guasto è hardware oppure i tempi di risoluzione del problema superano una certa soglia temporale prestabilita dagli standard di qualità aziendali si procede alla sostituzione dell'asset con un muletto per permettere all'utente di continuare a lavorare. La cosa deve essere ovviamente tracciata nella documentazione per permettere di avere una chiara situazione degli asset in ogni momento.

b. Gestione installazioni

Figura 36 - Gestione installazioni – comportamento

Se al momento della sincronizzazione il connettore SCCM-CRM rileva una modifica ai software installati sulla macchina, apre il caso sul CRM.

c. Gestione infezioni

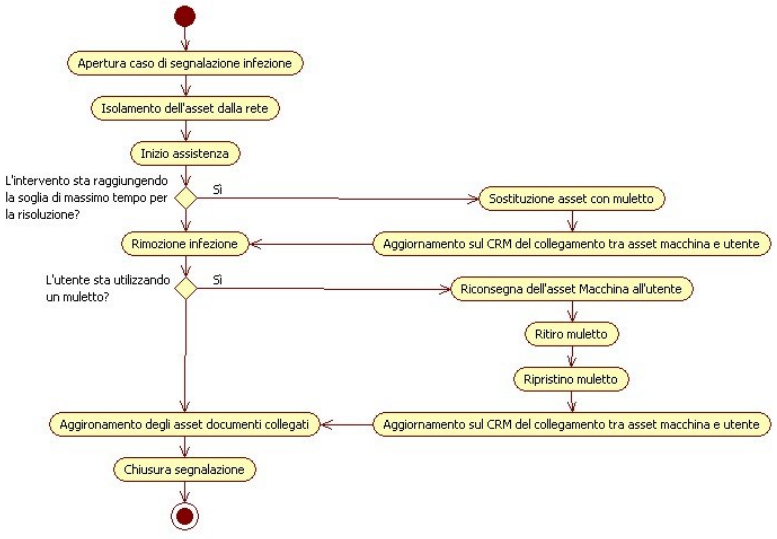

Figura 37 - Gestione infezioni – comportamento

La segnalazione di infezione è a carico dell'utente, perché si tratta di attacchi virali che l'antivirus non è in grado di individuare e rimuovere per cui si deve operare direttamente sulla macchina per rimuovere l'infezione. Come per i guasti, se il tempo di risoluzione supera il limite preposto, si deve procedere alla sostituzione dell'asset con un muletto per poter permette all'utente di lavorare.

e) Conformità legale

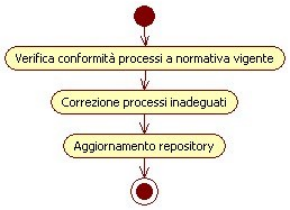

Figura 38 - Conformità legale – comportamento

4.2.3 Interazioni

a) Provisioning

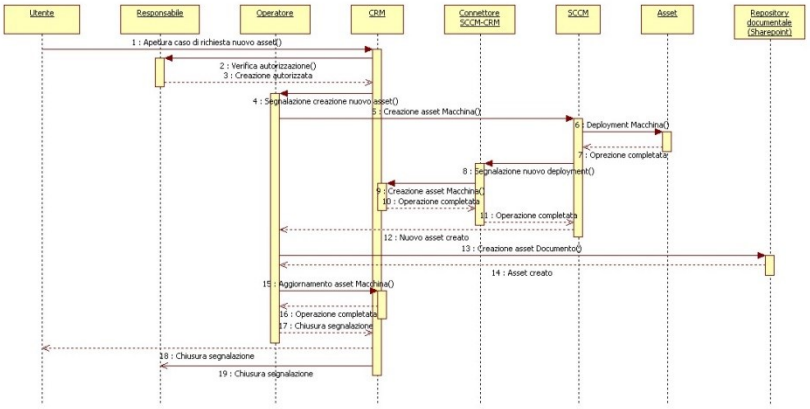

Figura 39 - Richiesta creazione nuovo asset – macchina client – interazione

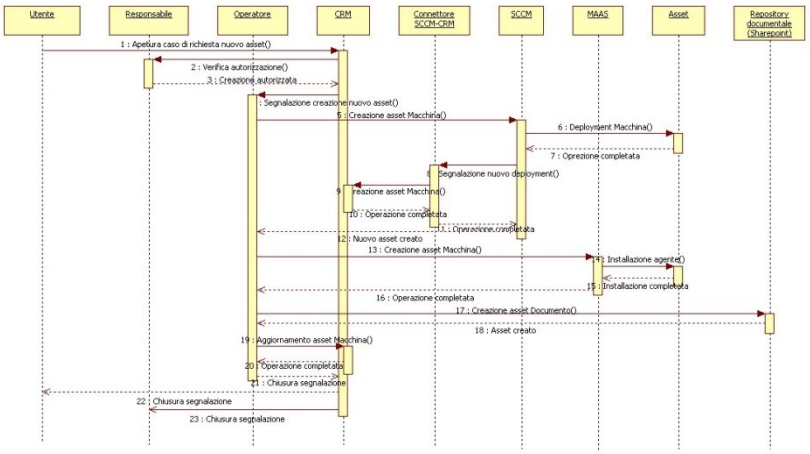

Figura 40 - Richiesta creazione nuovo asset – macchina server – interazione

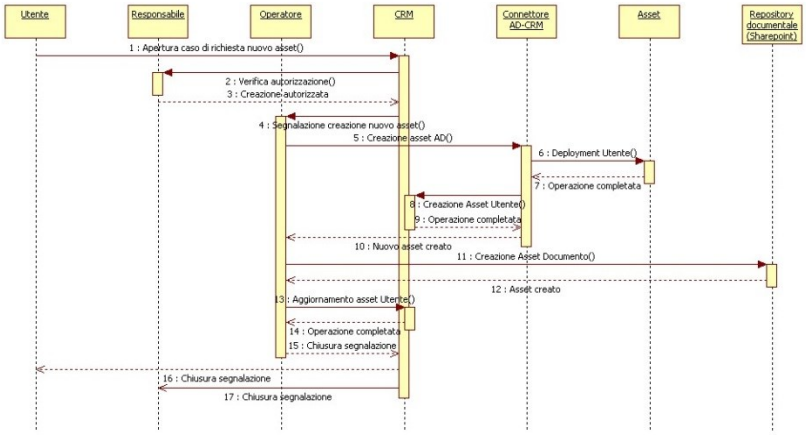

Figura 41 - Richiesta creazione nuovo asset – utente – interazione

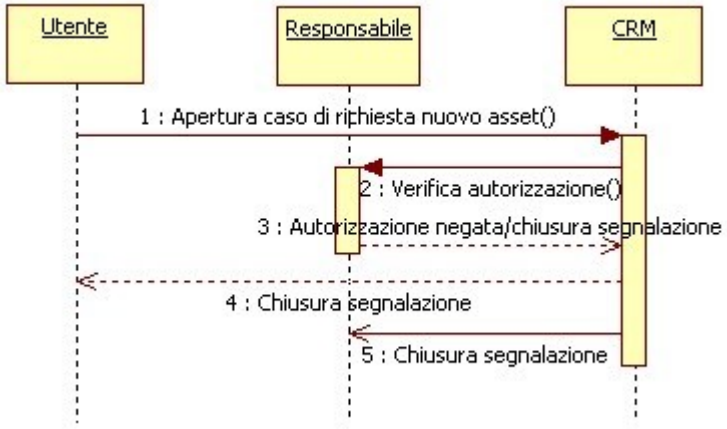

Figura 42 - Richiesta creazione nuovo asset – richiesta rifiutata – interazione

b) Deprovisioning

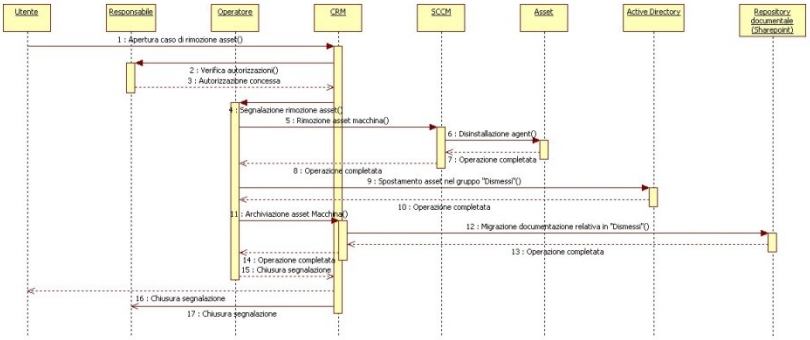

Figura 43 - Richiesta rimozione asset – macchina client – interazione

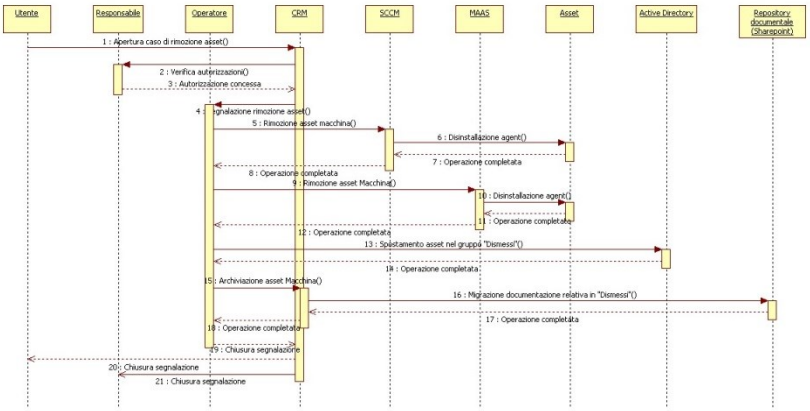

Figura 44 - Richiesta rimozione asset – macchina server – interazione

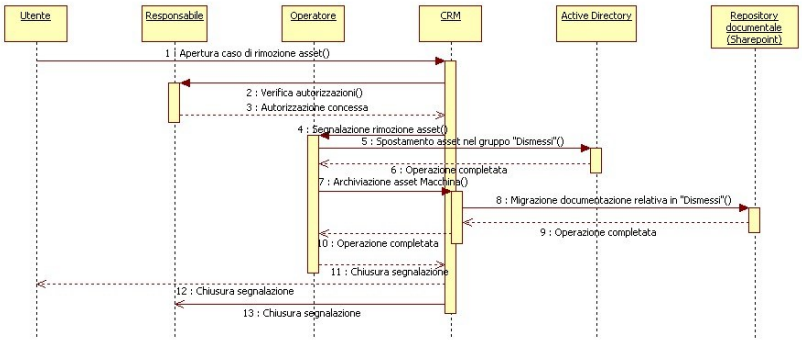

Figura 45 - Richiesta rimozione asset – utente – interazione

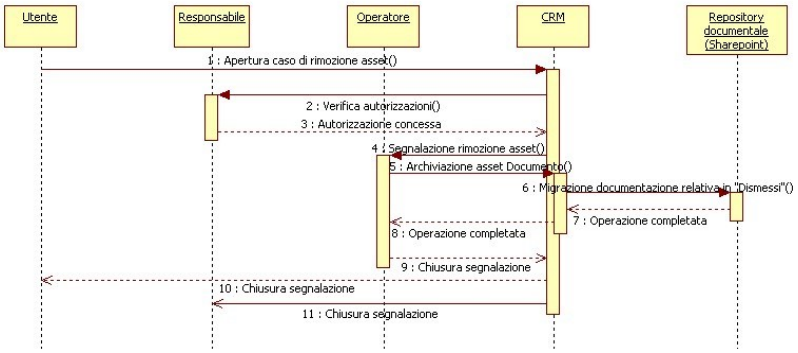

Figura 46 - Richiesta rimozione asset – documento – interazione

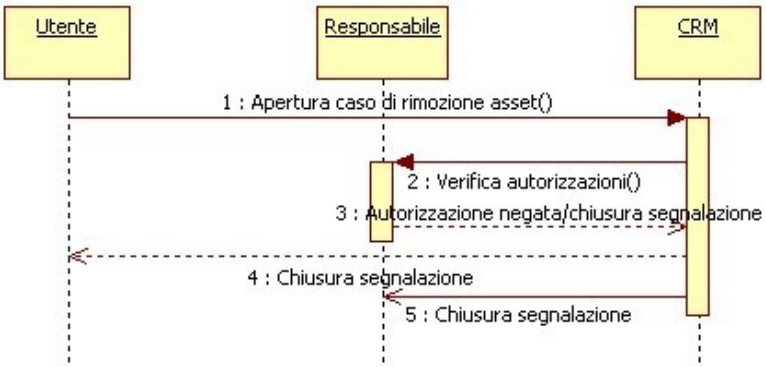

Figura 47 - Richiesta rimozione asset – richiesta rifiutata – interazione

c) Gestione ordinaria degli asset

a. Gestione manutenzioni

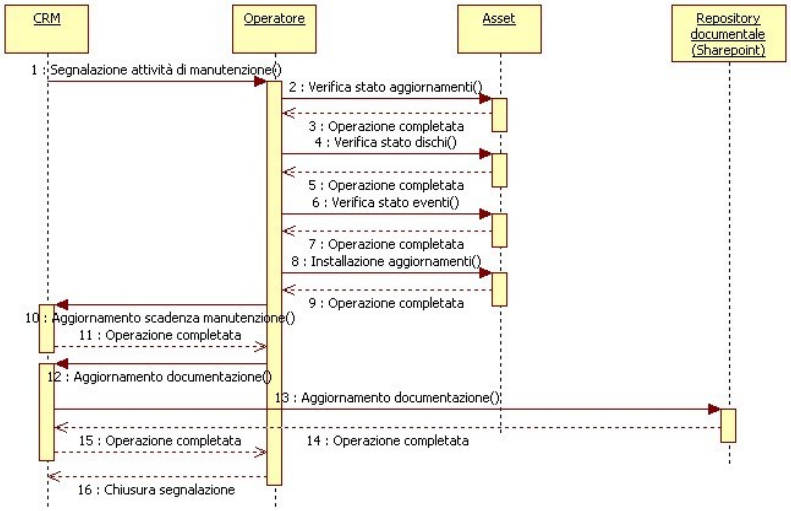

Figura 48 - Gestione manutenzioni – interazione

b. Gestione scadenze

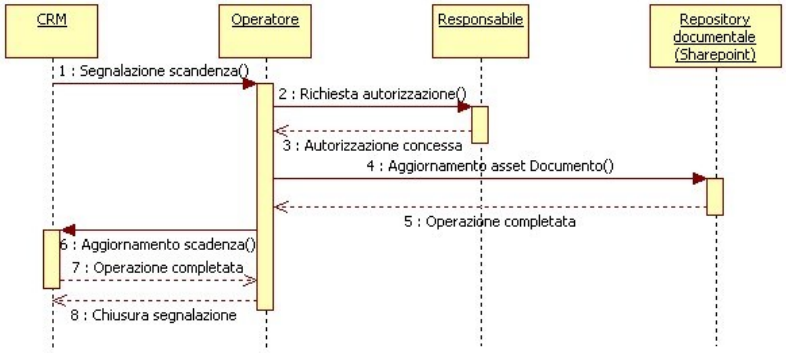

Figura 49 - Gestione scadenze – rinnovo autorizzato - interazione

Figura 50 - Gestione scadenze – rinnovo non autorizzato – interazione

Figura 51 - Gestione scadenze – requisiti non soddisfatti – interazione

c. Gestione eventi

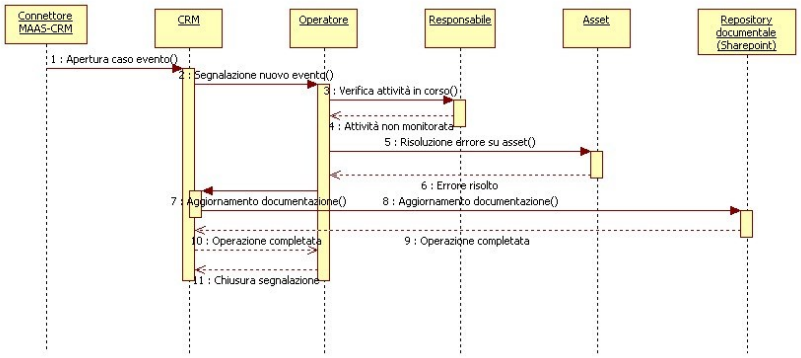

Figura 52 - Gestione eventi – evento non previsto – interazione

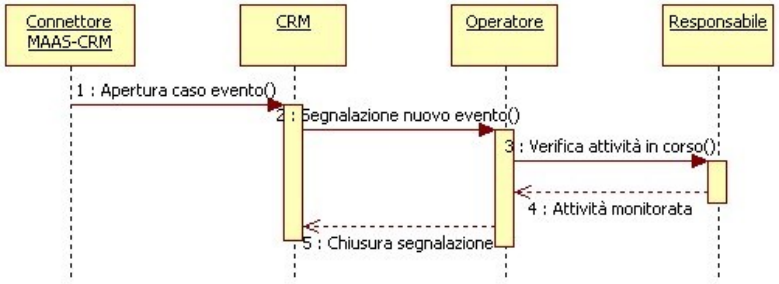

Figura 53 - Gestione eventi – attività monitorata – interazione

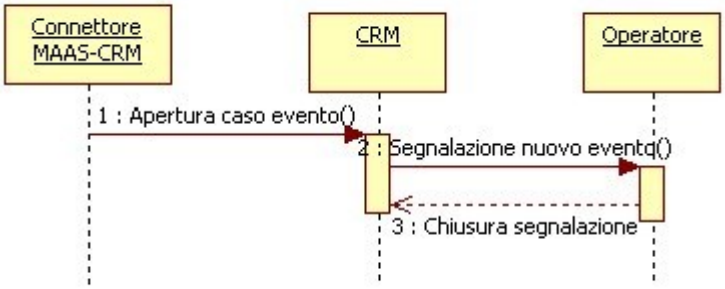

Figura 54 - Gestione eventi – falso positivo – interazione

d) Gestione straordinaria degli asset
    a. Gestione guasti

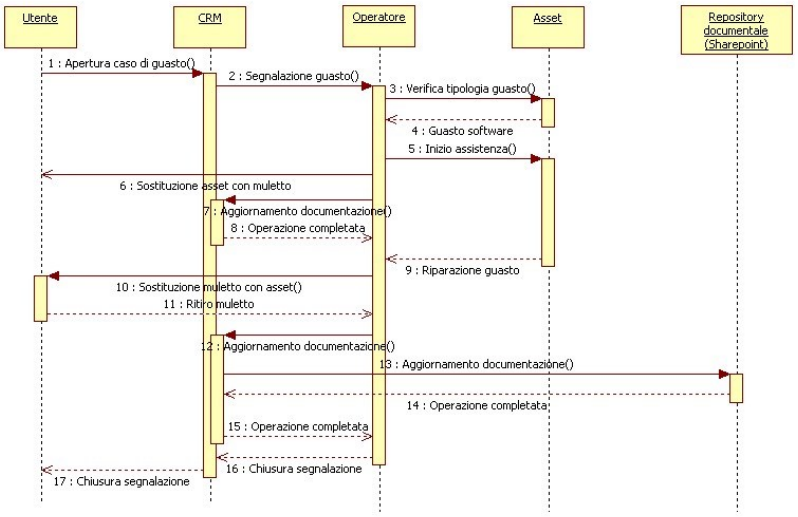

Figura 55 - Gestione guasti – guasto software con muletto – interazione

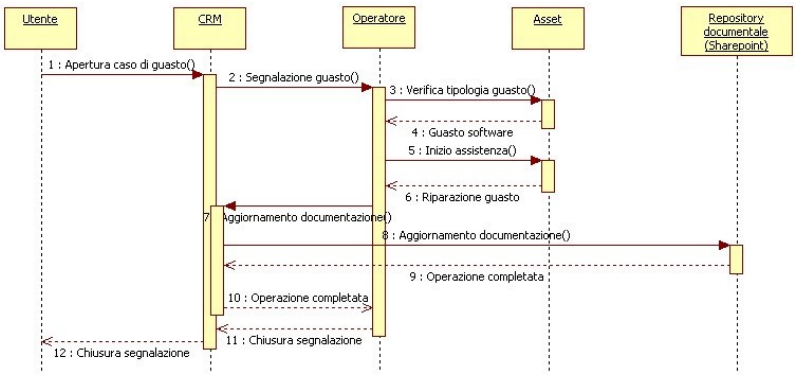

Figura 56 - Gestione guasto – guasto software – interazione

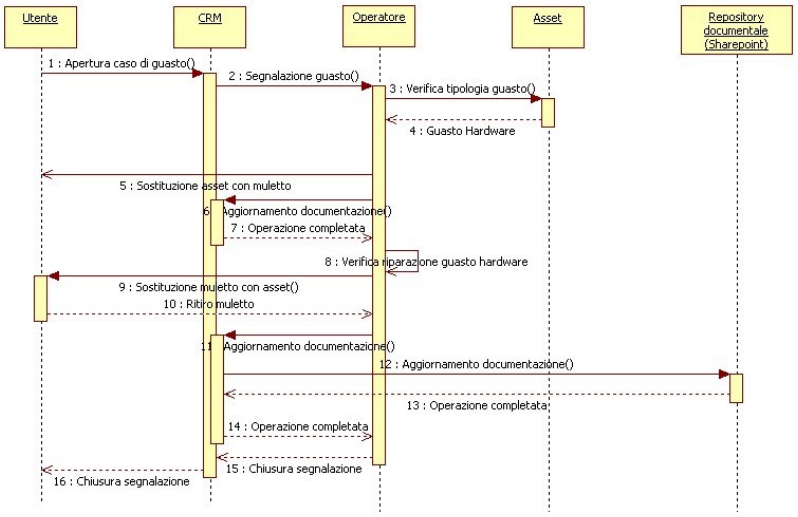

Figura 57 - Gestione guasti – guasto hardware – interazione

b. Gestione installazioni

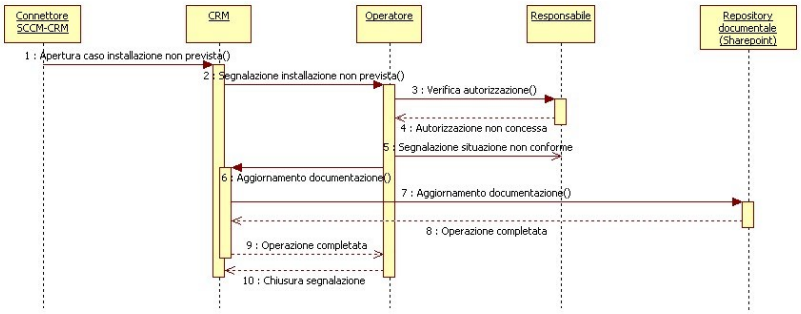

Figura 58 - Gestione installazioni – installazione non autorizzata – interazione

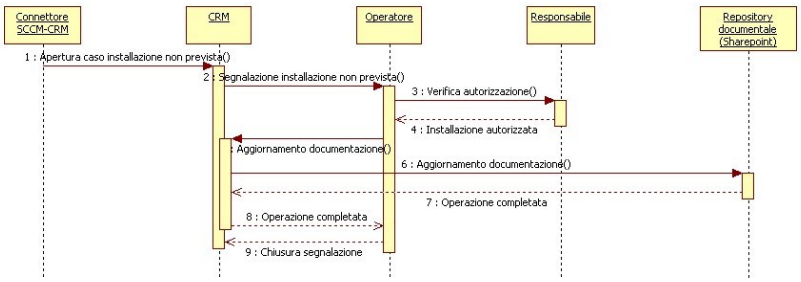

Figura 59 - Gestione installazioni – installazione autorizzata – interazione

c. Gestione infezioni

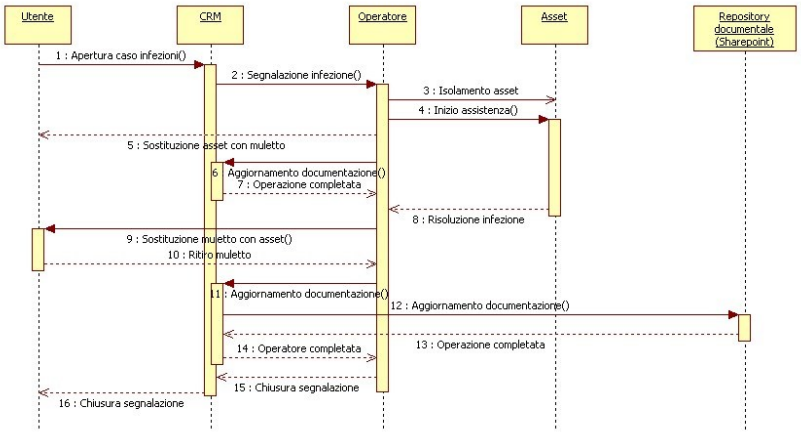

Figura 60 - Gestione infezioni – rimozione infezione con muletto – interazione

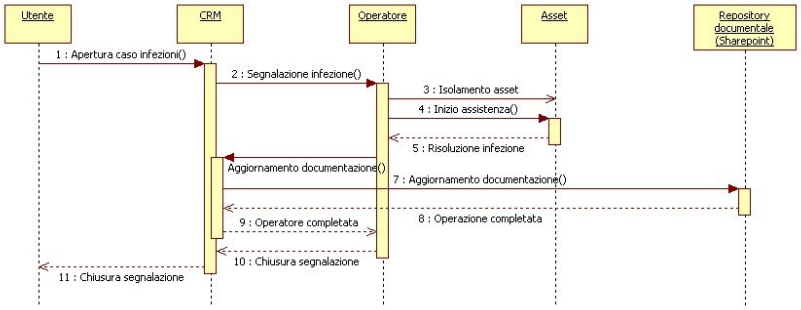

Figura 61 - Gestione infezioni – rimozione infezioni – interazione

4.3 Database

Il database comune, che verrà gestito attraverso CRM, sarà composto dalle seguenti tabelle e con il diagramma E/R posto in calce.

tUtente

Nome campo	**Tipo dati**
(*)IDAsset	Testo
Cognome	Testo
Nome	Testo

tAree

Nome campo	**Tipo dati**
(*)IDArea	Contatore
Descrizione	Testo

tIncarichi

Nome campo	**Tipo dati**
(*)IDIncarico	Contatore
Descrizione	Testo

tContatti

Nome campo	Tipo dati
(*)TipoContatto	Testo
(*)Utente	Testo
Contatto	Testo

tDocumenti

Nome campo	Tipo dati
(*)IDAsset	Testo
Tiolo	Testo
Localizzazione	Testo
Scadenza	Data/ora

tMacchina

Nome campo	Tipo dati
(*)IDAsset	Testo
Produttore	Testo
Modello	Testo
Sistema_Operativo	Testo
Utente_Principale	Testo
Fornitore	Testo
Scadenza	Data/ora

tSoftware

Nome campo	Tipo dati
(*)IDAsset	Testo
Produttore	Testo
Nome	Testo
Versione	Testo
Sistema_Operativo	Sì/No
Termine_Supporto	Data/ora

tSistemiCompatibili

Nome campo	Tipo dati
(*)Software	Testo
(*)Sistema_Operativo	Testo

tSoftwareInstallati

Nome campo	Tipo dati
(*)Macchina	Testo
(*)Software	Testo
Licenza	Testo

tIncarichiUtente

Nome campo	Tipo dati
(*)Utente	Testo
(*)Incarico	Numerico

tAreeUtente

Nome campo	Tipo dati
(*)Utente	Testo
(*)Area	Numerico

tDocumentazioneUtente

Nome campo	Tipo dati
(*)Utente	Testo
(*)Documento	Testo
Tipologia	Numerico

tDocumentazioneMacchina

Nome campo	Tipo dati
(*)Macchina	Testo
(*)Documento	Testo

Tipologia	Numerico

tDocumentazioneSoftware

Nome campo	Tipo dati
(*)Software	Testo
(*)Documento	Testo
Tipologia	Numerico

tTipologieDocumento

Nome campo	Tipo dati
(*)IDTipologia	Contatore
Descrizione	Testo

Diagramma E/R

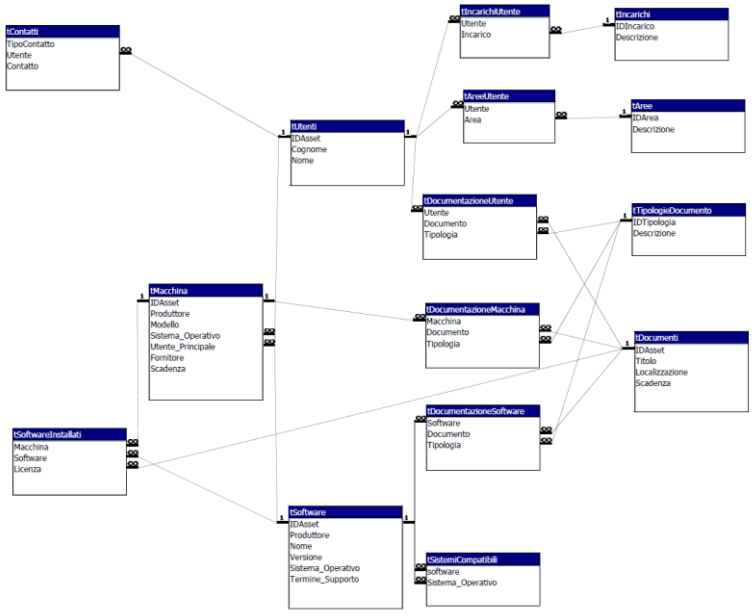

Figura 62 - Database – Schema E/R

4.4 Viste Cruscotto Utente

Di seguito alcune viste del Cruscotto Utente.

a) Vista casi utente

La vista casi utente è la schermata che si presenta agli utenti per verificare lo stato dei casi in corso da lui aperti e poterne aprire altri.

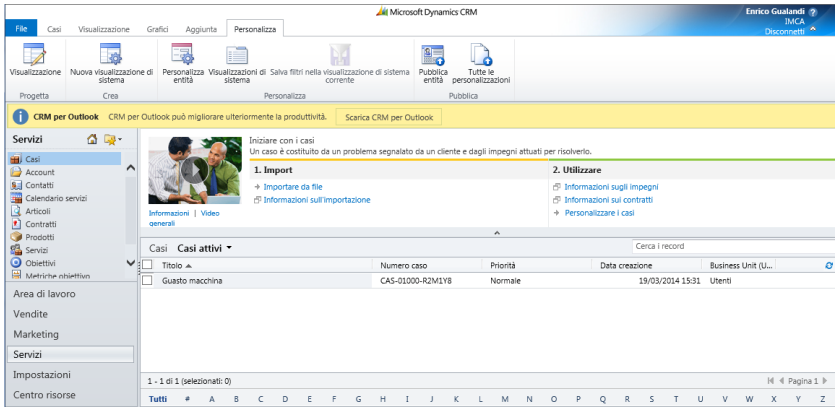

Figura 63 - Vista casi utente

b) Vista caso guasto

Questa è una vista di esempio di un caso di segnalazione guasto.

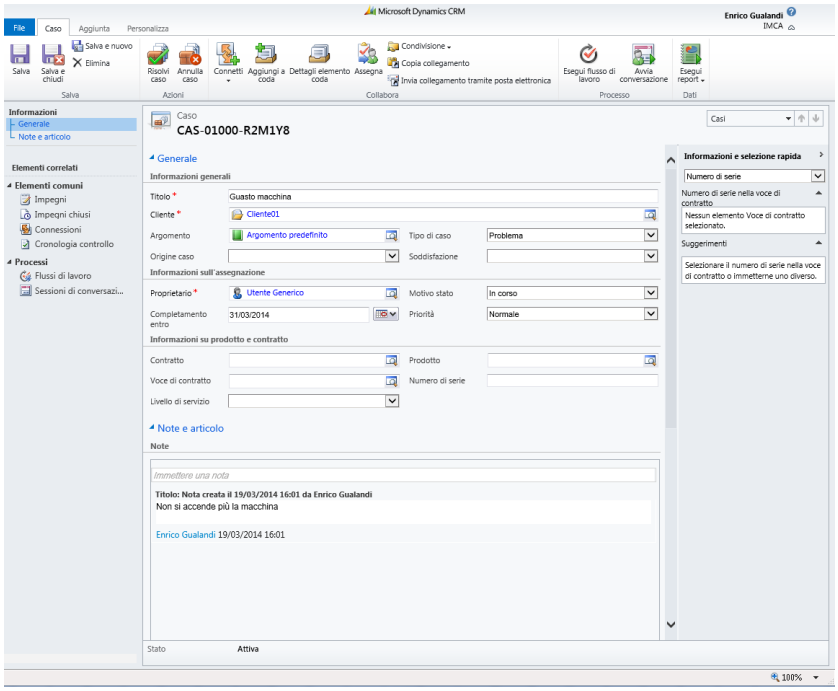

Figura 64 - Vista caso guasto

c) Vista elenco macchine

Questa vista e le seguenti fanno parte delle viste per operatori e responsabili. In particolare questa presenta l'elenco degli asset macchina presenti in azienda.

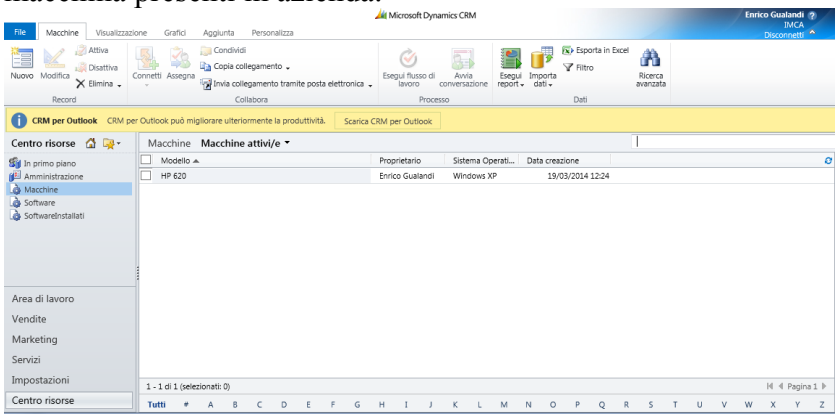

Figura 65 - Vista elenco macchine

d) Vista scheda macchina

Dalla vista precedente, selezionando una macchina specifica, si arriva alla seguente scheda che presenta i dati relativi alla macchina.

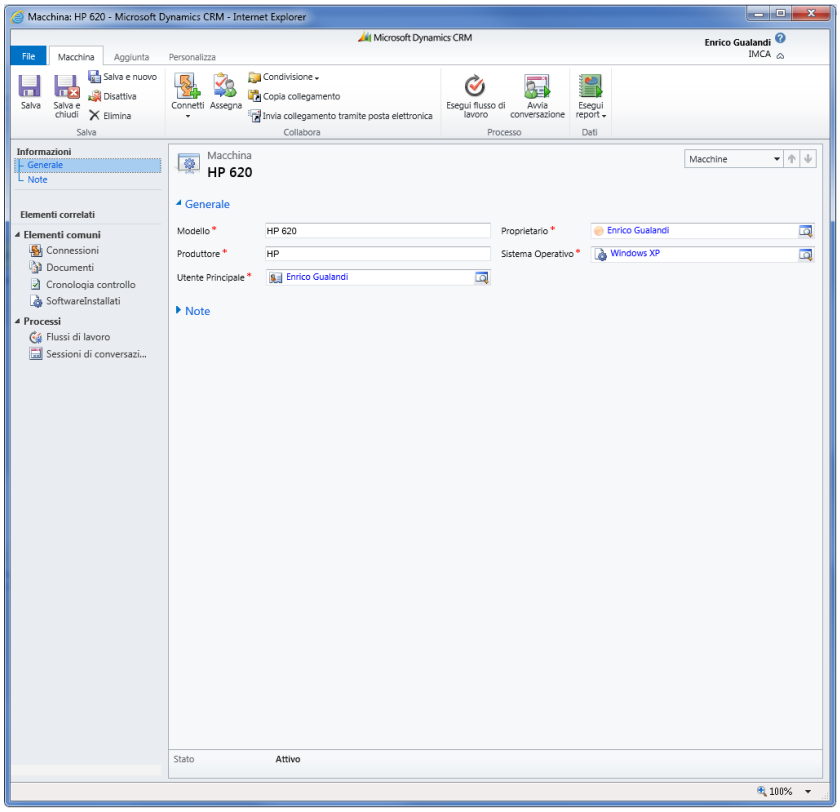

Figura 66 - Vista scheda macchina

e) Vista elenco software installati

Questa vista si raggiunge dalla precedente cliccando sulla scelta Software installati.

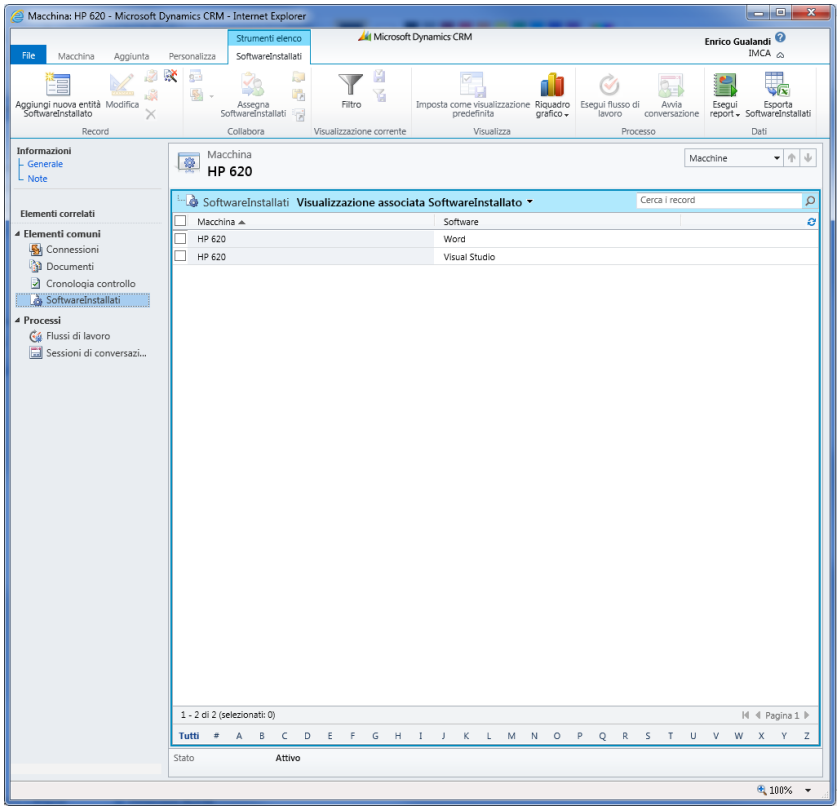

Figura 67 - Elenco software installati

f) Vista elenco software

La seguente è la vista che presenta l'elenco degli asset software presenti in azienda.

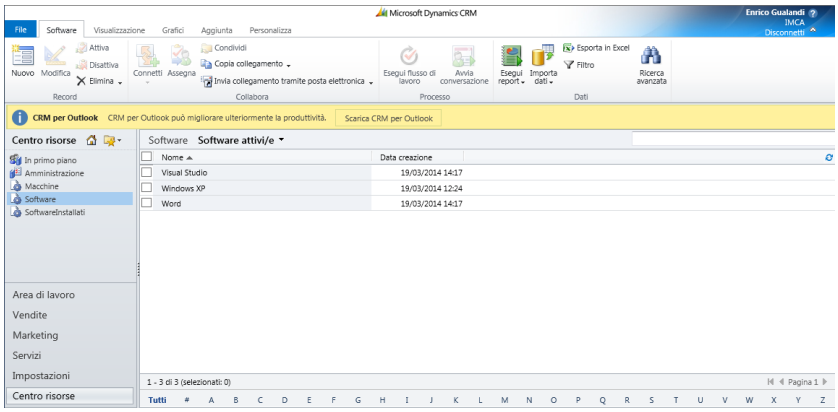

Figura 68 - Vista elenco software

Conclusioni e sviluppi futuri

Al termine del resoconto iniziale della situazione attuale, ho effettuato una profonda analisi di strumenti e normative da applicare per poi stilare un progetto di riorganizzazione dei processi e di componenti software da implementare per integrare tra loro i vari strumenti già presenti in azienda. L'elaborato fornisce quindi i dettagli progettuali per un sistema di gestione e le relative procedure da seguire per gestire gli asset aziendali secondo la vigente normativa e secondo le esigenze operative dei tecnici IT. Parte integrante dello stesso è anche la formazione del personale che lavora e collabora con l'azienda al fine di sensibilizzarli all'importanza e alla necessità di seguire le procedure qui presentate.

Il sistema deve ancora essere implementato. Inoltre è in continua evoluzione anche a livello progettuale. Vengono sviluppati e inseriti in azienda sempre nuovi device e tipi di strumenti diversi, che conseguentemente portano all'introduzione di nuovi strumenti per la loro gestione, che dovranno poi essere integrati.

Anche la normativa, per fornire indicazioni e disciplinare i nuovi device, evolve e si espande continuamente. Le procedure sono da verificate periodicamente, come peraltro previsto dalle procedure stesse, per garantire che esse siano allineate alla normativa e garantiscano una gestione agile e trasparente degli asset aziendali.

Bibliografia

http://www.normattiva.it/
http://www.legge231.net/informativa.html

Ringraziamenti

Voglio esprimere un sentito ringraziamento all'azienda Alya SRL che mi ha ospitato durante lo svolgimento della tesi e mi ha fornito gli strumenti per portarla avanti.