



UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII

Dipartimento di Ingegneria
dell'Informazione



unIMC

Magic come modulo di un software gestionale

Lorenzo Lambertucci

lorenzo@sistema3.it

3337484229

Martedì 19 settembre 2023



Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Definizione del rischio



Possiamo definire il rischio come la probabilità che si verifichi un evento “indesiderato o dannoso”, insieme all'entità delle conseguenze associate a tale.

In altre parole, il rischio rappresenta la possibilità di subire perdite, danni o conseguenze negative in relazione a una certa attività, situazione o decisione (includendo anche la scelta di non agire).

Esso è spesso valutato considerando sia la probabilità di accadimento dell'evento che l'impatto delle conseguenze che ne deriverebbero.

La gestione del rischio coinvolge l'identificazione, **l'analisi, la valutazione** e la mitigazione dei potenziali rischi al fine di prendere decisioni informate e ridurre al minimo l'incidenza di eventi dannosi.

Rischio informatico



Il **rischio informatico** si riferisce alla minaccia potenziale di danni o perdite che possono verificarsi a causa di vulnerabilità nei sistemi informatici, nelle reti o nei dati. Questo tipo di rischio può derivare da una serie di fonti, tra cui attacchi informatici, accessi non autorizzati, perdite di dati, errori umani, guasti hardware o software e molto altro ancora.

Una volta valutato il rischio, le organizzazioni possono adottare misure di sicurezza e strategie di mitigazione per ridurre al minimo la probabilità che si verifichino attacchi o incidenti informatici e per limitare l'impatto in caso di accadimento.

Le strategie di gestione del rischio informatico possono includere l'implementazione di sistemi di sicurezza informatica, la formazione del personale, la creazione di politiche di sicurezza, il monitoraggio costante dei sistemi e la pianificazione di piani di ripristino in caso di incidenti.

La continua evoluzione delle minacce informatiche richiede un approccio proattivo e flessibile per mantenere la sicurezza dei sistemi e dei dati.

Definizione del rischio



Il rischio è una combinazione di probabilità e di gravità:

$$R = P \times Vu \times Val$$

P = Probabilità dell'attacco

Vu = Vulnerabilità all'attacco

Val = Valore del danno provocato nel caso in cui l'attacco abbia successo

Come fare?





- La valutazione del rischio (informatico) comporta l'identificazione delle vulnerabilità nei sistemi informatici, la valutazione delle minacce che potrebbero sfruttarle e la stima delle conseguenze negative che potrebbero verificarsi in caso di violazione della sicurezza. Tale valutazione può essere effettuata attraverso molti approcci differenti,
- Le norme e gli standard forniscono delle indicazioni su come, in generale, valutare i rischi MA non forniscono degli strumenti per farlo,
- Molti strumenti sono stati sviluppati sia da enti nazionali e internazionali, sia nella letteratura scientifica:
 - Generalmente questi strumenti possono essere divisi in **QUALITATIVI** o **QUANTITATIVI**

Metodi QUALITATIVI



La valutazione **qualitativa** utilizza tipicamente una serie di metodi, principi o regole basati su categorie o livelli non numerici per la valutazione del rischio.


 É efficiente in termini di tempi e costi poiché non richiede la stima di valori esatti e possiamo identificare facilmente le aree di miglioramento


 Esperti diversi potrebbero produrre risultati diversi e riprodurre o confrontare i risultati può essere difficile, spesso impossibile

Metodi QUANTITATIVI



La valutazione **quantitativa** utilizza tipicamente una serie di metodi, principi o regole per la valutazione del rischio basati sull'uso di numeri

 I risultati della valutazione quantitativa sono rigorosi, ripetibili e riproducibili e la stima delle probabilità e degli impatti degli eventi può essere confrontata in modo diretto e oggettivo.

 La stima delle probabilità e degli impatti è molto impegnativa e i risultati potrebbero non essere sempre chiari, costi elevati e strumenti non disponibili.

Metodo HTMA



La procedura **HTMA** (Host-based Threat Modeling and Analysis) è una metodologia quantitativa utilizzata per valutare e mitigare le minacce e i rischi relativi ad un sistema o a un host specifico. Questo approccio è basato sulla Simulazione Monte Carlo.

La procedura HTMA segue generalmente questi passaggi:

1. Identificazione degli asset e analisi delle minacce: definire la lista degli eventi (minacce) di cui si vuole valutare il rischio. Questa fase aiuta a comprendere cosa è necessario proteggere.
2. Valutazione delle vulnerabilità: esaminare le potenziali vulnerabilità dell'host, configurazioni errate o debolezze nelle politiche di sicurezza, ecc. Questa fase richiede una valutazione accurata per comprendere le potenziali vie di attacco.
3. Determinazione del rischio, stima delle probabilità di accadimento e dell'impatto di ciascun evento: stimare il rischio associato a ciascuna vulnerabilità identificata.
4. Generazione degli scenari attraverso la simulazione Monte Carlo: l'obiettivo è quello di stimare il rischio totale annuale derivante dagli eventi cyber elencati nella lista, espresso in termini di perdita monetaria.
5. Interpretazione dei risultati, definizione delle contromisure, monitoraggio continuo: sulla base delle informazioni raccolte, identificare le contromisure adeguate per mitigare le vulnerabilità e ridurre il rischio. Effettuare valutazioni periodiche per identificare eventuali nuove vulnerabilità o modifiche nel rischio.

Metodo FAIR



La procedura **FAIR** (Factor Analysis of Information Risk) è un framework utilizzato per valutare e gestire i rischi informatici in modo quantitativo. Questa metodologia mira a fornire una valutazione più precisa e oggettiva dei rischi, prendendo in considerazione i fattori fondamentali che contribuiscono all'analisi del rischio ed è basato su un' Ontologia del Rischio e su Simulazioni Monte Carlo.

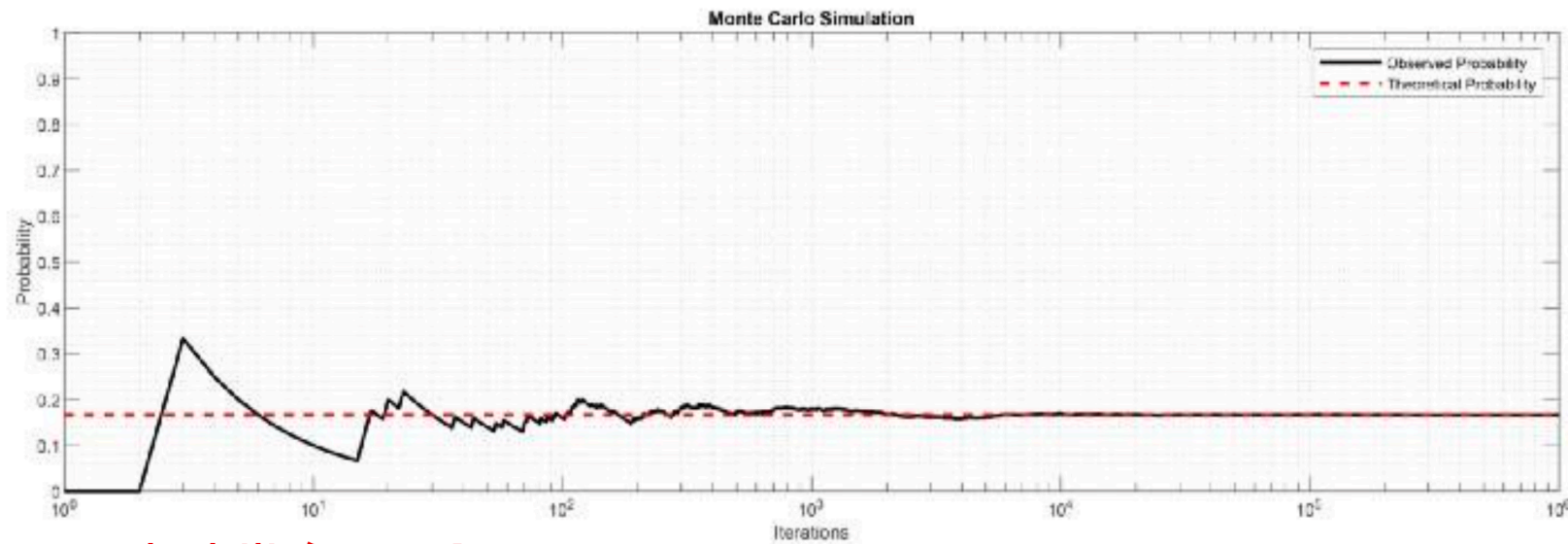
La procedura FAIR segue generalmente questi passaggi:

1. **Identificazione degli asset:** Definizione dello scenario sotto esame e decomposizione in sotto-scenari. Questa fase aiuta a comprendere cosa è necessario proteggere e quali sono le informazioni di maggiore importanza.
2. **Valutazione delle minacce, delle vulnerabilità e degli impatti:** Identificazione e stima per ogni sotto-scenario. Le minacce possono essere attacchi informatici, violazioni dei dati, disastri naturali o errori umani. Analizzare le vulnerabilità o le debolezze all'interno del sistema che potrebbero essere sfruttate dalle minacce identificate. Determinare gli impatti potenziali che possono verificarsi in caso di exploit delle vulnerabilità.
3. **Calcolo e gestione del rischio:** Utilizzando dati e metodi quantitativi, calcolare il rischio associato a ciascuna combinazione di minacce, vulnerabilità e impatti. Assegnazione di valori numerici alle probabilità di occorrenza delle minacce, alla gravità delle vulnerabilità e agli impatti previsti. Sulla base dei risultati della valutazione del rischio, sviluppare strategie di mitigazione e gestione del rischio. (Simulazione Monte Carlo)
4. **Monitoraggio, interpretazione dei dati e revisione continua:** La gestione del rischio è un processo in continuo sviluppo. È importante monitorare costantemente l'ambiente di sicurezza, rivedere e aggiornare le valutazioni del rischio e adattare le strategie di mitigazione in base all'evoluzione delle minacce e delle vulnerabilità.

Simulazione Monte Carlo



Un tipo di algoritmo che utilizza una campionatura casuale ripetuta un elevato numero di volte per ottenere la probabilità del verificarsi di un intervallo di risultati.

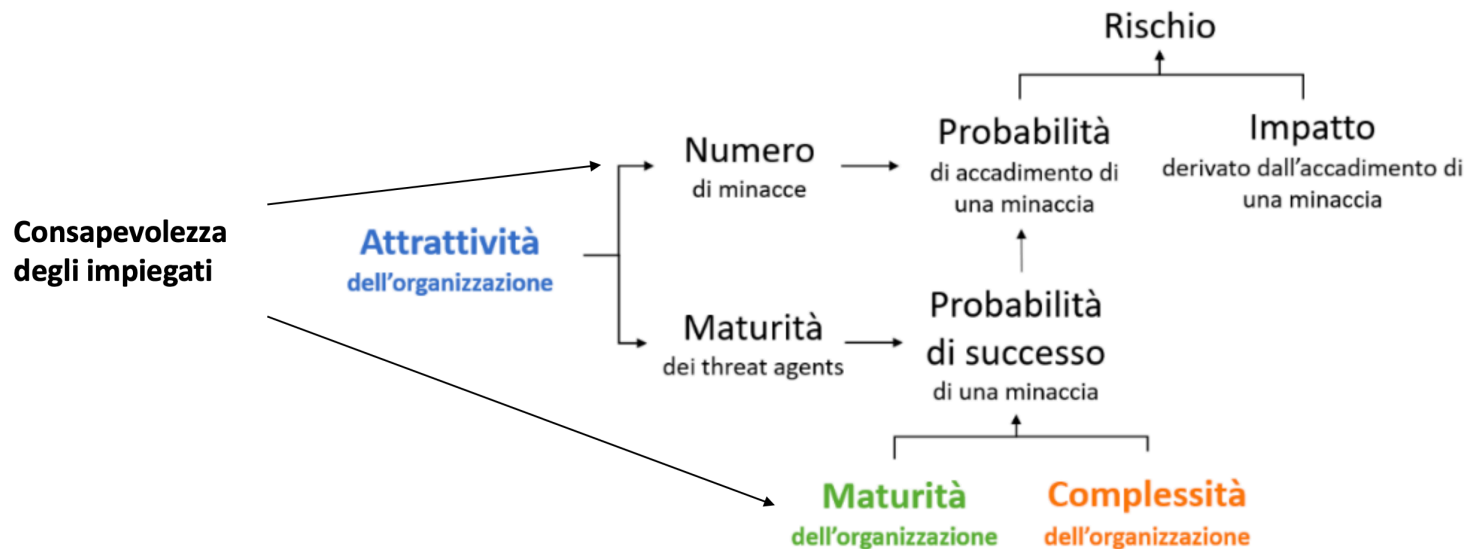


Probabilità **teorica**

MAGIC



- Metodo **quantitativo** semplice ed efficiente per valutare il rischio cyber. Modello probabilistico per calcolare la probabilità che si verifichi un incidente informatico, basato sulla valutazione della postura informatica dell'organizzazione/azienda bersaglio
- Magic consente di derivare input su misura per metodi di valutazione del rischio probabilistici, come HTMA (How To Measure Anything in cybersecurity risk), FAIR (Factor Analysis of Information Risk) e altri, riducendo così notevolmente il margine di soggettività nella valutazione del rischio informatico. Confermiamo il nostro approccio attraverso un confronto **qualitativo e quantitativo** con diversi metodi esistenti.



Magic e Logico cloud

Implementazione del modulo Magic all'interno del software gestionale Logico cloud



<https://magic.logico.cloud>



Magic e Logico cloud



- Permettere all'azienda "x" di fare un'analisi anche periodica o ricorrente per capire che probabilità ha di avere un'attacco.
- Adottare tecnologie e metodi migliorativi all'interno dell'azienda in modo di ricalcolare le probabilità e gli indici
- Possibilità di prevedere differenti scenari
- Personalizzazione e report dedicati

Inserimento dati di analisi - Generali



In questa pagina vengono inseriti i dati (come il caso d'uso e la tipologia dell'organizzazione) relativi all'azienda o all'organizzazione che sta effettuando la valutazione del rischio.

The screenshot shows the 'Logico-Cloud' interface for editing a questionnaire. The main title is 'MODIFICA QUESTIONARIO'. The left sidebar contains navigation options: 'Admin Sistema 3', 'Questionari', 'Impostazioni', 'Logout', and 'Riduci menu'. The top right corner has buttons for 'ANNULLA', 'APPLICA', and 'SALVA'. The main content area is titled 'DATI QUESTIONARIO' and includes the following fields:

- *Nome organizzazione:** Sistema3
- Referente:** Lorenzo Lambertucci
- Email:** lorenzo@sistema3.it
- *Data Valutazione:** 23/08/2023
- Caso d'uso:** CyberSecurity
- Tipologia organizzazione:** Online Services / Cloud
- Descrizione generale dell'infrastruttura:** (Empty text area)
- Descrizione generale delle modalità di gestione dell'infrastruttura:** (Empty text area)

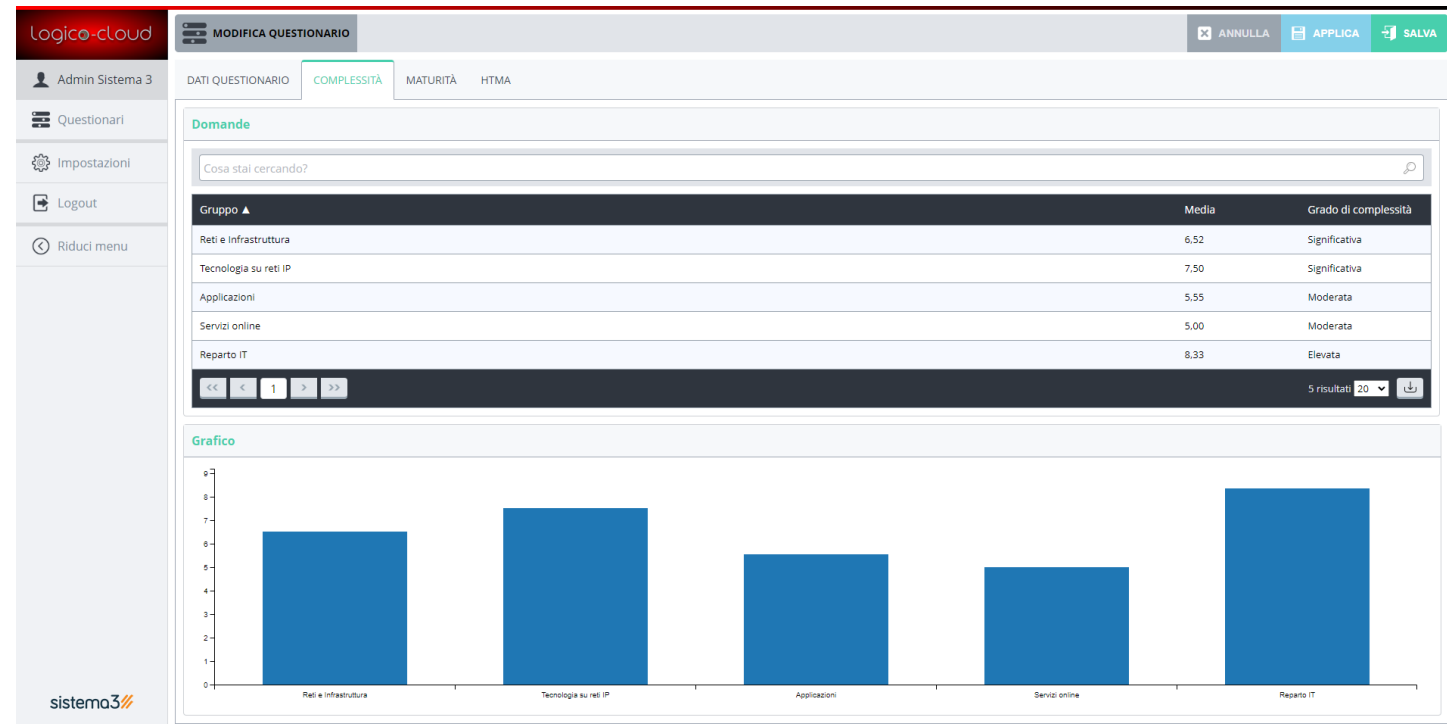
The 'sistema3' logo is visible in the bottom left corner of the interface.

Inserimento dati di analisi - Complessità organizzativa



In questa sezione l'utente andrà a rispondere ad una serie di domande divise per gruppo in base alla tipologia dell'azienda/organizzazione e al caso d'uso che valuteranno i gradi di complessità dell'azienda/organizzazione.

Subito sotto verrà generato un istogramma che mostra i livelli di complessità raggiunti. (Figura 2.2)



Inserimento dati di analisi - Complessità organizzativa



Elenco delle domande relative al caso d'uso "cybersercurity"

logico-cloud

MODIFICA GRUPPI QUESTIONARIO - SISTEMA3

ANNULLA APPLICA SALVA

Admin Sistema 3

Questionari

Impostazioni

Logout

Riduci menu

Gruppo: Reti e Infrastruttura Media: 6,522727

*Domanda:	*Risposta:	Risposta:
Numero complessivo di Postazioni di Lavoro (PdL)	Numero delle PdL tra 11 e 50	22
Numero totale di server, compresi i server virtuali	Numero dei server tra 31 e 100	33
Sistemi fisici connessi alla rete aziendale (servers, storage, switch, router, firewall) - escluso IoT	Numero dei sistemi tra 201 e 500	
Sistemi HW in End-of-life (server, storage, switch, router e firewall)	Diversi sistemi che raggiungeranno EOL entro 2 anni e alcuni ...	
Numero totale di connessioni esterne (sedi, uffici, punti vendita ecc.) comprese le connessioni Internet	21 - 50 connessioni	
Numero di connessioni (non utenti) dall'esterno non sicure (FTP, Telnet, rlogin, VNC ...)	4-7 connessioni non protette	
Clienti o partner con connessioni dedicate	9-20 connessioni dedicate	
Accesso a Reti Wireless	Numero significativo di utenti della rete wireless o di access p...	
Utilizzo di dispositivi personali in grado di collegarsi alla rete aziendale	Fino al <25% dei dipendenti autorizzati	
Numero di installazioni di Sistemi Operativi SERVER in End-of-life (privi di supporto ufficiale del produttore)	Numero x dei sistemi operativi SERVER che hanno superato E...	
Numero di installazioni di Sistemi Operativi CLIENT in End-of-life (privi di supporto ufficiale del produttore)	Numero x dei sistemi operativi CLIENT che hanno superato E...	

Creato da Admin Sistema 3 il 23/08/2023 09:50
Modificato da Admin Sistema 3 il 29/08/2023 18:45

ANNULLA APPLICA SALVA

UNA REALIZZAZIONE SISTEMA 3 INFORMATICA - PIATTAFORMA LOGICO-CLOUD v4.19.2

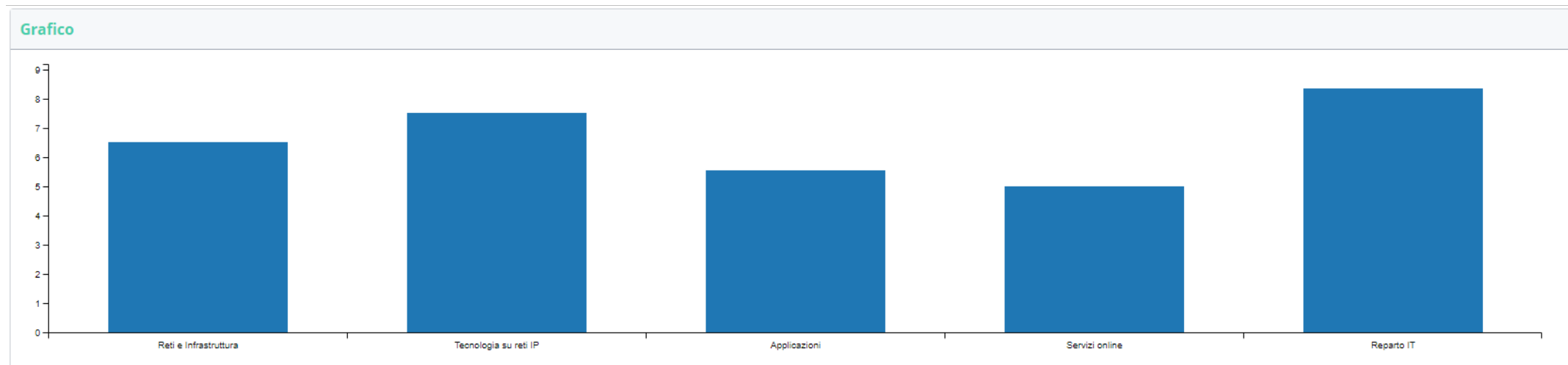
sistemo3

javascript:void(0)

Inserimento dati di analisi - Complessità organizzativa



Dalle risposte che verranno date sarà generato un istogramma che mostra i livelli di complessità raggiunti.



Inserimento dati di analisi - Maturità



In questa sezione del questionario andiamo a calcolare il livello di maturità dell'azienda/organizzazione rispondendo alle domande che verranno inserite a seconda del caso d'uso che stiamo analizzando.

The screenshot shows the 'logico-cloud' interface for editing a questionnaire. The main content area is titled 'MODIFICA QUESTIONARIO' and is divided into sections: 'DATI QUESTIONARIO', 'COMPLESSITÀ', 'MATURITÀ', and 'HTMA'. The 'MATURITÀ' section is active, showing a maturity level of 8,67 for 'Alta' attractiveness. Below this, there is a table of questions and answers.

*Domande:	Risposte:
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'intern...	Si
I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quel...	No
Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.	In parte
È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni...	In parte
Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.	Si
Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.	Si
Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più s...	Si
Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'acce...	Si
Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.	Si
Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro de...	Si
La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli...	Si
Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono con...	Si
Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-i...	Si
In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengon...	Si
Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obs...	Si

Inserimento dati di analisi - Maturità



Probabilità di attacco e di successo di varie minacce.

In questa sezione possono essere inserite 3 variabili per ogni minaccia (n° tentativi attacco (previsti), Limite Inferiore (Euro), Limite Superiore (Euro)).

Questi 3 valori vengono poi utilizzati nella simulazione di attacco, utilizzando il metodo Monte Carlo e per calcolare la probabilità di accadimento.

Minaccia	Probabilità di successo	n° tentativi attacco (previsto)	Probabilità accadimento	Limite inferiore (Euro)	Limite superiore (Euro)
Malware	12%	22	95%	1000	2500000
Web based attacks	15%	3	41%	100000	2000000
Phishing	27%	3	60%	1000	1600000
Web application attacks	15%	4	51%	1000	500000
Spam	19%	11	90%	1000	1600000
DDoS	19%	1	20%	50000	2000000
Identity Theft	6%	23	83%	1000	100000
Data breach	8%	2	18%	10000	4000000
Insider Threat	8%	6	46%	10000	700000
Botnets	12%	8	69%	50000	2000000
Physical manipulation damage theft and loss	8%	9	58%	1000	60000
Information leakage	9%	4	35%	10000	4000000
Ransomware	12%	11	79%	300	170000
Cyberespionage	12%	23	95%	1000	70000
Cryptojacking	19%	1	20%	1000	10000

Minaccia:	Malware	Probabilità accadimento:	% 99,98	Probabilità di successo:	% 89,85	n° tentativi attacco (previsto):	10
Limite inferiore (Euro):	1000	Limite superiore (Euro):	2500000				

Inserimento dati di analisi - Simulazione



Nella prima parte della schermata HTMA vengono inseriti tutti i parametri necessari allo svolgimento della simulazione di attacco tramite il metodo Monte Carlo.

(Numero di iterazioni, metodo Bin e le soglie per una probabilità di perdita al **X%**)

The screenshot shows the 'MODIFICA QUESTIONARIO' (Modify Questionnaire) interface in the Logico-cloud system. The 'HTMA' tab is selected. The 'Impostazioni simulazione' (Simulation Settings) section contains the following fields:

Field	Value
Iterazioni:	1000
Metodo Bin:	Default
Bin custom:	
Soglia per una probabilità di perdita pari allo 0% (in €):	4000000
Soglia per una probabilità di perdita pari al 10% (in €):	1100000
Soglia per una probabilità di perdita pari al 20% (in €):	900000
Soglia per una probabilità di perdita pari al 30% (in €):	700000
Soglia per una probabilità di perdita pari al 40% (in €):	600000
Soglia per una probabilità di perdita pari al 50% (in €):	550000
Soglia per una probabilità di perdita pari al 60% (in €):	500000
Soglia per una probabilità di perdita pari al 70% (in €):	450000
Soglia per una probabilità di perdita pari al 80% (in €):	400000
Soglia per una probabilità di perdita pari al 90% (in €):	350000
Soglia per una probabilità di perdita pari al 100% (in €):	300000

At the bottom of the form, there is a button labeled 'Avvia simulazione' (Start simulation).

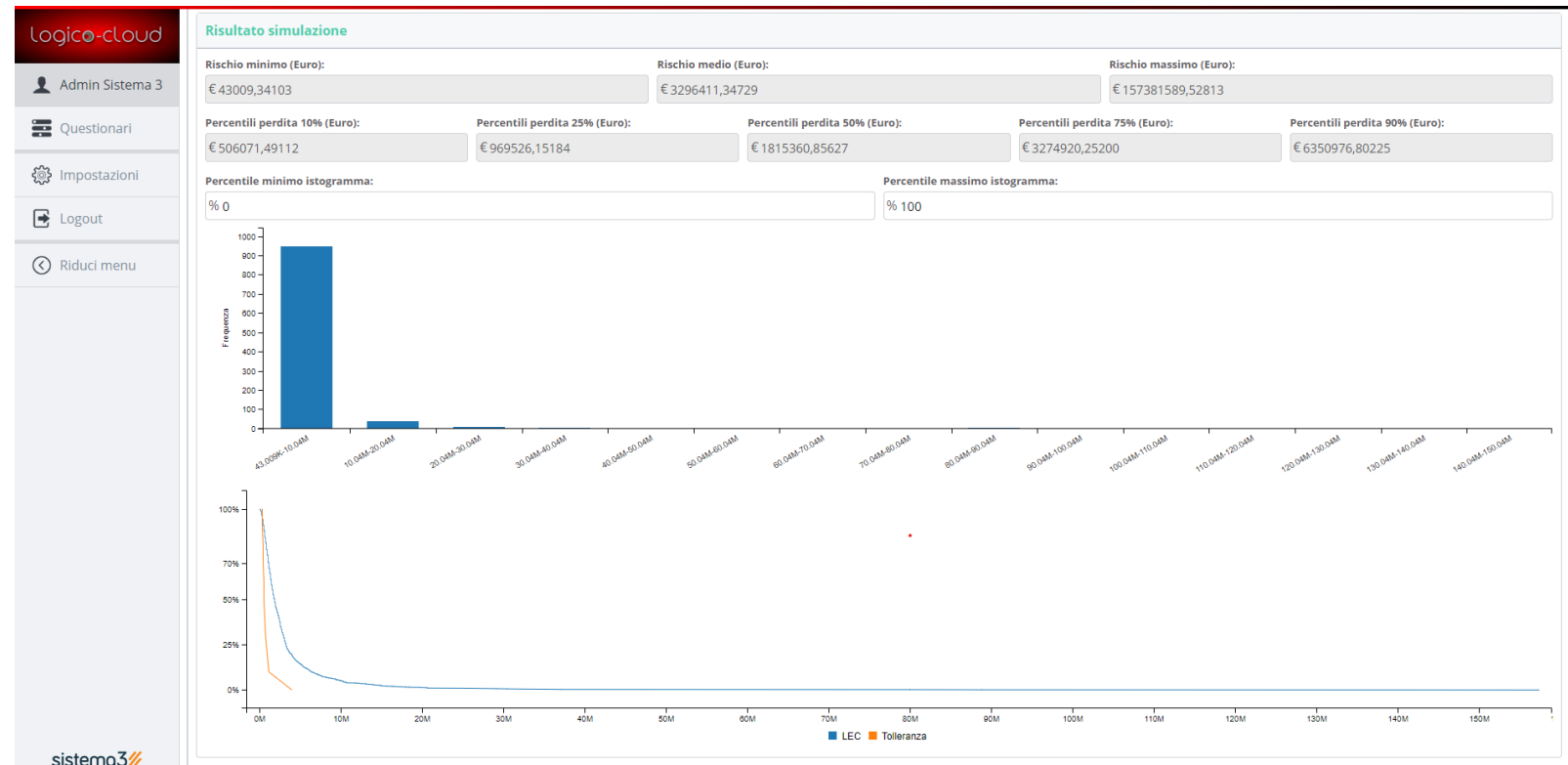
Avvia simulazione

Inserimento dati di analisi - Simulazione



In questa seconda sezione vengono mostrati i risultati della simulazione:

1. Rischio Minimo, Medio e Massimo,
2. Percentili di perdita,
3. Istogramma delle perdite,
4. Loss Exceedance Curve (LEC).



Configurazione iniziale del caso d'uso



In questa sezione, dedicata all'amministratore di sistema o alla figura identificata a svolgere questa attività, andremo a configurare i questionari.

Sarà possibile aggiungere e modificare i casi d'uso presenti nei questionari.

The screenshot displays the 'MODIFICA CASI D'USO' interface in Logico-Cloud. The top navigation bar includes 'Logico-cloud', 'MODIFICA CASI D'USO', and action buttons 'ANNULLA', 'APPLICA', and 'SALVA'. The left sidebar shows the user 'Admin Sistema 3' and menu items: 'Questionari', 'Impostazioni', 'Logout', and 'Riduci menu'. The main content area contains a form for editing a case named 'CyberSecurity'. The form includes fields for 'Nome' (CyberSecurity), 'Periodo di tempo per attacco' (365), and 'Step simulazione' (300). Below the form are two tables:

Gruppi domande	
Cosa stai cercando?	
Nome	
Reti e Infrastruttura	
Tecnologia su reti IP	
Applicazioni	
Servizi online	
Reparto IT	

5 risultati 20

Tipologia organizzazione	
Cosa stai cercando?	
Nome ▲	Indice Attrattività
Online Services / Cloud	Alta

1 risultato 20

Configurazione iniziale del caso d'uso



Nel dettaglio possiamo:

1. Modificare il nome del caso d'uso
2. Il periodo di tempo per l'attacco
3. Gli step da effettuare nella simulazione Monte Carlo
4. I gruppi di domande (Aggiungerne di nuovi o modificare quelli già esistenti)
5. Aggiungere o modificare la tipologia di organizzazione
6. Modificare o aggiungere i controlli per la valutazione della maturità
7. Aggiungere o modificare le minacce da mostrare nel questionario

The screenshot displays the Logico-Cloud interface. The top section is titled 'Controlli' and shows a list of 15 controls. The bottom section is titled 'Minacce' and shows a list of 15 threats. Both sections include a search bar, a '+ NUOVO' button, and a table with columns for 'Nome' and 'Ordine'. The 'Controlli' table has a 'Controllo' column with detailed descriptions. The 'Minacce' table has a 'Controllo' column with associated control names. At the bottom, there are buttons for 'ELIMINA', 'ANNULLA', 'APPLICA', and 'SALVA', along with a footer indicating 'UNA REALIZZAZIONE SISTEMA 3 INFORMATICA - PIATTAFORMA LOGICO-CLOUD v4.19.2'.

Nome	Controllo	Ordine
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	1
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	2
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	3
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	4
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	5
Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	6
Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	7
Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	8
Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	9
Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato...). I vertici aziendali hanno cura di ...	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	10
La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	11
Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	12
Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	13
In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	14
Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	15

Nome	Controllo	Ordine
Malware	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	1
Web based attacks	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	2
Phishing	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	3
Web application attacks	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	4
Spam	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	5
DDoS	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	6
Identity Theft	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda a...	7
Data breach	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda a...	8
Insider Threat	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda a...	9
Botnets	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	10
Physical manipulation d...	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda a...	11
Information leakage	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda a...	12
Ransomware	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	13
Cyberespionage	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	14
Cryptojacking	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in t...	15

■ Magic e Logico cloud



<https://magic.logico.cloud>