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.

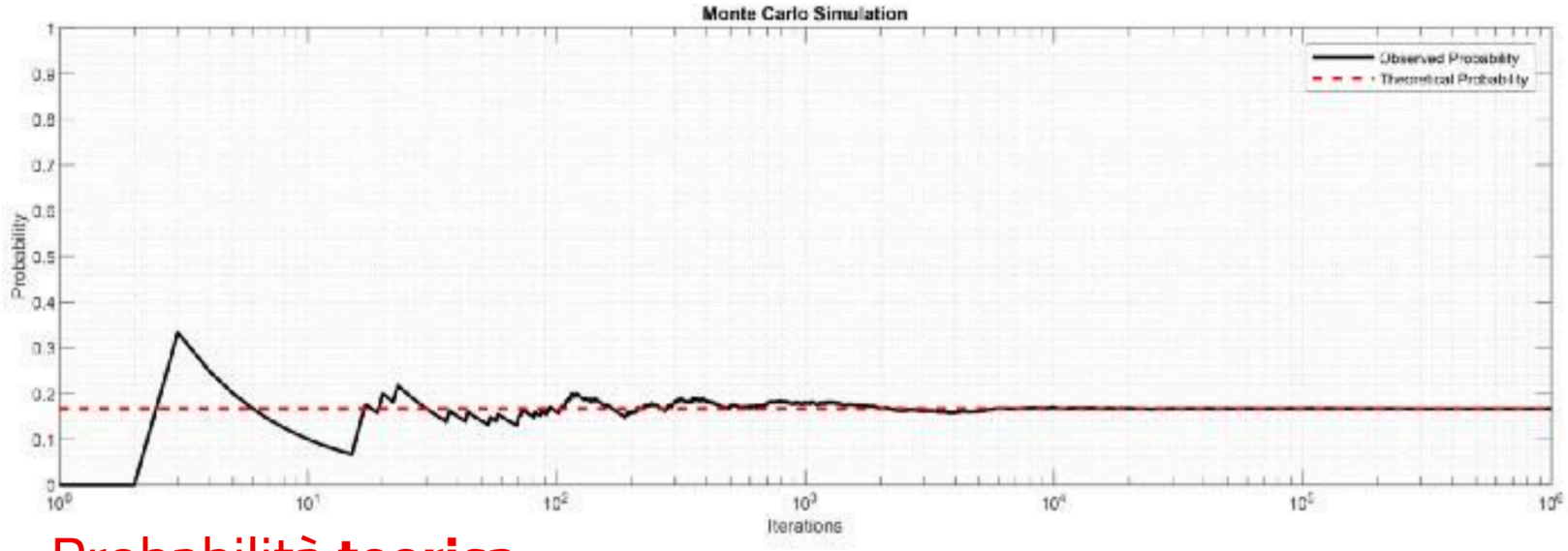
2. Valutazione delle minacce, delle vulnerabilità e degli impatti: Identificazione e stima per ogni sotto-scenario.
   Le minacce possono essere attacchi informatici, violazioni dei dati, disastri naturali o errori umani. Analizzare le vulnerabilità o le debolezze all'interno del sistema che potrebbero 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

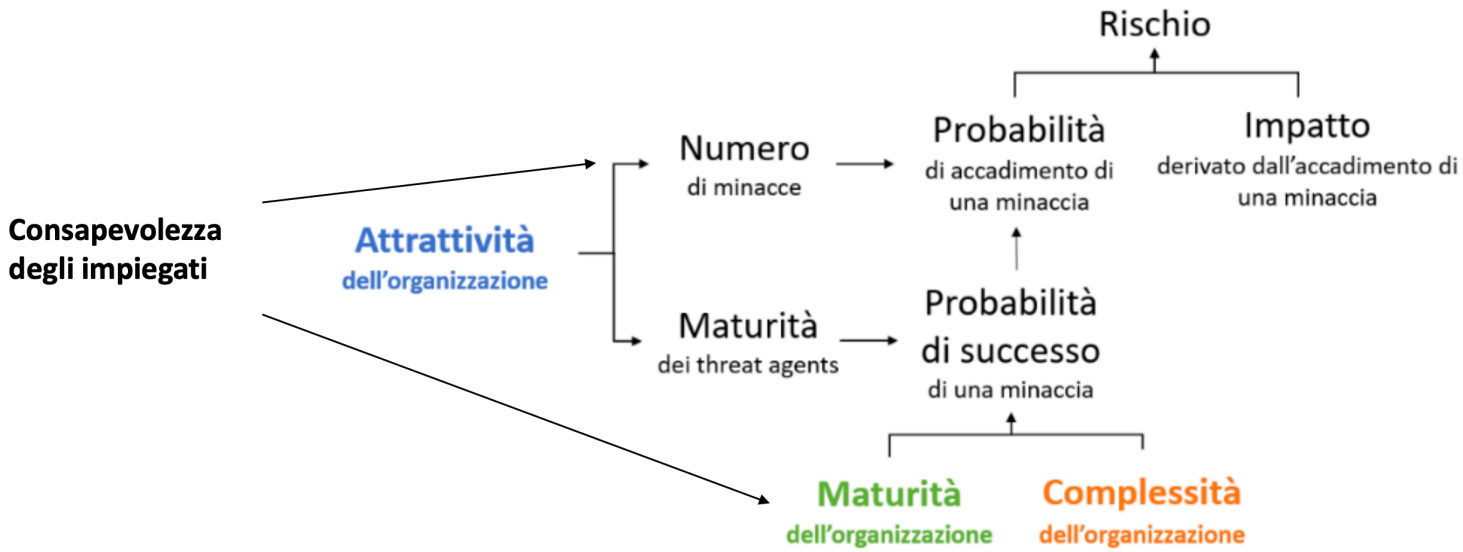
Un tipo di algoritmo che utilizza una campionatura casuale ripetuta un elevato numero di volte per ottenere la probabilità del verificarsi di un intervallo di risultati.



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

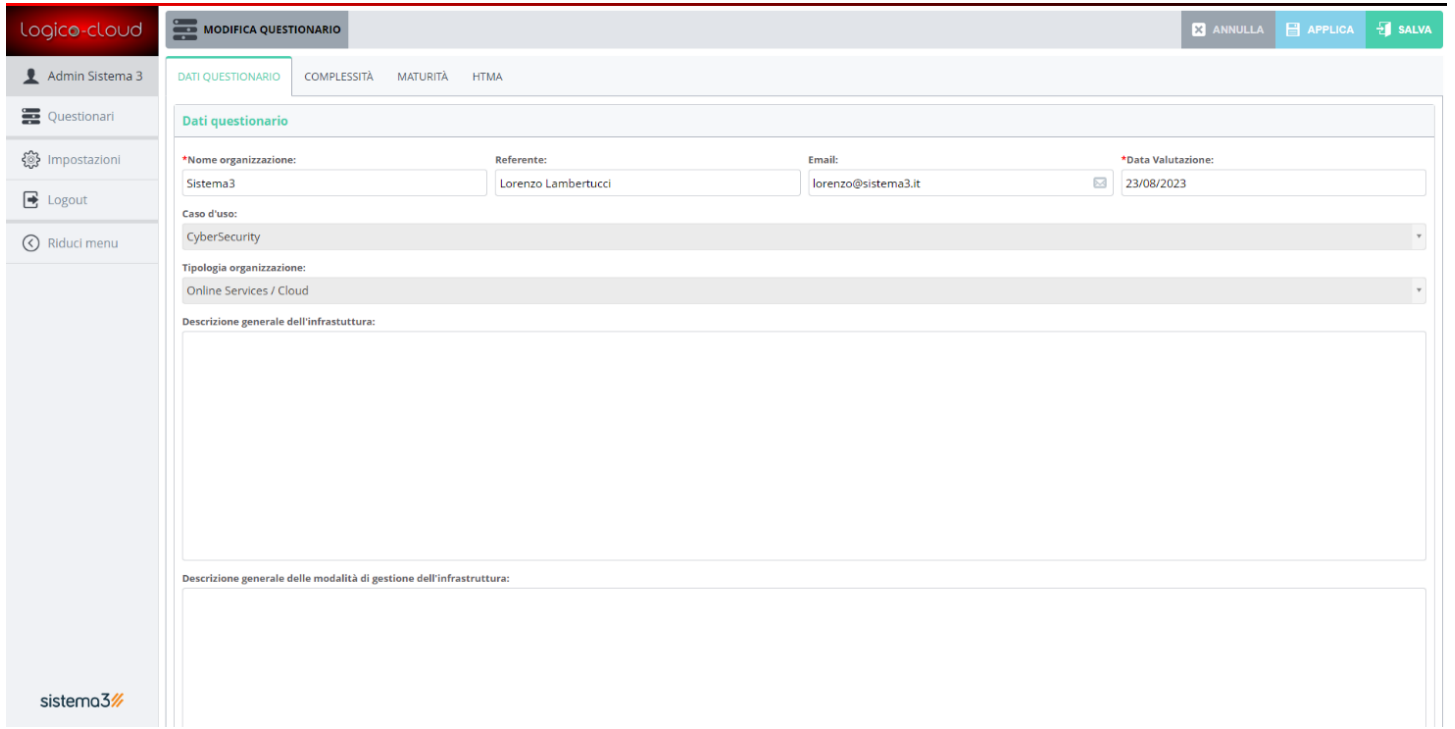
https://magic.logico.cloud

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

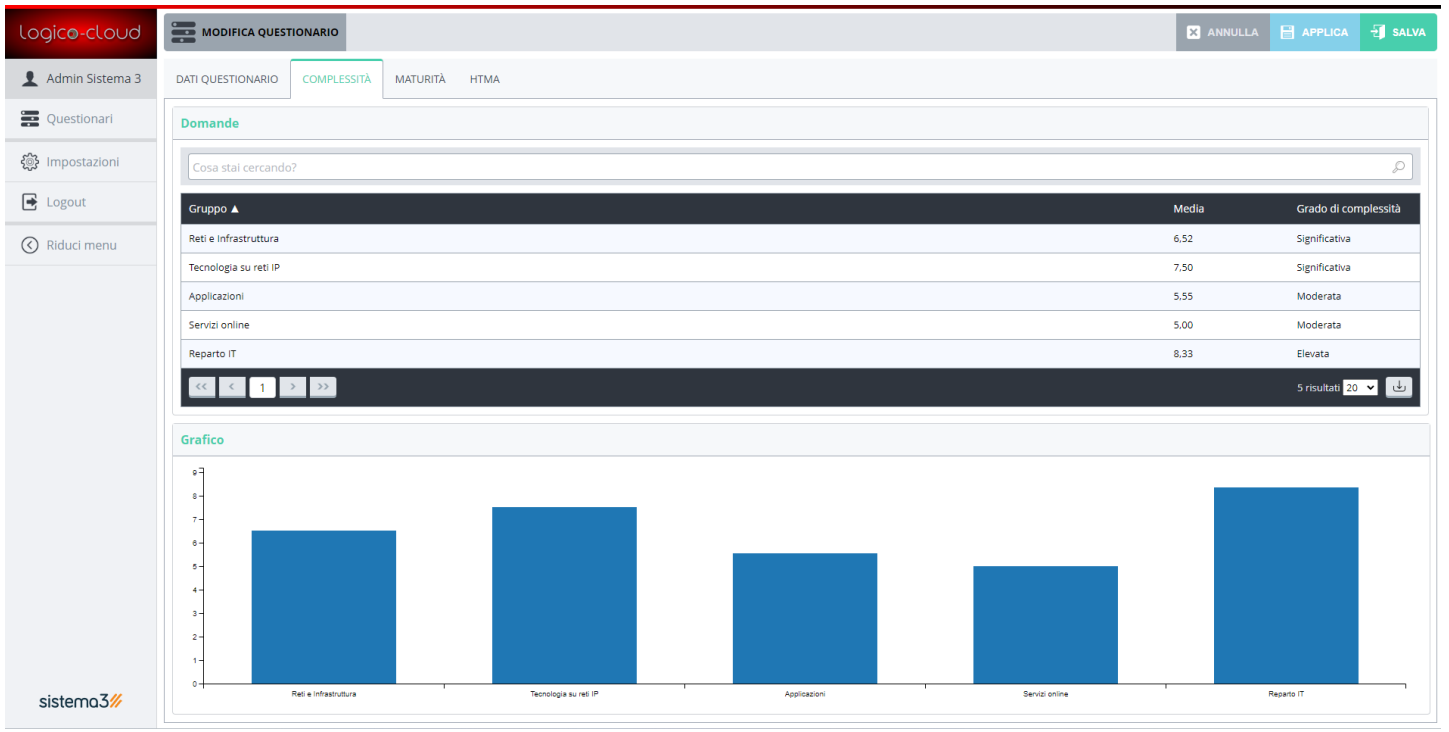
In questa pagina vengono inseriti i dati (come il caso d'uso e la tipologia dell'organizzazione) relativi all'azienda o all'organizzazione che sta effettuando la valutazione del rischio.



Inserimento dati di analisi - Complessità organizzativa

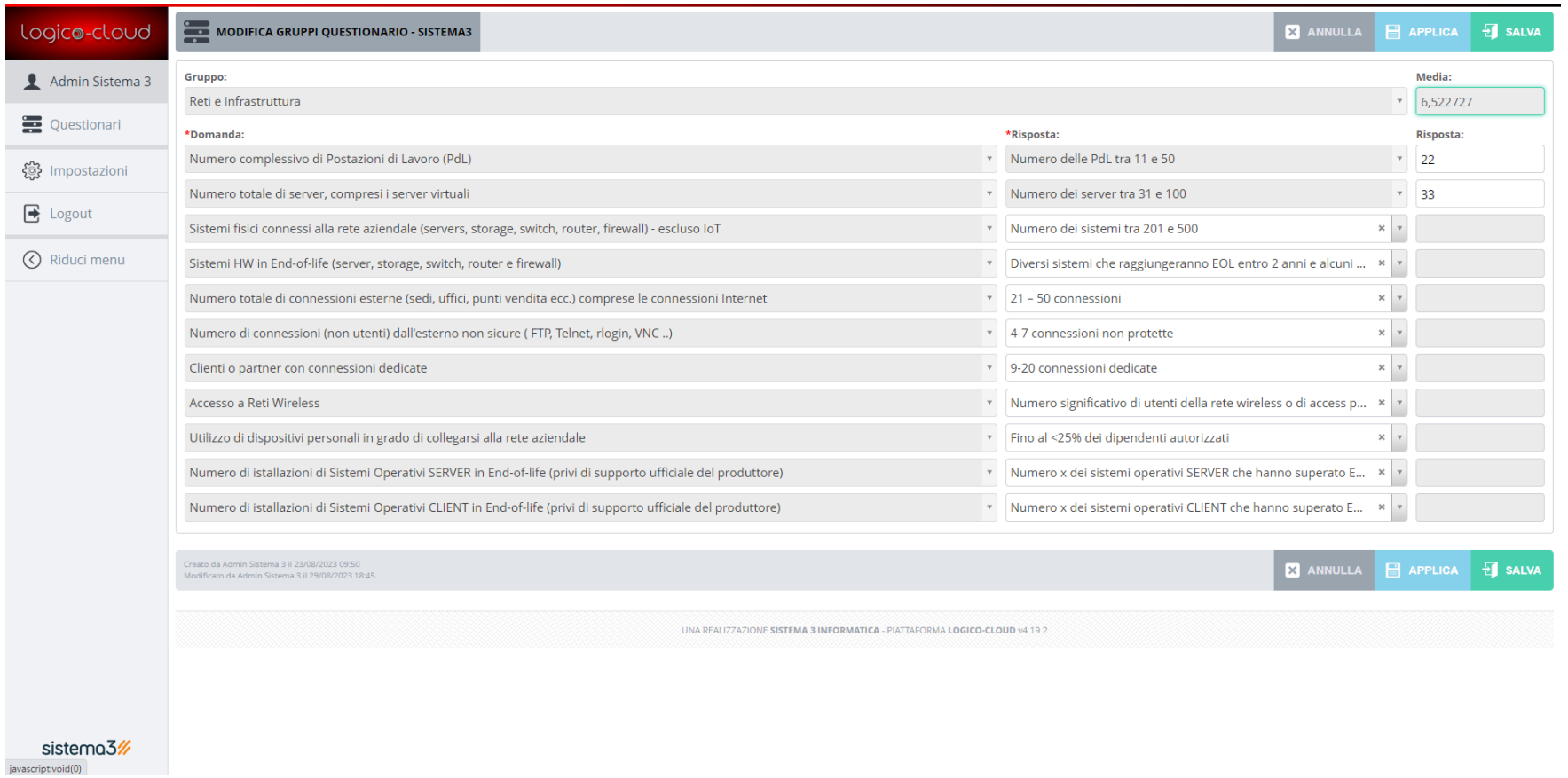
In questa sezione l'utente andrà a rispondere ad una serie di domande divise per gruppo in base alla tipologia dell'azienda/organizzazione e al caso d'uso che valuteranno i gradi di complessità dell'azienda/organizzazione.

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



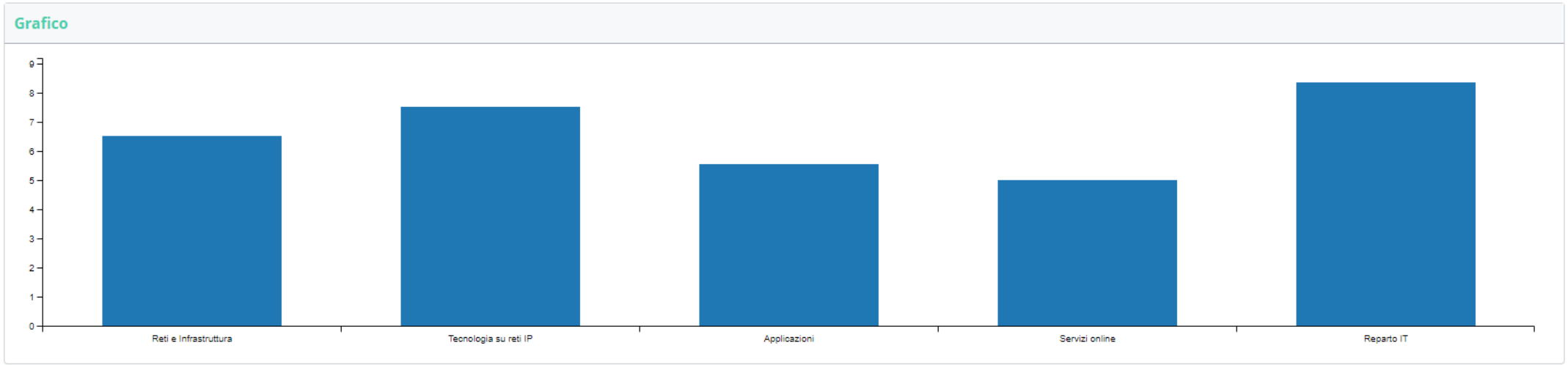
Inserimento dati di analisi - Complessità organizzativa

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



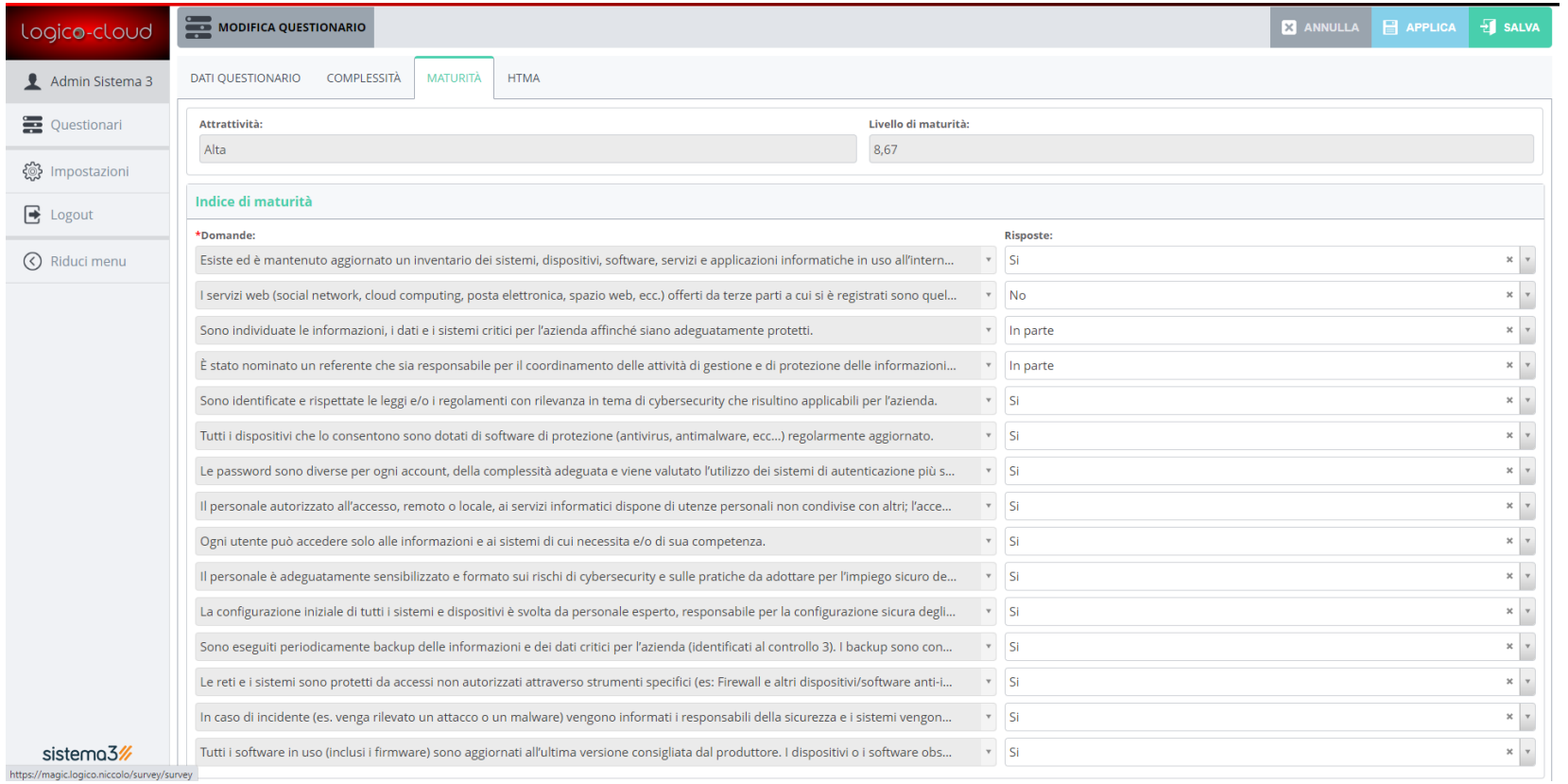
Inserimento dati di analisi - Complessità organizzativa

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.

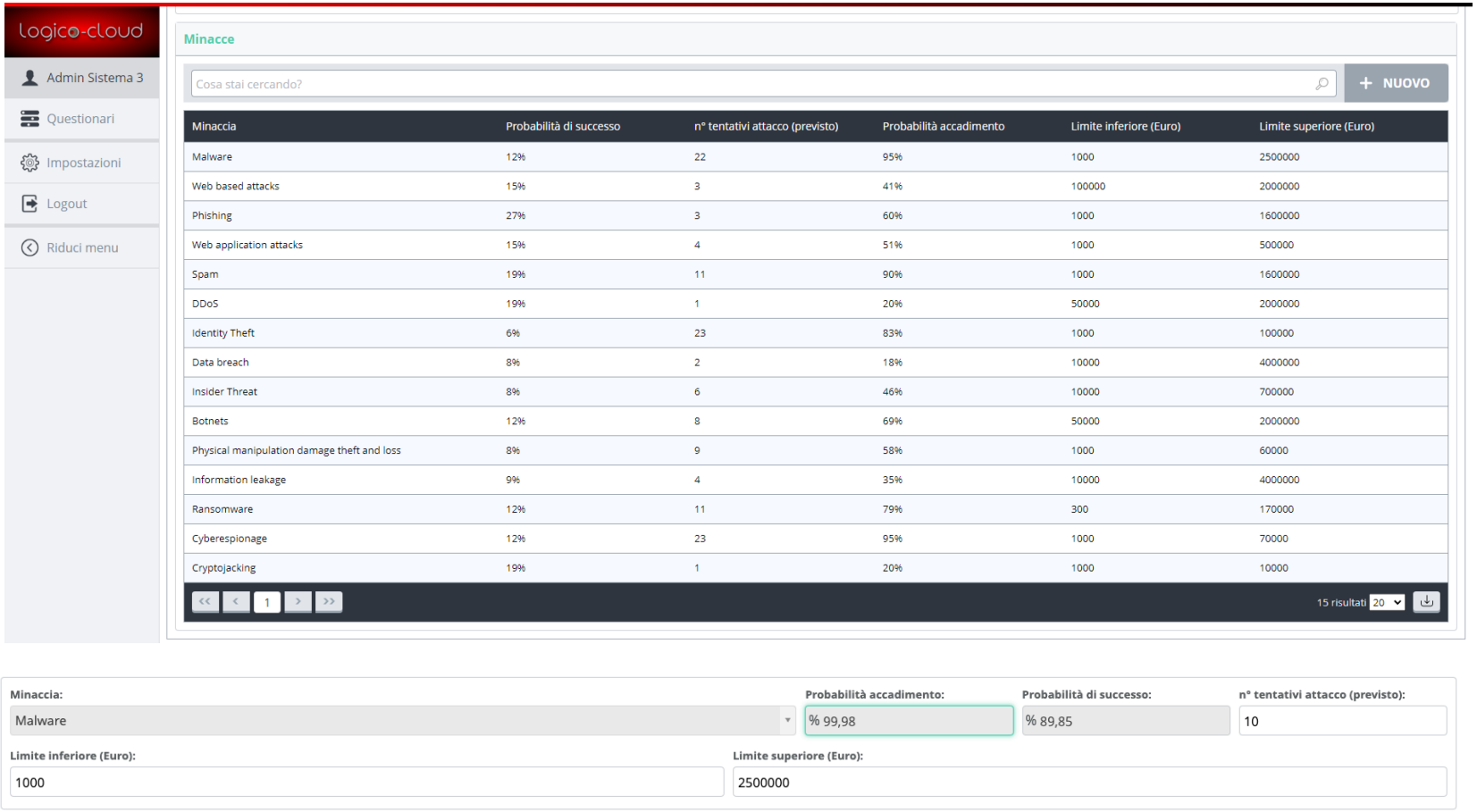


Inserimento dati di analisi - Maturità

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)).

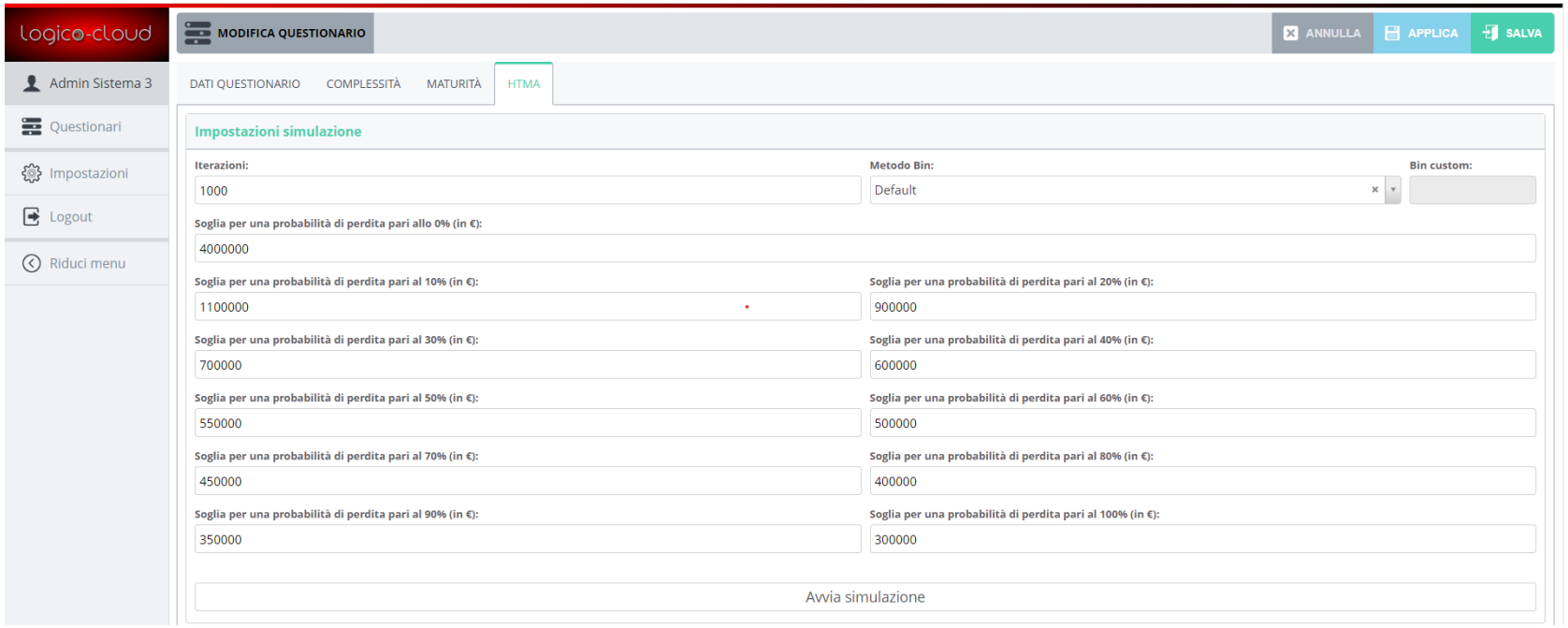
Questi 3 valori vengono poi utilizzati nella simulazione di attacco, utilizzando il metodo Monte Carlo e per calcolare la probabilità di accadimento.

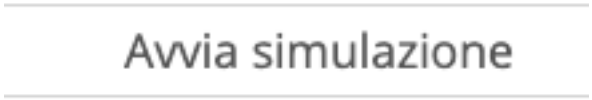


Inserimento dati di analisi - Simulazione

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**%)

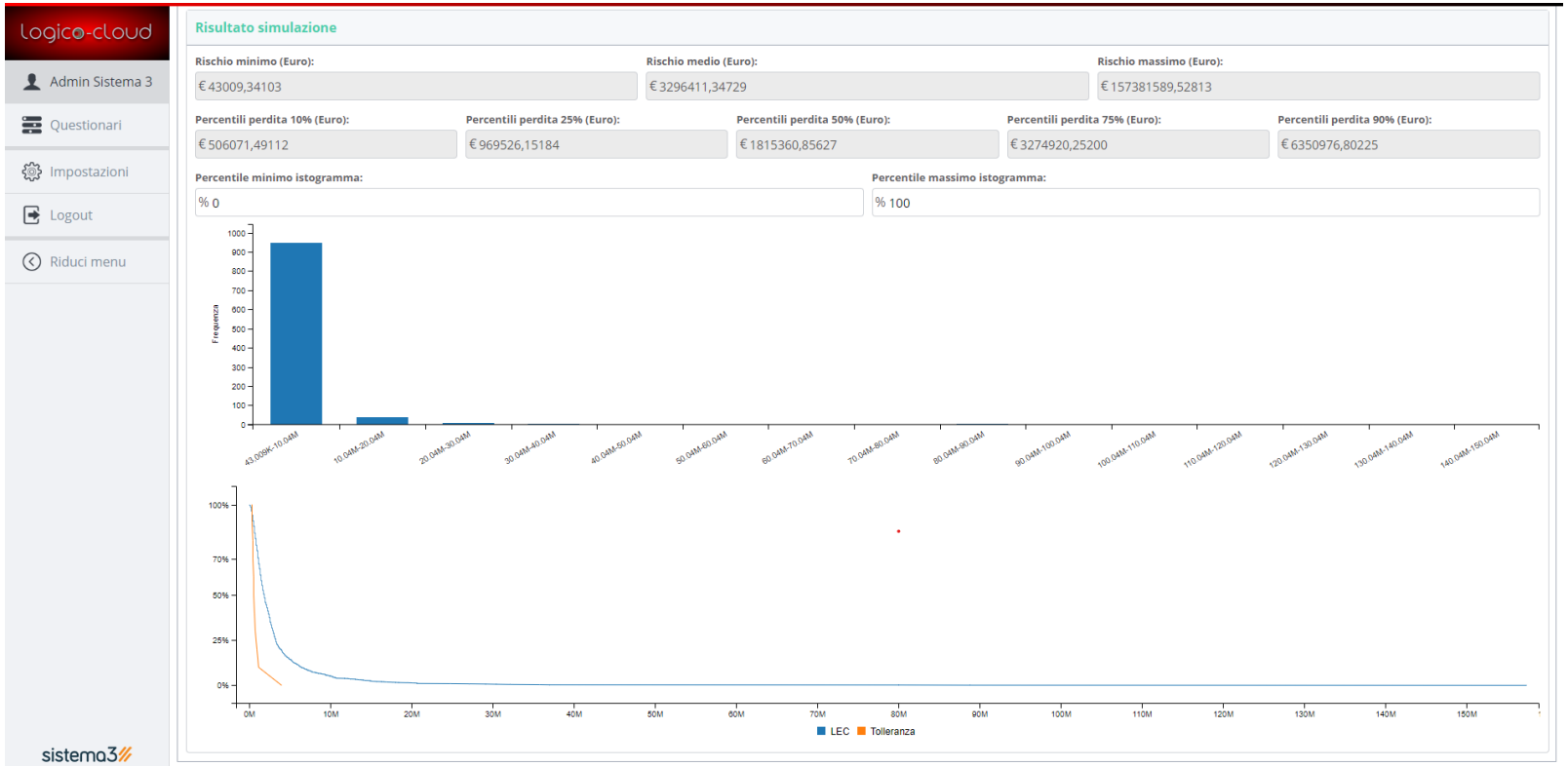




Inserimento dati di analisi - Simulazione

In questa seconda sezione vengono mostrati i risultati della simulazione:

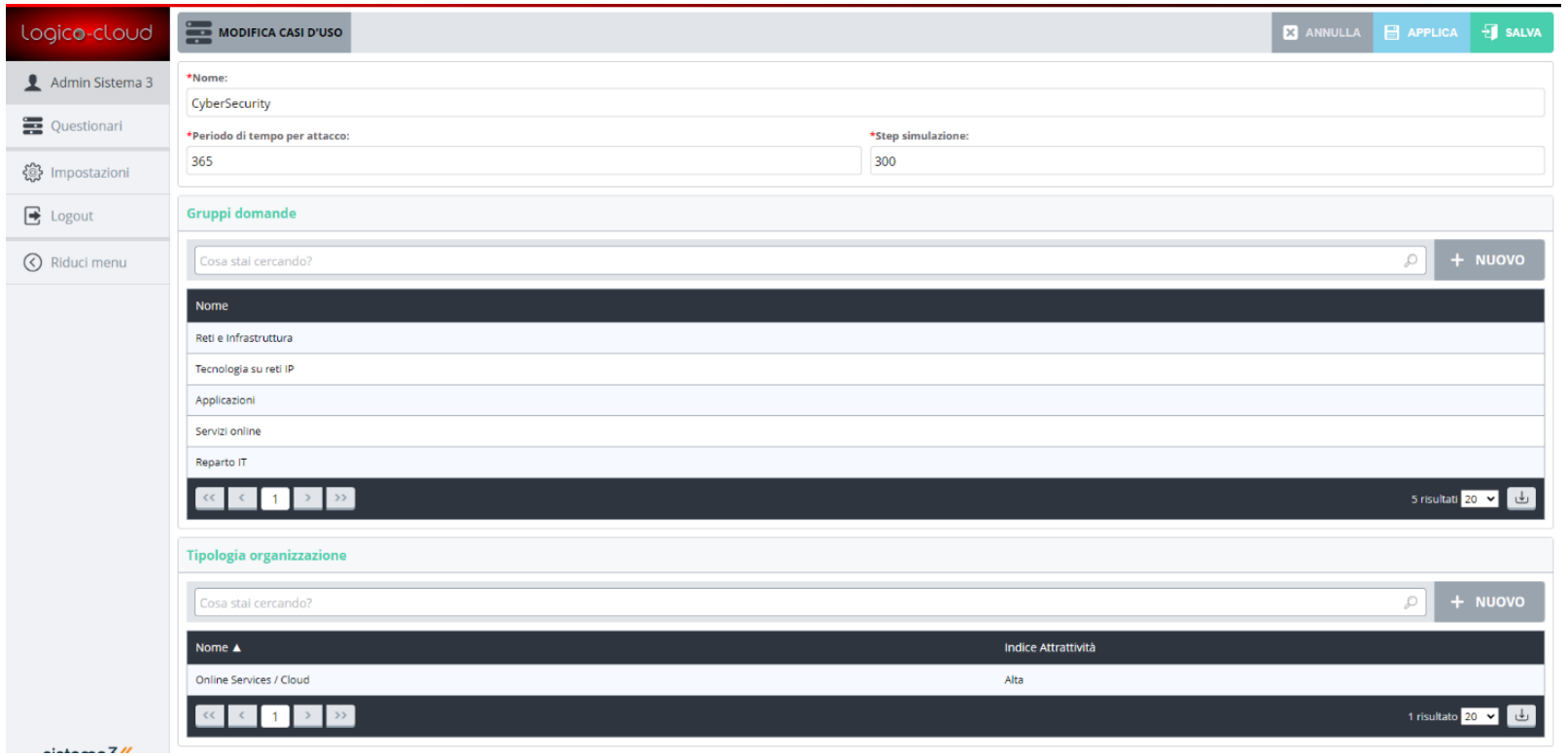
1. Rischio Minimo, Medio e Massimo,
2. Percentili di perdita,
3. Istogramma delle perdite,
4. Loss Exceedance Curve (LEC).



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.

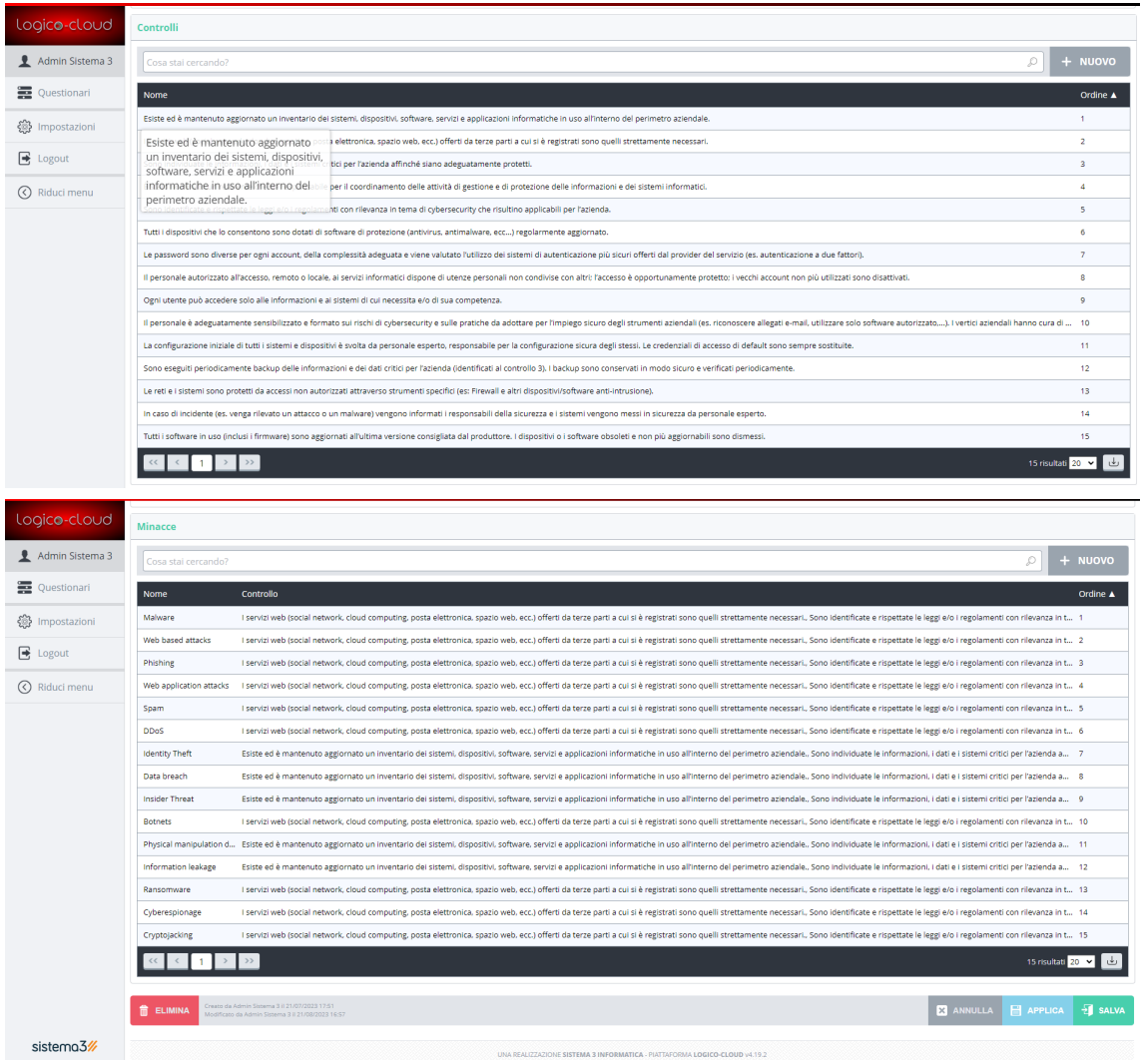
Sarà possibile aggiungere e modificare i casi d’uso presenti nei questionari.



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



Magic e Logico cloud

https://magic.logico.cloud