PROGETTO S2-L5
RISK ASSESSMENT

MARIA FLAVIA MINOTTI

ALEX FIORILLO

TRACCIA

Simulare un processo di Risk Assessment, solo Step 1 e Step 2 (tralasciando Step 3 e Step 4), seguendo **NIST SP 800-30**, per Tier 3 (considerate solo le sorgenti del Tier 3). Riutilizzate la mappa delle relazioni tra tabelle, che avete prodotto ieri, come guida.

Scenario:
L’azienda Alpha è un fornitore leader di servizi sanitari online che gestisce un'ampia infrastruttura IT che include sistemi basati su cloud, applicazioni web e dispositivi mobili.
L'azienda gestisce anche dati sanitari sensibili per i propri pazienti.

- L’organizzazione si è resa conto di essere target di un **gruppo criminale organizzato** con un buon livello di preparazione e delle significative risorse per condurre attacchi coordinati. Dai sistemi di monitoraggio, è emerso che solo questa azienda è continuamente sorvegliata dal gruppo criminale. Da ulteriori analisi, si arriva alla conclusione che il gruppo criminale vuole **esfiltrare delle informazioni all’azienda sui dati sanitari degli utenti per rivenderli, creando una persistenza all’interno dell’organizzazione e non facendosi rilevare.**
- In questo momento la sorgente delle minaccia è alla **fase di ricognizione esterna** con diversi metodi (scanning, sniffing, OSINT, sorveglianza), non si rilevano ricognizioni interne.
- L’organizzazione **non ha abilitato MFA** e **non effettua regolarmente Vulnerability Assessmen**t
- L’organizzazione tratta **informazioni personali** e il loro software deve consentire la **condivisione delle informazioni tra gli utenti**, ciò si applica alla maggior parte dei loro sistemi.
- Tutte le attività di ricognizioni sono attive, però lo **scanning e sniffing** portano a degli **impatti bassi** perché presente un firewall e WAF su cloud, invece gli effetti potrebbero essere **moderati** nella **ricerca open source o** nella **sorveglianza** di alcuni target particolari.
- Consideriamo solamente il danneggiamento degli asset dovuto a **perdita o danneggiamento degli asset informativi**, con un **impatto alto**.

Siete liberi di impostare scopo, ambito, ipotesi e vincoli per limitare l’estensione del RA. Utilizzate gli step visti a lezione e definite solamente le tabelle essenziali che vi serviranno per il calcolo finale del rischio: **• D-7 • E-5 • F-3 • F-6 • H-4 • I-5**

Ipotizzate che **l’organizzazione può accettare solamente un rischio basso per tutti gli eventi di rischio** identificati, dovuto al valore del loro asset principale «dati sanitari». Fate delle valutazioni e delle ipotesi sui prossimi passaggi da eseguire per riportare il livello di rischio ottenuto entro quello desiderato.

STEP 1: PREPARE FOR ASSESSMENT

Scopo: Procedere alla modellizzazione di un Risk Assessment relativo al solo asset dei dati sanitari detenuti dall'organizzazione. Inoltre, l'assessment si limiterà alle macro fasi **Prepare for assessment** e **Conduct Assessment** del NIST 800-30 per il solo Tier3.

Ambito: Il RA sarà limitato ai dati che sono archiviati e gestiti su cloud. Questi dati sono condivisi fra gli utenti, in particolare dipendenti e pazienti, e la condivisione delle informazioni tra gli utenti si applica alla maggior parte dei loro sistemi.

Ipotesi e Vincoli: L'azienda accetta solo un rischio residuo "Low", basso e l'intero RA si basa su una sola Threat source ovvero l'organizzazione criminale.

Sorgenti di informazioni per Threat, vulnerabilità e impatti:
Le informazioni ci vengono fornite nella traccia.

TABLE D-1: INPUTS – THREAT SOURCE IDENTIFICATION

From Tier 3: (Information system level) - Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). - Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes *via RAR*	Yes *via RAR*	Yes *via peer sharing*

STEP 2: CONDUCT ASSESSMENT

- **Identificare Fonti di Minaccia**

D-2.1 = La fonte della minaccia è di tipo avversaria e proviene dall'esterno dell'organizzazione.
Si tratta di un gruppo organizzato che cerca di sfruttare la dipendenza dell'organizzazione dalle risorse informatiche. Come possiamo vedere le caratteristiche sono Capacità, Intento e Targeting (inteso some obiettivo)

TABLE D-2: TAXONOMY OF THREAT SOURCES

Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

STEP 2: CONDUCT ASSESSMENT

- **<u>Identificare Fonti di Minaccia:</u> Capability**

HIGH= L'avversario ha un livello di competenza molto sofisticato, è ben fornito di risorse e può generare opportunità per sostenere attacchi multipli, continui e coordinati con successo.

TABLE D-3: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY CAPABILITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

STEP 2: CONDUCT ASSESSMENT

- **<u>Identificare Fonti di Minaccia:</u> Intent**

MODERATE= il gruppo criminale vuole esfiltrare delle informazioni all'azienda sui dati sanitari degli utenti per rivenderli, creando una persistenza all'interno dell'organizzazione e non facendosi rilevare.

TABLE D-4: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT

Qualitative Values	Semi-Quantitative Values		Description
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends.

STEP 2: CONDUCT ASSESSMENT

- **<u>Identificare Fonti di Minaccia:</u> Targeting**

HIGH = il gruppo criminale analizza le informazioni ottenute attraverso la ricognizione esterna per mirare in modo persistente a una specifica funzione aziendale (gestione dati), concentrandosi su informazioni specifiche di alto valore o critiche (i dati stessi).

TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

STEP 2: CONDUCT ASSESSMENT

- <u>Identificare Fonti di Minaccia</u>:

TABLE D-7: TEMPLATE – IDENTIFICATION OF ADVERSARIAL THREAT SOURCES

Identifier	Threat Source Source of Information	In Scope	Capability	Intent	Targeting
D-7-1	ADVERSARIAL - Group-Established	Yes	High	Moderate	High

STEP 2: CONDUCT ASSESSMENT

- **<u>Identificare Threat Events:</u> Eventi di minaccia avversari**

E-5-1 = ricognizione/scansione della rete perimetrale

E-5-2 = network sniffing delle reti esposte

E-5-3 = Raccolta informazioni organizzative utilizzando fonti open source

E-5-4 = ricognizione e sorveglianza dell'organizzazione in modo mirato

TABLE E-2: REPRESENTATIVE EXAMPLES – ADVERSARIAL THREAT EVENTS[54]

Threat Events (Characterized by TTPs)	Description
Perform reconnaissance and gather information.	
Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open source discovery of organizational information.	Adversary mines publically accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.

STEP 2: CONDUCT ASSESSMENT

- **<u>Identificare Threat Events:</u> Rilevanza Eventi di minaccia avversari**

CONFIRMED = Tutti e quattro gli eventi di minaccia sono stati individuati dall'organizzazione

TABLE E-4: RELEVANCE OF THREAT EVENTS

Value	Description
Confirmed	The threat event or TTP has been seen by the organization.
Expected	The threat event or TTP has been seen by the organization's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organization, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organization is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

STEP 2: CONDUCT ASSESSMENT

- <u>Identificare Threat Events:</u> Eventi di minaccia avversari

TABLE E-5: TEMPLATE – IDENTIFICATION OF THREAT EVENTS

Identifier	Threat Event Source of Information	Threat Source	Relevance
E-5-1	Perform perimeter network rennaissance/scanning.	D-7-1	Confirmed
E-5-2	Perform network sniffing of exposed networks.	D-7-1	Confirmed
E-5-3	Gather informations using open source discovery of organizational information.	D-7-1	Confirmed
E-5-4	Perform reconnaissance and surveillance of targeted organizations.	D-7-1	Confirmed

STEP 2: CONDUCT ASSESSMENT

- **<u>Identificare Vulnerabilità e condizioni predisponenti:</u> Severità Vulnerabilità**

  Assenza MFA: Severità **HIGH,** è di grande preoccupazione con controlli compensativi minimi

  Vulnerability Assessment non regolare: Severità **MODERATE,** di moderata preoccupazione

TABLE F-2: ASSESSMENT SCALE – VULNERABILITY SEVERITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

STEP 2: CONDUCT ASSESSMENT

- Identificare Vulnerabilità e condizioni predisponenti: Vulnerabilità

TABLE F-3: TEMPLATE – IDENTIFICATION OF VULNERABILITIES

Identifier	Vulnerability Source of Information	Vulnerability Severity
F-3-1	MFA non abilitato.	High
F-3-2	Vulnerability Assessment non regolare	Moderate

STEP 2: CONDUCT ASSESSMENT

- <u>Identificare Vulnerabilità e condizioni predisponenti:</u> Condizioni predisponenti

INFORMATION: informazioni personalmente identificabili

TECHNICAL– Architectural: Soluzioni e/o approcci alla collaborazione basata sull'utente e alla condivisione delle informazioni

TABLE F-4: TAXONOMY OF PREDISPOSING CONDITIONS

Type of Predisposing Condition	Description

INFORMATION-RELATED
- Classified National Security Information
- Compartments
- Controlled Unclassified Information
- Personally Identifiable Information
- Special Access Programs
- Agreement-Determined
  - NOFORN
  - Proprietary
	Needs to handle information (as it is created, transmitted, stored, processed, and/or displayed) in a specific manner, due to its sensitivity (or lack of sensitivity), legal or regulatory requirements, and/or contractual or other organizational agreements.

TECHNICAL
- Architectural
  - Compliance with technical standards
  - Use of specific products or product lines
  - Solutions for and/or approaches to user-based collaboration and information sharing
  - Allocation of specific security functionality to common controls
- Functional
  - Networked multiuser
  - Single-user
  - Stand-alone / nonnetworked
  - Restricted functionality (e.g., communications, sensors, embedded controllers)
	Needs to use technologies in specific ways.

STEP 2: CONDUCT ASSESSMENT

- **<u>Identificare Vulnerabilità e condizioni predisponenti:</u> Pervasività Condizioni predisponenti**

PERVASIVENESS: High, le condizioni predisponenti si applicano alla maggior parte dei sistemi dell'organizzazione

TABLE F-5: ASSESSMENT SCALE – PERVASIVENESS OF PREDISPOSING CONDITIONS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to **all** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to **most** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to **many** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to **some** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to **few** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

STEP 2: CONDUCT ASSESSMENT

- <u>Identificare Vulnerabilità e condizioni predisponenti:</u> Identificazione Condizioni predisponenti

TABLE F-6: TEMPLATE – IDENTIFICATION OF PREDISPOSING CONDITIONS

Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
F-6-1	INFORMATION - Personally Identifiable Information	High
F-6-2	TECHNICAL - Architectural - Solutions for and/or approaches to user-based collaboration and information sharing	High

STEP 2: CONDUCT ASSESSMENT

- **<u>Determinare Likelihood (Verosomiglianza):</u> Verosomiglianza che si inizino eventi di minaccia**

  La probabilità che gli avversari dia inizio all'evento di minaccia è **VERY HIGH**, è quasi certo

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

STEP 2: CONDUCT ASSESSMENT

- **<u>Determinare Likelihood (Verosomiglianza):</u> Verosomiglianza di evento di minaccia risultante in impatto avverso**

  La probabilità che le minacce risultino in un impatto avverso è **VERY HIGH**, è quasi certo.

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

STEP 2: CONDUCT ASSESSMENT

- **<u>Determinare Likelihood (Verosomiglianza):</u> Verosomiglianza complessiva**

  La probabilità che le minacce si verifichino e risultino in un impatto avverso è **VERY HIGH**, è quasi certo.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

STEP 2: CONDUCT ASSESSMENT

- <u>Determinare Impatto</u>

HARM TO ASSETS:
Danneggiamento a o perdita di asset informativi

TABLE H-2: EXAMPLES OF ADVERSE IMPACTS

Type of Impact	Impact

HARM TO OPERATIONS	- Inability to perform current missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Inability, or limited ability, to perform missions/business functions in the future.
	  - Inability to restore missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements (e.g., liability).
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to image or reputation (and hence future or potential trust relationships).

HARM TO ASSETS	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Injury or loss of life. - Physical or psychological mistreatment. - Identity theft. - Loss of Personally Identifiable Information. - Damage to image or reputation.

HARM TO OTHER ORGANIZATIONS	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements.
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to reputation (and hence future or potential trust relationships).

HARM TO THE NATION	- Damage to or incapacitation of a critical infrastructure sector.
	- Loss of government continuity of operations.
	- Relational harms.
	  - Damage to trust relationships with other governments or with nongovernmental entities.
	  - Damage to national reputation (and hence future or potential trust relationships).
	- Damage to current or future ability to achieve national objectives.
	  - Harm to national security.

STEP 2: CONDUCT ASSESSMENT

- <u>Determinare Impatto:</u> Impatto dell'evento di minaccia: HIGH

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

STEP 2: CONDUCT ASSESSMENT

- **<u>Determinare Impatto:</u> Identificazione impatto avverso**

  <u>Impatto Alto</u> L'impatto dell' inverarsi della minaccia, ovvero il danneggiamento o perdita di asset informativi (dati) è alto

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Maximum Impact
HARM TO ASSETS	Damage to or of loss of information assets	High

STEP 2: CONDUCT ASSESSMENT

- <u>Determinare il rischio</u>

Il rischio legato allo scanning e allo sniffing è moderato

Il rischio legato al Gathering Information open source e alla ricognizione/sorveglianza è alto

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								
E-5-1	D-7-1	H	M	H	C	VERY H	F-3-2	M	L	M	H	M
E-5-2	D-7-1	H	M	H	C	VERY H	F-3-2	M	L	M	H	M
E-5-3	D-7-1	H	M	H	C	VERY H	F-3-1	H	M	H	H	H
E-5-4	D-7-1	H	M	H	C	VERY H	F-3-1	H	M	H	H	H

Legenda:

- **L** = Low
- **M** =Moderate
- **H** = High

Controlli di mitigazione del rischio

Per ridurre il rischio a livello basso, l’unico accettabile per l’organizzazione, si propongono di seguito i seguenti controlli:

- Implementare una politica che preveda dettagliatamente i controlli da effettuare per valutare la resilienza dell’organizzazione alle minacce, prevedendo VA regolari ogni mese.
- Abilitare MFA implementando un controllo degli accessi basato su ruoli, che limiti i privilegi degli utenti in base alle loro funzioni e responsabilità all'interno dell'organizzazione.
- Creare e far applicare a dipendenti, operatori e pazienti una politica di password sicura: password complesse e cambiamento periodico ogni 3 mesi
- Formazione sulla sicurezza: Fornire formazione sulla sicurezza informatica per sensibilizzare gli utenti sulle minacce alla sicurezza e sulle migliori pratiche per proteggere le informazioni sensibili.
- Auditing e reporting sui sistemi per monitorare e documentare i comportamenti di coloro che accedono al sistema dell’organizzazione

IPOTESI SULLE FASI SUCCESSIVE

Il rischio calcolato durante l'Assessment viene comunicato agli stakeholders organizzativi designati con un rapporto documentato di valutazione del rischio

Comunicazione del Risk Assessment agli stakeholders

Secondo i nostri calcoli, le misure di sicurezza implementate diminuiscono il livello del rischio a quello accettabile dalla società

Effettuare un nuovo Risk Assessment per verificare l'efficacia dei controlli implementati, comunicando i risultati al personale organizzativo specifico.