UNIVERSITÀ DEGLI STUDI DI MILANO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Conduzione di un'analisi di requisiti, identificazione delle minacce e analisi dei rischi in un sistema di gestione delle cartelle mediche volto alla certificazione come MDR (Medical Devices Regulation, EU n. 2017/745)

Candidato: Giorgio Oppo

Matricola: 963768

Relatore: Prof. Ernesto Damiani

Correlatore: Prof. Paolo Ceravolo

Controrelatore: Prof. Valerio Bellandi

Indice

A mio nonno,

Al primo maestro che ho avuto, l'artigiano che con le sue mani ha plasmato il mio modo di vedere il mondo. La tua officina era il mio laboratorio, il tuo amore per la meccanica il mio primo incitamento a scoprire, a capire, a smontare e rimontare la realtà per vederne l'essenza.

A te, che non avresti compreso il linguaggio criptico dei codici e dei firewall, ma che mi hai insegnato che ogni problema ha una soluzione se si ha la pazienza di cercarla.

Non avrei potuto raggiungere questo traguardo senza il tuo esempio, senza la tua curiosità e la tua determinazione che mi hanno ispirato.

Certo che tu saresti stato fiero di me, come io lo sono sempre stato di te.

Questa tesi è dedicata a te, con tutto l'amore e il rispetto che un nipote può avere per il suo nonno.

Capitolo 1

Introduzione

Il presente documento prende in considerazione l'applicativo ArchiMed in uso presso l'Azienda Ospedaliera Universitaria Careggi e ne riassumere le normative e le best practice che insistono sui prodotti software che sono identificabili o che devono essere identificati come dispositivi medici (MD). L'analisi si è concentrata sull'applicativo software, evindenziando anche alcuni aspetti come file e configurazioni critiche che, tuttavia, esulano dal campo di applica di questa analisi ma sono da ritenersi componenti critiche per il software.
ArchiMed è una web application sviluppata principalmete in PHP dal dottor Bassam Dannaoui che consente la gestione completamente informatizzata dei reparti e ambulatori sia, per profili sanitari che per profili amministrativi.

Nel secondo capitolo sono state riassunte le normative più importanti e recenti a cui attenersi in termini di safety e secure.
In particolare il focus è stato posto sulle seguenti normative europee

- regolamento UE 2017/745 (MDR)
- Direttiva UE 2016/1148 (NIST)
- Regolamento UE 2016/679 (GDPR)

Il Regolamento UE 2017/745 (MDR) tratta l'aspetto più clinico dell'applicativo. Vedremo quindi quali sono gli aspetti essenziali che determinano se un software purché usato in ambito medico possa essere considerato come dispositivo medico (MD).
La Direttiva UE 2016/1148 (NIST) ha come scopo la determinazione delle linee guida che insistono sulla continuità dei servizi essenziali, nell'ottica del perimetro nazionale sulla

cybersicurezza italiana. Un MD usato all'interno di una struttura ospedaliera ricade pienamente sotto lo scopo e il campo di azione di questa normativa.
Il Regolamento UE 2016/679 (GDPR) ha come scopo la determinazione delle procedure atte alla protezione dei dati personali delle persone fisiche che potrebbero minare le libertà e l'incolumità delle stesse. In quest'ottica il MD in questione tratta moltissimi dati particolari, ovvero una categoria di dati sottoposta ad ancora maggior tutela rispetto ai dati personali in quanto possono minare maggiormente le libertà e l'incolumità delle degli interessati. [12]
Inoltre vi sono da considerare come obblighi di adempimento tutte le disposizione emesse dall'agenzia AGID in quanto software in uso ed sviluppato all'interno di una Pubblica Amministrazione.

Nel terzo capitolo sono descritti i principali requisiti del software, prendendo in considerazione lo stato dell'arte e le normative di riferimento.
E' stata altresì definita una lista di punti critici che rappresentano il contesto delle analisi dei successivi capitoli.

Nel quarto capitolo è presente il risultato di alcuni test automatizzati, principalmente tramite lo strumento Owasp Zap

Nel quinto capitolo in accordo con la governance aziendale, sono stati definiti i metodi di calcolo dei rischi e il rischio accettabile.

Nel sesto capitolo sono stati individuati quali siano i Thread Actor principali per questo software andando a indicare anche dei casi recenti su asset similari di altre organizzazioni. Questo è stato necessario al fine di effettuare un thread model

Nel settimo capitolo illustriamo alcune misure correttive e operazioni intraprese o da intraprendere per elevare il grado di sicurezza dell'applicazione. Tuttavia essendo operazioni critiche ed in corso di risoluzione non verranno descritte nella loro totalità.

Nell' nono capitolo descrivo una metodologia sul come effettuare una migrazione da un'applicazione web monolitica verso una struttura a microsevizi evidenziandone i pregi e i difetti e i possibili sviluppi futuri.

Nell'ultimo capitolo sono esplicitate alcune proposte e asset su cui si dovrebbe porre l'attenzione senza aver la pretesa di esaustività.

1.1 Inquadramento aziendale del SW ArchiMed

I sistemi sanitari e i processi assistenziali sono ormai diventati digitali con l'informatizzazione dei dati sanitari. La digitalizzazione offre immense opportunità di miglioramento dei processi di assistenza, didattica e ricerca. Tuttavia, i clinici spesso si dichiarano sopraffatti dalle correlate incombenze "amministrative".
Lo sviluppo del software ArchiMed si inserisce in questo contesto con lo scopo di intercettare queste necessità in linea con i principi della *value based medicine*. L'impatto positivo per un approccio basato sul valore è triplice come descritto nella pubblicazione [18]

- l'informatica sanitaria integrata può supportare il personale medico e di assistenza nel processo decisionale, nel lavoro di squadra e nella comunicazione, portando l'eccellenza clinica a nuovi livelli.
- l'informatica sanitaria aiuta a collegare i processi operativi: gli amministratori di sistema possono analizzare e ottimizzare quasi tutti gli aspetti operativi del sistema sanitario.
- nei modelli sanitari che hanno come prospettiva formule di pay for performance o di incentivazione del personale basata su questo razionale, l'informatica sanitaria può supportare la misurazione sistematica degli esiti, per dare evidenza e riconoscere adeguatamente le prestazioni più adeguate in termini di qualità, sicurezza e centralità del paziente.

In un panorama in cui l'informatica sanitaria è essenzialmente caratterizzata da applicativi elettronici prodotti da un piccolo numero di importanti software house, AOU Careggi ha avuto la possibilità di accompagnare e promuovere lo sviluppo di un software di cartella clinica elettronica di reparto (CCE). Esso è stato realizzato da un medico suo dipendente che, nel tempo, opportunamente sostenuto e supportato, si è dimostrato affidabile ed ergonomico, pertanto ideale per accompagnare l'evoluzione delle attività ospedaliere.
In un quadro generale di Sistema Informativo Ospedaliero sempre più complesso ed interconnesso, è interesse dell'Azienda accrescere la citata esperienza aumentando le funzioni del software. Allo scopo è necessaria la costituzione di una struttura, supportata da uno specifico Comitato Direttivo, in grado di potenziare le capacità di manutenzione e di sviluppo evolutivo di ArchiMed, affinché diventi l'unica piattaforma applicativa per il percorso di ricovero dell'Ospedale, completamente integrata con il resto degli applicativi.
ArchiMed possiede attualmente un'articolazione che ricomprende la maggior parte delle complessità sottese alle varie tipologie di assistenza di una AOU, da perfezionare e personalizzare

in alcuni ambiti altamente specialistici. La differenza rispetto ad altri SW è rappresentata da uno sviluppo effettuato nel tempo mantenendo un principio di usabilità ed ergonomia per l'utilizzatore finale a partire da chi lo ha concepito. Grazie alla visione fattuale da medico delle modalità operative ha permesso la rappresentazione delle categorie di fabbisogni, il loro senso ed il loro valore in termini di facilità di accesso alle informazioni secondo priorità di utilità clinica che altra figura tecnica avrebbero difficoltà a tradurre in programmazione.

Il SW ArchiMed viene concepito già negli anni '90 da un medico di una Unità Operativa dell'AOUC, a partire dalle istanze dei medici e infermieri, con le prime funzionalità di cartella clinica elettronica di ricovero, gestione dell'armadio farmaci (armadietto di reparto), dei posti letto, programmazione degli accessi e gestione della relativa documentazione sanitaria, automatizzazione del calcolo nelle scale di valutazione, dosaggio dei farmaci, trend di andamento clinico, con funzioni statistiche epidemiologiche e cliniche. Ai medici di altre Strutture chiamati a consulenza nel reparto è stato chiesto di registrare le consulenze in ArchiMed. Quest'ultimi ben presto, hanno apprezzano la praticità di utilizzo, la velocità e le potenzialità cliniche e gestionali dell'applicativo. Sempre più medici dell'Ospedale chiedono di poter utilizzare ArchiMed e con il Provv. del Direttore Generale AOUC 628 del 25 novembre 2009 ne viene approvato l'utilizzo sperimentale in alcune degenze.

A seguito di questa esperienza si constata l'esito positivo della sperimentazione in termini di qualità della documentazione sanitaria, tracciabilità degli atti clinici e di efficacia del SW.

Emerge inoltre l'utilità di ArchiMed a supporto di numerosi adeguamenti necessari al superamento delle valutazioni inerenti ai requisiti di accreditamento. Il Provv. DG n. 626 del 26 ottobre 2011 dispone pertanto di estendere la diffusione del software a tutte le strutture sanitarie della AOUC e di affidare la responsabilità del progetto al Dott. Dannaoui.

L'attività del Dr. Dannaoui in seno alla Direzione Sanitaria è proseguita oltre tale termine ed è tuttora attiva. ArchiMed è diventata la cartella clinica elettronica ufficiale di Careggi, con piena fruibilità e grande sviluppo.

Dal 2012 è pertanto iniziata la progressiva diffusione di ArchiMed in tutte le SOD e Aree di attività aziendali, previa formazione di tutti gli operatori sanitari e secondo un crono-programma condiviso con la Direzione.

Vista la progressiva rilevanza acquisita dal SW e considerati gli investimenti effettuati con risorse aziendali per lo sviluppo e l'innovazione, è stato deciso di proteggere il codice sorgente di ArchiMed, opportunamente documentato, depositandolo presso il Pubblico Registro per il Software della SIAE con data di decorrenza 22.04.2016 e con numero di registro D 009739.

In risposta alle crescenti richieste della Direzione, delle Strutture Centrali e dei sanitari, il

gestionale è stato arricchito di nuove funzioni e progressivamente integrato con gli altri software aziendali, a partire dalla possibilità di accogliere nella cartella clinica la restituzione elettronica dei referti dal LIS e dal RIS. La diffusione ha richiesto un importante cambiamento delle modalità operative nelle degenze aziendali e la formazione di oltre 4.000 operatori medici infermieri, OSS e amministrativi. Infine, nel novembre 2017 ha avuto luogo l'avvio dell'ultima area di attività del DAI Materno Infantile. L'utilizzo di ArchiMed in AOUC ha permesso di conseguire importanti obiettivi generali e di realizzare sviluppi verticali, con implementazione di ulteriori funzioni in vario modo correlate con le attività di degenza:

1. Tracciabilità — il SW traccia il momento e l'autore di ogni singolo atto clinico e assistenziale in regime di ricovero realizzando le azioni previste dalla vigente normativa relativa alla corretta compilazione della documentazione sanitaria ed alla normativa di accreditamento (completa tracciabilità elettronica delle attività con legame con l'operatore).

2. Digitalizzazione — è possibile disporre di gran parte della documentazione clinica senza ricorrere alla consultazione cartacea; la consultazione è possibile contemporaneamente da più operatori del reparto (medico che compila il diario clinico, infermiere che somministra la terapia, ecc.) e, dagli operatori abilitati, anche da remoto attraverso i servizi intranet e web.

3. Confronto con il pregresso — il SW permette di visionare agevolmente e immediatamente le annotazioni di tipo clinico ed assistenziale contenute nelle cartelle degli eventuali ricoveri precedenti senza i tempi e i costi della procedura di trasferimento dall'archivio centralizzato offrendo anche la possibilità di importazione dei dati di interesse (l'attività di archiviazione elettronica delle cartelle potrebbe essere sostitutiva dell'attuale procedura previo inserendo della firma digitale).

4. Visualizzazione fascicoli di più reparti nel corso del ricovero — si possono consultare immediatamente i fascicoli relativi ai reparti in cui il paziente è stato ed è assistito, nel caso di trasferimenti tra reparti e verso le diagnostiche/ servizi di interventistica durante lo stesso ricovero, senza alcun trasferimento di materiale cartaceo, abbattendo il rischio di smarrimento accesso improprio o scambio di documentazione nei percorsi del paziente al di fuori dell'area di ricovero. Nel marzo 2018, al riguardo, ArchiMed è stato avviato presso la Casa di Cura Villa Ulivella e Glicini per la gestione delle attività cliniche AOUC temporaneamente svolte presso quella sede.

5. Uniformare le modulistiche (informative, consensi, ecc.) e le schede di raccolta dati (VIRA, scale di valutazione, ecc.) superando le precedenti personalizzazioni al fine di utilizzare i modelli validati dalla Direzione Sanitaria, agevolandone l'adozione, l'aggiornamento e la revisione su scala aziendale, svincolate dai tempi dei processi tipografici di stampa.

6. ADT e Movimento — Nel maggio 2018 ArchiMed ha completamente sostituito il precedente sistema ADT incorporando in sé il motore informatico per la movimentazione dei pazienti in Careggi e la generazione dei relativi flussi informativi, offrendo così un entry point unico per i professionisti sanitari aumentando l'ergonomia e l'efficienza di processo. ArchiMed ha pertanto sostituito il precedente sistema di produzione e trasmissione del movimento cartaceo e incorporato interamente la complessa funzione di gestione della "spedalità stranieri" utilizzati dall'Ufficio Accettazione Amministrativa.

7. Cruscotto posti letto — ArchiMed permette di monitorare centralmente e perifericamente l'occupazione e la disponibilità istantanee di posti letto attraverso i layout di ogni singolo reparto e i cruscotti di bed anagement, in cui vengono riportati i dati istantanei e retroattivi del movimento (ammessi, trasferiti, dimessi), anche stratificati per provenienza (da PS, da altri reparti, dal territorio).

8. Braccialetto Identificativo — viene utilizzato e registrato per la procedura di richiesta emocomponenti e trasfusione, al fine di migliorare e semplificare la corretta identificazione dei pazienti ed il corretto matching tra paziente, prestazioni sanitarie erogategli e risultati diagnostici.

9. Banca dati elettronica — interrogabile per finalità cliniche, di ricerca, di budget e di monitoraggio dei processi sanitari e dei relativi indicatori di attività, da parte delle Strutture cliniche e delle Strutture centrali afferenti alla Direzione Sanitaria e Amministrativa.

10. Qualità della documentazione sanitaria — ArchiMed ha consentito di monitorare e migliorare la qualità della cartella clinica e della coerenza tra questa e la Scheda di Dimissione Ospedaliera in tutto l'ambito aziendale, agevolando la verifica sistematica rispetto alla verifica a campione. Il Nucleo Aziendale DRG si avvale del SW per le attività di verifica della correttezza e completezza della compilazione della SDO.

11. Flussi Ufficio Nascite — ArchiMed è utilizzato presso il DAI Materno Infantile anche per tutte le specifiche certificazioni correlate alla gravidanza. Vengono automaticamente generati i principali flussi di ostetricia e ginecologia (CAP, IVG e AS).

12. Legge Gelli, Ufficio Copia Documentazione Sanitaria — il SW consente di applicare e monitorare la L. 8 marzo 2017, n. 24 in ordine al diritto dell'utente di fruire della copia della documentazione entro i tempi previsti della suddetta legge ed al monitoraggio di alcuni ambiti di rischio specifici.

13. Sistema ridondante di continuità operativa — in aderenza alla completa revisione della procedura aziendale per emergenze informatiche, in caso di interruzione del server principale esistono 2 server di backup di cui uno equivalente al principale e che permette sia la lettura che la scrittura; l'altro invece è un sistema di sola lettura che, in caso di cedimento del database permette la consultazione della documentazione dei pazienti degenti. Per come è stato installato, in modo centralizzato su VM, il backup dei dati è garantito dell'architettura che lo ospita al TIX regionale.

14. Gestione trasporto malati — per la Centrale Trasporto Malati ArchiMed consente di prenotare e programmare i trasferimenti interni.

15. Servizio informazioni presso le portinerie degli edifici aziendali.

16. Ufficio libera professione Tra gli sviluppi più recenti si riportano i seguenti:

17. Diffusione nei comparti operatori — è iniziata nel 2019 ed è finalizzata sia per tracciare la movimentazione dei pazienti nei trasferimenti da e per la sala operatoria, sia a garantire nel comparto operatorio la continuità di gestione delle terapie somministrate, dei parametri rilevati e della documentazione sanitaria ulteriore al registro operatorio.

18. Informatizzazione del Progetto CaRED — ArchiMed ha reso possibile la realizzazione di un progetto di particolare interesse per una gestione integrata dei percorsi tra ospedale e territorio. Questo progetto, attivato in via sperimentale nel novembre 2015, permette ai medici MMG di essere avvisati al momento del ricovero e della dimissione di un loro assistito, accedere alle cartelle di ricovero e alle lettere di dimissione dei loro pazienti e di dialogare tramite chat con i medici AOUC. Nel 2018 è stato identificato un modo di installazione sicura su infrastruttura regionale, dal 2019 accessibile dall'esterno anche in mobilità e con livelli di sicurezza adeguati, che ha permesso di estendere l'idea originale e consolidare il modello di integrazione ospedale-territorio: attualmente la media mensile

di accesso dei MMG è di 1179 per un totale di 627 medici abilitati per la sola Area Vasta Centro.

Capitolo 2

Normative di riferimento

Vi sono una pletora di standard e normative di riferimento quando si tratta di un software medico che gestisce una così amplia moltitudine di dati e collegamenti con altri verticali.
Ho così cercato di definire quali a mio avviso siano le principali normative e da tenere in considerazione quando si vuole sviluppare un software MD.
Vi sono di fatti tre grossi regolamenti redatti a livello europeo che di seguito elencherò e descriverò. Partirò dal più recente MDR, entrato in vigore nel 2021.
Procedendo vi sarà la direttiva NIS entrata in vigore nel 2018 e che attualmente e in corso di revisione e superamento dalla direttiva NIS2.
L'ultima legislazione europea presa in questione sarà il regolamento GDPR entrato in vigore nel 2018.
Ho deciso di prendere in esame queste tre regolamentazioni europee in quanto vanno a formalizzare, prese nella loro totalità, la triade di sicurezza CIA (Confidenzialità, Integrità e Disponibilità), e descrivono quindi un elevato livello di complessità realizzativa.
In conclusione del presente capitolo cono illustrati alcuni dei provvedimenti emanati dall'AGID che vincolano le pubbliche amministrazioni.

2.1 MDR

Questo regolamento esplicita la volontà europea di elevare gli standard di sicurezza e affidabilità dei dispositivi medici sia essi apparati analogici, digitali embedded o distribuiti. Tale volontà viene espressa sia dai considerando, a partire dal primo:

> *È tuttavia necessario procedere a una revisione sostanziale di tali direttive allo scopo di stabilire un quadro normativo solido, trasparente, prevedibile e sostenibile per i dispositivi medici, che* ***garantisca un livello elevato di sicurezza*** *e di salute sostenendo nel contempo l'innovazione*

È evidente la necessità di una revisione significativa delle direttive attuali al fine di stabilire un quadro normativo solido, trasparente, prevedibile e sostenibile per i dispositivi medici. Tale quadro normativo deve garantire un elevato livello di sicurezza e salute, sostenendo nel contempo l'innovazione nel settore.

Questo tanto atteso Regolamento MDR porta con sé un maggiore controllo sulla documentazione tecnica. Affronta le preoccupazioni legate alla valutazione della sicurezza e delle prestazioni dei prodotti, imponendo rigorosi requisiti per la valutazione clinica e richiedendo un follow-up clinico dopo il lancio sul mercato. Inoltre, richiede una migliore tracciabilità dei dispositivi lungo l'intera catena di fornitura.

L'aspetto chiave introdotto dal MDR è il controllo più rigoroso sulla documentazione tecnica dei dispositivi medici. I fabbricanti devono fornire una documentazione completa e accurata, compresi i dati relativi alla progettazione, alle prestazioni, alla sicurezza e all'efficacia dei dispositivi. Questo maggiore controllo sulla documentazione contribuisce a garantire che i dispositivi medici rispettino gli standard di sicurezza e affidabilità richiesti.

Un'altra importante caratteristica del MDR è l'attenzione post-market sulla valutazione clinica dei dispositivi. I fabbricanti devono condurre un follow-up clinico per monitorare l'efficacia e la sicurezza dei loro prodotti dopo il loro rilascio sul mercato. Questo approccio mira a identificare tempestivamente eventuali problemi o effetti collaterali e a prendere le misure necessarie per mitigarli, garantendo così la sicurezza dei pazienti.

Infine, il MDR richiede una migliore tracciabilità dei dispositivi lungo l'intera catena di fornitura. I fabbricanti devono essere in grado di identificare e rintracciare i dispositivi medici in ogni fase del processo, dalla produzione alla distribuzione e all'uso finale. Questa tracciabilità aiuta a individuare eventuali dispositivi difettosi o non conformi e a intraprendere azioni correttive tempestive.

Complessivamente, il Regolamento MDR rappresenta un passo importante verso l'elevazione

degli standard di sicurezza e affidabilità dei dispositivi medici in Europa. I requisiti più rigorosi per la documentazione tecnica, la valutazione clinica post-market e la tracciabilità dei dispositivi contribuiranno a garantire che i pazienti abbiano accesso a dispositivi medici sicuri ed efficaci, promuovendo nel contempo l'innovazione nel settore.

2.2 NIS

La normativa NIS, si propone, in un'ottica di salvaguardia della cybersicurezza nazionale, di disporre l'attuazione di misure organizzative, pratiche e tecniche al fine di garantire la disponibilità dei servizi a seconda della loro caratterizzazione strategica. Vengono definite due differenti categorie:

- Gli OES, fornitori di servizi essenziali
- Gli FSD, Fornitori di servizi digitali

La normativa definisce gli OES sono enti pubblici o privati che forniscono

> **"servizi essenziali al mantenimento di attività sociali e/o economiche fondamentali, la cui fornitura o erogazione dipende dalla rete e dai sistemi informativi e sui quali un incidente avrebbe effetti negativi significativi"**

. La Direttiva considera essenziali i settori elencati di seguito:

- Energia (elettrica, petrolio, gas)
- Trasporti (aerei, ferroviari,marittimi/fluviali, stradali)
- Bancario (istituti di credito)
- Infrastrutture per il mercato finanziario (sedi di negoziazione e controparti centrali)
- **Sanità** (prestatori di assistenza sanitaria)
- Acqua (fornitori e distributori di acqua potabile)
- Infrastruttura digitale (operatori punti di interscambio Internet (IXP), fornitori di servizi (DNS), registri nomi di dominio di primo livello (TLD)
- Oltre a queste organizzazioni, alcuni operatori in determinati settori possono essere considerati fornitori di servizi essenziali, anche se non rispondono ai criteri proposti. Possono variare a seconda dello Stato membro

I FSD sono definiti come **"qualsiasi persona giuridica che fornisca un servizio digitale"**, definizione che include quanto specificato di seguito:

- Motori di ricerca: "servizi digitali che consentono agli utenti di effettuare, in linea di principio, ricerche su tutti i siti Web, o su siti Web in una lingua particolare sulla base di un'interrogazione sotto forma di parola chiave, frase o di altra immissione, e che fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto".

- Mercati on-line: “servizi digitali che consentono a utenti e/o commercianti (come definiti nella Direttiva UE 2013/11) di concludere on-line contratti di vendita o di servizio sia su un sito Web del mercato on-line o su un sito Web di un commerciante che utilizza servizi informatici forniti dal mercato on-line”.
- Servizi informatici su ‘cloud’: “servizi digitali che consentono l’accesso ad un insieme scalabile ed elastico di risorse informatiche condivisibili”.

Poiché questa normativa ha carattere e rilevanza sugli interessi strategici nazionali gli enti e gli apparati sottoposti a questa legislazione sono segretati e non è possibile definire, sapere o diffondere notizie in merito alla loro inclusione o meno. Ciò detto è plausibile supporre che un software di gestione di un grande ospedale possa ricadere sotto l’egida di questo regolamentazione.

2.3 GDPR

Il Regolamento Generale sulla Protezione dei Dati, come si evidenzia dal nome regola la protezione dei dati personali sia essi intesi in termini di riservatezza (proprietà più rilevante in questo contesto) ma anche in termini di integrità e disponibilità.
Questi aspetti infatti possono essere riscontrati fin dai considerando che per loro natura indicano la strada che si vuole intraprendere con le regolamentazioni.
Nel Considerando 49 del GDPR si citano le caratteristiche che il dato deve mantenere nel sistema di gestione e trattamento dello stesso.

> *Il titolare del trattamento deve assicurare che il dato sia autentico, integro, riservato e disponibile*

Inoltre l'articolo 5, par. 1, lett. f), ribadisce e enfatizza il concetto di sicurezza nelle accezioni di integrità e riservatezza. Vengono altresì citate le "misure organizzative" che tuttavia esulano dallo scopo del presente documento.

> *stabilisce che i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*

Il GDPR introduce anche il concetto di minimizzazione dei dati inteso sia in termini di mera memorizzazione che di visualizzazione espresso in termine di principio, ovvero come base fondante dello stesso regolamento. Capo II, art 5, lettera c

> *I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);*

questo implica l'utilizzo di **metodologie di gestione degli accessi a grana molto fine**.
I dati sanitari vengono altresì indicati come dati particolari e quindi suscettibili a maggior tutela in quanto possono porre in essere condotte estremamente lesive nei confronti delle libertà, della vita degli interessati. Questo principio viene sancito all'articolo 9, punto 1 **Trattamento di categorie particolari di dati personali**

> *..nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica,* ***dati relativi alla salute*** *o alla vita sessuale o all'orientamento sessuale della persona.*

2.4 AGID

L'agenzia per l'Italia digitale (AGID) è preposta alla realizzazione degli obiettivi dell'Agenda Digitale Italiana, in coerenza con gli indirizzi dettati dal Presidente del Consiglio dei ministri o dal Ministro delegato, e con l'Agenda digitale europea.
Tra i suoi svariati compiti risalta

> *emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea*

Negli anni infatti ha definito un notevole numero di guideline e regolamentazioni per le pubbliche amministrazioni. Di fatti dal 2015 ha emanato una regolamentazione stabilendo le misure minime di sicurezza che le pubbliche amministrazioni devono adottare in base al tasso di rischio [6].
Nel 2017 tali misure sono state ampliate aggiornate e ammodernate [7] e successivamente nel 2020 sono state redatte e integrate le linee guida per lo sviluppo, la manutenzione e la valutazione dei rischi cyber.
Si fa quindi riferimento ai seguenti documenti, coadiuvati da un tool di valutazione gratuito messo a disposizione per le pubbliche amministrazioni. Tuttavia quest'ultimo non è di pubblico dominio come le linee guida ma è disponibile solo a richiesta di parte.

- Linee Guida per l'adozione di un ciclo di sviluppo di software sicuro [2]
- Linee Guida per lo sviluppo sicuro di codice [5]
- Linee Guida per adeguare la sicurezza del software di base [3]
- Linee Guida per la modellazione delle minacce e individuazione delle azioni di mitigazione [4]

Capitolo 3

Definizione dei requisti

La raccolta dei requisiti software riveste un ruolo cruciale nello sviluppo e nell'evoluzione di un sistema esistente. Tuttavia, quando ci si trova di fronte a un sistema complesso con un elevato grado di personalizzazioni e una documentazione incompleta, è necessario adottare un approccio appropriato per garantire la corretta identificazione e comprensione dei requisiti. In questo articolo di ricerca, presenteremo le linee guida per la raccolta dei requisiti software utilizzando un approccio gray-layer su un sistema già esistente.

L'approccio gray-layer è un metodo flessibile e pragmatico per affrontare la raccolta dei requisiti su un sistema senza una documentazione completa, ma con accesso al codice sorgente. Questo approccio si basa sulla combinazione di analisi statica e dinamica del sistema, consentendo di esplorare le diverse componenti e funzionalità attraverso l'osservazione diretta del codice.

Nei seguenti paragrafi definisco quali siano i requisiti richiesti da contesti esterni all'organizzazione aziendale, valutando principalmente i requisiti imposti dalle normative che insistono su questo tipo di applicativi.

Inoltre è importante specificare i requisti funzionali e non che l'organizzazione intende implementare all'interno del software. Quest'ultimo processo porta con se numerosi passaggi e documenti che devono essere gestiti correttamente, a tal fine ho descritto i vari passaggi di gestione all'interno di alcuni documenti aziendali di procedure di sviluppo software compliant agli standard di qualità 9001.

3.1 Requisiti MDR

In accordo con il Dott. Dannaoui e con l'Ing. Frosini sotto indicazione del Professor Iadanza si è deciso di utilizzare il percorso di certificazione previsto per le sole istituzioni sanitarie all'Articolo 5(5) del MDR [9]. Questa scelta è stata effettuata poiché sotto determinate condizioni ben specificate e previste dal legislatore di usufruire di un percorso certificativo più snello e agevolato.
Le condizioni sono le seguenti:

1. Il dispositivo deve essere fabbricato e utilizzato esclusivamente in istituzioni sanitarie stabilite nell'Unione Europea.

2. Il dispositivo non sia trasferito a un'altra persona giuridica;

3. la fabbricazione e l'utilizzo dei dispositivi avvengano secondo sistemi adeguati di gestione della qualità;

4. l'istituzione sanitaria giustifichi nella sua documentazione il fatto che le esigenze specifiche del gruppo di pazienti destinatario non possono essere soddisfatte o non possono essere soddisfatte con risultati del livello adeguato da un dispositivo equivalente disponibile sul mercato

    - l'istituzione sanitaria fornisca su richiesta alla propria autorità competente informazioni in merito all'uso di tali dispositivi che comprendano una giustificazione della loro fabbricazione, modifica e utilizzo;
    - l'istituzione sanitaria rediga una dichiarazione che mette a disposizione del pubblico:
        - il nome e l'indirizzo dell'istituzione sanitaria in cui i dispositivi sono fabbricati;
        - le informazioni necessarie per identificare i dispositivi;
        - una dichiarazione che i dispositivi soddisfano **i requisiti generali di sicurezza e prestazione di cui all'allegato I** del presente regolamento e, se del caso, **informazioni sui requisiti che non sono pienamente soddisfatti, con la relativa giustificazione motivata**;
    - l'istituzione sanitaria compili una documentazione che consenta di conoscere il sito di fabbricazione, il processo di fabbricazione, i dati di progettazione e di prestazione dei dispositivi, compresa la destinazione d'uso, in maniera sufficientemente dettagliata affinché l'autorità competente possa accertare il rispetto dei requisiti generali di sicurezza e prestazione di cui all'allegato I del presente regolamento;

- l'istituzione sanitaria adotti tutte le misure necessarie per garantire che tutti i dispositivi siano fabbricati in conformità della documentazione di cui alla lettera f); e
- l'istituzione sanitaria valuti l'esperienza acquisita mediante l'utilizzazione clinica dei dispositivi e adotti tutte le azioni correttive necessarie.

Al fine di questo documento prenderemo in considerazione il punto 3 e il rispetto dei requisiti generali di sicurezza e prestazione di cui all'allegato I come definiti nel punto 4.2, in quanto elementi caratterizzanti dei requisiti del software ArchiMed.

3.1.1 Sistemi adeguati di gestione della qualità

Per ottemperare al requisito descritto al punto 3 dell'articolo 5 dell' MDR è stato deciso di procedere con la certificazione della AUO IPS diretta dal DR. Dannoui per quanto riguarda i processi di sviluppo e manutenzione software secondo lo standard ISO 9001. Tale certificazione essendo lo standard internazionalmente riconosciuto di Quality Management può ed dovrebbe essere considerato come "sistema adeguato di gestione della qualità".
A tal fine, è iniziato un percorso di collaborazione tra l'UO IPS e l'UO ACCREDITAMENTO, QUALITÀ E RISK MANAGEMENT. Grazie a questa sinergia è stato possibile procedere in maniera assai veloce ed efficente a portare a termine il percorso di certificazione [14].
É stato quindi necessario produrre le seguenti tre procedure che ritrovano le loro fondamenta sia nelle [2] che negli standard sul ciclo di vita del software che nella ISO 31000 sul Risk Management.

1. Sviluppo Software
2. Risoluzione dei problemi Software
3. Configurazione

3.1.2 Requisiti generali di sicurezza e prestazione allegato I

Dei Nove macro-punti dettati dalla normativa sono stati individuati due punti come requisiti riscontrabili e/o che debbano essere indicati nella procedura di sviluppo del software ovvero i punti:
3) **I fabbricanti stabiliscono, implementano, documentano e mantengono un sistema di gestione del rischio**. La gestione del rischio è intesa come un **processo iterativo** continuo durante l'intero ciclo di vita di un dispositivo che richiede un costante e

sistematico aggiornamento. Nella gestione del rischio i fabbricanti devono:

a) stabilire e documentare un **piano di gestione del rischio** per ciascun dispositivo;

b) **individuare e analizzare i pericoli noti e prevedibili** associati a ciascun dispositivo;

c) **stimare e valutare i rischi associati** e che si verificano durante l'uso previsto e durante l'uso scorretto ragionevolmente prevedibile;

d) **eliminare o controllare i rischi** di cui alla lettera c) conformemente ai requisiti del punto 4;

e) valutare l'impatto delle informazioni provenienti dalla fase di produzione e, in particolare, dal **sistema di sorveglianza post-commercializzazione, relative ai pericoli e alla loro frequenza**, alle stime dei relativi rischi, nonché al rischio complessivo, al rapporto benefici-rischi e all'accettabilità del rischio;

f) in base alla valutazione dell'impatto delle informazioni di cui alla lettera e), **se necessario modificare le misure di controllo** in linea con i requisiti di cui al punto 4.

4)Le misure di controllo del rischio adottate dai fabbricanti per la progettazione e la fabbricazione dei dispositivi si attengono a **principi di rispetto della sicurezza, tenendo conto dello stato dell'arte generalmente riconosciuto**. Per ridurre i rischi i fabbricanti li gestiscono in modo che il rischio residuo associato a ciascun pericolo, così come il rischio residuo globale, sia considerato accettabile. Nello scegliere le soluzioni più appropriate, i fabbricanti, in ordine di priorità:

a) **eliminano o riducono i rischi per quanto possibile attraverso la sicurezza nella progettazione e nella fabbricazione**;

b) se del caso, adottano le opportune misure di protezione, compresi i segnali di allarme se necessario, in relazione ai rischi che non possono essere eliminati; e

c) forniscono informazioni di sicurezza (avvertenze/precauzioni/controindicazioni) e, se del caso, una formazione agli utilizzatori. **I fabbricanti informano gli utilizzatori circa i rischi residui**

Da questi requisiti legislativi si sancisce quindi che il modello di sviluppo software da attuare deve essere un modello di sviluppo a rilascio incrementale. Questo sia per andare ad attuare i requisiti su citati ma anche per poter far ricadere il software sotto all'Articolo 5(5) del MDR in quanto un modello di sviluppo che non prevede un'evoluzione intrinseca non permetterebbe di asserire con facilità che le successive versioni del software siano lo stesso software delle versioni precedenti ed non un software di nuova ideazione/implementazione.

3.2 Requisiti GDPR

I requisiti tecnici imposti dal GDPR si concentrano sulle proprietà di visibilità che il software deve adottare al fine di minimizzare, proteggere e comportando una minimizzazione dei rischi connessi alla knowledge delle informazioni critiche dei pazienti (ricadono sotto la definizione di informazioni critiche poiché le informazioni sanitarie vengono identificate come sottogruppo di dati personali che meritano maggior tutela).
Al fine di attuare un risk assesment di tali informazioni è bene utilizzare risk level tool messo a disposizione dalla European Union Agency for Cybersecurity[11].
Ai fini di questo documento saranno considerati i soli requisiti di tipo tecnico applicabili al software e/o alla configurazione del server. Dato che l'applicativo ArchiMed viene inquadrato con un fattore di rischio critico per gli interessi e le liberà delle persone (GDPR), secondo la metrica su citata,verranno quindi considerati e valutati tutti i seguenti criteri (anche quelli più restrittivi):

- Access control policy: ovvero i requisiti C1,C2,C3,C4
- Access control and authentication: ovvero i requisiti K1,K2,K3,K4,K5,K6,K7,K8
- Logging and monitoring: ovvero i requisiti L1,L2,L3,L4,L5
- Server/Database security: M1,M2,M3,M4,M5,M6
- Workstation security: N1,N2,N3,N4,N5,N6,N7,N8,N9
- Network/Communication security: O1,O2,O3,O4,O5,O6,O7
- Back-ups: P1,P2,P3,P4,P5,P6,P7,P8,P9
- Application lifecycle security: R1,R2,R3,R4,R5,R6,R7,R8,R9

3.3 Requisiti NIS

Per quanto attiene a questo documento ci atterremo agli obblighi che devo essere attuati dagli OES in quanto considero che il software ArchiMed ricada al disotto di questa categoria poiché è il software gestionale in uso all'interno della più grande azienda sanitaria della Toscana. In particolare l'Articolo 14 della Direttiva stabilisce che gli OES devono:

- "adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni.". Tali misure dovrebbero "assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente",
- "adottare misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi"
- "notificare senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati.".

Se ne desume che i requisiti che il software deve avere siano

- utilizzo di un sistema di sviluppo software che intrinsecamente includa un sistema di monitoraggio e revisione del rischio.
- definire e determinare elevati livelli di Aviability.
- pianificare e tenere aggiornato un piano di incident response, contenete le modalità di comunicazione con l'autorità competente o il CSIRT

Al fine di formalizzare al meglio tali requisiti è bene partire dal prendere in considerazione lo standard ISO 27000. In questo caso esiste un' apposita eccezione ovvero [13] che definisce al meglio gli apporti di sicurezza da dover implementare.
Un'attenzione particolare è stata posta sui seguenti punti in quanto più tecnici/implementativi, tralasciando i punti organizzativi che, pur essendo necessari, esulano dallo scopo di questo documento.

- 9 Access control
- 10 Cryptography
- 12 Operations security

- 13 Communications security.
- 14 System acquisition, development and maintenance
- 16 Information security incident management
- 17 Information security aspects of business continuity management

3.4 Framework Nazionale per la Cybersecurity e la Data Protection

Un altro importante tool di valutazione controllo e indirizzamento dei lavori da intraprendere e tenere in considerazione è [8] realizzato dal CINI e dal Centro di Ricerca di Cyber Intelligence and Information Security dell' Università la Sapienza di Roma.

Questo tool è stato realizzato secondo le indicazioni dal NIST americano in merito ai framework di valutazione cyber, e pur non essendo uno strumento di stima della compliant come gli stessi autori dichiarano, è un ottimo punto di partenza molto utile nella gestione delle difformità e nella valutazione dello stato di salute del sistema.

Tramite questo lungo e piuttosto esaustivo metodo di valutazione della maturità della sicurezza informatica all'interno dell'azienda, inoltre aiuta a guidare l'organizzazione verso i passaggi più appropriati da intraprendere.

La valutazione dei processi di trasformazione dell'organizzazione viene accelerata poichè è possibile definire un piano programmatico stimando i costi e i benefici che questa comporti, tuttavia un aspetto che non si riesce a evincere facilmente da questo documento è il fattore umano. Specificatamente mi riferisco alla valutazione delle competenze, assegnazione dei ruoli e il numero di persone necessarie per soddisfare questo framework.

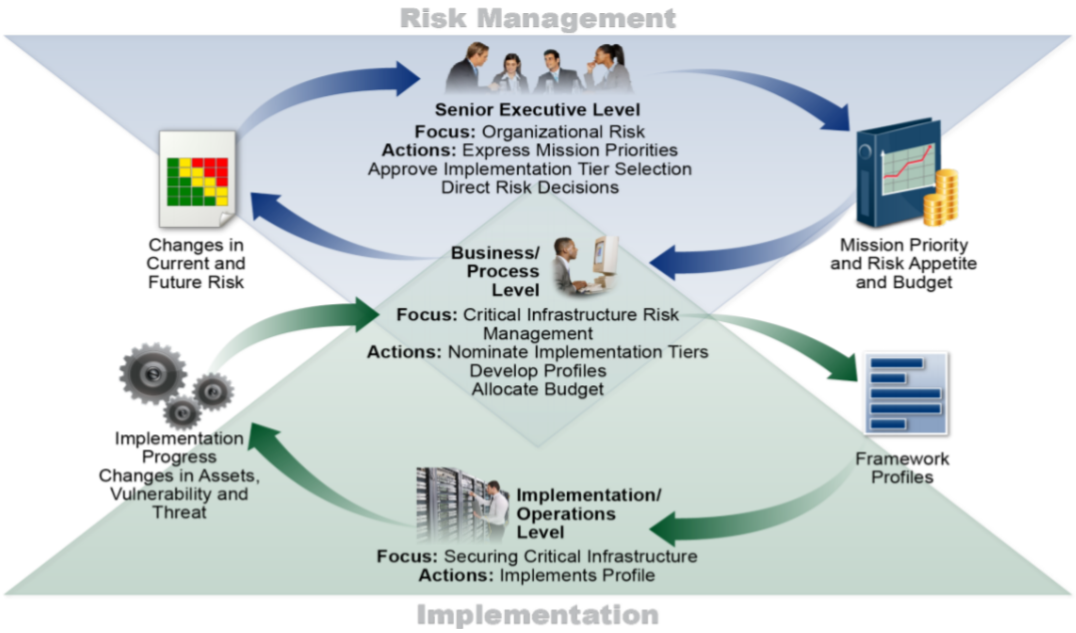


Figura 3.1: Framework Nazionale per la Cybersecurity e la Data Protection come si integra in azienda e perché migliora i processi

3.5 Totalità dei requisiti

Otteniamo quindi un sunto delle macropolitiche da implementare

- 1 Access control policy: ovvero i requisiti C1,C2,C3,C4
- 2 Access control and authentication: ovvero i requisiti K1,K2,K3,K4,K5,K6,K7,K8
- 3 Logging and monitoring: ovvero i requisiti L1,L2,L3,L4,L5
- 4 Server/Database security: M1,M2,M3,M4,M5,M6
- 5 Workstation security: N1,N2,N3,N4,N5,N6,N7,N8,N9
- 6 Network/Communication security: O1,O2,O3,O4,O5,O6,O7
- 7 Back-ups: P1,P2,P3,P4,P5,P6,P7,P8,P9
- 8 Application lifecycle security: R1,R2,R3,R4,R5,R6,R7,R8,R9
- 9 Access control
- 10 Cryptography
- 12 Operations security
- 13 Communications security.
- 14 System acquisition, development and maintenance
- 16 Information security incident management
- 17 Information security aspects of business continuity management

3.5.1 Access Control

Di seguito verranno riportate le considerazione in merito ai punti 1, 2, 3, 4, 6 del paragrafo precedente in quanto valutazione delle politiche da implementare. Mentre il resto dei punti ritrova il fondamento nelle procedure di sviluppo software adottate e descritte nei documenti aziendali di Procedure di sviluppo software [17].

3.5.2 Access Control: ArchiMed

Il sistema di gestione degli accessi si basa su un cookie di sessione, che viene generato dal server a seguito dell'inserimento delle credenziali corrette.
Il controllo degli accessi viene effettuato in maniera microscopica, di fatti per ogni utente vi è associato sia un identificativo per l'utente, un identificativo di classe e due identificativi di gruppo. Il primo permette di associare al singolo utente alcuni permessi non comuni e che non appartengono ai vari gruppi. I gruppi sono distinti per Area e Sod che identificano rispettivamente il luogo fisico dove l'operatore opera e la struttura gerarchica di competenza. L'identificativo di classe definisce la mansione svolta dall'utente e i relativi permessi concessi come le classi medico, infermiere e OSS, che per loro natura devono avere privilegi differenti (solo il medico può prescrivere farmaci). I permessi definiti delle Area e delle Sod sono cumulative questo per permettere al meglio di operare ed interagire con il programma.
Vi è anche la distinzione tra utente di base e amministratori, i cui privilegi sono gerarchici, di fatti un amministratore imposta i privilegi ai suoi sottoposto potendo scegliere esclusivamente da un sottogruppo delle sue autorizzazioni.
Le autorizzazioni sono statiche e vengono generalmente definite in fase di creazione dell'utente. Tuttavia è ogni amministratore di Area/SOD può modificare all'occorrenza le autorizzazione dei sui sottoposti in maniera manuale.
E' altresì possibile definire degli Operatori temporanei per permettere una flessibilità organizzativa, questo può essere fatto gerarchicamente degli operatori amministratori di Area/Sod.
Le caratteristiche che devono essere garantite nella creazione e gestione delle cookie di sessione sono:

- essere trasmesse in maniera sicura, per farlo è necessario che
  - siano utilizzabili solo in https con una catena di certificati fidati, **è necessario attivare il flag Secure**
  - sia accessibile solo al server e non possa essere letto da javascript e similari impostato il parametro **è necessario attivare il httponly**
- difficile da ricreare, per farlo è necessario che debba essere:
  - una stringa sufficientemente lunga
  - generata in maniera casuale o con parametri non noti (es partendo da una password)

- con una scadenza programmata per farlo è necessario impostarne la scadenza, per maggior sicurezza è bene che questa non sia solo impostata tramite il parametro Expires ma che la stessa sia indicata lato server

La trasmissione delle credenziali invece deve essere costruita in modo da rispondere ai seguenti requisiti:

- la trasmissione avviene in maniera sicura:
  - utilizzabile solo in http s con una catena di certificati fidati. La pagina deve essere accessibile solamente in https
  - utilizzando un meccanismo di hashing SHA256 o superiore coadiuvato da un nonce
- difficile da ricreare
  - imponendo che la password debba essere di 14 caratteri o superiore
- con una scadenza programmata

Queste condizione non venivano implementate in toto poiché la connessione in https avveniva solamente se la connessione era da una rete esterna. Misure di correzione 1.
L'invio della password pur risultando sicura se trasmessa in maniera cifrata tramite https, è bene che venga introdotta in un ulteriore layer di sicurezza cifrandola a livello applicativo con le opportune occorrenze del caso (utilizzo di metodi al fine di impedire un replay attack e tecniche similari) Misure di correzione 2

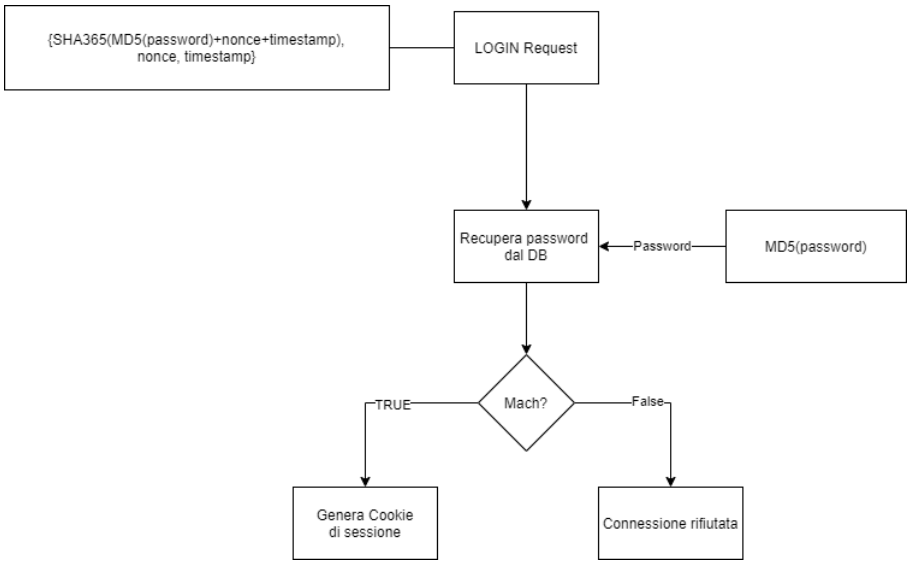


Figura 3.2: diagramma di flusso della fase di login tramite password

La politica di cambio password risulta correttamente implementata ed impone un aggiornamento della stessa entro tre mesi garantendo una sufficiente freshness.
Inoltre sarebbe opportuno separare la sessione dell'utente con le differenti pagine aperte consentendo di separare le autorizzazioni dell'utente con le autorizzazioni del processo. Misure di correzione 3.
Questo è estremamente importante al fine di garantire un controllo degli accessi più fine, **perché un utente che è nella pagina home può inserire un nuovo utente senza passare dalla pagina di inserimento dell'utente**. La mancata applicazione di questo correttivo porta alla violazione del concetto di minimo privilegio.

3.5.3 Access Control: Database

L'accesso al database è limitato tramite:

1. la creazione delle query ad hoc da parte dell'applicativo
2. l'accesso al DB per il solo localhost

Il primo punto di per se non è sufficiente in quanto il controllo di correttezza delle query dovrebbe essere fatto il più vicino possibile alla struttura dati, meglio ancora se tramite procedure nel DB, al fine di impedire che un malintenzionato possa andare ad interpellare direttamente il database scavalcando totalmente il controllo.
Il secondo punto necessita di una particolare attenzione dato che come per il software principale la politica di gestione delle password è da tenere in considerazione. La gestione del database quindi deve rispettare le seguenti regole minime di sicurezza

- essere trasmesse in maniera sicura:
  - utilizzabile solo in https con una catena di certificati fidati e la pagina è accessibile solamente in https
  - utilizzando un meccanismo di hashing SHA256 o superiore coadiuvato da un nonce
- difficile da ricreare
  - imponendo che la password debba essere di 14 caratteri o superiore
- con una scadenza programmata

Ciò detto saltano all'occhio le seguenti violazioni:

- la password di accesso al database non presenta una politica di freshness non venendo cambiata spesso.
- la trasmissione della stessa non avviene in maniera sicura in quanto la chiamata viene eseguita sull'indirizzo IP e quindi il certificato non può essere validato. Inoltre non vi è la presenza di un hash con un nonce e/o timestamp, permettendo così la replica e la decodifica della stessa. Segnalo tuttavia che essendo traffico locale solo una compromissione della macchina potrebbe analizzare o re-instradare il traffico.

Il suggerimento è di adottare dei controlli più stringenti implementati direttamente sul database per quanto riguarda gli accessi da parte degli utenti autorizzati, in modo da evitare rischi derivanti da errori del codice di ArchiMed o da accessi effettuati direttamente al DB.

3.6 Gestione dei profili

I profili sono mappati staticamente e implementati tramite una logica mandatoria basata sui ruoli (RuBAC).

L'amministratore di sistema ha stabilito vari ruoli, ciascuno con i propri permessi specifici. Questi ruoli vengono assegnati gerarchicamente attraverso una politica che concede autorizzazioni in modo ricorsivo ai capi dei reparti o delle sezioni, i quali fungono da sotto-amministratori, e successivamente distribuiti agli utenti.

Ogni utente può autorizzare un un altro utente solo per i criteri di cui lui stesso dispone. Questo meccanismo permette di fare partecipe gli owner di reparto al processo di autenticazione, condividendo oneri e responsabilità.

Il sistema prevede quindi un ottimale livello di gestione dei privilegi incarnando il principio di Privilegio Minimo, tuttavia si evidenzia come il sistema non abbia una distinzione tra autorizzazione dell'utente e autorizzazioni del processo andando quindi a vanificare in parte gli sforzi per soddisfare il principio del minimo privilegio. Ogni utente viene identificato tramite il suo codice fiscale a cui poi vengono associati un username e password.

Nei capitoli successivi nel punto definito dalla misura correttiva 3 7.1.2 viene indicato come implementare efficacemente una politica che tenga conto anche del contesto, andando a mitigare la problematica descritta nel capoverso precedente.

Per quanto riguarda la gestione delle autenticazioni nel paragrafo successivo vedremo nel dettaglio le modalità con cui sia possibile eseguire il login. Per quanto attiene a questo paragrafo vedremo l'unico metodo che non si basa su firma digitale ma su username e password e come venga gestita la politica di quest'ultima.

La password viene inizializzata casualmente al momento della creazione dell'account stesso ed viene inviata tramite email inserita in fase di registrazione.

Questa deve essere cambiata al primo accesso e può essere resettata solo dopo aver effettuato il login (metodo non bloccante in quanto esistono metodi differenti per il login, vedesi 3.7) o contattando l'owner del reparto di appartenenza o l'amministratore di sistema.

Si riscontra anche una buona politica di freshness della password che impone il cambiamento di quest'ultima entro tre mesi dall'ultima modifica.

3.7 Metodi di autenticazione

L'autenticazione dell'utente può avvenire con una modalità differente a seconda del fatto che l'utente sia connesso in rete locale o tramite internet. Se da rete esterna l'autenticazione può avvenire tramite SPID e Carta dei servizi. Mentre, se da rete interna per velocizzare la normale gestione l'utente si può autenticare anche con solo username e password. Quest'ultima è estremamente difficile da implementare nel contesto corrente.
Gli accessi tramite SPID e Carta dei servizi viene fatto controllando la firma del servizio terzo valutandone l'autenticità e la freshness.
Sarebbe opportuno introdurre un servizio centralizzato di autenticazione non solo per questo servizio ma anche per gli altri interni all'organizzazione in modo da diminuire significativamente il numero dei diversi metodi di accesso all'organizzazione, eseguire una serie di misure di rafforzamento delle policy di sicurezza lungo tutta la applicazione e sgravare l'utente dal dover ricordare molteplici password/nomi utente.
Un tipico esempio di integrazione sistemica potrebbe essere che l'autenticazione di un utente possa avvenire solo a seguito che l'utente abbia timbrato il cartellino aziendale
All'applicativo inoltre non si autenticano solo il personale aziendale ma anche altri applicativi tramite Basic authentication over HTTP, questo potrebbe essere sostituito mediante l'uso di certificati che garantiscono un notevole livello di protezione e sono facilmente impostabili e modificabili.

3.8 Metodi di tracciamento

Ad ora è prevista una politica di log solamente per determinate parti del sistema e per gli accessi al database.

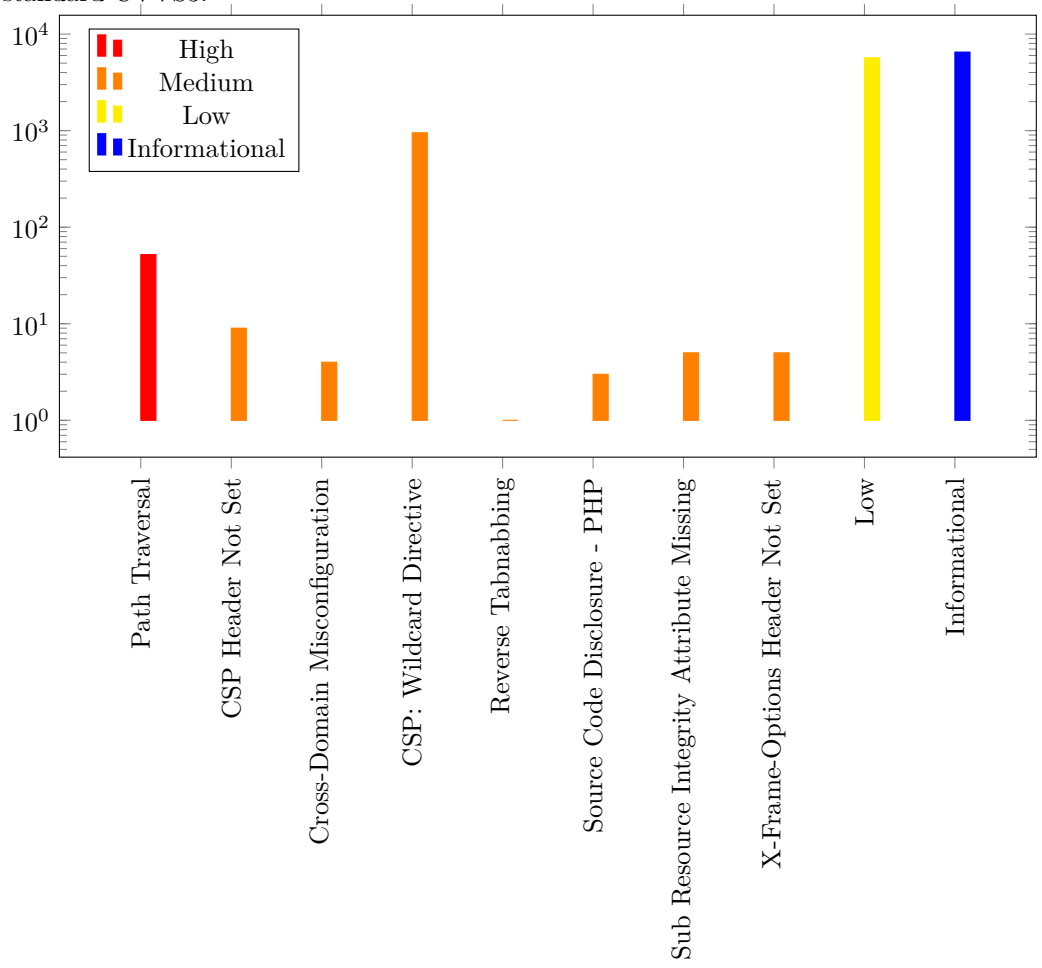
Vi sono alcune pagine in particolare del sistema in cui vengono salvate periodicamente con intervalli molto brevi di pochi secondi tutte gli inserimenti effettuati dagli operatori, questo al fine di facilitare l'utente anche a seguito di una disconnessione momentanea o anche per annotazione generale in cui mancano dei dati per completare l'istanza d'inserimento. Tuttavia questo potrebbe anche essere utilizzato per monitorare il comportamento dell'utente e valutare i punti di miglioramento del sistema. Non è stato riscontrato nessun metodo periodico di valutazione delle minacce o analisi dei log. Il tracciamento tuttavia ad ora non può essere implementato prima di implementare un identificativo per ogni pagina in modo da determinare Misure di correzione 3. Dopo ciò sarà necessario iniziare ad eseguire una raccolta statistica delle azione eseguite di norma dagli utenti o a grana più grossa dai reparti in modo da tracciare eventuali anomalie per poi procedere con un analisi mirata dei file di log.

Si evidenzia inoltre come sarebbe necessario dato il particolare contesto, introdurre un'integrazione con un SOC.

Capitolo 4

Owasp Zap test

Riporto i i risultati di una scansione statica effettuata tramite il tool Owasp ZAP, ponendo particolare attenzione a quei rischi che vengono individuati come medio/alti secondo lo standard CVVS3.



Il "Path Traversal" rappresenta una vulnerabilità critica in cui un attaccante può sfruttare un

difetto nell'implementazione del sistema per accedere a directory o file al di fuori della sua posizione prevista. Questo può consentire all'attaccante di visualizzare, modificare o eseguire file sensibili sul server, compromettendo la sicurezza dell'applicazione.

Nel tuo contesto specifico, il rischio di "Path Traversal" è emerso a causa della presenza di un parametro GET chiamato "torna" nell'URL di molte pagine dell'applicazione. Questo parametro viene utilizzato per comunicare tramite un pulsante "indietro" presente nell'interfaccia della pagina di destinazione. Tuttavia, la gestione di questo parametro non è stata implementata correttamente lato server, aprendo la porta a potenziali attacchi di Path Traversal.

Per mitigare questo rischio, è consigliabile implementare una politica di accesso basata sul contesto lato server per gestire correttamente il parametro "torna". Ciò può essere fatto verificando che il percorso specificato dal parametro sia limitato a una directory sicura o ad una lista di percorsi consentiti. Inoltre, è importante effettuare una valida validazione dei dati di input per assicurarsi che il parametro non possa essere manipolato per accedere a risorse non autorizzate.

In aggiunta, è essenziale effettuare una revisione approfondita del codice per identificare e correggere eventuali punti di vulnerabilità di Path Traversal esistenti. Questo dovrebbe includere l'analisi di tutte le funzioni o librerie che interagiscono con il filesystem per assicurarsi che i percorsi dei file siano correttamente validati e limitati alle directory consentite.

In conclusione, il rischio di "Path Traversal" individuato attraverso la scansione OWASP ZAP evidenzia la necessità di implementare misure di sicurezza adeguate per prevenire exploit dannosi. La corretta gestione dei parametri di input, in particolare il parametro "torna", e la validazione accurata dei percorsi dei file possono contribuire significativamente a mitigare questa vulnerabilità critica.

4.1 Manual test

L'utilizzo meramente passivo di un tool automatico descrive poco o nulla dello stato di un sistema, per cui si è effettuata un analisi manuale mirata su alcuni estratti del codice. Questo è stato fatto poichè risulta ad ora impossibile valutare attentamente tutto il sistema anche perché mancano delle specifiche formali su cui poter effettuare le verifiche. Tuttavia una serie di valutazioni su un numero sufficiente di diverse parti del codice può dare un'idea verosimile sullo stato della sicurezza del software.
Da quest'analisi sono state evidenziate la presenza di alcune vulnerabilità di cui taluni anche con un rischio piuttosto elevato queste tra cui possiamo trovare:

- l'utilizzo insicuro di funzioni Eval
- divulgazione di parametri di configurazione sensibili
- possibilità di aggirare i controlli imposti dal sistema (a livello di policy per alcune procedure)

Si raccomanda quindi di eseguire una serie di test molto più estensivi e onnicomprensivi, ricorrenti al fine di valutare al meglio lo stato del sistema. Tuttavia una soluzione che richieda molte meno risorse aziendali potrebbe essere quella di mettere a disposizione di tutti di un server di test in cui i dati sanitari vengano anonimizzati al fine di permettere a ricercatori e interessati di proporre delle responsible disclosure.

Capitolo 5

Definizione del rischio accettabile

Il rischio accettabile è stato definito da un'analisi di terze parti indipendenti come:

PONDERAZIONE DEI RISCHI E LIVELLI DI ACCETTABILITÀ

Definiamo una matrice di ponderazione del rischio nella quale:

1. in ascissa si trovano le categorie relative alla gravità delle conseguenze dannose (es. lesioni, peggioramento dello stile di vita) derivanti dalla situazione di pericolo imputabile all'utilizzo del dispositivo
2. in ordinata sono posizionati i differenti livelli di probabilità o frequenza di accadimento di tale situazione. La frequenza di accadimento viene ipotizzata sulla base di:
   2.1. diffusione sul mercato del dispositivo (numero di dispositivi prodotti e venduti)
   2.2. esposizione al dispositivo

Questa rappresentazione in forma di matrice, costituisce un semplice ed efficace modo di illustrare la combinazione tra frequenza di accadimento e gravità della conseguenza, sintetizzata in un livello di rischio.
Gravità (conseguenze):

- NULLA ..... nessun danno a cose o persone
- MINORE ..... danno reversibile: si risolve spontaneamente senza ulteriori conseguenze
- MAGGIORE ..... danno reversibile: per la risoluzione si prevede un intervento terapeutico non invasivo e un tempo relativamente breve per la sua scomparsa

- GRAVE ..... danno reversibile: per la risoluzione si prevede un intervento terapeutico invasivo per prevenire una menomazione di una funzione del corpo o una lesione di una struttura e/o un tempo alquanto lungo per la sua scomparsa e/o il prolungamento della degenza
- MOLTO GRAVE ..... danno irreversibile senza pericolo di vita: per la risoluzione si prevede un intervento terapeutico con compromissione della funzione, della struttura, della vita di relazione (disabilità permanente) ma senza pericolo di vita o Il danno può pregiudicare nel tempo la vita delle persone (non è letale nell'immediato)
- LETALE ..... il danno può pregiudicare nell'immediato la vita delle persone (paziente / terapista / medico / assistente)

Categorie di possibilità / frequenza

- NULLA ..... evento mai riscontrato
- MOLTO BASSA ..... la situazione di pericolo è improbabile durante l'intero ciclo di vita del dispositivo
- BASSA ..... la situazione di pericolo si verifica non più di una volta all'anno
- MEDIA..... la situazione di pericolo si può verificare una/due volte in un anno
- ALTA ..... la situazione di pericolo si può verificare fino a dieci volte in un anno
- MOLTO ALTA ..... la situazione di pericolo si può verificare più di dieci volte in un anno

La matrice generale di accettabilità del rischio è la seguente:

	None *Nulla*	Minor *Minore*	Major *Maggiore*	Serious *Grave*	Very Serious *Molto* Grave	Lethal *Letale*
Very High *Molto Alta*		**NAc**				
High *Alta*		**AFAP**				
Medium *Media*						
Low *Bassa*						
Very Low *Molto Bassa*						
None *Nulla*						

Figura 5.1: Matrice del rischio ArchiMed

DOVE:

- AFAP – As Far As Possible, Per quanto possibile, in confronto di una valutazione sul rapporto rischio-beneficio. Sono state applicate delle misure tecnicamente praticabili senza alterare l'uso previsto o il beneficio.
- NAc – Non accettabile conseguenze, probabilità e rischio, sono quantificate sulla base dell'esperienza diretta maturata dal personale del fabbricante e della bibliografia conosciuta.
- La zona verde indica il livello di rischio accettabile.

Come richiesto dal regolamento UE 2017/745 e s.m.i., sono gestiti tutti i rischi identificabili, anche quelli trascurabili, sulla base del rapporto rischio/beneficio.

Capitolo 6

Identificazione delle minacce

Nel contesto della sicurezza informatica, il threat modeling è diventato un'attività fondamentale per identificare e mitigare le potenziali minacce e vulnerabilità di un sistema. Il threat modeling consente agli sviluppatori, alla governance aziendale e agli amministratori dei sistemi di comprendere meglio i rischi associati a un'applicazione e quindi di prendere decisioni ponderate per mitigare tali rischi. Uno degli aspetti cruciali del threat modeling è l'analisi dei thread actor, che si concentra sulle entità che possono interagire con il sistema e potenzialmente sfruttare le sue debolezze.

Data la particolare struttura del sistema allo stato attuale non è possibile procedere con un vero e proprio Threat Model, in quanto manca una vera e propria lista di asset e la criticità che questi comportano.

Tuttavia è possibile andare a descrivendo al meglio i Threat Actor basandoci su casi storici documentati e rapporti interazionali che descrivano l'andamento delle minacce su sistemi analoghi e in contesti similari.

6.1 Threat Actor

Secondo quanto descritto dal ETDA (Electronic Transactions Development Agency) ad oggi sono presenti 13 gruppi di APT che potrebbero mirare alla compromissione di questo software. Grazie al tool messo a disposizione dall'ETDA, ente parastatale tailandese è possibile effettuare una ricerca dei gruppi di APT che avrebbero come scopo un ospedale italiano [1]. Molti di

APT Group	**Country**	**Active from**	**Notes**
Aggah	[Unknown]	10/2018 - 10/2021	
APT 20, Violin Panda	China	01/2014 - 12/2017	
APT 29, Cozy Bear, The Dukes	Russia	01/2008 - 03/2023	Attività negli ultimi 3 mesi
APT 41	China	01/2012 - 12/2022	Ha avuto operazioni di contrasto
APT 42	Iran	01/2015 - 09/2022	
Circus Spider	[Unknown]	01/2019 - 02/2022	Ha avuto operazioni di contrasto
Dark Caracal	Lebanon	01/2007 - 12/2020	
DarkHotel	South Korea	01/2007 - 12/2021	
FIN8	[Unknown]	01/2016 - 07/2021	
Parisite, Fox Kitten, Pioneer Kitten	Iran	01/2017 - 11/2020	
Stone Panda, APT 10, menuPass	China	01/2006 - 02/2022	Ha avuto operazioni di contrasto
TA2101, Maze Team	[Unknown]	01/2019 - 02/2022	Ha avuto operazioni di contrasto
Turbine Panda, APT 26, Shell Crew	China	10/2010 - 10/2018	

Tabella 6.1: APT Groups

questi gruppi sono ben finanziati anche da entità statali come il gruppo APT 29 che è stato associato ai servizi di inteligence russi, specificatamente al Foreign Intelligence Service (SVR) [15].

In particolare il Regno Unito ha diffuso un bollettino di allerta poiché il gruppo si è concentrato sull'attaccare gruppi coinvolti nella campagna di vaccinazione contro il COVID-19 [16].

Questo è un monito molto importante per sistemi come quello preso in oggetto da questa tesi poiché sottolinea come:

- vi sono attori interessati all'attaccare il sistema ArchiMed
- abbiano risorse importanti
- godano dell'appoggio di governi
- abbiano le capacità tecniche per portare a termine attacchi sempre più sofisticati

Come possiamo evincere dai grafici sottostanti:

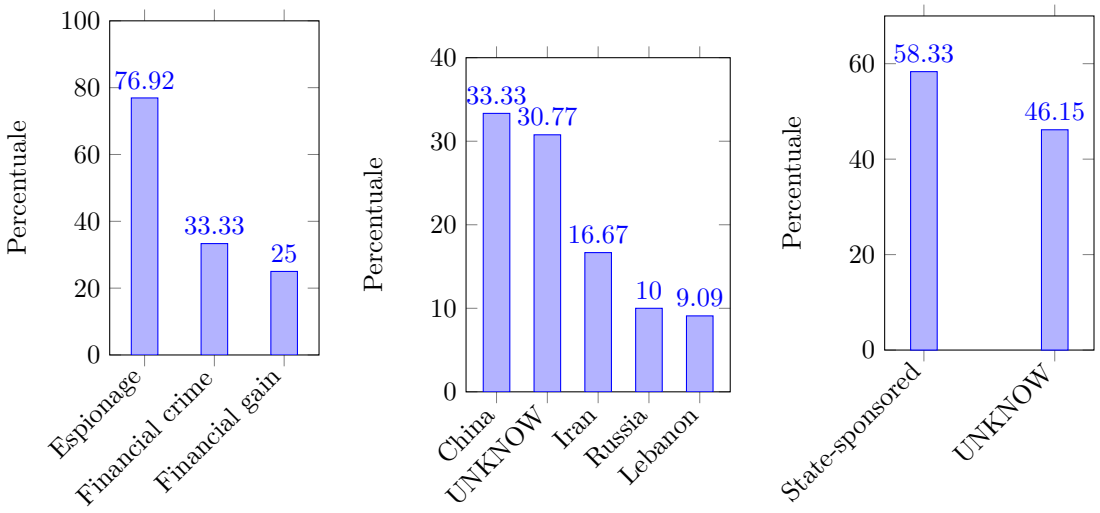


Figura 6.1: Grafici a barre per le tabelle

Dai dati raccolti emerge una preoccupante capacità d'attacco dato infatti che emerge sia da una lunga lista di attacchi che sono stati ricondotti e attribuiti a questi gruppi in passato ma soprattutto dall'enorme capacità economica che li sostiene.
Di fatti più della metà di questi gruppi sono riconducibili a stati esteri e possono quindi contare su un'enorme rete di risorse. Inoltre, emerge sempre dai grafici, che molti di questi gruppi hanno anche potenziali riserve proprie derivanti da attacchi passati o in corso che miravano proprio all'aspetto finanziario utilizzando anche ramsoware e rivendita di informazioni in black market.
Anche secondo il report del Clusit il settore dell'healtcare è una preda estremamente appetibile per gli attacchi informatici. Infatti nel 2022 è stato il secondo settore più colpito dagli attacchi rappresentando ben il 12,5% di tutti gli attacchi subiti nell'anno [19]. Tuttavia c'è da sottolineare che i dati del Clusit attribuiscono per l'Italia (e non per i settore specifico dell'healtcare) solo il 13% degli attacchi sono riconducibili a operazioni di Espionage/Sabotage e solo l'8% ad operazioni di Information Warfare. Quest'ultima comparazione mi porta a riflettere che i Threat Actor fino a qui analizzati siano una minoranza rispetto a una quantità molto maggiore di Attivisti.

6.2 Attacchi recenti a infrastrutture sanitarie italiane

Nel corso degli ultimi anni si è visto un elevato e sempre crescente numero di attacchi ai sistemi delle strutture sanitarie italiane.
Di fatti anche per quanto si evince dal rapporto del Clusit [19] la saverity degli attacchi nel settore heltcare hanno la gravità più alta sia per quanto riguarda la mediana sia la media. Inoltre anche il volume di attacchi ha un trend crescente e vi sono stati molti attacchi che hanno risuonato anche nella stampa non specializzata.

6.2.1 Cyber attacco alla Regione Lazio

Il primo caso di cyber attacco alla sanità che tutti ricordiamo, è quello che ha coinvolto la Regione Lazio. All'inizio di agosto 2021 aveva subito un attacco ransomware molto grave. Tra i vari servizi interessati, il portale di prenotazione dei vaccini Covid-19 aveva subito uno stop forzato. Non era possibile accedervi, con conseguente blocco delle prenotazioni e della gestione dei vaccini. La Regione, dopo giorni di caos e interruzione di molti servizi, era riuscita a ripristinare i dati attraverso un backup.
LockBit 3.0 è un altro gruppo affiliato con il servizi segreti russi, tuttavia eseguono anche azioni come RAAS (Ransomware As A Service).
Per questo particolare gruppo è particolarmente complicato identificare un sito web che disponga della cronistoria dei data breach poiché sono soliti crearne di vari in base ai target.

6.2.2 Cyber attacco all'Ulss di Padova

A fine anno 2021, si è verificato un altro importante attacco ransomware. Questa volta ai danni dell'Ulss 6 Euganea di Padova che ha bloccato per settimane alcuni servizi essenziali della struttura sanitaria. Il blocco ha colpito: Cup, punti prelievi, nuove registrazioni dei pazienti, il sistema dei laboratori, alcuni punti tamponi e gli hub vaccinali.. Ad agire è stato il gruppo LockBit 2.0. Essi hanno sequestrato i dati sensibili di migliaia di cittadini e chiesto un riscatto in bitcoin all'azienda ospedaliera che però è riuscita a ripristinare i servizi senza pagare il riscatto dopo una lunga e complessa operazione. I criminali informatici hanno comunque pubblicato decine di cartelle cliniche complete di nomi, cognomi, indirizzi di residenza e dati sensibili.
Allo stato attuale il gruppo LockBit 2.0 si è scisso ed è chiuso definitivamente tuttavia molti dei suoi componenti sono migrati in LockBit 3.0.
LockBit 2.0 è un altro gruppo affiliato con il servizi segreti russi, tuttavia eseguono anche azioni come RAAS (Ransomware As A Service).

6.2.3 Cyber attacco all'Usl Napoli 3

A distanza di poche settimane dall'attacco all'Usl di Padova, un altro evento di data breach e PA ha interessato ancora un'azienda sanitaria. Questa volta siamo a Napoli, con l'Usl Napoli 3 sud colpita da un attacco informatico (sempre tramite ransomware), ad opera del gruppo criminale informatico Sabbath (54bb47h). Ancora una volta è stata paralizzata l'infrastruttura e bloccato il sistema di prenotazione dei vaccini.
Sono stati inoltre diffusi dati sensibili custoditi dalla struttura sanitaria ed è seguita una minaccia di diffusione degli altri dati rubati, come tentativo di estorsione del riscatto. Ad oggi il loro sito web sembrerebbe essere inaccessibile, tuttavia non vi è certezza del fatto che potrebbero aver spostato il sito e servirà più tempo per far emergere il nuovo dominio.

6.2.4 Cyber attacco all'Asst Fatebenefratelli Sacco

Ultimo in ordine cronologico, ma non per questo meno importante, è il potente attacco hacker subito da varie strutture ospedaliere e sanitarie milanesi ad inizio maggio 2022. Gli hacker hanno colpito i sistemi informatici dell'Asst Fatebenefratelli Sacco. L'azienda gestisce gli ospedali Luigi Sacco, Fatebenefratelli e Oftalmico, nonché altri presidi ospedalieri e varie strutture sanitarie e sociosanitarie territoriali. L'attacco ha messo offline i siti di tutte le strutture gestite dall'azienda ma, secondo la Regione, non sono stati rubati dati dei pazienti.
Quest'attacco è stato condotto dal gruppo Vice Society, la particolarità di questo gruppo è che non ci sono evidenze forti di affiliazione con governi o entità statali o parastatali si noti comunque che utilizzano il linguaggio cirillico.

6.2.5 Ransomware AOAL Alessandria

Attacco rivendicato da RagnarLocker, un altro gruppo riconducibile al governo Russo. Quest'attacco sembrerebbe aver esfiltrato con successo circa 1TB di dati di pazienti e dipendenti e comunicato l'evento alla vittima il 20 Dicembre 2022 tramite un file contenente il seguente messaggio:

```
For ethical reasons we did not want to spread
the news of the attack on the hospital's
IT infrastructure before the news became public
knowledge. Indeed, on December 20, SuspectFile had
already become aware of the ransom note written
by the Ragnar_Locker group.
```

Non avendo pagato il riscatto AOAL Alessandria ha visto pubblicare i propri dati ancora accessibili pubblicamente http://xxxxxxxxx.onion/?5u3ARvh2Jv4q7CLA checksum di

```
xxxxxxxxx=4cc8b38b1571fad5235c5560e74bcec8b3e5cdcb3c3
3c23112c9c74a38bb358c80dd88ca53016998cc7d87f5ca848ecd
```

6.2.6 Ransomware ASL 1 Abruzzo

Quest'ultimo attacco è stato divulgato nell'ultimo mese e data la freschezza e la portata dell'evento ho ritenuto opportuno aggiungerlo in corsa alla lista di attacchi condotti contro infrastrutture sanitarie. Stando a quanto riportato tramite lo strumento `https://ransom.insicurezzadigitale.com/?country=ITA` e verificando l'attribuzione dell'attacco (tramite rivendicazione sul portale della stessa azienda hash identifier 537df6b3763a660b40ff503127d8205a8536e79056537ff83e0238e4c77a6ef9), l'attacco è stato condotto e rivendicato dal gruppo conti.
Questo come detto in precedenza è un attore riconducibile a governo Russo, e non ricevendo alcun riscatto ha deciso di rilasciare pubblicamente tutti i dati trafugati, più di 500GB di dati (per la precisione 522Gb compressi).

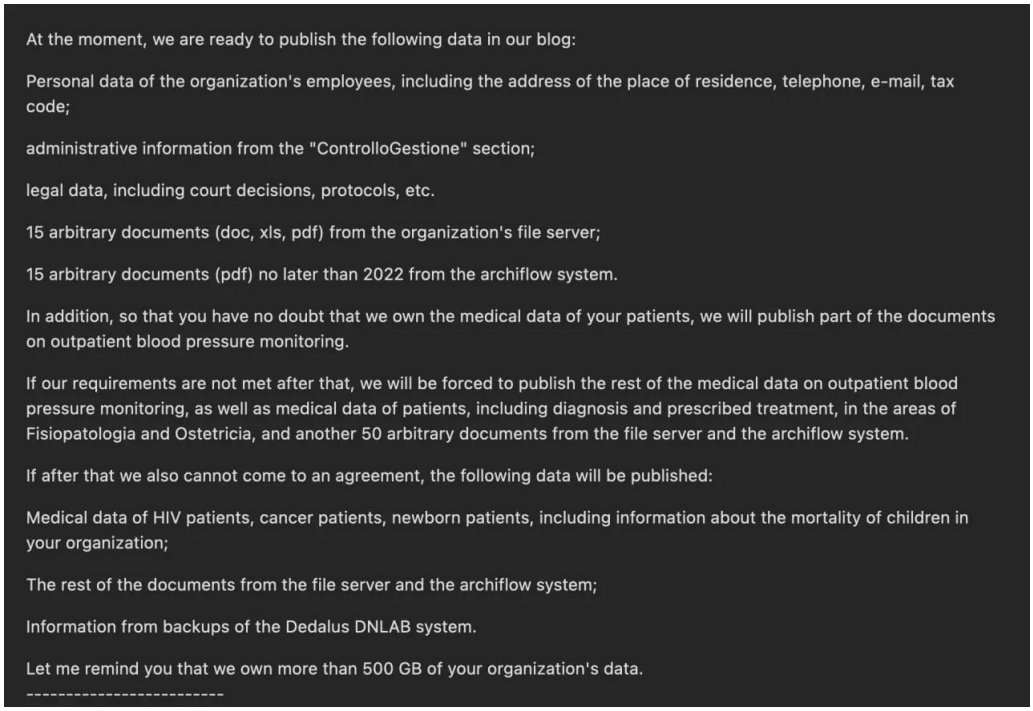


Figura 6.2: Rivendicazione attacco e info

Si noti che se queste informazioni trovano altre conferme, c'è stata una grave mancanza

poiché il sistema di backup è stato compromesso e questo è possibile solo per incuria (come ad esempio l'aver tenuto online il sistema di backup e non scollegato dalla rete, non aver cifrato i dati ed altre negligenze similari di basso livello)

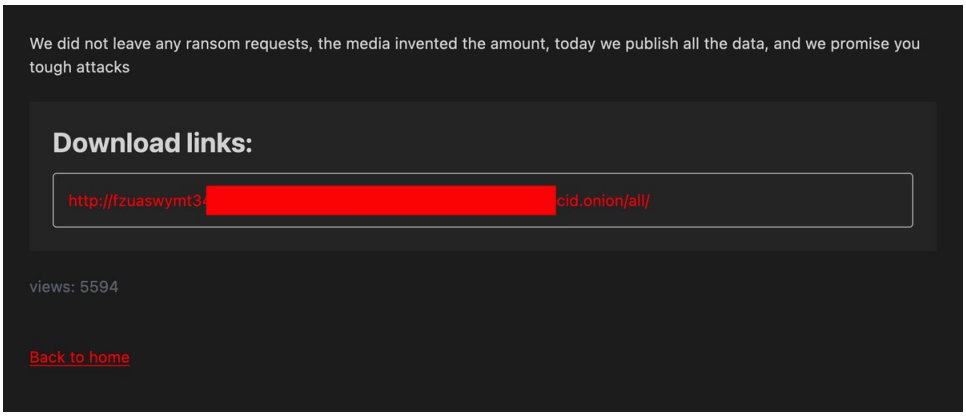


Figura 6.3: Pubblicazione dei dati

È bene evidenziare che il riscatto non è stato pagato e i dati sono stati resi pubblici nella giorno 15-05-2023, con un accesso e questi di quasi 7K differenti individui nel corso delle 24h successive. fonte anonimizzata http://xxxxxxxxxxxx.onion/all/

```
checksum=2931f3039a9f1c1aba68a4f04d4b5a0362c9bef02f8fd4f
e482a0eacc87ac7bd3388a45e4ce5c7588459030764f6e11f sha384
```

(il checksum è da riferirsi sono ad xxxxxxxxxxxx dove è avvenuta l'anonimizzazione)

Capitolo 7

Misure di correzione

Misure correttive Di gestione:

Misura correttiva	Descrizione	Stato di attuazione
1	definizione delle procedure di sviluppo software	eseguito
2	definizione delle procedure di manutenzione software	eseguito
3	definizione delle procedure di gestione degli errori	da implementare
4	definizione del software per il tracciamento errori	da implementare
5	definizione di una piattaforma per il testing	da implementare
6	definizione di una piattaforma per la gestione dei bug bounty **anche gratuiti con uno scoreboard per il riconoscimento	da implementare
7	redigere il manuale d'uso del software	implementazione parziale
8	redigere il manuale tecnico del software	implementazione parziale

Tabella 7.1: Misure correttive Di gestione 1 di 2

Misura correttiva	Descrizione	Stato di attuazione
9	redigere il manuale tecnico di configurazione software	implementazione parziale
10	redigere il manuale tecnico di gestione di sistema	implementazione parziale
11	redigere il manuale tecnico di configurazione del sistema	implementazione parziale
12	definizione dei requisiti del software	implementazione parziale
13	definizione dei requisiti di sistema	implementazione parziale
14	definizione dei requisiti di rete	Implementazione parziale
15	certificazione ISO9001	da implementare
16	definizione delle comunicazioni con gli stake holder esterni	da implementare
17	definizione della comunicazione con il CSIRT	da implementare
18	certificazione ISO27001	eseguito

Tabella 7.2: Misure correttive Di gestione 2 di 2

Misure correttive Tecniche:

Misura correttiva	Descrizione	Stato di attuazione
1	introduzione delle connessioni in https su tutto l'applicativo	eseguito
2	incorporazione dei parametri di sicurezza nella trasmissione della password a livello applicativo	eseguito
3	implementazione dell'access control basato sul contesto (l'utente ha i privilegi della pagina dove si trova)	da implementare
4	implementazione di una politica di freshness sulla password di accesso al database	da implementare
5	rafforzamento del controllo sull'origine delle richieste di login	implementazione parziale
6	verifica degli input non sanificati	implementazione parziale
7	realizzazione microservizi	valutazione in corso
8	utilizzo di indicatori di compromissione	non implementata

Tabella 7.3: Misure correttive Tecniche

Le misure di mitigazione non sono state descritte in maniera esaustiva in questo testo poiché potrebbero esporre troppe informazioni aziendali, comunque andrò a descrivere per quanto possibile alcune di queste misure adottate da adottare o in corso di valutazione.

7.1 Misura correttiva 3

7.1.1 Token di identificazione della sessione

Oltre a questo il server richiederà, come parametro per verificare la provenienza della query, il token di pagina. Esso sarà generato a seguito di una risposta affermativa dal server come

SHA256(url+sessionId+secret+nonce+timestamp), nonce, timestamp

7.1.2 Definizione dei privilegi considerando il contesto

La proposta di implementazione consiste nel mappare le azioni per ogni pagina web, ovvero i permessi di cui la stessa necessita per la sua esecuzione, includendo:

- comandi di reindirizzamento ad altre pagine
- invio di dati tramite Post/Get
- javascript che dinamicamente possono andare a richiedere risorse esterne alla pagina

Ogni pagina avrà una lista di permessi Lp{} che, ad ogni richiesta ricevuta dal server dovranno essere verificati con i permessi di cui l'utente dispone.
I permessi di cui disporrà ogni processo saranno definiti come la classification lattice

$$\lambda(p) := glb(\lambda(s), \lambda(c))$$

Dove:

- $\lambda(p)$ rappresenta i permessi associati al processo in corso
- $\lambda(s)$ rappresenta i permessi associati all'utente
- $\lambda(c)$ rappresenta i permessi associati al contesto

7.2 Misura correttiva 7

7.2.1 Microservizi

La scissione di una applicazione monolitica in una molteplicità di microservizi comporta innumerevoli vantaggi, oltre ai profili di sicurezza che illustrerò nei paragrafi successivi, offre una migliore elasticità nell'implementazione delle varie sezioni. Di fatti i microservizi si basano sul concetto di non avere punti in comune, variabili d'ambiente, OS, linguaggi di sviluppo dell'applicazione, differenti strutture dati, ecc... Pur potendo comunicare l'uno con gli altri tramite api solitamente modellate tramite REST. Questa risulta essere una soluzione ottimale per il lungo termine nello sviluppo di gestionali soprattutto in ambiti con scarsità di risorse e elevati requisiti. Tuttavia è importante sottolineare che questo deve essere fatto in maniera sostenibile, invece che usare macchine virtuali per per replicare ogni ambiente di ogni singolo microservizio sarebbe opportuno usare i container.

Container

I container permettono di virtualizzare ambienti differenti sulla stessa macchina, ma a differenza delle macchine virtuali non reinstanziando un vero e proprio OS per ogni ambiente, permettendo così di ridurre moltissimo i requisiti hardware necessari.

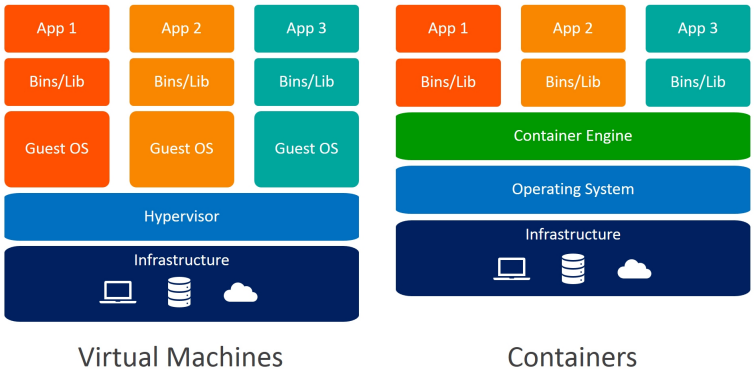


Figura 7.1: container vs Virtual machine

Da portare all'attenzione è sicuramente la possibilità di eseguire differenti ambienti con differenti versioni sui vari container. Ad esempio un'unica applicazione monolitica in PHP comporta notevoli difficoltà nell'aggiornare il software PHP si pensi ad esempio alle problematiche di compatibilità che possono sorgere in specifiche sezioni. In applicazioni containerizzate come i microservizi è possibile eseguire gradualmente gli aggiornamenti per ogni container, magari utilizzando altre strade per limitare i rischi la dove non sia possibile

aggiornare. Data la seguente struttura è possibile stanziare multiple istanze di diverse applicazioni allo stesso costo computazionale di un'unica macchina virtuale.

Ad esempio su un piccolissimo Raspberry è possibile parallelizzare più di 10 container, mentre già con una sola macchina virtuale risulta rallentato

Risulta inoltre molto importante sottolineare che il vantaggio più grande lo possiamo riscontrare a livello di rete. Nello stato dell'arte attuale possiamo notare come sia possibile virtualizzare buona parte del network andandone a definire e controllare le comunicazioni.
Per finire i vantaggi che apporta k8s (Kuberneties) sono estremante più significanti e immediatamente tangibili, di fatti è possibile creare dei cluster elasticità che permettano l'immediata scalabilità dei microservizi sia in caso di sovraccarico sia in caso di disservizio.

7.3 Misura correttiva 8

Uno dei sistemi più semplici ed efficaci da implementare a livello applicativo per migliorare la sicurezza informatica è l'utilizzo dei canaris. Storicamente, i canaris erano file trappola progettati per somigliare il più possibile a file reali, ma con la particolarità di attivare un allarme quando vengono aperti o letti. Questi file sono di solito configurati in modo tale che un utente normale non sia tentato di aprirli (ad esempio, potrebbero apparire come pazienti fantasma o pagine non linkate, ma con una configurazione apparentemente normale come "php.ini").
L'obiettivo principale di questi sistemi è quello di attuare una strategia di DECEPTION, cioè di rallentare un attaccante per ostacolare le sue azioni dannose, mentre si mettono in atto misure di mitigazione del rischio in situazioni di emergenza. In pratica, i canaris agiscono come indicatori precoci di intrusioni o attività sospette, attirando l'attenzione degli amministratori di sistema o degli analisti di sicurezza.
L'utilizzo di queste metodologie, integrate con sistemi XDR (eXtended Detection and Response) e SIEM (Security Information and Event Management), contribuisce in modo significativo ad aumentare la resilienza dei sistemi informatici. Gli XDR sono piattaforme di sicurezza che combinano diverse funzionalità, come il monitoraggio avanzato, la rilevazione delle minacce, l'indagine degli incidenti e la risposta automatizzata, consentendo di ottenere una visione più completa e integrata della sicurezza del sistema. I sistemi SIEM, invece, raccolgono, analizzano e correlano gli eventi di sicurezza provenienti da diverse fonti, al fine di identificare eventuali anomalie o comportamenti sospetti.
L'utilizzo dei canaris come sistema di allarme precoce e la loro integrazione con sistemi XDR e SIEM rappresentano un'importante aggiunta alla strategia di sicurezza informatica. Queste metodologie contribuiscono a migliorare la resilienza dei sistemi, consentendo di individuare e mitigare le minacce in modo tempestivo, nonché di acquisire una migliore

Capitolo 8

Proposta metodologia per la migrazione verso microservizi

Allo stato attuale risulta estremamente complicato verificare e implementare una qualche forma di euristica per la valutazione delle performance, normale uso e indicatori di compromissione puntuali.
Questa complessità delle interconnessioni è molto visibile solamente guardando le chiamate statiche effettuate dal front-end:

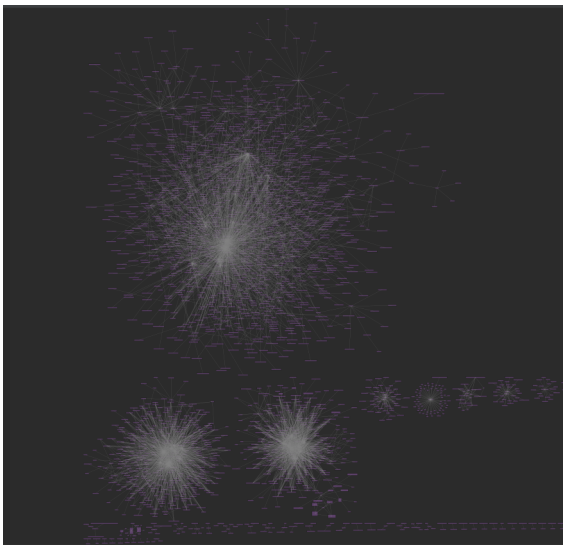


Figura 8.1: Interconnessioni dei javascript statici

A questo andrebbero aggiunte tutte le chiamate dinamiche generate dal PHP in run-time e non, aggiungendoci inoltre tutte le interconnessioni derivanti dal PHP.

La metodologia che è riportata di seguito ha come scopo principale l'isolamento delle varie azioni e dati in contesti estremante sensibili come in un applicativo di gestione medica. Questo comporta innumerevoli vantaggi sia a livello di sicurezza sia per quanto riguarda la manutenzione del codice.
Elementi di partenza:

- alto livello di rischio
- normative stringenti riguardo alla revisione del codice
- codice monolitico, con generazione dinamica delle pagine
- preesistenza di un back-end e un front-end HTML

L'idea si basa sul segregare il più possibile gli elementi aventi differenti tipologie di accessi/livelli con varie sensibilità, sia sul lato front-end sia sullo scindere l'applicativo back-end. Tramite l'uso di iframe con la proprietà sandbox è possibile creare differenti layer di segregazione front-end e, tramite una ristrutturazione del back-end in micro chiamate Rest, possiamo andare a creare una scissione del back-end. L'utilizzo combinato di queste strutture si può ottimizzare la scalabilità anche l'utilizzo di politiche di distribuzione del traffico utilizzando routing dns o reverse proxy.

8.1 Idea di base

Prendendo in esempio la figura sottostante possiamo notare che è composta da tre parti {*1, *2, *3}

Figura 8.2: Esempio di destrutturazione di un sito

Storicamente questa sarebbe stata realizzata usando un unico codice HTML/PHP oppure in versione più scalabile separando le tre parti ognuna in un file PHP e tramite l'uso di include si sarebbe creato un corpo unico.
Questa metodologia porta notevoli svantaggi come un errore, magari introdotto in fase di aggiornamento, potrebbe comportare la non risposta dell'applicativo o la compromissione lato front-end dei dati delle altre sezioni.
Per risolvere questa problematica propongo di introdurre ogni singolo componente {*1, *2, *3} in un iframe con la proprietà sandbox in modo tale che ogni pagina sia considerata come un ambiente a se stante. Di fatti il browser provvederà a fare tre differenti chiamate HTTP, una per ogni pagina, e ad isolare i contesti gli uni dagli altri.

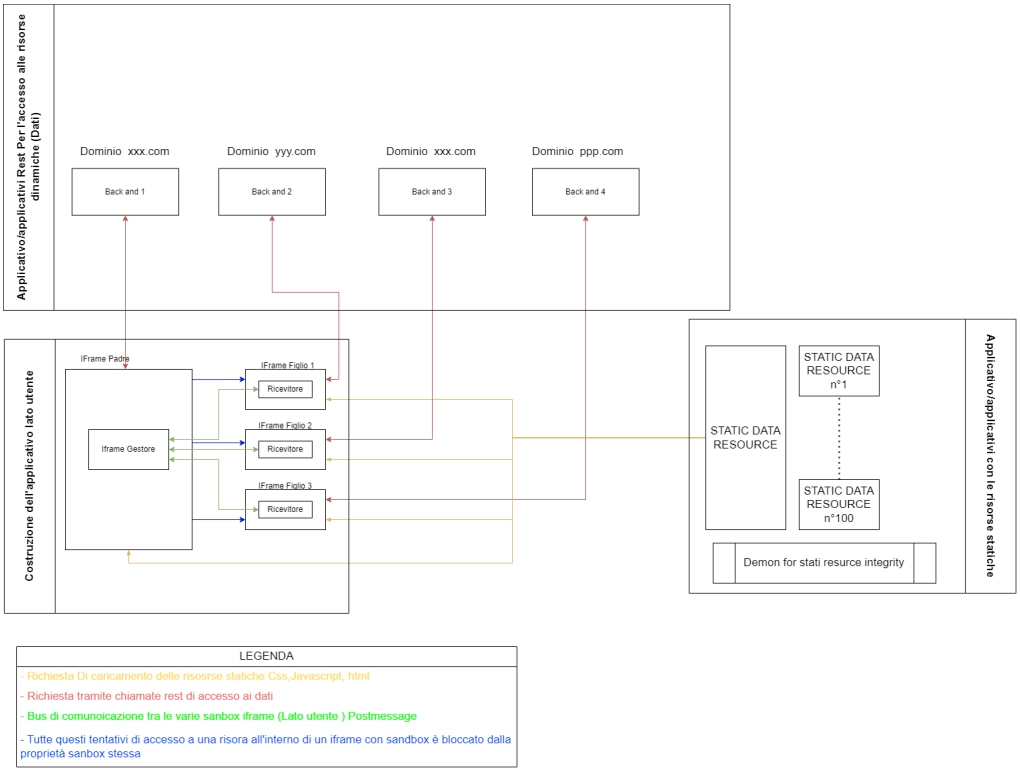


Figura 8.3: Macrostruttura del sistema implementato secondo la metodologia

In questa figura si riporta lo schema implementativo secondo la ristrutturazione ad iframe sandbox dell'immagine 8.2. Ogni iframe è segregato e accede alle proprie risorse pur potendo dialogare secondo la metodologia descritta successivamente (Rilassamento).

CODICE:

```
<header>
<iframe id="header-iframe" src="https://server1/header.php" sandbox></iframe>
</header>
<body>
<iframe id="body-iframe" src="https://server2/index.php" sandbox></iframe>
</body>
<footer>
<iframe id="footer-iframe" src="https://server3/footer.php" sandbox></iframe>
</footer>
```

Quindi ogni pagina avrà il suo contesto, i suoi fogli di stile e i sui dati.

8.2 Integrazioni

Questo però non risulta essere un metodo realmente utilizzabile salvo che in particolari contesti poiché se ogni frame è completamente isolato non può neanche interagire con gli altri elementi per le funzioni di base. Ad esempio, nel componente *1 abbiamo una barra di navigazione che avrà il compito di far cambiare il contesto *2 per passare dalla Home page alla pagina di contatti o alle news.
Per farlo bisogna introdurre Gestore di frame, cioè è necessario inserire uno script all'interno della pagina principale che ci consenta di ricevere le richieste dagli altri frame, andando difatti ad aprire una connessione con i vari frame figli. Questi ultimi a loro volta dovranno contenere uno script che permetta la comunicazione con il padre.

Problema Un iframe con proprietà sandbox non permette di default l'uso di script al suo interno.

8.2.1 Rilassamento e Renforcement

Gli iframe con metodo sandbox non hanno la possibilità di rilassare le proprietà con una grana fine, però è possibile utilizzare la proprietà allow-script per permettere l'uso dei javascript all'interno dei vari iframe Rilassamento.
Questo però può inficiare sensibilmente sulla nostra politica di segregazione. Banalmente un javascript malevolo potrebbe fingersi un processo legittimo all'interno del frame e inviare, tramite il canale di comunicazione che abbiamo aperto, comandi al Gestore degli iframe per eseguire azioni che possono impattare gli altri frame.
Per mitigare questo problema si è optato per una politica di Renforcement per consentire solo i javascript che hanno un determinato hash.

Rilassamento

Esso ci consentirebbe di creare dei canali di comunicazione tra i javascript dei vari frame tramite l'uso del comando nativo Postmessage. Quest'ultimo consente il passaggio di valori tra i frame che, attraverso un protocollo concordato e intermediato tramite il seguente esempio di comunicazione, possa avere una struttura ben definita che limita la propagazione di errori.

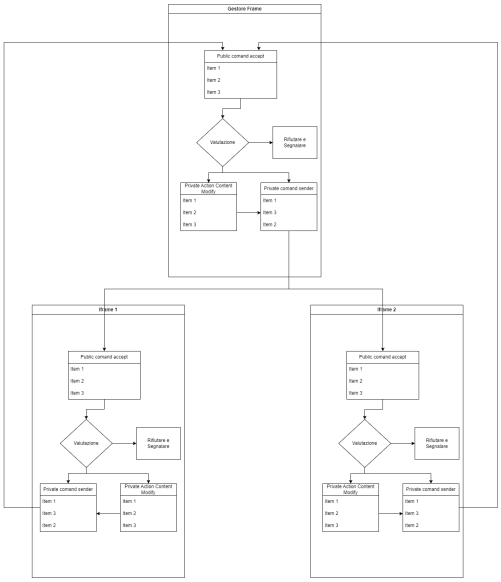


Figura 8.4: Esempio di comunicazione tra i frame

Nella figura 8.4 vediamo come i frame possano dialogare tra di loro solo tramite Postmessage che da un frame vanno ad un altro che ne analizza il contenuto e decide in base alla sua politica che azione intraprendere. Ogni frame ha un ambito di visibilità al suo interno, ovvero può vedere qualunque suo elemento e può accedere ai dati o comunicare solo con il consenso dell'elemento a cui i dati appartengono.

Renforcement

Per eseguire una politica di rinforzo si può utilizzare, all'interno di ogni frame, una politica Content-Security-Policy (CSP). Nello specifico invece che abilitare gli script per tutto il dominio li abilitiamo se rispettano un requisito di integrità.

Esempio di codice CSP

```
<meta id="csp" http-equiv="Content-Security-Policy"
content="script-src
'sha384-4V1lLOWgQTw8KhA50nhUvdXgybYo/XId/AeE/vqd6Wgu1F1PU7T+BZocFqF5XDcN'
'sha384-NSBeKWmwKF5JcjiqxUZm1NpVx3RXL79ea/XcxXqKH2B4wXTIlngJHCJAbsuKPzw0' ;">
```

Tramite questa proprietà il browser consentirà l'esecuzione solo di javascript aventi i due hash indicati. Per utilizzare questa politica non è possibile inserire javascript direttamente nel codice della pagina ma sarà necessario richiamarli tramite script source includendo il parametro di verifica d'integrità.

```
<script src="http://localhost/sito/index/comunica.js"
integrity="sha384-NSBeKWmwKF5JcjiqxUZm1NpVx3RXL79ea/XcxXqKH2B4wXTIlngJHCJAbsuKPzw0"
crossorigin="anonymous"></script>
```

8.2.2 Null origin, perché dobbiamo utilizzarla e come possiamo mitigare il problema

Quando si utilizza il metodo sandbox, se non si abilita allow-same-origin le richieste avranno come origine nell'header http null. Questo è dovuto a come la sandbox isola gli iframe, ovvero assegnando un 'dominio' unico ad ogni iframe, purtroppo è un problema che dobbiamo accettare, poiché altrimenti non avremmo la separazione tra i vari contesti.

Questo comporta che non possiamo utilizzare politiche quali x-frame-options per permettere o negare le richieste. Detto ciò un attaccante potrebbe ricreare un proprio sito includendo una chiamata ai nostri applicativi REST per esfiltrare i dati. Per farlo avrebbe comunque bisogno di accedere al cookie di sessione di un utente attivo, magari tramite una campagna di phishing o tramite l'inserimento di un link esterno all'interno di uno dei nostri verticali (Poisoning).

questo sarebbe possibile e andrebbe a inficiare sulla segretezza dei dati trasmessi dai nostri Verticali tramite api REST.

Dimostrazione:

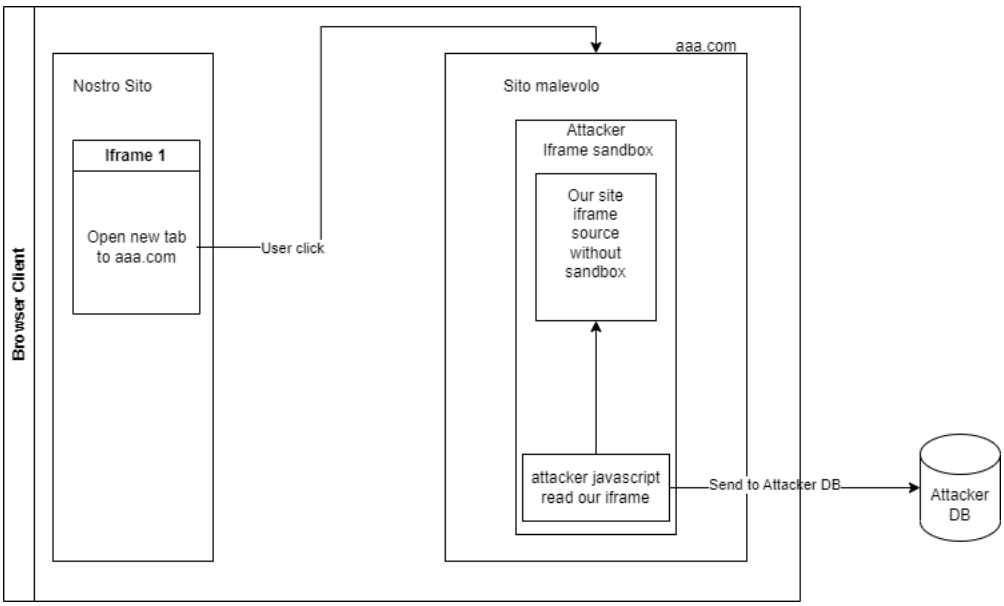


Figura 8.5: Esempio di esfiltrazione dei dati

Mitigazione null origin Per mitigare questo tipo di attacco possiamo andare a costruire una key-chain di autorizzazione per i frame.

Per avere una key chain affidabile dobbiamo comunque avere un punto di origine che possa essere tale. Questo può essere ottenuto poiché, secondo anche quanto descritto in 8.5, il frame padre è "statico", non cambia anche se i suoi sottostanti mutano. Per quest'unica pagina non abbiamo la limitazione descritta precedentemente dell'origine null, poichè non contenuta in nessun frame. Andiamo quindi a impostare *X-Frame-Options:DENY* sulla pagina principale:

APACHE2 esempio:

```
<IfModule mod_headers.c>
Header set Access-Control-Allow-Origin "null"
<FilesMatch "index.php">
Header set X-Frame-Options "SAMEORIGIN"
</FilesMatch>
</IfModule>
```

Questo non basta dobbiamo anche strutturare una key chain che parta quindi da questo elemento che sappiamo non poter essere caricato all'interno di un iframe verso i suoi figli. Per farlo propongo la seguente metodologia:

Dimostrazione:

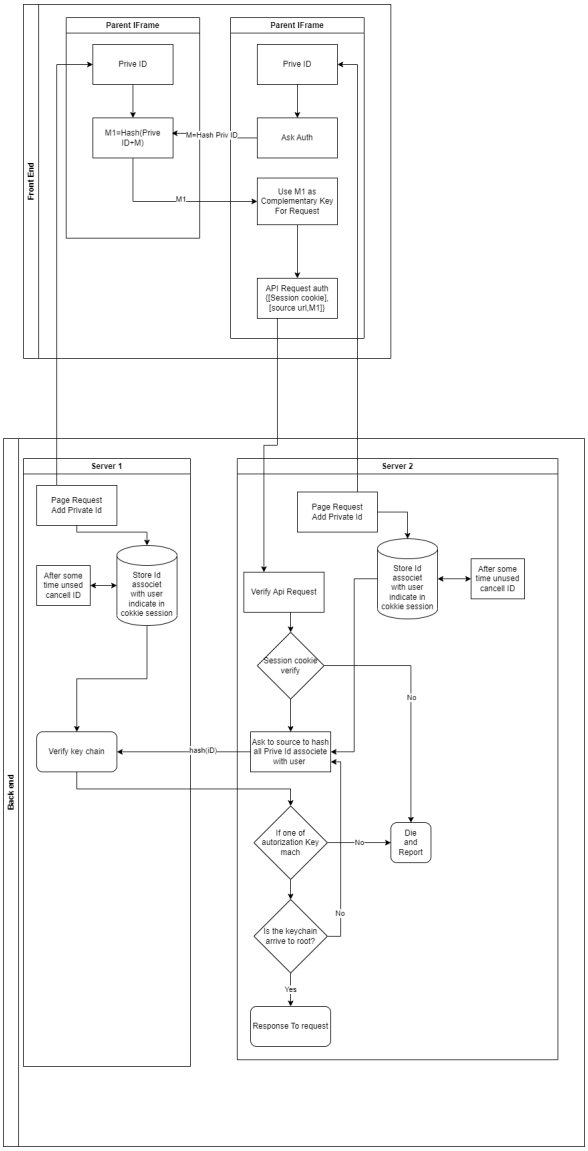


Figura 8.6: Esempio di key chain

Ad ogni richiesta di una qualsiasi pagina viene aggiunta una stringa casuale, questa rappresenta l'Id della pagina e tramite una struttura a catena basata su hash si correlano i vari Id delle pagine agli Id dei frame padre.

Il frame principale non potrà essere inserito in un frame e quindi un attacco come quello descritto in figura 4 non è possibile da attuare poichè non si riuscirebbe a chiudere la catena sull'elemento iniziale.

Si noti quindi che l'elemento padre ricopre un ruolo più importante degli altri in quanto potrebbe compromettere l'intera catena.

8.3 Separazione back-end

Avendo attuato una politica come quella descritta precedentemente possiamo quindi passare a separare i dati nella pagina con la sua composizione separando in maniera netta la struttura della pagina (ovvero i vari tag HTML) dai dati.
Questo comporta numerosi vantaggi quali la possibilità di eseguire/implementare una politica di cache per tutte le varie pagine html, css, javascript ecc.. consentendo quindi uno aumento delle performance percepite dall'utente e allo stesso tempo ridurre il carico di lavoro per il nostro/i server.
Una volta definita la pagina caricata la pagina vuota sarà poi compito di null'altro script andarla a popolare. Per farlo quest'ultimo dovrà eseguire una chiamata fetch verso le api specifiche per popolare quella determinata pagina.
Le api risponderanno con un oggetto json che opportunamente parsato dal javascript permetterà di introdurre il contenuto.
esempio di codice per l'implementazione di tale politica

```
  async function fetchProfiles() {
   try {
      const apiUrl = 'http://localhost/sito/ProfiliSuggeriti/Prendidati.php'
      const response = await fetch('apiUrl');
      const profiles = await response.json();
      displayProfiles(profiles);
   } catch (error) {
      console.error('Errore nel recupero dei profili suggeriti:', error);
   }
}

function checkLink(url) {
   return new Promise((resolve, reject) => {
      const xhr = new XMLHttpRequest();
      xhr.open('HEAD', url, true);
      xhr.onreadystatechange = () => {
         if (xhr.readyState === 4) {
            if (xhr.status === 200) {
               resolve(true);
```

```
            } else {
               reject(false);
            }
         }
      };
      xhr.send(null);
   });
}

function displayProfiles(profiles) {
   const container = document.getElementById('suggested-profiles-container');

   profiles.forEach(profile => {
      const profileDiv = document.createElement('div');
      profileDiv.className = 'profile';

      const name = document.createElement('h3');
      name.textContent = profile.name;
      profileDiv.appendChild(name);

      const description = document.createElement('p');
      description.textContent = profile.description;
      profileDiv.appendChild(description);

      const referenceTypes = ['website', 'youtubeChannel',
       'telegram', 'twitch', 'github', 'linkedin', 'discord'];

      referenceTypes.forEach(referenceType => {
         if (profile[referenceType]) {
            const reference = document.createElement('p');
            const referenceLink = document.createElement('a');
            // Imposta l'attributo href per evitare il comportamento
            // di default
            referenceLink.href = '';
            referenceLink.textContent = referenceType[0].toUpperCase() +
            referenceType.slice(1);
            // Aggiungi un listener per l'evento 'click'
```

```
            referenceLink.addEventListener('click', () => {
               sendMessageToParent("link external",profile[referenceType]);
            });
            reference.appendChild(referenceLink);
            profileDiv.appendChild(reference);
         }
      });

      container.appendChild(profileDiv);
   });
}
```

8.4 Vantaggi

L'utilizzo di questa metodologia consente un ottimale monitoraggio dello stato del sistema, ne implementa la sua scalabilità e consente l'isolamento degli errori.
Inoltre consente di prevenire CSS e XSS poiché i dati vengono sanificati front all'inserimento nella pagina end tramite *textContent* e gli script e tutti gli altri dati sono statici ben contrassegnati tramite Hash e anche le pagine in se sono statiche la cui integrità può essere controllata tramite hash anche da dei programmi di antivirus che dovrebbero essere presenti sul server.
Avendo suddiviso quindi le richieste e avendo già spiegato come verificare l'integrità dei file che compongono il front end non ci resta che verificare le api del back-end. Per farlo si può utilizzare o creare software per la verifica delle richieste api perché facilmente intellegibili e interpretabili da una macchina.
Una verifica delle richieste, le quali rispondevano in maniera mista tra html javascript e dati risultava estremante complesso e polinomiale, utilizzando il metodo descritto la complessità di analisi diventa quasi lineare poiché le interazioni tra i vari frame devono essere estremamente contenute e comunque ben specificate sia lato del lato dell'iframe richiedente sia lato del Gestore.
Per quanto riguarda le richieste REST/api anch'esse devono essere molto leggere e contenute.
Si sottolinea inoltre che una politica così modulare consente il riuso dei frame in vari contesti nell'intero sito garantendo le stesse proprietà poichè limitate dai sui margini.
Infine vi è la possibilità di eseguire un approccio ricorsivo di iframe in cui è possibile annidare in un iframe altri iframe in modo da ottenere una struttura di segregazione più granulare.

8.5 Svantaggi

Questo sistema presenta anche alcuni svantaggi, comunque risolvibili o mitigabili ma che sono da tenere in considerazione.

- una numero di richieste http più alte anche se indirizzate a diverse pagine
- gli iframe isolano i contesti quindi anche il semplice scroll del mouse viene letto dal frame sul quale si trova il cursore. Questo è aggirabile tramite un passaggio di valori dall'iframe al Gestore in cui si passa il valore di scorrimento del mouse e poi lui decide rispondendo ai vari frame una politica di scroll.
- è necessario impostare lato server Access-Control-Allow-Origin molto lasca poichè un iframe invierà le richiesta anonime e quindi con Access-Control-Allow-Origin=null. Questo consentirà anche ad altri siti di inglobale i nostri iframe nel loro sito. (Non avendo comunque accesso ai dati, Potenziale problema per una campagna di phishing, anche se ricreare solo nell'aspetto una pagina identica per un attaccante non sarebbe un problema)
- bisogna abilitare le richieste da origine null, quindi sarebbe possibile tramite una pagina falsa di phishing magari inserita all'interno di un nostro server compromesso facendo si che l'utente cliccandovi apra la possibilità ad un attaccante di fare le richieste dalla sua pagina falsificata ai nostri server REST. Per Evitare questo tipo di situazioni è necessario inserire un identificatore univoco nel Frame principale al momento della sua richiesta e limitare che questo sia possibile inserirlo in un Iframe. Questo metodo di risoluzione inoltre comporta il poter mappare l'apertura di varie tab che condividerebbero il token di autenticazione.
- La struttura a key chain è suscettibile ad attacchi man-in-the-middle, se l'attaccante riuscisse a inserire uno script all'interno di un nostro iframe, potrebbe recuperare l'ID della pagina e ridire il suo valore verso la sua finta pagina, portando a successo un attacco simile a quello mostrato in figura 8.5

8.6 Sviluppi futuri

Sarebbe bello poter utilizzare questa metodologia in maniera più efficiente e per farlo i Browser dovrebbero disporre di metodi a grana più fine per la valutazione dei permessi.
Ad esempio l'allentamento dell'origin null comporterebbe numerosi vantaggi come il non doversi preoccupare della catena delle chiamate poiché questo processo sarebbe controllato dal browser tramite l'attributo origin definito lato server.
Anche il sandbox gioverebbe di una grana più fine in cui sarebbe permesso specificare specifici javascript invece che tutti, o anche integrare il controllo di integrità di un iframe tramite hash sarebbe un ottimo passo per ottenere un maggior rafforzamento dei servizi web.

Capitolo 9

Verifica e suggerimenti

Si suggerisce di procedere ad ristrutturazione del codice attua ad ristrutturare l'applicativo ArchiMed:

- Separare il sistema back-end di accesso ai dati con il sistema di visualizzazione degli stessi in modo da poter eseguire test mirati a valutare in modo dettagliato l'accesso l'integrità e la disponibilità dei dati. Questo può essere fatto creando due differenti "Siti" dove:

  il primo contiene il servizio di accesso e gestione dei dati accessibili tramite chiamate REST, dove viene mostrato soltanto il dato

  il secondo contiene le pagine Html che dovranno eseguire le chiamate al primo servizio per popolare il soro contenuto.

  Questo processo è essenziale perché andare a costruire un meta-modello che possa implementare oltre a la verifica statica delle chiamate/risposte al servizio REST anche la valutazione dinamica delle chiamate eseguite tramite Javascript in run-time risulta estremamente complesso

- implementare all'interno dei processi di gestione del ciclo di vita del software l'attuazione di un sistema di penetration testing per migliorare il sistema di controllo post produzione esplicitato nel allegato 1 del MDR

- introducendo per ogni pagina una gestione tramite classi e metodi

- separare i file PHP dai file html la dove possibile

- come un applicativo web costruito dall'unione di una moltitudine di micro-servizi attuati tramite una strategia di iframe annidati utilizzando la proprietà sandbox. Quest'ultima

permetterebbe di ottenere un elevato grado di safety e secure in quanto scinderebbe la possibilità che un errore/malformazione di una parte del servizio si possa propagare anche su altre parti del sito.

Preso in considerazione il contesto organizzativo e l'importanza dell'applicativo all'interno del quadro aziendale nonché in conformità con le linee guida AGID[1] di implementare al più presto la politica di gestione del ciclo di vita del software come descritta nell'allegato A.
Si suggerisce, in conformità alle linee guida AGID [**Dan**], di determinare un piano di attuazione costante di penetration test al fine di valutare l'esistenza di problematiche gravi e oggettive che portino un grave danno a discapito sia dell'azienda che alle libertà degli individui.
Si suggerisce

9.1 Proposte db

Propongo di incrementare le attuali politiche d'implementazione delle query al database tramite Remote Procedure Call [10].
Dato che ad ora le query al db vengono effettuate mediante l'utilizzo di un apposita classe definita all'interno del codice PHP che esplicita sotto forma di stringa le query che possono essere effettuate, la loro trasposizione in PROCEDURE non risulterebbe particolarmente onerosa.
Questo comporta una serie di vantaggi, quali:

+ La riduzione delle dimensioni dei dati trasferiti sulla rete
+ Blindando l'utilizzo delle sole procedure si incrementano le garanzie in termini di integrità dei dati, in quanto si impedisce l'utilizzo delle singole query insert update e delete incontrollate sul database.
+ Diminuzione del carico di lavoro sul server spostando parte della computazione sul db
+ Dialogo e sanificazione degli input effettuato anche sul database
+ Doppia fonte di tracciamento delle richieste al db
+ Tramite l'utilizzo di canary tuple sarebbe possibile avere un indicatore di compromissione bloccando le scritture e attuando operazioni in emergenza. Prevenzione da ramsoware

Tutto ciò contribuirebbe significativamente ad implementare misure di sicurezza descritte negli standard, regolamentazioni, direttive e suggerimenti previsti per il software in questione.

- Privilegio minimo
- Definizione e Tracciamento delle interfacce
- Definizione dei metodi di accesso

Sarebbe molto utile inoltre aggiungere dei dati sintetici al fine di avere degli indicatori di compromissione.
Di fatti questa strategia e risulta molto efficace nella cyber deception, andando a rallentare un attore malevolo nell'esfiltrare le informazioni o nel cifrarle (Caso ramsoware), poiché a seguito di un alert del genere sarebbe possibile invalidare le credenziali dell'utente che ha scatenato quell'alert.
Ma la cosa più importante da evidenziare è la scomposizione del database, ovvero scindere i vari DB in modo da poter avere una resilienza più elevata.

9.2 Autenticazione e validazione degli accessi

Sarebbe altresì utile e estremamente integrabile e versatile implementare un sistema di autenticazione centralizzato non sarebbe utile solo per questo applicativo (anche con la scissione in microservizi). Di fatti un sistema Kerberos porterebbe a una semplificazione per gli utenti nel modello di accesso e incrementerebbe anche il livello di sicurezza poiché potrebbe essere integrato con un sistema Siem per la gestione degli accesso.

Ex.. Un utente che è contemporaneamente connesso da diverse postazioni, soprattutto se fisse non dovrebbe essere possibile (condivisione delle credenziali)

Capitolo 10

Allegati

RISK ASSESSMENT AND SECURITY MEASURE FOR PERSONAL DATA PROCESSING

Assessment of the level of risk for processing operation **Trattamento dati in** and a proposal for appropriate technical and organizational security measures.

Section I – Definition and Context of the Processing Operation

PROCESSING OPERATION DESCRIPTION	ANSWER	
Personal Data Processed	Dati sanitari, Dati personali	
Processing Purpose	Uso medico	
Data Subject	clienti	
Processing Means		
Recipients of Personal Data	Internal	Medici
	External	
	Internal	Infermieri
	Internal	OSS
Data Processor Used	Trattamento in UE	

Section II – Evaluation of the Impact

Confidentiality impact assessment: **Very High**

Poichè per portare a termine lo scopo di cure il sistema tratta e/o può trattare:
- immagini di parti del corpo sessuali.
- Dati sanitari
- Indirizzi di recapiti
- Informazioni sulla persona (come CF, nazzionalità, data di nascita, livello di instruzione)
- Informazioni sulle relazioni sociali

Integrity impact assessment: **Very High**

È stato modificato un record importante per l'accuratezza della cartella di un individuo in un servizio medico online.
L'accuratezza del dato può portare a una terapia erronea che porti anche alla morte del paziente come dati sulle allergie del paziente

Availability impact assessment: **Very High**

Un servizio critico (es. cartella clinica online) è inattivo e non può essere recuperato immediatamente

IMPACT ASSESSMENT		
Confidentiality	**Integrity**	**Availability**
Very High	Very High	Very High
	Overall Impact Evaluation	Very High

Section III – Analysis of the Threats per Assessment Area

Network and Technical Resources threat probability: Medium

- **Is any part of the processing of personal data performed through the internet? Yes**
  é un sistema gestionale integrato che interagisce con vari applicativi e deve permettere l'accesso a distanza di tali informazionei
- **Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)? Yes**
  viene fornito l'accesso a un sistema interno di elaborazione dei dati personali tramite Internet
- **Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service? Yes**
  Per sua natura un gestionale deve dialogare con gli altri applicativi
- **Can unauthorized individuals easily access the data processing environment? No**
  Datacenter con policy e garanzie in tal senso
- **Is the personal data processing system designed, implemented or maintained without following relevant documented best practices? No**
  Datacenter con policy e garanzie in tal senso

Processes/Procedures related to the processing of personal data threat probability: Medium

- **Are the roles and responsibilities with regard to personal data processing vague or not clearly defined? No**
  Esiste una policy in tal senso
- **Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined? No**
  Esistono delle policy in tal senso come l'utilizzo in rete dei soli dispositivi aziendali che abbiano ottenuto l'autorizzazione
- **Are the employees allowed to bring and use their own devices to connect to the personal data processing system? No**
- **Are the employees allowed to transfer, store or otherwise process personal data outside the premises of the organization? No**
- **Can personal data processing activities be performed without log files being created? No**
  Le azioni vengono loggate dal sistema

Parties/People involved in the processing of personal data threat probability: Low

- **Is the processing of personal data performed by an undefined number of employees? No**
  i soli dipendenti autorizzati ad accedere al sistema posso trattare i dati, vi è un record di persone autorizzate
- **Is any part of the data processing operation performed by a contractor/third party (data processor)? No**
  azienda utilizza una soluzione Platform as a service
- **Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated? No**
  esiste una privacy policy

- **Is the personnel involved in the processing of personal data unfamiliar with security matters?** **No**
- **Do the persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data?** **No**
  I dati sono archiviati e gestiti dal server

Business sector and scale of processing threat probability: **Medium**

- **Do you consider your business sector as being prone to cyberattacks?** **Yes**
  È stata data pubblicità a possibili minacce alla sicurezza e vulnerabilità del particolare settore (ospedale)
- **Has your organization suffered any cyberattack or other type of security breach over the last two years?** **-**
  NON SAPREI
- **Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?** **-**
  NON SAPREI
- **Does your processing operation concern a large volume of individuals and/or personal data?** **Yes**
  é la più grande azienda ospedaliera toscana
- **Are there any security best practices specific to your business sector that have not been adequately followed?** **Yes**
  MDR, AGID

ASSESSMENT AREA	PROBABILITY	
Network and Technical Resources	Medium	2
Processes/Procedures related to the processing of personal data	Medium	2
Parties/People involved in the processing of personal data	Low	1
Business sector and scale of processing	Medium	2
Overall Threat Occurrence Probability	Medium (7)	

Section IV – Evaluation of Risk

	IMPACT LEVEL			
THREAT OCCURRENCE PROBABILITY		Low	Medium	High / Very High
	Low			
	Medium			X
	High			

Section V – Organizational Security Measures

It should be noted that the adequacy of measures to specific risk levels should not be perceived as absolute. Depending on the context of the personal data processing, the organization can consider adopting additional measures, even if they are assigned to a higher level of risk. Furthermore, the proposed list of measures does not take into account other additional sector specific security requirements, as well as specific regulatory obligations, arising for example from the ePrivacy Directive or the NIS Directive. In an attempt to further facilitate this procedure a mapping of the proposed group of measures with the ISO/IEC 27001:2013 security controls is also included.

Security policy and procedures for the protection of personal data

Measure Identifier	Measure Description	Risk level
A.1	The organization should document its policy with regards to personal data processing as part of its information security policy.	
A.2	The security policy should be reviewed and revised, if necessary, on an annual basis.	
A.3	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties	
A.4	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.	
A.5	An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy.	
A.6	The security policy should be reviewed and revised, if necessary, on a semester basis.	
	Related to ISO 27001:2013 - A.5 Security policy	

Roles and responsibilities

Measure Identifier	Measure Description	Risk level
B.1	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	
B.2	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.	
B.3	Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer.	
B.4	The security officer should be formally appointed (documented). The tasks and responsibilities of the security officer should also be clearly set and documented.	
B.5	Conflicting duties and areas of responsibility, for examples the roles of security officer, security auditor, and DPO, should considered to be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data.	
	Related to ISO 27001:2013 - A.6.1.1 Information security roles and responsibilities	

Access control policy

Measure Identifier	Measure Description	Risk level
C.1	Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle.	
C.2	An access control policy should be detailed and documented. The organization should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.	
C.3	Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented.	
C.4	Roles with excessive access rights should be clearly defined and assigned to limited specific members of staff.	
	Related to ISO 27001:2013 - A.9.1.1 Access control policy	

Resource/asset management

Measure Identifier	Measure Description	Risk level
D.1	The organization should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register could include at least the following information: IT resource, type (e.g. server, workstation), location (physical or electronic). A specific person should be assigned the task of maintaining and updating the register (e.g. IT officer).	
D.2	IT resources should be reviewed and updated on regular basis.	
D.3	Roles having access to certain resources should be defined and documented.	
D.4	IT resources should be reviewed and updated on annual basis.	
	Related to ISO 27001:2013 - A.8 Asset management	

Change management

Measure Identifier	Measure Description	Risk level
E.1	The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place.	
E.2	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.	
E.3	A detailed and documented change policy should be in place. It should include: a process for introducing changes, the roles/users that have change rights, timelines for introducing changes. The change policy should be regularly updated.	
	Related to ISO 27001:2013 - A. 12.1 Operational procedures and responsibilities	

Data processors

Measure Identifier	Measure Description	Risk level
F.1	Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data controller and the data processor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy.	

Measure Identifier	Measure Description	Risk level
F.2	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay.	
F.3	Formal requirements and obligations should be formally agreed between the data controller and the data processor. The data processor should provide sufficient documented evidence of compliance.	
F.4	The data controller's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.	
F.5	The employees of the data processor who are processing personal data should be subject to specific documented confidentiality/ non-disclosure agreements.	
	Related to ISO 27001:2013 - A.15 Supplier relationships	

Incidents handling / Personal data breaches

Measure Identifier	Measure Description	Risk level
G.1	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.	
G.2	Personal data breaches should be reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. 33 and 34 GDPR.	
G.3	The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.	
G.4	Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.	
	Related to ISO 27001:2013 - A.16 Information security incident management	

Business continuity

Measure Identifier	Measure Description	Risk level
H.1	The organization should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).	
H.2	A BCP should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles.	
H.3	A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.	
H.4	Specific personnel with the necessary responsibility, authority and competence to manage business continuity in the event of an incident/personal data breach should be nominated.	
H.5	An alternative facility should be considered, depending on the organization and the acceptable downtime of the IT system.	
	Related to ISO 27001:2013 - A. 17 Information security aspects of business continuity management	

Confidentiality of personnel

Measure Identifier	Measure Description	Risk level
I.1	The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process.	
I.2	Prior to up taking their duties employees should be asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements.	
I.3	Employees involved in high risk processing of personal data should be bound to specific confidentiality clauses (under their employment contract or other legal act).	
	Related to ISO 27001:2013 - A.7 Human resource security	

Training

Measure Identifier	Measure Description	Risk level
J.1	The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.	
J.2	The organization should have structured and regular training programmes for staff, including specific programmers for the induction (to data protection matters) of newcomers.	
J.3	A training plan with defined goals and objectives should be prepared and executed on an annual basis.	
	Related to ISO 27001:2013 - A.7.2.2 Information security awareness, education and training	

Access control and authentication

Measure Identifier	Measure Description	Risk level
K.1	An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.	
K.2	The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.	
K.3	An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.	
K.4	The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity.	
K.5	A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.	
K.6	User passwords must be stored in a "hashed" form.	
K.7	Two-factor authentication should preferably be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.	
K.8	Device authentication should be used to guarantee that the processing of personal data is performed only through specific resources in the network.	
	Related to ISO 27001:2013 - A.9 Access control	

Logging and monitoring

Measure Identifier	Measure Description	Risk level
L.1	Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion).	
L.2	Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronised to a single reference time source	
L.3	Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.	
L.4	There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity.	
L.5	A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.	
	Related to ISO 27001:2013 - A.12.4 Logging and monitoring	

Server/Database security

Measure Identifier	Measure Description	Risk level
M.1	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.	
M.2	Database and applications servers should only process the personal data that are actually needeeds to process in order to achieve its processing purposes.	
M.3	Encryption solutions should be considered on specific files or records through software or hardware implementation.	
M.4	Encrypting storage drives should be considered	
M.5	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information	
M.6	Techniques supporting privacy at the database level, such as authorized queries, privacy preserving data base querying, searchable encryption, etc., should be considered.	
	Related to ISO 27001:2013 - A. 12 Operations security	

Workstation security

Measure Identifier	Measure Description	Risk level
N.1	Users should not be able to deactivate or bypass security settings.	
N.2	Anti-virus applications and detection signatures should be configured on a weekly basis.	
N.3	Users should not have privileges to install or deactivate unauthorized software applications.	
N.4	The system should have session time-outs when the user has not been active for a certain time period.	
N.5	Critical security updates released by the operating system developer should be installed regularly.	
N.6	Anti-virus applications and detection signatures should be configured on a daily basis.	
N.7	It should not be allowed to transfer personal data from workstations to external storage devices (e.g. USB, DVD, external hard drives).	
N.8	Workstations used for the processing of personal data should preferably not be connected to the Internet unless security measures are in place to prevent unauthorised processing, copying and transfer of personal data on store.	
N.9	Full disk encryption should be enabled on the workstation operating system drives	

Measure Identifier	Measure Description	Risk level
	Related to ISO 27001:2013 - A. 14.1 Security requirements of information systems	

Network/Communication security

Measure Identifier	Measure Description	Risk level
O.1	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).	
O.2	Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.	
O.3	Remote access to the IT system should in general be avoided. In cases where this is absolutely necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g. IT administrator/security officer) through pre-defined devices.	
O.4	Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.	
O.5	Connection to the internet should not be allowed to servers and workstations used for the processing of personal data.	
O.6	The network of the information system should be segregated from the other networks of the data controller.	
O.7	Access to the IT system should be performed only by pre-authorized devices and terminal using techniques such as MAC filtering or Network Access Control (NAC)	
	Related to ISO 27001:2013 - A.13 Communications Security	

Back-ups

Measure Identifier	Measure Description	Risk level
P.1	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.	
P.2	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.	
P.3	Execution of backups should be monitored to ensure completeness.	
P.4	Full backups should be carried out regularly.	
P.5	Backup media should be regularly tested to ensure that they can be relied upon for emergency use.	
P.6	Scheduled incremental backups should be carried out at least on a daily basis.	
P.7	Copies of the backup should be securely stored in different locations.	
P.8	In case a third party service for back up storage is used, the copy must be encrypted before being transmitted from the data controller.	
P.9	Copies of backups should be encrypted and securely stored offline as well.	
	Related to ISO 27001:2013 - A.12.3 Back-Up	

Mobile/Portable devices

Measure Identifier	Measure Description	Risk level
Q.1	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.	
Q.2	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.	
Q.3	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.	
Q.4	Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.	
Q.5	The organization should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised.	
Q.6	Mobile devices should support separation of private and business use of the device through secure software containers.	
Q.7	Mobile devices should be physically protected against theft when not in use.	
Q.8	Two factor authentication should be considered for accessing mobile devices	
Q.9	Personal data stored at the mobile device (as part of the organization's data processing operation) should be encrypted.	
	Related to ISO 27001:2013 - A. 6.2 Mobile devices and teleworking	

Application lifecycle security

Measure Identifier	Measure Description	Risk level
R.1	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.	
R.2	Specific security requirements should be defined during the early stages of the development lifecycle.	
R.3	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.	
R.4	Secure coding standards and practises should be followed.	
R.5	During the development, testing and validation against the implementation of the initial security requirements should be performed.	
R.6	Vulnerability assessment, application and infrastructure penetration testing should be performed by a trusted third party prior to the operational adoption. The application shall not be adopted unless the required level of security is achieved.	
R.7	Periodic penetration testing should be carried out.	
R.8	Information about technical vulnerabilities of information systems being used should be obtained.	
R.9	Software patches should be tested and evaluated before they are installed in an operational environment.	
	Related to ISO 27001:2013 - A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes	

Data deletion/disposal

Measure Identifier	Measure Description	Risk level
S.1	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed.	

Measure Identifier	Measure Description	Risk level
S.2	Shredding of paper and portable media used to store personal data shall be carried out.	
S.3	Multiple passes of software-based overwriting should be performed on all media before being disposed.	
S.4	If a third party's services are used to securely dispose of media or paper based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate.	
S.5	Following the software erasure, additional hardware based measures such as degaussing should be performed. Depending on the case, physical destruction should also be considered.	
S.6	If a third party, therefor data processor, is being used for destruction of media or paper based files, it should be considered that the process takes place at the premises of the data controller (and avoid off-site transfer of personal data.	
	Related to ISO 27001:2013 - A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment	

Physical security

Measure Identifier	Measure Description	Risk level
T.1	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.	
T.2	Clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the organization should be established, as appropriate.	
T.3	Secure zones should be defined and be protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored	
T.4	Intruder detection systems should be installed in all security zones.	
T.5	Physical barriers should, where applicable, be built to prevent unauthorized physical access.	
T.6	Vacant secure areas should be physically locked and periodically reviewed	
T.7	An automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room	
T.8	External party support service personnel should be granted restricted access to secure areas.	
	Related to ISO 27001:2013 - A.11 – Physical and environmental security	

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 1
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 2
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 · **Misure Minime AgID** ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6 · **Misure Minime AgID** ABSC 13.1.1, 13.2.1
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11 · **D.Lgs. 18/5/2018 n. 65** Art. 16(2)-(4) · **Misure Minime AgID** ABSC 5.2.1, 5.4, 5.10, 8.11.1
		DP-ID.AM-7: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	· **GDPR** - Artt. 24, 26-29, 37-39 · **D.Lgs. 30/6/2003 n. 196** Artt. 2-quaterdecies, 2-quinquiesdecies, 2-sexiesdecies · **ISO/IEC 29100:2011** 4.2, 4.3, 5.10
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati	· **GDPR** - Art. 30 · **ISO/IEC 29100:2011** 4.4
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	**ID.BE-1:** Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 4** PM-8 · **D.Lgs. 18/5/2018 n. 65** Art. 4
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio)	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-1:** È indetificata e resa nota una policy di cybersecurity	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families · **D.Lgs. 18/5/2018 n. 65** Artt. 13(2), 15(2)
		ID.GV-2: Ruoli e responsabilità inerenti la cybersecurity sono coordinati ed allineati con i ruoli interni ed i partner esterni	· **CIS CSC** 19 · **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families · **D.Lgs. 18/5/2018 n. 65** Art. 1-11 · **GDPR** - Artt. 5-11 · **D.Lgs. 30/6/2003 n. 196** Artt. 2-ter, 2-quater, 2-quinquies, 2-sexies, 2-septies, 2-octies, 2-novies, 2-decies · **ISO/IEC 29100:2011** 4.5.1, 5.3
		ID.GV-4: La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1), 14(1)
		ID.RA-1: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 · **Misure Minime AgID** ABSC 4.1.1, 4.1.2, 4.6.1
		ID.RA-2: L'organizzazione riceve informazioni su minacce, vulnerabilità ed altri dati configurabili come Cyber Threat Intelligence da fonti esterne (e.g. CERT, fonti aperte, forum di information sharing)	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16 · **Misure Minime AgID** ABSC 4.4.2
		ID.RA-3: Le minacce, sia interne che esterne, sono identificate e documentate	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2

			· **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-4:** Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11 · **Misure Minime AgID** ABSC 4.8.1
		ID.RA-5: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	· **CIS CSC** 4 · **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16 · **Misure Minime AgID** ABSC 4.8.1
		ID.RA-6: Sono identificate e prioritizzate le risposte al rischio	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9
		DP-ID.RA-7: Viene effettuata una valutazione di impatto sulla protezione dei dati personali	· **GDPR** - Artt. 35, 36 · **ISO/IEC 29100:2011** 4.5 · **ISO/IEC 29134:2017**
	Risk Management Strategy (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale.	**ID.RM-1:** I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili dell'organizzazione (c.d. stakeholder)	· **CIS CSC** 4 · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 · **NIST SP 800-53 Rev. 4** PM-9 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1), 14(1), 14(13)
		ID.RM-2: Il rischio tollerato dall'organizzazione è identificato ed espresso chiaramente	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** PM-9 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1), 14(1), 14(13)
		ID.RM-3: Il rischio tollerato è determinato tenendo conto del ruolo dell'organizzazione come infrastruttura critica e dei rischi specifici presenti nel settore industriale di appartenenza	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1), 14(1), 14(13)
	Supply Chain Risk Management (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.	**ID.SC-1:** I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: I contratti con i fornitori e i partner terzi sono utilizzati per realizzare appropriate misure progettate per rispettare gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Fornitori e partner terzi sono regolarmente valutati utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: La pianificazione e la verifica della risposta e del ripristino sono condotti con i fornitori e i partner terzi	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
	Data Management (DP-ID.DM): i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.	**DP-ID.DM-1:** Il ciclo di vita dei dati è definito e documentato	· **GDPR** - Art. 5,6,9-11, 30
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati	· **GDPR** - Artt. 12-14 · **ISO/IEC 29100:2011** 5.2, 5.8 · **ISO/IEC 29151:2017** A.3, A.9 · **ISO/IEC 27018:2014** A.1, A.7
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati	· **GDPR** - Artt. 7, 8 · **D.Lgs. 30/6/2003 n. 196** Art. 2-quinquies · **ISO/IEC 29100:2011** 5.2 · **ISO/IEC 29151:2017** A.3 · **ISO/IEC 27018:2014** A.1
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato	· **GDPR** - Art 15-22 · **D.Lgs. 30/6/2003 n. 196** Art. 2-terdecies · **ISO/IEC 29100:2011** 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 · **ISO/IEC 29151:2017** A.5, A.6, A.7, A.8, A.9, A.10 · **ISO/IEC 27018:2014** A.3, A.4, A.5, A.6, A.7, A.8
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale	· **GDPR** - Artt. 44-49 · **ISO/IEC 29100:2011** 4.5
		PR.AC-1: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte a audit sicurezza	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.6.1, 5.7, 5.8.1, 5.11 · **GDPR** - Artt. 25, 32 · **ISO/IEC 29100:2011** 5.11
		PR.AC-2: L'accesso fisico alle risorse è protetto e amministrato	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.11.2, 10.4.1 · **GDPR** - Art. 32

			· **ISO/IEC 29100:2011** 5.11
		PR.AC-3: L'accesso remoto alle risorse è amministrato	· **CIS CSC** 12 · **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.4.1, 8.3.2 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
	Identity Management, Authentication and Access Control (PR.AC): L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.1.1, 5.1.2, 5.1.3, 13.9.1 · **GDPR** - Artt. 25, 32 · **ISO/IEC 29100:2011** 5.11
		PR.AC-5: L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	· **CIS CSC** 9, 14, 15, 18 · **COBIT 5** DSS01.05, DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 13.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.AC-6: Le identità sono comprovate, associate a credenziali e verificate durante le interazioni	· **CIS CSC**, 16 · **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 · **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.AC-7: Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)	· **CIS CSC** 1, 12, 15, 16 · **COBIT 5** DSS05.04, DSS05.10, DSS06.10 · **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 · **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
	Awareness and Training (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti	**PR.AT-1:** Tutti gli utenti sono informati e addestrati	· **CIS CSC** 17, 18 · **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 · **NIST SP 800-53 Rev. 4** AT-2, PM-13 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 8.7.2, 8.7.3, 8.7.4
		PR.AT-2: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	· **CIS CSC** 5, 17, 18 · **COBIT 5** APO07.02, DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.2.1, 5.6.1, 5.7.1, 5.7.2, 5.7.3, 5.7.6, 5.8.1, 5.9.1, 5.10.3, 5.10.4, 5.11.1
		PR.AT-3: Tutte le terze parti (es. fornitori, clienti, partner) comprendono i loro ruoli e responsabilità	· **CIS CSC** 17 · **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13)
		PR.AT-4: I dirigenti ed i vertici aziendali comprendono i loro ruoli e responsabilità	· **CIS CSC** 17, 19 · **COBIT 5** EDM01.01, APO01.02, APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13)
		PR.AT-5: Il personale addetto alla sicurezza fisica e alla cybersecurity comprende i suoi ruoli e responsabilità	· **CIS CSC** 17 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13)
		PR.DS-1: I dati memorizzati sono protetti	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 13.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-2: I dati sono protetti durante la trasmissione	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, DSS05.02, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.3.2 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
			· **CIS CSC** 1 · **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1

PROTECT (PR)	**Data Security (PR.DS):** I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-3:** Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale	· **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-4: I sistemi hanno adeguate risorse a disposizione per poter garantire la disponibilità	· **CIS CSC** 1, 2, 13 · **COBIT 5** APO13.01, BAI04.04 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	· **CIS CSC** 13 · **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.12.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 13.2.1, 13.7.1, 13.8.1, 13.9.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-6: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	· **CIS CSC** 2, 3 · **COBIT 5** APO01.06, BAI06.01, DSS06.02 · **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** SC-16, SI-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.5.1, 3.5.2, 10.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 4.10.1, 8.2.3
		PR.DS-8: Sono impiegati meccanismi di controllo dell'integrità per verificare l'integrità del hardware	· **COBIT 5** BAI03.05 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISO/IEC 27001:2013** A.11.2.4 · **NIST SP 800-53 Rev. 4** SA-10, SI-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.	**PR.IP-1:** Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	· **CIS CSC** 3, 9, 11 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.1.1, 3.1.2, 3.2.1, 5.3.1, 8.4 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-2: Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle).	· **CIS CSC** 18 · **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.1.3, 3.2.2, 3.3 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-3: Sono attivi processi di controllo della modifica delle configurazioni	· **CIS CSC** 3, 11 · **COBIT 5** BAI01.06, BAI06.01 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.2.3, 3.5.3, 3.5.4, 3.6.1, 3.7.1, 5.4, 8.2.1, 8.2.2 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-4: I backup delle informazioni sono eseguiti, amministrati e verificati	· **CIS CSC** 10 · **COBIT 5** APO13.01, DSS01.01, DSS04.07 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.1, 10.2.1, 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-5: Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-6: I dati sono distrutti in conformità con le policy	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 5, 17, 32 · **ISO/IEC 29100:2011** 5.11
			· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8

		PR.IP-7: I processi di protezione sono sottoposti a miglioramenti	· **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa	· **COBIT 5** BAI08.04, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro	· **CIS CSC** 19 · **COBIT 5** APO12.06, DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-10: I piani di risposta e recupero a seguito di incidenti/disastri sono verificati nel tempo	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-11: Le problematiche inerenti la cybersecurity sono incluse nei processi di gestione del personale (es: screening, deprovisioning)	· **CIS CSC** 5, 16 · **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità	· **CIS CSC** 4, 18, 20 · **COBIT 5** BAI03.10, DSS05.01, DSS05.02 · **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 4.7, 4.8, 4.9.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 4.5, 8.2.2
		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.4.1, 8.2.2
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	**PR.PT-1:** Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16 · **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Family · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.5.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.PT-2: I supporti di memorizzazione removibili sono protetti ed il loro uso è ristretto in accordo alle policy	· **CIS CSC** 8, 13 · **COBIT 5** APO13.01, DSS05.02, DSS05.06 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.9.1, 8.7.1, 8.8.1, 13.5 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.PT-3: Viene adottato il principio di minima funzionalità configurando i sistemi in modo che forniscano solo le funzionalità necessarie	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.1.1, 5.1.2, 5.1.3, 5.9.1, 8.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.PT-4: Le reti di comunicazione e controllo sono protette	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.9.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1

		che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	· **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
DETECT (DE)	**Anomalies and Events (DE.AE):** Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.	**DE.AE-1:** Sono definite, rese note e gestite delle pratiche di riferimento (c.d. baseline) inerenti l'utilizzo della rete ed i flussi informativi attesi per utenti e sistemi	· **CIS CSC** 1, 4, 6, 12, 13, 15, 16 · **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4 · **Misure Minime AgID** ABSC 5.1.4, 5.5.1, 8.3.2, 13.3.1
		DE.AE-2: Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 · **Misure Minime AgID** ABSC 8.1.3
		DE.AE-4: Viene determinato l'impatto di un evento	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Vengono definite delle soglie di allerta per gli incidenti	· **CIS CSC** 6, 19 · **COBIT 5** APO12.06, DSS03.01 · **ISA 62443-2-1:2009** 4.2.3.10 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 · **Misure Minime AgID** ABSC 5.5.1
	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-1:** Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	· **CIS CSC** 1, 7, 8, 12, 13, 15, 16 · **COBIT 5** DSS01.03, DSS03.05, DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 · **D.Lgs. 18/5/2018 n. 65** Art. 14(2)-(3) · **Misure Minime AgID** ABSC 5.5.1, 8.1.2, 8.1.3, 8.5.1, 8.6.1, 8.9, 8.10.1, 13.4.1, 13.6, 13.7.1, 13.8.1
		DE.CM-2: Viene svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity	· **COBIT 5** DSS01.04, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 · **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20 · **D.Lgs. 18/5/2018 n. 65** Art. 14(2)-(3)
		DE.CM-3: Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity	· **CIS CSC** 5, 7, 14, 16 · **COBIT 5** DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 · **D.Lgs. 18/5/2018 n. 65** Art. 14(2)-(3) · **Misure Minime AgID** ABSC 5.2
		DE.CM-4: Il codice malevolo viene rilevato	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8 · **Misure Minime AgID** ABSC 8.1.1, 8.2.2, 8.2.3, 8.5, 8.6.1, 8.7.2, 8.7.3, 8.7.4, 8.8.1, 8.9, 8.10.1, 8.11.1
		DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	· **CIS CSC** 7, 8 · **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44 · **Misure Minime AgID** ABSC 8.1.1
		DE.CM-6: Viene svolto il monitoraggio delle attività dei service provider esterni per rilevare potenziali eventi di cybersecurity	· **COBIT 5** APO07.06, APO10.05 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4 · **D.Lgs. 18/5/2018 n. 65** Art. 14(9)
		DE.CM-7: Viene svolto il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 · **Misure Minime AgID** ABSC 5.8.1, 8.3
		DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	· **CIS CSC** 4, 20 · **COBIT 5** BAI03.10, DSS05.01 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5 · **Misure Minime AgID** ABSC 4.1, 4.2, 4.3, 4.4.1, 4.6.1
	Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	**DE.DP-1:** Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	· **CIS CSC** 19 · **COBIT 5** APO01.02, DSS05.01, DSS06.03 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14 · **Misure Minime AgID** ABSC 8.2.1
		DE.DP-2: Le attività di monitoraggio soddisfano tutti i requisiti applicabili	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: I processi di monitoraggio vengono testati	· **COBIT 5** APO13.02, DSS05.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14 · **D.Lgs. 18/5/2018 n. 65** Art. 14(2)-(3)
		DE.DP-4: L'informazione relativa agli eventi rilevati viene comunicata	· **CIS CSC** 19 · **COBIT 5** APO08.04, APO12.06, DSS02.05 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 · **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: I processi di monitoraggio sono oggetto di periodici miglioramenti e perfezionamenti	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6

			· **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati.	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	· **CIS CSC** 19 · **COBIT 5** APO12.06, BAI01.10 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8 · **GDPR** Art. 33
	Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**RS.CO-1:** Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	· **CIS CSC** 19 · **COBIT 5** EDM03.02, APO01.02, APO12.03 · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 · **D.Lgs. 18/5/2018 n. 65** Art. 9(2) · **Misure Minime AgID** ABSC 8.1.3
		RS.CO-2: Sono stabiliti dei criteri per documentare gli incidenti	· **CIS CSC** 19 · **COBIT 5** DSS01.03 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(7), 14(5)
		RS.CO-3: Le informazioni sono condivise in maniera coerente con il piano di risposta	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Il coordinamento con le parti interessate dell'organizzazione avviene in coerenza con i piani di risposta	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: È attuata una condivisione spontanea delle informazioni con le parti interessate esterne all'organizzazione (information sharing) per ottenere una maggior consapevolezza della situazione (c.d. situational awareness)	· **CIS CSC** 19 · **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(5), 12(7)-(8), 14(4)-(5), 14(7)-(9) · **Misure Minime AgID** ABSC 8.11.1
		DP-RS.CO-6: Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati	· **GDPR** - Artt. 33, 34 · **ISO/IEC 29100:2011** 5.10 · **ISO/IEC 291510:2017** A.11 · **ISO/IEC 27018:2014** A.9.1 · **ISO/IEC 27001:2013** A.16 · **Misure Minime AgID** ABSC
	Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace riposta e supporto alle attività di ripristino.	**RS.AN-1:** Le notifiche provenienti dai sistemi di monitoraggio vengono sempre visionate e analizzate	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: Viene compreso l'impatto di ogni incidente	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(5), 12(7)-(8), 14(4)-(5), 14(7)-(9)
		RS.AN-3: A seguito di un incidente viene svolta un'analisi forense	· **COBIT 5** APO12.06, DSS03.02, DSS05.07 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Gli incidenti sono categorizzate in maniera coerente con i piani di risposta	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.	**RS.MI-1:** In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(2), 14(2)-(3) · **Misure Minime AgID** ABSC 8.1.3, 8.4
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(2), 14(2)-(3) · **Misure Minime AgID** ABSC 8.4
		RS.MI-3: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	· **CIS CSC** 4 · **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5 · **Misure Minime AgID** ABSC 4.7, 4.9.1
	Improvements (RS.IM): Le attività di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	**RS.IM-1:** I piani di risposta agli incidenti tengono in considerazione le esperienze passate (lesson learned)	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Le strategie di risposta agli incidenti sono aggiornate	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1:** Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 · **Misure Minime AgID** ABSC 3.2.2
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1:** I piani di riprisitino tengono in considerazione le esperienze passate (lesson learned)	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 · **Misure Minime AgID** ABSC 3.1.3

		RC.IM-2: Le strategie di recupero sono aggiornate	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT).	**RC.CO-1:** A seguito di un incidente vengono gestite le pubbliche relazioni	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: A seguito di un incidente viene ripristinata la reputazione	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Le attività di ripristino condotte a seguito di un incidente vengono comunicate alle parti interessate interne ed esterne all'organizzazione, inclusi i dirigenti ed i vertici dell'organizzazione	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4

Bibliografia

[1] Electronic Transactions Development Agency. URL: https://apt.etda.or.th/cgi-bin/listgroups.cgi?c=&v=Italy&s=Healthcare&m=&x.

[2] AGID. *LINEE GUIDA PER L'ADOZIONE DI UN CICLO DI SVILUPPO DI SOFTWARE SICURO*. URL: https://www.sicurezzait.gov.it/cyber/pdf/Allegato%201-%20Linee%20Guida%20per%20l%E2%80%99adozione%20di%20un%20ciclo%20di%20sviluppo%20di%20software%20sicuro.pdf (visitato il 2020).

[3] AGID. *Linee Guida per la configurazione per adeguare la sicurezza del software di base*. URL: https://www.sicurezzait.gov.it/cyber/pdf/Allegato%203%20-%20Linee%20Guida%20per%20la%20configurazione%20per%20adeguare%20la%20sicurezza%20del%20software%20di%20base.pdf (visitato il 2020).

[4] AGID. *LINEE GUIDA PER LA MODELLAZIONE DELLE MINACCE ED INDIVIDUAZIONE DELLE AZIONI DI MITIGAZIONE CONFORMI AI PRINCIPI DEL SECURE/PRIVACY BY DESIGN*. URL: https://www.sicurezzait.gov.it/cyber/pdf/Allegato%204%20-%20Linee%20Guida%20per%20la%20modellazione%20delle%20minacce-DLT.pdf (visitato il 2020).

[5] AGID. *Linee guida per lo sviluppo sicuro*. URL: https://www.sicurezzait.gov.it/cyber/pdf/Allegato%202%20-%20Linee%20Guida%20per%20lo%20sviluppo%20sicuro%20di%20codice.pdf (visitato il 2020).

[6] AGID. *misure minime di sicurezza versione*. URL: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict (visitato il 2015).

[7] AGID. *misure minime di sicurezza versione*. URL: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict (visitato il 2017).

[8] SAPIENZA CINI. *Framework Nazionale per la Cybersecurity*. 2022. URL: https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_v2.0_core_ITA.xlsx.

[9] PARLAMENTO EUROPEO E DEL CONSIGLIO. *Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.)* URL: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017R0745 (visitato il 2023).

[10] Oracle Corporation. *MySQL 8.0 Reference Manual; 13.2.1 CALL Statement.* URL: https://dev.mysql.com/doc/refman/8.0/en/call.html (visitato il 12/03/2022).

[11] ENISA. *Evaluating the level of risk for a personal data processing operation.* 2022. URL: https://www.enisa.europa.eu/risk-level-tool/risk.

[12] European Parliament e Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council.* of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 4 Mag. 2016. URL: https://data.europa.eu/eli/reg/2016/679/oj (visitato il 13/04/2023).

[13] *Health informatics — Information security management in health.* Standard. Milano, IT: Ente Nazionale Italiano di Unificazione, Agosto 2016. URL: https://www.sis.se/api/document/preview/920656/.

[14] *quality management system.* Standard. Geneva, CH: International Organization for Standardization, settembre 2015.

[15] MITRE. URL: https://attack.mitre.org/groups/G0016/.

[16] ncsc. URL: https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development.

[17] Giorgio Oppo. *Procedure di sviluppo software.*

[18] Teisberg EO. Porter ME. *Redefining health care creating value-based competition on results.* Boston: Harvard Business School Press, 2006.

[19] *Rapporto Clusit 2023 sulla sicurezza ICT in Italia.* URL: https://clusit.it/rapporto-clusit/#form_edl.

Elenco delle figure

Elenco delle tabelle