

Metodologia di analisi dei rischi adottata

La presente sezione riporta la metodologia utilizzata dall'organizzazione per analizzare i rischi relativi al trattamento dei dati personali, al fine di tutelare i dati personali, con particolare riferimento a disponibilità, riservatezza e integrità dei dati.

Sommario

1. Introduzione
2. Processo di valutazione dei rischi
3. Elementi del processo di analisi del rischio
4. Metodologia applicata
5. Scala dell'indice di rischio

1. Introduzione

Lo schema utilizzato per l'analisi dei rischi si basa sui principi e sulle linee guida dello **standard ISO 31000 Risk Management – Principles and guidelines** e dello **standard ISO 27001** per il trattamento del rischio relativo alla sicurezza delle informazioni, applicati in funzione dell'obiettivo specifico dell'organizzazione di **tutelare i dati personali, con particolare riferimento a disponibilità, riservatezza e integrità dei dati**.

Conseguentemente **i rischi valutati sono focalizzati sulla tutela dei diritti e delle libertà delle persone fisiche** e non sui rischi per l'organizzazione stessa, come avviene in altri ambiti (a titolo esemplificativo, per la sicurezza delle informazioni).

Il sistema di gestione del rischio adottato mira ad essere:

- un approccio alla gestione del rischio sistematico, strutturato e tempestivo;
- adattabile ai trattamenti di dati specifici di ogni organizzazione;
- dinamico, iterativo e reattivo al cambiamento;
- parte integrante di tutti i processi di trattamento dei dati;
- di supporto al titolare ed ai responsabili nell'assunzione di scelte consapevoli e ponderate.

2. Processo di valutazione dei rischi

Il processo adottato può essere così semplificato:

Definizione del Contesto: definizione della natura, ambito di applicazione, contesto e finalità del trattamento

Identificazione del rischio: identificazione delle minacce, ossia degli eventi indesiderati che incidono su disponibilità, riservatezza e integrità dei dati personali oggetto di trattamento

Analisi del rischio: identificazione delle vulnerabilità che gravano sull'organizzazione, tenuto conto dello stato di attuazione delle contromisure, della verosimiglianza di accadimento dei rischi e delle relative conseguenze

Ponderazione del rischio: predisposizione di una griglia di valutazione dell'esposizione al rischio per ogni trattamento

Trattamento del rischio: predisposizione di un piano di trattamento del rischio

Attività trasversali al processo di gestione del rischio

Monitoraggio e riesame: metodologia sistematica di verifica e sorveglianza con registrazioni documentate e conseguente aggiornamento

Comunicazione e consultazione: metodologia sistematica di partecipazione di tutti i soggetti coinvolti nel processo di gestione del rischio

3. Elementi del processo di analisi del rischio

Di seguito sono elencati gli elementi coinvolti nel processo di analisi dei rischi.

RISCHIO

Per rischio ci si riferisce al grado di probabilità di attuazione di un evento indesiderato (minaccia) tenuto conto della gravità della sua concretizzazione.

I rischi definiti consistono in 36 minacce, che incombono sulla disponibilità, integrità e riservatezza dei dati personali.

ASSET

Per asset, ai fini dell'analisi dei rischi, ci si riferisce ai beni, intesi come luoghi fisici, risorse umane, risorse strumentali, soggetti esterni, che sono, direttamente o indirettamente, collegati al trattamento dei dati.

VULNERABILITA'

Per vulnerabilità si intendono le suscettibilità intrinseche dell'organizzazione, nel suo insieme o per specifici asset, ad essere danneggiate da un attacco, con conseguente concretizzazione delle relative minacce.

Il sistema prende in considerazione circa 160 vulnerabilità intrinseche degli asset, sulla base di:

- obiettivi di controllo di cui allo standard **UNI CEI ISO IEC 27001** per il trattamento del rischio relativo alla sicurezza delle informazioni;
- **Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni** emanate dall'**AgID** (Agenzia per l'Italia Digitale) di cui alla *Circolare 2/2017 del 18 aprile 2017*.

CONTROMISURE

Le contromisure sono le misure da applicare o applicate dall'organizzazione per contrastare l'attuazione dell'evento indesiderato.

Il sistema analizza lo stato di attuazione di circa 160 contromisure atte a contrastare le vulnerabilità dell'organizzazione. L'attuazione di talune contromisure può influenzare il peso (livello di criticità) di molteplici vulnerabilità correlate indirettamente, tramite un sistema di *coefficienti di ponderazione*.

QUESITI

Il sistema si fonda su un complesso sistema di quesiti, tra loro interconnessi, che consentono di:

- semplificare e standardizzare la rilevazione delle informazioni necessarie al processo di gestione del rischio;
- favorire la partecipazione di soggetti diversi al processo.

Le risposte fornite dall'utente ai quesiti hanno una duplice finalità:

- popolare il sistema con le informazioni relative all'organizzazione;
- raccogliere i dati necessari al calcolo dell'indice di rischio.

TRATTAMENTO

Trattandosi di una valutazione del rischio finalizzata alla protezione dei dati personali per i diritti e le libertà delle persone fisiche, tale valutazione non può prescindere dal Trattamento dei dati personali, che può essere considerato il **Contesto del processo di gestione del rischio**.

PROBABILITA'

La probabilità di concretizzazione della minaccia è l'elemento dell'analisi che il sistema chiede di valorizzare all'utente in base alla **frequenza storica di accadimento**. Tale coefficiente viene assegnato ai singoli rischi (minacce) correlati ad ogni specifico trattamento. Tale correlazione consente di elaborare l'analisi dei rischi tenendo conto della **Definizione del contesto**, che in ambito di tutela dei dati personali, si sostanzia in natura, ambito, contesto e finalità del trattamento (cfr. *Considerando 90 Regolamento 2016/679 e UNI ISO 31000 Risk Management – Principles and guidelines*).

DANNO

Il danno è la **gravità** delle conseguenze in caso di attuazione della minaccia. Il sistema consente di valorizzare il danno derivante dall'attuazione di uno specifico rischio (minaccia) per ogni singolo trattamento. Tale valorizzazione si basa, in larga parte, sui criteri proposti nel **WP 248** Rev. 01 "*Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento 'possa presentare un rischio elevato' ai sensi del Regolamento 2016/679*" per individuare i trattamenti che possono presentare un rischio elevato e che quindi sono soggetti a DPIA (Data Protection Impact Assessment).

Il sistema così sviluppato consente all'Organizzazione di:

- valutare in modo continuativo i rischi che gravano sui propri trattamenti, così da individuare quelle situazioni in cui una determinata tipologia di trattamenti “può presentare un rischio elevato per i diritti e le libertà delle persone fisiche”;
- completare tale analisi valutando anche i criteri relativi alla realizzazione di una **Valutazione di impatto** (DPIA) di cui al *Regolamento 2016/679 art. 35 commi 1 e 3 integrati, ai sensi del comma 4, dai criteri di cui al WP248 Rev. 01.*

4. Metodologia applicata

A livello di singolo trattamento il sistema individua gli asset direttamente o indirettamente ad esso collegati. Per ognuno di essi, il processo di analisi dei rischi analizza le vulnerabilità, ossia le suscettibilità intrinseche ad essere danneggiati da un attacco, con conseguente concretizzazione delle relative minacce, e le contromisure, dirette o indirette, attuate, fornendo il livello di rischio. Tale livello tiene anche conto della probabilità e dell’impatto che l’attuazione della minaccia avrebbe sui dati personali trattati, per mezzo degli specifici asset.

Tale metodologia può essere riassunta nella seguente funzione:

$$R_T = f (V_T , P_T , D_T)$$

dove:

R_T è l’indice di rischio che insiste sul Trattamento, espresso in valori percentuali,

V_T è l’indice di vulnerabilità degli asset coinvolti nel trattamento, tenuto conto delle contromisure, dirette o indirette, attuate e del livello di criticità espresso sul singolo asset,

P_T è la probabilità di accadimento dell’evento indesiderato sul trattamento,

D_T è la gravità delle conseguenze della concretizzazione dell’evento indesiderato sul trattamento.

Il sistema può essere così rappresentato:



5. Scala dell’indice di rischio

La scala del livello di rischio utilizzata si configura come segue:

- Rischio molto basso
- Rischio basso
- Rischio medio
- Rischio alto
- Rischio molto alto

In base al livello di rischio ottenuto il sistema fornisce indicazioni sulle azioni di contrasto e miglioramento da attuare. Nel sistema sono inoltre disponibili i report necessari ai titolari ed ai responsabili per ponderare il rischio e predisporre i piani di trattamento dello stesso.

Privacy – Livello di rischio generale per trattamenti

Il presente documento, "Privacy – Livello di rischio generale sul trattamento", fornisce un elenco dei trattamenti di dati personali svolti dal titolare del trattamento con l'indicazione di un valore di rischio generale incombente sul trattamento.

Tale valore va inquadrato come il livello massimo di rischio a cui è esposto il singolo trattamento e viene assegnato al trattamento stesso selezionando, tra tutti i rischi che incombono sul medesimo, quello che ha raggiunto il livello più alto.

Trattamento	Rischio
 Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	13%

Privacy - Livello di rischio specifico per trattamento

Il presente documento, "Privacy - Livello di rischio specifico per trattamento", fornisce, per ogni specifico trattamento di dati personali svolti dal titolare del trattamento, l'elenco delle minacce incombenti, con indicazione degli asset coinvolti e del grado di rischio.

Nel dettaglio, il report che segue mostra, per ogni trattamento:



- l'elenco dei rischi (minacce) che incombono sul trattamento;
- l'elenco delle tipologie di asset collegate al trattamento;
- il livello massimo di ogni rischio per ogni tipologia di asset.

Per asset, ai fini dell'analisi dei rischi, ci si riferisce ai beni, intesi come luoghi fisici, risorse umane, strumenti informatici, che sono direttamente o indirettamente collegati al trattamento.

Per ogni tipologia di asset collegata, il processo di analisi dei rischi analizza le vulnerabilità, ossia le suscettibilità intrinseche ad essere danneggiate da un attacco, con conseguente concretizzazione delle relative minacce, e le contromisure, dirette e indirette, attuate per ridurre l'attuazione delle minacce, fornendo conseguentemente il livello di rischio (%) visualizzato. Tale livello tiene anche conto della probabilità e dell'impatto che l'attuazione della minaccia avrebbe sui dati personali trattati per mezzo degli specifici asset.

Le ultime tre colonne rappresentano l'ambito di impatto del rischio(minaccia).

Rischio	Asset										Impatto		
	Applicativi di comunicazione elettronica	Applicativi software	Firewall	Luoghi	Organizzazione generale	Postazioni di lavoro fisse	Postazioni di lavoro portatili	Rete interna	Switch	Disponibilità	Riservatezza	Integrità	
 Trattamento: Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale													
R0001 - Malfunzionamento o degrado apparecchiature	12%	13%	10%		12%	12%		12%	X		X		
R0005 - Ingressi non autorizzati a locali e/o aree ad accesso ristretto	9%	11%	8%	8%	10%	10%		9%			X		
R0008 - Esposizione a condizioni metereologiche estreme			8%									X	
R0009 - Incendio			8%							X		X	
R0010 - Terremoto			8%							X		X	
R0011 - Allagamento			8%							X		X	
R0013 - Copia abusiva di dati	13%	12%	13%	10%	8%	12%	12%		11%		X		
R0014 - Furto di dati	13%	12%	13%	10%		12%	12%	10%	11%	X	X		
R0015 - Modifica non autorizzata di dati	13%	12%	13%		9%	12%	12%		11%			X	
R0016 - Presa visione abusiva di dati	13%	12%	13%	10%	8%	12%	12%		11%		X		
R0017 - Corruzione e/o inaccessibilità dei dati	11%	9%	11%			10%	10%	8%	9%	X		X	
R0018 - Trattamento illecito dei dati		9%	10%	8%	8%				9%		X		
R0019 - Uso non autorizzato dei dati	11%	9%	11%		8%	10%	10%		9%		X		
R0020 - Comunicazione illegale dei dati		9%	10%		8%				9%		X		
R0021 - Diffusione illegale dei dati				8%								X	
R0022 - Mancata conservazione di dati		9%	11%	8%		10%	10%		9%	X		X	
R0024 - Mancata eliminazione dei dati raggiunta la finalità					8%	8%	8%				X		
R0031 - Accessi non autorizzati	11%	9%	11%	8%	8%	10%	10%	8%	9%		X		
R0032 - Carenza di consapevolezza, disattenzione o incuria		10%	12%		9%	11%	11%		10%	X	X	X	
R0033 - Errore nello svolgimento di mansioni		10%	12%		9%	11%	11%		10%	X	X	X	

 R0034 - Ignoranza procedure di gestione					7%					X	X	X
 R0036 - Guasto ai sistemi complementari			10%	8%		9%	9%		9%	X		X

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
Accessi logici	<p>V0074 - Accessi _ Assenza sistema di autenticazione</p> <p>La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:</p> <p>Sono utilizzate credenziali di autenticazione per l'accesso degli utenti</p>	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	9%	<input checked="" type="checkbox"/>	13%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	9%	<input checked="" type="checkbox"/>	13%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	9%	<input checked="" type="checkbox"/>	13%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	9%	<input checked="" type="checkbox"/>	13%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	9%	<input checked="" type="checkbox"/>	11%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	9%	<input checked="" type="checkbox"/>	11%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	9%	<input checked="" type="checkbox"/>	11%
Accessi_Carenza tipo autenticazione	<p>V0076 - Accessi_Carenza tipo autenticazione</p> <p>La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:</p> <p>Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.</p>	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	11%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	11%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	11%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	8%	<input checked="" type="checkbox"/>	11%
Accessi_Carenza requisito di complessità	<p>V0077 - Accessi_Carenza requisito di complessità</p> <p>La contromisura associata alla suddetta vulnerabilità, viene</p>	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	13%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
	riportata di seguito: Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	13%
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	13%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	13%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	11%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	11%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	11%	
V0075 - Accessi_Carenza profili di autorizzazione La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0033	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0032	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	10%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	10%	
V0078 - Accessi_Carenza credenziali utenze amministrative La contromisura associata alla suddetta vulnerabilità, viene	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	8%	<input checked="" type="checkbox"/>	10%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%	

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
	riportata di seguito: Sono utilizzate per le utenze amministrative credenziali di elevata robustezza sostituite con sufficiente frequenza.	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	12%
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	10%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	10%	
	V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	12%
	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	8%	<input checked="" type="checkbox"/>	10%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	10%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%	
V0088 - Accessi_Assenza lockout	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: E' attivo un sistema di lockout in caso di errato inserimento credenziali oltre una soglia predefinita	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%
PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	10%		
PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%		

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
V0089 - Accessi_Assenza timeout di inattività La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	12%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	10%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%	
V0149 - Accessi_Mancanza di sistema di lockout a livello di IP La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: E' previsto un sistema di lockout a livello di IP per le richieste anomale	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	7%	<input checked="" type="checkbox"/>	11%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	7%	<input checked="" type="checkbox"/>	9%	
	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	7%	<input checked="" type="checkbox"/>	9%	
V0079 - Accessi_Inadeguatezza utenze amministratori La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: E' assicurata la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse	App Mobile - Monitoraggio pazienti affetti da patologie epatiche (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0033	7%	<input checked="" type="checkbox"/>	10%	
V0081 - Accessi_Mancato cambio password periodico La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	7%	<input checked="" type="checkbox"/>	9%	
V0083 - Accessi_Permissione utilizzo sequenza password La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	7%	<input checked="" type="checkbox"/>	9%	

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
	V0084 - Accessi_Mancata univocità codice identificativo La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	7%	<input checked="" type="checkbox"/>	9%
	V0090 - Accessi_Assenza screensaver La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Sono attivi gli screensaver protetti con password	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	6%	<input checked="" type="checkbox"/>	9%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	6%	<input checked="" type="checkbox"/>	9%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	9%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	6%	<input checked="" type="checkbox"/>	9%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	6%	<input checked="" type="checkbox"/>	7%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	7%
	V0080 - Accessi_Mancato cambio password iniziale La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Se previste, le parole chiave (password) vengono modificate al primo utilizzo	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
	V0085 - Accessi_Utilizzo utenze amministrative anonime La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
	V0086 - Accessi_Mancata disattivazione credenziali inutilizzate La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	7%
Gestione sistema IT	V0105 - Gestione IT_Mancata esecuzione aggiornamento patch La contromisura associata alla suddetta vulnerabilità, viene	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0001	9%	<input checked="" type="checkbox"/>	13%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
	riportata di seguito: Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	11%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	11%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	8%	<input checked="" type="checkbox"/>	11%
	V0151 - Gestione IT_Presenza asset obsoleti La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0001	9%	<input checked="" type="checkbox"/>	13%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	11%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	11%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	8%	<input checked="" type="checkbox"/>	11%
	V0103 - Gestione IT_Mancata manutenzione e aggiornamento sistemi IT La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0001	8%	<input checked="" type="checkbox"/>	12%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	8%	<input checked="" type="checkbox"/>	10%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0036	8%	<input checked="" type="checkbox"/>	10%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	10%
V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità La contromisura associata alla suddetta vulnerabilità, viene	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%	

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
	riportata di seguito: Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	10%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%
	V0108 - Gestione IT_Inadeguato utilizzo strumenti di scansione delle vulnerabilità	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	7%	<input checked="" type="checkbox"/>	11%
	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Se sì, sono utilizzati strumenti di scansione delle vulnerabilità ad ogni modifica significativa della configurazione	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	7%	<input checked="" type="checkbox"/>	9%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	7%	<input checked="" type="checkbox"/>	9%
	V0109 - Gestione IT_Mancanza di blocco di modifiche software a utenti non autorizzati	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	7%	<input checked="" type="checkbox"/>	11%
	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: L'installazione, modifica e aggiornamento di software sugli strumenti è permessa solo agli amministratori	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	7%	<input checked="" type="checkbox"/>	11%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	7%	<input checked="" type="checkbox"/>	9%
Firewall	V0122 - Assenza firewall per tutti i dispositivi collegati in rete	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%
	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: E' presente un firewall per tutti i dispositivi collegati in rete (individuale o centralizzato)	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	8%	<input checked="" type="checkbox"/>	10%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	10%
Log	V0115 - Log_Modificabilità dati di log degli amministratori	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	12%
	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: I dati di log degli amministratori sono imm modificabili	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	10%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%
	V0117 - Log_Assenza sistema di log degli eventi La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: E' attivo un sistema di log degli eventi	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	10%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%
	V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	8%	<input checked="" type="checkbox"/>	10%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%
	V0114 - Log_Assenza sistema di log degli amministratori La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: E' attivo un sistema di log degli amministratori	ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	7%	<input checked="" type="checkbox"/>	11%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	7%	<input checked="" type="checkbox"/>	11%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	7%	<input checked="" type="checkbox"/>	11%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	7%	<input checked="" type="checkbox"/>	11%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	7%	<input checked="" type="checkbox"/>	9%
		ICE (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	7%	<input checked="" type="checkbox"/>	9%
	V0116 - Log_Mancato riesame dei dati di log degli amministratori La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	6%	<input checked="" type="checkbox"/>	10%
	I dati di log degli amministratori vengono periodicamente riesaminati	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	6%	<input checked="" type="checkbox"/>	10%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	6%	<input checked="" type="checkbox"/>	10%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	10%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	6%	<input checked="" type="checkbox"/>	8%
Malware	V0119 - Malware_Assenza o inadeguatezza sistemi di protezione da malware La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%
	Sono presenti e aggiornati idonei sistemi di protezione da malware (software dannoso)	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	10%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	8%	<input checked="" type="checkbox"/>	10%
	V0120 - Malware_Mancata esecuzione scansioni con i sistemi di protezione La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	8%	<input checked="" type="checkbox"/>	10%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
	Vengono periodicamente eseguite le scansioni con i sistemi di protezione	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	8%	<input checked="" type="checkbox"/>	10%
Rete	V0125 - Rete_Carenza protezione accesso da esterno La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: L'accesso dall'esterno è protetto da credenziali di autenticazione e consentito solo a personale autorizzato	App Mobile - Monitoraggio pazienti affetti da patologie epatiche (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	7%	<input checked="" type="checkbox"/>	12%
		App Mobile - Monitoraggio pazienti affetti da patologie epatiche (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	7%	<input checked="" type="checkbox"/>	12%
		App Mobile - Monitoraggio pazienti affetti da patologie epatiche (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	7%	<input checked="" type="checkbox"/>	12%
		App Mobile - Monitoraggio pazienti affetti da patologie epatiche (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	7%	<input checked="" type="checkbox"/>	9%
		App Mobile - Monitoraggio pazienti affetti da patologie epatiche (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	7%	<input checked="" type="checkbox"/>	9%
		App Mobile - Monitoraggio pazienti affetti da patologie epatiche (Servizio)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	7%	<input checked="" type="checkbox"/>	9%
	V0131 - Rete_Trasmissione informazioni tramite protocolli e canali non sicuri La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le informazioni sono trasmesse tramite protocolli e canali sicuri	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	8%	<input checked="" type="checkbox"/>	12%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	8%	<input checked="" type="checkbox"/>	12%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	8%	<input checked="" type="checkbox"/>	12%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0018	8%	<input checked="" type="checkbox"/>	10%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	8%	<input checked="" type="checkbox"/>	10%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0020	8%	<input checked="" type="checkbox"/>	10%
	V0126 - Rete_Mancata disabilitazione delle porte non utilizzate La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le porte non utilizzate sono disabilitate	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	7%	<input checked="" type="checkbox"/>	11%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	7%	<input checked="" type="checkbox"/>	9%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	7%	<input checked="" type="checkbox"/>	9%
	V0123 - Rete_Mancata disabilitazione dei punti rete non utilizzati	LAN	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	9%
	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: I punti rete non utilizzati sono disabilitati	LAN	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	7%
		LAN	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	6%	<input checked="" type="checkbox"/>	7%
Accessi fisici	V0002 - Accesso fisico_Accesso fisico luoghi non selezionato	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	6%	<input checked="" type="checkbox"/>	10%
	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni sono ad accesso selezionato (si intende per accesso selezionato l'accesso consentito solo a personale specificatamente autorizzato, a titolo esemplificativo, tramite utilizzo di badge, chiavi ecc.)	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	10%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	6%	<input checked="" type="checkbox"/>	10%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0018	6%	<input checked="" type="checkbox"/>	8%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	6%	<input checked="" type="checkbox"/>	8%
	V0003 - Accesso fisico_Accesso fisico archivi non selezionato	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	6%	<input checked="" type="checkbox"/>	10%
	La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Gli archivi che contengono informazioni sensibili o critiche sono ad accesso selezionato (si intende per accesso selezionato l'accesso consentito solo a personale specificatamente autorizzato, a titolo esemplificativo, tramite utilizzo di cassetti o armadi con serratura, cassaforte ecc.)	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	6%	<input checked="" type="checkbox"/>	10%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	10%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	6%	<input checked="" type="checkbox"/>	8%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0018	6%	<input checked="" type="checkbox"/>	8%
	V0005 - Accesso fisico_Mancanza di sistema antintrusione La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Presenza di un sistema anti-intrusione nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni	ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	10%
		ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
		ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%
	V0010 - Accesso fisico_Accesso al pubblico senza presidio La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Se è consentito l'accesso al pubblico nelle aree di trattamento dati, l'accesso avviene con presidio	ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	10%
		ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%
		ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
	V0004 - Accesso fisico_Accesso fisico non videosorvegliato La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Presenza di un sistema di videosorveglianza nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni	ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	9%
		ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%
		ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
	V0007 - Accesso fisico_Accessi non antisfondamento La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le porte/finestre nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni sono antisfondamento	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	9%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
	V0008 - Accesso fisico_Assenza servizio di vigilanza La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: E' attivo un servizio di vigilanza negli orari di chiusura	ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0014	6%	<input checked="" type="checkbox"/>	9%
		ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
		ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
	V0006 - Accesso fisico_Mancata registrazione accessi fisici La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%
	Gli accessi fisici nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni vengono registrati	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
	V0001 - Accesso fisico_Aree non chiaramente definite e segnalate La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	5%	<input checked="" type="checkbox"/>	7%
	Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni sono chiaramente definite e segnalate	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	5%	<input checked="" type="checkbox"/>	7%
Sicurezza fisica	V0016 - Sicurezza fisica_Assenza sistema di climatizzazione La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0001	6%	<input checked="" type="checkbox"/>	10%
	E' installato e correttamente funzionante un sistema di climatizzazione	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0036	6%	<input checked="" type="checkbox"/>	8%
		Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0008	6%	<input checked="" type="checkbox"/>	8%
	V0017 - Sicurezza fisica_Assenza gruppi di continuità e/o gruppi elettrogeni La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0001	6%	<input checked="" type="checkbox"/>	10%
	Sono presenti uno o più gruppi di continuità e/o gruppi elettrogeni						
	V0019 - Sicurezza fisica_Assenza filtri di protezione La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0001	6%	<input checked="" type="checkbox"/>	10%
	Sono presenti filtri di protezione per sbalzi di tensione						
	V0013 - Sicurezza fisica_Mancanza sistema antincendio La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0009	6%	<input checked="" type="checkbox"/>	8%
	E' presente un sistema antincendio idoneo e periodicamente revisionato						
	V0014 - Sicurezza fisica_Locali non antisismici La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:	ASST Papa Giovanni XXIII	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0010	6%	<input checked="" type="checkbox"/>	8%
	I locali che contengono informazioni sensibili o critiche o le strutture di elaborazione delle informazioni sono antisismici						

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
	V0015 - Sicurezza fisica_Aree a rischio allagamento La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni non sono a rischio allagamento (piani interrati)	Stanza 22	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0011	6%	<input checked="" type="checkbox"/>	8%
Backup	V0096 - Backup_Inadeguatezza memorizzazione immagini di installazione La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Le immagini d'installazione sono memorizzate offline	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0032	6%	<input checked="" type="checkbox"/>	9%
	V0091 - Backup_Strumenti non ridonati La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Lo strumento è ridonato	Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0036	6%	<input checked="" type="checkbox"/>	8%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0022	6%	<input checked="" type="checkbox"/>	8%
		Firewall	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0017	6%	<input checked="" type="checkbox"/>	8%
Dispositivi portatili	V0111 - Mancata cancellazione dati La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: I dati vengono cancellati dai dispositivi portatili e dai supporti esterni cancellabili prima di procedere al loro riutilizzo, riassegnazione o smaltimento	PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	6%	<input checked="" type="checkbox"/>	9%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0024	6%	<input checked="" type="checkbox"/>	8%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	7%
		PC_CG(Windows 10 Pro)	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	6%	<input checked="" type="checkbox"/>	7%
Incarichi	V0024 - Incarichi_Carenza definizione e assegnazione incarichi La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Gli incarichi e le responsabilità del personale e dei collaboratori relative alla sicurezza delle informazioni sono definiti, assegnati formalmente e mantenuti aggiornati	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0033	6%	<input checked="" type="checkbox"/>	9%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	6%	<input checked="" type="checkbox"/>	9%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	6%	<input checked="" type="checkbox"/>	8%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
	<p>V0030 - Incarichi_Inadeguatezza nomina DPO</p> <p>La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:</p> <p>In caso di nomina di un Responsabile della protezione dei dati - DPO (Data Protection Officer), il Titolare (o responsabile) del trattamento si è assicurato che il soggetto nominato possieda un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, adempia alle sue funzioni in piena indipendenza ed in assenza di conflitto di interesse, abbia la disponibilità delle risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.</p>	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0032	6%	<input checked="" type="checkbox"/>	9%
	<p>V0031 - Incarichi_Mancata comunicazione DPO</p> <p>La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:</p> <p>Il Responsabile della protezione dei dati - DPO (Data Protection Officer) ha comunicato le proprie generalità all'Autorità di controllo</p>	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0034	5%	<input checked="" type="checkbox"/>	7%
Trattamento	<p>V0141 - Trattamento_Mancata individuazione tipologie di dato</p> <p>La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:</p> <p>Sono stati individuati i tipi di dato oggetto di trattamento</p>	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0033	6%	<input checked="" type="checkbox"/>	9%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0032	6%	<input checked="" type="checkbox"/>	9%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0021	6%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0020	6%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	6%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0018	6%	<input checked="" type="checkbox"/>	8%
	<p>V0143 - Trattamento_Carenza definizione ambito di trattamento</p> <p>La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito:</p> <p>E' attuato un processo formale di definizione e aggiornamento dell'ambito di trattamento</p>	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0033	6%	<input checked="" type="checkbox"/>	9%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0032	6%	<input checked="" type="checkbox"/>	9%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	6%	<input checked="" type="checkbox"/>	9%

Contromisure per Categorie di Vulnerabilità Dettagliato

FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore - Analisi dei rischi del 3/13/2024

Cat. Vulnerabilità	Vulnerabilità / Contromisura	Asset	Trattamento	Rischio	% Pura	Attuata	% Infl.
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	6%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0005	6%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0018	6%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0024	6%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0031	6%	<input checked="" type="checkbox"/>	8%
Processo disciplinare	V0035 - Processo disciplinare_Mancata informazione su processi disciplinari La contromisura associata alla suddetta vulnerabilità, viene riportata di seguito: Il personale dipendente e i collaboratori sono informati sulla possibilità di incorrere in un processo disciplinare in caso di mancato rispetto delle policy in tema di trattamento dei dati	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0032	5%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0013	5%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0016	5%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0015	5%	<input checked="" type="checkbox"/>	8%
		FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	Epidemiologia clinica nei pazienti contemporanei con mielofibrosi (ERNEST-3). Uno studio osservazionale dell'European LeukemiaNet (ELN).	R0019	5%	<input checked="" type="checkbox"/>	7%

Analisi vulnerabilità e contromisure

L'Organizzazione, ai fini dell'analisi dei rischi relativi alla sicurezza delle informazioni, in funzione dell'obiettivo specifico di tutelare i dati personali, con particolare riferimento a disponibilità, riservatezza e integrità dei dati, ha implementato un sistema di rilevazione delle vulnerabilità che incombono sugli asset dell'Organizzazione e delle relative misure di sicurezza attuate o da attuare.

Per una migliore comprensione delle informazioni fornite nel presente documento, si considerino le seguenti definizioni:

ASSET

Per asset, ai fini dell'analisi dei rischi, ci si riferisce ai beni, intesi come luoghi fisici, risorse umane, risorse strumentali, soggetti esterni, che sono, direttamente o indirettamente, collegati al trattamento dei dati.

VULNERABILITA'

Per vulnerabilità si intendono le suscettibilità intrinseche dell'Organizzazione, nel suo insieme o per specifici asset, ad essere danneggiate da un attacco, con conseguente concretizzazione delle relative minacce. Il sistema prende in considerazione le vulnerabilità intrinseche degli asset, sulla base di:



















- obiettivi di controllo di cui allo standard UNI CEI ISO IEC 27001 per il trattamento del rischio relativo alla sicurezza delle informazioni;
- Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni emanate dall'AgID (Agenzia per l'Italia Digitale) di cui alla Circolare 2/2017 del 18 aprile 2017;
- Misure Minime di Sicurezza di cui all'Allegato B del Decreto legislativo 30 giugno 2003, n. 196.

CONTROMISURE



















Le contromisure sono le misure da applicare o applicate dall'Organizzazione per contrastare l'attuazione dell'evento indesiderato. Il sistema analizza lo stato di attuazione di molteplici contromisure atte a contrastare le vulnerabilità dell'Organizzazione. L'attuazione di talune contromisure può influenzare il peso (livello di criticità) di molteplici vulnerabilità correlate indirettamente, tramite un sistema di coefficienti di ponderazione.

Per i dettagli vedere il documento: **Analisi dei rischi - Vulnerabilità e contromisure - Allegato1**



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
Applicativi di comunicazione elettronica	ICE (Servizio)	 V0074 - Accessi _ Assenza sistema di autenticazione	9%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	13%
		 V0117 - Log_Assenza sistema di log degli eventi	8%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	12%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	8%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	12%
		 V0115 - Log_Modificabilità dati di log degli amministratori	8%	I dati di log degli amministratori sono imm modificabili	<input checked="" type="checkbox"/>	12%
		 V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità	8%	Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	<input checked="" type="checkbox"/>	12%
		 V0108 - Gestione IT_Inadeguato utilizzo strumenti di scansione delle vulnerabilità	7%	Se si, sono utilizzati strumenti di scansione delle vulnerabilità ad ogni modifica significativa della configurazione	<input checked="" type="checkbox"/>	11%
		 V0114 - Log_Assenza sistema di log degli amministratori	7%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	11%
Firewall	Firewall	 V0077 - Accessi_Carenza requisito di complessità	8%	Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	13%
		 V0074 - Accessi _ Assenza sistema di autenticazione	8%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	13%
		 V0151 - Gestione IT_Presenza asset obsoleti	9%	Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	<input checked="" type="checkbox"/>	13%
		 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	9%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	<input checked="" type="checkbox"/>	13%
		 V0076 - Accessi_Carenza tipo autenticazione	8%	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.	<input checked="" type="checkbox"/>	13%
		 V0103 - Gestione IT_Mancati manutenzione e aggiornamento sistemi IT	8%	Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	<input checked="" type="checkbox"/>	12%
		 V0131 - Rete_Trasmisione informazioni tramite protocolli e canali non sicuri	8%	Le informazioni sono trasmesse tramite protocolli e canali sicuri	<input checked="" type="checkbox"/>	12%
		 V0078 - Accessi_Carenza credenziali utenze amministrative	8%	Sono utilizzate per le utenze amministrative credenziali di elevata robustezza sostituite con sufficiente frequenza.	<input checked="" type="checkbox"/>	12%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	8%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	12%
		 V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità	8%	Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	<input checked="" type="checkbox"/>	12%
		 V0115 - Log_Modificabilità dati di log degli amministratori	8%	I dati di log degli amministratori sono imm modificabili	<input checked="" type="checkbox"/>	12%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0117 - Log_Assenza sistema di log degli eventi	8%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	12%
		 V0089 - Accessi_Assenza timeout di inattività	8%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	12%
		 V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	8%	Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	<input checked="" type="checkbox"/>	12%
		 V0075 - Accessi_Carenza profili di autorizzazione	8%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	12%
		 V0149 - Accessi_Mancanza di sistema di logout a livello di IP	7%	E' previsto un sistema di logout a livello di IP per le richieste anomale	<input checked="" type="checkbox"/>	11%
		 V0126 - Rete_Mancata disabilitazione delle porte non utilizzate	7%	Le porte non utilizzate sono disabilite	<input checked="" type="checkbox"/>	11%
		 V0114 - Log_Assenza sistema di log degli amministratori	7%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	11%
		 V0116 - Log_Mancato riesame dei dati di log degli amministratori	6%	I dati di log degli amministratori vengono periodicamente riesaminati	<input checked="" type="checkbox"/>	10%
		 V0019 - Sicurezza fisica_Assenza filtri di protezione	6%	Sono presenti filtri di protezione per sbalzi di tensione	<input checked="" type="checkbox"/>	10%
		 V0017 - Sicurezza fisica_Assenza gruppi di continuità e/o gruppi elettrogeni	6%	Sono presenti uno o più gruppi di continuità e/o gruppi elettrogeni	<input checked="" type="checkbox"/>	10%
		 V0081 - Accessi_Mancato cambio password periodico	7%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	9%
		 V0084 - Accessi_Mancata univocità codice identificativo	7%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	9%
		 V0083 - Accessi_Permesso utilizzo sequenza password	7%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	9%
		 V0080 - Accessi_Mancato cambio password iniziale	6%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	8%
		 V0091 - Backup_Strumenti non ridondati	6%	Lo strumento è ridondato	<input checked="" type="checkbox"/>	8%
		 V0085 - Accessi_Utilizzo utenze amministrative anonime	6%	Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'immutabilità di chi ne fa uso	<input checked="" type="checkbox"/>	8%
Applicativi software	App Mobile - Monitoraggio pazienti affetti da patologie epatiche (Servizio)	 V0077 - Accessi_Carenza requisito di complessità	7%	Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	12%
		 V0125 - Rete_Carenza protezione accesso da esterno	7%	L'accesso dall'esterno è protetto da credenziali di autenticazione e consentito solo a personale autorizzato	<input checked="" type="checkbox"/>	12%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0074 - Accessi _ Assenza sistema di autenticazione	7%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	12%
		 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	8%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	<input checked="" type="checkbox"/>	12%
		 V0117 - Log_Assenza sistema di log degli eventi	7%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	10%
		 V0109 - Gestione IT_Mancanza di blocco di modifiche software a utenti non autorizzati	7%	L'installazione, modifica e aggiornamento di software sugli strumenti è permessa solo agli amministratori	<input checked="" type="checkbox"/>	10%
		 V0079 - Accessi_Inadeguatezza utenze amministratori	7%	E' assicurata la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse	<input checked="" type="checkbox"/>	10%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	7%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	10%
		 V0075 - Accessi_Carenza profili di autorizzazione	7%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	10%
		 V0131 - Rete_Trasmissione informazioni tramite protocolli e canali non sicuri	7%	Le informazioni sono trasmesse tramite protocolli e canali sicuri	<input checked="" type="checkbox"/>	10%
		 V0089 - Accessi_Assenza timeout di inattività	7%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	10%
		 V0084 - Accessi_Mancata univocità codice identificativo	6%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	8%
		 V0083 - Accessi_Permesso utilizzo sequenza password	6%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	8%
		 V0081 - Accessi_Mancato cambio password periodico	6%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	8%
		 V0080 - Accessi_Mancato cambio password iniziale	5%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	7%
		Postazioni di lavoro fisse	PC_AG (Microsoft Windows 10)	 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	8%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi
 V0119 - Malware_Assenza o inadeguatezza sistemi di protezione da malware	8%			Sono presenti e aggiornati idonei sistemi di protezione da malware (software dannoso)	<input checked="" type="checkbox"/>	12%
 V0077 - Accessi_Carenza requisito di complessità	8%			Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	12%
 V0151 - Gestione IT_Presenza asset obsoleti	8%			Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	<input checked="" type="checkbox"/>	12%
 V0122 - Assenza firewall per tutti i dispositivi collegati in rete	8%			E' presente un firewall per tutti i dispositivi collegati in rete (individuale o centralizzato)	<input checked="" type="checkbox"/>	12%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0074 - Accessi _ Assenza sistema di autenticazione	8%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	12%
		 V0120 - Malware_Mancata esecuzione scansioni con i sistemi di protezione	8%	Vengono periodicamente eseguite le scansioni con i sistemi di protezione	<input checked="" type="checkbox"/>	12%
		 V0088 - Accessi_Assenza lockout	8%	E' attivo un sistema di lockout in caso di errato inserimento credenziali oltre una soglia predefinita	<input checked="" type="checkbox"/>	12%
		 V0076 - Accessi_Carenza tipo autenticazione	8%	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.	<input checked="" type="checkbox"/>	12%
		 V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità	7%	Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	<input checked="" type="checkbox"/>	11%
		 V0089 - Accessi_Assenza timeout di inattività	7%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	11%
		 V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	7%	Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	<input checked="" type="checkbox"/>	11%
		 V0075 - Accessi_Carenza profili di autorizzazione	7%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	11%
		 V0103 - Gestione IT_Mancati manutenzione e aggiornamento sistemi IT	7%	Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	<input checked="" type="checkbox"/>	11%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	7%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	11%
		 V0117 - Log_Assenza sistema di log degli eventi	7%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	11%
		 V0115 - Log_Modificabilità dati di log degli amministratori	7%	I dati di log degli amministratori sono immutabili	<input checked="" type="checkbox"/>	11%
		 V0109 - Gestione IT_Mancanza di blocco di modifiche software a utenti non autorizzati	7%	L'installazione, modifica e aggiornamento di software sugli strumenti è permessa solo agli amministratori	<input checked="" type="checkbox"/>	11%
		 V0114 - Log_Assenza sistema di log degli amministratori	6%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	10%
		 V0111 - Mancata cancellazione dati	6%	I dati vengono cancellati dai dispositivi portatili e dai supporti esterni cancellabili prima di procedere al loro riutilizzo, riassegnazione o smaltimento	<input checked="" type="checkbox"/>	9%
		 V0019 - Sicurezza fisica_Assenza filtri di protezione	6%	Sono presenti filtri di protezione per sbalzi di tensione	<input checked="" type="checkbox"/>	9%
		 V0017 - Sicurezza fisica_Assenza gruppi di continuità e/o gruppi elettrogeni	6%	Sono presenti uno o più gruppi di continuità e/o gruppi elettrogeni	<input checked="" type="checkbox"/>	9%
		 V0116 - Log_Mancato riesame dei dati di log degli amministratori	6%	I dati di log degli amministratori vengono periodicamente riesaminati	<input checked="" type="checkbox"/>	9%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0096 - Backup_Inadeguatezza memorizzazione immagini di installazione	6%	Le immagini d'installazione sono memorizzate offline	<input checked="" type="checkbox"/>	9%
		 V0090 - Accessi_Assenza screensaver	6%	Sono attivi gli screensaver protetti con password	<input checked="" type="checkbox"/>	9%
		 V0083 - Accessi_Percesso utilizzo sequenza password	6%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	8%
		 V0084 - Accessi_Mancata univocità codice identificativo	6%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	8%
		 V0081 - Accessi_Mancato cambio password periodico	6%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	8%
		 V0080 - Accessi_Mancato cambio password iniziale	6%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	7%
		 V0086 - Accessi_Mancata disattivazione credenziali inutilizzate	6%	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	<input checked="" type="checkbox"/>	7%
		 V0085 - Accessi_Utilizzo utenze amministrative anonime	6%	Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso	<input checked="" type="checkbox"/>	7%
	PC_CG(Windows 10 Pro)	 V0120 - Malware_Mancata esecuzione scansioni con i sistemi di protezione	8%	Vengono periodicamente eseguite le scansioni con i sistemi di protezione	<input checked="" type="checkbox"/>	12%
		 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	8%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	<input checked="" type="checkbox"/>	12%
		 V0077 - Accessi_Carenza requisito di complessità	8%	Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	12%
		 V0074 - Accessi _ Assenza sistema di autenticazione	8%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	12%
		 V0151 - Gestione IT_Presenza asset obsoleti	8%	Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	<input checked="" type="checkbox"/>	12%
		 V0088 - Accessi_Assenza logout	8%	E' attivo un sistema di logout in caso di errato inserimento credenziali oltre una soglia predefinita	<input checked="" type="checkbox"/>	12%
		 V0119 - Malware_Assenza o inadeguatezza sistemi di protezione da malware	8%	Sono presenti e aggiornati idonei sistemi di protezione da malware (software dannoso)	<input checked="" type="checkbox"/>	12%
		 V0122 - Assenza firewall per tutti i dispositivi collegati in rete	8%	E' presente un firewall per tutti i dispositivi collegati in rete (individuale o centralizzato)	<input checked="" type="checkbox"/>	12%
		 V0076 - Accessi_Carenza tipo autenticazione	8%	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.	<input checked="" type="checkbox"/>	12%
		 V0117 - Log_Assenza sistema di log degli eventi	7%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	11%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0075 - Accessi_Carenza profili di autorizzazione	7%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	11%
		 V0089 - Accessi_Assenza timeout di inattività	7%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	11%
		 V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	7%	Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	<input checked="" type="checkbox"/>	11%
		 V0103 - Gestione IT_Mancati manutenzione e aggiornamento sistemi IT	7%	Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	<input checked="" type="checkbox"/>	11%
		 V0115 - Log_Modificabilità dati di log degli amministratori	7%	I dati di log degli amministratori sono immutabili	<input checked="" type="checkbox"/>	11%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	7%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	11%
		 V0109 - Gestione IT_Mancanza di blocco di modifiche software a utenti non autorizzati	7%	L'installazione, modifica e aggiornamento di software sugli strumenti è permessa solo agli amministratori	<input checked="" type="checkbox"/>	11%
		 V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità	7%	Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	<input checked="" type="checkbox"/>	11%
		 V0114 - Log_Assenza sistema di log degli amministratori	6%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	10%
		 V0017 - Sicurezza fisica_Assenza gruppi di continuità e/o gruppi elettrogeni	6%	Sono presenti uno o più gruppi di continuità e/o gruppi elettrogeni	<input checked="" type="checkbox"/>	9%
		 V0019 - Sicurezza fisica_Assenza filtri di protezione	6%	Sono presenti filtri di protezione per sbalzi di tensione	<input checked="" type="checkbox"/>	9%
		 V0111 - Mancata cancellazione dati	6%	I dati vengono cancellati dai dispositivi portatili e dai supporti esterni cancellabili prima di procedere al loro riutilizzo, riassegnazione o smaltimento	<input checked="" type="checkbox"/>	9%
		 V0116 - Log_Mancato riesame dei dati di log degli amministratori	6%	I dati di log degli amministratori vengono periodicamente riesaminati	<input checked="" type="checkbox"/>	9%
		 V0096 - Backup_Inadeguatezza memorizzazione immagini di installazione	6%	Le immagini d'installazione sono memorizzate offline	<input checked="" type="checkbox"/>	9%
		 V0090 - Accessi_Assenza screensaver	6%	Sono attivi gli screensaver protetti con password	<input checked="" type="checkbox"/>	9%
		 V0084 - Accessi_Mancata univocità codice identificativo	6%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	8%
		 V0083 - Accessi_Permesso utilizzo sequenza password	6%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	8%
		 V0081 - Accessi_Mancato cambio password periodico	6%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	8%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0080 - Accessi_Mancato cambio password iniziale	6%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	7%
		 V0085 - Accessi_Utilizzo utenze amministrative anonime	6%	Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso	<input checked="" type="checkbox"/>	7%
		 V0086 - Accessi_Mancata disattivazione credenziali inutilizzate	6%	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	<input checked="" type="checkbox"/>	7%
	PC_FF (Windows 10 Pro)	 V0088 - Accessi_Assenza lockout	8%	E' attivo un sistema di lockout in caso di errato inserimento credenziali oltre una soglia predefinita	<input checked="" type="checkbox"/>	12%
		 V0119 - Malware_Assenza o inadeguatezza sistemi di protezione da malware	8%	Sono presenti e aggiornati idonei sistemi di protezione da malware (software dannoso)	<input checked="" type="checkbox"/>	12%
		 V0077 - Accessi_Carenza requisito di complessità	8%	Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	12%
		 V0122 - Assenza firewall per tutti i dispositivi collegati in rete	8%	E' presente un firewall per tutti i dispositivi collegati in rete (individuale o centralizzato)	<input checked="" type="checkbox"/>	12%
		 V0151 - Gestione IT_Presenza asset obsoleti	8%	Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	<input checked="" type="checkbox"/>	12%
		 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	8%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	<input checked="" type="checkbox"/>	12%
		 V0120 - Malware_Mancata esecuzione scansioni con i sistemi di protezione	8%	Vengono periodicamente eseguite le scansioni con i sistemi di protezione	<input checked="" type="checkbox"/>	12%
		 V0076 - Accessi_Carenza tipo autenticazione	8%	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.	<input checked="" type="checkbox"/>	12%
		 V0074 - Accessi _ Assenza sistema di autenticazione	8%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	12%
		 V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità	7%	Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	<input checked="" type="checkbox"/>	11%
		 V0089 - Accessi_Assenza timeout di inattività	7%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	11%
		 V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	7%	Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	<input checked="" type="checkbox"/>	11%
		 V0075 - Accessi_Carenza profili di autorizzazione	7%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	11%
		 V0103 - Gestione IT_Mancati manutenzione e aggiornamento sistemi IT	7%	Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	<input checked="" type="checkbox"/>	11%
		 V0117 - Log_Assenza sistema di log degli eventi	7%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	11%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0115 - Log_Modificabilità dati di log degli amministratori	7%	I dati di log degli amministratori sono immutabili	<input checked="" type="checkbox"/>	11%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	7%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	11%
		 V0109 - Gestione IT_Mancanza di blocco di modifiche software a utenti non autorizzati	7%	L'installazione, modifica e aggiornamento di software sugli strumenti è permessa solo agli amministratori	<input checked="" type="checkbox"/>	11%
		 V0114 - Log_Assenza sistema di log degli amministratori	6%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	10%
		 V0111 - Mancata cancellazione dati	6%	I dati vengono cancellati dai dispositivi portatili e dai supporti esterni cancellabili prima di procedere al loro riutilizzo, assegnazione o smaltimento	<input checked="" type="checkbox"/>	9%
		 V0017 - Sicurezza fisica_Assenza gruppi di continuità e/o gruppi elettrogeni	6%	Sono presenti uno o più gruppi di continuità e/o gruppi elettrogeni	<input checked="" type="checkbox"/>	9%
		 V0019 - Sicurezza fisica_Assenza filtri di protezione	6%	Sono presenti filtri di protezione per sbalzi di tensione	<input checked="" type="checkbox"/>	9%
		 V0116 - Log_Mancato riesame dei dati di log degli amministratori	6%	I dati di log degli amministratori vengono periodicamente riesaminati	<input checked="" type="checkbox"/>	9%
		 V0090 - Accessi_Assenza screensaver	6%	Sono attivi gli screensaver protetti con password	<input checked="" type="checkbox"/>	9%
		 V0096 - Backup_Inadeguatezza memorizzazione immagini di installazione	6%	Le immagini d'installazione sono memorizzate offline	<input checked="" type="checkbox"/>	9%
		 V0081 - Accessi_Mancato cambio password periodico	6%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	8%
		 V0084 - Accessi_Mancata univocità codice identificativo	6%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	8%
		 V0083 - Accessi_Permesso utilizzo sequenza password	6%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	8%
		 V0085 - Accessi_Utilizzo utenze amministrative anonime	6%	Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso	<input checked="" type="checkbox"/>	7%
		 V0080 - Accessi_Mancato cambio password iniziale	6%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	7%
		 V0086 - Accessi_Mancata disattivazione credenziali inutilizzate	6%	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	<input checked="" type="checkbox"/>	7%
Postazioni di lavoro portatili	PC_AF(Windows 11 Pro)	 V0088 - Accessi_Assenza lockout	8%	E' attivo un sistema di lockout in caso di errato inserimento credenziali oltre una soglia predefinita	<input checked="" type="checkbox"/>	12%
		 V0120 - Malware_Mancata esecuzione scansioni con i sistemi di protezione	8%	Vengono periodicamente eseguite le scansioni con i sistemi di protezione	<input checked="" type="checkbox"/>	12%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0077 - Accessi_Carenza requisito di complessità	8%	Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	12%
		 V0122 - Assenza firewall per tutti i dispositivi collegati in rete	8%	E' presente un firewall per tutti i dispositivi collegati in rete (individuale o centralizzato)	<input checked="" type="checkbox"/>	12%
		 V0151 - Gestione IT_Presenza asset obsoleti	8%	Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	<input checked="" type="checkbox"/>	12%
		 V0119 - Malware_Assenza o inadeguatezza sistemi di protezione da malware	8%	Sono presenti e aggiornati idonei sistemi di protezione da malware (software dannoso)	<input checked="" type="checkbox"/>	12%
		 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	8%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	<input checked="" type="checkbox"/>	12%
		 V0076 - Accessi_Carenza tipo autenticazione	8%	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.	<input checked="" type="checkbox"/>	12%
		 V0074 - Accessi _ Assenza sistema di autenticazione	8%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	12%
		 V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità	7%	Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	<input checked="" type="checkbox"/>	11%
		 V0089 - Accessi_Assenza timeout di inattività	7%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	11%
		 V0075 - Accessi_Carenza profili di autorizzazione	7%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	11%
		 V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	7%	Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	<input checked="" type="checkbox"/>	11%
		 V0103 - Gestione IT_Mancati manutenzione e aggiornamento sistemi IT	7%	Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	<input checked="" type="checkbox"/>	11%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	7%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	11%
		 V0117 - Log_Assenza sistema di log degli eventi	7%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	11%
		 V0115 - Log_Modificabilità dati di log degli amministratori	7%	I dati di log degli amministratori sono immutabili	<input checked="" type="checkbox"/>	11%
		 V0109 - Gestione IT_Mancanza di blocco di modifiche software a utenti non autorizzati	7%	L'installazione, modifica e aggiornamento di software sugli strumenti è permessa solo agli amministratori	<input checked="" type="checkbox"/>	11%
		 V0114 - Log_Assenza sistema di log degli amministratori	6%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	10%
		 V0111 - Mancata cancellazione dati	6%	I dati vengono cancellati dai dispositivi portatili e dai supporti esterni cancellabili prima di procedere al loro riutilizzo, riassegnazione o smaltimento	<input checked="" type="checkbox"/>	9%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0116 - Log_Mancato riesame dei dati di log degli amministratori	6%	I dati di log degli amministratori vengono periodicamente riesaminati	<input checked="" type="checkbox"/>	9%
		 V0096 - Backup_Inadeguatezza memorizzazione immagini di installazione	6%	Le immagini d'installazione sono memorizzate offline	<input checked="" type="checkbox"/>	9%
		 V0090 - Accessi_Assenza screensaver	6%	Sono attivi gli screensaver protetti con password	<input checked="" type="checkbox"/>	9%
		 V0084 - Accessi_Mancata univocità codice identificativo	6%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	8%
		 V0083 - Accessi_Percesso utilizzo sequenza password	6%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	8%
		 V0081 - Accessi_Mancato cambio password periodico	6%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	8%
		 V0085 - Accessi_Utilizzo utenze amministrative anonime	6%	Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso	<input checked="" type="checkbox"/>	7%
		 V0080 - Accessi_Mancato cambio password iniziale	6%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	7%
		 V0086 - Accessi_Mancata disattivazione credenziali inutilizzate	6%	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	<input checked="" type="checkbox"/>	7%
PC_ES (Windows 10 Pro)		 V0119 - Malware_Assenza o inadeguatezza sistemi di protezione da malware	8%	Sono presenti e aggiornati idonei sistemi di protezione da malware (software dannoso)	<input checked="" type="checkbox"/>	12%
		 V0120 - Malware_Mancata esecuzione scansioni con i sistemi di protezione	8%	Vengono periodicamente eseguite le scansioni con i sistemi di protezione	<input checked="" type="checkbox"/>	12%
		 V0088 - Accessi_Assenza logout	8%	E' attivo un sistema di logout in caso di errato inserimento credenziali oltre una soglia predefinita	<input checked="" type="checkbox"/>	12%
		 V0151 - Gestione IT_Presenza asset obsoleti	8%	Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	<input checked="" type="checkbox"/>	12%
		 V0077 - Accessi_Carenza requisito di complessità	8%	Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	12%
		 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	8%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	<input checked="" type="checkbox"/>	12%
		 V0122 - Assenza firewall per tutti i dispositivi collegati in rete	8%	E' presente un firewall per tutti i dispositivi collegati in rete (individuale o centralizzato)	<input checked="" type="checkbox"/>	12%
		 V0074 - Accessi_Assenza sistema di autenticazione	8%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	12%
		 V0076 - Accessi_Carenza tipo autenticazione	8%	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.	<input checked="" type="checkbox"/>	12%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità	7%	Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	<input checked="" type="checkbox"/>	11%
		 V0103 - Gestione IT_Mancati manutenzione e aggiornamento sistemi IT	7%	Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	<input checked="" type="checkbox"/>	11%
		 V0075 - Accessi_Carenza profili di autorizzazione	7%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	11%
		 V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	7%	Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	<input checked="" type="checkbox"/>	11%
		 V0089 - Accessi_Assenza timeout di inattività	7%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	11%
		 V0115 - Log_Modificabilità dati di log degli amministratori	7%	I dati di log degli amministratori sono immutabili	<input checked="" type="checkbox"/>	11%
		 V0109 - Gestione IT_Mancanza di blocco di modifiche software a utenti non autorizzati	7%	L'installazione, modifica e aggiornamento di software sugli strumenti è permessa solo agli amministratori	<input checked="" type="checkbox"/>	11%
		 V0117 - Log_Assenza sistema di log degli eventi	7%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	11%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	7%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	11%
		 V0114 - Log_Assenza sistema di log degli amministratori	6%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	10%
		 V0111 - Mancata cancellazione dati	6%	I dati vengono cancellati dai dispositivi portatili e dai supporti esterni cancellabili prima di procedere al loro riutilizzo, riassegnazione o smaltimento	<input checked="" type="checkbox"/>	9%
		 V0116 - Log_Mancato riesame dei dati di log degli amministratori	6%	I dati di log degli amministratori vengono periodicamente riesaminati	<input checked="" type="checkbox"/>	9%
		 V0090 - Accessi_Assenza screensaver	6%	Sono attivi gli screensaver protetti con password	<input checked="" type="checkbox"/>	9%
		 V0096 - Backup_Inadeguatezza memorizzazione immagini di installazione	6%	Le immagini d'installazione sono memorizzate offline	<input checked="" type="checkbox"/>	9%
		 V0084 - Accessi_Mancata univocità codice identificativo	6%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	8%
		 V0083 - Accessi_Permesso utilizzo sequenza password	6%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	8%
		 V0081 - Accessi_Mancato cambio password periodico	6%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	8%
		 V0080 - Accessi_Mancato cambio password iniziale	6%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	7%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0085 - Accessi_Utilizzo utenze amministrative anonime	6%	Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso	<input checked="" type="checkbox"/>	7%
		 V0086 - Accessi_Mancata disattivazione credenziali inutilizzate	6%	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	<input checked="" type="checkbox"/>	7%
	PC_MF (Windows 11 Pro)	 V0122 - Assenza firewall per tutti i dispositivi collegati in rete	8%	E' presente un firewall per tutti i dispositivi collegati in rete (individuale o centralizzato)	<input checked="" type="checkbox"/>	12%
		 V0119 - Malware_Assenza o inadeguatezza sistemi di protezione da malware	8%	Sono presenti e aggiornati idonei sistemi di protezione da malware (software dannoso)	<input checked="" type="checkbox"/>	12%
		 V0088 - Accessi_Assenza lockout	8%	E' attivo un sistema di lockout in caso di errato inserimento credenziali oltre una soglia predefinita	<input checked="" type="checkbox"/>	12%
		 V0151 - Gestione IT_Presenza asset obsoleti	8%	Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	<input checked="" type="checkbox"/>	12%
		 V0077 - Accessi_Carenza requisito di complessità	8%	Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	12%
		 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	8%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	<input checked="" type="checkbox"/>	12%
		 V0120 - Malware_Mancata esecuzione scansioni con i sistemi di protezione	8%	Vengono periodicamente eseguite le scansioni con i sistemi di protezione	<input checked="" type="checkbox"/>	12%
		 V0076 - Accessi_Carenza tipo autenticazione	8%	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.	<input checked="" type="checkbox"/>	12%
		 V0074 - Accessi _ Assenza sistema di autenticazione	8%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	12%
		 V0107 - Gestione IT_Carenza strumenti di scansione delle vulnerabilità	7%	Sono utilizzati strumenti di scansione delle vulnerabilità, regolarmente aggiornati, con tutte le più rilevanti vulnerabilità di sicurezza	<input checked="" type="checkbox"/>	11%
		 V0075 - Accessi_Carenza profili di autorizzazione	7%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	11%
		 V0103 - Gestione IT_Mancati manutenzione e aggiornamento sistemi IT	7%	Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	<input checked="" type="checkbox"/>	11%
		 V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	7%	Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	<input checked="" type="checkbox"/>	11%
		 V0089 - Accessi_Assenza timeout di inattività	7%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	11%
		 V0115 - Log_Modificabilità dati di log degli amministratori	7%	I dati di log degli amministratori sono immutabili	<input checked="" type="checkbox"/>	11%
		 V0109 - Gestione IT_Mancanza di blocco di modifiche software a utenti non autorizzati	7%	L'installazione, modifica e aggiornamento di software sugli strumenti è permessa solo agli amministratori	<input checked="" type="checkbox"/>	11%



















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0117 - Log_Assenza sistema di log degli eventi	7%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	11%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	7%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	11%
		 V0114 - Log_Assenza sistema di log degli amministratori	6%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	10%
		 V0111 - Mancata cancellazione dati	6%	I dati vengono cancellati dai dispositivi portatili e dai supporti esterni cancellabili prima di procedere al loro riutilizzo, riassegnazione o smaltimento	<input checked="" type="checkbox"/>	9%
		 V0116 - Log_Mancato riesame dei dati di log degli amministratori	6%	I dati di log degli amministratori vengono periodicamente riesaminati	<input checked="" type="checkbox"/>	9%
		 V0096 - Backup_Inadeguatezza memorizzazione immagini di installazione	6%	Le immagini d'installazione sono memorizzate offline	<input checked="" type="checkbox"/>	9%
		 V0090 - Accessi_Assenza screensaver	6%	Sono attivi gli screensaver protetti con password	<input checked="" type="checkbox"/>	9%
		 V0083 - Accessi_Percesso utilizzo sequenza password	6%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	8%
		 V0084 - Accessi_Mancata univocità codice identificativo	6%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	8%
		 V0081 - Accessi_Mancato cambio password periodico	6%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	8%
		 V0080 - Accessi_Mancato cambio password iniziale	6%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	7%
		 V0085 - Accessi_Utilizzo utenze amministrative anonime	6%	Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso	<input checked="" type="checkbox"/>	7%
		 V0086 - Accessi_Mancata disattivazione credenziali inutilizzate	6%	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono automaticamente disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	<input checked="" type="checkbox"/>	7%
Switch	Switch	 V0151 - Gestione IT_Presenza asset obsoleti	7%	Gli asset vengono sostituiti o aggiornati a nuova versione quando i produttori non rilasciano più aggiornamenti di sicurezza	<input checked="" type="checkbox"/>	12%
		 V0105 - Gestione IT_Mancata esecuzione aggiornamento patch	7%	Vengono effettuati gli aggiornamenti (patch) per contrastare la vulnerabilità dei sistemi informativi	<input checked="" type="checkbox"/>	12%
		 V0074 - Accessi _ Assenza sistema di autenticazione	7%	Sono utilizzate credenziali di autenticazione per l'accesso degli utenti	<input checked="" type="checkbox"/>	11%
		 V0076 - Accessi_Carenza tipo autenticazione	7%	Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato oppure in una caratteristica biometrica dell'incaricato.	<input checked="" type="checkbox"/>	11%
		 V0077 - Accessi_Carenza requisito di complessità	7%	Se prevista, le parole chiave (password) rispettano il requisito di complessità (a titolo esemplificativo: alfanumerico, minimo 8 caratteri, Minuscole, Maiuscole, Simboli) e non sono riconducibili agevolmente all'incaricato	<input checked="" type="checkbox"/>	11%


















Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0115 - Log_Modificabilità dati di log degli amministratori	6%	I dati di log degli amministratori sono imm modificabili	<input checked="" type="checkbox"/>	10%
		 V0087 - Accessi_Mancata disattivazione credenziali per variazione incarico	6%	Le credenziali sono disattivate anche in caso di perdita delle qualità che consentono all'Incaricato l'accesso al sistema informatico e ai dati personali in esso custoditi o all'area ad accesso ristretto	<input checked="" type="checkbox"/>	10%
		 V0117 - Log_Assenza sistema di log degli eventi	6%	E' attivo un sistema di log degli eventi	<input checked="" type="checkbox"/>	10%
		 V0103 - Gestione IT_Mancati manutenzione e aggiornamento sistemi IT	7%	Viene effettuata periodicamente la manutenzione ordinaria e l'aggiornamento delle apparecchiature del sistema informativo	<input checked="" type="checkbox"/>	10%
		 V0078 - Accessi_Carenza credenziali utenze amministrative	6%	Sono utilizzate per le utenze amministrative credenziali di elevata robustezza sostituite con sufficiente frequenza.	<input checked="" type="checkbox"/>	10%
		 V0118 - Log_Inadeguatezza protezione strumenti e informazioni di log	6%	Gli strumenti per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati	<input checked="" type="checkbox"/>	10%
		 V0089 - Accessi_Assenza timeout di inattività	6%	Per le sessioni di lavoro (amministrative e non) sono impostati dei timeout di inattività	<input checked="" type="checkbox"/>	10%
		 V0131 - Rete_Trasmisione informazioni tramite protocolli e canali non sicuri	7%	Le informazioni sono trasmesse tramite protocolli e canali sicuri	<input checked="" type="checkbox"/>	10%
		 V0075 - Accessi_Carenza profili di autorizzazione	7%	Gli accessi ed i permessi degli utenti garantiscono i profili di autorizzazione degli incaricati in ambito di trattamento dei dati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	<input checked="" type="checkbox"/>	10%
		 V0017 - Sicurezza fisica_Assenza gruppi di continuità e/o gruppi elettrogeni	5%	Sono presenti uno o più gruppi di continuità e/o gruppi elettrogeni	<input checked="" type="checkbox"/>	9%
		 V0126 - Rete_Mancata disabilitazione delle porte non utilizzate	6%	Le porte non utilizzate sono disabilite	<input checked="" type="checkbox"/>	9%
		 V0019 - Sicurezza fisica_Assenza filtri di protezione	5%	Sono presenti filtri di protezione per sbalzi di tensione	<input checked="" type="checkbox"/>	9%
		 V0114 - Log_Assenza sistema di log degli amministratori	6%	E' attivo un sistema di log degli amministratori	<input checked="" type="checkbox"/>	9%
		 V0081 - Accessi_Mancato cambio password periodico	6%	Se previste, le parole chiave (password) vengono modificate almeno ogni sei mesi	<input checked="" type="checkbox"/>	8%
		 V0123 - Rete_Mancata disabilitazione dei punti rete non utilizzati	5%	I punti rete non utilizzati sono disabilitati	<input checked="" type="checkbox"/>	8%
		 V0083 - Accessi_Permesso utilizzo sequenza password	6%	Se previste, la sequenza delle parole chiave (password) non può essere la medesima di quelle precedenti	<input checked="" type="checkbox"/>	8%
		 V0084 - Accessi_Mancata univocità codice identificativo	6%	Il codice per l'identificazione (user name), laddove utilizzato, in particolare quello per utenze amministrative, non è assegnato ad altri incaricati, neppure in tempi diversi.	<input checked="" type="checkbox"/>	8%
		 V0116 - Log_Mancato riesame dei dati di log degli amministratori	5%	I dati di log degli amministratori vengono periodicamente riesaminati	<input checked="" type="checkbox"/>	8%





Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0080 - Accessi_Mancato cambio password iniziale	5%	Se previste, le parole chiave (password) vengono modificate al primo utilizzo	<input checked="" type="checkbox"/>	7%
		 V0085 - Accessi_Utilizzo utenze amministrative anonime	5%	Le utenze amministrative anonime, quali "Administrator", sono utilizzate solo per le situazioni di emergenza e le relative credenziali sono gestite in modo da assicurare l'imputabilità di chi ne fa uso	<input checked="" type="checkbox"/>	7%
		 V0091 - Backup_Strumenti non ridondati	5%	Lo strumento è ridondato	<input checked="" type="checkbox"/>	7%
Luoghi	ASST Papa Giovanni XXIII	 V0005 - Accesso fisico_Mancanza di sistema antintrusione	6%	Presenza di un sistema anti-intrusione nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni	<input checked="" type="checkbox"/>	10%
		 V0016 - Sicurezza fisica_Assenza sistema di climatizzazione	6%	E' installato e correttamente funzionante un sistema di climatizzazione	<input checked="" type="checkbox"/>	10%
		 V0010 - Accesso fisico_Accesso al pubblico senza presidio	6%	Se è consentito l'accesso al pubblico nelle aree di trattamento dati, l'accesso avviene con presidio	<input checked="" type="checkbox"/>	10%
		 V0004 - Accesso fisico_Accesso fisico non videosorvegliato	6%	Presenza di un sistema di videosorveglianza nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni	<input checked="" type="checkbox"/>	9%
		 V0008 - Accesso fisico_Assenza servizio di vigilanza	6%	E' attivo un servizio di vigilanza negli orari di chiusura	<input checked="" type="checkbox"/>	9%
		 V0007 - Accesso fisico_Accessi non antisfondamento	6%	Le porte/finestre nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni sono antisfondamento	<input checked="" type="checkbox"/>	9%
		 V0006 - Accesso fisico_Mancata registrazione accessi fisici	6%	Gli accessi fisici nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni vengono registrati	<input checked="" type="checkbox"/>	8%
		 V0015 - Sicurezza fisica_Aree a rischio allagamento	6%	Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni non sono a rischio allagamento (piani interrati)	<input checked="" type="checkbox"/>	8%
		 V0014 - Sicurezza fisica_Locali non antisismici	6%	I locali che contengono informazioni sensibili o critiche o le strutture di elaborazione delle informazioni sono antisismici	<input checked="" type="checkbox"/>	8%
		 V0013 - Sicurezza fisica_Mancanza sistema antincendio	6%	E' presente un sistema antincendio idoneo e periodicamente revisionato	<input checked="" type="checkbox"/>	8%
	Stanza 22	 V0002 - Accesso fisico_Accesso fisico luoghi non selezionato	6%	Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni sono ad accesso selezionato (si intende per accesso selezionato l'accesso consentito solo a personale specificatamente autorizzato, a titolo esemplificativo, tramite utilizzo di badge, chiavi ecc.)	<input checked="" type="checkbox"/>	10%
		 V0016 - Sicurezza fisica_Assenza sistema di climatizzazione	6%	E' installato e correttamente funzionante un sistema di climatizzazione	<input checked="" type="checkbox"/>	10%
		 V0003 - Accesso fisico_Accesso fisico archivi non selezionato	6%	Gli archivi che contengono informazioni sensibili o critiche sono ad accesso selezionato (si intende per accesso selezionato l'accesso consentito solo a personale specificatamente autorizzato, a titolo esemplificativo, tramite utilizzo di cassette o armadi con serratura, cassaforte ecc.)	<input checked="" type="checkbox"/>	10%
		 V0007 - Accesso fisico_Accessi non antisfondamento	6%	Le porte/finestre nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni sono antisfondamento	<input checked="" type="checkbox"/>	9%
		 V0006 - Accesso fisico_Mancata registrazione accessi fisici	6%	Gli accessi fisici nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni vengono registrati	<input checked="" type="checkbox"/>	8%

Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.	
	Stanza 23	 V0015 - Sicurezza fisica_Aree a rischio allagamento	6%	Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni non sono a rischio allagamento (piani interrati)	<input checked="" type="checkbox"/>	8%	
		 V0016 - Sicurezza fisica_Assenza sistema di climatizzazione	6%	E' installato e correttamente funzionante un sistema di climatizzazione	<input checked="" type="checkbox"/>	10%	
		 V0007 - Accesso fisico_Accessi non antisfondamento	6%	Le porte/finestre nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni sono antisfondamento	<input checked="" type="checkbox"/>	9%	
		 V0006 - Accesso fisico_Mancata registrazione accessi fisici	6%	Gli accessi fisici nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni vengono registrati	<input checked="" type="checkbox"/>	8%	
		 V0015 - Sicurezza fisica_Aree a rischio allagamento	6%	Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni non sono a rischio allagamento (piani interrati)	<input checked="" type="checkbox"/>	8%	
	Ufficio Biostatistici	 V0016 - Sicurezza fisica_Assenza sistema di climatizzazione	6%	E' installato e correttamente funzionante un sistema di climatizzazione	<input checked="" type="checkbox"/>	10%	
		 V0007 - Accesso fisico_Accessi non antisfondamento	6%	Le porte/finestre nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni sono antisfondamento	<input checked="" type="checkbox"/>	9%	
		 V0006 - Accesso fisico_Mancata registrazione accessi fisici	6%	Gli accessi fisici nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni vengono registrati	<input checked="" type="checkbox"/>	8%	
		 V0015 - Sicurezza fisica_Aree a rischio allagamento	6%	Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni non sono a rischio allagamento (piani interrati)	<input checked="" type="checkbox"/>	8%	
	Stanza 25 - Studio prof. Barbui	 V0007 - Accesso fisico_Accessi non antisfondamento	6%	Le porte/finestre nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni sono antisfondamento	<input checked="" type="checkbox"/>	9%	
		 V0006 - Accesso fisico_Mancata registrazione accessi fisici	6%	Gli accessi fisici nelle aree che contengono informazioni sensibili o critiche e nelle strutture di elaborazione delle informazioni vengono registrati	<input checked="" type="checkbox"/>	8%	
		 V0015 - Sicurezza fisica_Aree a rischio allagamento	6%	Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni non sono a rischio allagamento (piani interrati)	<input checked="" type="checkbox"/>	8%	
	Rete interna	LAN	 V0126 - Rete_Mancata disabilitazione delle porte non utilizzate	6%	Le porte non utilizzate sono disabilite	<input checked="" type="checkbox"/>	10%
			 V0123 - Rete_Mancata disabilitazione dei punti rete non utilizzati	6%	I punti rete non utilizzati sono disabilitati	<input checked="" type="checkbox"/>	9%
Organizzazione generale	FROM - Fondazione per la Ricerca Ospedale di Bergamo - Ente del Terzo Settore	 V0141 - Trattamento_Mancata individuazione tipologie di dato	6%	Sono stati individuati i tipi di dato oggetto di trattamento	<input checked="" type="checkbox"/>	9%	
		 V0143 - Trattamento_Carenza definizione ambito di trattamento	6%	E' attuato un processo formale di definizione e aggiornamento dell'ambito di trattamento	<input checked="" type="checkbox"/>	9%	
		 V0030 - Incarichi_Inadeguatezza nomina DPO	6%	In caso di nomina di un Responsabile della protezione dei dati - DPO (Data Protection Officer), il Titolare (o responsabile) del trattamento si è assicurato che il soggetto nominato possieda un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, adempia alle sue funzioni in piena indipendenza ed in assenza di conflitto di interesse, abbia la disponibilità delle risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.	<input checked="" type="checkbox"/>	9%	

Analisi delle Vulnerabilità per Asset

Tipologia Asset	Asset	Nome Vulnerabilità	% Pura	Contromisura	Attuata	% Infl.
		 V0024 - Incarichi_Carenza definizione e assegnazione incarichi	6%	Gli incarichi e le responsabilità del personale e dei collaboratori relative alla sicurezza delle informazioni sono definiti, assegnati formalmente e mantenuti aggiornati	<input checked="" type="checkbox"/>	9%
		 V0035 - Processo disciplinare_Mancata informazione su processi disciplinari	5%	Il personale dipendente e i collaboratori sono informati sulla possibilità di incorrere in un processo disciplinare in caso di mancato rispetto delle policy in tema di trattamento dei dati	<input checked="" type="checkbox"/>	8%
		 V0001 - Accesso fisico_Aree non chiaramente definite e segnalate	5%	Le aree che contengono informazioni sensibili o critiche e le strutture di elaborazione delle informazioni sono chiaramente definite e segnalate	<input checked="" type="checkbox"/>	7%
		 V0031 - Incarichi_Mancata comunicazione DPO	5%	Il Responsabile della protezione dei dati - DPO (Data Protection Officer) ha comunicato le proprie generalità all'Autorità di controllo	<input checked="" type="checkbox"/>	7%