



POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea

**Analisi di sicurezza e aspetti di  
certificazione di una piattaforma in  
ambito Product Lifecycle Management**

**Relatore**

Assist. Prof. Diana Gratiela Berbecaru

**Candidato**

Andrea FOIS

DICEMBRE 2023



# Sommario

Il presente lavoro di tesi si propone di esplorare in profondità il campo delle certificazioni di sicurezza informatica, focalizzando l'attenzione sugli standard di riconosciuta importanza a livello internazionale, ovvero il National Institute of Standards and Technology (NIST), l'ISO/IEC 27001 e il Common Criteria.

Questa tesi si prefigge di analizzare in modo dettagliato i processi e le criticità legate a tali standard, evidenziando le sfide e le opportunità che essi comportano per le organizzazioni impegnate nella protezione delle loro risorse digitali. La sicurezza informatica è diventata un tema cruciale nel contesto odierno, in cui l'evoluzione delle tecnologie digitali ha portato a un aumento esponenziale delle minacce cibernetiche. L'adozione di standard di sicurezza, come quelli menzionati, è diventata una pratica comune per garantire la protezione dei dati e dei sistemi informatici. Tuttavia, la corretta implementazione di tali standard richiede un approccio meticoloso e un'analisi attenta dei processi coinvolti.

Inoltre, questa tesi presenterà un caso di studio concreto basato su una piattaforma utilizzata nell'ambito del Product Lifecycle Management (PLM). È stato necessario installare tale piattaforma, con l'obiettivo di assicurare che fosse configurata in modo da rispettare tutte le normative di sicurezza vigenti. Questo caso di studio rappresenta un esempio pratico delle sfide affrontate nell'implementazione di standard di sicurezza in un ambiente aziendale reale, mettendo in luce le strategie e le misure adottate per garantire la conformità alle certificazioni.

In sintesi, questa tesi si propone di fornire una panoramica esaustiva sulle certificazioni di sicurezza informatica, concentrandosi su standard di riconosciuta importanza. Attraverso l'analisi critica dei processi e delle sfide associate a tali standard e l'illustrazione di un caso di studio concreto, si mira a contribuire al miglioramento della comprensione e dell'applicazione delle migliori pratiche in materia di sicurezza informatica, promuovendo la consapevolezza dell'importanza della protezione dei dati e dei sistemi informatici in un'epoca in cui la digitalizzazione è sempre più predominante.

# Indice

<b>1</b>	<b>Introduzione</b>	8
1.1	Azienda	8
1.2	Certificazioni di Sicurezza	8
1.3	Fasi di una certificazione	9
<b>2</b>	<b>Security Plan</b>	10
2.1	Cos'è il Security Plan	10
2.2	Gli obiettivi	10
2.3	Chi redige il Security Plan	10
2.4	In cosa consiste il Security Plan	11
2.5	Risk Management e Security Plan	11
2.6	Il supporto offerto dal Security Plan	12
2.7	Come dev'essere redatto il Security Plan	12
2.8	Il fattore umano	12
2.9	Le fasi del Security Plan	12
2.9.1	Fase 1: Il commitment	13
2.9.2	Fase 2: Il processo di Risk Assessment	13
2.9.3	Fase 3: Il processo di Risk Treatment e Reporting	16
2.9.4	Fase 4: Monitoraggio e riesame	17
<b>3</b>	<b>Descrizione del sistema da certificare</b>	18
3.1	Introduzione	18
3.1.1	Contesto e Motivazione	18
3.1.2	Scopo e Obiettivi della Certificazione di Sicurezza	18
3.1.3	Definizione del Sistema da Certificare	18
3.2	In riferimento al NIST	19
3.2.1	Fasi del processo di certificazione	20

<b>4</b>	<b>Definizione delle proprietà di sicurezza da certificare</b>	<b>23</b>
4.1	Introduzione	23
4.1.1	Identificazione dei Requisiti di Sicurezza	23
4.1.2	Classificazione delle Proprietà di Sicurezza	23
4.1.3	Descrizione Dettagliata delle Proprietà di Sicurezza	24
4.1.4	Aggiornamenti e Mantenimento	24
4.2	In riferimento al Common Criteria	24
4.2.1	Concetti chiave	24
4.2.2	Metodologia del Common Criteria	26
<b>5</b>	<b>Processo di Certificazione</b>	<b>28</b>
5.1	Linee guida generali	28
5.1.1	Preparazione per la Certificazione	28
5.1.2	Scelta delle Normative e Standard Applicabili	28
5.1.3	Collaborazione con Enti di Certificazione	28
5.1.4	Preparazione della Documentazione	29
5.1.5	Esecuzione dei Test e delle Valutazioni	29
5.1.6	Valutazione e Risoluzione delle Non Conformità	29
5.1.7	Certificazione e Mantenimento	29
5.2	In Riferimento allo standard ISO/IEC 27001	29
5.2.1	Fase uno: creare un Project Plan	30
5.2.2	Fase due: definire l'ambito dell'ISMS	30
5.2.3	Fase tre: eseguire un risk assessment e gap analysis	30
5.2.4	Fase quattro: progettare e implementare politiche di sicurezza e controlli	30
5.2.5	Fase cinque: formazione dei dipendenti	31
5.2.6	Fase sei: documentare e raccogliere prove	31
5.2.7	Fase sette: completare un audit di certificazione	31
5.2.8	Fase otto: mantenere una conformità continua	31
5.3	Processo di audit di certificazione per ISO/IEC 27001	31
5.3.1	Stage 1: ISMS Design review	32
5.3.2	Stage 2: Certification audit	32
5.3.3	Surveillance audits	32
5.3.4	Recertification audit	32
5.4	Requisiti ISO/IEC 27001	32

<b>6</b>	<b>Criticità e Debolezze</b>	34
6.1	Criticità Generali	34
6.1.1	Limiti dell'Approccio Statico	34
6.1.2	Falsa Sensazione di Sicurezza	34
6.1.3	Elevato Costo e Complessità	34
6.1.4	Ritardo nell'Adozione di Nuove Tecnologie	35
6.1.5	Ristretta Copertura Geografica	35
6.1.6	Scarsa Compatibilità tra Standard e Normative	35
6.2	Barriere del Common Criteria	35
6.2.1	Assenza di Categoria Tecnologica	35
6.2.2	Tempo richiesto e aggiornamento	35
6.2.3	Mancanza di riconoscimento reciproco	36
6.2.4	Mancanza di esperienza nella valutazione della sicurezza	36
6.2.5	Costi elevati	36
6.2.6	Non è un fattore chiave per le decisioni di acquisto	36
<b>7</b>	<b>Certificazioni Fuorvianti</b>	37
7.1	Cause e Conseguenze	37
7.2	Caso Reale	37
<b>8</b>	<b>Confronto con il passato</b>	40
8.1	TCSEC	40
8.1.1	Obiettivi e requisiti fondamentali	40
8.1.2	Linee guida per i test sulla sicurezza	44
8.2	L'evoluzione	44
8.2.1	Test	45
8.2.2	Differenze tra TCSEC e Common Criteria	45
<b>9</b>	<b>Caso di Studio: Piattaforma 3DEXPERIENCE</b>	48
9.1	Introduzione	48
9.1.1	Product Lifecycle Management (PLM): Un Fondamento dell'Innovazione	48
9.1.2	Elementi Chiave della Piattaforma 3DEXPERIENCE	49
9.1.3	Installazione 3DEXPERIENCE	51
9.1.4	Panoramica su Proprietà di sicurezza 3DEXPERIENCE	52
9.2	Analisi su piattaforma 3DEXPERIENCE	53
9.2.1	Struttura della piattaforma 3DEXPERIENCE	54

9.2.2	Disponibilità	56
9.2.3	Crittografia dei dati	60
9.2.4	Autenticazione	65
9.2.5	Autorizzazione	71
9.2.6	Audit e Monitoraggio	73
<b>10</b>	<b>Conclusioni</b>	<b>78</b>
	<b>Bibliografia</b>	<b>79</b>

# Capitolo 1

## Introduzione

### 1.1 Azienda

Questo lavoro di tesi è stato svolto in collaborazione con l'azienda Hermes Reply, a seguito di un periodo di tirocinio curriculare all'interno della stessa azienda. Hermes Reply offre servizi di consulenza manageriale, consulenza in ambito IT e servizi di implementazione per l'introduzione di tecnologie industria 4.0. L'azienda si divide in 5 rami principali:

- R&D Design: Gestione del ciclo di vita del prodotto (Soluzione PLM)
- Planning: Pianificazione della produzione (schedulazione & dispacciamento) (Soluzioni MES - MOM)
- Manufacturing: Gestione del plant, Gestione della qualità, Edge connection, Controllo dello Shop floor e asservimento linea (Soluzioni MES – MOM)
- Logistics: Gestione materiali (Soluzioni MOM)
- Repair & Maintenance: Manutenzione del plant (Soluzioni MOM)

Il mio tirocinio e conseguente lavoro di tesi è stato svolto nel team PLM, dunque l'ambito della gestione del ciclo di vita del prodotto

### 1.2 Certificazioni di Sicurezza

Una certificazione di sicurezza di un sistema o prodotto è un processo attraverso il quale un'organizzazione indipendente valuta e attesta che il sistema o prodotto soddisfa determinati standard e requisiti di sicurezza. Questa certificazione conferisce una valida conferma della conformità del sistema o prodotto alle migliori pratiche e agli standard di sicurezza stabiliti. Il processo di certificazione di sicurezza coinvolge solitamente un'organizzazione di certificazione riconosciuta e affidabile che esegue una serie di valutazioni, test e controlli per valutare la sicurezza del target. Questi test possono riguardare aspetti come la protezione dei dati, l'accesso autorizzato, le vulnerabilità di sicurezza, la gestione degli incidenti e altre misure di sicurezza. L'obiettivo principale di una certificazione di sicurezza è assicurare agli utenti, ai clienti o agli acquirenti che il sistema



o prodotto soddisfa determinati standard di sicurezza. Questo può aumentare la fiducia degli utenti nel prodotto e dimostrare l'impegno dell'organizzazione nella sicurezza dei loro prodotti o servizi. Le certificazioni di sicurezza possono variare a seconda del settore e dell'applicazione specifica. Ad esempio, nel campo delle tecnologie dell'informazione e della sicurezza informatica, ci sono certificazioni come Common Criteria (CC), ISO 27001 e molte altre. Queste certificazioni stabiliscono requisiti specifici che un sistema o prodotto deve soddisfare per ottenere la certificazione. È importante notare che una certificazione di sicurezza non è eterna. Le certificazioni di sicurezza devono essere periodicamente rinnovate e aggiornate per riflettere gli sviluppi e le nuove minacce nel campo della sicurezza. Pertanto, è essenziale mantenere una conformità continua con gli standard di sicurezza e partecipare a valutazioni e audit regolari per mantenere attiva la certificazione.

### 1.3 Fasi di una certificazione



Figura 1.1. Le fasi del processo di certificazione

Questo lavoro di tesi si propone di esaminare in dettaglio il processo di certificazione, suddividendolo in quattro fasi fondamentali:

1. **Security Plan:** In questa fase iniziale, si sviluppa un piano di sicurezza completo, che definisce gli obiettivi di sicurezza, le risorse necessarie, e le strategie di mitigazione dei rischi. Il Security Plan costituisce il fondamento su cui si baseranno le successive fasi di certificazione.
2. **Descrizione del sistema da certificare:** Una volta definiti i requisiti di sicurezza nel Security Plan, si procede con la descrizione dettagliata del sistema oggetto della certificazione. Questo passo comprende la documentazione dell'architettura, dei componenti, delle interazioni e delle vulnerabilità potenziali del sistema.
3. **Definizione delle proprietà di sicurezza da certificare:** Qui si identificano le specifiche proprietà di sicurezza che devono essere testate e dimostrate per garantire la conformità ai requisiti. Queste proprietà possono includere l'integrità dei dati, la riservatezza delle informazioni, la disponibilità dei servizi e altre caratteristiche cruciali per la sicurezza.
4. **Il processo di certificazione:** L'ultima fase mette insieme tutto ciò che si è svolto nelle fasi precedenti e coinvolge l'effettiva esecuzione dei test e delle verifiche necessarie per valutare se il sistema soddisfa le proprietà di sicurezza definite.

## Capitolo 2

# Security Plan

### 2.1 Cos'è il Security Plan

[1] Il Security Plan, o piano di sicurezza, è il processo che analizza la sicurezza all'interno dell'organizzazione, con l'obiettivo di prevenire situazioni problematiche e dannose. Risulta necessario per progettare, pianificare, implementare e gestire un sistema di sicurezza robusto e che, successivamente, potrà anche garantire l'ottenimento delle certificazioni di sicurezza.

All'interno di un'azienda, il Security Plan rappresenta un processo fondamentale di gestione della sicurezza, analizzandola metodicamente e facendola passare da possibile problematica a un punto di forza dell'azienda stessa. Il Security Plan contribuisce a prevenire situazioni potenzialmente dannose per il raggiungimento degli obiettivi, la salvaguardia degli asset e il sostentamento della produttività d'impresa.

### 2.2 Gli obiettivi

Una gestione metodica e strutturata dei processi legati alla sicurezza è lo scopo finale del Security Plan, la cui stesura ed attuazione è parte dei compiti del professionista della sicurezza. È necessario valutare le criticità e le problematiche di sicurezza con metodo, con un approccio sistematico che tenga conto del contesto all'interno del quale agisce in modo da trovare le migliori soluzioni per il raggiungimento degli obiettivi.

### 2.3 Chi redige il Security Plan

Come detto, il professionista della sicurezza in azienda è colui che deve redigere il Security Plan in modo da prevenire possibili eventi dannosi. La prevenzione è sicuramente il metodo più efficace per difendersi, ma è anche quello più complicato, in quanto richiede molteplici capacità che non sono solamente di carattere tecnico o tecnologico. Un approccio preventivo alla sicurezza richiede professionalità, attitudine, competenza e soprattutto esperienza. Il professionista della sicurezza è la figura professionale che deve essere in grado di precedere gli eventi e prevedere i possibili scenari futuri.

## 2.4 In cosa consiste il Security Plan

La definizione e l'analisi degli obiettivi strategici, tattici e operativi globali dell'organizzazione viene usata come input per il piano di sicurezza. Il Security Plan va inteso come una tabella di marcia da seguire che, una volta assegnate le priorità in base ai potenziali rischi e agli obiettivi prefissati, stabilisce le risorse e i progetti specifici necessari per rispondere alle esigenze di sicurezza individuate nell'ambito di un'azienda.

Il Security Plan consiste nella pianificazione di policy, programmi, protocolli, procedure gestionali e prassi operative strettamente correlate alle attività di:

- Identificazione
- Analisi
- Valutazione
- Trattamento
- Comunicazione del rischio di sicurezza

Tutto ciò volto al fine di identificare le procedure e le risorse necessarie da attivare per raggiungere gli obiettivi, identificando le possibili alternative e stabilendo le priorità di intervento.

## 2.5 Risk Management e Security Plan

Per redigere un Security Plan è necessario servirsi dei principi del risk management enunciati nella Norma ISO 31000:2018 e applicare una tecnica di governance multilivello dei rischi che sia in grado di salvaguardare le risorse e garantire il normale proseguimento delle varie attività di business. Il principio comune che ispira tutti i modelli internazionali di risk management rimane il ciclo di Deming (Figura 2.1), un metodo di gestione di quattro fasi usato per il controllo e il miglioramento continuo dei processi e dei prodotti.



Figura 2.1. Le fasi del ciclo di Deming [2]

## 2.6 Il supporto offerto dal Security Plan

Il Security Plan deve essere efficace nel supportare l'azienda nel:

- Definire le strategie di business in funzione dei rischi a cui è esposta, contribuendo alla creazione e protezione del valore dell'organizzazione;
- Raggiungere gli obiettivi, procedendo secondo un metodo rischi/benefici che tenga conto di ogni possibile incertezza capace di trasformarsi in fattore sfavorevole;
- Gestire in maniera ottimale ed efficace le misure di prevenzione e mitigazione adottate nell'ambito della sicurezza;
- Prendere decisioni basate su una conoscenza approfondita della materia in esame;
- Accrescere la sensibilità nei confronti degli argomenti di sicurezza all'interno dell'azienda;
- Favorire il miglioramento continuo dell'azienda, attivando processi di controllo e revisione.

## 2.7 Come dev'essere redatto il Security Plan

Per risultare realmente efficace un Security Plan deve essere:

- Costruito su misura, ad hoc, con caratteristiche e requisiti unici e personalizzati per ogni progetto, coerenti con il contesto e gli obiettivi prefissati, e conformi alle reali esigenze di sicurezza dell'azienda;
- Parte integrante delle attività dell'azienda;
- Coinciso, strutturato e funzionale;
- Facilmente comprensibile, trasparente e condiviso.

## 2.8 Il fattore umano

L'elemento più critico, l'anello debole di tutta la catena di sicurezza, resta sempre il fattore umano, determinante per costruire e mantenere un sistema di sicurezza aziendale di qualità. Esso rappresenta il punto centrale di ogni progetto di sicurezza e risulta il punto più facile da attaccare e dove dunque è maggiormente necessario applicare la difesa.

Il Security Plan rappresenta un sistema pianificato di sicurezza collettiva. Il coinvolgimento attivo di tutto il personale nei processi di sicurezza aziendale è necessario per il mantenimento di elevati livelli di protezione.

## 2.9 Le fasi del Security Plan

Il processo di Security Plan è un insieme di step sequenziali diviso in quattro fasi.



Figura 2.2. Le fasi del Security Plan

### 2.9.1 Fase 1: Il commitment

Non è possibile sviluppare piani di prevenzione e protezione efficaci se non si ha un'idea chiara di ciò che vogliamo proteggere. Per questa ragione, prima di avviare un processo di Security Plan all'interno di un'organizzazione, ci si dovrebbe porre alcune domande chiave, necessarie a redigere una sorta di checklist preventiva, fare il punto della situazione di partenza e definire e visualizzare gli obiettivi cui si tende.

### 2.9.2 Fase 2: Il processo di Risk Assessment

Il Risk Assessment [3], come detto, è una fase fondamentale e dipende dal contesto all'interno del quale ci si trova. Esso rappresenta il processo globale di individuazione, analisi e valutazione dei rischi che si realizza sotto tre fasi ben distinte:

- Risk identification
- Risk analysis
- Risk evaluation

Si inizia dunque con l'identificazione dei rischi e dopo si passa ad un'analisi e a una valutazione dei rischi identificati. Questa fase è importantissima perché da questa valutazione dipende il successivo risk treatment. A questa prima fase appartengono:

- Identificazione degli asset
- Identificazione delle minacce (Threat Modeling)
- Identificazione delle vulnerabilità (Vulnerability Assessment)



Figura 2.3. Le fasi del Risk Assessment

### Identificazione degli asset [4]

Il processo di identificazione ha lo scopo di identificare gli asset aziendali rilevanti per i requisiti riguardanti la sicurezza delle informazioni e per evidenziare, nelle fasi successive, le possibili minacce e vulnerabilità. Essendo gli asset di diversi tipi (risorse fisiche, risorse umane, processi), le metodologie di valutazione dei requisiti di sicurezza sono diverse per ogni tipo di asset. Gli asset possono essere classificati in due principali tipologie: asset primari e asset di supporto. Alla prima classe appartengono:

- Processi di business e attività:
  - Processi la cui mancata operatività o danneggiamento renderebbero impossibile perseguire la mission dell'organizzazione;
  - Processi che includono trattamenti di informazioni particolari o che coinvolgono tecnologie proprietarie;
  - Processi che, se modificati, possono significativamente condizionare il compimento della mission aziendale;
  - Processi che sono necessari per soddisfare requisiti contrattuali, legali o regolamentari.
- Informazioni:
  - Informazioni vitali per il business aziendale;
  - Dati personali;
  - Informazioni strategiche richieste per perseguire determinati obiettivi;
  - Informazioni la cui gestione richiede tempi e costi elevati.

Alla seconda classe invece appartengono gli asset soggetti a vulnerabilità che possono danneggiare gli asset primari.

## Threat Modeling [5]

Il Threat modeling è il processo con il quale vengono identificate, classificate e analizzate potenziali minacce, valutando rischi e fornendo le necessarie contromisure. Quest'ultimo punto viene affrontato nella fase di Risk Treatment.

Questo processo può essere adottato sia come misura proattiva durante le fasi di design e sviluppo sia come misura reattiva successiva al deploy di un prodotto. A tal proposito è utile ricordare che la sicurezza è un elemento che deve essere considerato e gestito in maniera attiva, sin dalle prime fasi di progettazione di un prodotto, e per tutto il suo ciclo di vita. Tale considerazione è alla base di tre principi di sicurezza fondamentali: security by design, security by default e security by deployment. Adottare il suo approccio proattivo, infatti, non basta. Non tutte le minacce possono essere previste durante la fase di progettazione e dunque è importante adottare anche l'approccio reattivo periodicamente. Questo vale anche per tutti gli altri processi di sicurezza.

**Identificazione delle minacce:** esistono possibilità quasi infinite di minacce, è quindi importante utilizzare un metodo strutturato per riuscire ad indentificare solo quelle pertinenti al contesto, e ciò può essere fatto utilizzando uno o più dei seguenti approcci:

- Approccio incentrato sugli asset. Questo metodo utilizza i risultati dell'identificazione degli asset e tenta di trovare potenziali minacce collegate agli asset più di valore per il contesto
- Approccio incentrato sugli attaccanti. Qui ci si basa sull'identificazione di potenziali attaccanti, identificando le minacce in base ai possibili obiettivi che essi potrebbero voler compromettere.
- Approccio incentrato sul software. Se un'organizzazione sviluppa software, si possono voler identificare minacce che potrebbero colpirlo.

**Principali metodologie di threat modeling:** Esistono varie metodologie per categorizzare le minacce, di seguito verranno elencate le quattro più note:

- **STRIDE:** nel 1999 Microsoft fornisce agli sviluppatori un modo per poter individuare le minacce che potevano colpire i propri prodotti, sviluppando uno schema noto come STRIDE, il cui acronimo sta per:
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of Service (DoS)
  - Elevation of Privilege (EoP)
- **PASTA** (Process for Attack Simulation and Threat Analysis): è una metodologia basata sugli attaccanti, che si sviluppa attraverso un processo di sette fasi, con l'obiettivo di individuare e progettare contromisure per la protezione degli asset. Lo scopo di questo metodo è quello di fornire un processo dinamico di identificazione, enumerazione e valutazione delle minacce, in modo da poter successivamente sviluppare un'analisi dettagliata delle minacce identificate.

- **VAST** (Visual, Agile and Simple Threat): questa metodologia è basata sui principi di sviluppo Agile. L'obiettivo è quello di integrare il threat e risk management all'interno di programmi Agile.
- **TRIKE**: è una metodologia con approccio risk-based, il cui scopo è quello di usare il threat model in modo affidabile e ripetibile, così da poter essere usato per descrivere in modo esaustivo le caratteristiche di sicurezza di un sistema.

### Vulnerability Assessment [6]

Ma che differenza c'è tra Risk Assessment e Vulnerability Assessment? Il Risk Assessment prende in considerazione la totalità della struttura, mentre il Vulnerability Assessment si focalizza solamente sull'aspetto tecnologico. Il VA dunque valuta il livello di sicurezza dell'infrastruttura IT e la sua esposizione verso possibili attacchi, esterni o interni, che potrebbero aggirare le contromisure di sicurezza adottate. Si va ad eseguire una specie di scansione del sistema, allo scopo di rilevare eventuali debolezze che potrebbero essere sfruttate ad un aggressore per compromettere la sicurezza dell'infrastruttura.

Il VA è anch'esso diviso in fasi, molto simili al processo di Risk Assessment, che sono elencate di seguito:

- Valutazione dell'esposizione ai rischi
- Classificazione delle vulnerabilità in base al livello di rischio
- Indicazione delle azioni da effettuare per mitigare le vulnerabilità trovate
- Report

Per quanto riguarda la classificazione delle vulnerabilità si può fare riferimento al Common Vulnerability and Exposure (CVE) database. Esso è un glossario pubblico di vulnerabilità note sulla sicurezza informatica. A ciascuna vulnerabilità presente nel CVE, oltre a un identificatore e a una descrizione, è spesso associato un punteggio, il CVSS (Common Vulnerability Scoring System). Il CVSS è uno dei diversi modi per misurare l'impatto delle vulnerabilità, ed è comunemente noto come CVE score. Il punteggio per valutare la gravità di una data vulnerabilità viene assegnato secondo una scala da 0 a 10. La versione attuale di CVSS è la 4.0, che suddivide la scala come segue:

Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

### 2.9.3 Fase 3: Il processo di Risk Treatment e Reporting

[7] La valutazione dei rischi non è sufficiente per gestirli, essa infatti ci suggerisce solamente cosa non si dovrebbe fare ma non cosa si dovrebbe fare. Il Risk Treatment è il processo di selezione e implementazione delle misure per modificare il rischio. Una volta identificati e valutati i



rischi, il passo successivo riguarda l'identificazione delle possibili alternative delle azioni necessarie per gestire questi rischi, la valutazione dei risultati e dell'impatto di tali azioni e l'attuazione dei piani di trattamento. I piani di trattamento sono necessari per descrivere come le opzioni scelte saranno implementate. Tali piani dovranno essere esaustive e dovranno fornire tutte le informazioni necessarie su:

- Azioni proposte, priorità o piani temporali;
- Requisiti di risorse;
- Ruoli e responsabilità di tutte le parti coinvolte nelle azioni proposte;
- Misurazione delle performance
- Requisiti di report e monitoraggio

#### **Identificazione del Rischio Residuo**

Il rischio residuo è un rischio che rimane dopo aver identificato le opzioni e dopo aver implementato piano di azione del Risk Management. Comprende anche tutti i rischi inizialmente non identificati e tutti quei rischi identificati e valutati ma che non sono considerati all'interno del Risk Treatment.

#### **2.9.4 Fase 4: Monitoraggio e riesame**

Il processo di gestione del rischio non sarebbe completo se non prevedesse una fase di revisioni periodiche e di monitoraggio volta a verificare l'efficacia nel tempo e il buon funzionamento del piano di sicurezza, in termini di risultati ottenuti rispetto agli obiettivi prefissati.

Questa attività di monitoraggio costante consente anche di apportare eventuali modifiche e correzioni nel processo di gestione dei rischi.

## Capitolo 3

# Descrizione del sistema da certificare

### 3.1 Introduzione

#### 3.1.1 Contesto e Motivazione

La complessità e la rapida evoluzione delle minacce informatiche ha posto una notevole attenzione sulla volontà di una rigorosa valutazione e certificazione della sicurezza dei sistemi, al fine di proteggere dati sensibili, risorse aziendali e la privacy degli utenti. Questo capitolo esplora il contesto delle certificazioni di sicurezza e la motivazione dell'importanza di definire e descrivere accuratamente il sistema oggetto di certificazione.

#### 3.1.2 Scopo e Obiettivi della Certificazione di Sicurezza

Il primo passo nella comprensione delle certificazioni di sicurezza è definire il loro scopo e gli obiettivi. Il processo di certificazione mira a fornire una valutazione indipendente e imparziale della sicurezza di un sistema, verificando che rispetti determinati standard o regolamentazioni. La chiara definizione del sistema da certificare svolge un ruolo fondamentale nel garantire che il processo di certificazione sia accurato, rilevante e coerente.

#### 3.1.3 Definizione del Sistema da Certificare

##### Identificazione del Perimetro del Sistema

La definizione del sistema da certificare inizia con l'identificazione del suo perimetro. Questo processo coinvolge la delimitazione chiara delle componenti hardware, software e umane coinvolte nel sistema. La definizione del perimetro è essenziale poiché aiuta a stabilire quali parti del sistema saranno sottoposte alla valutazione di sicurezza e quali no.

## Descrizione delle Funzionalità e dei Servizi del Sistema

Una volta identificato il perimetro del sistema, è necessario descrivere le funzionalità e i servizi offerti dal sistema stesso. Questa descrizione dovrebbe essere dettagliata e comprensibile per gli stakeholder coinvolti nel processo di certificazione, compresi i certificatori e i rappresentanti del sistema.

## Rilevamento dei Requisiti di Sicurezza

La definizione del sistema dovrebbe includere un'analisi dettagliata dei requisiti di sicurezza pertinenti. Questi requisiti possono essere derivati da standard di sicurezza specifici, regolamentazioni governative o da altre linee guida riconosciute a livello internazionale. Rilevare i requisiti di sicurezza sin dall'inizio aiuta a identificare potenziali lacune nella sicurezza del sistema e a pianificare le misure necessarie per affrontarle.

## Identificazione delle Parti Interessate

Nella definizione del sistema, è essenziale identificare tutte le parti interessate coinvolte nel suo ciclo di vita. Queste parti interessate possono includere utenti finali, proprietari del sistema, sviluppatori, amministratori di sistema, fornitori e altre entità che interagiscono con il sistema. La comprensione delle esigenze e delle aspettative di ciascuna parte interessata aiuta a garantire che la valutazione di sicurezza sia completa e allineata agli obiettivi globali del sistema.

## 3.2 In riferimento al NIST

In linea con quanto esposto finora, nel seguente paragrafo si farà riferimento a quale approccio offra il NIST per questa fase del processo di certificazione.



Il National Institute of Standards and Technology (NIST), un'agenzia federale degli Stati Uniti, ha assunto il ruolo di baluardo nella promozione di standard tecnici volti a migliorare la sicurezza e la privacy delle informazioni all'interno di sistemi informativi e organizzazioni.

Tra i documenti chiave emessi dal NIST, spicca il NIST Special Publication 800-53, noto come "Security and Privacy Controls for Information Systems and Organizations." Questo documento fornisce un dettagliato insieme di controlli di sicurezza e misure di protezione, destinati a organizzazioni governative federali e aziende private che operano con il governo federale degli Stati Uniti. Il NIST SP 800-53 [8] è suddiviso in varie sezioni che comprendono famiglie di controlli, controlli e sottocontrolli specifici, nonché supplementi di controllo che offrono linee guida per ambienti o tecnologie specifiche.

Al fianco del NIST SP 800-53, il NIST emana altri standard complementari, ognuno dedicato a una specifica area della sicurezza informatica. Tra questi, il NIST SP 800-37 [9] definisce il Framework del Risk Management (Gestione del Rischio), mentre il NIST SP 800-171 si concentra sulla protezione dei dati sensibili non classificati. Inoltre, il NIST collabora con altre organizzazioni e istituzioni per creare standard globali come l'ISO/IEC 27001, enfatizzando l'importanza di una visione condivisa della sicurezza informatica oltre i confini nazionali.

### 3.2.1 Fasi del processo di certificazione



Figura 3.1. Le fasi del processo di certificazione NIST

Come si evince dal documento *Guide for the Security Certification and Accreditation of Federal Information Systems* [10] pubblicato dal NIST, il processo di certificazione della sicurezza consiste in quattro fasi distinte:

1. Initiation Phase
2. Security Certification Phase
3. Security Accreditation Phase
4. Continuous Monitoring Phase

Ogni fase è costituita da un insieme ben definito di task e sotto-task che devono essere svolte da soggetti responsabili. Le attività di certificazione della sicurezza possono essere applicate ad un sistema informativo nelle fasi appropriate del ciclo di vita dello sviluppo del sistema.

Il livello di sforzo applicato per le task di certificazione della sicurezza dovrebbe essere commisurato al livello di sicurezza e al rigore che si vogliono ottenere.

#### Initiation Phase

Questa fase consiste in 3 task:

1. Preparation
2. Notification e Resource identification
3. System security plan analysis, update, and acceptance

Lo scopo di questa fase è assicurare che i vari attori coinvolti siano d'accordo con i contenuti del piano di sicurezza del sistema, compresi i requisiti di sicurezza documentati, prima che inizi la valutazione dei controlli di sicurezza del sistema. Una significativa porzione delle informazioni necessarie per questa fase dovrebbe essere già stata generata in precedenza dal proprietario del sistema informativo durante:

1. Lo sviluppo del security plan del sistema con risk assessment iniziale

## 2. Lo svolgimento delle valutazioni precedenti

Nella maggior parte dei casi, il security plan è già stato precedentemente revisionato e approvato. Per questo le sotto-task della preparation task non dovrebbero richiedere altro lavoro da parte del proprietario del sistema al di là di quanto già realizzato nell'ambito del ciclo di vita dello sviluppo del sistema. Piuttosto, l'Initiation Phase serve per confermare che il security plan e il risk assessment sono stati completati. Se questo non è avvenuto queste attività dovrebbero essere completate prima di procedere con il processo di certificazione.

**Preparation:** l'obiettivo del preparation task è quello di prepararsi per la certificazione di sicurezza rivedendo il security plan del sistema e confermando che i contenuti del piano sono consistenti con il risk assessment iniziale.

## 1. INFORMATION SYSTEM DESCRIPTION:

Conferma del fatto che il sistema informativo sia stato completamente descritto e documentato nel security plan o in un documento equivalente. Una tipica descrizione del sistema informativo include:

- Il nome del sistema
- Un identificativo univoco per il sistema
- Lo stato del sistema rispetto al suo ciclo di sviluppo
- Il nome e l'ubicazione dell'organizzazione responsabile del sistema
- Informazioni di contatto del proprietario del sistema
- Informazioni di contatto dei responsabili della sicurezza del sistema
- Gli scopi, funzioni e capacità del sistema
- Il tipo di informazioni elaborate, archiviate e trasmesse dal sistema
- Il perimetro dell'autorizzazione operativa del sistema
- I requisiti funzionali del sistema
- Le leggi, le direttive, le policy, i regolamenti o gli standard che riguardano la sicurezza delle informazioni e del sistema
- Le persone che utilizzano e supportano il sistema
- L'architettura del sistema
- Dispositivi hardware e firmware
- Applicazioni software
- Hardware, software e interfacce di sistema
- Flussi informativi (input, output)
- La topologia di rete
- Le regole di connessione di rete per le comunicazioni con l'esterno
- Sistemi informativi interconnessi e identificatori univoci per questi sistemi
- Tecniche di cifratura usate per l'elaborazione, trasmissione e archiviazione delle informazioni
- Public Key Infrastructures, Certificate Authorities e istruzioni sull'utilizzo dei certificati

- L'ambiente fisico in cui il sistema opera
- I protocolli web e gli ambienti distributivi e collaborativi (processi e applicazioni)

## 2. SECURITY CATEGORIZATION:

Conferma che la categoria di sicurezza del sistema è stata determinata e documentata nel security plan o in un documento equivalente. Il FIPS 199 stabilisce tre livelli di potenziale impatto (low, moderate, high) per ognuno degli obiettivi di sicurezza (riservatezza, integrità e disponibilità). La categoria di sicurezza del sistema che elabora, archivia e trasmette molteplici tipi di informazioni dovrebbe essere come minimo il livello più alto di impatto che è stato determinato per ciascun tipo di informazioni per i vari obiettivi di sicurezza di riservatezza, integrità e disponibilità.

## 3. THREAT IDENTIFICATION:

Conferma che le potenziali minacce che potrebbero sfruttare i flaw o le debolezze del sistema sono già state identificate e documentate nel security plan, nel risk assessment o in un altro documento equivalente. È importante considerare tutte le possibili minacce che potrebbero causare danno al sistema, pregiudicando la riservatezza, l'integrità o la disponibilità del sistema. Le minacce possono essere:

- Naturali
- Umane
- Ambientali

Bisogna sottolineare il fatto che non tutte le possibili minacce che si possono trovare nell'ambiente devono essere inserite, ma solo quelle rilevanti per la sicurezza del nostro sistema.

## 4. VULNERABILITY IDENTIFICATION:

Conferma che flaw e debolezze che potrebbero essere sfruttate da potenziali minacce sono state identificate e documentate nel security plan, nel risk assessment o in un documento equivalente.

## Capitolo 4

# Definizione delle proprietà di sicurezza da certificare

### 4.1 Introduzione

Dopo aver presentato l'importanza della certificazione di sicurezza e aver esposto la descrizione del sistema che si desidera certificare nella fase iniziale del processo, è fondamentale procedere con la fase successiva, ovvero la definizione accurata delle proprietà di sicurezza da verificare. Questa fase svolge un ruolo cruciale poiché stabilisce le basi per la successiva valutazione della conformità del sistema alle normative e agli standard di sicurezza applicabili.



Figura 4.1. Le fasi per la definizione delle proprietà di sicurezza

#### 4.1.1 Identificazione dei Requisiti di Sicurezza

Nel primo passo si procede con l'individuazione e l'analisi dei requisiti di sicurezza rilevanti per il sistema o il prodotto oggetto di valutazione. Questi requisiti possono derivare da standard di sicurezza internazionali, regolamenti specifici del settore, normative governative o persino requisiti interni dell'organizzazione. È fondamentale coinvolgere esperti di sicurezza e consulenti specializzati in questa fase per garantire la completezza e l'accuratezza dell'insieme di requisiti identificati.

#### 4.1.2 Classificazione delle Proprietà di Sicurezza

Una volta identificati i requisiti di sicurezza, essi vengono organizzati e classificati in categorie o livelli di importanza. Questo processo di classificazione aiuta a concentrare l'attenzione sulle

proprietà di sicurezza critiche e prioritariamente necessarie per la protezione del sistema. Le categorie potrebbero includere aspetti come la protezione dei dati sensibili, il controllo degli accessi, la gestione delle identità, la protezione contro attacchi informatici e altre tematiche rilevanti alla sicurezza del sistema.

### 4.1.3 Descrizione Dettagliata delle Proprietà di Sicurezza

Ogni proprietà di sicurezza viene descritta in modo approfondito. Questa descrizione dovrebbe essere chiara, misurabile e comprensibile da parte di tutti gli stakeholder coinvolti nel processo di certificazione. Ogni proprietà dovrebbe essere corredata da informazioni sulla sua funzionalità, modalità di implementazione, requisiti tecnici e contromisure previste per mitigare eventuali minacce. Inoltre, è consigliabile fornire riferimenti agli standard o alle best practice utilizzati per definire tali requisiti, al fine di garantire l'allineamento alle normative riconosciute a livello internazionale.

### 4.1.4 Aggiornamenti e Mantenimento

Infine, va considerato che i requisiti di sicurezza possono evolvere nel tempo a causa delle mutevoli minacce informatiche e delle nuove tecnologie emergenti. Pertanto, è essenziale mantenere il set di requisiti di sicurezza aggiornato e revisionarlo periodicamente per assicurarsi che sia sempre allineato alle esigenze del contesto operativo e agli standard di sicurezza in continua evoluzione.

La fase di definizione delle proprietà di sicurezza costituisce un passaggio cruciale nel processo di certificazione di sicurezza, poiché fornisce la base per valutare l'efficacia delle misure di sicurezza implementate nel sistema. Attraverso una corretta e dettagliata analisi, è possibile garantire che il sistema raggiunga un livello di protezione adeguato e affidabile per fronteggiare le minacce informatiche attuali e future.

## 4.2 In riferimento al Common Criteria

Il Common Criteria (CC) è uno standard internazionale ampiamente riconosciuto e utilizzato per la valutazione della sicurezza dei sistemi informatici e dei prodotti tecnologici. Noto anche come ISO/IEC 15408, il Common Criteria è stato sviluppato da un consorzio internazionale di paesi chiamato "Common Criteria Recognition Arrangement" (CCRA). Lo standard si basa sull'idea di fornire un framework unificato per valutare la sicurezza dei prodotti IT in modo da consentire una valutazione oggettiva e comparabile tra i vari prodotti.

### 4.2.1 Concetti chiave

[11] Nell'ambito del Common Criteria la parte del sistema o del prodotto che deve essere certificato è chiamato "Target of Evaluation" (TOE). Per definire un set standard di requisiti di sicurezza per una particolare classe di prodotti, viene sviluppato il "Protection Profile" (PP). Il PP serve come template riutilizzabile per i requisiti di sicurezza per supportare la definizione di standard funzionali. Il PP è un insieme, indipendente dall'implementazione, di requisiti di sicurezza per una particolare tecnologia che consente valutazioni ripetibili.

Se un venditore ha un prodotto ICT che vuole certificare con il Common Criteria, è necessario che venga completata la descrizione del "Security Target" (ST). Il Security Target è un documento



usato per identificare le proprietà di sicurezza del TOE. Inoltre, include le valutazioni dei potenziali rischi definendo le misure funzionali e di garanzia di sicurezza che il TOE dovrebbe offrire per soddisfare i requisiti del CC.

Class	Class name
APE	Protection Profile Evaluation
ASE	Security Target Evaluation
ADV	Development
AGD	Guidance Documents
ALC	Life-Cycle Support
ATE	Tests
AVA	Vulnerability Assessment
ACO	Composition

Figura 4.2. Le classi dei Security Assurance Requirements. [11]

Come mostrato in figura, nel Common Criteria sono identificate otto categorie di “Security Assurance Requirements” (SARs), ossia valutazioni dei requisiti di controllo della sicurezza usate come base per ottenere la certezza che le misure di sicurezza dichiarate siano implementate correttamente.

Il CC definisce inoltre undici categorie di “Security Functional Requirements” (SFRs) in relazione alle funzionalità di sicurezza desiderabili per fornire un modo standard di esprimere i requisiti per un TOE, come mostrato in figura.

Class	Class name
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPR	Privacy
FPT	Protection of the TOE Security Functionality
FRU	Resource Utilization
FTA	TOE Access
FTP	Trusted Path/Channels

Figura 4.3. Le classi dei Security Functional Requirements. [11]

Per valutare il processo di certificazione vengono usati gli “Evaluation Assurance Levels” (EAL). Tali livelli definiscono come il prodotto è testato e quanto profondamente è stato valutato. I livelli EAL vanno da EAL1, il più basso, fino a EAL7, il più alto. Il valore espresso dal livello EAL non misura la sicurezza del prodotto ma il livello di quanto questo sia stato testato.

## 4.2.2 Metodologia del Common Criteria

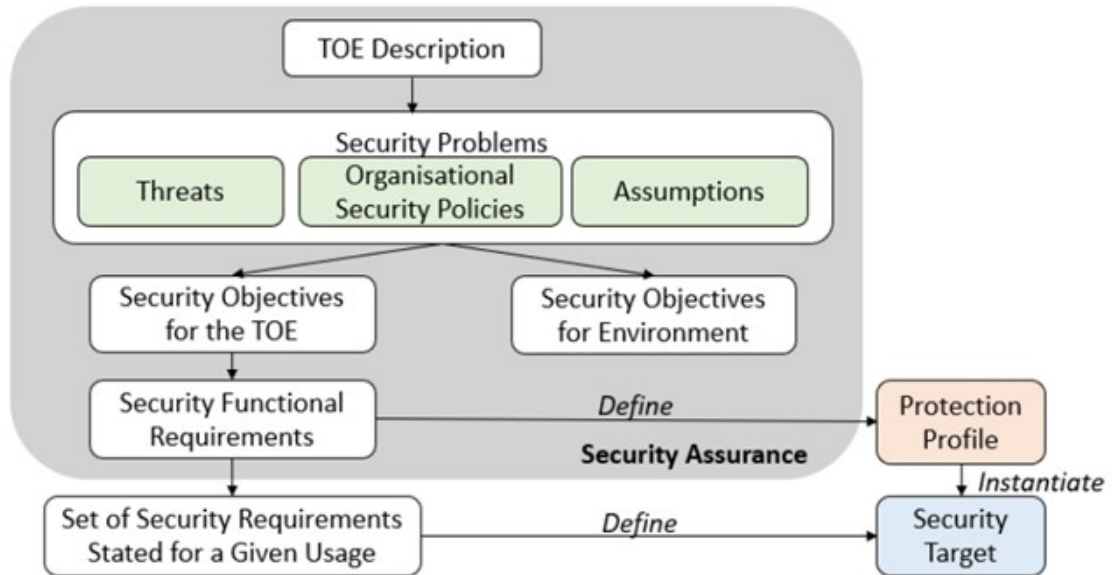


Figura 4.4. Metodologia del Common Criteria [11]

### TOE Description

Come già visto in precedenza sia in modo generale sia in riferimento al NIST, anche per quanto riguarda il Common Criteria il primo step risulta essere la descrizione del TOE.

### Security Problems

In linea con la descrizione del TOE, i problemi di sicurezza verranno definiti secondo tre aspetti: minacce, politiche organizzative di sicurezza e assunzioni.

- Minaccia: consiste in azioni ostili eseguite da un agente di minaccia su una risorsa.
- Politiche organizzative di sicurezza: sono regole di sicurezza, procedure o linee guida imposte da un'azienda, reale o ipotetica, che devono essere applicate al TOE e/o al suo ambiente operativo.
- Assunzioni: possono essere fatte sull'ambiente operativo, inclusi l'ambiente fisico, abilità e comportamenti personali e connettività.

### Security Objectives

Gli obiettivi di sicurezza sono la soluzione prevista, espressa come una risposta concisa e astratta. Servono per tre scopi principali:

- Fornire una soluzione di alto livello per i problemi di sicurezza.
- Suddividere la soluzione in obiettivi che devono essere soddisfatti dal TOE e obiettivi che devono essere soddisfatti dall'ambiente.
- Dimostrare che queste soluzioni parziali possono formare una soluzione completa al problema della sicurezza.

### **Security Functional Requirements (SFRs)**

Sono una traduzione degli obiettivi di sicurezza per il TOE. Gli SFR forniscono una descrizione più dettagliata e completa per fare in modo che gli obiettivi di sicurezza possano essere completamente affrontati.

Il CC richiede che la traduzione dagli obiettivi di sicurezza agli SFR sia condotta con un linguaggio standardizzato. I vantaggi e le ragioni per utilizzare un linguaggio standardizzato sono duplici: uno è fornire una descrizione esatta di quale sia la funzionalità da valutare a differenza del linguaggio naturale; un altro vantaggio è consentire il confronto tra prodotti della stessa classe che verranno valutati. Il linguaggio standardizzato impone l'uso della stessa terminologia e concetti che rendono molto più facile il confronto. Il CC supporta la traduzione standardizzata fornendo dei requisiti funzionali di sicurezza, operazioni e dipendenze predefiniti.

### **Security Assurance Requirements (SARs)**

A differenza dei SFR, i SAR descrivono le misure da prendere durante il processo di sviluppo e valutazione del prodotto per garantire il rispetto delle funzionalità di sicurezza. .

## Capitolo 5

# Processo di Certificazione

### 5.1 Linee guida generali

Il processo di certificazione di sicurezza rappresenta il cuore dell'intero sforzo di garantire che un sistema o un prodotto soddisfi gli standard e i requisiti di sicurezza stabiliti. Questo capitolo fornisce un'analisi del processo di certificazione, delineando le fasi chiave, le pratiche raccomandate e le linee guida generali da seguire.

#### 5.1.1 Preparazione per la Certificazione

Il processo di certificazione di sicurezza rappresenta il cuore dell'intero sforzo di garantire che un sistema o un prodotto soddisfi gli standard e i requisiti di sicurezza stabiliti. Questo capitolo fornisce un'analisi dettagliata del processo di certificazione, delineando le fasi chiave, le pratiche raccomandate e le linee guida generali da seguire. Si prevede che queste linee guida siano integrate in seguito con esempi specifici di standard di sicurezza che verranno analizzati in dettaglio nei capitoli successivi.

#### 5.1.2 Scelta delle Normative e Standard Applicabili

In base al settore di appartenenza e alle esigenze del sistema o del prodotto, è necessario identificare le normative e gli standard di sicurezza pertinenti. Questa scelta influenzerà il percorso di certificazione e i requisiti che dovranno essere soddisfatti. Si raccomanda di selezionare normative e standard ampiamente riconosciuti e accettati per garantire che la certificazione abbia valore a livello internazionale.

#### 5.1.3 Collaborazione con Enti di Certificazione

L'interazione con enti di certificazione è un passo cruciale nel processo. Questi enti indipendenti valuteranno il sistema o il prodotto in base ai requisiti stabiliti dalle normative e dagli standard selezionati. È importante comprendere il processo di valutazione del rispettivo ente di certificazione, inclusi i criteri, i test e le procedure specifiche che verranno eseguiti.

#### 5.1.4 Preparazione della Documentazione

La documentazione accurata è essenziale per dimostrare la conformità alle normative e agli standard di sicurezza. Questa fase comporta la preparazione di report dettagliati, documenti di supporto, prove tecniche e altre evidenze richieste dall'ente di certificazione. La documentazione dovrebbe essere chiara, completa e ben organizzata.

#### 5.1.5 Esecuzione dei Test e delle Valutazioni

Questa fase coinvolge l'esecuzione dei test e delle valutazioni definite dalle normative e dagli standard selezionati. Gli aspetti testati possono riguardare la sicurezza funzionale, la resistenza agli attacchi, la gestione delle vulnerabilità e altro ancora. I risultati dei test e delle valutazioni determineranno se il sistema o il prodotto raggiunge gli standard richiesti.

#### 5.1.6 Valutazione e Risoluzione delle Non Conformità

Qualora durante i test e le valutazioni emergessero non conformità, queste dovrebbero essere valutate e risolte. È importante comprendere l'entità delle non conformità e adottare le misure appropriate per affrontarle. Questo potrebbe includere modifiche al design, implementazione di nuove misure di sicurezza o correzioni di vulnerabilità.

#### 5.1.7 Certificazione e Mantenimento

Una volta che il sistema o il prodotto ha superato con successo tutte le fasi di valutazione e le non conformità sono state affrontate, viene rilasciata la certificazione di sicurezza. Tuttavia, la sicurezza è un processo continuo, pertanto è necessario un impegno costante per mantenere il livello di sicurezza nel tempo. Questo potrebbe richiedere valutazioni periodiche, aggiornamenti per affrontare nuove minacce e una costante vigilanza sulla sicurezza.

### 5.2 In Riferimento allo standard ISO/IEC 27001

[12] Lo standard ISO/IEC 27001 è una norma internazionale che contiene i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni. La ISO 27001 non è unicamente uno standard di sicurezza informatica in quanto, oltre alla sicurezza logica, include anche la sicurezza fisica/ambientale e la sicurezza organizzativa.

Dal momento che l'informazione è un bene di incredibile valore per l'azienda, e che ormai la maggior parte delle informazioni risiedono su supporti informatici, ogni azienda ha il dovere di essere in grado di garantire la sicurezza dei propri dati. L'obiettivo di questo standard è proprio quello di proteggere i dati e le informazioni da minacce di ogni tipo.

Lo standard ISO/IEC 27001 è uno standard particolarmente rigoroso, e questo può spaventare chi vuole ottenere la certificazione per la prima volta. Le domande e i dubbi possono essere tanti, da dove cominciare? Di quali controlli abbiamo bisogno? Come possiamo sapere se siamo pronti per richiedere una verifica?

Di seguito verranno indicate le principali fasi del processo di certificazione [13], che ripercorrono anche le fasi iniziali già precedentemente descritte fino ad arrivare all'implementazione delle politiche di sicurezza e all'audit di certificazione.

### **5.2.1 Fase uno: creare un Project Plan**

Per iniziare bisogna creare un piano per il progetto di certificazione, che includa l'indicazione di chi all'interno dell'azienda supervisionerà il processo, stabilirà le aspettative e gestirà le tappe fondamentali di esso. Inoltre in questa fase prevede anche lo studio dello standard e i suoi 114 controlli.

### **5.2.2 Fase due: definire l'ambito dell'ISMS**

Ogni azienda è unica e gestisce diversi tipi di dati. Prima di costruire l'ISMS (Information Security Management Systems) è necessario determinare esattamente che tipo di informazioni si devono proteggere. Per alcune aziende, l'ambito del loro ISMS include l'intera organizzazione, per altre include solo uno specifico dipartimento o sistema.

### **5.2.3 Fase tre: eseguire un risk assessment e gap analysis**

Un risk assessment formale è un requisito per la conformità alla norma ISO 27001. Questo significa che i dati, le analisi e i risultati del risk assessment devono essere documentati.

Per iniziare bisogna considerare la propria linea di base per la sicurezza. A quali obblighi legali, regolamentari o contrattuali è tenuta l'azienda?

Molte startup che non dispongono di un team dedicato alla conformità scelgono di assumere un consulente ISO per aiutarle con l'analisi delle lacune e il piano di risoluzione. Un consulente che ha esperienza di lavoro con aziende simili può fornire una guida esperta per aiutare a soddisfare i requisiti di conformità. Oltre a questo, un consulente può aiutarti a stabilire le best practice che rafforzerebbero il livello di sicurezza dell'azienda.

### **5.2.4 Fase quattro: progettare e implementare politiche di sicurezza e controlli**

Una volta identificati i rischi, è necessario decidere come l'azienda risponderà ad essi. Quali rischi l'azienda è disposta a tollerare e quali invece deve affrontare? Durante l'audit di certificazione l'auditor vorrà esaminare le decisioni prese riguarda a ciascun rischio identificato. Bisognerà inoltre produrre un "Statement of Applicability" e un "Risk Treatment Plan" come parte delle prove dell'audit. Lo "Statement of Applicability" riassume e spiega quali controlli e politiche dello standard sono rilevanti per l'azienda. Questo documento è una delle prime cose che l'auditor esterno esaminerà durante l'audit di certificazione.

Il "Risk Treatment Plan" è un altro documento essenziale per la certificazione. Registra il modo in cui l'azienda risponderà alle minacce identificate durante il risk assessment. Lo standard ISO/IEC 27001 delinea quattro azioni per affrontare i rischi:

- Modificare il rischio stabilendo controlli che riducano la possibilità che si verifichi
- Evitare il rischio prevenendo le circostanze in cui potrebbe verificarsi
- Condividere il rischio con terze parti (ad esempio, affidare le attività di sicurezza a un'altra società)
- Accettare il rischio perché il costo per affrontarlo è maggiore del danno potenziale

Successivamente dovranno essere implementati politiche e controlli in risposta ai rischi identificati. Le politiche di sicurezza dovrebbero stabilire e rafforzare le migliori pratiche di sicurezza, come, per esempio, richiedere ai dipendenti di utilizzare l'autenticazione a più fattori e bloccare i dispositivi ogni volta che lasciano le loro postazioni di lavoro.

### **5.2.5 Fase cinque: formazione dei dipendenti**

Lo standard richiede che tutti i dipendenti siano formati sulla sicurezza informatica. Questo garantisce che tutti all'interno dell'azienda comprendano l'importanza della sicurezza dei dati e il loro ruolo sia nel raggiungimento che nel mantenimento della conformità allo standard.

### **5.2.6 Fase sei: documentare e raccogliere prove**

Per ottenere la certificazione, è necessario provare all'auditor esterno che siano stati stabiliti politiche e controlli efficaci e che funzionano come richiesto dallo standard ISO 27001. Raccogliere e organizzare tutte queste prove può richiedere molto tempo. Per questo motivo esistono software di automazione della conformità per tale standard che possono aiutare a velocizzare questo processo.

### **5.2.7 Fase sette: completare un audit di certificazione**

In questa fase, un auditor esterno valuterà l'ISMS per verificare che verifichi i requisiti dello standard e rilasciare la certificazione. L'audit di certificazione si svolge in due fasi. Per prima cosa l'auditor completerà un audit di Stage 1, dove esaminerà la documentazione dell'ISMS per assicurarsi che siano in atto le politiche e le procedure corrette. Successivamente, un audit di Stage 2 esaminerà i processi aziendali e i controlli di sicurezza. Una volta completati i due audit, verrà rilasciata una certificazione ISO/IEC 27001 valida per tre anni.

### **5.2.8 Fase otto: mantenere una conformità continua**

La norma ISO/IEC 27001 è incentrata sul miglioramento continuo. Si dovrà continuare ad analizzare l'ISMS per assicurarsi che funzioni ancora in modo efficace. E man mano che l'azienda si evolve ed emergono nuovi rischi, si dovranno cercare opportunità per migliorare i processi e i controlli esistenti. Lo standard richiede audit interni periodici come parte di questo monitoraggio continuo. Gli auditor interni esaminano i processi e le politiche per cercare potenziali punti deboli e aree di miglioramento prima di un audit esterno.

## **5.3 Processo di audit di certificazione per ISO/IEC 27001**

- Stage 1: ISMS Design review
- Stage 2: Certification audit
- Surveillance audits
- Recertification audit

Dopo aver creato l'ISMS, completato il gap assessment, implementato i controlli, formato il personale e raccolto prove, si è pronti per iniziare il processo di audit.

### **5.3.1 Stage 1: ISMS Design review**

Esaminare la documentazione dell'ISMS per assicurarsi che le politiche e le procedure siano progettate correttamente. In questa fase, l'auditor si assicurerà che la documentazione è conforme ai requisiti dello standard elencati nelle clausole 4-10. Indicheranno inoltre eventuali non conformità o opportunità per migliorare l'ISMS. Una volta implementati i cambiamenti suggeriti, si sarà pronti per l'audit di stage 2.

### **5.3.2 Stage 2: Certification audit**

Esaminare i processi e i controlli aziendali per assicurarsi che siano conformi allo standard. In questa fase è dove l'auditor completerà una valutazione dettagliata per determinare se l'azienda soddisfa i requisiti ISO/IEC 27001. Una volta che lo Stage 1 e lo Stage 2 sono completati, la certificazione è valida per 3 anni.

### **5.3.3 Surveillance audits**

Durante il periodo di certificazione di tre anni si dovranno condurre audit continui. Questi audit garantiscono che il programma di conformità sia ancora efficace e mantenuto.

Gli audit di sorveglianza verificano per assicurarsi che le aziende mantengano correttamente i propri controlli. Gli auditor di sorveglianza verificano inoltre che eventuali non conformità o eccezioni rilevate durante l'audit di certificazione siano state affrontate.

### **5.3.4 Recertification audit**

Durante l'ultimo anno dei tre di certificazione, l'azienda può sottoporsi a un audit di ricertificazione. Analogamente allo Stage 2, l'auditor completerà una valutazione dettagliata per determinare se l'azienda soddisfa i requisiti ISO/IEC 27001.

Dopo aver completato l'audit di ricertificazione, la nuova certificazione ha validità per ulteriori tre anni. La maggior parte delle aziende impiega dai 6 ai 12 mesi per prepararsi e completare un audit di certificazione, il che per alcune aziende potrebbe risultare proibitivo.

## **5.4 Requisiti ISO/IEC 27001**

Durante l'audit di certificazione, l'auditor dovrà valutare diversi aspetti dell'ISMS, comprese le politiche, i processi aziendali e le prove a supporto.

Ecco una linea di base della documentazione che si dovrà fornire all'auditor:

- Ambito dell'ISMS
- Information security policy
- Processo di information security risk assessment
- Processo di information security risk treatment
- Statement of Applicability



- Information security objectives
- Prova di competenza
- Programma di formazione sulla sensibilizzazione alla sicurezza e risultati
- Risultati dell'information security risk assessment
- Risultati dell'information security risk treatment
- Prova del monitoraggio e della misurazione dei risultati
- Processo di audit interno documentato
- Prova del programma di audit e dei risultati
- Prova dei risultati dei management reviews
- Prova delle non conformità e delle azioni correttive
- Prova dei risultati delle azioni correttive

## Capitolo 6

# Criticità e Debolezze

Nonostante le certificazioni di sicurezza siano un importante strumento per garantire l'affidabilità e la robustezza dei sistemi e dei prodotti IT, è essenziale comprendere che possono presentare alcune criticità e debolezze. Queste problematiche vanno attentamente prese in considerazione affinché il processo di certificazione sia migliorato continuamente e i livelli di sicurezza raggiunti siano adeguati alle sempre crescenti sfide del panorama della sicurezza informatica.

### 6.1 Criticità Generali

#### 6.1.1 Limiti dell'Approccio Statico

Le certificazioni di sicurezza sono spesso basate su un approccio statico, il quale valuta il sistema o il prodotto in uno specifico momento nel tempo. Tuttavia, il panorama della sicurezza è dinamico e in costante evoluzione, con nuove minacce che emergono regolarmente. Di conseguenza, una valutazione statica potrebbe non essere sufficiente per garantire che il sistema rimanga sicuro nel lungo periodo. Potrebbero essere necessarie valutazioni periodiche o meccanismi di valutazione più dinamici per affrontare questa criticità.

#### 6.1.2 Falsa Sensazione di Sicurezza

Una certificazione di sicurezza non garantisce che il sistema sia invulnerabile agli attacchi o alle violazioni. Talvolta, gli sviluppatori potrebbero concentrarsi esclusivamente sui requisiti necessari per ottenere la certificazione senza affrontare adeguatamente tutte le possibili minacce. Questo potrebbe portare a una falsa sensazione di sicurezza e a una mancanza di preparazione per gli attacchi reali. È fondamentale comprendere che una certificazione è solo un passo nel processo di sicurezza complessivo e che è necessario continuare a implementare misure di sicurezza aggiuntive e ad affrontare le vulnerabilità scoperte.

#### 6.1.3 Elevato Costo e Complessità

Il processo di certificazione di sicurezza può essere estremamente costoso e complesso, specialmente per i prodotti di elevata complessità o per le organizzazioni di dimensioni ridotte. Questo potrebbe

scoraggiare alcune aziende dal perseguire una certificazione formale, lasciando potenzialmente scoperti sistemi e prodotti che necessitano di una valutazione di sicurezza.

#### **6.1.4 Ritardo nell'Adozione di Nuove Tecnologie**

Il processo di certificazione può richiedere del tempo, e ciò potrebbe causare ritardi nell'adozione di nuove tecnologie o nell'introduzione di aggiornamenti di sicurezza urgenti. Questa situazione può essere problematica quando è necessario rispondere rapidamente a minacce emergenti o vulnerabilità critiche.

#### **6.1.5 Ristretta Copertura Geografica**

Le certificazioni di sicurezza possono essere emesse da enti o agenzie specifici che potrebbero avere un'area di copertura geografica limitata. Questo potrebbe comportare limitazioni nell'accettazione delle certificazioni da parte di organizzazioni o governi di altre regioni, creando complicazioni per la vendita o l'utilizzo dei prodotti certificati in ambiti internazionali.

#### **6.1.6 Scarsa Compatibilità tra Standard e Normative**

Esistono diversi standard e normative di sicurezza, e ciò potrebbe creare complessità per le organizzazioni che cercano di ottenere certificazioni multiple o cercano di allinearsi a diverse linee guida di sicurezza.

### **6.2 Barriere del Common Criteria**

[14] Nell'articolo "How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond" vengono analizzate le barriere che la maggior parte delle aziende riscontrano nell'adozione del Common Criteria. Tramite un questionario a diverse aziende Australiane è stata stilata una lista di problemi riscontrati nell'adozione di tale standard, che non discosta di molto dalle criticità generali elencate precedentemente.

#### **6.2.1 Assenza di Categoria Tecnologica**

Il Common Criteria usa un framework nel quale i venditori e gli acquirenti possono specificare i loro requisiti di sicurezza per i prodotti ICT. Il portale del Common Criteria archivia i Protection Profiles e i Certified Products sotto un'ampia gamma di categorie e diversi tipi di tecnologia. Nonostante attualmente il Common Criteria ha 15 categorie (come si vede nella figura 3), una grande percentuale di partecipanti al questionario afferma che l'assenza di Protection Profiles approvati per la categoria dei prodotti rende difficile ottenere la certificazione.

#### **6.2.2 Tempo richiesto e aggiornamento**

Come abbiamo già visto, il processo di valutazione del Common Criteria richiede una serie di fasi. Di media, il tempo richiesto per la certificazione va dai sei mesi a un anno. Più della metà dei partecipanti al questionario hanno affermato che il tempo di valutazione è troppo lungo rispetto al ciclo di vita del prodotto.

### 6.2.3 Mancanza di riconoscimento reciproco

La mancanza di riconoscimento reciproco tra diversi standard di sicurezza è un ostacolo all'adozione delle certificazioni di sicurezza, inclusi i Common Criteria.

### 6.2.4 Mancanza di esperienza nella valutazione della sicurezza

Il Common Criteria è alquanto complesso e non facile da seguire per condurre una valutazione in termini di usabilità e leggibilità. Circa il 43% dei partecipanti concordano sul fatto che i requisiti di documentazione per la valutazione Common Criteria sono proibitivi, ed è dunque difficile ottenere la certificazione.

### 6.2.5 Costi elevati

Tutti i partecipanti, chi in maniera più decisa e chi meno, hanno dichiarato che i costi di valutazione del Common Criteria sono troppo elevati rispetto ai benefici portati dal prodotto valutato. Questa è senza dubbio una barriera molto importante, specialmente per le aziende con un budget limitato e prodotti a basso margine di profitto.

### 6.2.6 Non è un fattore chiave per le decisioni di acquisto

La maggioranza dei partecipanti hanno dichiarato che non è vero che la certificazione del Common Criteria non aggiunga benefici ai loro prodotti, ma hanno anche concordato sul fatto che questi benefici non risultano un fattore chiave nelle vendite dei loro prodotti.

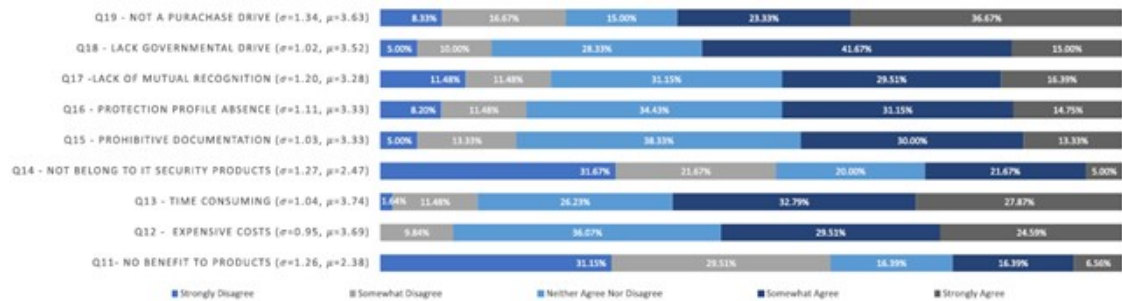


Figura 6.1. Risultati di alcune domande del questionario [14]

## Capitolo 7

# Certificazioni Fuorvianti

Le certificazioni di sicurezza, come detto, sono un pilastro fondamentale per garantire la robustezza e l'affidabilità dei sistemi e dei prodotti IT. Tuttavia, è importante riconoscere che, in alcuni casi, potrebbero verificarsi situazioni in cui un sistema o un prodotto venga certificato nonostante non soddisfi appieno gli standard di sicurezza.

### 7.1 Cause e Conseguenze

Le certificazioni fuorvianti possono verificarsi per diverse ragioni. Una delle cause principali è ovviamente la mancanza di un'adeguata valutazione delle misure di sicurezza implementate nel sistema o nel prodotto. Questo potrebbe essere il risultato di una valutazione superficiale, mancanza di risorse, pressioni economiche o altre considerazioni che portano a una valutazione non accurata. Inoltre, le aziende potrebbero essere motivate a cercare una certificazione solo per soddisfare requisiti contrattuali o di mercato, anziché per un reale impegno per la sicurezza.

Le conseguenze delle certificazioni errate possono essere gravi. Potrebbero indurre in errore gli acquirenti o gli utenti finali, facendo loro credere che il sistema o il prodotto sia più sicuro di quanto effettivamente sia. Ciò potrebbe portare a esposizioni a rischio o a violazioni della sicurezza nonostante la presunta certificazione.

### 7.2 Caso Reale

Nell'articolo "How Certification System Fail" [15] vengono descritti e analizzati casi reali in cui è stata prodotta una certificazione di sicurezza errata. Il primo caso che viene analizzato nello specifico è quello di dispositivi di immissione PIN per sistemi di pagamento, che nonostante venissero pubblicizzati per aver superato la valutazione Common Criteria, consentivano l'inserimento di dispositivi di PIN-tapping. Nel caso delle valutazioni dei dispositivi PED (PIN Entry Device), il dispositivo non deve permettere l'inserimento di un dispositivo in grado di acquisire il PIN del cliente, perché con il PIN e i dettagli della carta è possibile creare una carta a banda magnetica duplicata da usare negli sportelli bancomat non aggiornati con lettori di smart card.

Nel gergo del Common Criteria, la specifica richiede che vengano rilevati i dispositivi di PIN-tapping. Tuttavia, è stato dimostrato che numerosi PED sul mercato presentavano dei difetti che

consentivano l'acquisizione di PIN e dettagli della carta. Uno di questi era l'Ingenico i3300, che era dotato addirittura di uno scomparto posteriore in cui era possibile riporre un dispositivo di intercettazione. Tutto quello che era necessario fare era praticare un piccolo foro nella custodia e agganciare una graffetta a una linea di comunicazione sulla quale venivano inviati i PIN e i dettagli della carta non crittografati. I criminali hanno eseguito questo tipo di attacchi su questo dispositivo.



Figura 7.1. Ingenico i3300 PIN entry device [15]

Ingenico i3300 è uno dei numerosi PED pubblicizzati per aver superato la valutazione Common Criteria, ma era veramente banale manometterlo. Cosa è andato storto? Le indagini condotte dagli autori dell'articolo non hanno portato a determinare quale laboratorio avesse effettuato la valutazione del dispositivo. Successivamente si è scoperto che la valutazione non era stata eseguita correttamente: un laboratorio di test autorizzato valutava i PED ma non coinvolgeva un ente governativo autorizzato a rilasciare certificazioni Common Criteria. Saltare questa fase cruciale elimina la pressione sui laboratori di test affinché svolgano un buon lavoro, e dunque le valutazioni non venivano fatte in modo ottimale.

Un altro caso analizzato è quello del dispositivo IBM 4758 HSM, un crypto-processore trovato insicuro nonostante fosse stato certificato. Il dispositivo aveva ottenuto la certificazione FIPS-140 livello 4 (il più alto possibile) a seguito di una rigorosa valutazione delle sue misure di resistenza alla manomissione e della funzionalità crittografica.

Gli aggressori che desideravano estrarre le chiavi da questo dispositivo attraverso manomissione fisica, dovevano gestire più strati di rete anti-manomissione, resinatura epossidica, sensori di temperatura e rilevatori a raggi X. Tuttavia, la valutazione non ha incluso il software caricato sul dispositivo, l'IBM Common Cryptographic Architecture (CCA).

Il CCA era stato concepito per garantire che nessuno potesse avviare una procedura in grado di compromettere la sicurezza delle chiavi più sensibili richiedendo che le chiavi generate venissero divise in due parti e consegnate a due persone diverse.

La crittografia e l'autenticazione nel settore dei pagamenti utilizzavano, ai tempi di questo studio, il 3DES con due chiavi a 56 bit (ovvero una chiave a 112 bit). Il 3DES era sufficientemente sicuro per la maggior parte degli scopi, ma per compatibilità con le versioni precedenti, il dispositivo IBM 4758 supportava anche il single DES (chiavi a 56 bit) che poteva essere facilmente "rotto" con un attacco brute force.

Il problema con l'IBM 4758 derivava dunque dal fatto che il FIPS-140 valutava l'hardware che però usava un software CCA non certificato, e la conseguenza era un prodotto non sicuro.

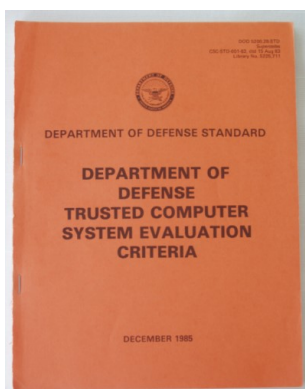
Questo è un esempio specifico di un problema più generale, ossia determinare se l'ambiente del sistema certificato è sufficiente per assicurare il raggiungimento degli obiettivi di sicurezza. Per aggiungere questo al processo di certificazione sono stati proposti tre tipi di certificazione:

- **Design Certification:** una serie di test e controlli che stabiliscono che le misure di sicurezza progettate nell'hardware e nel software del sistema sono operative, funzionano come previsto e costituiscono controlli accettabili per la salvaguardia delle informazioni classificate.
- **Installation Certification:** una serie di test e controlli eseguiti secondo le specifiche stabilite durante la fase di design certification per garantire che l'insieme di misure di sicurezza richiesto (hardware, software e procedurali) siano effettivamente presenti e funzionanti nelle apparecchiature installate e su tutti i collegamenti di comunicazione che trasportano informazioni riservate a terminali remoti o altri computer.
- **Recertification:** un certo livello di ricertificazione deve essere raggiunto periodicamente.

## Capitolo 8

# Confronto con il passato

### 8.1 TCSEC



[16] Il Trusted Computer System Evaluation Criteria (TCSEC) è uno standard del Dipartimento della Difesa (DoD) del governo degli Stati Uniti che stabilisce i requisiti di base per valutare l'efficacia dei controlli di sicurezza informatica integrati in un sistema informatico. È riconosciuto per essere il primo vero standard per la sicurezza informatica.

Il TCSEC veniva usato per valutare, classificare e selezionare i sistemi informatici presi in considerazione per l'elaborazione, l'archiviazione e il recupero di informazioni sensibili.

Il TCSEC, frequentemente chiamato anche "Orange Book", è il fulcro delle pubblicazioni "Rainbow Series" del Dipartimento della Difesa. Inizialmente emesso nel 1983 dal National Computer Security Center (NCSC), un ramo della National Security Agency, e poi aggiornato nel 1985, il TCSEC è stato infine sostituito dallo standard internazionale Common Criteria, pubblicato nel 2005.

#### 8.1.1 Obiettivi e requisiti fondamentali

##### Policy

La politica di sicurezza deve essere esplicita, ben definita e applicata dal sistema informatico. Vengono specificate tre politiche di sicurezza di base:

- **Mandatory Security Policy:** applicare regole di controllo dell'accesso basate direttamente sull'autorizzazione di un individuo, sull'autorizzazione per le informazioni e sul livello di riservatezza delle informazioni richieste. Altri fattori indiretti sono fisici e ambientali. Questa politica deve anche riflettere accuratamente le leggi, le politiche generali e altri orientamenti pertinenti da cui derivano le regole.



- **Marking:** sistemi progettati per applicare una “mandatory security policy” devono archiviare e preservare l'integrità delle etichette di controllo dell'accesso e conservare le etichette se l'oggetto viene esplorato.
- **Discretionary Security Policy:** applica un insieme coerente di regole per il controllo e la limitazione dell'accesso in base a individui identificati che si ritiene abbiano bisogno di conoscere le informazioni.

### Accountability

La responsabilità individuale, indipendentemente dalla politica, deve essere applicata. Deve esistere un mezzo sicuro per garantire l'accesso di un agente autorizzato e competente che possa quindi valutare le informazioni sulla responsabilità entro un periodo di tempo ragionevole e senza eccessive difficoltà. L'obiettivo dell'accountability comprende tre requisiti:

- **Identificazione:** il processo utilizzato per riconoscere un singolo utente.
- **Autenticazione:** la verifica dell'autorizzazione di un singolo utente a specifiche categorie di informazioni.
- **Auditing:** le informazioni di audit devono essere conservate e protette in modo che le azioni che influiscono sulla sicurezza possano essere ricondotte all'individuo autenticato.

### Assurance

Il sistema informatico deve contenere hardware/software che possono essere valutati in modo indipendente per fornire una garanzia sufficiente che il sistema applichi i requisiti citati sopra. Per estensione, la garanzia deve includere la garanzia che la parte attendibile del sistema funzioni solo come previsto.

### Documentazione

All'interno di ogni classe, una serie aggiuntiva di documentazione riguarda lo sviluppo, l'implementazione e la gestione del sistema e le sue capacità.

### Divisione e Classi

Il TCSEC definisce quattro divisioni: D, C, B, e A, dove la divisione A ha la sicurezza più elevata. Ciascuna divisione rappresenta una significativa differenza nella fiducia che si può riporre nel sistema. Inoltre le divisioni C, B e A sono a loro volta suddivise in una serie di classi: C1, C2, B1, B2, B3 e A1. Ciascuna divisione e classe espande o modifica i requisiti della divisione o classe immediatamente precedente.

### D – Minimal protection

- Riservata a quei sistemi che sono stati valutati ma che non soddisfano i requisiti per una divisione superiore

## C – Discretionary protection

- C1 – Discretionary Security Protection
  - Identificazione e autenticazione
  - Separazione di utenti e dati
  - Discretionary Access Control (DAC) in grado di imporre limitazioni di accesso su base individuale
  - Documentazione di sistema e manuali utente richieste
- C2 – Controlled Access Protection
  - DAC a maggiore granularità
  - Responsabilità individuale attraverso procedure di login
  - Percorsi di audit
  - Riutilizzo degli oggetti
  - Isolamento delle risorse

## B – Mandatory protection

- B1 - Labeled Security Protection
  - Dichiarazione informale del security policy model
  - Etichette di sensibilità dei dati
  - Mandatory Access Control (MAC) su soggetti e oggetti selezionati
  - Etichetta le capacità di esportazione
  - Alcuni flaw scoperti devono essere rimossi o almeno mitigati
  - Specifiche di progettazione e verifica
- B2 - Structured Protection
  - Security policy model chiaramente definito e formalmente documentato
  - DAC e MAC Enforcement estesi a tutti i soggetti e oggetti
  - I Covert storage channel di archiviazione sono analizzati per occorrenza e larghezza di banda. (Un covert channel è qualsiasi canale di comunicazione che può essere sfruttato da un processo per trasferire informazioni in un modo che viola la politica di sicurezza del sistema.)
  - Strutturato con cura in elementi critici e non critici
  - La progettazione e l'implementazione consentono test e revisioni più completi
  - Meccanismi di autenticazione rafforzati
  - Il Trusted facility management è fornito con amministratore e segregazione dell'operatore
  - Vengono imposti rigorosi controlli di gestione della configurazione
  - I ruoli dell'operatore e dell'amministratore sono separati
- B3 - Security Domains

- Soddisfa i requisiti del reference monitor
- Strutturato per escludere il codice non essenziale per l'applicazione della politica di sicurezza
- Ingegneria di sistema significativa diretta per ridurre al minimo la complessità
- Definizione del ruolo di Security Administrator
- Audit degli eventi rilevanti per la sicurezza
- Intrusion detection, notifica e risposta automatizzati
- Percorso affidabile al TCB per la funzione di autenticazione utente
- Procedure affidabili di recupero del sistema
- I Covert timing channels sono analizzati per occorrenza e larghezza di banda

### A – Verified protection

- A1 - Verified Design
  - Identico al B3 a livello funzionale
  - Tecniche di progettazione e verifica formale tra cui una specifica formale di alto livello
  - Procedure di gestione e distribuzione formale

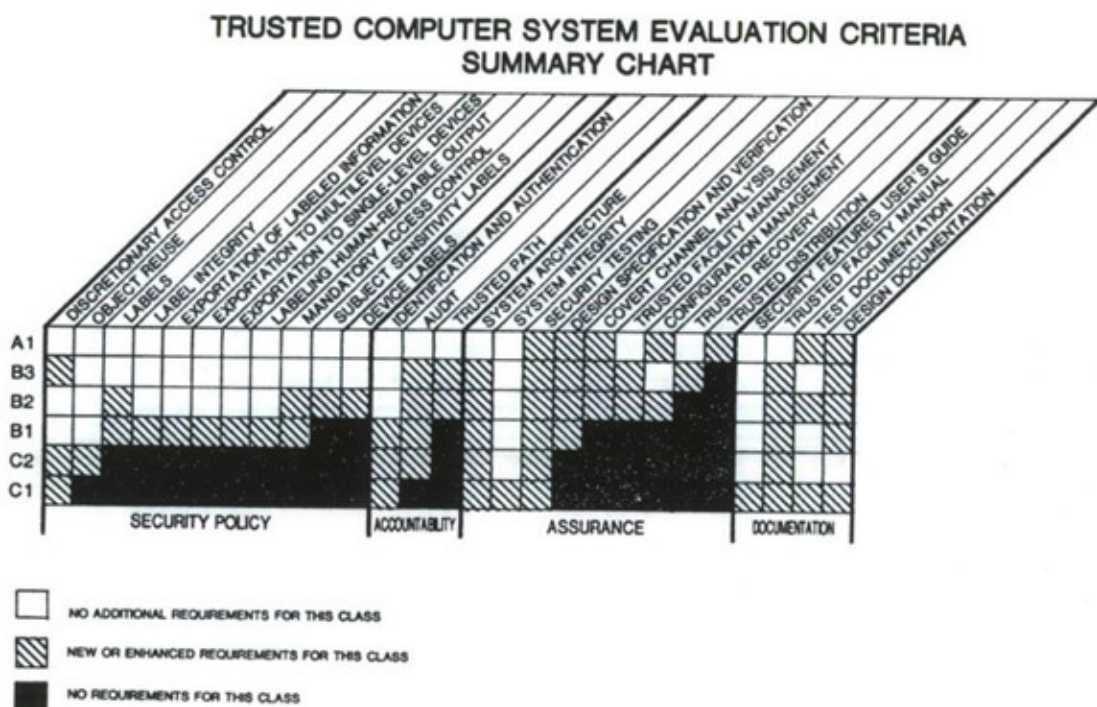


Figura 8.1. Grafico riassuntivo del TCSEC Evaluation Criteria [17]

### 8.1.2 Linee guida per i test sulla sicurezza

[17] Di seguito verranno riportate le principali linee guida presenti nell'Orange Book riguardo i security test per un sistema informatico.

#### Test per la Divisione C

Il “security testing team” deve essere composto da almeno due persone con laurea in informatica o una laurea equivalente. I membri del team dovranno essere in grado di seguire i piani di test preparati dal system developer. Prima dell’inizio dei test, i membri del team dovranno avere una conoscenza funzionale dell’intero sistema che dovrà essere valutato.

Il team dovrà essere coinvolto ”praticamente” in un’esecuzione indipendente dei test utilizzati dallo sviluppatore del sistema. Il team dovrà progettare e implementare in modo indipendente almeno cinque test specifici nel tentativo di aggirare i meccanismi di sicurezza del sistema. Il tempo per eseguire i test dovrà essere compreso tra un minimo di un mese e un massimo di tre mesi.

#### Test per la Divisione B

A livello di team differisce dalla divisione precedente perché almeno un membro del team dovrebbe avere una laurea magistrale in informatica o una equivalente. Oltre ai requisiti già presenti prima, almeno un membro del team dovrà aver già precedentemente completato dei security test su un altro sistema.

Il team dovrà progettare e implementare in modo indipendente almeno quindici test specifici del sistema nel tentativo di aggirare i meccanismi di sicurezza del sistema. Il tempo dedicato ai test dovrà essere di almeno due mesi e non superiore ai quattro mesi.

#### Test per la Divisione A

Il team dovrà essere composto da almeno un membro con laurea triennale in informatica e almeno due membri con laurea magistrale. In aggiunta ai requisiti visti nelle divisioni precedenti, almeno un membro del team deve avere sufficiente familiarità con l’hardware del sistema per comprendere i programmi diagnostici di manutenzione e la documentazione hardware di supporto. Almeno due membri del team dovranno aver già precedentemente completato dei security test su un altro sistema.

Il team dovrà progettare e implementare in modo indipendente almeno trenta test specifici del sistema nel tentativo di aggirare i meccanismi di sicurezza del sistema. Il tempo dedicato ai test dovrà essere di almeno tre mesi e non superiore ai sei mesi.

## 8.2 L’evoluzione

Come detto in precedenza il TCSEC, o Orange Book, può essere considerato uno dei capostipiti degli standard di sicurezza. Ovviamente ha subito nel corso degli anni numerose variazioni, dovute all’evoluzione della tecnologia e di conseguenza della sicurezza informatica, fino ad essere stato sostituito dal Common Criteria. Verranno quindi di seguito sottolineate alcune delle differenze negli approcci dei due diversi standard.

### 8.2.1 Test

[18] La classe di test comprende cinque famiglie: Coverage, Depth, Independent testing, Functional tests e Composite functional testing.

#### Coverage

Questa famiglia stabilisce che le proprietà di sicurezza del TOE (TSF) sono state testate rispetto alle specifiche funzionali. I componenti di questa famiglia vengono livellati in base alle specifiche.

#### Depth

I componenti di questa famiglia riguardano il livello di dettaglio con cui il TSF viene testato dallo sviluppatore. I test si basano su informazioni sempre più approfondite derivate da rappresentazione e descrizioni di progettazione aggiuntive.

L'obiettivo è contrastare il rischio di perdere un errore nello sviluppo del TOE. I test che esercitano specifiche interfacce interne possono garantire non solo che il TSF mostri il comportamento di sicurezza desiderato, ma anche che questo comportamento derivi dal corretto funzionamento delle funzionalità interne.

I componenti di questa famiglia vengono livellati sulla base del crescente dettaglio fornito nelle rappresentazioni TSF, dalla progettazione del TOE alla sua rappresentazione implementativa.

La prova del test della progettazione del TOE deve dimostrare che le interfacce interne siano state esercitate e viste comportarsi come descritto. Ciò può essere ottenuto testando tramite le interfacce esterne del TSF o testando il sottosistema del TOE o le interfacce del modulo in maniera isolata, magari utilizzando un cablaggio di prova.

#### Functional tests

I test funzionali eseguiti dallo sviluppatore garantiscono che i test nella documentazione di test siano eseguiti e documentati correttamente. La corrispondenza di questi test alle descrizioni progettuali del TFS è ottenuta attraverso le famiglie di Coverage e Depth. Questa famiglia contribuisce a garantire che la probabilità di difetti non scoperti sia relativamente piccola.

#### Independent testing

Gli obiettivi di questa famiglia si basano sulle garanzie ottenute grazie alle famiglie viste in precedenza, verificando i test dello sviluppatore ed eseguendo test aggiuntivi da parte del valutatore.

Il livellamento si basa sulla quantità di documentazione di test dello sviluppatore e di supporto al test e sulla quantità di test del valutatore.

### 8.2.2 Differenze tra TCSEC e Common Criteria

Con il passare degli anni e l'evolversi delle minacce informatiche e della tecnologia, l'Orange Book è stato gradualmente superato da una più moderna e flessibile iniziativa nota come il Common Criteria (CC). Quest'ultimo rappresenta un cambiamento di paradigma nella valutazione della

sicurezza informatica, introducendo concetti innovativi che hanno contribuito a ridefinire il modo in cui affrontiamo la sicurezza dei sistemi informatici.

Come si può notare più nello specifico nella descrizione dei test nei due diversi standard, l'approccio è ovviamente differente. Questo ovviamente accade anche in altri ambiti, non solo nel campo dei test. Di seguito verranno riportate le principali differenze tra i due standard.

### **Approccio di Valutazione**

- Il TCSEC utilizzava un approccio basato su livelli di sicurezza, suddividendo i sistemi in categorie di classificazione, come D, C, B e A, con A come il livello più alto. Ogni livello aveva specifici requisiti di sicurezza associati.
- Il CC utilizza un approccio basato su profili di protezione (PP) e riconoscimenti di garanzia (ST), consentendo una maggiore flessibilità nella definizione dei requisiti di sicurezza. Gli utenti possono selezionare i profili di protezione appropriati per le loro esigenze e confrontarli con le dichiarazioni di garanzia dei prodotti.

### **Struttura e Documentazione**

- Il TCSEC aveva una struttura di valutazione rigidamente definita con requisiti specifici per ciascun livello di sicurezza. La documentazione era pesante e dettagliata.
- Il CC offre una struttura più modulare e flessibile. La documentazione può essere adattata alle esigenze specifiche e ai profili di protezione selezionati, consentendo una maggiore adattabilità.

### **Copertura Internazionale**

- Inizialmente, il TCSEC era specificamente un'iniziativa degli Stati Uniti, e la sua adozione internazionale era limitata.
- Il CC è stato sviluppato come uno standard internazionale, con il coinvolgimento di molti paesi. Ciò ha contribuito a una sua diffusione più ampia a livello globale e alla sua accettazione come uno standard di riferimento per la valutazione della sicurezza.

### **Aggiornamenti e Mantenimento**

- Il TCSEC ha subito revisioni limitate nel tempo ed è stato sostituito solo gradualmente dal CC.
- Il CC è stato soggetto a revisioni regolari per tenere il passo con gli sviluppi tecnologici e le nuove minacce. Questo processo di aggiornamento ha contribuito a mantenere la sua rilevanza nel corso degli anni.

### **Flessibilità e Adattabilità**

- Il TCSEC spesso è stato criticato per la sua rigidità e per il fatto che poteva non essere facilmente adattato a sistemi moderni e complessi.

- Il CC è stato progettato per essere più flessibile e adattabile alle varie esigenze dei prodotti e dei sistemi, consentendo una maggiore applicabilità pratica.

Queste differenze riflettono l'evoluzione delle esigenze nel campo della sicurezza informatica e la transizione da un approccio basato su classificazioni di sicurezza a uno più flessibile e orientato agli standard internazionali, come il Common Criteria.

## Capitolo 9

# Caso di Studio: Piattaforma 3DEXPERIENCE

### 9.1 Introduzione

Con una storia ricca di innovazioni, Dassault Systèmes ha sviluppato la piattaforma 3DEXPERIENCE, una soluzione rivoluzionaria progettata per elevare la progettazione, la produzione e la gestione dei prodotti a nuovi livelli di efficienza e collaborazione.

La piattaforma 3DEXPERIENCE rappresenta un ecosistema digitale unificato che si estende oltre i confini tradizionali della progettazione e della produzione. È un'infrastruttura tecnologica all'avanguardia che permette a organizzazioni di varie dimensioni e settori di affrontare le sfide complesse legate all'innovazione, alla qualità, alla collaborazione e alla sicurezza dei dati.

Al centro di questo capitolo, esploreremo in dettaglio la piattaforma 3DEXPERIENCE, le sue funzionalità di base e, in particolare, le proprietà di sicurezza implementate per garantire la protezione delle informazioni sensibili e il controllo degli accessi. Prima di immergerci nell'analisi delle caratteristiche di sicurezza, è fondamentale acquisire una comprensione approfondita dei concetti chiave che sottendono questa piattaforma e il motivo per cui essa riveste un ruolo così rilevante nel contesto delle aziende moderne.

#### 9.1.1 Product Lifecycle Management (PLM): Un Fondamento dell'Innovazione

Al centro della 3DEXPERIENCE sta il concetto di Product Lifecycle Management (PLM), un approccio strategico e tecnologico alla gestione di prodotti e informazioni correlate lungo l'intero ciclo di vita. Il PLM non è solamente una metodologia, ma una filosofia che mira a ottimizzare la progettazione, lo sviluppo, la produzione e il supporto dei prodotti.

Attraverso il PLM, le aziende possono realizzare una gestione più efficace delle risorse, migliorare la collaborazione tra team multidisciplinari, accelerare il time-to-market dei prodotti e, soprattutto, garantire la qualità e la sicurezza dei dati che guidano le decisioni di progettazione e produzione. La 3DEXPERIENCE di Dassault Systèmes è stata progettata con il PLM come fondamento, offrendo un ambiente digitale in cui i dati, i processi e le persone sono connessi in modo sinergico per consentire una gestione del ciclo di vita del prodotto completa e integrata.



Nei paragrafi seguenti, esploreremo ulteriormente la piattaforma 3DEXPERIENCE e le sue specifiche funzionalità di sicurezza, mettendo in luce come queste caratteristiche siano state progettate per proteggere le informazioni critiche e facilitare una gestione affidabile dei dati all'interno del contesto del PLM.

### 9.1.2 Elementi Chiave della Piattaforma 3DEXPERIENCE

- **Unificazione dei processi di Progettazione e Produzione:** La piattaforma 3DEXPERIENCE consente l'integrazione completa delle diverse fasi del ciclo di vita del prodotto. Dai concetti iniziali alla progettazione, dalla simulazione alla produzione, fino alla manutenzione e alla gestione delle varianti, tutto è unificato in un ambiente digitale. Questa sinergia tra reparti e funzioni favorisce la riduzione degli errori, il risparmio di tempo e il miglioramento complessivo dell'efficienza.
- **Collaborazione globale e connettività:** La 3DEXPERIENCE abilita la collaborazione in tempo reale tra team distribuiti in tutto il mondo. Questo è particolarmente rilevante in un'epoca in cui i progetti spesso coinvolgono professionisti e partner in diverse regioni geografiche. Gli utenti possono condividere dati, progetti e risorse in un ambiente sicuro e controllato.
- **Gestione avanzata dei dati e delle informazioni:** La piattaforma offre un sistema di gestione dei dati altamente avanzato, consentendo agli utenti di organizzare, tracciare e controllare i dati di progetto in modo preciso. Questo garantisce la coerenza delle informazioni e una maggiore trasparenza in tutto il ciclo di vita del prodotto.
- **Simulazione e Analisi:** La 3DEXPERIENCE offre strumenti avanzati di simulazione e analisi che consentono agli ingegneri e ai progettisti di testare virtualmente i loro concetti e progetti prima di passare alla produzione fisica. Ciò riduce i costi e accelera il processo di sviluppo.
- **Sicurezza dei dati:** Una caratteristica fondamentale della 3DEXPERIENCE è la sicurezza dei dati. Dato che le informazioni sui prodotti possono essere altamente sensibili e riservate, la piattaforma incorpora solide funzionalità di sicurezza per proteggere l'accesso non autorizzato e garantire la confidenzialità delle informazioni.
- **Personalizzazione e adattabilità:** La piattaforma è altamente personalizzabile per adattarsi alle esigenze specifiche di ciascuna organizzazione. Gli utenti possono configurare l'ambiente di lavoro secondo le proprie preferenze e i requisiti del progetto.
- **Integrazione con tecnologie emergenti:** La 3DEXPERIENCE è in costante evoluzione per integrare le tecnologie emergenti come l'intelligenza artificiale, la realtà virtuale e aumentata, e altro ancora, per migliorare ulteriormente le capacità di progettazione e produzione.

### Panoramica della Piattaforma

La piattaforma 3DEXPERIENCE offre una serie di applicazioni e widget utili a ricoprire la maggior parte dei casi d'uso necessari per un'azienda in ambito PLM. La piattaforma si presenta come in [Figura 9.1](#). Tale figura mostra la visualizzazione della Dashboard, una finestra in cui è possibile creare vari tab dove a sua volta è possibile inserire i widget. Sulla sinistra si visualizzano le applicazioni e i widget, contrassegnati dalla freccia in alto a destra nell'icona, a cui l'utente attualmente connesso ha accesso.

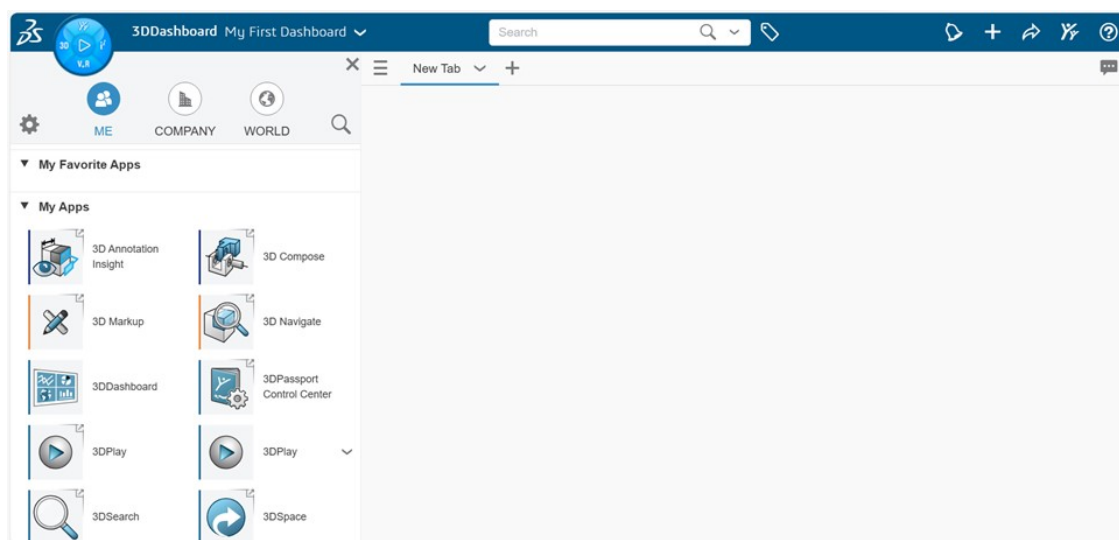


Figura 9.1. Screenshot della Dashboard della 3DEXPERIENCE

I widget possono essere trascinati all'interno del tab della dashboard come mostrato in [Figura 9.2](#), in questo modo è possibile avere più widget nello stesso tab. Questo risulta essere molto utile soprattutto quando si utilizzano widget che comunicano tra loro trascinando oggetti da uno all'altro.

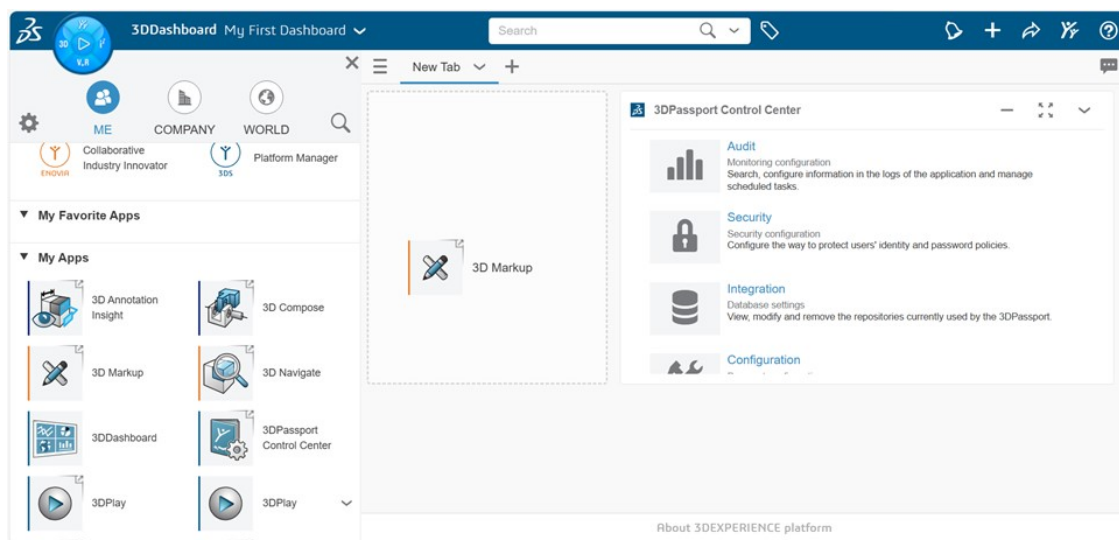


Figura 9.2. Screenshot della Dashboard della 3DEXPERIENCE con widget

All'interno della piattaforma esistono ovviamente altre interfacce e schede utili per altre attività, come per esempio quella di gestione della piattaforma lato amministrativo, gestione delle utenze e altre ancora, ma la descrizione dettagliata della piattaforma è al di fuori degli obiettivi della tesi.

### 9.1.3 Installazione 3DEXPERIENCE

L'installazione della piattaforma della 3DEXPERIENCE all'interno di un ambiente di test è stata il risultato di una necessità aziendale per poter soddisfare le richieste di un cliente che desiderava adottare la soluzione on-premise. In un contesto aziendale in cui l'uso predominante è sempre stato orientato verso la soluzione on-cloud, questa transizione rappresentava una nuova sfida che richiedeva un'ottima comprensione dei processi di installazione e configurazione specifici per l'ambiente on-premise.

La complessità dell'installazione e della configurazione della piattaforma 3DEXPERIENCE non poteva essere sottovalutata, considerando la natura sfaccettata e interconnessa dei suoi numerosi servizi. L'installazione richiedeva la corretta integrazione e il funzionamento ottimale di tutti i suoi diversi componenti, nonché la garanzia che questi servizi potessero comunicare in modo affidabile e sicuro tra loro.

L'acquisizione delle conoscenze e competenze per poter installare e configurare la piattaforma senza problemi non è limitato al singolo progetto in corso, ma rappresenta anche un investimento a lungo termine per l'azienda, in previsione di potenziali richieste future da parte di altri clienti interessati ad adottare la soluzione on-premise.

#### Il processo di installazione

Di seguito verrà spiegato molto brevemente il processo seguito per l'installazione della piattaforma, in modo da dare un giusto contesto e un'idea generale dei vari step eseguiti.

Inizialmente, il processo è iniziato con la definizione degli URL di ogni endpoint per i singoli servizi della piattaforma, andando a modificare il file "hosts" all'interno della macchina. Questo passaggio preliminare ha consentito di stabilire connessioni e punti di accesso chiari per ogni servizio, facilitando così la configurazione successiva e la gestione delle interazioni tra i vari moduli.



```

22
23 127.0.0.1 localhost 3dpassport.heritplm.com 3ddashboard.heritplm.com
   untrusted.3ddashboard.heritplm.com 3dsearch.heritplm.com 3dspace.heritplm.com
   fcs.heritplm.com
24
25 127.0.0.1 3dswym.heritplm.com 3dcomment.heritplm.com 3dnotification.heritplm.com
   3dmessaging.heritplm.com 3dspace.fulltextsearch.heritplm.com
   3dswym.fulltextsearch.heritplm.com

```

Figura 9.3. Configurazione del file "hosts" nell'ambiente di test

Successivamente, è stata data priorità alla configurazione dei database, con la creazione di un database dedicato per ciascuno dei servizi principali della piattaforma. Questa fase ha richiesto una gestione adeguata delle risorse per garantire che ogni database fosse configurato correttamente e allineato con le specifiche esigenze e i requisiti funzionali dei rispettivi servizi.

Dopo il setup dei database, è stato necessario procedere con l'installazione e la configurazione di un server Apache come reverse proxy. Questa componente è fondamentale per consentire una comunicazione sicura e affidabile tra gli utenti e i diversi servizi della piattaforma, garantendo al contempo una protezione aggiuntiva contro potenziali minacce esterne.

Infine, il focus si è spostato sull'installazione e la configurazione di ciascun servizio. Durante questa fase, oltre alla configurazione accurata in base alle specifiche dei database e degli URL,

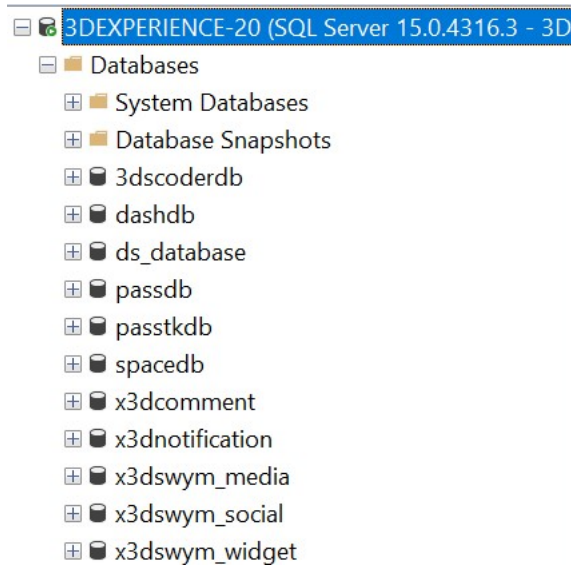


Figura 9.4. I database creati per l'installazione della piattaforma

è stato necessario eseguire la configurazione di un server di applicazione TomEE per ciascun servizio. Questo approccio consente di ottimizzare le prestazioni e di garantire un funzionamento ottimale di ciascun modulo della piattaforma, soprattutto in vista di un'installazione reale che prevederebbe la divisione dei servizi su diverse macchine per necessità di performance.

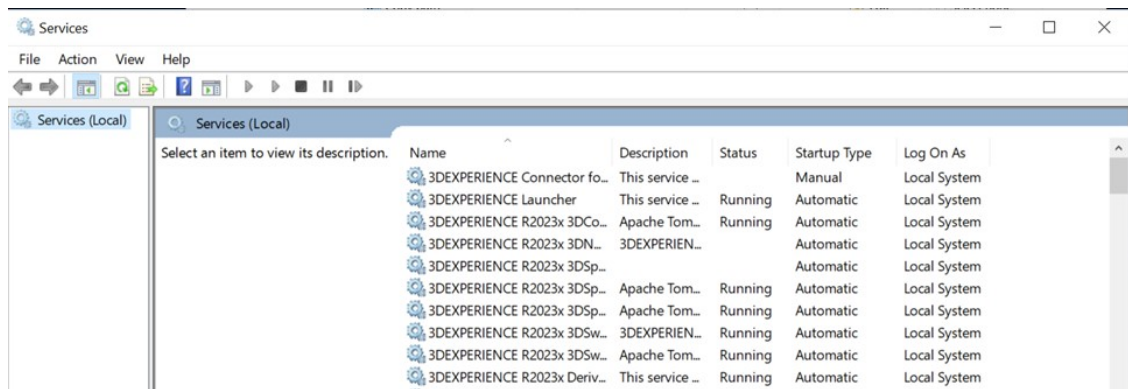


Figura 9.5. Tutti i servizi generati dai server TomEE per la piattaforma

### 9.1.4 Panoramica su Proprietà di sicurezza 3DEXPERIENCE

Di seguito, sono elencati alcuni degli aspetti tipici della sicurezza all'interno della 3DEXPERIENCE, insieme a possibili strategie utilizzate per garantire tali proprietà:

- **Access Control:** La 3DEXPERIENCE offre un robusto sistema di controllo degli accessi basato su ruoli e permessi. Gli utenti sono assegnati a ruoli specifici, ciascuno dei quali

ha accesso solo alle funzionalità e ai dati necessari per svolgere il proprio lavoro. Le autorizzazioni sono configurate in modo granulare per garantire che solo le persone autorizzate possano accedere a determinate informazioni.

- **Autenticazione:** Per proteggere l'accesso agli account utente, la piattaforma 3DEXPERIENCE supporta l'autenticazione forte, che richiede l'uso di metodi aggiuntivi oltre alle semplici credenziali, come l'autenticazione a due fattori (2FA) o l'autenticazione biometrica.
- **Crittografia dei dati:** I dati sensibili sono crittografati durante la trasmissione e in archivio. Questa crittografia garantisce che i dati siano protetti da accessi non autorizzati, anche se dovessero essere intercettati durante il trasferimento.
- **Autorizzazione:** L'autorizzazione è essenziale per garantire che solo utenti autorizzati possano accedere alla piattaforma. La 3DEXPERIENCE supporta l'integrazione con servizi di gestione delle identità (Identity and Access Management, IAM) per un controllo più completo delle identità degli utenti.
- **Audit e Monitoraggio:** La piattaforma registra le attività degli utenti e le modifiche ai dati. Questi log di audit consentono di monitorare l'utilizzo della piattaforma e di individuare comportamenti sospetti o anomalie. In caso di violazioni o intrusioni, questi log forniscono una traccia utile per le indagini.
- **Protezione dei dati durante collaborazioni:** La 3DEXPERIENCE facilita la collaborazione tra team e partner esterni. Tuttavia, per garantire la sicurezza dei dati condivisi, vengono implementate strategie come l'uso di link di condivisione protetti da password o l'accesso tramite token temporanei.
- **Rilevamento e risposta agli incidenti:** È importante avere un piano di rilevamento e risposta agli incidenti in caso di compromissione della sicurezza. La piattaforma dovrebbe consentire di isolare le minacce e mitigare gli attacchi in modo tempestivo.
- **Backup e ripristino dei dati:** La piattaforma dovrebbe offrire un sistema di backup e ripristino dei dati in modo che le informazioni critiche possano essere recuperate in caso di perdita o danneggiamento.

Queste sono solo alcune delle principali proprietà di sicurezza e delle relative strategie implementate nella piattaforma 3DEXPERIENCE. La sicurezza informatica è un aspetto critico per l'ambiente di gestione del ciclo di vita del prodotto e la piattaforma è progettata per fornire solide funzionalità di protezione e controllo per garantire la confidenzialità, l'integrità e la disponibilità dei dati.

## 9.2 Analisi su piattaforma 3DEXPERIENCE

Nel paragrafo precedente sono state elencate le principali proprietà di sicurezza implementate nella piattaforma 3DEXPERIENCE di Dassault Systemès. Ora ci immergeremo più in profondità in alcune di queste proprietà, esaminando le sfide e le strategie specifiche utilizzate per garantire un ambiente di lavoro sicuro.

Durante il tirocinio, ho avuto l'opportunità di installare la piattaforma 3DEXPERIENCE nella sua versione on-premise, concentrandomi non solo sul garantire il suo normale funzionamento, ma anche sulla configurazione dei componenti per garantire la massima sicurezza dei dati e delle informazioni. Va sottolineato che l'installazione è stata effettuata in un ambiente di test e non

in un contesto operativo completo. Inoltre il mio ruolo non è stato quello di avviare un processo di certificazione di sicurezza, il quale, come abbiamo più volte visto nei capitoli precedenti, richiederebbe tempo e risorse di esperti dedicati. Tuttavia, l'analisi delle fasi di installazione e delle configurazioni necessarie per garantire la sicurezza è stata un passo cruciale nell'ambito della valutazione della robustezza della piattaforma.

La 3DEXPERIENCE è già conforme a standard di sicurezza riconosciuti a livello internazionale:

- **ISO/IEC 27001:** Questo standard internazionale definisce i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS) e fornisce linee guida per stabilire, implementare, mantenere e migliorare la sicurezza delle informazioni all'interno di un'organizzazione. L'adozione di ISO/IEC 27001 assicura che la piattaforma 3DEXPERIENCE segua un approccio sistematico per la gestione della sicurezza delle informazioni;
- **NIST SP 800-53:** Questo documento pubblicato dal NIST fornisce un insieme di controlli di sicurezza e linee guida per gli ambienti informatici federali negli Stati Uniti. L'implementazione dei controlli di sicurezza definiti in NIST SP 800-53 assicura che la piattaforma 3DEXPERIENCE adotti le misure di sicurezza adeguate per proteggere i dati e i sistemi;
- **GDPR:** Il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea stabilisce le norme per la protezione dei dati personali dei cittadini europei. La piattaforma 3DEXPERIENCE tiene conto delle disposizioni del GDPR per garantire la protezione dei dati personali degli utenti e il rispetto della privacy.

Nonostante questo, in un'installazione on-premise è fondamentale adottare misure specifiche per adattare la piattaforma alle esigenze e alle politiche di sicurezza dell'organizzazione ospitante.

Nei prossimi paragrafi verranno esaminati alcuni degli aspetti più importanti dell'installazione della piattaforma e le configurazioni specifiche necessarie per garantire un ambiente di lavoro sicuro. Vedremo come le strategie di controllo degli accessi, l'autenticazione, la crittografia dei dati e altre misure di sicurezza abbiano contribuito a mitigare i rischi e a proteggere le informazioni all'interno della piattaforma.

### 9.2.1 Struttura della piattaforma 3DEXPERIENCE

La piattaforma 3DEXPERIENCE comprende una serie di servizi, ognuno dedicato a determinate funzionalità e tutti collegati tra loro. L'installazione della piattaforma comprende l'installazione e la configurazione separata per ogni servizio e l'associazione ad un preciso indirizzo URL per raggiungere tale servizio. La guida all'installazione fornita da Dassault Systemès [19] fornisce il diagramma presente in [Figura 9.6](#) che illustra la distribuzione della piattaforma on-premise che include anche load balancers, failover clusters e un reverse proxy.

**Reverse Proxy:** Un reverse proxy è un tipo di proxy server che recupera risorse per conto di un client da uno o più server. Queste risorse sono poi restituite al client come se avessero avuto origine dal proxy stesso. Mentre un forward proxy fa da intermediario per i suoi client associati per contattare qualunque server, un reverse proxy è un intermediario per i suoi server associati per essere contattato da qualunque client. In altre parole, un forward proxy agisce per conto dei client, mentre il reverse per conto dei server.

Il reverse proxy viene tipicamente configurato configurando il web-server. Le utilità del reverse proxy sono molteplici, ecco alcune delle più importanti:

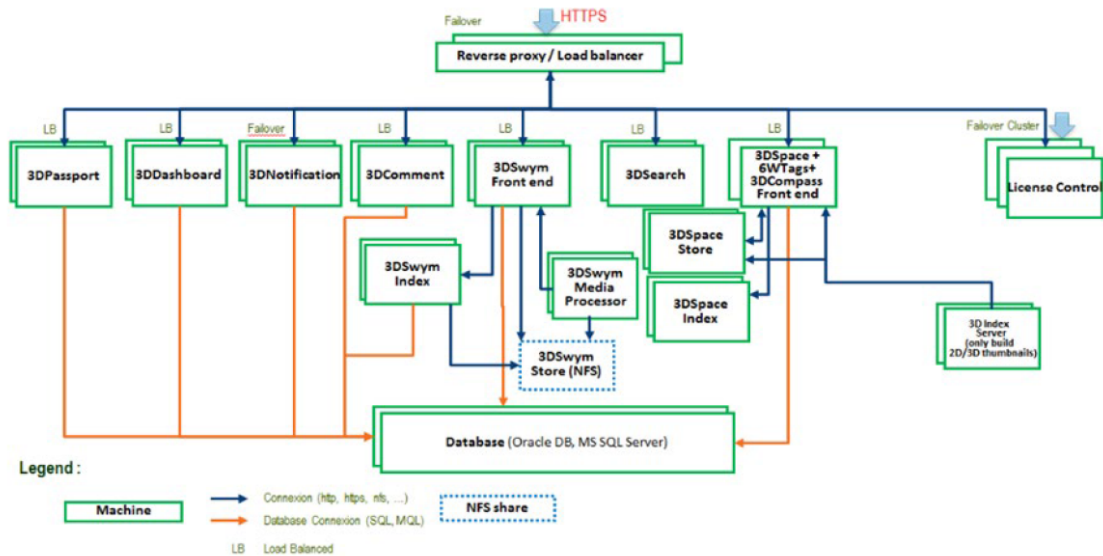


Figura 9.6. Distribuzione della piattaforma 3DEXPERIENCE on-premise [19]

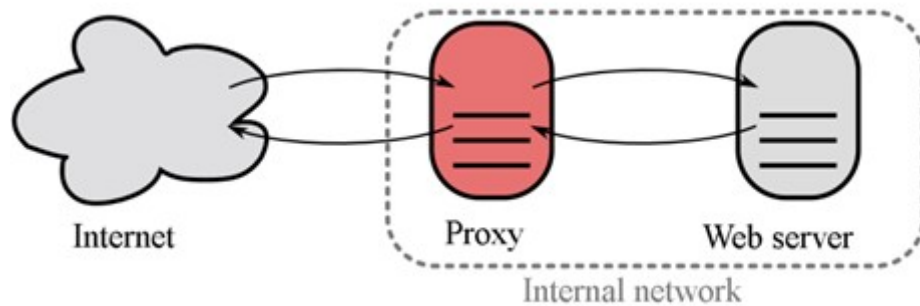


Figura 9.7. Reverse Proxy [20]

- Può nascondere l'esistenza e le caratteristiche dei server di origine
- Le funzionalità dell'application firewall possono proteggere contro gli attacchi più comuni web-based, come il DoS o il DDoS. Senza un reverse proxy, rimuovere i malware o iniziare la rimozione, per esempio, può essere complicato
- In caso di siti web sicuri, un server web potrebbe non eseguire la crittografia TLS ma lasciare questa task al reverse proxy
- Un reverse proxy può distribuire il carico delle richieste in arrivo sui diversi server, con ciascun server che supporta la propria area di applicazione. Questo è chiamato Load Balancing:
  - Il load balancer si trova tra i dispositivi client e i backend server, e ricevendo e poi distribuendo le richieste in arrivo a qualsiasi application-server disponibile

- Il load balancing è un componente chiave per infrastrutture ad alta affidabilità

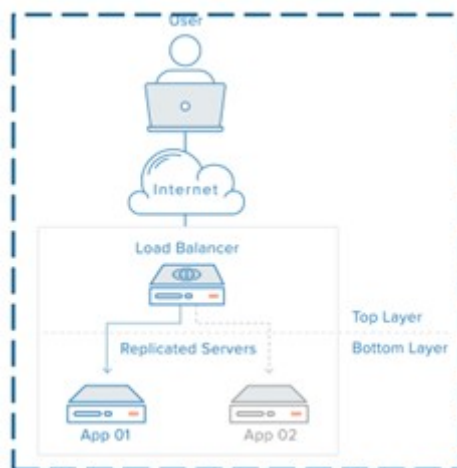


Figura 9.8. Load Balancing [20]

**Failover Clusters:** I failover clusters (o cluster di failover) sono una tecnologia utilizzata nel campo dell'informatica e delle reti per garantire l'alta disponibilità e la ridondanza dei servizi e delle applicazioni. Questi cluster sono progettati per gestire situazioni in cui un nodo o un componente di sistema fallisce, consentendo una transizione fluida verso un altro nodo funzionante senza interrompere il servizio o l'applicazione in uso. In questo caso specifico sono rappresentati dall'utilizzo di più macchine per un solo servizio. Ovviamente ciò che altamente difficile da realizzare per tutti i servizi, quindi di norma si utilizza questa strategia per quelli più importanti.

Nei paragrafi successivi affronteremo più nello specifico questi due concetti fondamentali per la disponibilità dei servizi e per la prevenzione da eventuali attacchi DoS.

## 9.2.2 Disponibilità

Come visto in precedenza le soluzioni adottate dalla piattaforma 3DEXPERIENCE per garantire la disponibilità continua dei servizi sono principalmente un Reverse Proxy con funzione di Load Balancer e Failover Clusters. Queste soluzioni garantiscono protezione a notevoli minacce, tra le quali:

- **Guasti Hardware:** Un componente hardware difettoso o in avaria, come un disco rigido, una scheda di rete o una fonte di alimentazione, può causare l'interruzione di un server. Il failover cluster o il reverse proxy possono mitigare questo rischio, trasferendo il carico di lavoro a un nodo funzionante.
- **Errori di sistema:** Gli errori di sistema, come il blocco del sistema operativo o un'applicazione che si blocca, possono provocare un'interruzione del servizio. Il failover cluster o il reverse proxy possono rilevare tali errori e commutare su un nodo operativo.



- **Aggiornamenti e Manutenzione:** Durante gli aggiornamenti del sistema o la manutenzione pianificata, un nodo potrebbe essere temporaneamente non disponibile. Failover cluster e il reverse proxy in questo caso consentono di spostare il carico di lavoro su altri nodi durante queste operazioni, riducendo al minimo l'impatto sui servizi.
- **Attacchi informatici:** Le minacce informatiche, come gli attacchi di tipo Denial of Service (DoS) o Distributed Denial of Service (DDoS), possono sovraccaricare un server o una rete, causando interruzioni. Anche in questo caso gli effetti di tali attacchi possono essere mitigati distribuendo il carico su più nodi.
- **Errore umano:** Gli errori umani, come la configurazione errata di un'applicazione o la cancellazione accidentale di dati critici, possono portare a interruzioni. Un failover cluster può contribuire a ripristinare il servizio in tali situazioni.
- **Catastrofi naturali:** Eventi imprevisti come terremoti, incendi o allagamenti possono danneggiare i data center o i server. La distribuzione geografica dei nodi in un failover cluster, spesso in diverse località fisiche, offre protezione contro tali catastrofi.
- **Carico di lavoro elevato:** In situazioni in cui un server o un'applicazione riceve un carico di lavoro superiore alla capacità, un failover cluster può bilanciare il carico tra i nodi per garantire le prestazioni ottimali.

L'utilizzo di queste due soluzioni dunque consente di indirizzare il traffico in modo uniforme tra più server backend, garantendo una distribuzione efficiente del carico di lavoro e riducendo il rischio di sovraccarico dei server. Inoltre, il reverse proxy può svolgere un ruolo cruciale nella gestione della sicurezza, proteggendo l'infrastruttura e nascondendola dagli attacchi esterni.

Nell'installazione svolta come caso di test è stato configurato un server Apache come reverse proxy per distribuire le richieste tra i server backend. Il server è stato configurato modificando il suo file di configurazione "httpd.conf" affinché potesse comunicare, ovviamente in modo sicuro tramite HTTPS, con tutti i servizi. Per permettere al reverse proxy di avere anche funzionalità di load balancer sono stati abilitati i moduli "mod\_proxy" e "mod\_proxy\_balancer". Il primo modulo consente la gestione delle richieste inoltrate ai server, mentre il secondo offre funzionalità di bilanciamento del carico, consentendo la distribuzione equa del traffico tra i server.

È importante notare che, nell'ambiente di test dedicato all'installazione e alla configurazione della piattaforma 3DEXPERIENCE, non è stata implementata un'infrastruttura completa di failover cluster. L'intera piattaforma è stata infatti installata in un'unica macchina virtuale mentre i failover avrebbero richiesto una configurazione specifica e l'allocazione di risorse dedicate che non erano a disposizione per questo tipo di attività.

In conclusione, la 3DEXPERIENCE adotta un approccio completo per garantire la disponibilità dei suoi servizi, sfruttando sia il reverse proxy con funzionalità di load balancer che, in situazioni più complesse, i failover clusters. La scelta di implementare specifiche soluzioni dipenderà dalle esigenze e dalla complessità dell'ambiente in cui la piattaforma viene installata.

### In Riferimento al NIST 800-53

Nel documento Security and Privacy Controls for Information Systems and Organizations del NIST Special Publication 800-53 [8] nella sezione Denial-Of-Service Protection, ciò che viene consigliato è:

*Gestire la capacità, la larghezza di banda o altre ridondanze per limitare gli effetti degli attacchi Denial of Service di information flooding. La gestione della capacità garantisce la disponibilità di*

capacità sufficiente per contrastare gli attacchi flooding. Questo include la definizione di priorità di utilizzo, quote, partizionamento o load balancing.

## Esempio Security Plan

In questo paragrafo andremo ad analizzare un possibile scenario sul Security Plan in cui si cerca di garantire la disponibilità della piattaforma. Verranno dunque analizzate le varie fasi spiegate in precedenza applicate però al caso reale.

Nel Risk Assessment vengono analizzati i rischi relativi a potenziali disservizi da parte dei server di applicazione che causerebbero un malfunzionamento della piattaforma. Tali disservizi potrebbero scatenarsi per diverse cause, prenderemo in considerazione le due più probabili:

- Malfunzionamento hardware
- Sovraccarico del traffico

Una volta indentificati e valutati i rischi, si passa, come visto in precedenza, al Risk Threatment, fase nella quale si vanno a valutare e scegliere le possibili contromisure per modificare tali rischi. Per i due rischi in questione le possibili mitigazioni potrebbero essere le seguenti:

- Per il malfunzionamento hardware si potrebbe predisporre una macchina di backup per la macchina che ospita il server di applicazione in questione. In questo modo si potrebbe garantire la continuità del servizio anche se una delle due macchine dovesse riscontrare dei malfunzionamenti. Tale soluzione potrebbe essere implementata in due modi:
  - **ATTIVO-ATTIVO:** in questo caso entrambe le macchine sarebbero sempre in funzione, dividendosi il carico di lavoro. Con questa soluzione si andrebbe a prevenire lo spreco di risorse in quanto non si avrebbe una macchina non attiva per gran parte del tempo ma sarebbero entrambe sempre in funzione. Il problema di questa soluzione sarebbe che entrambe le macchine sarebbero dimensionate per poter sopportare il 50% del traffico totale, quindi in caso di malfunzionamento di una delle due ci sarebbero dei rallentamenti e si dovrebbe gestire il fatto che tutto il traffico sarebbe preso in gestione da una sola macchina che però non è dimensionata per la totalità del traffico possibile.
  - **ATTIVO-PASSIVO:** con questa soluzione si mantiene una macchina sempre attiva e una spenta. La seconda macchina di backup verrà messa in funzione solo in caso di malfunzionamento della prima. Questa soluzione è migliore da un punto di vista di performance, in quanto non si avrà una perdita in tal senso nel caso la macchina principale abbia dei problemi. D'altro canto è ovviamente la soluzione più onerosa dal punto di vista delle risorse, essendo necessario avere entrambe le macchine dimensionate per poter reggere il 100% del possibile traffico massimo. In questo caso non sarebbe strettamente necessario l'utilizzo di un load balancer in quanto una sola macchina può garantire il supporto della totalità del traffico.
- Per il sovraccarico del traffico si inizia con un dimensionamento coerente al traffico stimato. Tale calcolo viene direttamente comunicato da Dassault Systemes una volta indicato il numero di utenti che hanno accesso alla piattaforma e una stima sulle connessioni contemporanee. In base a questi dati Dassault indica le caratteristiche minime e il numero minimo di macchine necessarie per ospitare i vari servizi della piattaforma. In questo modo si ha la certezza che l'infrastruttura sarà in grado di reggere il traffico atteso. Come esempio verrà di seguito riportata, in [Figura 9.9](#), una possibile infrastruttura pensata per il cliente

sulla base di alcune stime del possibile traffico ed utilizzo della piattaforma in tale azienda. L'infrastruttura comprende, oltre al server di licenza e al reverse proxy, ulteriori quattro macchine virtuali adibite ad ospitare i servizi della piattaforma ed i relativi database. Per

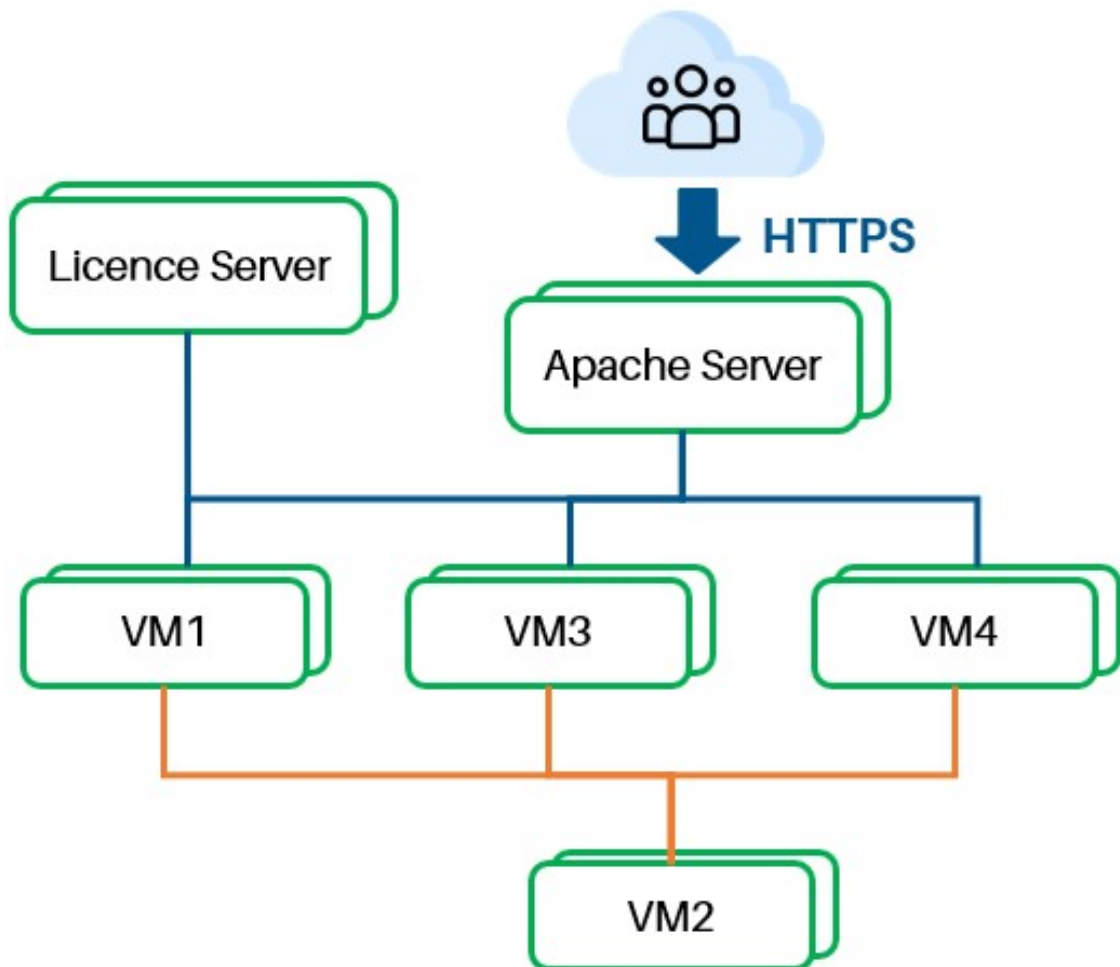


Figura 9.9. Esempio di possibile architettura della piattaforma

ciascuna macchina virtuale si era pensato una divisione dei servizi, mostrata in [Tabella 9.1](#), per sfruttare al massimo le risorse disponibili.

Per ogni macchina è stato effettuato un calcolo, in collaborazione con Dassault Systèmes, per poter ottenere il dimensionamento minimo necessario al fine di poter garantire la solidità dell'infrastruttura coerentemente con il traffico atteso. Tale dimensionamento è illustrato in [Tabella 9.2](#).

Oltre a questo è opportuno impostare un reverse proxy con funzionalità di load balancer come descritto in precedenza, non solo per gestire in modo efficace i vari accessi dall'esterno, ma anche per bloccare gli accessi non autorizzati, prevenendo anche attacchi DoS effettuati tramite l'invio di molteplici richieste in contemporanea.

VM1	VM2	VM3	VM4
3D PassportApp	3DPassport DB	3DSpace App	MQL Crawler
3D Dashboard App	3D Dashboard DB	3DSpace App Utilities	2D/3D Thumbnails Builder
3DSwym Foundation App	3DSwym Foundation DB		3DSpace Index file converter
3DSwym Media Converter App	3DOrchestrate DB		3DSwym Index
3DOrchestrate App	3DNotification DB		FCS Sync
3DNotification App 3	3DComment DB		3DSpace Index
3DComment App	3DSpace DB		FCS Central - HQ
3DSearch App Federated			

Tabella 9.1. Distribuzione dei servizi su ogni macchina virtuale

VM	Core	RAM	SSD
VM1	5,30	21,90 GB	1 TB
VM2	4,90	22,90 GB	1 TB
VM3	7	40,00 GB	2 TB
VM4	13,90	54,40 GB	1 TB
License 3	320	3,00 GB	256 GB

Tabella 9.2. Dimensionamento minimo delle macchine virtuali

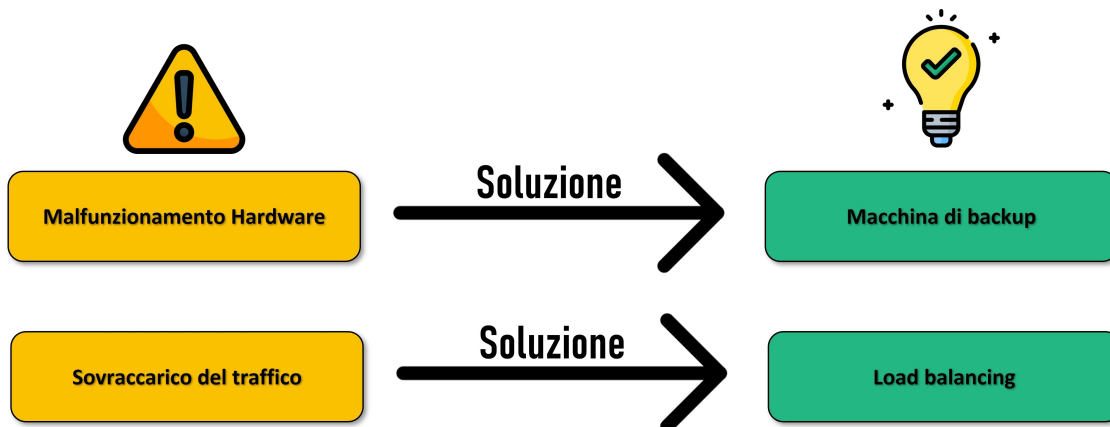


Figura 9.10. Schema di un Security Plan per minacce alla disponibilità della piattaforma

### 9.2.3 Crittografia dei dati

La protezione dei dati è un aspetto cruciale all'interno dell'ecosistema della piattaforma 3DEXPERIENCE, e uno dei pilastri fondamentali di questa protezione è l'utilizzo di HTTPS. Ma cosa significa concretamente HTTPS e come viene implementato all'interno di questa soluzione?

## HTTPS

L'HyperText Transfer Protocol over Secure Socket Layer (HTTPS) è un protocollo per la comunicazione sicura attraverso una rete di computer utilizzato su Internet. La porta utilizzata generalmente (ma non necessariamente) è la 443. Consiste nella comunicazione tramite il protocollo HTTP (Hypertext Transfer Protocol) all'interno di una connessione criptata, tramite crittografia asimmetrica, dal Transport Layer Security (TLS) [21] o dal suo predecessore, Secure Sockets Layer (SSL) [22] fornendo come requisiti chiave:

- un'autenticazione del sito web visitato;
- protezione della privacy (riservatezza o confidenzialità);
- integrità dei dati scambiati tra le parti comunicanti.

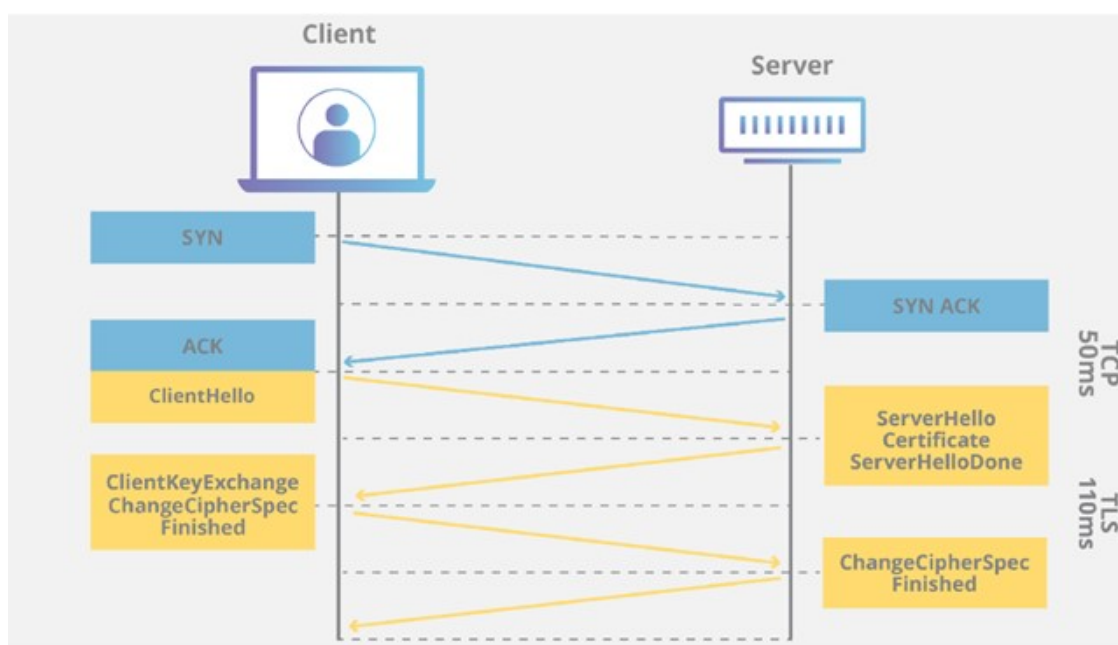


Figura 9.11. Schema del funzionamento di TLS [23]

Nel suo popolare funzionamento su Internet, HTTPS fornisce la sicurezza del sito web e del server web associato con cui una delle parti sta comunicando, proteggendo la comunicazione dagli attacchi noti tramite la tecnica del man in the middle. Inoltre, HTTPS fornisce una cifratura bidirezionale delle comunicazioni tra un client e un server, che protegge la stessa contro le possibili operazioni di eavesdropping, (azione mediante la quale viene ascoltata segretamente la conversazione privata tra le parti senza il loro consenso) e tampering (letteralmente manomissione o alterazione della comunicazione) falsificandone i contenuti. In pratica, tale meccanismo fornisce una garanzia soddisfacente del fatto che si sta comunicando esattamente con il sito web voluto (al contrario di un sito falso), oltre a garantire che i contenuti delle comunicazioni tra l'utente e il sito web non possano essere intercettate o alterate da terzi.

## HTTPS nella Soluzione On-Premise della 3DEXPERIENCE

Nella configurazione on-premise della piattaforma 3DEXPERIENCE, l'uso di HTTPS è una prassi comune per garantire la sicurezza delle comunicazioni tra i vari componenti della piattaforma. In questo contesto, HTTPS viene implementato attraverso l'uso di certificati digitali.

Ogni servizio all'interno della piattaforma 3DEXPERIENCE è tenuto a disporre di un proprio certificato valido. I certificati digitali sono dati crittografati che confermano l'identità del servizio e permettono di stabilire connessioni sicure. Ogni certificato contiene informazioni come il nome del servizio, la chiave pubblica, la data di scadenza e altro.

È possibile ottenere singoli certificati per ogni dominio, oppure servirsi del Subject Alternative Name (SAN), un'estensione dei certificati X.509 che consente di proteggere un dominio principale e successivamente i domini secondari che vanno indicati nella sezione dei Subject Alternative Names del profilo del certificato. L'ottenimento di un certificato può essere realizzato attraverso Certification Authorities (CA) commerciali o mediante altri servizi come per esempio Let's Encrypt [24].

Il formato di base dei certificati X.509 per un server web è il Domain Validation (DV), rilasciato dopo che la CA conferma che il richiedente controlla effettivamente il dominio per il quale è stato richiesto il certificato. Nonostante non esista una procedura standard per condurre tale verifica, di solito vengono impiegati i seguenti metodi di convalida:

- Tramite DNS
- Tramite Email
- Tramite validazione basata sul Web
- Tramite TLS handshake con Server Name Indication (TLS-SNI)

Let's Encrypt, per esempio, verifica l'identità del server attraverso la validazione DNS, la validazione basata sul Web e tramite TLS-SNI. Questo tipo di certificato è sufficiente per implementare il protocollo HTTPS all'interno della piattaforma, ma esistono anche dei formati più sicuri come i certificati Extended Validation (EV). I certificati EV offrono il livello più alto di affidabilità, fornendo garanzie maggiori sull'organizzazione che gestisce il server web. Sono stati creati per affrontare il crescente numero di frodi online, in grado di erodere la sicurezza dei consumatori nelle transazioni sul web. [25]

Per richiedere il certificato è necessario produrre una Certificate Signing Request (CSR) ed inviarla alla CA che sarà quindi in grado di generare il certificato. Per generare la CSR è possibile seguire i seguenti passaggi:

1. Impostare la variabile d'ambiente OPENSSL\_CONF per poter usare i servizi offerti da OpenSSL;
2. Usando OpenSSL generare una chiave privata con il seguente comando:

```
openssl genrsa 1024 > C:\SSL\3dserver.key
```

3. Creare i certificati per ogni singolo servizio, per esempio per 3DPassport:

```
openssl req -config C:\Apache24\conf\openssl.cnf -passin  
pass:changeit -new -subj  
"/C=IN/ST=Maharashtra/L=Pune/O=IT/CN=3dpassport.mydomain.com"  
-key C:\SSL\3dserver.key -out C:\SSL\3dpassport.csr
```

Questo dev'essere fatto per tutti i servizi, in modo da generare un file .csr per ciascun servizio. Per essere accettato dai server della piattaforma 3DEXPERIENCE, il Common Name (CN) del certificato dev'essere uguale all'URL del server (per esempio: 3dpassport.mydomain.com) o a un dominio con la wildcard (per esempio: \*.mydomain.com). Una volta generate le CSR per ogni servizio è possibile contattare una CA valida per poter ottenere i certificati.

L'aspetto cruciale è che questi certificati vengono configurati all'interno del file httpd.conf del server Apache, che funge da reverse proxy e svolge un ruolo chiave nella gestione delle comunicazioni tra i vari servizi all'interno dell'ambiente on-premise. Grazie a questa configurazione, il server Apache è in grado di autenticare e cifrare le comunicazioni tra i vari servizi, garantendo un flusso di dati sicuro e protetto da potenziali minacce esterne.

La sicurezza dei certificati è di vitale importanza per garantire l'integrità e l'affidabilità delle connessioni HTTPS. Possono essere adottati diversi approcci per salvare in modo sicuro i certificati creati da una Certificate Authority (CA). Uno di questi approcci è l'utilizzo di Hardware Security Module (HSM): un HSM è un dispositivo crittografico dedicato, progettato per la gestione sicura delle chiavi crittografiche e delle operazioni di crittografia. Nella gestione dei certificati per HTTPS, un HSM può essere utilizzato, tra le altre cose, per la custodia sicura delle chiavi private: l'HSM fornisce un ambiente sicuro e isolato in cui le chiavi private associate ai certificati SSL/TLS possono essere immagazzinate. Ciò protegge le chiavi da accessi non autorizzati e previene potenziali falle di sicurezza.

In sintesi, HTTPS svolge un ruolo fondamentale nella protezione dei dati all'interno della soluzione on-premise della 3DEXPERIENCE. La sua implementazione attraverso certificati digitali e la configurazione accurata all'interno del server Apache consentono di garantire comunicazioni sicure tra i servizi, garantendo la privacy e l'integrità dei dati sensibili all'interno dell'ecosistema 3DEXPERIENCE.

La guida all'installazione fornita da Dassault definisce alcuni step fondamentali per la configurazione del protocollo HTTPS per tutti i servizi. Per prima cosa è necessario configurare correttamente il file di configurazione di ogni servizio come in [Figura 9.12](#).

```
SSLEngine on

SSLProxyEngine On

SSLCertificateFile "C:\SSL\3dpassport.crt"

SSLCertificateKeyFile "C:\SSL\3dserver.key"
```

Figura 9.12. Direttive del file di configurazione del servizio 3DPassport [19]

La direttiva SSLEngine è utilizzata per abilitare o disabilitare il supporto SSL/TLS per una specifica istanza di un host virtuale o per l'intero server Apache. Quando SSLEngine è impostato su "on", il server inizia a negoziare le connessioni SSL/TLS con i client che richiedono una connessione protetta.

La direttiva SSLProxyEngine è utilizzata per abilitare o disabilitare il supporto SSL/TLS per le connessioni di proxy. Quando SSLProxyEngine è impostato su "on", il server Apache inizierà a negoziare le connessioni SSL/TLS con i client e i server di destinazione quando agisce come proxy per una richiesta.

Le ultime due direttive invece indicano il percorso in cui sono salvati rispettivamente il file contenente il certificato del servizio e il file contenente la chiave privata associata al certificato del server. Tali certificati vanno come detto richiesti per ogni servizio, mentre la chiave privata del server è una unica.

Nel caso dell'installazione di test tali certificati sono stati creati come self-signed, dunque non sono stati rilasciati da una Certification Authority. Questa soluzione ovviamente non è valida, in quanto non garantisce sicurezza per la mancanza di verifica di terze parti: i certificati self-signed non vengono emessi da un'autorità di certificazione di fiducia riconosciuta a livello globale, pertanto, i visitatori del sito web o degli altri servizi protetti non possono verificare facilmente l'identità del server, aprendo la possibilità di attacchi di tipo "man-in-the-middle".














Name	Date modified	Type	Size
 3dcomment	7/14/2023 10:25	Security Certificate	
 3dcomment.csr	7/14/2023 10:02	CSR File	
 3dcomment.pem	7/14/2023 10:25	PEM File	
 3ddashboard	7/14/2023 10:30	Security Certificate	
 3ddashboard.csr	7/14/2023 09:54	CSR File	
 3ddashboard.pem	7/14/2023 10:29	PEM File	
 3dnotification	7/14/2023 10:31	Security Certificate	
 3dnotification.csr	7/14/2023 10:02	CSR File	
 3dnotification.pem	7/14/2023 10:30	PEM File	
 3dpassport	7/14/2023 10:31	Security Certificate	
 3dpassport.csr	7/14/2023 09:52	CSR File	
 3dpassport.pem	7/14/2023 10:31	PEM File	
 3dsearch	7/14/2023 10:33	Security Certificate	

Figura 9.13. Certificati self-signed generati per ogni servizio

Per questo motivo con la soluzione adottata nell'ambiente di test la risposta del browser quando si accede a uno dei servizi è quella di avvisare l'utente che la connessione con tale servizio non è sicura, come mostrato in [Figura 9.14](#).

### In Riferimento al NIST 800-53

Come per la disponibilità dei dati, anche per confidenzialità e integrità il NIST 800-53 [8] definisce alcune linee guida come per esempio nella sezione Protection of Confidentiality and Integrity using Encryption dove viene indicato:

*Implementare meccanismi crittografici per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto. Le Virtual Private Networks possono essere utilizzate per proteggere la riservatezza e l'integrità delle sessioni di accesso remoto. Transport Layer Security (TLS) è un esempio di protocollo crittografico che fornisce sicurezza delle comunicazioni end-to-end sulle reti e viene utilizzato per le comunicazioni Internet e le transazioni online.*



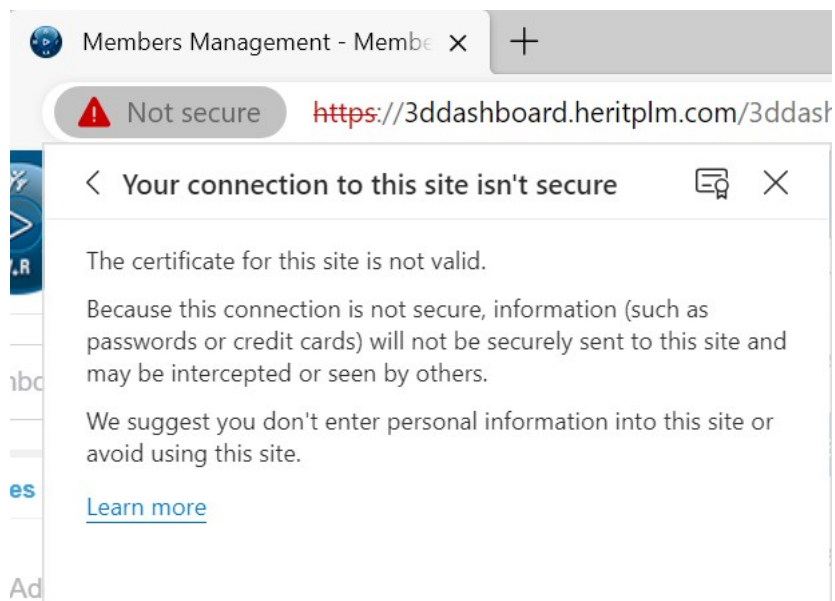


Figura 9.14. Messaggio del browser quando si utilizzano certificati self-signed

### Esempio Security Plan

In questo caso nella fase di Risk Assessment si andrebbero ad analizzare i potenziali rischi riguardanti l'integrità e la riservatezza dei dati in transito nella piattaforma e anche l'autenticità dei server dell'infrastruttura. In particolare nell'identificazione di potenziali possiamo dividerle come segue:

- Intercettazione dei dati: senza protezioni un utente malintenzionato potrebbe intercettare i dati scambiati all'interno dell'infrastruttura.
- Attacchi Man-In-The-Middle (MITM): questi attacchi si verificano quando un aggressore si inserisce tra il client e il server per intercettare e manipolare i dati scambiati.
- Spoofing: gli attaccanti potrebbero tentare di creare un sito web falso che sembri identico al sito della piattaforma, al fine di rubare informazioni sensibili dagli utenti.
- Sniffing: questi attacchi si verificano quando gli aggressori monitorano il traffico di rete per estrarre informazioni sensibili come nomi utente, password e altre informazioni personali.

Per questo tipo di minacce la soluzione scelta è sicuramente l'utilizzo del protocollo HTTPS per tutte le comunicazioni all'interno della piattaforma, sia le comunicazioni tra i diversi servizi, sia quelle con il reverse proxy. Per poter implementare tale soluzione è necessario, come già visto in precedenza, avere un certificato per ogni servizio e per il server Apache.

### 9.2.4 Autenticazione

L'autenticazione alla piattaforma 3DEXPERIENCE viene gestita dal servizio 3DPassport e avviene attraverso un sistema di gestione delle identità e degli accessi (Identity and Access Management,

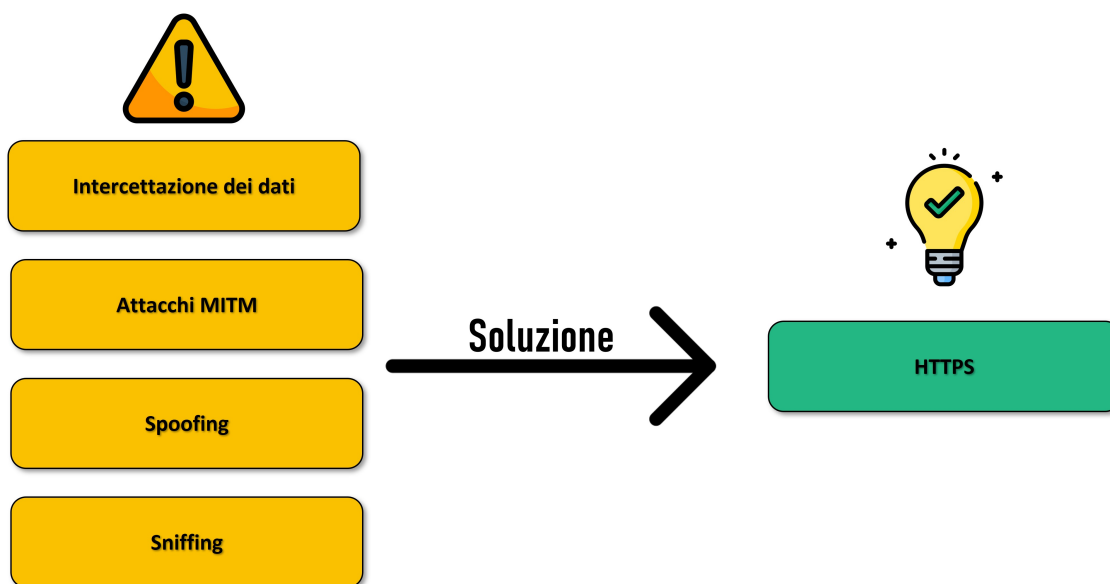


Figura 9.15. Schema di un Security Plan per minacce alla sicurezza dei dati

IAM) robusto e personalizzabile. La piattaforma offre diverse opzioni per l'autenticazione, consentendo agli utenti di accedere in modo sicuro ai servizi in base alle loro credenziali e ruoli designati. Alcuni dei metodi di autenticazione comunemente utilizzati sulla piattaforma 3DEXPERIENCE includono:

- **Autenticazione a più fattori (MFA):** La piattaforma supporta l'autenticazione a più fattori, che richiede ai utenti di fornire più prove della propria identità oltre alle semplici credenziali, come una password. Questo può includere l'uso di token di sicurezza, codici inviati tramite SMS o autenticazione biometrica.
- **SSO (Single Sign-On):** La piattaforma supporta anche la funzionalità di Single Sign-On, che consente agli utenti di accedere a più applicazioni e servizi con un'unica coppia di credenziali. Questo semplifica l'esperienza degli utenti e riduce la necessità di memorizzare e gestire diverse password per diverse applicazioni.
- **Politiche di Password Personalizzabili:** La piattaforma consente la definizione di politiche di password personalizzabili che possono imporre requisiti specifici per la complessità delle password, come lunghezza minima, caratteri speciali, e scadenze periodiche per la modifica delle password al fine di garantire la sicurezza degli account.

Nella configurazione di default, come si può notare in [Figura 9.16](#), la piattaforma 3DEXPERIENCE offre agli utenti la flessibilità di scegliere tra l'autenticazione a due fattori e l'autenticazione basata su singola password. L'opzione per l'autenticazione a due fattori, sebbene non obbligatoria, fornisce un livello aggiuntivo di sicurezza che va oltre la semplice autenticazione tramite credenziali di accesso. Quando gli utenti optano per l'autenticazione a due fattori, oltre all'inserimento della password, potrebbe essere richiesto loro di fornire una seconda forma di verifica dell'identità, come un codice generato da un'applicazione di autenticazione sul dispositivo mobile o un token di sicurezza inviato via SMS. Questa pratica riduce significativamente il rischio

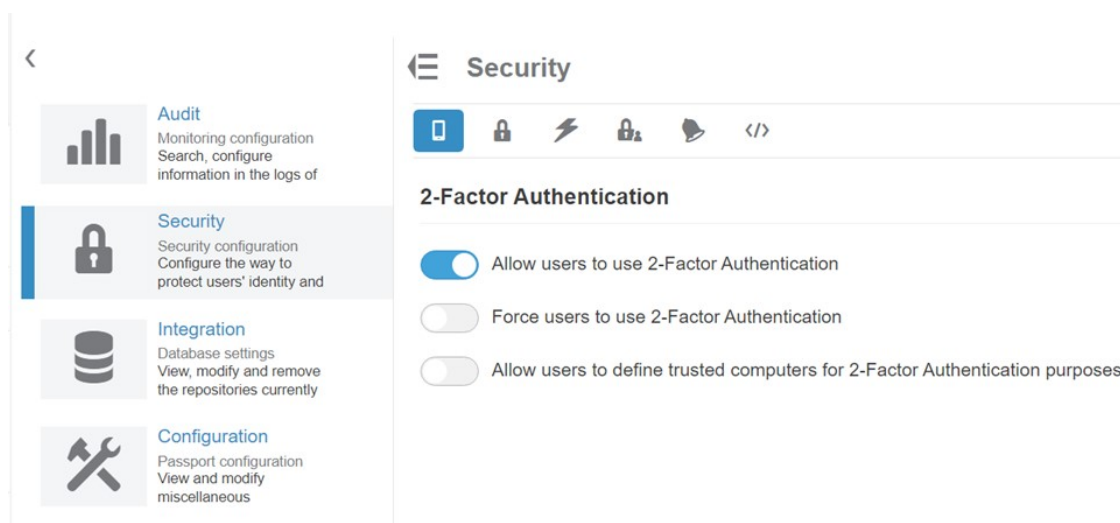


Figura 9.16. Possibilità di scelta del tipo di Autenticazione nella 3DEXPERIENCE

di accessi non autorizzati, poiché anche se le credenziali di accesso dovessero essere compromesse, un potenziale intruso avrebbe comunque bisogno di superare un secondo livello di autenticazione.

D'altro canto, nei casi in cui gli utenti scelgono di utilizzare esclusivamente l'autenticazione basata su singola password, il protocollo HTTPS, come discusso in precedenza, continua a garantire la crittografia dei dati durante la trasmissione, riducendo il rischio di attacchi di tipo Man-in-the-Middle (MITM) e proteggendo la confidenzialità delle informazioni scambiate tra il client e il server. Tuttavia, questa soluzione presenta alcune debolezze rispetto all'autenticazione a due fattori. Ad esempio:

- **Vulnerabilità alle violazioni delle credenziali:** Se le credenziali di accesso vengono compromesse o rubate, l'assenza di un secondo fattore di autenticazione potrebbe rendere più facile per gli aggressori accedere ai dati sensibili.
- **Rischi legati all'ingegneria sociale:** Le tecniche di ingegneria sociale potrebbero indurre gli utenti a divulgare le proprie credenziali, fornendo agli aggressori l'accesso senza la necessità di superare un secondo livello di autenticazione.
- **Accesso non autorizzato ai dispositivi smarriti o rubati:** In caso di smarrimento o furto di dispositivi contenenti le credenziali di accesso, l'autenticazione a due fattori fornirebbe un livello aggiuntivo di protezione impedendo l'accesso non autorizzato da parte di terzi.
- **Password deboli:** Nell'autenticazione basata solo su username e password, l'assenza di un secondo fattore di autenticazione rende le password vulnerabili a tentativi di accesso non autorizzati. Le password deboli o facili da indovinare rappresentano un rischio significativo, poiché gli aggressori potrebbero facilmente ottenere l'accesso ai dati sensibili sfruttando l'uso di password comuni, sequenze numeriche o informazioni personali facilmente reperibili online. In assenza di un secondo livello di autenticazione, il pericolo di accessi non autorizzati è amplificato.

Nell'autenticazione basata solo su username e password, l'assenza di un secondo fattore di autenticazione rende le password vulnerabili a tentativi di accesso non autorizzati. Le password

deboli o facili da indovinare rappresentano un rischio significativo, poiché gli aggressori potrebbero facilmente ottenere l'accesso ai dati sensibili sfruttando l'uso di password comuni, sequenze numeriche o informazioni personali facilmente reperibili online. In assenza di un secondo livello di autenticazione, il pericolo di accessi non autorizzati è amplificato, mettendo a repentaglio la riservatezza e l'integrità dei dati critici.

Tuttavia, per mitigare la vulnerabilità delle password deboli la piattaforma 3DEXPERIENCE ha implementato regole stringenti per la scelta delle password. Gli utenti sono tenuti a selezionare password che rispettino determinati requisiti di complessità, come si può notare in [Figura 9.17](#). Questa pratica aiuta a prevenire l'adozione di password deboli e facilmente indovinabili, riducendo così il rischio di accessi non autorizzati e garantendo un livello di protezione più elevato.

- ✔ Should not contain your username
- ✔ Should not contain your first name
- ✔ Should not contain your last name
- ✘ Must be at least 8-characters long
- ✘ Must contain at least 1 number(s)
- ✘ Must contain at least 1 letter(s)
- ✘ Must contain at least 1 lowercase character(s)
- ✘ Must contain at least 1 uppercase character(s)
- ✔ Cannot contain special characters other than the following: ! # = @ [ \ ] ^ \_ { | } \$ % & ( ) \* + -

Figura 9.17. Vincoli per la scelta della password nella piattaforma 3DEXPERIENCE

Tali regole nella versione on-premise sono personalizzabili a proprio piacere, come mostrato in [Figura 9.18](#) e successive. Ovviamente questa configurazione standard è quella consigliata e sotto tale soglia di controlli non si dovrebbe scendere in modo da non consentire password troppo deboli.

Oltre alle restrizioni della password è anche possibile, sempre per ragioni di sicurezza, impostare una durata per la password, oltre la quale è obbligatorio cambiarla ([Figura 9.21](#)). Questo è altamente consigliato, in quanto aumenta notevolmente la sicurezza per le password rendendo ancora più difficile riuscire a compromettere la password poiché la finestra di possibili attacchi si restringe.

## ☰ Security



### Password management

#### ▼ Password format policy

Allow password to contain username

Allow password to contain first name

Allow password to contain last name

#### Minimum length \*

Figura 9.18.

#### Minimum number of digits \*

#### Minimum number of characters \*

#### Minimum number of lowercase characters \*

Figura 9.19.

### Esempio Security Plan

Per quanto riguarda l'autenticazione l'analisi è senza dubbio più semplice, in quanto in un sistema informatico è ormai obbligatorio avere un sistema di autenticazione che, come abbiamo visto,

**Minimum number of uppercase characters \***

1

**Minimum number of special characters \***

0

**Special characters allowed \***

!#=@[\]^\_{}\$%&()\*+,-

Apply

Figura 9.20.

Enable Password renewal policy

**Age Limit (in days)**

Age Limit (in days)

**Minimum age (in days)**

Minimum age (in days)

**Remind user before (in days)**

Remind user before (in days)

Allow password reuse

**Password history length \***

5

Figura 9.21.

è presente anche nella piattaforma 3DEXPERIENCE. In questo caso non è dunque necessario analizzare i rischi e proporre una soluzione, in quanto essa è già presente all'interno di uno dei servizi fondamentali per la piattaforma, ma ciò che è doveroso analizzare è la tipologia di autenticazione che si vuole utilizzare tra quelle che la piattaforma mette a disposizione. Come

abbiamo visto infatti, il servizio 3DPassport mette a disposizione diversi tipi di autenticazione ed è opportuno scegliere quella più consona all'infrastruttura che si vuole mettere in piedi in una fase di analisi precedente all'installazione, come il Security Plan.

Tale scelta si basa principalmente sul livello di sicurezza richiesto, e dunque indirettamente anche sul valore dei dati che si intendono inserire all'interno della piattaforma. La scelta consigliata è ovviamente quella più sicura, ovvero l'implementazione dell'autenticazione a 2 fattori.

Anche per quanto riguarda l'autorizzazione, che verrà analizzata nel paragrafo seguente, le attività richieste all'interno del security plan riguardano solamente la scelta tra le opzioni già implementate nella piattaforma. Come verrà spiegato in seguito infatti, la 3DEXPERIENCE mette a disposizione un sistema di ruoli e privilegi che dovranno essere assegnati ai vari utenti nella fase preliminare di Security Plan, e potranno subire delle successive modifiche a seconda delle necessità.

### 9.2.5 Autorizzazione

Nella piattaforma 3DEXPERIENCE, la gestione delle autorizzazioni è un aspetto fondamentale per garantire che gli utenti e i servizi abbiano accesso solo alle risorse e alle funzionalità pertinenti alle proprie responsabilità e ruoli all'interno del sistema. Questa gestione è implementata attraverso un sistema di controllo degli accessi che si basa su diversi elementi chiave:

- **Modello di autorizzazione basato sui ruoli:** La piattaforma 3DEXPERIENCE utilizza un modello di autorizzazione basato sui ruoli, assegnando a ciascun utente specifici privilegi e permessi in base al suo ruolo all'interno dell'organizzazione. Ciò significa che gli utenti hanno accesso solo alle funzionalità e ai dati rilevanti per le loro responsabilità specifiche, garantendo che le informazioni sensibili siano accessibili solo a coloro che ne hanno il legittimo bisogno.
- **Controllo flessibile dei livelli di accesso:** Il sistema di gestione delle autorizzazioni consente un controllo flessibile sui livelli di accesso alle risorse, consentendo agli amministratori di definire e configurare i livelli di accesso in base ai requisiti specifici dell'organizzazione. Questo livello di flessibilità aiuta a garantire che la condivisione e l'accesso ai dati siano regolamentati in modo adeguato, mantenendo la sicurezza e la riservatezza delle informazioni sensibili
- **Controllo dei privilegi di accesso alle funzionalità:** Oltre al controllo degli accessi ai dati, il sistema di autorizzazione regola anche l'accesso alle diverse funzionalità e agli strumenti all'interno della piattaforma. Ciò assicura che gli utenti possano utilizzare solo le funzionalità per le quali sono autorizzati, riducendo il rischio di utilizzo improprio delle risorse e delle funzionalità critiche.
- **Audit e monitoraggio degli accessi:** La piattaforma 3DEXPERIENCE è in grado di registrare e monitorare gli accessi e le attività degli utenti, consentendo agli amministratori di condurre audit dettagliati per individuare eventuali anomalie o attività sospette. Questo livello di trasparenza aiuta a garantire la conformità alle normative e a individuare tempestivamente eventuali tentativi di accesso non autorizzati.

Più nello specifico nella piattaforma è presente un tab di Platform Management, accessibile solo da chi ha i privilegi di amministratore, in cui, tra le altre cose, è possibile gestire gli utenti presenti nella piattaforma. In [Figura 9.22](#) si può notare la gestione di privilegi e ruoli per ogni singolo utente. In questo caso l'utente ha i privilegi di amministratore e, nella sezione ruoli, è

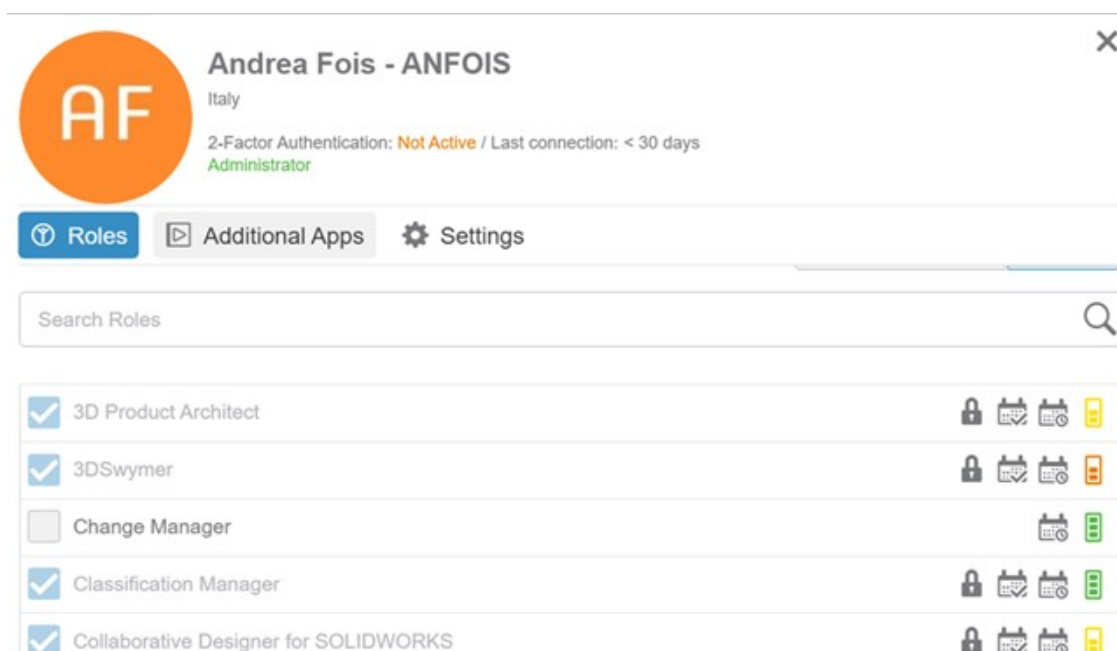


Figura 9.22. Esempio di gestione dei ruoli per un utente all'interno della piattaforma.

possibile notare una serie di ruoli all'interno della piattaforma che garantiscono accessi e privilegi ad alcune funzionalità specifiche.

Oltre alla gestione dei ruoli che garantiscono l'accesso a determinate applicazioni della piattaforma, è possibile gestire anche i privilegi all'interno dei singoli Collaborative Space. I Collaborative Space sono aree di lavoro separate, utilizzate per dividere i dati all'interno della piattaforma per gestire progetti diversi. In un'altra area del Platform Management è possibile impostare i privilegi degli utenti per ogni Collaborative Space come in [Figura 9.23](#). Questo permette di differenziare i privilegi di ciascun utente per ogni area di lavoro, in modo da applicare con efficienza i principi di Least Privilege e Need to Know.

### In Riferimento al NIST 800-53

Nel documento del NIST 800-53 [8] vengono nominate più volte le politiche di autorizzazione e per diversi controlli di sicurezza. Di seguito sono riportati i principali controlli in cui è fondamentale l'autorizzazione:

- **Account Management:**
  - *Concessione dell'accesso al sistema sulla base di: una valida autorizzazione all'accesso, utilizzo previsto del sistema e altri attributi richiesti dall'organizzazione o dalle funzioni aziendali associate.*
  - *Il sistema informativo gestisce dinamicamente i privilegi degli utenti e le relative autorizzazioni di accesso.*
- **Separation of duties:**










Vincenzo		★ Leader 🔑 & Owner
Daniele		★ Leader 🔑 & Owner
Marta		👁️ Reader
Andrea FOIS		★ Leader 🔑 & Owner
Roberto		★ Leader 🔑 & Owner
Davide		★ Leader 🔑 & Owner
Natale		🖋️ Author

Figura 9.23. Gestione dei privilegi degli utenti per i singoli Collaborative Space.

- *L'organizzazione attua la separazione dei compiti attraverso autorizzazioni di accesso assegnate al sistema informativo.*

- **Least privileges:**

- *L'organizzazione utilizza il concetto di privilegio minimo, consentendo solo gli accessi autorizzati agli utenti (e ai processi che agiscono per conto degli utenti) necessari per svolgere i compiti assegnati in conformità con le missioni organizzative e le funzioni aziendali.*

## 9.2.6 Audit e Monitoraggio

Nella piattaforma 3DEXPERIENCE, il processo di audit e monitoraggio viene gestito attraverso l'implementazione di strumenti e protocolli dedicati che consentono la registrazione dettagliata delle attività degli utenti e la supervisione costante delle operazioni all'interno dell'ambiente di lavoro. Questo approccio mira a garantire la conformità normativa, a individuare tempestivamente le attività sospette e a prevenire potenziali minacce per la sicurezza. Alcuni dei principali metodi utilizzati per la gestione di audit e monitoraggio includono:

- **Registrazione dettagliata delle attività degli utenti:** La piattaforma 3DEXPERIENCE registra in modo dettagliato tutte le attività degli utenti, inclusi gli accessi, le modifiche apportate ai dati, le azioni eseguite e le transazioni effettuate. Questa registrazione dettagliata consente agli amministratori di identificare le attività specifiche svolte dagli utenti e di individuare rapidamente eventuali violazioni o anomalie.
- **Monitoraggio in tempo reale delle operazioni di sistema:** La piattaforma dispone di strumenti di monitoraggio in tempo reale che consentono agli amministratori di supervisionare le operazioni di sistema e le prestazioni dell'infrastruttura. Questo monitoraggio costante aiuta a identificare eventuali problemi di prestazioni, errori di sistema o attività sospette che potrebbero richiedere un intervento immediato.
- **Sistema di allarme e notifica automatica:** La piattaforma è configurata per generare avvisi e notifiche automatiche in caso di attività sospette o comportamenti anomali rilevati all'interno del sistema. Questi avvisi consentono agli amministratori di rispondere prontamente a potenziali minacce e di adottare misure correttive tempestive per prevenire danni o compromissioni dei dati.
- **Archiviazione sicura dei registri di audit:** I registri di audit vengono archiviati in modo sicuro e protetti per garantire l'integrità e la non alterabilità delle informazioni registrate. Questo approccio assicura che i registri di audit siano disponibili per l'analisi e le verifiche di conformità, fornendo una traccia chiara e dettagliata di tutte le attività svolte dagli utenti e dal sistema.

Anche l'audit come l'autenticazione e altre proprietà di sicurezza è gestito dal servizio 3D Passport. Come mostrato in [Figura 9.24](#) tale servizio permette, tramite un'applicazione all'interno della piattaforma, di gestire varie impostazioni di audit: nel tab Log configuration impostare delle categorie di eventi che verranno registrati, che di default sono i seguenti:

- ADMINOPS
- USERAUDIT
- TASK
- FRAUD
- CONFIGURATION
- FUNCTIONAL
- EXCEPTION
- TECHNICAL
- MESSAGE
- CAS
- TRACABILITY
- SCHEDULER
- SERVICE

A questa lista, oltre a eliminare le categorie già presenti, è possibile aggiungerne delle altre che sono:

- PERFORMANCE
- SAML
- SOAP

Oltre alle categorie di eventi, per ciascuna di esse è possibile impostare il livello di informazioni da registrare, che sono:

- FATAL
- ERROR
- WARN
- IMPORTANT
- INFO
- DEBUG
- TRACE

⇒ Audit

⚙️ Logs configuration   🖨️ Logs   👤 User

### Logging configuration

Add new log category

PERFORMANCE ▼   [Add category](#)

	FATAL	ERROR	WARN	IMPORTANT	INFO	DEBUG	TRACE	
ADMINOPS	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	🗑️
USERAUDIT	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	🗑️
TASK	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	🗑️
FRAUD	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	🗑️
CONFIGURATION	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	🗑️









FUNCTIONAL	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
EXCEPTION	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
TECHNICAL	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
MESSAGE	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
CAS	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
TRACABILITY	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
SCHEDULER	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
SERVICE	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Figura 9.24.

### In Riferimento al NIST 800-53

Come fatto anche in precedenza di seguito verranno riportate le direttive del NIST [8] riguardanti i controlli di sicurezza relativi ad audit e monitoraggio.

- **Event Logging:**

- *Identificare i tipi di eventi che il sistema è in grado di registrare a supporto della funzione di audit.*
- *Fornire una motivazione per cui i tipi di eventi selezionati per la registrazione sono ritenuti adeguati a supportare le indagini a posteriori sugli incidenti*

I tipi di eventi che richiedono la registrazione sono quegli eventi significativi e rilevanti per la sicurezza dei sistemi e la privacy delle persone. La registrazione degli eventi supporta inoltre esigenze specifiche di monitoraggio e controllo. I tipi di eventi includono modifiche della password, accessi non riusciti o accessi non riusciti relativi ai sistemi, modifiche agli attributi di sicurezza o privacy, utilizzo di privilegi amministrativi, modifiche di azioni dati, parametri di query o utilizzo di credenziali esterne. Nel determinare l'insieme dei tipi di eventi che richiedono la registrazione, le organizzazioni considerano il monitoraggio e l'auditing appropriati per ciascuno dei controlli da implementare.

- **Content of audit records:**

- *Garantire che i record di audit contengano informazioni che stabiliscano quanto segue:*
  - \* Che tipo di evento si è verificato;
  - \* Quando si è verificato l'evento;
  - \* Dove è avvenuto l'evento;
  - \* Fonte dell'evento;
  - \* Esito dell'evento;
  - \* Identità di eventuali individui, soggetti o oggetti/entità associati all'evento.

- *Il contenuto dei record che potrebbe essere necessario per supportare la funzione di controllo include descrizioni di eventi, timestamp, indirizzi di origine e destinazione, identificatori di utenti o processi, indicazioni di successo o fallimento e nomi di file coinvolti.*

- **Audit record review, Analysis and Reporting:**

- *La revisione, l'analisi e il reporting dei record di audit riguardano la registrazione relativa alla sicurezza delle informazioni e alla privacy eseguita dalle organizzazioni, inclusa la registrazione risultante dal monitoraggio dell'utilizzo dell'account, dell'accesso remoto, della connettività wireless, della connessione del dispositivo mobile, delle impostazioni di configurazione, dell'inventario dei componenti di sistema, dell'uso di strumenti di manutenzione e comunicazioni alle interfacce di sistema. La frequenza, l'ambito e/o la profondità della revisione, dell'analisi e del reporting dei registri di audit possono essere adeguati per soddisfare le esigenze organizzative in base alle nuove informazioni ricevute.*

- **Protection of audit information:**

- *Proteggere le informazioni di audit e gli strumenti di registrazione di audit da accessi, modifiche ed eliminazioni non autorizzate. Avviso in caso di rilevamento di accesso non autorizzato, modifica o eliminazione delle informazioni di controllo. Soluzioni:*
  - \* Scrivere le tracce di audit su supporti write-once basati su hardware.
  - \* Archiviare i record di controllo in un repository che fa parte di un sistema o componente di sistema fisicamente diverso dal sistema o dal componente sottoposto a controllo. La memorizzazione delle registrazioni di audit su sistemi o componenti fisici separati preserva inoltre la riservatezza e l'integrità delle registrazioni di audit.
  - \* Implementare meccanismi crittografici per proteggere l'integrità delle informazioni di audit e degli strumenti di audit.
  - \* Autorizzare l'accesso alla gestione della funzionalità di registrazione di controllo solo a un determinato sottoinsieme di utenti o ruoli privilegiati definito dall'organizzazione.
  - \* Applicare la doppia autorizzazione per determinate azioni sulle registrazioni di audit (cancellazione, modifica, etc.).
  - \* Autorizzare l'accesso in sola lettura alle informazioni di controllo a un sottoinsieme di utenti o ruoli con privilegi definito dall'organizzazione.

## Capitolo 10

# Conclusioni

In conclusione, questa tesi ha offerto un'analisi approfondita delle complesse dinamiche che ruotano attorno al processo per ottenere le certificazioni di sicurezza informatica. Attraverso lo studio dei processi di certificazione e degli standard internazionali, è emerso chiaramente che la sicurezza informatica non è semplicemente una misura statica, ma piuttosto un processo dinamico che richiede un impegno continuo per adattarsi alle mutevoli minacce e alle normative sempre più stringenti. Facendo riferimento ad alcuni dei più famosi standard internazionali si è cercato di spiegare con maggiore chiarezza e dettaglio l'importanza e le difficoltà delle varie fasi del processo, cercando di porre maggiore enfasi sulla necessità di un approccio organizzato e su una pianificazione ben fatta.

L'approfondimento della piattaforma 3DEXPERIENCE ha fornito un'opportunità per esplorare le proprietà di sicurezza implementate in un ambiente on-premise. Nonostante le limitazioni nell'accesso al codice sorgente e ad altri materiali interni, l'installazione della piattaforma ha consentito un'analisi dettagliata delle sue funzionalità di sicurezza chiave, come l'integrità e confidenzialità dei dati, l'autenticazione e l'autorizzazione degli utenti, nonché la gestione degli audit e del monitoraggio. Tali analisi hanno portato ad individuare requisiti di sicurezza fondamentali e alcune delle possibili scelte implementative e di configurazione necessarie per garantire le proprietà di sicurezza citate in precedenza per la piattaforma.

Questo studio ha inoltre fatto emergere che la sicurezza informatica non può essere garantita da un singolo componente o da una singola misura. La necessità di adottare un approccio globale è diventata sempre più evidente, considerando la natura sempre più sofisticata e diversificata delle minacce informatiche. Ciò richiede un costante aggiornamento delle politiche di sicurezza, una formazione adeguata del personale e un'attenta valutazione dei rischi per mantenere un'alta protezione delle informazioni e la continuità operativa. Tuttavia, è importante sottolineare che la sicurezza informatica rimane un campo in continua evoluzione, con nuove sfide e opportunità che emergono costantemente. Pertanto, il proseguimento della ricerca e dello sviluppo nel campo della sicurezza informatica è fondamentale per affrontare le minacce emergenti e per garantire la protezione efficace dei dati e dei sistemi critici.

In definitiva, questa ricerca ha fornito un'ampia visione delle sfide e delle opportunità nel campo della sicurezza, offrendo spunti importanti per futuri sforzi di ricerca e per lo sviluppo di strategie avanzate per proteggere le infrastrutture informatiche e per affrontare le minacce sempre più sofisticate nel panorama tecnologico in rapida evoluzione.

# Bibliografia

- [1] Redazione-InSic, “Security Plan: che cos’è, a cosa serve e chi lo redige”, 2022, <https://www.insic.it/privacy-e-sicurezza/security-articoli/security-plan-che-cose-a-cosa-serve-e-chi-lo-redige/>
- [2] Redazione-InSic, “Il ciclo di Deming: cos’è e come funziona il PDCA per la sicurezza sul lavoro”, 2021, <https://www.insic.it/tutela-ambientale/plan-do-check-act-cose-il-ciclo-di-deming-e-come-funziona/>
- [3] “NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View”, 2011. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>
- [4] C. Solera, “Gestione degli asset, identificarli e valutarli per la compliance GDPR: la checklist.” <https://www.cybersecurity360.it/legal/privacy-dati-personali/gestione-degli-asset>
- [5] G. Prò, “Threat modeling, cos’è e quali metodologie usare per l’identificazione delle minacce”, 2020, <https://www.cybersecurity360.it/soluzioni-aziendali/threat-modeling-cose-e-quali-metodologie-usare-per-lidentificazione-delle-minacce/>
- [6] S. Bergamaschi, “Vulnerability Assessment: se sai dove ti trovi sai anche come migliorare.” <https://blog.t-consulting.it/vulnerability-assessment>
- [7] “Risk Treatment.” <https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment>
- [8] “NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations”, 2020. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
- [9] “NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations”, 2018. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>
- [10] R. Ross, M. Swanson, G. Stoneburner, S. Katzke, and A. Johnson, “NIST Guide for the Security Certification and Accreditation of Federal Information Systems”, NIST Special Publication 800-37, 2004
- [11] N. Sun, C.-T. Li, H. Chan, B. D. Le, M. Z. Islam, L. Y. Zhang, M. R. Islam, and W. Armstrong, “Defining Security Requirements With the Common Criteria: Applications, Adoptions, and Challenges”, IEEE Access, 2022
- [12] “ISO/IEC 27001.” [https://it.wikipedia.org/wiki/ISO/IEC\\_27001](https://it.wikipedia.org/wiki/ISO/IEC_27001)
- [13] “The ISO 27001 Certification Process: A Step-by-Step Guide.” <https://secureframe.com/hub/iso-27001/certification-process>
- [14] N. Sun, C.-T. Li, H. Chan, M. Z. Islam, M. R. Islam, and W. Armstrong, “How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond”, IEEE Access, 2022
- [15] S. J. Murdoch, M. Bond, and R. Anderson, “How Certification Systems Fail: Lessons from the Ware Report”, IEEE Xplore, 2012

- [16] “Trusted Computer System Evaluation Criteria.” <https://en.wikipedia.org/wiki/Trusted-Computer-System-Evaluation-Criteria>
- [17] U. S. government department of defense, “Department of defense trusted computer system evaluation criteria”, 1985
- [18] “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components”, 2022. <https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART3R1.pdf>
- [19] S. Masutage, J. Lesourd, N. Patil, and A. Desai, “3DEXPERIENCE R2023x, Windows/MSSQL DB on Premises Installation”, 2023
- [20] 3DEXPERIENCE-R2021x, “3DEXPERIENCE Widget Development Fundamentals”, 2021
- [21] “RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3”, 2018. <https://www.rfc-editor.org/rfc/rfc8446>
- [22] “RFC 6101: The Secure Sockets Layer (SSL) Protocol Version 3.0”, 2011. <https://www.rfc-editor.org/rfc/rfc6101>
- [23] “What is TLS (Transport Layer Security)?.” <https://www.cloudflare.com/de-de/learning/ssl/transport-layer-security-tls/>
- [24] Let’s Encrypt, <https://letsencrypt.org/>
- [25] D. G. Berbecaru and A. Lioy, “An Evaluation of X.509 Certificate Revocation and Related Privacy Issues in the Web PKI Ecosystem”, IEEE Access, 2023