Studio Dell'Agnello S.r.l.

RiskXRStudio™ 2021

IS&ISO27001 Enterprise e Professional

Manuale Utente e Installazione

Rel. 1.0.7.0

v. 14.26

INDICE

INTRODUZIONE

I prodotti "RiskXRStudio™ 2021 IS&ISO27001 Enterprise" e "RiskXRStudio™ 2021 IS&ISO27001 Professional" sono dei software di Security Risk Management in grado di permettere la valutazione dei rischi delle organizzazioni e il trattamento di quest'ultimi tramite procedure automatizzate che supportano con stime, grafici e tabelle, nonché indicazioni di priorità di intervento il management aziendale. Permettono inoltre di ottenere le certificazioni di sicurezza, fornendo una impostazione metodologica e operativa completa per l'Analisi e il Trattamento dei rischi.

I due prodotti differiscono per la **struttura di licensing** e per il **numero di postazioni** possibili, per i **componenti/kit** e per gli **standard/certificazioni** in essi compresi, nonché per la configurazione, mantengono però la stessa interfaccia operativa e la metodologia di riferimento. Anche le procedure di installazione di ciascun componente sono comparabili.

Il presente documento è composto da tre sezioni:

1. la prima descrive in sintesi la **METODOLOGIA** e le sue caratteristiche principali,

2. la seconda indica come utilizzare tutte le funzioni del pacchetto, cioè presenta la sua **OPERATIVITA'**,

3. la terza descrive come procedere all'**INSTALLAZIONE** delle applicazioni che fanno parte della suite del prodotto.

La "**Metodologia RiskXRStudio (TLQE XR)**" è la metodologia implementata nello strumento, evoluzione/estensione avanzata della metodologia delle precedenti versioni.

È una metodologia conforme allo standard internazionale **ISO/IEC 27001** e **ISO 22301** ed è utilizzata per ottenere le relative certificazioni di sicurezza, conforme inoltre agli standard **ISO/IEC 27017** e **ISO/IEC 27018**, nonché allo Standard **ISO/IEC 27005** che dettaglia ulteriormente la parte di Information security risk management dell'ISO/IEC 27001 e allo standard **ISO 31000** di Risk Management.

RiskXRStudio™ 2021 consente di verificare i requisiti richiesti ad una organizzazione e di valutare i rischi dei suoi trattamenti secondo quanto indicato dal **Regolamento UE 2016/679 GDPR** relativo alla privacy, permette inoltre di verificare se sono stati soddisfatti i requisiti richiesti dalle "**Misure minime di sicurezza per le Pubbliche Amministrazioni di AGID**", posto come riferimento per la sicurezza di tutta la Pubblica Amministrazione.

La **metodologia RiskXRStudio** recepisce fasi e passi degli standard citati, aggiungendo metodi di dettaglio relativi ad aspetti da essi non definiti, ma necessari per una reale completa implementazione di una efficace attività di **Security Risk Management** e di **Auditing**.

Questo consente a "**RiskXRStudio™ 2021**" implementando la relativa metodologia di rappresentare **"una soluzione completa di Security Risk Management**" per le **aziende**, **società di consulenza** e le **PA**.

Le funzioni implementate nello strumento e indicate nella metodologia sono "**funzioni generali di Security Risk Management**", pertanto sono utilizzabili per tutte le impostazioni metodologiche di Security Risk Management che definiscono in genere un livello più alto di dettaglio.

Lo strumento consente di accedere alle funzioni in maniera immediata e perciò molto efficiente tramite il menu principale, anche in ordine random, eccetto che per alcune funzioni che appaiono solo dopo aver completato altre funzioni per un corretto flusso delle attività da svolgere.

La "**flessibilità**" di cui godono le funzioni nello strumento consente di svolgere attività di Security Risk Management secondo impostazioni e aggregazioni di fasi e attività anche diverse da quelle indicate dagli standard ISO, pur essendo queste ultime il riferimento principale.

Dal 25 maggio 2018 si applica il **Regolamento UE 2016/679 (GDPR – General Data Protection Regulation)** per la protezione dei dati personali delle persone fisiche (privacy). Tale regolamento considera "rilevanti" per dimostrare l'adeguatezza delle misure di sicurezza eventuali certificazioni **ISO/IEC 27001** e l'**ISO 22301**, specifici set di domande relative a tale regolamento e a tali standard di certificazione sono inserite tra le risorse dello strumento.

RiskXRStudio™ 2021 rappresenta un sistema integrato per risolvere tutte le problematiche di Security Risk Assessment delle aziende private e delle PA.

1. LA METODOLOGIA DI RISK MANAGEMENT RISKXRSTUDIO

1.1 PREMESSA

La "**Metodologia RiskXRStudio (TLQE XR)"** nasce dall'esperienza di consulenza per la sicurezza, sviluppo di metodologie e di prodotti del personale della società negli ultimi venti anni presso le maggiori organizzazioni pubbliche e private italiane ed estere insieme a quella dei propri partner internazionali leader a livello mondiale nel campo delle metodologie e prodotti per l'Analisi e la gestione dei rischi.

Tale metodologia come già ricordato è allineata agli Standard internazionali **ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27005 e ISO 22301 e ISO 31000** e si inquadra all'interno del "framework" in cui questi sono posizionati, costituendone una completa implementazione fino alla fase operativa.

La **Metodologia RiskXRStudio** e il prodotto relativo consentono di gestire tutte le fasi di competenza del processo di **Security Risk Management** e diventano parte della "**Risk Management strategy**" dell'organizzazione**.**

1.2 LA MISSIONE/BUSINESS E GLI OBIETTIVI AZIENDALI

Ogni organizzazione ha una propria **"Missione"**, magari costituita da più missioni/business. Per soddisfare la propria Missione l'organizzazione deve raggiungere una serie di **"obiettivi"** ad essa correlati e derivati dalle esigenze dei propri "stakeholder" (azionisti, dipendenti, cittadini, ecc.), cioè di tutti coloro che interagiscono a diverso titolo con l'organizzazione.

Ogni **evento** che aumenti l'**incertezza** di raggiungere tali obiettivi rappresenta un **rischio** per l'organizzazione e può dare luogo a conseguenze negative (tangibili o intangibili), costituendo una "**minaccia**", od ottenere eventuali conseguenze positive allora tale evento pur rappresentando un rischio, costituisce una "**opportunità**" (ISO 31000).

Il **Security Risk Management** si occupa in particolare degli **eventi aventi conseguenze negative** sulle risorse dell'organizzazione, cioè si occupa delle "**Minacce**", con particolare riguardo ai sistemi informativi, elemento strategico per il raggiungimento degli obiettivi aziendali, e focalizza su come "**prevenirle**", "**rilevarle**" ed effettuare azioni di "**recovery**", se necessario, per salvaguardare il "**valore**" dell'organizzazione e in particolare la condizione "ottimale" dei processi interni, elementi chiave per il "**raggiungimento degli obiettivi definiti"**.

1.3 DEFINIZIONE DEL CONTESTO

Per effettuare un efficace Security Risk Management è necessario, perciò, rilevare e identificare tutte le informazioni relative all'organizzazione, quali:

1. la sua missione,
2. gli obiettivi di business, le strategie e politiche correlati e le aspettative degli stakeholder
3. i processi di business che supportano la missione,
4. le funzioni necessarie per ottenere il corretto andamento dei processi,
5. la sua Struttura organizzativa,
6. la sua strategia di Risk Management
7. Le informazioni critiche di supporto ai processi per soddisfare la missione
8. Le locazioni e le loro caratteristiche
9. i vari requisiti che deve soddisfare l'organizzazione
10. il contesto esterno/interno dell'ambito in valutazione
11. le applicazioni (programmi applicativi, basi di dati, personale, sistemi informativi – HW/SW)
12. le risorse di supporto ulteriori a quanto prima indicato (sistemi di supporto, sistemi di sicurezza fisica, sistemi antincendio, edifici, ecc.)

    con l'intenzione di compilare un "Modello dell'organizzazione" che ci consenta di effettuare la valutazione dei rischi relativi.

A tal fine è necessario procedere:

1. alla istituzione di una "**struttura organizzativa che gestisca il Risk Management"** e che porti avanti le attività relative.
2. alla definizione dei "**Criteri di base"** da utilizzare per il **Security risk management,** in particolare per **l'Information Security Risk Management**,
3. alla indicazione nell'analisi dei rischi a cui si vuole procedere dell'**ambito da considerare** e dei suoi "**confini"**,

Tale "ambito oggetto di valutazione" sarà definito "**Caso**" in RiskXRStudio e i suoi confini permetteranno di identificare tutte le risorse/Asset tangibili e intangibili in esso comprese e da considerare nell'analisi dei rischi.

I confini di un caso possono essere quelli relativi anche ad una intera organizzazione/azienda, oppure ad una sua divisione o ufficio, un CED, un

servizio, un'applicazione o qualunque altro "ambito" si abbia esigenza di valutare.

1.4 MODELLO XR DEGLI ASSET E ANALISI ORGANIZZATIVA

Elemento chiave dell'analisi organizzativa e della valutazione dei rischi di un'organizzazione o di una sua parte è il "**modello degli asset**".

I "nomi" in RiskXRStudio delle **Categorie degli asset** dell'organizzazione che devono far parte di tale modello (In RiskXRStudio **Modello XR**) sono descritti nei paragrafi che seguono evidenziati **IN GRASSETTO.**

La missione di un'organizzazione comprende in genere la fornitura di servizi e/o lo sviluppo e la produzione di prodotti. Per soddisfare la propria missione è necessario portare avanti in modo adeguato un insieme di **Processi** (Ambiti di classe "**PRC**") che possono essere direttamente legati alla missione, correlati con essa, o riguardanti la gestione dell'organizzazione, oppure essere processi di controllo o semplicemente processi generali, utili ma improduttivi.

La loro rilevanza/criticità è un elemento determinante per valutare il loro valore al fine di soddisfare gli obiettivi della missione aziendale.

Ogni processo è portato avanti tramite delle **procedure** seguite dal personale, parte di queste sono manuali e parte invece sono "**procedure applicative automatizzate**", "Applicazioni" in senso lato (Ambiti di classe "**A**").

Le procedure sono costituite da una serie di **attività** che possono essere eseguite in sequenza, in parallelo o miste secondo la pianificazione definita per ottenere gli output che ci si aspetta dai processi in base agli input ricevuti.

Attualmente i **Processi** sono fortemente legati alla disponibilità di Applicazioni automatizzate perché esse consentono di svolgere le attività in maniera più rapida ed efficiente.

Una procedura viene svolta dal personale, cioè da **Persone** che la gestiscono ed è supportata da uno o più "programmi applicativi" (asset di categoria "**Applicazioni"** software) di cui uno in genere è il Programma applicativo principale ed opera insieme ad una o più **Basi di dati.** Spesso una di queste è la base dati principale dell'applicazione, altre fanno parte di una "Database generale dell'organizzazione" costituito da molti archivi correlati alle attività aziendali comuni a più applicazioni.

I programmi applicativi, il **Software di base** e il **Software di communication** delle reti, sono eseguiti in un "**Sistema di elaborazione"** (Ambito di classe "**S"),** costituito da server, PC o altro **HW Sistemi IT** e **HW di communication.** I server sono allocati nei CED e i client, in genere, si trovano in aree uffici di **Edifici**, che possono essere separati dai CED.

I CED contengono spesso un numero elevato di server e apparati di rete e hanno l'esigenza per il loro corretto funzionamento di rientrare sempre in un range di temperature definito. Di qui la necessità sia di avere dei **Sistemi di supporto** come i Sistemi di aria condizionata specie in estate sia di **Sistemi antincendio,** visto l'elevato numero di cavi necessari al corretto funzionamento degli apparati e dei sistemi presenti con i rischi che ne conseguono.

L'alimentazione elettrica è una **Utenza** indispensabile per il funzionamento dei sistemi di elaborazione senza la quale la catena degli asset che permette di svolgere le attività di supporto ai processi si fermerebbe. Per salvaguardare la continuità di questa risorsa occorrono contromisure come UPS e gruppi elettrogeni in grado di sopperire a situazione critiche.

Altrettanto necessario è il controllo degli accessi fisici agli edifici e ai CED che può essere attuato tramite tornelli, accessi con badge, telecamere e altri **Sistemi di sicurezza** quali allarmi antifurto e sistemi perimetrali.

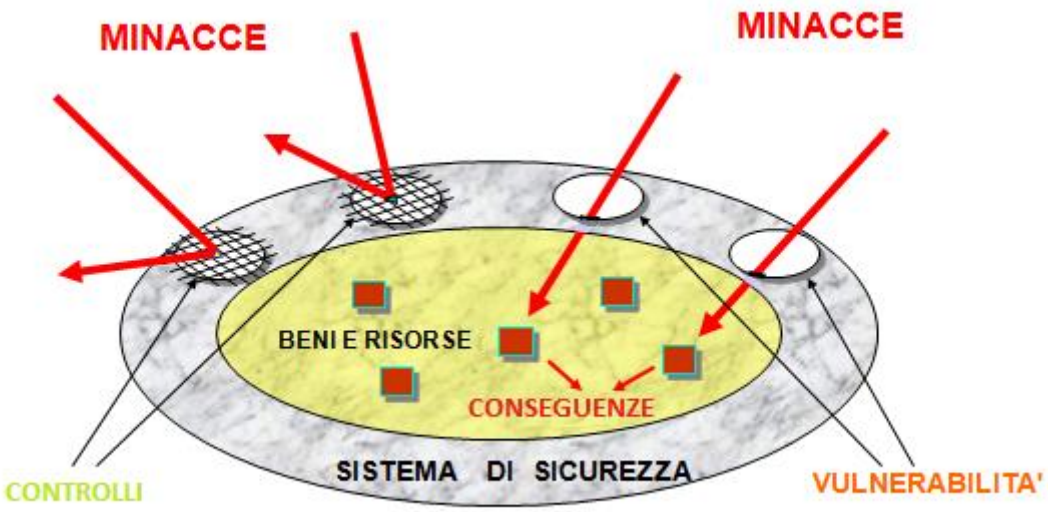
L'analisi organizzativa e dei sistemi informativi consente di sviluppare un modello dell'organizzazione e dei suoi sistemi informativi con le categorie e le classi degli elementi prima citati e permette allo strumento di effettuare la valutazione dei rischi relativa ai vari elementi.

1.5 GLI ELEMENTI DI BASE DEGLI SCENARI DI RISCHIO

La metodologia **RiskXRStudio** si basa sulle relazioni fra cinque fattori chiave - che costituiscono gli elementi di base degli **Scenari di Rischio**, tali elementi sono schematizzati nella figura che segue:

- **Bene/Asset**: Risorsa dell'organizzazione tangibile o intangibile che sia utile o abbia un valore per essa.
- **Minaccia/Rischio(Evento rischioso)**: Un evento, un processo o un atto che, quando avviene, provoca "conseguenze negative" su uno o più beni rendendo più incerto il raggiungimento degli obiettivi.
- **Impatto/Conseguenze**: La misura usata per descrivere le conseguenze possibili di una minaccia che si concretizza (evento rischioso) e che influisce sul raggiungimento degli obiettivi.
- **Vulnerabilità**: Condizione di debolezza/suscettibilità di un bene o di un gruppo di beni nei confronti della possibilità di avere perdite/danni di vario tipo a causa di eventi rischiosi (minacce).
- **Controllo/Salvaguardia/Contromisura**: Una misura di sicurezza o azione presa per eliminare una vulnerabilità esistente o diminuire la vulnerabilità di un bene ad una minaccia o ad un numero di minacce possibili. Questo può risultare nella diminuzione della probabilità e/o dell'impatto per una minaccia, oppure nella sua eliminazione. Per "Controllo" si intende in generale un "**criterio di sicurezza**", pertanto è in grado di rappresentare

non solo le esigenze relative ad un **meccanismo di sicurezza**, ma anche una **condizione** necessaria di contesto, ad esempio, e in generale qualsiasi elemento positivo per ottenere un adeguato livello di sicurezza delle risorse e dei processi e il raggiungimento degli obiettivi della missione.



In questa rappresentazione schematica le minacce sono rappresentate come provenire dall'esterno, devono però essere intese in senso lato in quanto sono comprese anche le minacce provenienti dall'interno dell'organizzazione.

1.6 GLI INDICI E LE METRICHE

Gli indici e le metriche di base della metodologia sono:

- **RLE** (Risk Level Estimate) **Rischio Effettivo**. Questo indice esprime il livello di rischio reale che si ha quando viene considerato l'effetto di protezione delle contromisure/controlli in essere. La scala di valori di questa metrica è: 0-10, cioè 10 livelli (da 1 a 10) ed il valore 0 per rischio nullo.

- **RMLE** (Maximum RLE) **Rischio Potenziale/Intrinseco**. Questo indice esprime il livello di rischio che si avrebbe se "nessuna" misura di sicurezza fosse stata attuata. La scala di valori di questa metrica è: 0-10.

L'indice della metodologia della **Vulnerabilità** e perciò correlato al **Livello di protezione** è:

- **IRI** (Impact Relative Index) Esso rappresenta la misura della "**Mancanza di Protezione**", cioè della **vulnerabilità**. La metrica di questo indice utilizza una scala di valori da 0 a 100. Con **0** si indica lo stato di "**Vulnerabilità nulla**", relativo nella condizione di "protezione ottimale completa" e con **100** si indica la condizione di **Vulnerabilità massima** e perciò di "**massimo**

rischio" nei confronti di una specifica minaccia, corrispondente a nessuna misura di sicurezza applicata.

Il valore di rischio effettivo **RLE** viene ottenuto elaborando i valori del Rischio potenziale/intrinseco **RMLE** e della vulnerabilità/mancanza di protezione **IRI**.

Il rischio effettivo **RLE** aumenta all'aumentare del valore dell'**IRI** fino al valore massimo **RMLE**.

1.7 LA DEFINIZIONE DELLE POLITICHE DI SICUREZZA

Salvaguardare la sicurezza di un'organizzazione vuol dire assicurare l'andamento ottimale dei suoi processi proteggendo le risorse/asset necessarie alle sue attività.

Visto il numero elevato degli asset tangibili e intangibili coinvolti nelle grandi organizzazioni occorre definire delle "**Politiche di sicurezza**" che definiscono dei precisi "Criteri di sicurezza (controlli)" da applicare e attuare per le varie Categorie di Asset o gruppi di asset.

Le Politiche di sicurezza hanno funzione di indirizzo e vengono definite ad alto livello basandosi su standard internazionali, nazionali, normative interne e "best practices" di sicurezza, ma per essere efficaci devono essere definite anche a livello più di dettaglio, magari con il contributo dei costruttori, arrivando fino a che si possa assicurare un'adeguata sicurezza per l'organizzazione. Le risorse utilizzate e il dettaglio saranno proporzionati all'efficacia e convenienza di tale processo.

I Piani di sicurezza hanno invece una funzione operativa, si basano sulle politiche di sicurezza e devono fornire tutti i criteri operativi da applicare ai vari asset dell'organizzazione da parte del personale della sicurezza.

Le *Politiche di sicurezza* e i *Piani di sicurezza* stabiliscono set di Criteri di sicurezza (Controlli) ai vari livelli di dettaglio che, se esaustivi e sviluppati come prima detto, costituiscono un "riferimento" chiave per "un'analisi e verifica la più oggettiva possibile" con cui confrontare la situazione reale di sicurezza dell'organizzazione. La selezione dei controlli su cui basare un'analisi dei rischi è legata agli "obiettivi" e "confini" dell'ambito di valutazione di cui vogliamo calcolare i rischi e perciò degli Asset coinvolti.

L' "attuazione ed efficacia al 100%" di tali set di Controlli, difficilmente raggiungibile, rappresenterebbe la protezione ottimale allo stato dell'arte attuale e, teoricamente, la condizione di rischio nullo per gli obiettivi e confini definiti per l'analisi.

In realtà come sappiamo non vi è mai realmente la condizione di rischio nullo, ma il rischio che non è possibile eliminare viene coperto da assicurazioni o accettato in quanto non gestibile o rilevabile tecnicamente.

A livello operativo si procederà pertanto valutando il "livello di vulnerabilità" tramite l'acquisizione di risposte a questionari composti di "domande" che semplicemente chiedono di stimare "*quanto è attuato e efficace ciascun controllo del set di riferimento*", che in RiskXRStudio si esprime con un valore da 0 a 10 corrispondente a 0% e 100% di attuazione ed efficacia.

Quando un controllo è attuato/efficace meno di un livello di soglia fissata (normalmente 80%, personalizzabile) allora è considerato una VULNERABILITA', cioè una "lacuna" nella protezione di cui una minaccia può approfittare, tanto più quanto meno è attuato/efficace.

Con i controlli si possono rappresentare anche condizioni ambientali o di stato, "criteri" quali ad esempio non scegliere siti in zone alluvionali o vicino a industrie a rischio. Non vi sono limiti.

Questo approccio strutturato consente di calcolare in maniera più oggettiva la "vulnerabilità" rispetto a domande di tipologia variabile, che aggiungono elementi di valutazione più soggettivi. I controlli sono raggruppati per pertinenza secondo le varie Aree di Sicurezza, consentendo così il calcolo del livello di vulnerabilità di ciascuna area.

Le Aree rilevanti per la sicurezza sono considerate in una visione di valutazione del rischio, visto quanto prima detto, come AREE DI VULNERABILITA'.

Il livello di rischio di una Minaccia dipende da un insieme di Aree di vulnerabilità specifiche rilevanti nello scenario di rischio che comprendente anche gli asset coinvolti.

Per ottenere adeguata efficacia occorre che il set di controlli scelto sia adeguato ed esaustivo, cioè fotografi la situazione ottimale, eventualmente introducendo ulteriori controlli. RiskXRStudio permette facilmente questa integrazione.

Lo strumento costituisce un "Sistema integrato" che permette di acquisire per la valutazione dei rischi anche i dati ottenuti da "**strumenti di Vulnerability Assessment"**, se desiderato, al fine di effettuare una misurazione integrata dei rischi per ciascun asset o ambito dell'organizzazione.

1.8 LO SVILUPPO DEI PIANI DI SICUREZZA

Una volta definite le *Politiche di sicurezza* ai vari livelli per le varie tipologie di asset dell'organizzazione occorre definire, e dunque "associare" a ciascun asset, quali controlli sono pertinenti e da attuare per ottenere una sicurezza adeguata delle risorse. Questo processo porta alla definizione dei **Piani di sicurezza** per tutti gli asset dell'organizzazione.

Lo strumento permette di effettuare una **valutazione dei rischi** che tenga conto delle Politiche di sicurezza e dunque dei controlli pertinenti applicate su tutta l'organizzazione basandosi sulla % di attuazione del controllo nell'ambito del

Caso in valutazione, tenendo conto se è sempre attuato, attuato in una certa percentuale o non attuato del tutto, per gli asset pertinenti.

Consente inoltre, se desiderato, di associare gruppi di controlli a ciascun asset o gruppi di asset **definendone i Piani di sicurezza specifici**. In questo caso lo strumento sarà in grado di generare poi dei **report sullo stato attuale dei Piani di sicurezza specifici,** con **il numero e quali Criticità siano presenti** per lo specifico asset o gruppo di asset nelle mappe di rischio, nonché, se desiderato, mostrando anche il numero di vulnerabilità derivate da **strumenti di Vulnerability assessment** per quell'asset o gruppo di asset e quanti Host sono coinvolti.

Si otterranno come risultato dei file con il "nome degli ambiti" del modello XR degli asset, con una scheda per ciascun asset in essi compreso avente la lista dei controlli con il livello di URGENZA di intervento, se necessario, espressa in 5 classi e dipendente dai rischi calcolati nell'analisi. Tali file rappresentano "lo stato dei Piani di sicurezza applicati" da mostrare anche per eventuali certificazioni insieme alle mappe di rischio degli asset per ciascuna minaccia.

1.9 IL PROCESSO DI ANALISI E TRATTAMENTO DEI RISCHI

I passi che costituiscono il processo di analisi e trattamento dei rischi sono mostrati nella figura che segue.

1.10 LO STUDIO DEL CASO E DEI SUOI ASSET

Una volta indicato il nome del **Caso** in analisi, si indicherà l'**Ambito del Caso**, che sarà al top del **modello XR** degli asset definendone i confini, e la **Descrizione del Caso**, cioè gli obiettivi di tale analisi.

Occorre specificare "**di che cosa**" **vogliamo sapere i rischi**, cioè di quali entità tangibili o intangibili: **Sedi, CED, server, applicazioni, ma anche processi,**

attività, servizi, unità organizzative, server, aziende, P.A, ecc. La metodologia **RiskXRStudio** consente di valutare e modellare ogni entità che si ritenga rilevante senza limiti.

Una volta identificate tali entità si inseriranno nel **Modello XR** degli **Asset** e **Ambiti**, con al top il **Caso,** come già indicato, insieme agli **Asset/Beni** che lo costituiscono e lo supportano.

In base alle esigenze del committente dell'attività di valutazione e delle risorse messe a disposizione l'analista sceglierà di utilizzare un **modello semplice** oppure **un modello più sofisticato,** impostando la filosofia di modellazione di conseguenza.

Nel paragrafo che segue sono descritte tutte le caratteristiche per creare un **Modello XR degli ASSET**.

1.11 IL MODELLO XR DEGLI ASSET

La metodologia **RiskXRStudio** ha come caratteristica peculiare, di poter creare un modello degli Asset a "n" livelli con un numero di livelli e di elementi "praticamente" illimitato.

La libertà di modellazione consente di creare un **modello al livello ottimale di dettaglio**, in base alle proprie esigenze e risorse, senza nessuna limitazione perciò da parte della metodologia o dello strumento.

Vediamo di seguito un modello esemplificativo degli elementi base.

È composto da tre tipologie di elementi:

- Il **CASO** che identifica il Contesto (Ambito del Caso), cioè tutto ciò che è compreso nell'area di valutazione definita ed è posizionato
    - al **top** del Modello.
    - ha **Figli**, che possono essere asset o altri ambiti.
- L'**AMBITO** (sistema) è come un contenitore di un insieme di Asset o altri Ambiti, che identifica una sottoparte del Caso "non caratterizzata", in quanto contiene vari elementi con caratteristiche anche molto diverse. Esso ha:
    - un **Ambito padre** che può anche essere il **Caso**.
    - uno o più **Figli**, sia asset che ambiti, che lo rappresentano (componenti interne) o che lo supportano (componenti esterni) e dai quali deriva eventuali rischi.
    - Non è necessario inserire valori negli Ambiti (sistemi) in quanto i loro rischi sono costituiti dai rischi dei componenti interni loro figli che li rappresentano o derivati da componenti esterni che li supportano.
    - Se un Ambito ha una sua identità specifica da salvaguardare al di là dei suoi componenti figli si inserirà, come figlio, un asset "Intangibile" che lo identifica e sarà un suo ulteriore componente. In pratica un Ambito è un contenitore degli asset del suo sottomodello e da essi deriva i suoi rischi.
- L'**ASSET,** che identifica un bene o un gruppo di beni dell'organizzazione, è un elemento che può essere sia fisico tangibile che intangibile e che ha una sua "**caratterizzazione specifica**". L'ASSET ha:
    - un **Ambito padre** che può anche essere il **Caso**,
    - **non ha Figli**, altrimenti sarebbe un ambito (sistema) ed è sempre una foglia del modello.
    - Un **Asset** può essere figlio anche di un **Ambito** di livello alto, compreso il **Caso.**
    - negli **Asset** vengono inseriti i dati in input nella forma dei "**Valori esposti al rischio**" ad essi associati.

Il Modello ha una struttura "non strettamente gerarchica". Questo termine è derivato dal fatto che la maggior parte degli elementi del modello sono relazionati tra loro con una struttura gerarchica nella quale gli elementi **figli** "supportano" il loro "**ambito padre**", ma vi è una eccezione che vedremo più avanti.

Infatti, una struttura gerarchica per rappresentare la realtà da valutare ha bisogno a volte di poter inserire in più punti del modello uno stesso **Ambito**.

Per evitare duplicazioni di sottomodelli già inseriti, è stato introdotto il concetto di:

- **AMBITO RIFERITO**, è un ambito avente il "**NOME**" esatto di un altro ambito già rappresentato nel modello. All'ambito riferito non associamo figli, perché avrà i figli dell'ambito a cui si riferisce con lo stesso nome. Questo evita di dover inserire più copie del sottomodello di uno stesso Ambito, riducendo significativamente il numero di elementi complessivi del modello.

L'ambito riferito crea un legame "non strettamente gerarchico" tra i rami del modello, perché crea un legame trasversale tra rami diversi.

Evitare di riferire un ambito che sia il proprio padre o un avo in scala di discendenza, perché questo creerebbe un "riferimento circolare" non risolvibile, che non consentirebbe di ottenere la valutazione del modello. Lo strumento è in grado automaticamente di riconoscere eventuali riferimenti circolari e segnalarli come ERRORE premendo il tasto specifico di verifica della circolarità. Ogni altro legame riferito è possibile.

1.12 LA VALUTAZIONE DEI RISCHI

Dopo aver effettuato lo studio dell'Ambito del Caso, identificando gli asset e gli ambiti del modello XR e dopo aver inserito nel modello i valori a rischio (AST_V) corrispondenti si procederà con la valutazione dei rischi.

Per ogni ASSET del modello (per Asset si intende anche un "gruppo di asset", nel caso che vi siano più asset dello stesso tipo che possono essere colpiti da una stessa minaccia) lo strumento automaticamente selezionerà una lista di minacce pertinenti in base alla Categoria dell'asset stesso.

Ogni minaccia colpisce l'asset e sfruttando alcune vulnerabilità (Aree di vulnerabilità) provoca delle conseguenze negative (Impatti) sull'organizzazione e sui suoi obiettivi.

Si parla di "**Incidente**" come dell'insieme costituito da una **Minaccia**, un **Asset** e una **tipologia di impatto** conseguente (RIDPU – Danni correlati alla Riservatezza, Integrità, Disponibilità, diretti e Intangibili), nonché da una **vulnerabilità/mancanza di protezione** sfruttata dalla minaccia per provocare il danno. Il tutto è definito anche come "**Scenario di Rischio**" in cui si può comprendere eventuali **controlli/salvaguardie** presenti.

Tutti gli Asset del modello XR sono valutati in base agli incidenti che possono avvenire a causa delle minacce loro pertinenti. Dai valori degli impatti potenziali (SLLE), delle probabilità di accadimento (AFLE) e dal valore della vulnerabilità/mancanza di protezione (IRI) si ricavano i valori di rischio che si

ritrovano nelle mappe relative. Tenendo conto che il livello di rischio di un asset è il livello più alto di rischio che può avere per tipologia di impatto per le minacce che possono colpirlo.

Come detto precedentemente la valutazione dei rischi secondo la metodologia RiskXRStudio implica la valutazione sia dei **rischi potenziali** che dei **rischi effettivi** ottenuti con la valutazione comprendente la presenza delle contromisure di protezione.

La valutazione dei rischi utilizza la formula mostrata nella pagina seguente la quale tiene conto dei 4 fattori alla base del rischio effettivo (RLE).

RLE = AST_V * SLI * AFLE * IRI

- **SLLE (Impatto Singolo) = --o**
- **RMLE (Rischio Potenziale) = ----------o**
- **RLE (Rischio Effettivo) = ----------o**

- **AST_V Valori degli Asset (Asset Value)**
- **SLI Indice di compromissione (Standard Loss Index)**
- **AFLE Probabilità/Frequenza (Annual Frequency Level Estimate)**
- **IRI Vulnerabilità/Mancanza di Protezione (Impact Relative Index)**
- **SLLE Impatto Singolo (Single Loss Level Expectancy)**

Il processo di elaborazione e **valutazione del livello di rischio** è effettuato utilizzando sia operazioni matematiche sia tabelle di verità a secondo della maggiore adeguatezza per la elaborazione.

Dai **valori degli asset (AST_V)** che tengono conto per ciascun elemento del Modello XR anche della quantità (gruppi di asset), considerata la minaccia e la sua capacità di compromissione (SLI) degli asset, nonché la tipologia di impatto (RIDPU) si ottiene il valore dell'**impatto potenziale del singolo incidente (SLLE)**.

Considerando l'SLLE e tenendo conto del probabilità/Livello della frequenza nell'unità di tempo (AFLE) si ottiene il **Rischio potenziale (RMLE)** che ci indica la gravità di quella minaccia per l'organizzazione.

Dall'RMLE considerando la Vulnerabilità/Mancanza di protezione (IRI) è possibile calcolare il **Rischio effettivo (RLE)** per quella Minaccia.

1.12.1 LOGICA DELLA PRIORITÀ DI INTERVENTO SULLE AREE DI VULNERABILITÀ

Uno dei risultati più importanti dell'analisi dei rischi è il grafico e la tabella che indicano quali sono le **"aree di vulnerabilità in cui è più conveniente intervenire"** per prime per ottenere **i maggiori risultati di riduzione di rischio**. L'indice che sintetizza questa valutazione è: "**Indice composito di Intervento pesato**". La logica con cui è calcolato è la seguente.

Nel **Report di dettaglio delle Minacce** per ogni minaccia viene indicato se il rischio RLE effettivo è **SOPRA** la soglia accettata dal management (**soglia 1 in OPZIONI**).

In tal caso nella colonna "**ACCETTABILITA' RISCHIO**", se il livello di rischio è superiore alla soglia accettata c'è indicato "**INTERVENIRE**".

Nella colonna "**INTERVENTO**" si può trovare "in tale condizione" due possibili indicazioni di intervento per ciascuna AREA di VULNERABILITA' rilevante per quella Minaccia:

- intervento **NECESSARIO**

- intervento **DA VALUTARE**

Sarà **NECESSARIO** a meno che "**l'attuazione media dei controlli**" in tale Area sia SUPERIORE alla "**soglia 2**" presente in **OPZIONI**, indicando già un livello di attuazione "alto" e perciò solo un **piccolo margine di miglioramento** possibile. In tal caso si troverà intervento nell'area **DA VALUTARE** essendoci meno convenienza per ridurre il rischio. Sarà compiti dell'analista valutare se intervenire nell'area specifica.

Se invece la minaccia **non ha un livello di rischio superiore** alla soglia accettata dal management (**soglia 1**), allora si possono avere le seguenti due indicazioni di intervento:

- **NESSUNO**

- Intervento **DA VALUTARE**

Sarà **NESSUNO** a meno che "**l'attuazione media dei controlli**" in tale Area sia **INFERIORE** alla "**soglia 3**" presente in **OPZIONI**, indicando un livello di attuazione "non sufficiente" anche in condizioni di basso rischio.

Infatti, le condizioni di rischio possono cambiare nel tempo e se il livello di protezione è basso mettere a rischio l'organizzazione prima che possa rilevare e reagire alle minacce con protezioni adeguate alle nuove condizioni.

È necessario perciò un livello minimo di protezione sotto il quale non andare ed è rappresentato dalla **soglia 3**.

Come ultima condizione da considerare c'è la **Soglia 4 in OPZIONI** che indica il **livello % minimo di "rilevanza**" nella misurazione del rischio/impatto per una specifica MINACCIA di un'area di vulnerabilità "per essere considerata".

Se è **INFERIORE** alla **Soglia 4** non viene considerata. La soglia è normalmente del 10%, ma è personalizzabile.

I tre livelli di INTERVENTO che rappresentano valori di priorità alta, media e bassa sempre minori:

1. **NECESSARIO**
2. **DA VALUTARE**
3. **NESSUNO**

influiscono sul Grafico e la tabella della **Priorità di intervento.** Inoltre sono fondamentali per rilevare se sono stati soddisfatti i **CRITERI DI ACCETTAZIONE DEL RISCHIO** e quali interventi sono necessari o meno per rientrare in tali criteri.

Nel Sommario dell'analisi vi è la **Tabella degli interventi**. In questa tabella alla colonna "**Numero Minacce che richiedono come NECESSARIO**" sono conteggiate tutte le minacce che nel **Report di dettaglio delle minacce** indicano come **NECESSARIO** l'intervento in quell'area.

Alla colonna "**Numero Minacce che richiedono come DA VALUTARE**" sono conteggiate tutte le minacce che nel **Report di dettaglio delle minacce** indicano come **DA VALUTARE** l'intervento in quell'area.

Dalla somma di questi due numeri pesati si ottiene **l'INDICE COMPOSITO DI INTERVENTO PESATO** che fornisce la priorità di intervento tra le aree di vulnerabilità e da cui è derivato il grafico relativo.

In sintesi, la formula per l'indice di priorità di intervento è:

Priorità di intervento = N1*p1+ N2*p2

Dove:

N1 = Numero di Minacce che richiedono intervento NECESSARIO

N2 = Numero di Minacce che richiedono intervento DA VALUTARE

P1 = Peso associato ad una minaccia N1 (100)

P2 = Peso associato ad una minaccia N2 (8)

Riassumendo quanto detto precedentemente:

Una Minaccia è di tipo **N1** per quell'Area di vulnerabilità se:

1. Ha un **livello di rischio maggiore dell'accettato** da parte del management.
2. L'Area di vulnerabilità contribuisce al rischio della Minaccia più del 10% (default soglia 4), cioè è **rilevante per il rischio** di quella minaccia.
3. L'Area di vulnerabilità è attuata meno della soglia 2 di OPZIONI (default 80%), cioè **ha un margine consistente di miglioramento**.

Una Minaccia è di tipo **N2** per quell'Area di vulnerabilità se:

1. Pur nelle condizioni 1 e 2 precedenti l'Area di vulnerabilità ha un livello di Attuazione medio **sopra** la soglia 2 di OPZIONI (default 80%), cioè **ha un margine di miglioramento ridotto**.

   Oppure
2. **Ha un livello di rischio minore o uguale alla "soglia 1" accettata** da parte del management.
3. Il livello di attuazione/efficacia (Media risposte) dell'Area di vulnerabilità è inferiore alla "soglia 3" di OPZIONI (default 75%), cioè **la protezione è ritenuta comunque troppo bassa**.

1.13 LA GESTIONE DELLE AREE A SICUREZZA DIFFERENZIATA

l "**Profili di protezione XR**" sono una caratteristica rilevante della metodologia RiskXRStudio perché consentono di valutare in uno stesso Caso, con un unico modello degli asset, "Aree con differenti livelli di sicurezza", consentendo così di ottenere un calcolo dei rischi più accurato.

Questa caratteristica consente:

1. di creare un Modello XR anche per tutta l'organizzazione,

2. suddividere il modello in "**Aree a sicurezza differenziata**",

3. valutare un **"Profilo di Protezione XR (PP)"** per ciascuna area, assegnando un PP specifico pertinente a ciascun Asset del modello.

Questo consentirà di valutare con accuratezza i rischi dei servizi di tutta l'organizzazione con una sola analisi complessiva di SINTESI. Riferirsi ai paragrafi indicati nell'indice per i dettagli relativi all'uso delle "Aree a sicurezza differenziata".

1.14 I QUESTIONARI SPECIFICI PER LA VALUTAZIONE DEGLI ASSET O AMBITI

Una caratteristica metodologica di particolare utilità è il poter creare un **Questionario personalizzato (Custom)** per valutare la sicurezza di un **Asset** o di un **gruppo di asset** nello specifico.

Questo consente di avere informazioni al livello di dettaglio che si desideri, dettaglio altrimenti impossibile da ottenere.

Il questionario può tenere conto non solo della tipologia, ma se desiderato anche della Marca dell'Asset e del Modello, consentendo di fare domande sulla **configurazione e le sue criticità** rilevanti per la sicurezza.

Spesso sono gli stessi costruttori che forniscono i questionari specifici.

Associando questionari specifici ad asset e ambiti si potrà ottenere la rilevazione del numero di Criticità in tali beni con evidenziazione nelle **Mappe di rischio XR**.

1.15 I REPORT PREVISTI DALLA METODOLOGIA

Il principale Report del tool è il "**Report di Sommario**" che contiene una sintesi significativa con tutte le sezioni relative ai risultati delle elaborazioni e valutazioni dello strumento in base ai dati di input forniti.

A questo seguono più di dieci ulteriori report che forniscono in maniera completa e in dettaglio tutti gli elementi per l'analisi e la gestione dei rischi, compreso i piani di intervento e rientro dai rischi.

L'essere già in un formato completo e praticamente consegnabile al Committente, sia essa una Direzione generale, un Amministratore delegato o un Cliente è un grande valore, specie se si pensa che è possibile personalizzare i report con il logo dell'organizzazione committente e il formato standard per essa.

Infatti spesso è necessario variare dei dati di input o di calibrazione, in tali casi l'automazione permette un ciclo di ri-produzione dei Report veloce e questo consente di risparmiare molto tempo/uomo.

La **generazione XR** ha consentito di aggiungere al Report di sommario i report di dettaglio relativi ai **Rischi per gli Asset**, ma anche per gli **Ambiti** quali applicazioni, gruppi di server, unità organizzative, ecc. in una stessa analisi ed elaborazione.

I report su menzionati sono i **Report XR di Valutazione dei rischi** sia con la vista Minacce, in cui si hanno i rischi per ciascuna minaccia relativa alle risorse dell'analisi sia la Vista Asset in cui vengono identificati i rischi per ciascuno degli asset collegati ai rispettivi ambiti di appartenenza. In quest'ultimo report sono mostrate anche le "relazioni" di tutti gli elementi asset e ambiti coinvolti nel Caso in valutazione, e si può vedere il "**Numero delle Criticità**" per ciascun asset o ambito del modello.

Vi sono altri report generati dallo strumento tra questi ricordiamo in particolare per la sua rilevanza il **Report di dettaglio delle Vulnerabilità** che contiene per ciascun Controllo di sicurezza, le VULNERABILITA' pendenti, la gravità della non attuazione ed eventuali commenti che specificano la vulnerabilità.

Altri report sono: il Report sulla attuazione di Norme e Standard, Report di Audit per intervistato, Report di Analisi Costi/Benefici, Report degli impatti medi per Evento rischioso, Report di dettaglio delle Minacce, ecc.

Rimandiamo ai capitoli successivi, ad esempio **Generare i Report di Dettaglio XR,** per visionare le tabelle e i grafici dei vari Report ed avere ulteriori informazioni al riguardo.

1.16 REGOLAMENTO UE 2016/679 RGPD (GDPR)

Il Regolamento UE 2016/679 riguardante la protezione dei dati personali delle persone fisiche presuppone degli adempimenti che "RiskXRStudio" supporta nella loro attuazione per la parte automatizzabile. Essi sono:

1) Identificare i Trattamenti attuati dall'organizzazione e il loro contesto.

2) Predisporre un Registro dei Trattamenti

3) Effettuare una Valutazione dei rischi di Contesto per ciascun trattamento che permetta di decidere se occorre effettuare una DPIA – Data Protection Impact Analysis.

4) Verificare la conformità al Regolamento UE 2016/679 compreso il caso di trasferimenti di dati personali in paesi terzi o ad organizzazioni internazionali.

5) Effettuare una DPIA sui trattamenti pertinenti riguardante la salvaguardia in particolare dei Diritti e delle libertà nonché degli altri possibili impatti per i Soggetti interessati dai trattamenti di dati personali.

6) Decidere sulla nomina di Responsabili e di Responsabili della protezione dei Dati (RPD-DPO).

7) In caso di rischi residui superiori all'accettabile procedere alla segnalazione al Garante della Privacy per consultazione.

8) In caso di violazioni della riservatezza o dell'integrità dei dati (data breach) segnalare al Garante e ai soggetti interessati l'accaduto.

RiskXRStudio consente di creare un modello XR relazionale in cui è possibile inserire più "viste" di una stessa realtà. Se si prende l'organizzazione si possono collegare ad essa due viste, la "vista operativa" e la "vista privacy" in un unico Modello XR.

La vista operativa consente di legare tra loro l'organizzazione o parte di essa, le "unità organizzative" ad essa riferite e i "trattamenti" da queste effettuate, mentre la "vista Privacy" consente di legare i "Soggetti interessati" con gli stessi "trattamenti".

Sotto i trattamenti si collegheranno tutti i componenti del "sistema informativo" che elabora i dati usati con i trattamenti: Server, Database, HW e SW communication, CED, sistemi di supporto, ecc.

Ogni "Elemento" nel modello avrà una valutazione per ciascuna delle tipologie di impatto/rischio relativa alle varie minacce/eventi rischiosi possibili.

Si otterranno gli impatti/rischi dei "Soggetti interessati" e di ciascun "trattamento" sia per la riservatezza dei dati, la loro integrità, ma anche per la disponibilità, se richiesto, di accedere ai loro dati, inoltre saranno indicati anche i rischi per la reputazione i diritti e le libertà, nonché per eventuali impatti fisici ed economici diretti (paradigma RIDPU).

Saranno indicati i rischi, ad esempio, per il "furto di credenziali" o per "accessi non autorizzati" ai dati, nonché attacchi "denial of service" che possono impedire di esercitare il diritto di accesso ai soggetti interessati per indisponibilità degli database.

1.16.1 ANALISI DEI RISCHI DI CONTESTO

L'Analisi dei rischi di contesto per decidere se è pertinente effettuare una DPIA per uno specifico trattamento è derivata dalle indicazioni date dalle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato" del WP248 che si basano su 9 condizioni di contesto per cui se vi sono almeno 2 condizioni che lo richiedono si procede alla DPIA del trattamento, se vi è una condizione sarà compito del Titolare decidere se effettuare comunque la DPIA.

RiskXRStudio mette a disposizione un set di domande che permette ad un "intervistato" di rispondere sulle 9 condizioni, associando poi le risposte ad uno specifico trattamento. Se si attua questa procedura per tutti trattamenti (vedi in seguito come associare un questionario ad un elemento del modello XR) si può generare la mappa dei rischi XR (vista asset), vedere associata una indicazione del numero di condizioni critiche alla colonna delle "criticità".

Con il criterio prima detto (da 2 o più effettuare la DPIA) si possono identificare i trattamenti pertinenti in questa fase.

1.16.2 DPIA – DATA PROTECTION IMPACT ANALYSIS

Il regolamento (UE) 2016/679 ("Regolamento generale sulla protezione dei dati") all'articolo 35 del regolamento introduce il concetto di valutazione d'impatto sulla protezione dei dati DPIA.

La valutazione d'impatto sulla protezione dei dati va effettuata "prima del trattamento" (articolo 35, paragrafi 1 e 10, considerando 90 e 93), in coerenza con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (articolo 25 e considerando 78).

La valutazione d'impatto sulla protezione dei dati è un processo continuo, soprattutto quando un trattamento è dinamico ed è soggetto a variazioni continue.

Questo rende di grande aiuto l'uso di uno strumento in grado di "rivalutare i rischi complessivi di tutti i soggetti interessati e dei trattamenti" con rapidità a fronte anche di poche variazioni dei dati dei trattamenti o dei sistemi informativi di elaborazione, generando automaticamente tutta la documentazione di dettaglio anche per un numero elevato di trattamenti.

Per effettuare la DPIA è necessario effettuare contemporaneamente una analisi dei rischi (quando si parla di impatto si intende nell'unità di tempo, cioè rischio) relativa alla salvaguardia della riservatezza, integrità e disponibilità dei dati, come pure alla salvaguardia della reputazione, libertà e diritti, nonché della non discriminazione dei soggetti interessati. Di qui oltre ai questionari, ad esempio, della ISO 27001 per la parte informatica, o altri se ritenuti più opportuni, si associerà il set di domande relative al GDPR che valutano se determinati diritti siano stati o meno violati nei trattamenti. Selezionare perciò le categorie di domande relative al GDPR nello strumento. La maggior parte riguarda l'area di attuazione delle "norme privacy" con indicazioni, comunque, di alcune misure di sicurezza chiave per tale normativa.

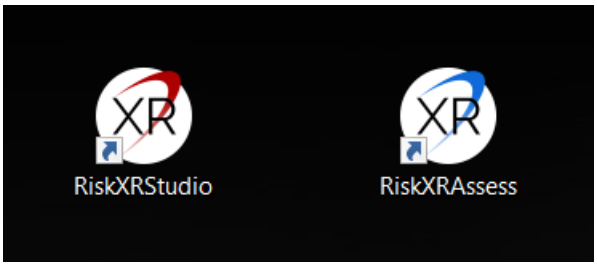
Fondamentale avere presente che tra un'analisi del rischio aziendale e una DPIA cambia la prospettiva nella valutazione dei rischi, perciò stesso modello XR come elementi, ma essendo gli obiettivi da raggiungere riguardanti principalmente la salvaguardia dei diritti e libertà dei Soggetti interessati e non dei rischi per il Titolare, i valori da associare agli asset possono essere diversi, perché il valore di un asset dipende dall'insieme degli obiettivi chiave che si vuole raggiungere, per il Titolare un asset può essere poco rilevante e procurargli poco danno e per la salvaguardia dei diritti del Soggetto interessato invece essere fondamentale.

Una armonizzazione dei due interessi con il giusto equilibrio come in parte indicato in alcune parti del Regolamento potrebbe portare ad un risultato condiviso.

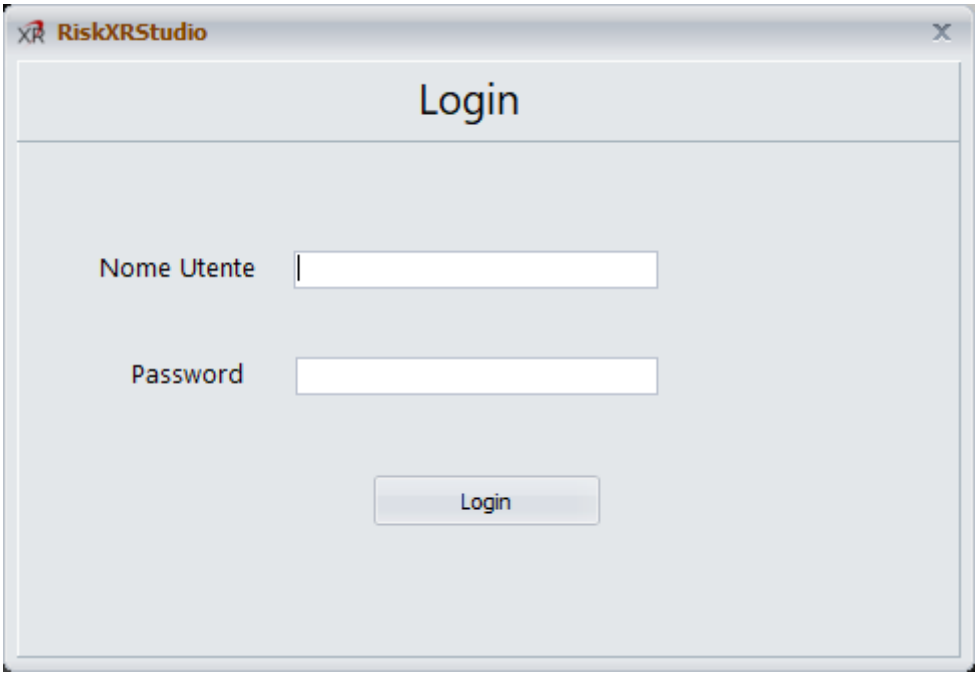
2. PROCESSO DI ANALISI E GESTIONE DEI RISCHI - MODALITA' OPERATIVE

2.1 LANCIARE L'APPLICATIVO

RiskXRStudio™ 2021 viene lanciato con un doppio click sull'icona "**RiskXRStudio**" nel desktop.



Al lancio dell'applicazione seguirà la videata di login con la quale accedere all'applicazione stessa dopo la digitazione del Nome Utente e della password.



Dopo il login si passerà alla videata iniziale con la quale sarà possibile:

1. avere "Informazioni" sulla versione dell'applicazione e il referente dell'account della licenza,

2. creare un "Nuovo Caso",
3. "aprire un Caso" già sviluppato,
4. "creare un Caso" salvandolo come copia di quello già aperto dandogli un nuovo Nome e una nuova Password,
5. "Uscire" dall'applicazione,

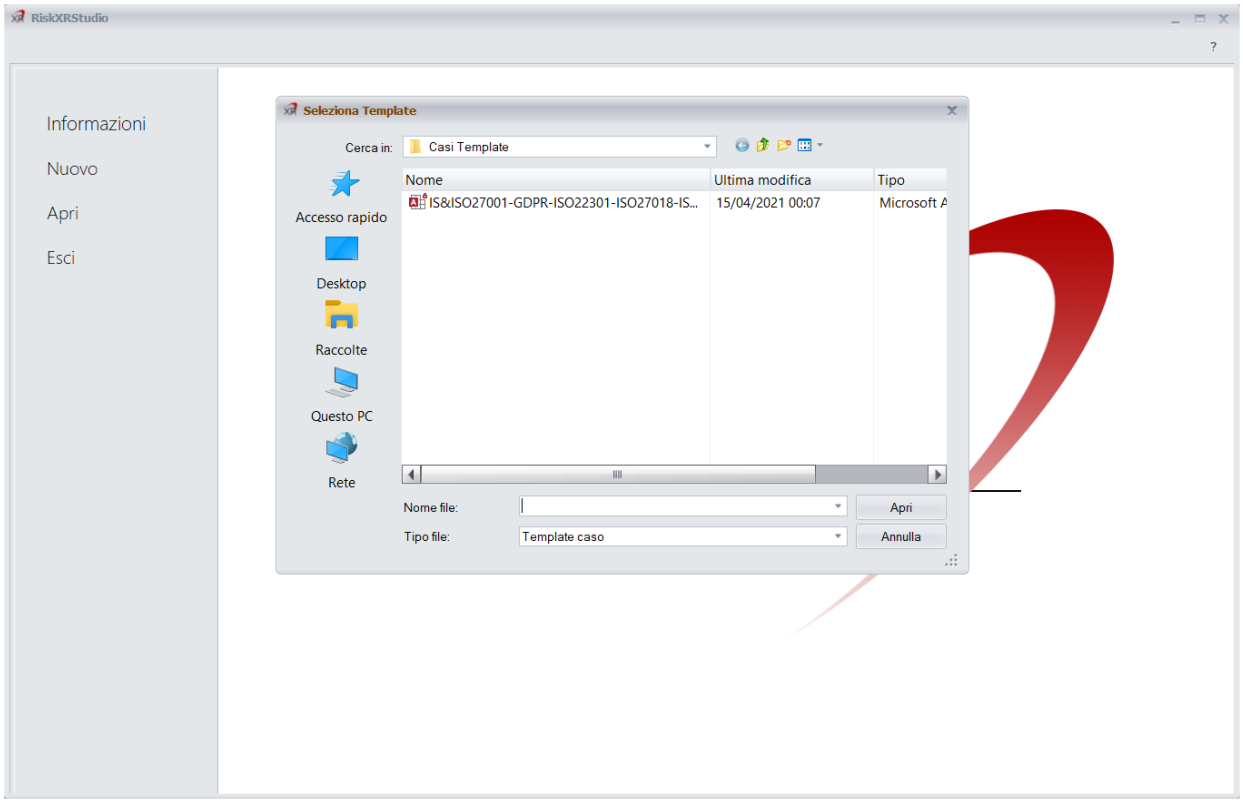
Inizialmente se non si è ancora entrati in un Caso la funzione "Salva con nome" è inibita.

Quando si sarà creato un Nuovo caso o Aperto un caso già esistente allora, ritornando al tab File, si troverà anche la funzione "Salva con nome".

2.2 CREARE UN NUOVO CASO

La procedura da seguire è la seguente:

- Premere "**Nuovo**";
- Si accede in tal modo ad una "Lista di TEMPLATE" tra cui si sceglierà quello che desideriamo utilizzare. Ad esempio quello "IS&ISO27001-GDPR-ISO22301-ISO27018-…..".

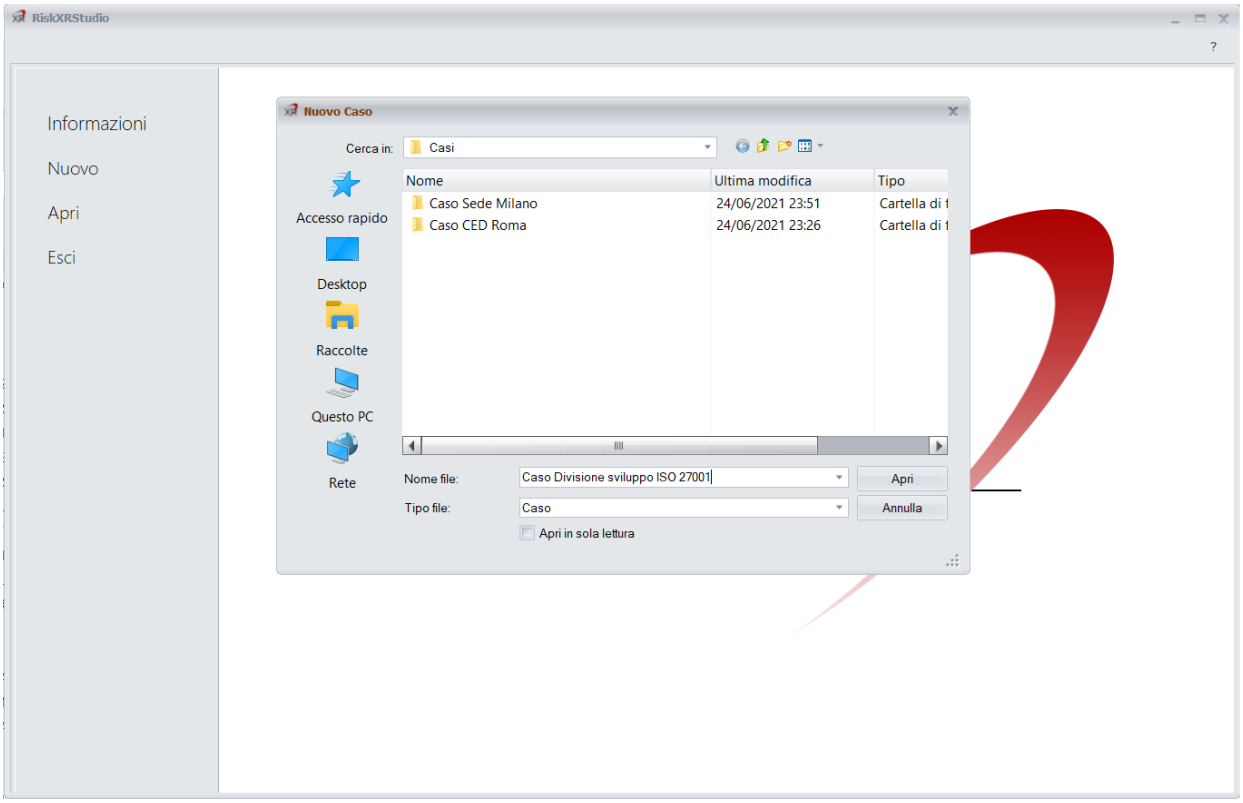


La successiva directory in cui il prodotto ci porterà è quella di "default" per la creazione dei casi, tipicamente la directory "**Casi**" sotto documenti (documents). I casi possono essere posizionati in qualunque directory locale o di rete desiderata.

Occorre poi inserire il Nome che desideriamo assegnare al caso.

L'analista che utilizza RiskXRStudio™ 2021 deve avere sulla directory prescelta e le sue sottodirectory dei casi autorizzazioni di controllo completo.

Nota: la directory dei casi scelta deve essere definita per Excel e per Access come percorso attendibile. Senza questa configurazione le routine di calcolo dei report non vengono eseguite ed i risultati non risulterebbero corretti. Microsoft Office non fornisce alcuna segnalazione in merito. (VEDI CONFIGURARE UN PERCORSO ATTENDIBILE IN EXCEL).



- Ogni Caso è protetto da una sua password specifica definita in fase di creazione.

Inserire la password nel campo "Nuova Password Caso" e nel campo "Conferma Password". Premere poi OK per creare il Caso con il nome e la password scelta.

Tra i criteri per la scelta della password essa deve contenere "*almeno un carattere alfabetico minuscolo, uno maiuscolo, uno numerico e avere una lunghezza di almeno 8 caratteri*".

- Premendo OK si passa alla videata del "**Caso**" in analisi in cui è possibile Inserire il "Nome Ambito del Caso" (**obbligatorio**), il Nome dell'organizzazione o impresa, l'Unità organizzativa coinvolta, il "Titolo del Caso" che apparirà con il Nome dell'organizzazione nei Report, una descrizione del Caso con eventuali note.

- Premendo "Salva" si confermeranno i dati e si passerà alla pagina in cui saranno disponibili tutte le schede delle funzioni del pacchetto eccetto la scheda Report che apparirà solo dopo le elaborazioni.

- Le schede di menu nella parte superiore sono lo "strumento di gestione" del "processo di analisi e gestione dei rischi" e consentono di accedere ai vari gruppi di funzioni disponibili in maniera rapida e immediata nella riga funzioni.

- L'applicazione rende disponibili le schede delle funzioni dello strumento in base alla fase del processo e alle autorizzazioni dell'utente. Molte delle funzioni non hanno esigenze specifiche di sequenza in quanto sono solo dati di input da inserire prima delle elaborazioni e della generazione dei report.

- Quando si generano i report lo strumento prende tutti i dati inseriti e per quelli non inseriti, prende anche i "**dati di default**" che sono visionabili premendo i nomi del menu visibili.

- In generale, dopo avere completato l'inserimento dei dati in una pagina "**salvarli**" premendo il tasto "Salva.

Premendo "Salva" i dati del Caso saranno memorizzati e si passerà alla predisposizione del "Modello XR" utilizzato per l'analisi.

Da ora in poi sarà possibile creare "Aree a sicurezza differenziata" per l'analisi, come spiegato successivamente, tramite un tasto specifico che apparirà in tale pagina.

2.3 ACCEDERE AL MANUALE TRAMITE L'ICONA DELL'HELP

Il "manuale" dell'applicazione in formato elettronico contenente sia la metodologia che l'operatività si trova nella directory "Documenti\Casi tools\Manuali". Esso contiene indicazioni anche per l'installazione delle varie applicazioni.

L'icona in alto a destra con il "?" di HELP consente un accesso immediato al "manuale" in ogni successiva videata.

Tramite l'indice cliccando sui numeri di pagina si può accedere direttamente alle varie sezioni del documento.

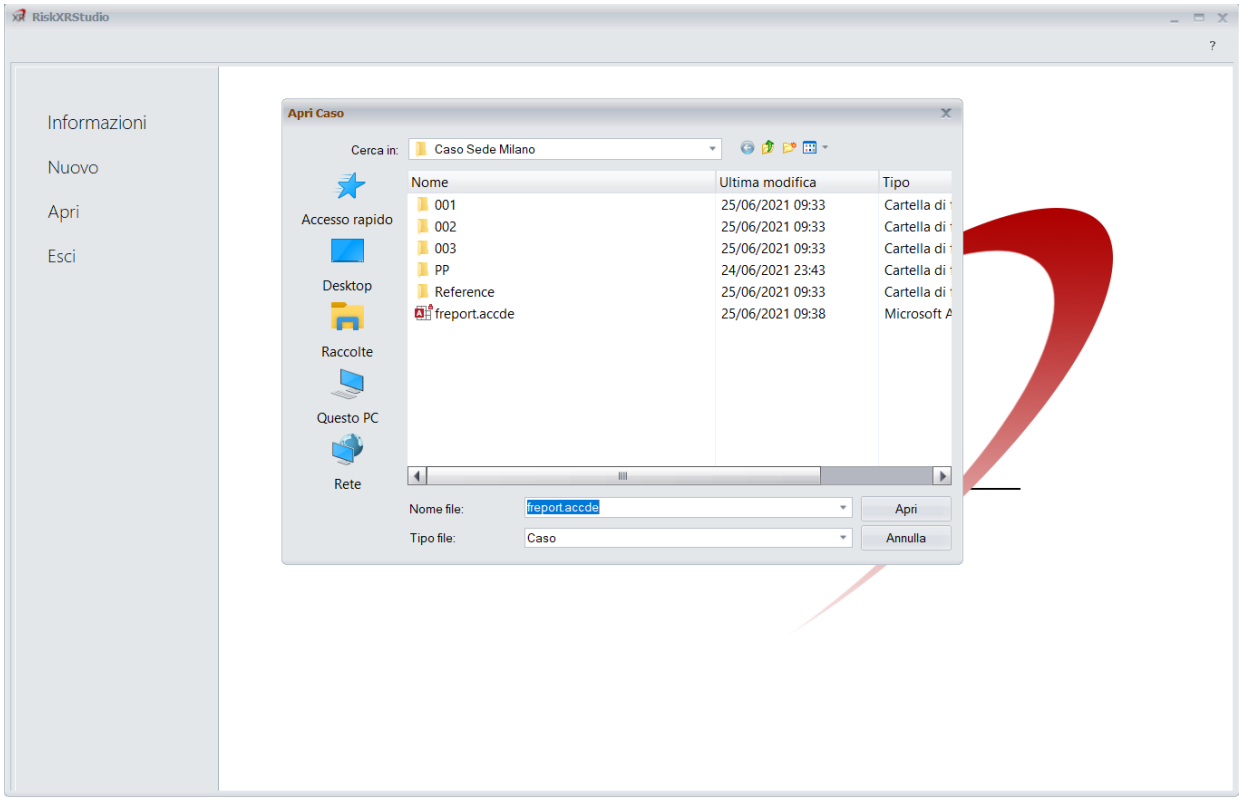
2.4 APRIRE UN CASO ESISTENTE

Se invece arrivati alla videata iniziale si desidera aprire un Caso già esistente:

- premere "Apri".

- Nella finestra che seguirà cercare la directory del caso desiderato.

- Scegliere il Caso su cui lavorare aprendo con un doppio click la cartella con il Nome del Caso e lanciando il file standard "freport.accde" al suo interno.



- All'interno della directory del Caso si può vedere la directory PP con il file dei profili di sicurezza XR delle Aree a sicurezza differenziata (se utilizzati).

- In questo esempio ci sono 3 Aree a sicurezza differenziata 001, 002, 003 (opzionali)

- La directory Reference, di servizio, non usata dall'utente, con una copia del Caso (opzionale).

2.5 DEFINIRE IL CASO

Nella scheda "Caso" come già detto è possibile inserire i "**Parametri Generali**" relativi che sono:

- **Nome dell'organizzazione** per cui si effettua il Risk Assessment.

- **Unità organizzativa** coinvolta, se si vuole specificare.

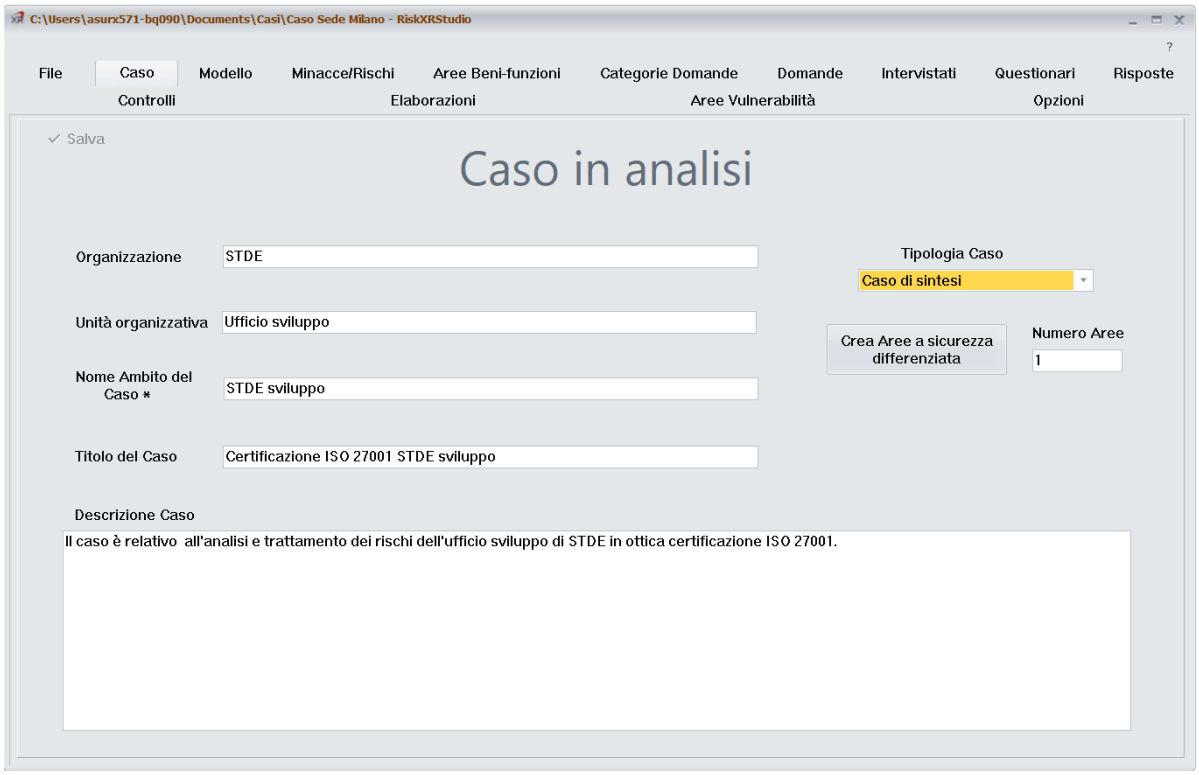
- **Ambito del "Caso"**. Indica l'**Ambito complessivo** considerato nell'analisi (unico parametro obbligatorio). Rappresenta il Nome al Top del modello degli asset XR.

- **Titolo del Caso**. Viene inserito nel frontespizio dei Report generati dallo strumento.

- **Tipologia del Caso (**appare solo dopo che il Caso è stato creato. Cioè è stato inserito il nome dell'Ambito del Caso ed è stato salvato).

  Specifica se è un:

  - **Caso standard** (default), cioè un Caso senza Aree a sicurezza differenziata.
  - **Area a sicurezza differenziata**, una delle Aree in cui è stato suddiviso il modello XR con diverso Profilo di sicurezza XR.
  - **Caso di sintesi**, caso che sintetizza nei suoi risultati quanto risulta dalla valutazione dei rischi differenziata delle varie Aree a sicurezza differenziata considerate.



2.6 COMPILARE I "VALORI DEGLI ASSET ESPOSTI AL RISCHIO"

RiskXRStudio utilizza come dati di INPUT per gli ASSET i "**Valori potenziali esposti al rischio"** caratteristici di tali elementi.

Più alti sono questi valori e maggiore è il possibile impatto che si avrà al concretizzarsi di una MINACCIA.

Ogni "minaccia" provoca su uno specifico **Asset** solo determinate **tipologie di Impatto**.

Dalla presenza di **"valori esposti al rischio"** per quelle tipologie di impatto nell'asset e dalla **"pericolosità della minaccia (gravità delle conseguenze)"** su quell'asset verrà valutato l'**impatto potenziale** su singolo incidente conseguente.

La metodologia RiskXRStudio considera 5 tipologie di impatti individuate tramite il cosiddetto "Paradigma RIDPU".

Il PARADIGMA "RIDPU" è l'insieme di 5 parametri che si riferiscono alle 5 **"tipologie di VALORI"** e corrispondentemente alle 5 "**tipologie di possibili impatti standard"** che sono correlate (a possibili danni a):

R Riservatezza

I Integrità

D Disponibilità

P Valore Economico/ Fisico/ Ripristino/ Costi diretti/ Tangibili

U Reputazione/ Diritti/ Libertà/ Business/ Intangibili

Nella metodologia si definisce "**Profilo di esposizione XR"** l'insieme dei "**Valori esposti al rischio**" dell'oggetto considerato che può essere un **Caso**, un **Ambito** o un **Asset**.

Il paradigma RIDPU viene utilizzato anche per rappresentare le tipologie di valori di OUTPUT delle elaborazioni, dell'**IMPATTO** e del **RISCHIO** sia potenziali che effettivi stimati.

Vediamo come esprimere il "**Profilo di esposizione XR**" tramite i vari parametri del paradigma RIDPU.

Tenere presente che la scala dei valori è stata predisposta per essere **compatibile** e utilizzabile sia in **ambiente CIVILE** che **MILITARE**, questo ha generato le scale di valori mostrate nel seguito.

Si specificano di seguito i valori di riferimento utilizzabili:

- **VALORE RISERVATEZZA (R)**:
  - È il valore di esposizione relativo alla confidenzialità/segretezza delle informazioni trattate, dipende dalla loro classificazione (valori 0 – 6 metrica livelli), possono essere sia non classificate che classificate, ambedue le tipologie sono state inserite nella lista di riferimento dello strumento:

Valori Classificazione Dati (Classifica di Segretezza)		
Descrizione	COD.	Livello
Pubblici	P	0
Ad uso interno	I	2
Comuni (personali)	C	3
Particolari	SP	4
Giudiziari	G	4
Riservati/ Proprietari	RP	4
Genetici	GE	5
Non classif. Controllato	U	1
Riservato	R	3
Riservatissimo	RR	4
Segreto	S	5
Segretissimo	SS	6
Nessuna Classifica di Segretezza		0

Si suppone di considerare una quantità di dati contenuta. Per grandi quantità di dati il livello di riservatezza potrebbe scattare di livello.

I valori di "Riservatezza" sono assegnabili alle "Basi di dati" che rappresentano le "INFORMAZIONI" in quanto tali (anche una singola informazione se rilevante) e non rappresentano l'hardware del supporto che è di categoria "HW Sistemi IT".

I valori di riservatezza sono assegnabili anche alle Applicazioni e importante al "SW di communication".

Per quest'ultima categoria il **valore per la Riservatezza** è da dare in base alla "**classificazione del flusso di dati**" gestito nella rete da tale software avente maggiore confidenzialità.

Solo inserendo un valore esposto non nullo di Riservatezza in un "SW di communication" che gestisce le reti potremo avere valori di rischio per la minaccia "Intercettazioni di Rete" diverse da 0.

- **VALORE INTEGRITA' (I)**:
  - È il valore di esposizione relativo alla Integrità delle informazioni primariamente, cioè la gravità rappresentata dalla perdita della loro integrità, ma in generale, se riferito ad altro oggetto, integrità dello stesso o dei suoi componenti (valori 0 – 6 metrica livelli standard).

Valori Integrità		
Livello	Cod. Liv.	Descrizione
6	AA	Altissimo
5	A	Alto
4	MA	Medio-Alto
3	M	Medio
2	MB	Medio-Basso
1	B	Basso
0		Nullo o da non valutare

- **VALORE DISPONIBILITA' (D)**:
  - È il valore di esposizione relativo alla Disponibilità del Bene o dei Beni a cui si riferisce. È legato qui in modo proporzionale al tempo per cui si può fare a meno di tale/i elemento/i, ma può non essere l'unico fattore per la scelta del valore, in quanto è da considerare la **criticità dell'ambito supportato** che può essere legata anche ad altri fattori:

Valori Disponibilità

Livello	Cod. Liv.	Descrizione
6	AA	immediato
5	A	Fino a 4 ore
4	MA	Fino a 1 giorno
3	M	Fino a 3 giorni
2	MB	Fino a 7 giorni
1	B	Fino a 15 giorni
0		> di 15 giorni

- **VALORE ECONOMICO/ FISICO/ RIPRISTINO (P)**:
  - È il valore di esposizione relativo al "valore diretto" associato all'oggetto, può essere il valore di acquisto o di leasing o comunque quanto si può esprimere il valore necessario per ottenerlo (costo di ripristino), se per varie ragioni non lo avessimo più. Per i dati e il software può corrispondere al costo di una operazione di Ripristino da backup, se possibile (valori 0 – 6 metrica livelli standard). Per una persona è relativo al danno economico, fisico o a costi diretti che può avere. E' un danno tangibile/fisico o diretto.

Valori Economico/ Fisico		
Livello	Cod. Liv.	Descrizione
6	AA	Altissimo
5	A	Alto
4	MA	Medio-Alto
3	M	Medio
2	MB	Medio-Basso
1	B	Basso

0		Nullo o da non valutare

- **VALORE REPUTAZIONE/ DIRITTI/ LIBERTA'/ BUSINESS/ INTANGIBILI (U)**:
  - È il valore di esposizione relativo alla Reputazione/ Immagine che ha impatto sullo "Share di mercato" per un'azienda privata e perciò con il suo Business, mentre riguarda la reputazione nei confronti dei cittadini, il valore sociale, ma anche la reputazione verso le autorità politiche e del governo che possono influire sul Budget reso disponibile ad una Amministrazione, sul suo assetto organizzativo e sull'allargamento o riduzione della sua Missione. Per una Persona fisica oltre la reputazione riguarda i diritti e le libertà specie in campo privacy e tutti gli aspetti intangibili non informatici. Se non si ritiene rilevante o valutabile adeguatamente si può inserire il valore 0 escludendo questa tipologia di rischio (valori 0 – 6 metrica livelli standard).

Valori Reputazione/ Diritti/ Libertà/ Business		
Livello	Cod. Liv.	Descrizione
6	AA	Altissimo
5	A	Alto
4	MA	Medio-Alto
3	M	Medio
2	MB	Medio-Basso
1	B	Basso
0		Nullo o da non valutare

2.7 CRITERI INTEGRATIVI DI CLASSIFICAZIONE

In questo paragrafo possiamo trovare alcuni criteri che possono consentire di individuare dalla tipologia di dato il livello corretto dei valori esposti al rischio di basi di dati dell'analisi in corso.

INTEGRITA'

1. Dati dei processi di business A (MA)
2. Dati dei processi Amministrativo e contabile M
3. Dati del Controllo di gestione MB

DISPONIBILITA'

1. Dati dei processi legati ai Ricavi/Mission A (MA)
2. Dati legati ad Obblighi di legge correlati alla disponibilità dei dati MA
3. Dati legati ai Flussi finanziari M

RISERVATEZZA

1. Dati riservati legati ai Ricavi/Mission A (MA)
2. Dati legati per la confidenzialità alla competitività nell'erogazione servizi M
3. Dati che se rivelati potrebbero complicare l'interazione con l'esterno o la gestione di terze parti MB

NOTE: la scelta di A o MA nei criteri 1. dipende dal valore esposto al rischio della mission dell'organizzazione ad esempio la natura militare o civile. Nel militare può arrivare anche ad AA.
Ciascun criterio e livello indicato costituisce un supporto alla decisione della persona che sola conosce la reale situazione e tipologia del dato e dunque del valore esposto al rischio da considerare nel complesso.

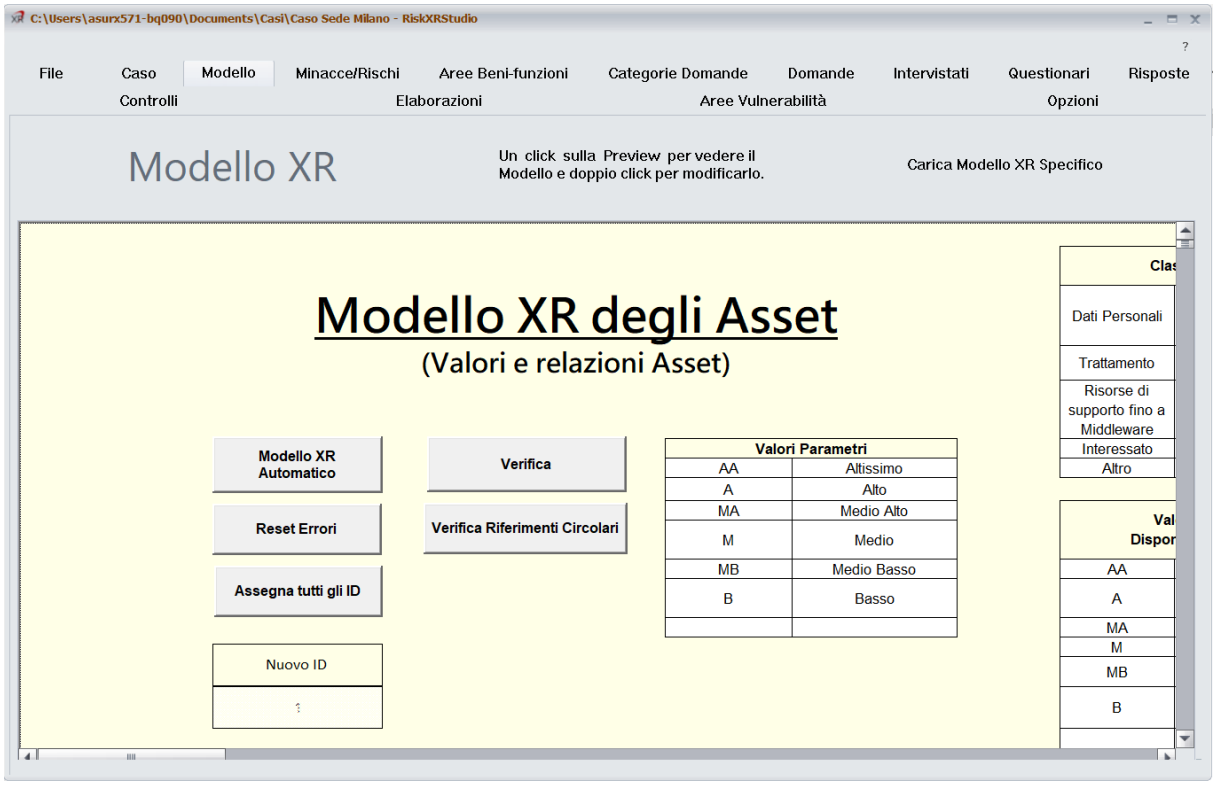
2.8 INSERIRE I DATI DEI BENI/ASSET E DEGLI AMBITI

In RiskXRStudio™ 2021 i **valori esposti al rischio dei Beni/Asset** si inseriscono tramite il modulo applicativo Excel:

"modeldatacollection.xlsm"

Questo modulo separato dall'applicazione e dalla base dati del Caso consente di utilizzarlo per più Casi, importandolo con l'apposita funzione di RiskXRStudio.

Quando si crea un **nuovo Caso** lo strumento mette a disposizione un **modello "vuoto"** senza asset a cui si può accedere con un doppio click nella **PREVIEW** della pagina del modello di anteprima (**scheda Modello**) e **modificarlo** opportunamente.



Il caricamento del modello XR può richiedere un certo tempo di attesa.

L'applicazione sfrutta la flessibilità di Excel per facilitare al massimo l'acquisizione tramite **COPIA/INCOLLA VALORI** dei dati da varie fonti. Questo è facilitato dal copiare per "colonne" in quanto diventa indipendente dai campi dei record della fonte di dati (**spreadsheet o database**).

Una volta terminato l'input dei dati in tale applicazione si preme il tasto "**VERIFICA"** e poi "**VERIFICA RIFERIMENTI CIRCOLARI**".

Se nessun errore viene segnalato il modello XR è completato. RiskXRStudio lo importerà automaticamente.

Con il Tasto "**Carica Modello XR specifico**" è possibile importare/caricare una copia di un modello già predisposto con gli asset e sostituirlo a quello presente nel Caso al momento.

Se si desidera sviluppare da un modello vuoto in tempi successivi alla creazione del Caso, allora si può copiare dal TEMPLATE che è presente nella directory **Documenti\Casi Tools\Modeldatacollection XR** e poi modificarlo direttamente.

Basta poi copiare il file nella directory del Caso "rinominandolo" esattamente "**modeldatacollection.xlsm**".

2.8.1 MODELDATACOLLECTION XR

Come detto precedentemente l'applicazione "Modeldatacollection XR" è uno strumento intermedio che facilita l'acquisizione dei dati in input a RiskXRStudio. Esso ha una pagina **Istruzioni** contenente alcune indicazioni importanti per l'utilizzo dello strumento.

Per ciascuna analisi (CASO) si utilizza un solo MODELLO XR.

Si può però utilizzare più modelli XR dal TEMPLATE per raccogliere i dati di sottomodelli le cui righe saranno poi copiate in un unico Modello XR congruente da usare per il Caso.

L'Applicazione excel "Modeldatacollection XR" può essere copiata più volte e distribuita per l'acquisizione pur avendo un'unica licenza di RiskXRStudio.

Il modello XR unico consente di fare un controllo complessivo tramite le funzioni VERIFICA e VERIFICA RIFERIMENTI CIRCOLARI del Caso prima di iniziare l'analisi.

Il Modello XR degli asset si crea nel foglio "BENI" usando gli "elenchi a cascata" di valori, "digitando direttamente i valori da tastiera" o copiando valori da spreadsheet e database per colonna. I valori sono espressi come B (basso), MB (medio basso), M (medio), ecc. o come "valore monetario numerico", ad esempio: 380 (euro) se si possiedono dati affidabili. Lo strumento armonizzerà i dati inseriti normalizzandoli.

Il modello è di tipo "gerarchico con eccezioni (Ambiti riferiti)" ed ha al top il CASO (l'ambito complessivo) che è implicito e non viene inserito come NOME.

Un MODELLO XR può essere utilizzato per più CASI in quanto il nome del Caso non è presente nel modello. Il file corrispondente ha sempre un nome fisso "**modeldatacollection.xlsm**" ed è posto nella "Directory del CASO".

Definizioni:

- Si dice **CASO** l'ambito complessivo oggetto di analisi.

- Si dice **ASSET** qualsiasi risorsa che abbia un Valore e di cui si conoscono le caratteristiche, la CATEGORIA di appartenenza e i VALORI.

Con un ASSET (una riga della tabella) si può rappresentare anche un "gruppo di asset" es. per 50 PC come "PC (50)". Non mettere un numero iniziale perché un numero iniziale ha un significato speciale nella metodologia che non è il numero di asset.

- Si dice **AMBITO** (sistema) un "insieme di asset" (o altri Ambiti) suoi componenti sia di tipo fisico che concettuale che lo rappresentano (figli).

Un Ambito può avere anche figli esterni che costituiscono sue possibili fonti di rischio esterne (eventi concatenati/rischi ambientali).

- Si dice **AMBITO RIFERITO** un ambito nel modello avente il NOME ESATTO di un ambito già presente e con cui si "identifica". Consente di modellare un figlio con più padri. L'ambito RIFERITO non ha figli indicati, perché i suoi figli sono già rappresentati nel modello dall'ambito con lo stesso nome.

Questo evita di dover duplicare il sottomodello di uno stesso Ambito (come Ambito riferito) quando collegato a Padri diversi.

Regole:

- Gli ASSET possono essere inseriti in qualunque livello del modello, anche nello stesso livello con degli Ambiti, ma sono sempre le FOGLIE del modello, non hanno figli.

- Gli AMBITI possono stare in qualunque livello del modello, hanno sempre figli, non sono mai foglie del modello (eccetto ambiti riferiti).

Procedura:

- Il MODELLO si crea generalmente iniziando dai livelli più alti e passando poi a quelli inferiori.

Specifichiamo di che cosa vogliamo sapere il rischio e poniamolo nel modello legandolo poi a tutti gli asset e ambiti da cui dipende e al top del modello. Per ogni elemento del modello:

1. **Nome.** Si inserisce il **NOME** dell'ASSET o dell'AMBITO nella colonna "**NOME BENE**".

2. **Categoria del Bene.** Si inserisce poi la **CATEGORIA DEL BENE**, selezionandola dal rispettivo menu a discesa. Selezionare questo come primo parametro di un asset, in tal modo i campi da "non compilare" si presenteranno "zigrinati".

Gli **ambiti** hanno come CATEGORIA DEL BENE "**AMBITI**". Inserire I nomi degli "**Ambiti**" per primi, così da poterli selezionare per gli altri asset come Ambito Padre.

Se non si vedessero gli AMBITI nella lista a discesa quando si inseriscono gli asset, assicurarsi di avere raggiunto la testa (**top**) della "lista", premendo la freccia a destra verso l'alto.

3. **Padre**. La scelta dell'Ambito padre viene fatta selezionandolo dalla lista a discesa nella colonna. Se la lista a discesa sembra vuota scorrere la freccia fino al limite superiore. Se un ambito è stato dichiarato appare sicuramente

nella lista. Se la lista è particolarmente lunga può essere conveniente copiare il nome del padre dalla colonna NOME Asset/Ambito e incollarlo nella colonna PADRE con "Incolla speciale/Valori" per non modificare i formati delle celle.

Gli asset o gli ambiti che siano collegati direttamente al **CASO** devono avere la cella PADRE "**vuota**".

4. **Valori.** Si compilano i **VALORI** A RISCHIO, "solo" per gli **ASSET**, essi dipendono anche dalla criticità degli **AMBITI/SERVIZI** superiori che essi supportano. Per gli **AMBITI** non è necessario inserire DATI, perché i risultati di rischio sono ottenuti dagli Asset interni figli del sottomodello che li supporta e li rappresenta.

I **VALORI degli ASSET** vengono compilati valutando l'impatto che una mancanza relativa alla caratteristica specifica (RIDPU - riservatezza, integrità, disponibilità, Valore Economico/Fisico e Valore Reputazione/Diritti e Libertà) **comporterebbe** per l'"insieme degli obiettivi rilevanti per l'organizzazione (**mission**)" al **massimo possibile**.

Inserire i VALORI esposti al rischio selezionando il valore corrispondente: dalla lista a discesa, il dato riguarda il singolo bene o un gruppo di beni a secondo di quanto specificato nell'elemento del modello.

Per i singoli campi RIDPU riferirsi al capitolo relativo in cui vi si troveranno tutti i dettagli necessari.

I valori (es. A, MB, …) si possono anche digitare direttamente.

Si possono digitare anche valori monetari (es. 30000) che lo strumento normalizzerà all'interno della base dati. Verrà chiesto se è un numero voluto, per accertare che si voglia effettivamente mettere un valore numerico monetario e non sia un errore di digitazione.

5. **Classe.** - Il campo "CLASSE" specifica la classe di un AMBITO e viene usato in particolare in campo **privacy** secondo una struttura specifica:

. Il valore "T" specifica che l'Ambito è un "TRATTAMENTO".
La "T" non si pone per gli AMBITI RIFERITI.

. Il valore "S" indica un Ambito che ha come figli tutte le RISORSE di BASE e MIDLLEWARE di quel trattamento. È a sua volta figlio del TRATTAMENTO.

. Il valore "I" specifica che è una classe di INTERESSATI o un interessato. Es. clienti, dipendenti, Mario Rossi, ecc. Ha come figli i Trattamenti ("T") che si riferiscono all'interessato.

. Se il campo è VUOTO invece indica che è un ambito standard, non "T", "S" o "I".

Sotto un Ambito "T" in generale si pongono:

. un programma applicativo,

. una base dati relativa alle informazioni gestite nel trattamento,

. le persone che effettuano il trattamento,

. un Ambito di classe "S" che avrà come figli le risorse informatiche fino al Middleware utilizzate dal Trattamento.

6. **Descrizione dell'Asset o Ambito.** (opzionale) Si può compilare una descrizione dell'Asset o Ambito, oppure utilizzare il campo per specificare il **Risk Owner o Referente** per l'asset/ambito a cui potranno essere inviati i **Piani di Rientro** dalle vulnerabilità. In tal caso il formato deve essere:

a. nome e cognome

b. il carattere " # " cancelletto (con uno spazio avanti e uno spazio dietro)

c. la E-mail del Risk Owner.

Esempio: **Mario Rossi # m.rossi@organizz.it**

6. **Classificazione dati**. Viene qui specificata la classificazione dei dati. Vale per gli Archivi, i database e i dati in genere, quando ritenuto opportuno. È un campo "multiplo" vi si possono inserire più Classi di dati correlate all'Asset, saranno esplicitati i relativi livelli di Riservatezza. Sarà cura dell'analista vedere il livello più elevato indicato (es. A, MA, ecc.) ed inserirlo nel campo relativo alla **Riservatezza.** Con un numero elevato di record o di interessati si può valutare anche un valore superiore.

7. **Verifica.**

La funzione/Tasto **VERIFICA** evidenzia gli errori e fornisce le seguenti indicazioni ponendo:

a) **ROSSI gli AMBITI** nella colonna NOME che nel modello siano senza figli e non siano Ambiti riferiti (**ERRORE Ambito in foglia**).

b) **GIALLI** gli **AMBITI RIFERITI**, facilitando il controllo della logica del modello (È una Informazione, non è un errore).

c) **ROSSI** gli **AMBITI PADRE** che siano richiamati, ma che non siano ancora stati dichiarati (**ERRORE Ambito non dichiarato**).

ID	Ambito Padre	Nome Bene (Asset/Ambito)	Categoria Bene	Descrizione
1	sempronio	pippo	Ambiti	ERRORE Ambito in ciclo
2		caio	Ambiti	ERRORE AMBITO senza figli
3	caiox	pippo	Ambiti	NOME AMBITO PADRE non esistente e AMBITO RIFERITO
4		caio	Applicazioni	ERRORE ASSET con NOME di un AMBITO
5		gepi	sempronio	ERRORE NOME CATEGORIA non esistente

d) **VIOLA.** Il nome dell'ASSET della cella è uguale al nome di un AMBITO (**ERRORE di Nome non univoco**).

e) **X** con linea singola nella colonna CATEGORIA BENE- Errore di **CATEGORIA BENE NON ESISTENTE**.

Gli **spazi** davanti e dopo i NOMI e PADRI vengono automaticamente eliminati dalla funzione VERIFICA.

- La funzione **RESET ERRORI** elimina i colori e le X posti dalle funzioni di VERIFICA e per "CATEGORIA BENE NON ESISTENTE" poste dalla funzione ESPORTA.

- La funzione **VERIFICA RIFERIMENTI CIRCOLARI** consente di identificare tutte gli AMBITI che sono linkati in modo circolare (Errore di riferimento circolare, CICLO), l'errore non consente la valutazione per ereditarietà. L'efficacia di questo test è al 100% solo dopo che la funzione "Verifica" non indica più errori.

a) X con linee doppie nella colonna NOME BENE - Indica AMBITO che fa parte di una circolarità - ERRORE DI RIFERIMENTO CIRCOLARE.

<u>Come fare per:</u>

- **COPIARE DA FONTI ESTERNE O INTERNE** IN CELLE DELLA TABELLA-> Usare COPIA, poi INCOLLA (speciale) VALORI (da spreadsheet o database).

Usando COPIA completa, non solo valori, si potrebbero avere problemi di formattazione.

- **CANCELLARE DELLE CELLE** -> Usare il tasto CANC per cancellare solo il valore.

- **SPOSTAMENTO DI CELLE** -> SPOSTARE LE RIGHE DI CELLE DELLA TABELLA SELEZIONANDOLE su tutta la loro larghezza e premendo "SHIFT" durante lo spostamento.

- **STAMPARE GLI ELENCHI DEI BENI** -> Stampare il foglio "Stampe" oppure selezionare la parte da stampare e copiarla in Word.

- Per **INSERIRE un ID** in maniera automatica UNIVOCO per ciascun ASSET/AMBITO del modello XR premere il tasto "**ASSEGNA TUTTI GLI ID**".

Questo eliminerà eventuali numeri spuri davanti ai nomi delle colonne "Nome Asset/Ambito" e "Padre", inserendo davanti agli ASSET o AMBITI un **ID corretto univoco di 3 cifre**.

L'ID univoco davanti agli Asset/Ambiti è usato per associare ad essi un questionario o un file di dati derivato da uno strumento di Vulnerability Assessment (VA). Viene resa disponibile anche l'indicazione **dell'ID da usare se si desidera inserire manualmente un nuovo Asset/Ambito**.

Questa possibilità viene usata quando avendo modificato il modello dopo l'uso del tasto di ID automatico, non si vuole che possano essere modificati i valori degli ID, avendo già associato ad essi questionari o file VA.

- Premendo il tasto "**MODELLO XR AUTOMATICO**" è possibile ottenere automaticamente un Modello XR con ciascun ambito PADRE avente tutti i suoi FIGLI aggregati insieme, indipendentemente dalla posizione precedente degli asset nel modello.

St De
Studio Dell'Agnello S.r.l.

MODELDATACOLLECTION XR

Valori Ambiti/Asset in Valutazione

Modello XR

Modello XR Automatico | Verifica
Reset Errori | Verifica Riferimenti Circolari
Assegna tutti gli ID

Nuovo ID
70

Valori Parametri	
AA	Altissimo
A	Alto
MA	Medio Alto
M	Medio
MB	Medio Basso
B	Basso

Classe	
Dati Personali	P
Trattamento	T
Risorse di supporto fino a Middleware	S
Interessato	I
Altro	

Valori Disponibilità	
AA	Immediato
A	fino a 4 ore
MA	fino a 1 giorno
M	fino a 3 giorni
MB	fino a 7 giorni
B	fino a 15 giorni
	> di 15 giorni

Valori Classificazione Dati (Classifica di Segretezza)	
P	Pubblici -> 0
I	Ad uso interno -> MB
C	Comuni (personali) -> M
SP	Particolari/Sensibili -> MA
G	Giudiziari -> MA
RP	Riservati / Proprietari -> MA
GE	Genetici -> A
U	Non classif. Controllato -> B
R	Riservato -> M
RR	Riservatissimo -> MA
S	Segreto -> A
SS	Segretissimo -> AA
	Nessuna Classifica di Segretezza

Scheda Beni

Classe	Padre	Nome Asset/Ambito	Categoria	Descrizione	Valore Economico/ Fisico (P)	Valore Riservatezza (R)	Valore Disponibilità (D)	Valore Integrità (I)	Valore Reputazione/ Diritti e Libertà (U)	Classificazione Dati
		001 Operatività	Ambiti							
		002 Vista Privacy	Ambiti							
	001 Operatività	003 Gestione Fornitori	Ambiti							
	001 Operatività	004 Gestione HR	Ambiti							
	001 Operatività	005 Marketing	Ambiti							

	006 Clienti	012 Trattamento Analisi di mercato	Ambiti							
	006 Clienti	013 Trattamento offerte	Ambiti							
	007 Fornitori	014 Trattamento Gestione Acquisti	Ambiti							
	007 Fornitori	015 Trattamento Gestione Fornitori	Ambiti							
	007 Fornitori	016 Trattamento Gestione Albo Fornitori	Ambiti							
	008 Dipendenti	017 Trattamento Contributi	Ambiti							
	008 Dipendenti	018 Trattamento TFR	Ambiti							
	008 Dipendenti	019 Trattamento stipendi	Ambiti							
T	009 Ufficio Gestione Fornitori	016 Trattamento Gestione Albo Fornitori	Ambiti							
T	009 Ufficio Gestione Fornitori	014 Trattamento Gestione Acquisti	Ambiti							
T	009 Ufficio Gestione Fornitori	015 Trattamento Gestione Fornitori	Ambiti							
T	010 Ufficio HR	018 Trattamento TFR	Ambiti							
T	010 Ufficio HR	019 Trattamento stipendi	Ambiti							
T	010 Ufficio HR	017 Trattamento Contributi	Ambiti							
T	011 Ufficio Marketing	012 Trattamento Analisi di mercato	Ambiti							
T	011 Ufficio Marketing	013 Trattamento offerte	Ambiti							
	016 Trattamento Gestione Albo Fornitori	028 Applicazione di Gestione Albo Fornitori	Applicazioni		B		MA	MA		
P	016 Trattamento Gestione Albo Fornitori	029 Archivio di Gestione Fornitori	Basi di Dati		B	M	MA	A	MA	Riservato -> M
	016 Trattamento Gestione Albo Fornitori	030 Personale Ufficio Gestione Fornitori	Persone		B		M			
S	016 Trattamento Gestione Albo Fornitori	031 S.I A1 Client-server nel CED Roma 1	Ambiti	Sistema di elaborazione con architettura Client-Server						
S	014 Trattamento Gestione Acquisti	031 S.I A1 Client-server nel CED Roma 1	Ambiti	Sistema di elaborazione con architettura Client-						

	014 Trattamento Gestione Acquisti	033 Applicazione di Gestione Acquisti	Applicazioni		B		MA	MA		
P	014 Trattamento Gestione Acquisti	034 Archivio di Gestione Acquisti	Basi di Dati		B	MB	M	A		Ad uso interno -> MB
	014 Trattamento Gestione Acquisti	035 Personale Ufficio Gestione Acquisti	Persone		B		M			
	015 Trattamento Gestione Fornitori	036 Applicazione di Gestione Fornitori	Applicazioni		B		MA	MA		
P	015 Trattamento Gestione Fornitori	029 Archivio di Gestione Fornitori	Basi di Dati		B	M	MA	A	A	Riservato -> M
	015 Trattamento Gestione Fornitori	030 Personale Ufficio Gestione Fornitori	Persone		B		M			
S	015 Trattamento Gestione Fornitori	031 S.I A1 Client-server nel CED Roma 1	Ambiti	Sistema di elaborazione con architettura Client-Server						
	018 Trattamento TFR	040 Applicazione Gestione Personale	Applicazioni		B	MB	MA	MA		
P	018 Trattamento TFR	041 Archivio del Personale	Basi di Dati		B	MB	MA	A	A	Sensibili -> MA
	018 Trattamento TFR	042 Personale Ufficio HR	Persone		MB	MB	M			
S	018 Trattamento TFR	031 S.I A1 Client-server nel CED Roma 1	Ambiti	Sistema di elaborazione con architettura Client-Server						
	019 Trattamento stipendi	040 Applicazione Gestione Personale	Applicazioni		B	MA	A	MA		
P	019 Trattamento stipendi	041 Archivio del Personale	Basi di Dati		B	MA	A	A	A	Sensibili -> MA
	019 Trattamento stipendi	042 Personale Ufficio HR	Persone		MB	MA	MA			
S	019 Trattamento stipendi	031 S.I A1 Client-server nel CED Roma 1	Ambiti	Sistema di elaborazione con architettura Client-Server						
	017 Trattamento Contributi	042 Personale Ufficio HR	Persone		MB	MB	M			
S	017 Trattamento Contributi	049 S.I A2 Cloud Based	Ambiti	Sistema di elaborazione con architettura basata sul Cloud						
	012 Trattamento Analisi di mercato	050 Applicazione Analisi di mercato	Applicazioni		B		MA	MA		
P	012 Trattamento Analisi di mercato	051 Archivio Analisi di mercato	Basi di Dati		B	MA	M	A		Riservato -> M
	012 Trattamento Analisi di mercato	052 Personale Ufficio Marketing	Persone		B		M			
S	012 Trattamento Analisi di mercato	031 S.I A1 Client-server nel CED Roma 1	Ambiti	Sistema di elaborazione con architettura Client-Server						

	013 Trattamento offerte	054 Applicazione GestioneOfferte	Applicazioni		B		A	MA		
P	013 Trattamento offerte	055 Archivio Offerte	Basi di Dati		B	MA	A	A		Riservatissimo -> MA
	013 Trattamento offerte	052 Personale Ufficio Marketing	Persone		B		MA			
S	013 Trattamento offerte	031 S.I A1 Client-server nel CED Roma 1	Ambiti	Sistema di elaborazione con architettura Client-Server						
	031 S.I A1 Client-server nel CED Roma 1	058 Server UNIX VX45	HW Sistemi IT		MB		A			
	031 S.I A1 Client-server nel CED Roma 1	059 S.O. Ubuntu	SW Sistemi IT		B		A	MA		
	031 S.I A1 Client-server nel CED Roma 1	060 Symantec Appliance Firewall sw	SW Communication		B	MA	A	A		Sensibili -> MA
	031 S.I A1 Client-server nel CED Roma 1	061 Router Cisco XD45	HW Communication		MB		A			
	031 S.I A1 Client-server nel CED Roma 1	062 CED Roma1	Ambiti							
	062 CED Roma1	063 Palazzina C - via dei eremi 15 Roma	Edifici e Servizi		AA		A			
	062 CED Roma1	064 Sistema di aria condizionata CED Roma 1	Sistemi di Supporto		M		A			
	062 CED Roma1	065 Sistema antincendio CED Roma 1	Sistemi Antincendio		MB		MA			
	062 CED Roma1	066 Accessi con badge CED Roma 1	Sistemi di Sicurezza		MB		A	A		
	062 CED Roma1	067 Cabina Elettrica privata dell'organizzazione	Utenze		M		A			
	049 S.I A2 Cloud Based	068 Applicazione Cloud Contributi	Applicazioni		B	MB	MA	MA		
P	049 S.I A2 Cloud Based	069 Base dati Cloud Contributi	Basi di Dati		B	MB	MA	A	A	Sensibili -> MA

2.8.2 SCEGLIERE IL NOME DEGLI ASSET PER IL MODELLO XR

Il **nome** degli ASSET e degli AMBITI nella metodologia RiskXRStudio può essere scelto liberamente, tenendo conto però che alcune funzioni utilizzano il NOME per svolgere il loro compito. Vediamo queste regole sui nomi.

2.8.3 COME ASSOCIARE "QUESTIONARI PERSONALIZZATI" PER GLI ASSET

Se si desidera valutare con controlli specifici uno o più Asset o Ambiti.

1. Si pongono 3 cifre davanti al Nome dell'Asset da valutare es. NOME ASSET: **"041 server HP45B"**.

2. Si crea un questionario/intervistato avente nel nome le stesse 3 cifre iniziali come NOME INTERVISTATO/QUESTIONARIO: es. **"041 Questionario server HP45B - Bianchi"**.

3. Lo strumento assocerà il QUESTIONARIO all'ASSET/AMBITO. Questo consentirà di individuare il numero di "Criticità (risposte non attuate di controlli critici (peso da 8 a 10)" nelle mappe di rischio XR.

4. Ogni ASSET o AMBITO deve avere un **NUMERO di 3 cifre**, se assegnato, **UNIVOCO**. Questo consente la valutazione corretta dei Piani di sicurezza associati agli asset.

5. È possibile anche porre le stesse 3 cifre a più questionari di intervistati diversi. Tutte le risposte saranno associate all'asset o ambito avente lo stesso numero (conteggio delle criticità derivate da tutti gli intervistati).

6. Per quanto detto prima, il "numero di beni di un gruppo", se lo si vuole esplicitare, deve essere posto successivamente nel NOME. Come ad esempio: Client PC x 250 – AB4x

NOTA: i tre caratteri finali di un nome, se hanno la forma "#nnn", con nnn tre cifre numeriche indicano il Profilo di protezione XR di sicurezza differenziata, evitare perciò questa forma e # nel nome se non per questo uso specifico (vedi successivamente).

2.8.4 COME GESTIRE LE AREE A SICUREZZA DIFFERENZIATA

Obiettivo delle Aree a sicurezza differenziata è una valutazione "più accurata" dei rischi degli Asset basata sulla specificità dei Profili di

protezione XR ad essi applicati, pur utilizzando un unico Modello degli Asset ed effettuando un'unica elaborazione di sintesi.

Per utilizzare questa modalità di valutazione seguire i passi elencati:

1. Definire l'ambito complessivo del **Caso di sintesi,** che può essere anche l'intera organizzazione.

2. Creare il **Modello XR** del Caso con tutti gli Asset e le loro relazioni.

3. Indicare come si intende suddividere gli ASSET del Modello XR tra le varie **Aree a sicurezza differenziata** definite, mettendo in fondo al nome di ciascun asset "#nnn", con nnn il numero dell'area di appartenenza (esempio: Windows server KXW#001). Si considera l'asset Windows server KXW appartenente all'Area 001. Maggiore è il numero di Aree a sicurezza differenziata, maggiore è l'accuratezza dell'analisi, ma anche il tempo necessario a condurla. La suddivisione, perciò, deve avere una sua giustificazione.

4. Il **Caso di Sintesi** deve contenere tutte le Domande relative ai controlli utilizzati nell'analisi di sintesi e nelle aree a sicurezza differenziata, se ulteriori.

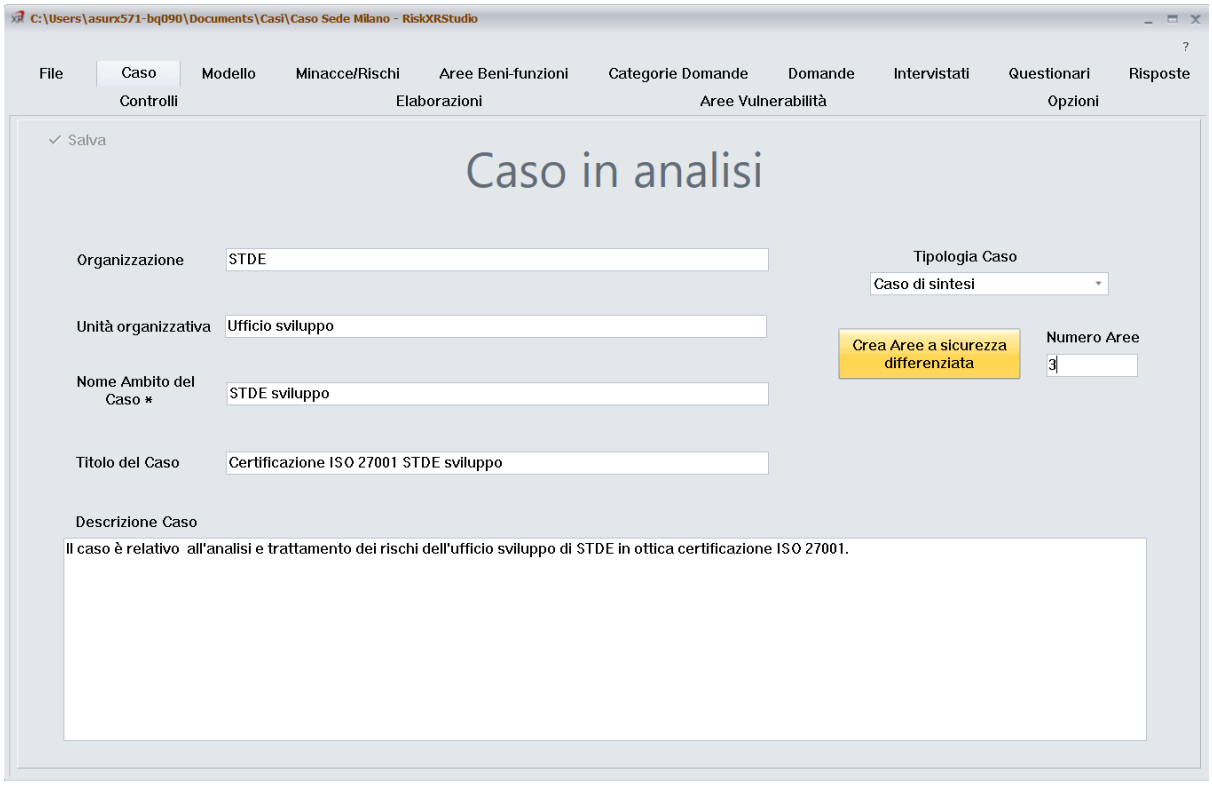
5. Creare una **Griglia di importazione risposte** con la lista delle **Interviste/Intervistati** e le **Aree a sicurezza differenziata**, indicando con una "**X**" tutte le interviste le cui risposte sono da importare, perché pertinenti, per ogni specifica **AREA**. Di seguito una griglia esemplificativa.

GRIGLIA DELLE RISPOSTE	Aree a sicurezza differenziata	001 ROMA	002 MILANO	003 CED FIUMICINO
Interviste/ questionari				
Gruppo server Windows MI - Neri			X	
Gruppo server Linux MI - Rossi			X	
APP Gestione personale MI - Verdi			X	
Oracle DB Personale MI - Viola			X	
Gruppo server Windows RM - Gialli		X		
Gruppo server Linux RM - Rossi		X		
APP Gestione personale RM - Verdi		X		
Oracle DB Personale RM - Viola		X		
Dominio NET 1 - Pinco		X		X
Dominio Net 2 - Laquiti			X	X

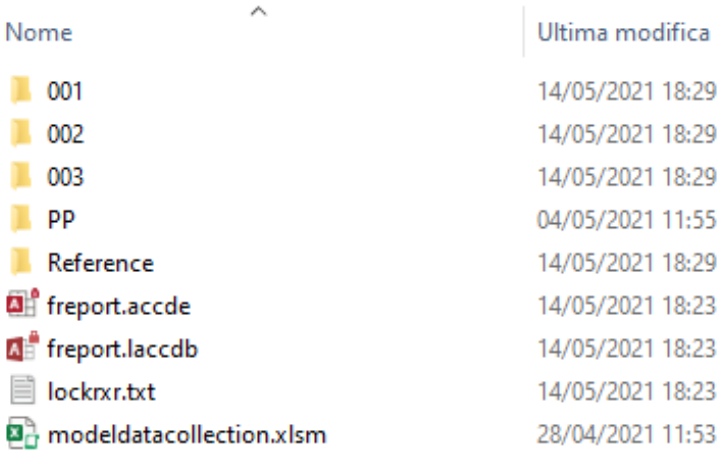
6. Generare i **questionari** per ciascuna **intervista/intervistato** della griglia. Alcuni questionari possono anche essere uguali come serie di domande, ma saranno **diversi come risposte** perché riguardanti aree diverse con livelli di protezione diversi, perciò interviste che avranno **Nomi diversi**. Si possono avere più **Questionari/Interviste** (Pagina Intervistati) per una stessa persona relativamente a asset o aspetti diversi.

7. Importare tutte le risposte nel **Caso di sintesi**.

8. Andare alla pagina "Caso" e apparirà un campo in cui mettere il numero di Aree a sicurezza differenziata, ad esempio "3". Premendo il tasto "**Crea Aree a sicurezza differenziata**" verranno create automaticamente 3 directory con Casi per le aree a sicurezza differenziata, copie del Caso di sintesi, nella directory del Caso di sintesi con i Nomi: **001, 002 e 003**.



Nella figura seguente si vedono le directory dei Casi relativi alle Aree differenziate da andare ad aprire ed elaborare con il comando **Apri** del menu File di RiskXRStudio.



9. Aperti uno per volta i **Casi creati**, effettuare le seguenti azioni:
   a. Eliminare tutte le risposte con il Tasto relativo.
   b. Importare le risposte selezionando "**solo**" le risposte pertinenti ad una specifica Area o comuni (vedere la griglia delle risposte).

c. Importare le risposte per ciascuna "Area a sicurezza differenziata" nei relativi Casi.

d. Occorre verificare che **OGNI AREA DI VULNERABILITA', SE NON DESELEZIONATA, ABBIA ALMENO UNA RISPOSTA** (vedere il "Grafico della Media delle risposte" per Area di vulnerabilità, se ha **barre a "0** nel "**Sommario dell'Analisi"** del Caso di ogni Area a sicurezza differenziata). Infatti se un'area di vulnerabilità non è Rilevante per l'analisi deve essere deselezionata e non sarà considerata. Se invece è presente e non ci sono risposte "**non si ha evidenza della presenza di contromisure"** e perciò si avrà come se si fosse risposto "0" a tutte le domande dell'area, ottenendo vulnerabilità massima per quell'area.

e. Lanciare le elaborazioni per quell'Area.

10. Completate le elaborazioni per tutte le Aree a sicurezza differenziata, poi aprire di nuovo il Caso di sintesi e **lanciare le elaborazioni.** Il **Profilo di protezione XR di ciascuna Area** è stato già riportato nel **Caso sintesi** automaticamente da parte dello strumento.

11. Visionare **i risultati nel Caso di sintesi** che si basano su una valutazione specifica per ciascuna Area e dunque particolarmente accurata ed efficace.

Nei **"Casi" delle Aree a sicurezza differenziata** interessa ottenere i report e le sezioni del Sommario solo fino alla valutazione dell'**IRI** (vulnerabilità/mancanza di protezione) per il Profilo di sicurezza XR in quanto **i rischi reali sono valutati nel Caso di sintesi**.

2.9 COME COPIARE DEGLI ASSET DA FONTI ESTERNE

In Modeldatacollection si copia da fonti esterne Excel o Database usando Copia e Incolla speciale "valori". Se dopo aver scelto "Incolla speciale" non viene presentata la voce "Valori" necessario per una corretta copia, allora seguire la seguente procedura.

1. Creare un "nuovo foglio di lavoro" scegliendo la voce "Inserisci" e "Foglio di lavoro".

2. Fare Copia dei dati da trasferire dalla fonte esterna in tale foglio con "Incolla" normale.

3. Copiare i dati in tale foglio con "Copia"

4. Andare nel foglio "Beni" e selezionare "Incolla speciale" e "Valori", del menu Modifica, che ora sicuramente apparirà.

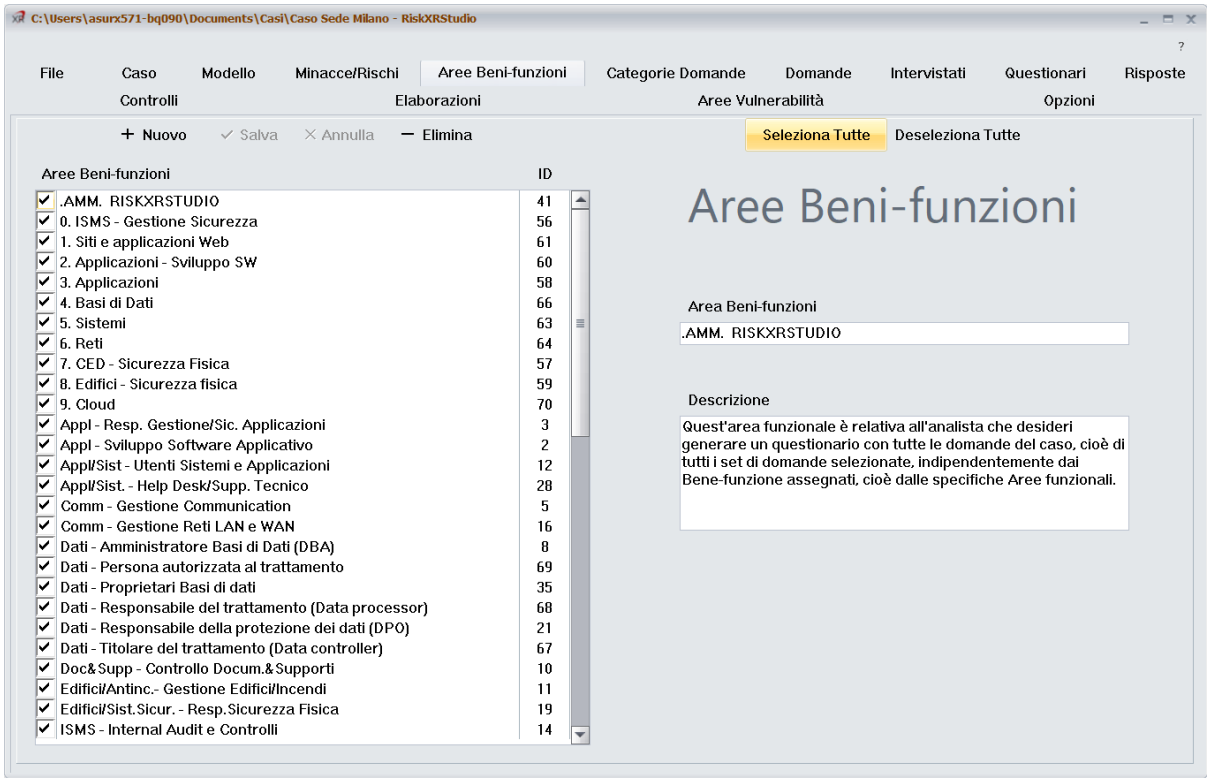
5. Eliminare il foglio creato solo per la copia dei dati, utilizzando "Elimina foglio" del menu Modifica.

2.10 SELEZIONARE LE AREE BENI-FUNZIONI

Definire il contesto nel quale si effettua la valutazione dei rischi implica individuare le "Aree Beni/Asset" che sono ad esso correlate e l'organizzazione con le sue Funzioni. L'individuazione di queste aree permette di selezionare i controlli di sicurezza e corrispondentemente le domande più appropriate per una efficace e completa valutazione del "livello di protezione" esistente.

Questa lista di selezione di Aree beni-funzioni costituisce un "Filtro" tramite il quale inserire nel "Questionario di valutazione" di un asset o asset/funzione le Domande ad esso appropriate con delle semplici selezioni.

Deselezionando qui le aree non pertinenti, le renderemo non selezionabili quando si "Creeranno i Questionari" di valutazione per gli Intervistati.



NOTA: La "non deselezione" di alcuna Area non comporta comunque nessun elemento negativo al Risk Assessment, semplicemente nelle scelte successive si troverà la lista di tutte le possibili Aree. Questo può anche essere una modalità rapida di gestire questo passo, non influisce sui risultati.

L'Area ".Amm. RISKXRSTUDIO" include nel questionario tutte le domande selezionate nella pagina "Categorie di domande".

Le Aree dalla 0 alla 9 permettono di includere le domande in base alla tipologia di Asset principalmente.

Le successive aree costituiscono una "lista di Aree dettagliata beni-funzioni" che permettono di includere domande in modo più accurato in base alle funzioni. È possibile anche selezionare queste ultime con le precedenti, lo strumento sceglie le domande in modo univoco per ciascun questionario/intervista.

Verificare la completa copertura delle Aree di vulnerabilità da parte delle domande. In questo può essere di aiuto il Report delle vulnerabilità al tab "Report".

Le Classi Beni-Funzione sono "elementari" nel senso che vi sarà la possibilità di aggregarle per predisporre un "**questionario personalizzato per ogni intervistato**" in base alle sue funzioni e alle sue responsabilità sui Beni.

Con le funzioni indicate con "**+ e –"** delle **Aree Beni-Funzioni**" è possibile "creare" e "eliminare" aree beni-funzione e predisporre una struttura personalizzata di Aree diversa **orientata all'organizzazione specifica**.

Ad esempio, si può inserire un'area per ciascuna intervista/intervistato selezionando in maniera specifica le domande pertinenti, rinunciando al sistema dei gruppi per funzione e asset, ma avendo un controllo estremamente preciso delle domande assegnate.

2.11 EFFETTUARE L'ANALISI DELLE MINACCE

L'Analisi delle minacce è uno dei passi fondamentali per la valutazione del rischio in un ambito sotto analisi. L'attività viene svolta tramite una apposita riunione a cui vengono fatte partecipare tutte le persone che direttamente o indirettamente possono fornire informazioni su eventi rischiosi avvenuti nell'ambito considerato e che operano nei vari settori interessati. Un approfondimento dei dati emersi sarà poi effettuato, insieme a dati locali ottenuti da varie fonti, per definire i valori definitivi

RiskXRStudio™ 2021 presenta una lista di Minacce su cui si acquisirà dai presenti informazioni sulla possibilità che tali minacce si concretizzino e con quale probabilità.

RiskXRStudio™ 2021 fornisce statistiche standard su cui basarsi. Questo è molto importante, perché le persone normalmente hanno difficoltà a dare dei valori, ma gli è molto più facile dare dei giudizi di eccesso o difetto a valori che gli vengano proposti. Se i giudizi provengono da varie persone è possibile effettuare una valutazione statistica iterativa.

E' possibile cioè utilizzare anche tecniche come il metodo Delfi o simili, se ritenuto il caso.

Le statistiche sono fondamentali perché orientano su qual è la probabilità con cui può avvenire un certo evento dannoso, nel contempo la loro precisione nei valori oltre un certo limite perde di rilevanza in quanto essendo una stima aiuta noi a cercare valori mediati non puntuali.

Non si cerca il valore puntuale di quante volte accadrà il prossimo anno per l'organizzazione sotto analisi, non è possibile saperlo, perché i valori rientrano in un intervallo particolarmente ampio, ma il valore più probabile in base allo scenario di rischio per un certo numero di organizzazioni che hanno una situazione simile al nostro. Di qui la rilevanza delle statistiche, ma non oltre un certo limite di precisione, che diventa irrilevante.

Le minacce non pertinenti, non possibili o irrilevanti potranno essere deselezionate dall'analisi nella lista che segue.

La deselezione delle minacce essendo esse indipendenti nella valutazione può essere fatta anche a posteriori, prima comunque di emettere i report finali.

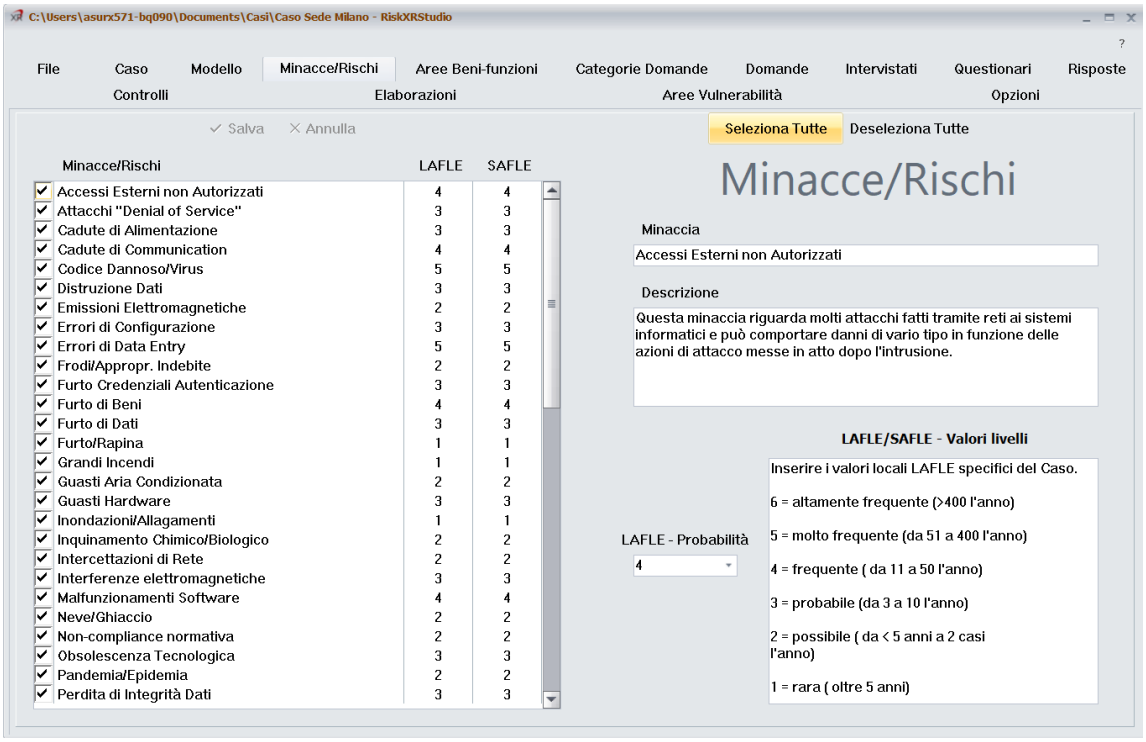
La deselezione è definitiva per un'analisi, una minaccia deselezionata elimina i suoi scenari di rischio e non può dunque essere rivalutata in quell'analisi. Ragione di più per eventualmente rimandare operativamente la deselezione.

Il non deselezionare le minacce "che non sono possibili" o irrilevanti è un errore nei dati di input forniti allo strumento, in quanto lo strumento in tal caso esclude che si possa essere in tale situazione. Lo strumento segnala comunque situazioni di incongruenza, ad esempio una minaccia da valutare che non abbia Beni su cui provocare danno (vedi Elaborazione). L'analista però può continuare comunque il processo di valutazione se vuole.

Ora è possibile inserire la "**Probabilità** delle minacce". Anche questa tipologia di parametri viene valutata durante la riunione relativa all'**Analisi delle Minacce**.

RiskXRStudio™ 2021 ha già al suo interno dei "valori standard" per la Probabilità (SAFLE – Standard Annual Frequency Level Estimate) delle Minacce derivati da ricerche statistiche ricavati da fonti diverse.

Sarà compito del responsabile del Risk Assessment, insieme alle persone in grado nell'organizzazione di fornire una indicazione in merito, di raffinare i valori di probabilità in base alla situazione specifica del Caso analizzato (LAFLE – Local Annual Frequency Level Estimate).



I valori di LAFLE da inserire sono da 1 a 6 secondo la scala posta sulla destra.

Per l'inserimento selezionare la Minaccia da cambiare e inserire il valore nell'apposito campo.

2.12 SELEZIONARE GLI STANDARD E I SET DI DOMANDE

Per acquisire le informazioni dell'ambito sotto analisi che consentano di ottenere un efficace ed esaustivo mezzo di valutazione con il minimo di domande è necessaria una impostazione metodologica e operativa strutturata.

I principi su cui si basa tale modalità operativa sono i seguenti:

1. In base ai beni presenti nell'ambito sotto analisi vengono selezionati i set di domande relativi agli **Standard di sicurezza** a cui desideriamo essere conformi e i set di domande derivati dall'esperienza di esperti, in grado di valutare la realtà dell'ambito sotto analisi con un modello di riferimento ritenuto avere un livello di sicurezza ottimale.

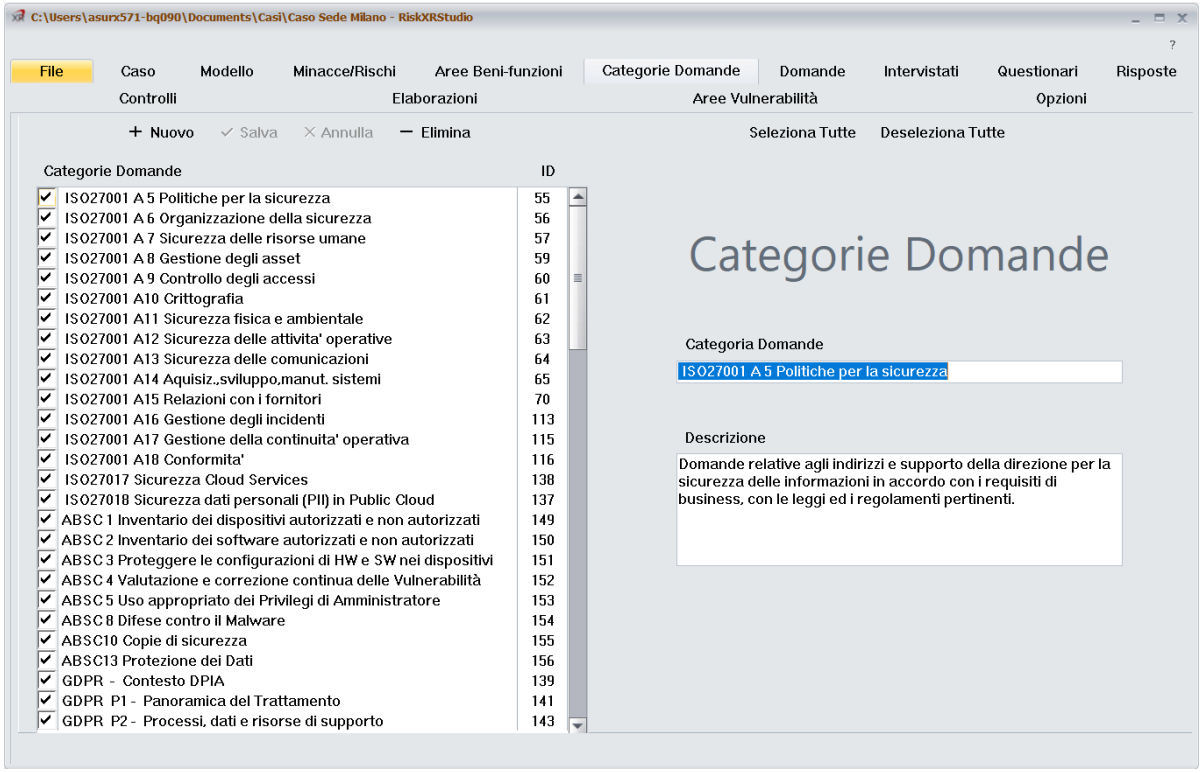
2. Il modello è costituito da standard di controllo la cui non attuazione genera un elemento di vulnerabilità per l'ambito sotto analisi.

3. Ogni domanda è da rivolgere solo alle persone pertinenti, cioè aventi elementi di conoscenza per l'aspetto sotto analisi.

Vediamo come procedere dal punto di vista operativo.

- Selezionare il tab "Categorie Domande". Deselezionare poi i set di domande che ritenete non pertinenti per la vostra analisi, lasciando selezionati solo i questionari rilevanti per il vostro Caso. Poi confermare la scelta.

La funzione "Aggiungi/Edita domande" consente di aggiungere domande, modificare il testo delle domande, associare la domanda ad un'Area di vulnerabilità, ad una o più Aree funzionali, ecc.



Selezionare il tab "Domande".

È possibile:

- Deselezionare le singole domande dopo aver scelto la categoria di appartenenza nel Combo in alto oppure inserendo l'ID della domanda e premendo il tasto "Cerca ID".

- Modificare i testi delle domande o del Controllo standard o il Titolo

- Modificare l'AREA DI VULNERABILITA' di appartenenza della domanda.

- Modificare il peso della domanda da 1 a 10, in cui i valori da 8 a 10 indicano CONTROLLO CRITICO.

- Muovere la Domanda selezionata da una Categoria ad un'altra semplicemente selezionando la NUOVA CATEGORIA nel Combo di nome "Cambio Categoria Domanda".

- Aggiungere o togliere domande dalla categoria corrente tramite "+ e –"

Al termine delle modifiche premere sempre il tasto di spunta Salvaper conferma o la X Annulla per eliminare le modifiche.

2.13 INSERIRE GLI "INTERVISTATI" E I QUESTIONARI RELATIVI

Le risposte ai questionari da parte di persone che svolgono le attività rilevanti per l'assessment sono la chiave dell'assessment stesso. La generazione dei questionari per essere efficace deve tenere conto:

1. della possibilità dell'intervistato di conoscere la materia specifica,
2. una chiara e strutturata modalità con cui dare la risposta
3. una rapida procedura per rispondere e per acquisire le risposte.

Dalle risposte si potrà effettuare la **valutazione del livello di protezione** in essere per gli asset/beni negli ambiti in analisi nei confronti delle varie minacce.

Il punto 1 è soddisfatto associando ad un intervistato delle "Funzioni svolte su Asset da lui gestiti (Aree Beni-Funzioni)".

Ogni intervistato può avere più funzioni e beni gestiti, si selezionerà tali Beni-funzioni e automaticamente lo strumento predisporrà un unico Questionario con le domande pertinenti a tale intervistato.

Il punto 2 è soddisfatto perché la modalità di risposta è unica, costituita da un numero da 0 a 10 con significati precisi posti nella form per rispondere.

Il punto 3 è soddisfatto perché si può rispondere tramite un applicativo locale, oppure via WEB con un apposito sito intranet.

I questionari possono essere GENERALI per il Caso o specifici di un asset o ambito **(Questionario Asset specific)** se gli si pone davanti due cifre es. "**31 Server AL**"e si pone ad esempio"**.31 Rossi - Server AL**" come nome "questionario", cioè stesse due cifre precedute da un "**punto**". Dopo le due cifre il nome può essere qualsiasi sono le due cifre che creano il legame tra questionario e asset/ambito.

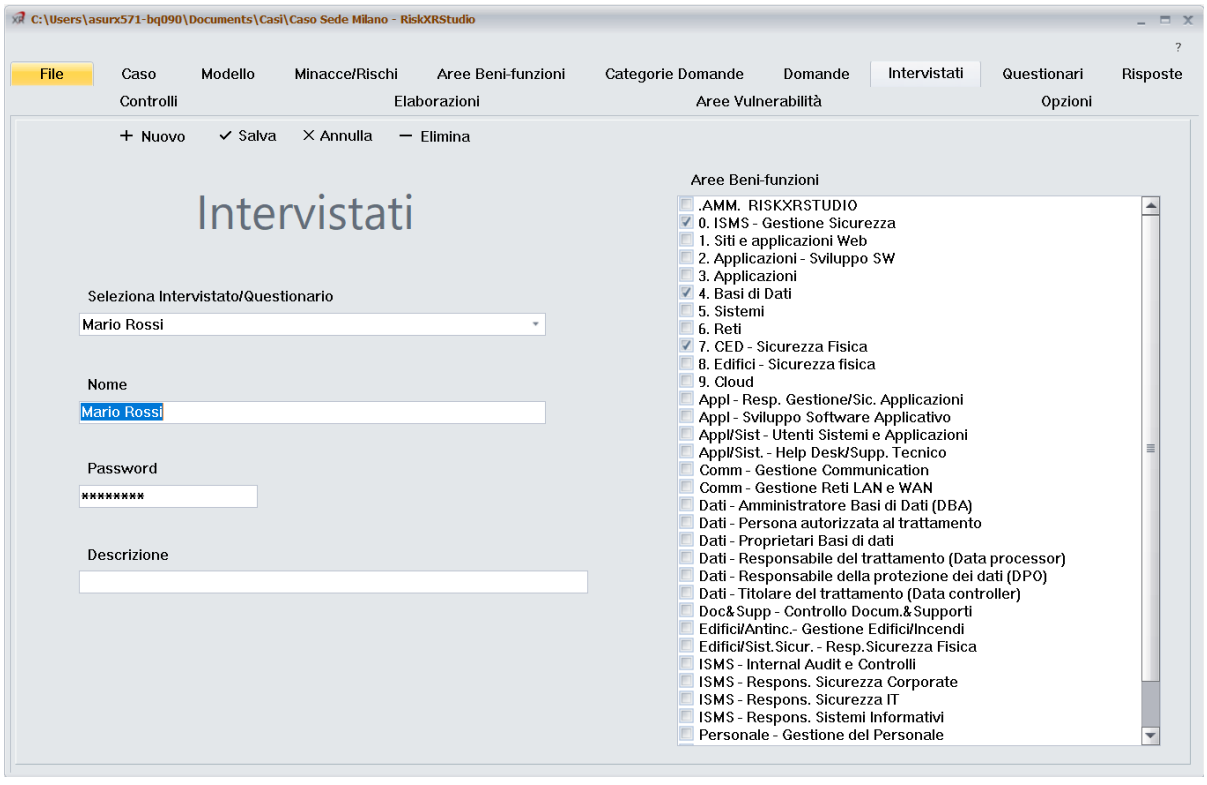
Come detto lo strumento è costituito da Questionari a cui devono rispondere intervistati che per la loro attività o responsabilità sono a conoscenza della situazione reale dei controlli proposti dalle varie domande.

Ogni domanda riguarda un controllo, cioè un criterio di protezione, la risposta è sempre il livello di attuazione del controllo da parte dell'organizzazione per il bene o i beni correlati. La risposta va da 0 a 10, con 10 completa attuazione e 0 nessuna attuazione del criterio. I valori 8,9 e 10 sono ritenuti conformi, mentre i valori da 0 a 7 non conformi. Per rendere più efficace la rilevazione, ad ogni risposta è possibile associare un commento, in cui spiegare la ragione di eventuali valori di non conformità. Un intervistato può rispondere ad uno o più questionari visto che una persona può avere più ruoli o funzioni nell'organizzazione.

- Premendo il tab "Intervistati" sarà possibile inserire i nomi delle persone che risponderanno alle domande e gli asset e funzioni per cui rispondono. Ad esempio ".27 server HP45 - Costini" che indica un Questionario relativo ad un asset che inizia con 27 di cifra ed è un server di codice HP45. La persona che risponde si chiama Costini. Nessuno vieta di associare un questionario di codice 27 anche a due o tre asset, basta mettere il 27 davanti a ciascuno di loro.

- Premere "+" e Inserire un Nome "univoco" per identificare il bene e la persona a cui saranno rivolte le domande su tale bene o gruppo di beni con i criteri detti prima.

E' da notare che "Intervistato" deve essere inteso come "Intervista", infatti è possibile creare "Intervistati" del tipo: "Rossi-Server Windows" e "Rossi-Server Unix", che si riferiscono alla stessa persona che risponde, ma ad aspetti diversi. Saranno generati 2 questionari distinti per tali interviste. I 2 questionari potrebbero anche avere eventualmente le stesse domande, ma le risposte saranno diverse perché si riferiscono a due aspetti/gruppi asset diversi.



- Digitare una password (sarà usata come password di accesso per le risposte. Tra i criteri per la scelta della password essa deve contenere "*almeno un carattere alfabetico minuscolo, uno maiuscolo, uno numerico e avere una lunghezza di almeno 8 caratteri*"

- Selezionare una o più "Aree Beni-Funzioni" associate alla singola persona. Questo consentirà di fargli delle domande pertinenti con le funzioni svolte. Poi premere "√" Salva di conferma. Ripetere per tutte le persone.

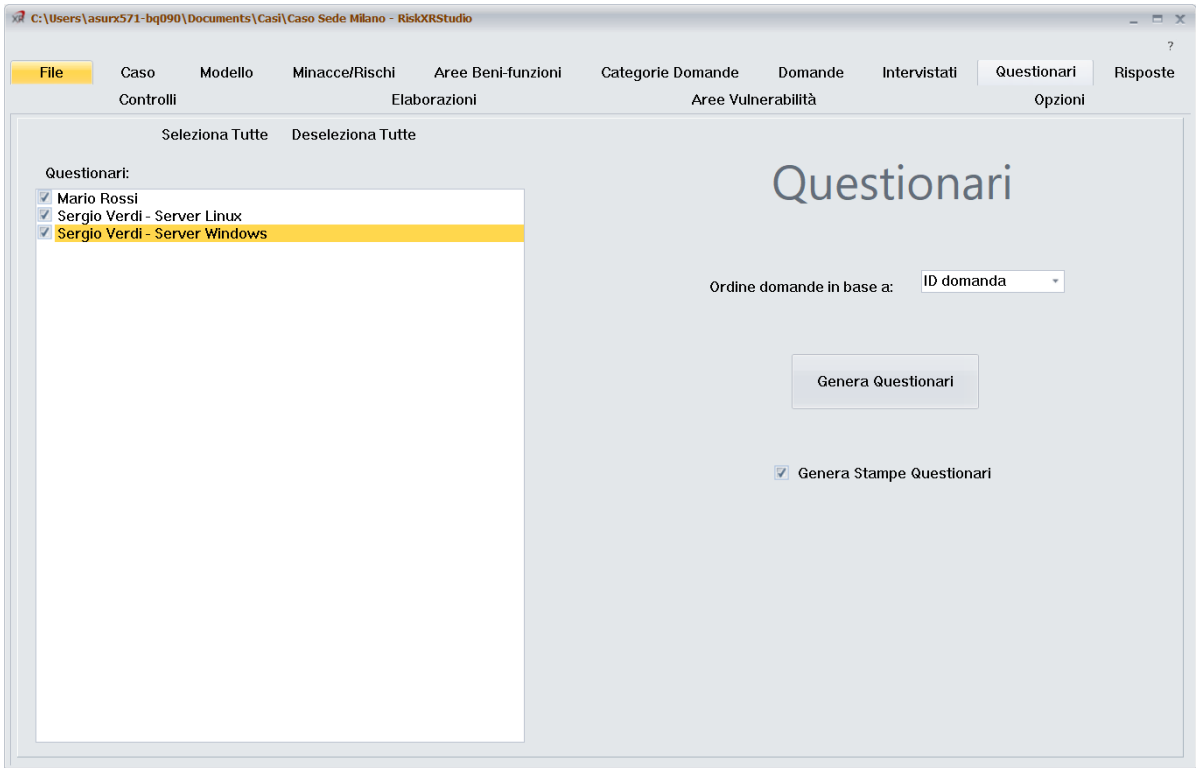
2.14 GENERARE GLI APPLICATIVI DI ACQUISIZIONE RISPOSTE

Per generare gli applicativi per l'acquisizione interattiva distribuita delle risposte ai questionari, aventi anche la funzione di controllo accesso protetta da password, occorre seguire la seguente procedura.

- Premere il tab "Questionari".

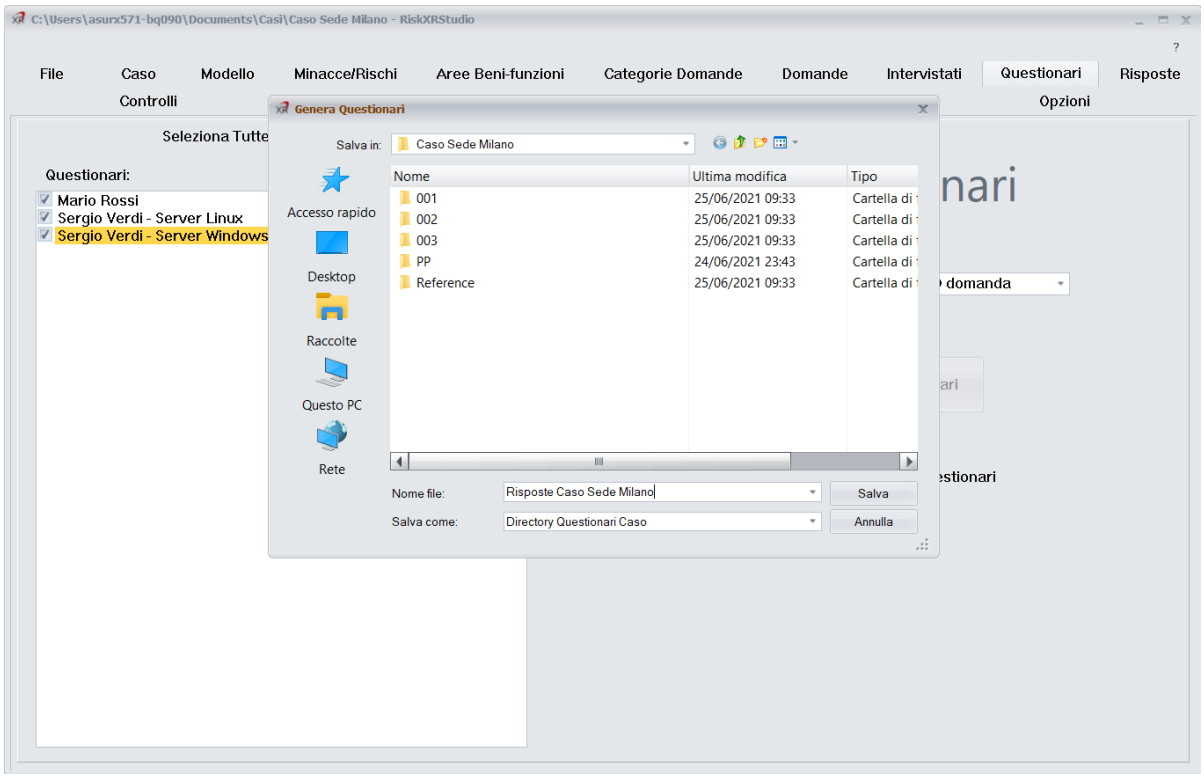
- Selezionare l'inervistato o gli intervistati per i quali si desidera preparare l'applicativo dall'elenco già inseriti in RiskXRStudio™ 2021, utilizzando eventualmente i tasti "Seleziona tutti i questionari" o "Deseleziona tutti i questionari".

- Selezionare il flag "Genera Stampe Questionari" se si intende utilizzare delle stampe cartacee dei questionari da sottoporre agli intervistati, oltre ad ottenerli in forma elettronica.



- Premere poi il tasto "Genera Questionari".

- Scegliere, quando richiesto, la Directory dove generare i questionari. Per usare le applicazioni **RiskXRAssess** (icona desktop) o **RXRASSESSAPP** (web) è obbligatoria la directory "**C:\web\rxrdata**", invece se si usa l'applicazione "**rxrassess.exe**" posta nella directory delle domande da RiskXRStudio™ 2021, allora può essere qualsiasi directory anche di rete o remota.



- Indicare il "**nome del Caso**" e premere per la generazione dei questionari attendendo il messaggio di completamento.

I questionari cartacei (Stampe) si troveranno nella directory del Caso, nella sottodirectory "Questionari" con nome ad esempio: **QuestionarioAnna.docx** per l'intervistato **Anna**.

2.15 RISPONDERE AI QUESTIONARI VIA WEB

Per rispondere ai questionari via web basta lanciare un browser ed aprire la pagina dove viene presentata la videata di login dell'applicazione "RXR Assess App" (/rxrassessapp) che fa parte di RiskXRStudio™ 2021.

Digitare negli appositi campi il "**Nome**" del Questionario-Intervistato a cui si desidera rispondere, la "**Password**" relativo per l'accesso ed il "**Nome del Caso**" di cui il questionario fa parte.

Inserendo i dati corretti apparirà la pagina che segue.

A sinistra è presente la "**Lista degli ID delle Domande**" che fanno parte del questionario personalizzato per l'intervistato. In alto, sempre a sinistra evidenziato si trova **l'ID della domanda corrente** presentata nella parte centrale insieme al corrispondente Standard di controllo.

Sulla destra è presente la "**Lista delle possibili Risposte**" da assegnare alla domanda corrente, con i relativi "significati".

Tra questi si può selezionare anche "**NON SO**" se non si è in grado di rispondere alla domanda, "**NON APPLICABILE**" se si ritiene che la domanda non sia applicabile allo specifico contesto.

In caso si risponda **NON APPLICABILE (NA)** la risposta non avrà alcuna influenza sulla valutazione dei valori di rischio, ma risulterà come semplice informazione. Invece se si risponde **NON SO** o non si risponde ad una domanda **NESSUNA RISPOSTA (NR)** lo strumento non avendo alcuna assicurazione che il criterio di sicurezza (controllo) sia attuato, nemmeno parzialmente, presupporrà la situazione peggiore ipotizzando risposta "**0**". Solo inserendo una risposta si potrà cambiare tale giudizio.

In basso nella parte centrale vi è la possibilità di inserire un **COMMENTO** che chiarisca le ragioni della risposta data. Fornire le ragioni di una risposta di attuazione non adeguata è fondamentale nella fase di trattamento dei rischi e nel rientro dalle vulnerabilità. Ne risulterà un Report efficace con indicazioni precise di analisi e risoluzione dei problemi.

Vi sono quattro tasti che consentono di gestire la fase delle risposte con facilità.

Premere "**Prossima**" per rispondere alla Domanda successiva, oppure "**Prossima da rispondere**" per rispondere alla Domanda successiva che non

ha avuto ancora una risposta. L'applicazione è in grado di ricercare tale domanda sia nella parte che segue sia ritornando alle domande precedenti di cui non si sia ancora fornito una risposta. Se non trova una domanda senza risposta segnala "Tutte le domande hanno avuto una risposta".

È possibile poi premendo il tasto "**Salva ed esci**" salvare tutte le risposte e i commenti uscendo poi dalla sessione di lavoro e ritornando al login.

È disponibile inoltre il tasto "**Salva**" che consente di salvare le risposte e i commenti inseriti senza uscire dalla sessione di lavoro.

Questi salvataggi intermedi sono importanti, perché evitano che se si lascia la sessione di lavoro (sempre premere Salva) per eventuali telefonate o interruzioni da parte di altre persone non si abbia lo scatto dei **time-out di sessione** con perdita delle risposte non salvate.

Le domande che hanno ricevuto già una risposta sono in campo **AZZURRO**, mentre le domande che devono ancora avere una risposta sono poste in campo **BIANCO**. L'identificazione delle risposte da rispondere perciò è immediata.

Si può andare ad una **domanda di numero ID specificato** selezionandone il numero di ID nella lista a sinistra nella parte sottolineata. Il corrispondente ID viene evidenziato in campo "**giallo**" in alto.

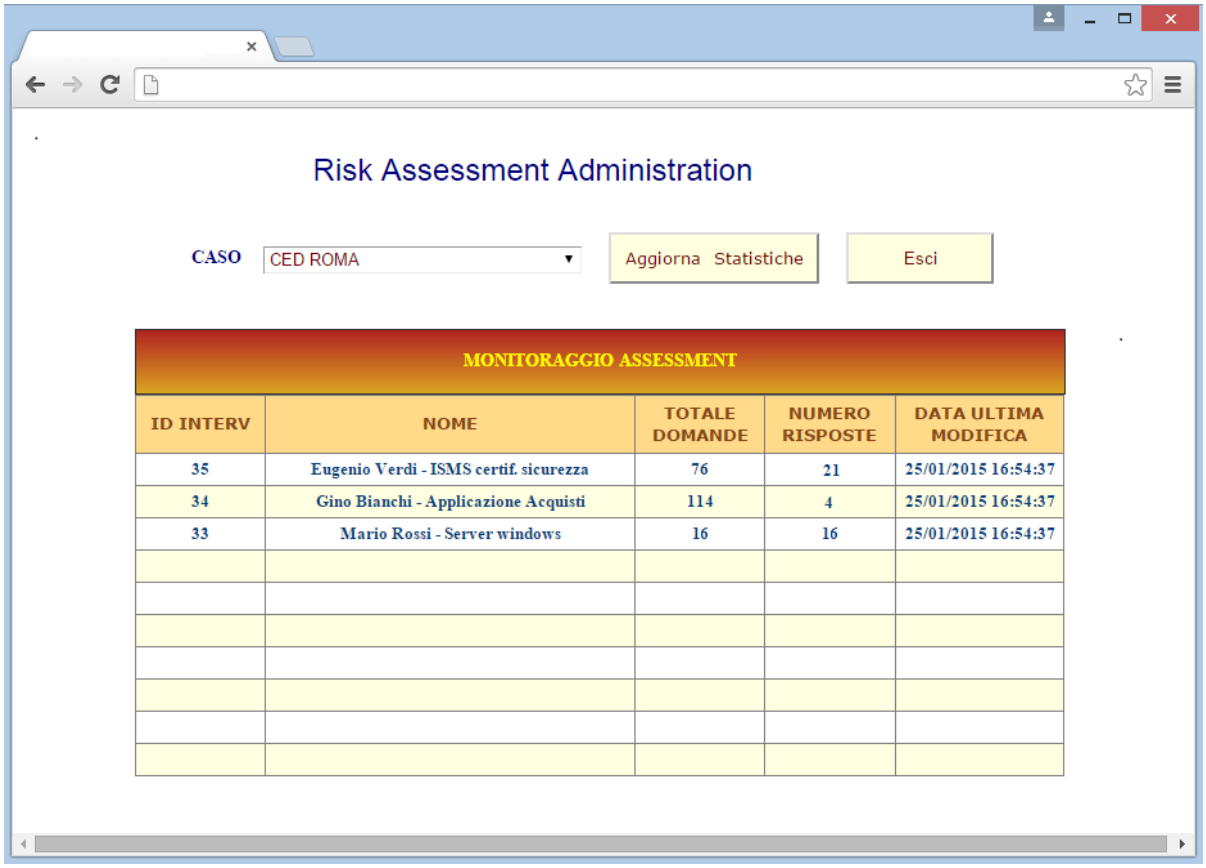
Come già indicato una volta terminata la fase di inserimento delle risposte premere "**Salva ed Esci**" per uscire dalla procedura.

2.16 AMMINISTRARE L' ASSESSMENT VIA WEB

Un assessment via Web presuppone che vi sia la possibilità di un monitoraggio in grado di mostrare l'andamento dell'assessment. Occorre cioè conoscere tramite una vista sintetica e immediata il numero di persone che hanno già completato i questionari proposti, le persone che lo devono ancora completare o iniziare tali questionari, quando è stata l'ultima volta che le persone hanno risposto, per evidenziare problemi e prospettive al fine di predisporre le azioni necessarie al completamento del processo.

Per monitorare l'assessment occorre effettuare il LOGIN con lo user-ID e password dell'Amministratore di RiskXRStudio™ 2021 al sito di /RXRAssessApp.

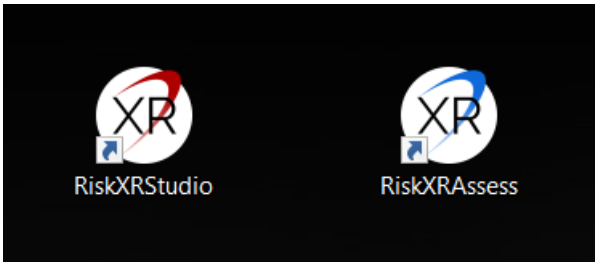
Per visionare le statistiche di monitoraggio selezionare il "**Caso**" a cui si è interessati e premere il tasto" **Aggiorna statistiche**".



A fine monitoraggio dei Casi utilizzare il tasto "**Esci**" per ritornare al login.

2.17 RISPONDERE AI QUESTIONARI IN LOCALE

Vi è la possibilità di rispondere ai questionari dopo la loro generazione anche in locale con l'applicazione **RiskXRAssess** lanciandola dall'icona sul desktop. La directory dove generare i file delle domande/risposte è come per le risposte da WEB c:\web\rxrdata.



Con tale applicazione si potrà rispondere alle domande con la stessa interfaccia del web prima vista. In più vi è la funzione "**Prossima domanda da rispondere automatica**". Tale opzione, se selezionata, consente di ottenere l'immediato

spostamento alla successiva domanda non ancora risposta in maniera automatica al click su una risposta per la domanda corrente.

Da considerare che quando è selezionata tale opzione ci si può muovere solo sulle "domande senza risposte NR".

Deselezionarla per potersi muovere su una qualsiasi domanda sia con risposta che senza risposta.

Oltre questa modalità è possibile rispondere ai questionari lanciando l'applicativo "**rxrassessx.exe**" presente in ogni directory dove vengono generati i questionari. Questo consente di inviare ad esempio via e-mail magari compressi con password, i questionari e la piccola applicazione rxrassessx.exe ad un intervistato che può poi ritornare il tutto con le risposte.

2.18 CONSIDERAZIONI SUI DATI STATISTICI DEL SOMMARIO DELL'ANALISI

Per capire i valori statistici che vengono indicati nel sommario dell'analisi occorre conoscere le modalità di valutazione dei dati effettuata.
Si hanno due tipi di risultati statistici:

1. Statistiche sulle RISPOSTE
2. Statistiche sui CONTROLLI

Ogni CONTROLLO può avere nessuna, una o più RISPOSTE. Se si ha una risposta valida per controllo le due statistiche coincidono.
Le risposte possono essere di una delle seguenti tipologie:

1. RISPOSTA VALIDA: se indica una risposta con valore da 0 a 10 (corrispondente a da 0% a 100% di attuazione).

2. RISPOSTA NON VALIDA: se non fornisce alcuna indicazione sulla conformità o meno del controllo (al massimo indica la pertinenza di tale controllo).

    a. NON RISPONDE: non viene data alcuna risposta, per considerare il controllo e valutarlo occorre cercare un interlocutore che sappia almeno fornire una risposta valida altrimenti viene considerata la condizione peggiore (0).

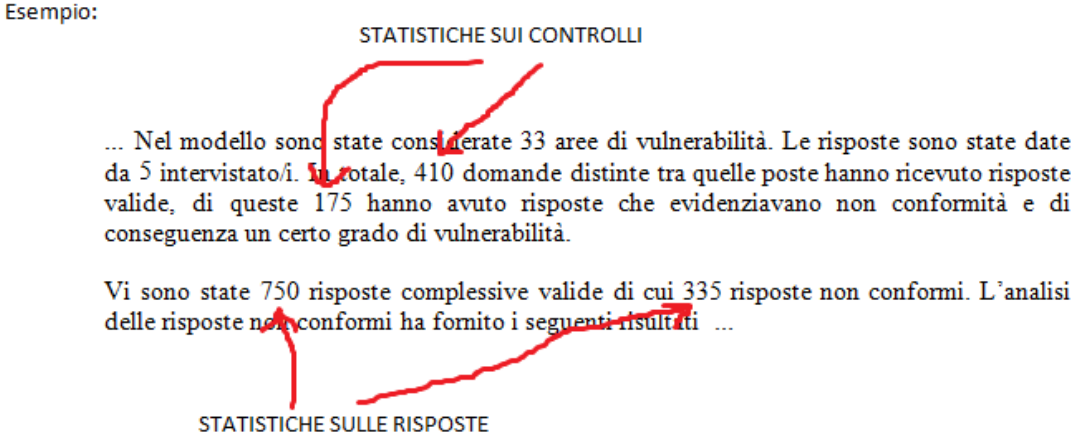
    b. NON APPLICABILE: il controllo è ritenuto "non pertinente", da valutare la fondatezza di quanto indicato durante "la fase di validazione degli input", in ottica SOA (Statement of Applicability). Per considerare il controllo e valutarlo occorre cercare un interlocutore che sappia fornire una risposta valida, in caso di

risposta NA sia il controllo che la risposta non vengono considerati.

c. NON SO: non si risponde alla domanda in oggetto in quanto non si è in grado di esprimere una valutazione sul Controllo per mancanza di sufficienti conoscenze in proposito. Per considerare il controllo occorre cercare un interlocutore che sappia fornire almeno una risposta valida, altrimenti viene considerato il caso peggiore (0).

Le STATISTICHE SUI CONTROLLI sono possibili solo se si ha per ciascun "controllo considerato" e ritenuto pertinente almeno una risposta valida. Altrimenti la statistica può non corrispondere.
Le statistiche si fanno sull'insieme delle RISPOSTE VALIDE, con indicazioni anche sul numero delle risposte NA, NON SO e NON RISPONDE. Il prodotto fornisce nel report finale statistiche "sia" sulle risposte "che" sui controlli.

Esempio:



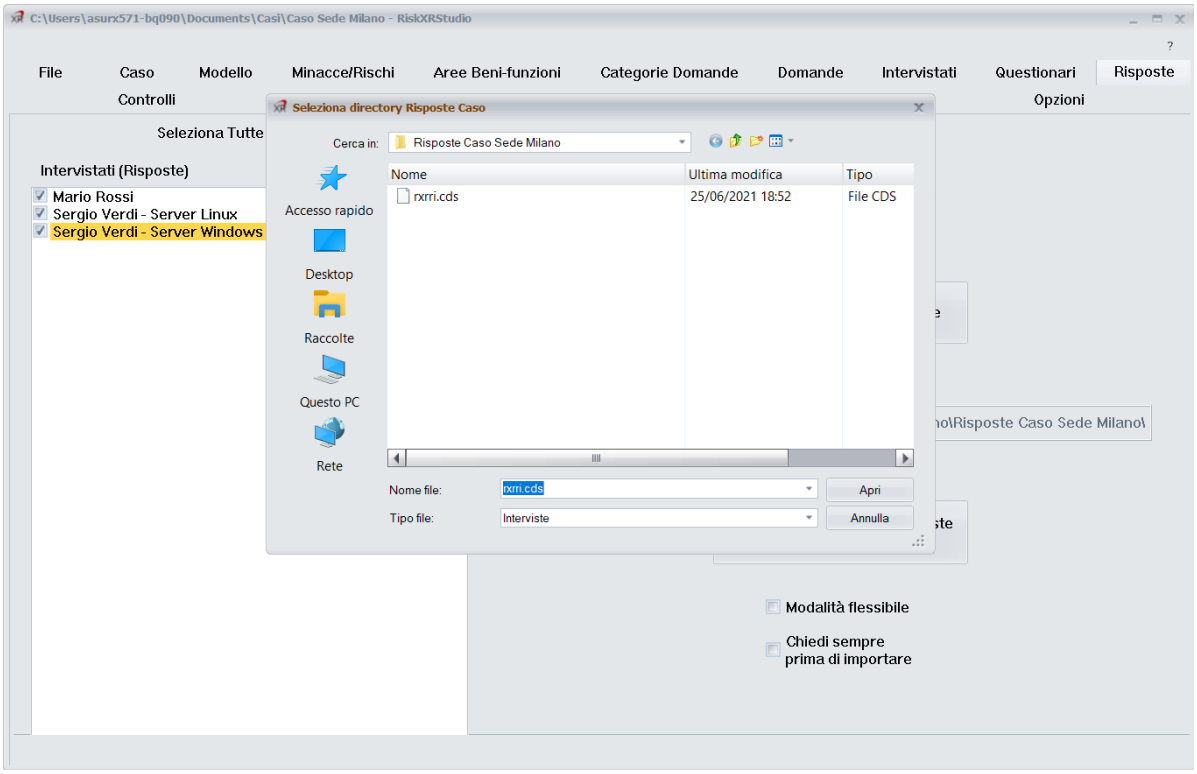
Le tabelle lavorano sulle RISPOSTE. Questo consente di effettuare statistiche significative anche con pochi controlli per Area di Vulnerabilità. Ad esempio, se si ha un caso limite con 1 domanda e 30 persone che rispondono è comunque una situazione che fornisce una situazione significativa con le statistiche sulle Risposte (30 dati), non altrettanto con la statistica sui controlli/domande (1 dato).

2.19 IMPORTARE LE RISPOSTE

L'import delle risposte fornisce i dati di base per l'analisi e la valutazione dei rischi, insieme ai valori del modello XR degli asset e alle opzioni specifiche scelte.

Tramite il tasto "**Seleziona Directory risposte**" è possibile ricercare la directory dove si trovano i file dei Questionari generati dallo strumento a cui gli intervistati hanno già fornito delle risposte.

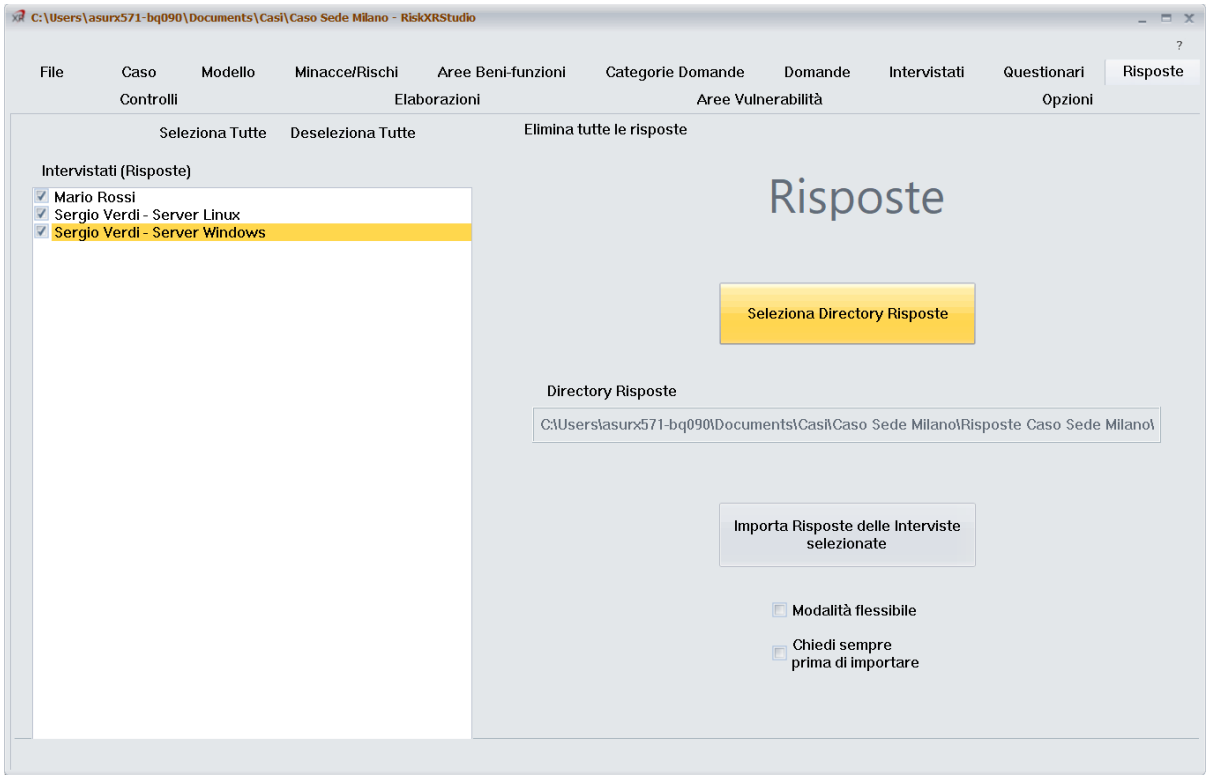
In tale directory si troverà sempre un file di nome "rxrri.cds", selezionarlo e aprirlo. Verrà mostrata alla sinistra **la lista degli intervistati** di cui sono disponibili le risposte.



Selezionare gli intervistati/interviste di cui si desidera importare le risposte e premere il tasto "**Importa Risposte delle Interviste selezionate**".

Esistono due modalità per l'importazione "**Modalità standard**" e "**Modalità flessibile**". Utilizzando la "**Modalità standard**", che fornisce la massima sicurezza, quando si importa viene verificato che le risposte **riguardino un intervistato già definito** nella lista degli intervistati del Caso. Se l'intervistato invece non è conosciuto allora la cosa viene segnalata, inoltre si chiede se passare alla "**Modalità flessibile**". Se si risponde "OK" allora lo strumento consente di **creare il nuovo intervistato mancante** con una nuova password.

La "Modalità flessibile" può essere selezionata manualmente anche prima della fase di importazione delle domande se si vuole.



Se gli intervistati/interviste sono già **presenti nel Caso** le loro risposte saranno importate tutte in maniera **silente**. Altrimenti, come già detto, verrà chiesto se settare la "**Modalità flessibile"**.

Se il set di risposte di un intervistato/intervista **è già stato importato**, allora lo strumento chiede se si vuole **"sostituire"** il set di risposte o se si vuole assegnare ad un nuovo od altro intervistato settando la modalità flessibile.

Selezionando il flag "**Chiedi sempre prima di importare**" si apre alla possibilità di **scegliere il NOME dell'intervistato durante la fase di import per tutte le risposte** e non solo nei casi di impossibilità di individuazione dell'intervistato o di risposte già importate.

Inserendo un numero specifico identificativo di un **asset/ambito** in testa al **NOME di un intervistato/intervista** (questionario) si potranno "associare" le risposte relative a tale ASSET o AMBITO.

Con le funzioni "**Deseleziona tutte le interviste**" e "**Seleziona tutte le interviste**" o tramite una selezione puntuale di esse, potremo indicare di quali intervistati vogliamo importare le risposte.

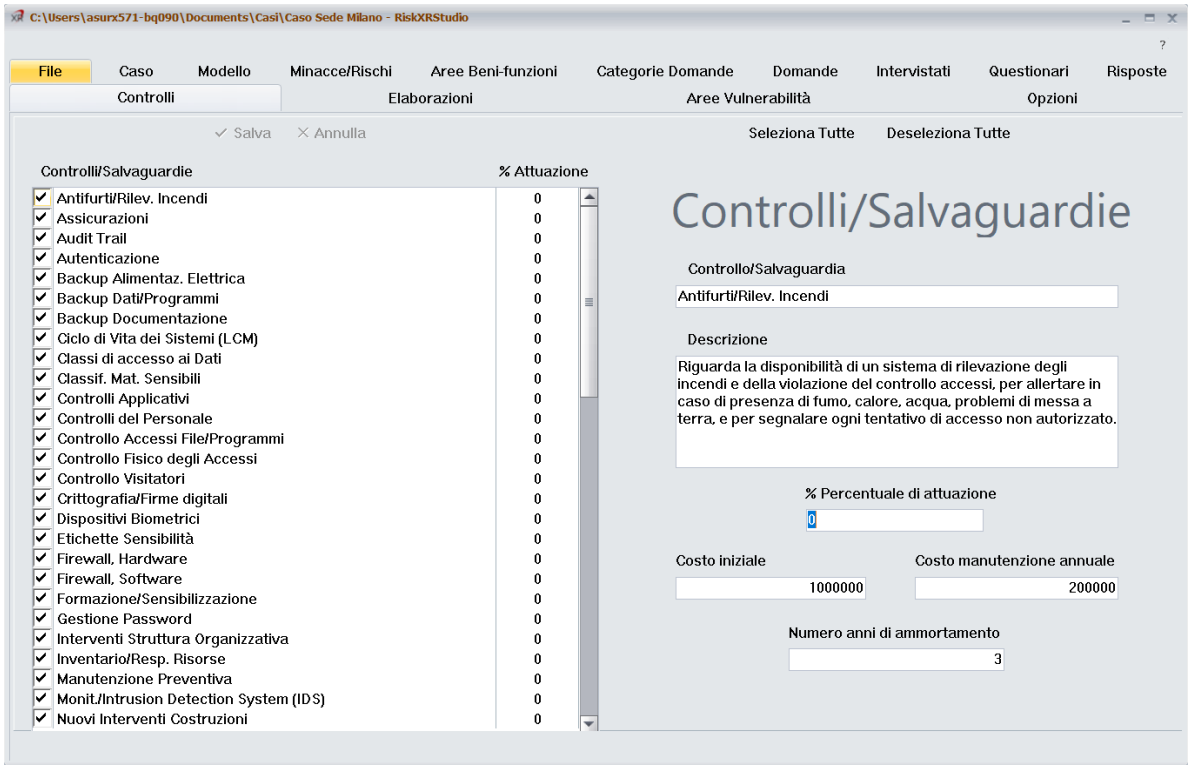
Nel caso si desiderasse cambiare le risposte importate basta premere il tasto "**Elimina tutte le risposte**" ed iniziare di nuovo la procedura di selezione.

Evitare di inserire file spuri nella directory delle risposte, è conveniente porci solo i file generati da RiskXRStudio.

Si ricordi che **i nomi degli intervistati devono essere univoci** prima del lancio dell'elaborazione dati altrimenti non si riesce a distinguerli nei report. Per flessibilità però nella fase di preparazione la non univocità non viene rilevata e bloccata dallo strumento. Nessuna necessità di univocità per le password.

2.20 LISTA CONTROLLI / SALVAGUARDIE DA VALUTARE

Nella pagina dei Controlli/Salvaguardie è possibile vedere l'elenco delle contromisure che è possibile utilizzare per la riduzione del rischio ed inserire la percentuale di attuazione attuale di tali controlli.



Tale informazione consente allo strumento di escludere dalle valutazioni per la riduzione del rischio quei controlli che hanno già avuto una implementazione al 100%. Tali controlli, infatti, non potendo essere ulteriormente migliorati non possono generare alcuna riduzione di rischio.

I risultati dell'analisi delle possibili % di riduzione di rischio ottenibili completando o introducendo i vari controlli/Salvaguardie viene esposto nella sezione relativa al trattamento dei rischi.

Sulla sinistra è possibile vedere come si possano deselezionare i controlli che riteniamo non rilevanti per la nostra analisi delle salvaguardie. I controlli deselezionati non saranno inseriti e valutati per la riduzione del rischio cumulativo e l'analisi costi/benefici.

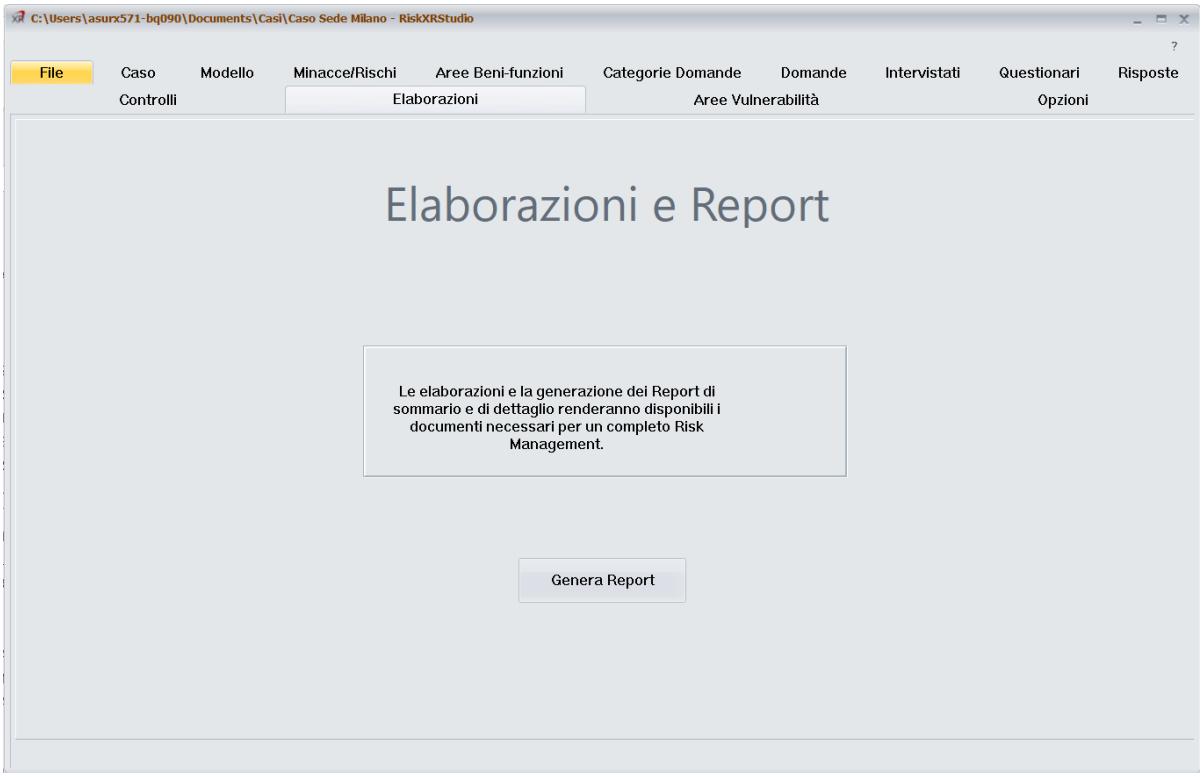
I seguenti parametri monetari consentono, se desiderato, di effettuare un'analisi Costi/Benefici quantitativa prendendo come input ulteriore una stima della riduzione di rischio ottenibile dall'introduzione singola o cumulativa di controlli/salvaguardie. I parametri da fornire in euro sono: costo iniziale, costo manutenzione annuale e numero di anni di ammortamento.

3. ELABORARE I DATI E GENERARE I REPORT DELL'ANALISI

Selezionando il tab "Elaborazioni" è possibile ottenere la generazione dei Report sia di sommario che di dettaglio.

Occorre ricordarsi che per la generazione dei report sono utilizzati anche programmi VBA (Visual Basic for Application). Si **deve** perciò porre il path **Documents\Casi, o altro percorso dei Casi utilizzato**, come **PERCORSO ATTENDIBILE** nelle Opzioni di **Excel e di Access** (Andare al menù "File", Opzioni, Centro Protezione, Impostazioni Centro protezione, Percorsi Attendibili e "aggiungere" tale percorso, selezionando anche il flag per le sottodirectory).

Per la generazione dei report, premere il TAB OPZIONI, scegliere il "Livello Target di Rischio" tra Livello 1 a Livello 3, con il Livello 2 come valore di default, e premere il tasto presente nella videata delle elaborazioni. Si otterranno così i Report dell'analisi. Il Piano Generale di Rientro, i Piani di Rientro specifici e i Piani di Sicurezza si potranno generare solo dopo l'esecuzione delle elaborazioni di base. Stessa cosa per generare il file Excel (GraficiExcel.xlsx) che contiene i grafici dei risultati dell'analisi in tale formato con le tabelle collegate.



La scheda "Report", che si renderà visibile dopo la generazione, permetterà di accedere a tutti i report disponibili, compreso il "Sommario dell'Analisi".

3.1 ACCEDERE AI REPORT DELL'ANALISI

Dopo la generazione dei report si avranno a disposizione i documenti finali dell'analisi in Word e, per i grafici, se desiderato, anche in formato Excel per eventuali personalizzazioni e successive analisi.

3.2 ESEMPI DI REPORT DELL'ANALISI

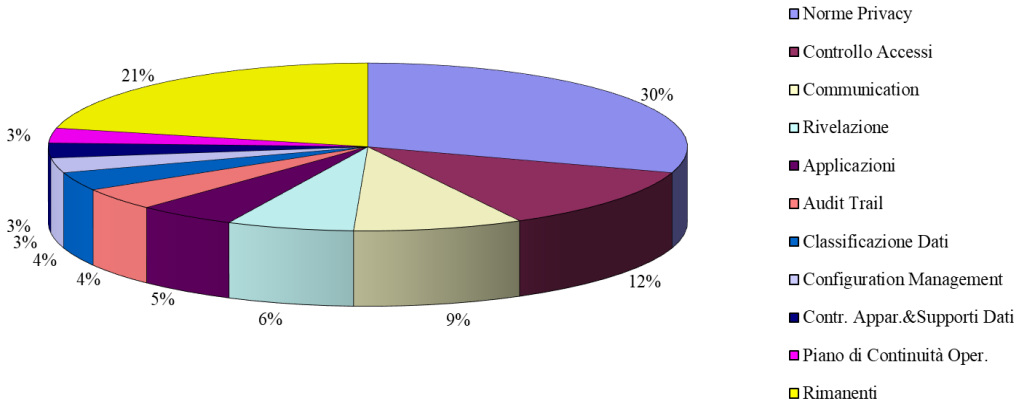
In questo paragrafo verranno mostrati degli esempi dei vari report forniti con lo strumento.

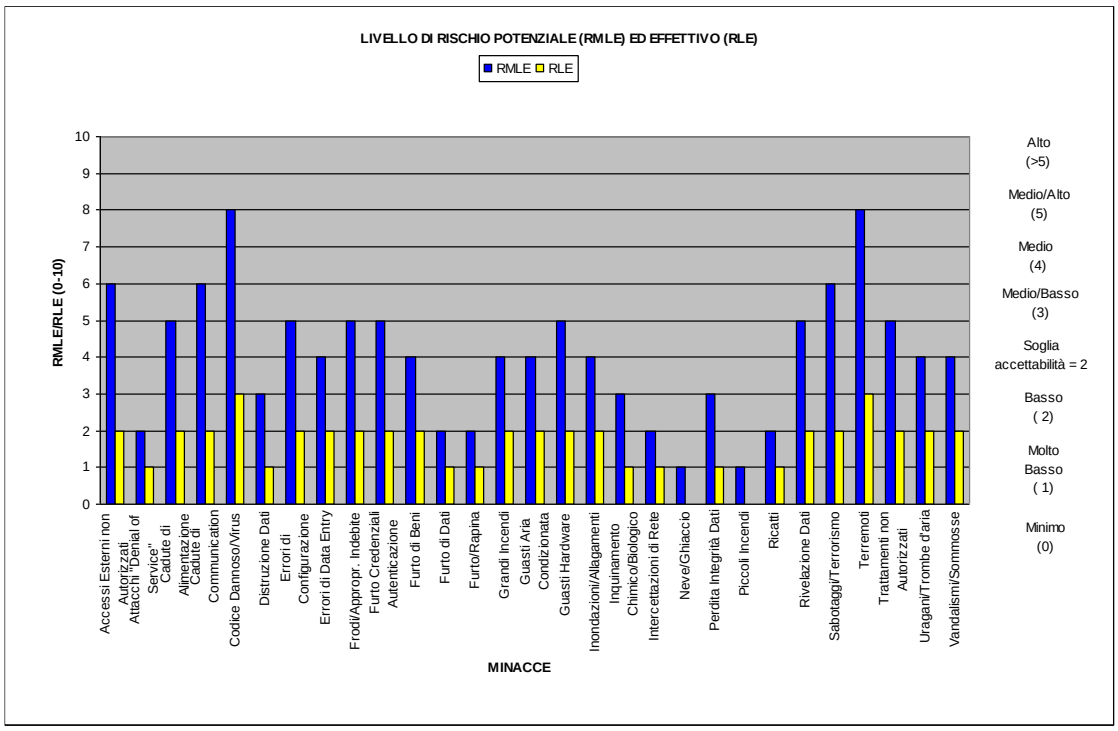
3.2.1 GRAFICI NEI REPORT

Il Sommario dell'analisi consente di fornire alla Direzione un documento sintetico che contiene tutti i punti chiave delle attività di Risk Assessment e di trattamento dei rischi.

Nel seguito sono mostrati alcuni grafici di tale report: Distribuzione delle risposte non conformi e Grafico di confronto del Rischio Potenziale e Rischio Effettivo.

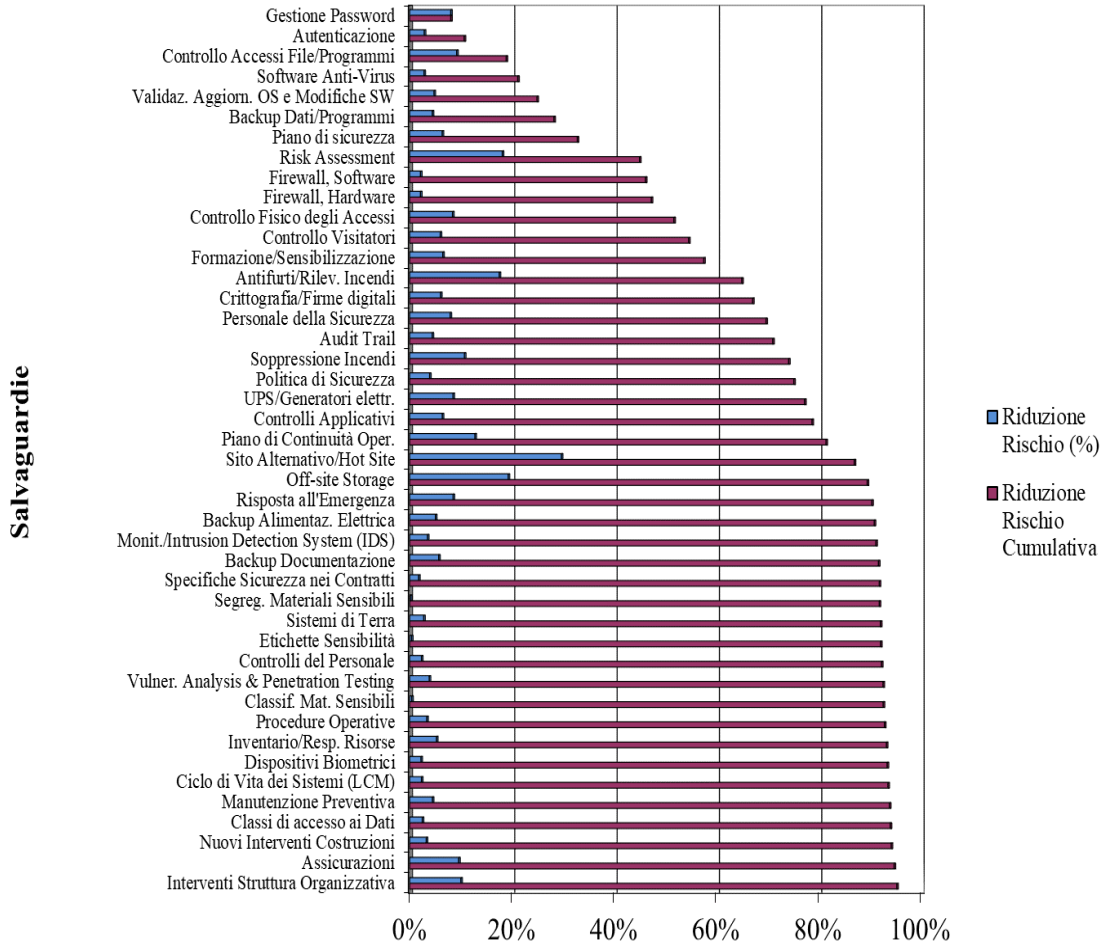
Distribuzione Risposte non conformi per area di Vulnerabilità





Il grafico che segue mostra le riduzioni di rischio percentuali sia per singolo controllo/salvaguardia che cumulativo, cioè presupponendo di attuare anche tutte le salvaguardie più in alto nel grafico.

GRAFICO DI RIDUZIONE DEI RISCHI



È possibile deselezionare i controlli/salvaguardie che si ritenga di non considerare nell'analisi cumulativa della riduzione dei rischi intervenendo nella pagina al tab "Controlli".

Se si ritiene che alcuni controlli/salvaguardie siano state attuate completamente e che dunque non vi è né necessità né volontà di intervenire su tali contromisure. Inserire in tal caso 100% nel campo della salvaguardia per porla come completamente attuata (al tab Controlli).

Questo genererà una riduzione del rischio pari a 0 nel grafico delle salvaguardie in corrispondenza di tale Controllo. Anche le barre del grafico della riduzione di rischio cumulativa terranno conto dell'informazione fornita.

Nella figura che segue è possibile notare come la barra blu della riduzione di rischio assoluta per la salvaguardia Audit trail sia nulla e che quindi il valore della riduzione di rischio cumulativo rimanga uguale a quella della precedente salvaguardia introdotta.

3.2.2 REPORT DI DETTAGLIO DELLE VULNERABILITA'

Questo report per ciascuna **Area di vulnerabilità** elenca i controlli relativi alle domande poste agli intervistati. Per ciascuna domanda sono presentate le risposte date ed eventuali Commenti.

REPORT DI DETTAGLIO VULNERABILITA'

Ambito di sicurezza dei controlli	Rif. Normativo	ID Controllo	Controllo	Peso	Questionario Intervistato	Conformità	Commento	ID Risposta
Alimentazione Elettrica	ALIMELETR - A.11.2.2 Infrastrutture di supporto	76	Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari.	9	Bianchi - CED Largo Arcibaldo	100		974
					Verdi - Sviluppo Applicazioni Operative	80		975
					Rossi - Server Windows	70		976

3.2.3 REPORT DI CONFORMITA' A NORME E STANDARD

Questo report per ciascuna Sezione di una Norma o Standard elenca i controlli relativi alle domande poste agli intervistati. Per ciascuna domanda sono presentate le risposte date ed eventuali Commenti.

REPORT DI CONFORMITA' A NORME E STANDARD

Sezioni della norma	Rif. Normativo	ID Controllo	Controllo	Peso	Questionario Intervistato	Conformità	Commento	ID Risposta
GDPR - Reg.UE 2016/679 C II Principi	A5.1a - Liceità, correttezza e trasparenza.	479	I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»).	8	002 Aldo Bianchi	90		219
	A5.1b - Finalità determinate, esplicite e legittime.Limitazioni.	480	I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità	8	002 Aldo Bianchi	90		220
	A5.1c - Minimizzazione dei dati.	481	I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»).	8	002 Aldo Bianchi	90		221
	A5.1d - Esattezza dei dati	482	I dati personali sono esatti e, se necessario, aggiornati.	8	002 Aldo Bianchi	90		222
	A5.1e - Limitazione della conservazione dei dati.	483	I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.	8	002 Aldo Bianchi	80		223
	A5.1f - Integrità e riservatezza dei dati personali.	484	I dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).	8	002 Aldo Bianchi	70		224
	A5.2 - Responsabilizzazione del titolare	485	Il titolare del trattamento è competente per il rispetto dei "Principi applicabili al trattamento di dati personali" e in	8	002 Aldo Bianchi	70		225

3.2.4 REPORT DI DETTAGLIO DELLE MINACCE

Il "Report di dettaglio delle Minacce" presenta i "risultati del Risk Assessment riguardanti le possibili minacce in dettaglio. In particolare consente di verificare quali "aree di vulnerabilità" influiscano sul rischio per ciascuna "minaccia", quale percentuale di contributo al rischio esse apportino nel contesto di tale minaccia e se è necessario o da valutare un eventuale intervento con ulteriori controlli in tali aree.

La tabella presentata mostra la relazione tra minacce e Aree di vulnerabilità, e quanto sia consistente la "mancanza di protezione (Impact Relative Index - IRI)" per ciascuna minaccia e per le aree di vulnerabilità pertinenti nel contesto di tale minaccia.

Il report di dettaglio delle minacce insieme a quello di dettaglio delle vulnerabilità, e alla tabella/Grafico delle "Priorità di intervento", nonché al grafico delle Riduzioni di rischio, costituisce il quadro della sicurezza su cui la direzione può individuare gli interventi da predisporre e pianificare.

REPORT DI DETTAGLIO DELLE MINACCE

MINACCE	ACCETTABILITA' RISCHIO	LIVELLO RISCHIO (RLE 0-10)	MANCANZA PROTEZIONE (IRI 0-100)	AREE VULNERABILITA' RILEVANTI	%IMPATTO VULN	MEDIA RISPOSTE (0-100)	CONFORMITA' (% Risposte>85)	INTERVENTO	RACCOMANDAZIONI
Accessi Esterni non Autorizzati	INTERVENIRE	8	74	Assegn. Responsab.	1,8%	34,0	18,5%	DA VALUTARE	Assegnare la responsabilità di tutti i beni dell'organizzazione e delle procedure da attuare per ottenere gli obiettivi prefissati.
				Controllo Accessi	19,2%	55,0	59,3%	NECESSARIO	Attuare completamente i criteri di gestione delle password, uso dei badge e smart card; della gestione dei diritti di accesso a file, programmi, sistemi e reti. Configurare correttamente i firewall e i router, nonché tutti gli apparati ed i meccanismi di accesso logico alle informazioni.
				Classificazione Dati	17,6%	12,0	3,8%	NECESSARIO	Sopperire alle carenze relative al processo di classificazione dei dati, verificando la completezza delle procedure definite e operando per la sensibilizzazione e attuazione da parte del personale.

3.2.5 REPORT XR DI VALUTAZIONE DEI RISCHI (VISTA MINACCE)

Questo Report consente di ottenere la Mappa XR dei Rischi relazionale per tutti i rischi delle MINACCE pertinenti per ogni asset o ambito del Modello.

Cliccando con "Ctrl" sul **numero di criticità** si salterà alla lista delle **"Descrizioni delle criticità"** specifiche di tale asset o ambito.

I livelli di rischio, per una più immediata interpretazione, sono associati a dei colori:

1. **Verde** per i livelli fino al "livello di soglia definito accettabile" per l'analisi, generalmente il livello 2;
2. **Giallo** fino al livello 5;
3. **Rosso** dal livello 6 fino al livello 10.

Per quanto riguarda invece la colonna Vuln/Host relativa al numero di vulnerabilità di gravità massima e il numero di Host, ottenuta nel caso dell'opzione VA (Vulnerability Assessment) selezionata, i colori utilizzati per la gravità delle vulnerabilità sono i seguenti:

1. **Giallo** - Bassa;
2. **Arancione** - Media
3. **Rosso** - Alta.
4. **Marrone** - Critica.

St De
Studio Dell'Agnello S.r.l.

REPORT XR DI VALUTAZIONE DEI RISCHI (VISTA MINACCE)

^ AMBITO PADRE	NOME BENE (Asset/Ambito)	CATEGORIA BENE	MINACCE	PROBABILITA'	Criticità	Rischio Effettivo (RLE)	R	I	D	P	U	Vul /Host	Rischio Potenziale (RMLE)	R	I	D	P	U
^Server GX8	Oracle DB 1	Basi di Dati	BENE		8	6	5	5	5	1	6	0	9	8	9	9	5	9
			Accessi Esterni non Autorizzati	frequente (da 11 a 50)		5	4	4	3	0	5		8	8	8	7	0	8
			Attacchi "Denial of Service"	probabile (da 3 a 10)		4	0	0	4	0	4		7	0	0	7	0	7
			Cadute di Alimentazione	probabile (da 3 a 10)		3	0	0	3	0	0		6	0	0	6	3	0
			Cadute di Communication	frequente (da 11 a 50)		3	0	0	3	0	3		7	0	0	7	2	7
			Codice Dannoso/Virus	molto frequente (da 51 a 400)		6	4	5	5	0	6		9	8	9	9	0	9
			Distruzione Dati	probabile (da 3 a 10)		5	0	4	5	0	4		7	0	6	7	0	6

-

3.2.6 REPORT XR DI VALUTAZIONE DEI RISCHI (VISTA ASSET)

La seconda mappa è la "**Report XR di Valutazione dei Rischi (Vista Asset)"** in essa vengono rappresentati cromaticamente i rischi derivati non solo dalle vulnerabilità degli specifici asset, ma anche quelli derivati da asset "esterni" da cui dipendono e sono supportati, modellati tramite relazioni del modello XR (catene di eventi, interazione tra sistemi).

Cliccando con "Ctrl" sul **numero di criticità** si salterà alla lista delle **"Descrizioni delle criticità"** specifiche di tale asset o ambito.

I livelli di rischio, per una più immediata interpretazione, sono associati a dei colori come nella mappa precedente:

1. **Verde** per i livelli fino al "livello di soglia definito accettabile" per l'analisi, generalmente il livello 2;
2. **Giallo** fino al livello 5;
3. **Rosso** dal livello 6 fino al livello 10.

Per quanto riguarda invece la colonna Vuln/Host relativa al numero di vulnerabilità di gravità massima e il numero di Host, ottenuta nel caso dell'opzione VA (Vulnerability Assessment) selezionata, i colori utilizzati per la gravità delle vulnerabilità sono i seguenti:

1. **Giallo** - Bassa;
2. **Arancione** - Media
3. **Rosso** - Alta.
4. **Marrone** - Critica.

.

St De
Studio Dell'Agnello S.r.l.

REPORT XR DI VALUTAZIONE DEI RISCHI (VISTA ASSET)

^ AMBITO PADRE	NOME BENE (Asset/Ambito)	CATEGORIA BENE	Criticità	Rischio Effettivo (RLE)	R	I	D	P	U	Vul/Host	Rischio Potenziale (RMLE)	R	I	D	P	U
	Trattamento offerte	Ambiti	0	5	4	4	5	5	0	0	8	6	8	8	7	0
^ 04 S.I A1 Communi cation CED Roma 1	CED Roma1	Ambiti	0	5	0	4	5	5	0	0	7	0	7	6	7	0
	Router Cisco XD45	HW Communi cation	0	5	0	0	5	1	0	0	6	0	0	6	2	0
	S.O. Ubuntu	SW Sistemi IT	0	5	0	4	5	1	0	0	8	0	7	8	2	0
	DB di Sistema	Basi di Dati	8	5	0	4	5	1	0	18/4	8	0	7	8	2	0
	Server UNIX VX45 4	HW Sistemi IT	0	5	0	0	5	1	0	0	6	0	0	6	2	0
	Symantec Appliance Firewall sw	SW Communi cation	0	5	0	4	5	1	0	0	8	0	8	8	2	0
^ CED Roma1	Accessi con badge CED Roma 1	Sistemi di Sicurezza	0	5	0	4	5	1	0	0	7	0	7	6	3	0
	Cabina Elettrica privata dell'organizza zione	Utenze	0	5	0	0	5	3	0	0	6	0	0	6	4	0
	Palazzina C - via dei eremi 15 Roma	Edifici e Servizi	0	5	0	0	5	5	0	0	7	0	0	6	7	0
	Sistema antincendio	Sistemi Antincend	0	5	0	0	5	1	0	0	6	0	0	6	2	0

3.2.7 LOGICA PER LE SEGNALAZIONI DI CRITICITA' NEI REPORT XR

La "**Logica nei REPORT XR**" utilizzata dallo strumento è la seguente.

Si dice **CRITICITA'** una "non attuazione di un controllo/domanda di "**peso**" tra 8 e 10.

Supponiamo che vi sia un **Asset/Bene** con Nome che inizia con il numero **"35"** (ad es. **35 Server Windows**) Lo strumento cerca un **Questionario/Intervistato** che inizi con le stesse cifre (35) (ad es. **35 Neri – Sicurezza Server Windows**) e, se lo trova, **lo "associa" a tale Asset**. Inoltre**:**

- inserisce il **Numero di Criticità** derivato dalle risposte al questionario nelle **Mappe XR di rischio,** alla colonna "**Criticità**", e alla riga corrispondente a tale asset.

- Se non trova il questionario/intervistato con "35" mette "0" nel campo "(numero di) Criticità".

La colonna Vuln/Host è presente solo se si seleziona nelle OPZIONI il flag Vulnerability Assessment e si pone una directory di nome "VA" nella directory del Caso, con i file .XML generati dallo strumento di vulnerability assessment.

Chiedere ulteriori informazioni e documentazione a STDE per questa funzionalità.

3.2.8 REPORT ANALISI COSTI/BENEFICI

Questo report riguarda l'analisi costi/benefici relativi alla introduzione di nuove contromisure/controlli. La valutazione qui espressa è di tipo economico, deve perciò essere considerata insieme alle altre indicazioni di priorità, ai problemi organizzativi e di fattibilità.

I dati di input a questo processo di valutazione sono il costo iniziale della contromisura e i costi annuali per il suo mantenimento, nonché gli anni di utilizzo della contromisura. Insieme al valore della riduzione di rischio ottenibile, derivata dal risk assessment, vista la correlazione tra livelli di rischio e importi reali monetari utilizzata nello strumento, si potrà ottenere, tenuto conto anche del valore dell'inflazione attualmente valutata nel 2% tendenziale, il ROI e il payback period, cioè il numero di anni entro il quale si potrà rientrare dall'investimento.

Il report segnala i casi in cui non sia possibile rientrare dall'investimento e dunque la poca convenienza dell'introduzione della contromisura.

REPORT ANALISI COSTI/BENEFICI

Controlli / Salvaguardie	Anni Ammor/ Utilizzo	% Implem.	Costo medio (Euro) per Anno	Riduzione Rischio (Euro)	Riduz. Rischio %	ROI (Inflazione 2%)	Payback Period (Inflazione 2%)
Off-site Storage	10	0,0%	31.000	1.356.500	19,2%	47,7	1
UPS/Generatori elettr.	20	0,0%	25.000	596.000	8,5%	21,0	1
Risk Assessment	2	0,0%	80.000	1.275.800	18,1%	18,5	1
Piano di sicurezza	3	0,0%	26.667	447.500	6,3%	18,0	1
Piano di Continuità Oper.	2	0,0%	57.500	899.000	12,8%	17,8	1
Risposta all'Emergenza	3	0,0%	45.000	597.550	8,5%	14,4	1
Controllo Accessi File/Programmi	3	0,0%	53.333	647.750	9,2%	12,7	1
Inventario/Resp. Risorse	3	0,0%	36.667	369.000	5,2%	11,2	1
Politica di Sicurezza	3	0,0%	26.667	274.500	3,9%	10,6	1
Backup Documentazione	3	0,0%	43.333	400.000	5,7%	9,8	1
Interventi Struttura Organizzativa	2	0,0%	100.000	704.950	10,0%	8,4	1
Controlli Applicativi	3	0,0%	66.667	448.750	6,4%	8,0	1

3.2.9 COME GESTIRE I PIANI DI SICUREZZA

Lo scopo dei **Piani di Sicurezza** generati da RiskXRStudio è quello di presentare le **contromisure predisposte** per la protezione delle risorse dell'organizzazione per ottenere gli obiettivi definiti e di mostrare lo **stato di attuazione** e l'**efficacia** di tali contromisure.

Per ogni risorsa/Asset saranno individuati un certo numero di Controlli/criteri di sicurezza (meccanismi di sicurezza o semplici criteri) che se attuati consentiranno di ottenere l'obiettivo desiderato.

L'associazione di 2 cifre davanti ai nomi delle risorse/asset e davanti ai nomi dei questionari/interviste con i controlli/criteri di sicurezza necessari permetteranno di correlare Piani e Risorse.

Di questi controlli **una parte sarà già stata attuata** compiutamente in maniera efficace, **una parte parzialmente attuata** ed una parte pur pianificata **sarà ancora da attuare**. Lo stato effettivo con queste informazioni è mostrato dai report dei **Piani di Sicurezza** generati da RiskXRStudio.

Ogni risorsa/asset avrà inoltre un **Risk Owner** che è responsabile o referente per la gestione dei rischi ad essa connessi. L'owner insieme alla sua e-mail verrà inserito nel campo **descrizione** del "Modello XR" alla riga associata alla risorsa.

Una volta completato il risk assessment e generati tutti i report relativi, andando al TAB Report si potrà premere il tasto **"Piani di sicurezza"**. Questo farà generare i Piani nella Directory del Caso sotto la sottodirectory "Report/Piani di Sicurezza".

I Piani di sicurezza potranno essere **inviati per e-mail agli "owner"** dopo l'effettuazione del Risk Assessment e la generazione dei report.

Le risorse che non avranno un riferimento specifico saranno aggregate al referente del Caso o in mancanza di questi sarà generato un file "Responsabile caso.xlsm", tutto automaticamente.

L'owner è uno dei "Riferimenti" di aggregazione dei Piani di sicurezza (mettendo in Descrizione "Mario Rossi#mario.rossi@stde.it), è possibile però in alternativa porre nella descrizione del Modello XR di un insieme di Asset, ad esempio, la stringa "CED Roma 1#" con il cancelletto finale.

Si otterrà che il "Riferimento" dei Piani diventa "CED Roma 1", non si è associato una e-mail perché non ci interessa e si avranno i Piani per tutti gli Asset del CED Roma 1 in uno stesso file di nome "CED Roma 1.xlsm".

Il report dei "Piani di sicurezza" fornisce lo "stato" come detto della protezione di ciascuna risorsa sia a livello di pianificazione sia a livello di attuazione attuale. Le Mappe di rischio danno i valori di rischio conseguenti che permettono di individuare gli interventi futuri più urgenti necessari per ottenere un'adeguata protezione.

I "Piani di sicurezza" consentono anche di **mostrare al certificatore** le contromisure scelte per raggiungere gli obiettivi di protezione da raggiungere per la **certificazione** e mostreranno lo stato attuale, nonché i rischi residui.

Vediamo ora delle pagine (fogli) esemplificative dei Piani di sicurezza.

RiskXRStudio

Piani di Sicurezza

v.1.0.15

Questo documento contiene i Piani di Sicurezza (l'insieme di criteri di sicurezza - controlli) per la protezione di ciascuna Risorsa (Asset e Ambito) tangibile o intangibile utilizzata dall'organizzazione.

Esso elenca prima i controlli già completamente attuati, poi quelli attuati parzialmente seguiti da quelli pianificati da attuare con date e responsabili dell'attuazione.

Il foglio "Istruzioni" descrive le modalità per l'utilizzo dei piani e delle funzioni associate.

Il Riferimento di questi Piani è:

RIFERIMENTO: ***CED Roma1***

DATA GENERAZIONE PIANI: ***05/09/2020***

Piani di Sicurezza

Istruzioni

I Piani di sicurezza qui presentati contengono i controlli/criteri di sicurezza attuati o pianificati per ottenere un adeguato livello di sicurezza per le risorse asset/ambiti dei servizi forniti dall'organizzazione a clienti, imprese e/o cittadini o per il supporto interno.

I Piani sono aggregati in questo file per Riferimento e vi è la possibilità di inviarli ad uno o più indirizzi e-mail se desiderato.

Per Riferimento si intende la "ragione di aggregazione dei Piani", che può essere il Referente, un Ambito di livello superiore che contiene gli Asset oggetto dei piani o qualsiasi altro riferimento. Tale riferimento viene inserito nel campo "descrizione" del modello XR.

Per ciascun Asset/Ambito del Modello considerato di pertinenza del Riferimento si ha un foglio, con lo stesso nome dell'Asset/Ambito con i "Controlli attuati (0 - NESSUNA urgenza), parzialmente attuati o da attuare". I campi delle azioni di intervento, quando necessarie, i tempi e le responsabilità presenti si riferiscono al singolo controllo.

Se necessario i Piani di Sicurezza possono essere integrati con eventuali "note" da parte dell'analista e inviati al Riferimento e ad eventuali altri destinatatari come "cc". Il referente una volta compilati i campi delle soluzioni con i tempi e i responsabili delle singole azioni spedirà indietro i piani completati in risposta.

La tabella che segue consente di "interpretare" correttamente i "valori di attuazione" di ciascun Controllo dei Piani.

A questo punto l'analista può prendere le E-MAIL dei PIANI DI SICUREZZA generate nella directory "Piani di Sicurezza" sotto la directory "Report" e verificare, se vuole, tutte le schede di ciascun Ambito/Asset predisposte.

Lista Protezioni (Controlli)

RIFERIMENTO: CED Roma1 **ASSET/AMBITO:** 05 Accessi con badge CED Roma 1

ID Controllo	Controllo	Asset/ Ambito	Urgenza di intervento	% Attuata del Controllo	Rilevanza (peso)	Obiettivi di Controllo	Rif. Normativo	Area di sicurezza del controllo	Commento	ID Rientro	Soluzione Adottata/Prevista	Pianificazione	Responsabile
25	I supporti che contengono informazioni devono essere protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto.	05 Accessi con badge CED Roma 1	0 - NESSUNA	100	10	ISO27001 A.8 Gestione degli asset	CTRLAMEDIA - A.8.3.3 Trasporto dei supporti fisici	Contr. Appar.&Supporti Dati		8			
33	I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi alla cessazione del rapporto di	05 Accessi con badge CED Roma 1	0 - NESSUNA	100	10	ISO27001 A.9 Controllo degli accessi	CONTR ACC - A.9.2.6 Rimozione o adattamento dei diritti di accesso	Controllo Accessi		519			

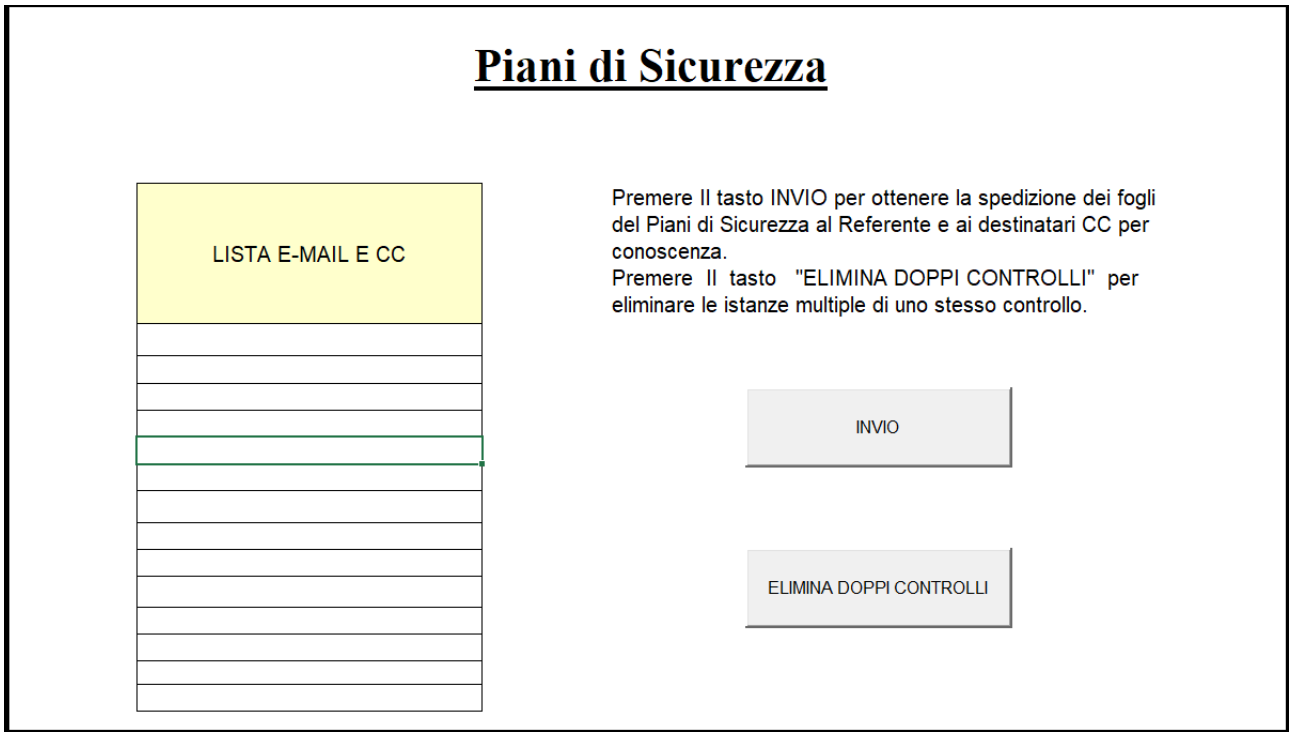
ELIMINAZIONE DEI DOPPI CONTROLLI. Uno stesso controllo può essere verificato con una domanda posta a più intervistati. Ogni risposta viene registrata e valutata se sia o meno attuata, ma dalla seconda istanza viene colorata in giallo.

Dopo la verifica è possibile eliminare tutte le istanze, eccetto la prima, nella quale possono essere inserite anche note e considerazioni.

Per eliminare i doppi controlli automaticamente eccetto la prima istanza dal piano basta premere l'apposito pulsante "ELIMINA DOPPI CONTROLLI" prima dell'invio.

Al termine della verifica è possibile inviare i Piani al referente e, se si ritiene il caso, ad altre persone pertinenti.

Nella immagine che segue si può vedere il tab dove vi sono il pulsante "ELIMINA DOPPI CONTROLLI" e quello di INVIO.



Con la Valutazione dei rischi, l'interpretazione dei risultati relativi e le indicazioni di urgenza d'intervento inseriti nei Piani di sicurezza, nonché i successivi Piani di rientro si ottiene l'implementazione di un completo processo di RISK MANAGEMENT dopo la verifica della implementazione delle azioni proposte.

L'**URGENZA** è basata come indice globale su tre fattori:

1. **L'INDICE DI NECESSITA' dell'intervento** nell'area del controllo che è correlato ai **livelli di rischio residuo**:

   a. NECESSARIO,

   b. DA VALUTARE

   c. NESSUNO

   Basato sull'**Indice composito di Priorità**.

2. La rilevanza specifica del "controllo" per i rischi (peso).

3. Il livello della % di attuazione/efficacia attuale del controllo.

L'ordine dei controlli relativi alle protezioni predisposte per le risorse dell'organizzazione nei **Piani di Sicurezza** viene riordinata con i seguenti criteri.

1. Si pongono prima i controlli con NESSUNA urgenza perché già attuati ed efficaci in base ai valori di rischio residuo, poi i controlli parzialmente attuati e di minore efficacia con livello di "urgenza" sempre maggiore, suddivisi in 5 classi;

2. All'interno di queste 5 classi di urgenza si pongono prima i controlli "più attuati in %" perché lo scopo è evidenziare le protezioni predisposte;

3. Inoltre, per una stessa % di attuazione sono posti prima i controlli di maggiore rilevanza in generale per il rischio (peso).

3.2.10 COME GESTIRE I PIANI DI RIENTRO

Lo scopo dei **Piani di Rientro** è di pianificare gli interventi necessari per **far rientrare i valori di rischio** dell'organizzazione entro i margini dei **Criteri di accettabilità** da parte della Direzione.

RiskXRStudio™ 2021 consente di gestire i Piani di rientro dai rischi e i Risk Owner all'interno del processo di RISK MANAGEMENT.

Compito dell'Owner è di identificare le azioni operative per il rientro dai rischi, indicare i tempi previsti di risoluzione e a chi sarà affidato il compito di implementare tali azioni e/o rispondere per esse. I Piani di rientro sono generati automaticamente dallo strumento, precompilati con i campi da completare già predisposti.

Le "vulnerabilità" causa dei rischi sono individuate tramite dei questionari posti alle persone in grado di rispondere con correttezza, per competenza e pertinenza.

Ad ogni Ambito/Asset vengono associati istanze di questionari specifici e dalle risposte saranno detratte le vulnerabilità e dunque suggerite le tipologie di intervento da predisporre inviandole al Risk owner dell'ambito stesso.

Una volta completato il risk assessment e generati tutti i report relativi, andando al TAB Report si potrà premere il tasto **"Piani di Rientro dai rischi"**. Questo farà generare i Piani di rientro nella Directory del Caso sotto la sottodirectory "Report/Piani di Rientro".

Le vulnerabilità che non avranno un referente specifico saranno mandate al referente del Caso o in mancanza di questi sarà generato un file "Responsabile caso.xlsm", tutto automaticamente.

Vediamo ora delle pagine (fogli) esemplificative di un Piano di rientro. Esso è composto:

- da una pagina di testata,
- una di Istruzioni,
- una o più di dettaglio con le "vulnerabilità" e i campi per il Piano di rientro, per ciascun Ambito o Asset,
- una pagina finale con il tasto INVIO.

RiskXRStudio

Piani di Rientro

v.1.0.11

Questo documento contiene i Piani di Rientro per la protezione di ciascuna Risorsa (Asset e Ambito) tangibile o intangibile utilizzata dall'organizzazione.

Esso elenca i controlli non attuati e insufficientemente attuati al fine di individuare azioni per raggiungere un'adeguato livello di sicurezza.

Il foglio "Istruzioni" descrive le modalità per l'utilizzo dei piani e delle funzioni associate.

Il Referente di questi Piani è:

NOME REFERENTE:

DATA GENERAZIONE PIANI: ***01/09/2020***

NOTE

Generali | Istruzioni | 02 Ufficio HR | 01 Ufficio Gestione Fornitori | Invio

Piani di Rientro

Istruzioni

I presenti Piani di rientro contengono i controlli/criteri di sicurezza "non attuati" o insufficientemente attuati per un adeguato livello sicurezza dei servizi forniti dall'organizzazione ai clienti, imprese e/o cittadini o per il supporto interno.

Questi piani descrivono le azioni necessarie per ottenere la protezione delle risorse indispensabili per raggiungere gli obiettivi definiti di dall'organizzazione. Il Referente di questi Piani e la data di generazione sono indicate nel foglio "Generali".

Per ciascun Ambito del Modello degli asset considerato di pertinenza del Referente si ha un foglio, con lo stesso nome dell' ambito, con i "Controlli non attuati o parzialmente attuati". I campi delle azioni di intervento, i tempi e le responsabilità qui presenti si riferiscono al singolo controllo.

I Piani di Rientro possono essere integrati con eventuali "note" da parte dell'analista e inviati al Referente nonché ad eventuali altri destinatatari come "cc". Il referente una volta compilati i campi delle soluzioni con i tempi e i responsabili delle singole azioni spedirà indietro i piani all'indirizzo e-mail di riferimento.

Generali | Istruzioni | 02 Ufficio HR | 01 Ufficio Gestione Fornitori | Invio

A questo punto l'analista può prendere le E-MAIL dei PIANI DI RIENTRO generate nella directory "Piani di Rientro" sotto la directory "Report" e verificare, se vuole, tutte le schede di ciascun Ambito/Asset predisposte.

Lista Controlli con vulnerabilità

REFERENTE: Mario Rossi **AMBITO:** SUPPORTO

ID Controllo	Controllo non adeguato (Vulnerabilità)	Asset/ Ambito	Urgenza di intervento	% Attuata del Controllo	Rilevanza (peso)	Obiettivi di Controllo	Rif. Normativo	Area di sicurezza dei controlli	Commento	ID Rientro	Soluzione Adottata/Prevista	Pianificazione rientro	Responsabile
92	Tutti i requisiti di sicurezza delle informazioni sono da stabilire e concordare con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione.	SUPPORTO	5 - ALTA	40	10	ISO27001 A15 Relazioni con i fornitori	ASS. RESP - A.15.1.2 Inserire la sicurezza all'interno degli accordi con i forni	Assegn. Responsab.		1044			
93	Gli accordi con i fornitori devono includere i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni associati ai servizi e ai prodotti della filiera di fornitura per l'ICT.	SUPPORTO	2 - MEDIO BASSA	60	8	ISO27001 A15 Relazioni con i fornitori	RISKMANAG - A.15.1.3 Filiera di fornitura per ICT	Risk Manag. Program		1043			
11	Gli accordi contrattuali con il personale e con i collaboratori	PERSONALE	2 - MEDIO BASSA	70	8	ISO27001 A.7 Sicurezza delle	PERSONALE - A.7.1.2 Termini e condizioni di	Personale		1045			

ELIMINAZIONE DEI DOPPI CONTROLLI. Uno stesso controllo può essere verificato con una domanda posta a più intervistati. Ogni risposta viene registrata e valutata se sia o meno attuata, ma dalla seconda istanza viene colorata in giallo.

Dopo la verifica è possibile eliminare tutte le istanze, eccetto la prima, nella quale possono essere inserite anche note e considerazioni.

Per eliminare i doppi controlli automaticamente eccetto la prima istanza dal piano basta premere l'apposito pulsante "ELIMINA DOPPI CONTROLLI" prima dell'invio.

Al termine della verifica è possibile inviare i Piani al referente e, se si ritiene il caso, ad altre persone pertinenti.

Nella immagine che segue si può vedere il tab dove vi sono il pulsante "ELIMINA DOPPI CONTROLLI" e quello di INVIO.

La lista dei controlli per Priorità di intervento dei Piani di Rientro viene riordinata con i seguenti criteri.

1. Si pongono prima i controlli con livello di "urgenza" maggiore;

2. All'interno di queste 5 classi si pongono prima i controlli meno attuati con % di attuazione minore, che hanno maggiore margine per ridurre il rischio se completamente attuati;

3. Inoltre, per uno stesso livello di attuazione sono posti prima i controlli di maggiore importanza per il rischio (peso).

3.2.11 COME GESTIRE IL PIANO GENERALE DI RIENTRO

A volte si desidera avere un'unica visione delle problematiche di sicurezza prima di affidare la risoluzione a ciascun responsabile specifico. La risposta a questo quesito è data dal "**Piano generale di rientro",** uno dei report che si possono generare al **TAB Report,** che in una sola lista indica tutti gli **INTERVENTI** da fare in ordine di **Priorità decrescente,** l'asset o l'**ambito** coinvolto, il livello di **URGENZA** (su 5 livelli) dell'intervento e la **%** di **attuazione/efficacia** attuale del controllo corrispondente, oltre a informazioni (commenti) sulle cause del problema indicato.

Di seguito viene mostrato un caso esemplificativo di un "**Piano generale di rientro**". Si noti come i commenti in fase di acquisizione delle risposte forniscano informazioni basilari per una efficace reporting della situazione di rischio e per la predisposizione degli interventi.

L'**URGENZA** è basata come indice globale su tre fattori:

1. **L'INDICE DI NECESSITA' dell'intervento** nell'area del controllo che è correlato ai **livelli di rischio residuo**:

   a. NECESSARIO,

   b. DA VALUTARE

   c. NESSUNO

   Basato sull'**Indice composito di Priorità**.

2. La rilevanza specifica del "controllo" per i rischi (peso).

3. Il livello della % di attuazione/efficacia attuale del controllo.

La **Priorità di intervento** del Piano generale di Rientro viene riordinata con i seguenti criteri.

1. Si pongono prima i controlli con livello di "**URGENZA**" maggiore;

2. All'interno di queste 5 classi si pongono prima i controlli meno attuati in % che hanno maggiore margine per ridurre il rischio se completamente attuati;

3. Inoltre, per uno stesso livello di attuazione sono posti prima i controlli di maggiore importanza per il rischio (peso).

St De
Studio Dell'Agnello S.r.l.

Piano Generale di Rientro

REFERENTE: Mario Rossi

ID Controllo	Controllo non adeguato (Vulnerabilità)	Asset/ Ambito	Urgenza di intervento	% Attuata del Controllo	Rilevanza (peso)	Obiettivi di Controllo	Rif. Normativo	Area di sicurezza dei controlli	Commento	ID Rientro	Soluzione Adottata/Prevista	Pianificazione rientro	Responsabile
148	L'azienda deve stabilire delle procedure per accompagnare e controllare i visitatori in tutte le aree sensibili.	SEDE via Zara	5 - ALTA	30	10	Sicurezza Edifici ed ambientale	PROCEDURE - Controllo visitatori	Procedure	Carenza di personale	126			
148		SEDE via Comini	5 - ALTA	40	10	Sicurezza Edifici ed ambientale	PROCEDURE - Controllo visitatori	Procedure	Occorre fare conoscere meglio le procedure al personale	560			
148		Sede Centrale	5 - ALTA	60	10	Sicurezza Edifici ed ambientale	PROCEDURE - Controllo visitatori	Procedure	Non sempre viene applicato.	994			
148		CED Lucumano	5 - ALTA	60	10	Sicurezza Edifici ed ambientale	PROCEDURE - Controllo visitatori	Procedure	Vi è una criticità sulle procedure di accesso e accompagnamento.	1428			
92	Tutti i requisiti di sicurezza delle informazioni sono da stabilire e concordare con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione.	Uffico 9	4 - MEDIO ALTA	50	8	ISO27001 A15 Relazioni con i fornitori	ASS. RESP - A.15.1.2 Inserire la sicurezza all'interno degli accordi con i forni	Assegn. Responsab.	I contratti sono carenti per una completa efficacia del criterio esposto.	71			
92		Ufficio 4	4 - MEDIO ALTA	60	8	ISO27001 A15 Relazioni con i fornitori	ASS. RESP - A.15.1.2 Inserire la sicurezza all'interno	Assegn. Responsab.	I contratti sono carenti per una completa efficacia del criterio esposto.	505			

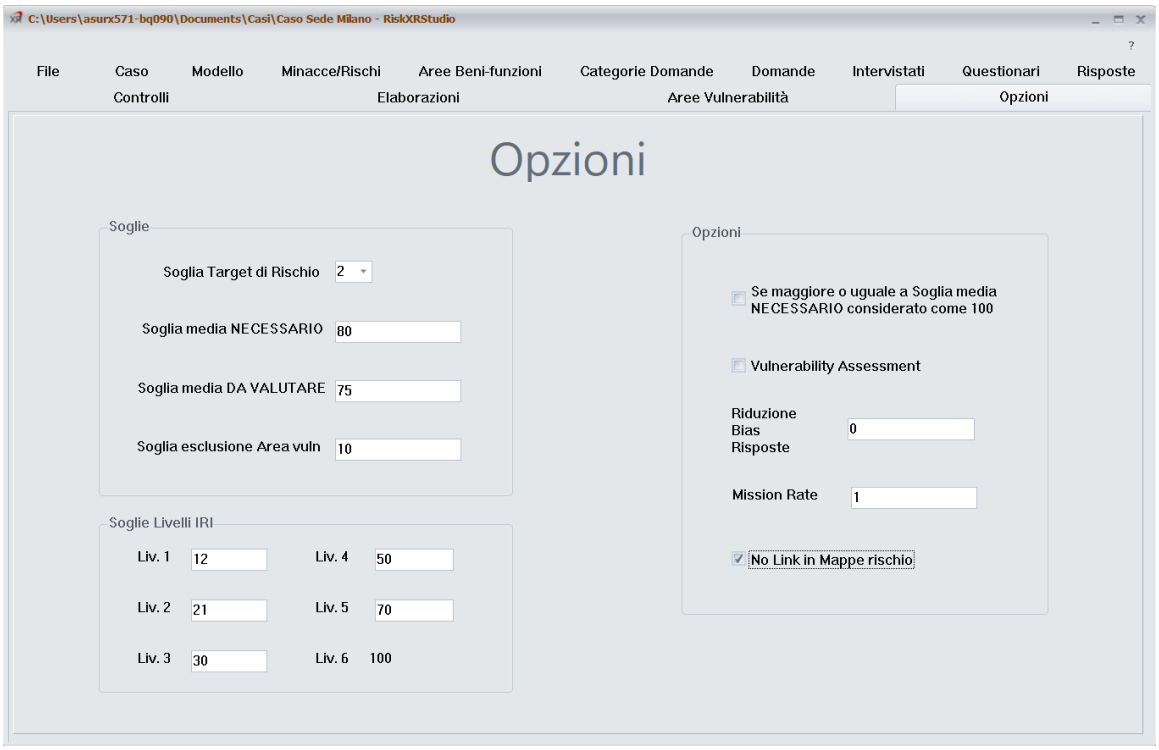
... Piano Generale di Rientro | Opzioni

3.3 GENERARE ALTRI REPORT

I report presentati in precedenza sono particolarmente completi a tutti i livelli da quello di sintesi a quelli di dettaglio, è comunque possibile generare altri report elencati nella pagina del tab Report.

3.4 COME CAMBIARE LE OPZIONI E LE SOGLIE DELL'ANALISI

Modificando le OPZIONI dell'apposita form dello strumento è possibile personalizzare i risultati ottenuti secondo le proprie esigenze.



Selezionando le seguenti opzioni si possono definire le soglie di rischio con cui effettuare la valutazione. Le opzioni sono:

1. **Se maggiore o uguale a "Soglia media NECESSARIO" considerato come 100**. Nel caso che un'area di vulnerabilità ha tutte le risposte sopra la "Soglia media NECESSARIO" in OPZIONI (vedi successivo paragrafo) ottiene una % di controlli attuati pari a 100%. In questo caso si considererà vulnerabilità "0" per il calcolo rischio (come se tutte le risposte di quell'area fossero state 100(10)) anche se inferiori. Inoltre su quell'area sarà raccomandato nessun intervento.

2. **Vulnerability Assessment.** Se si vuole considerare come input i dati derivanti da strumenti di Vulnerability Assessment si

selezioni questa opzione, ponendo i dati di Vulnerability assessment in una directory di nome "VA" sotto la directory del Caso. Si chiedano poi istruzioni ulteriori per i formati dei dati.

3. **Riduzione Bias Risposte.** Questo valore sarà applicato ad ogni risposta ai questionari quando si ritenga per ragioni statistiche che, ad esempio essendo tutti gli intervistati dei responsabili di U.O. tendano a fornire risposte troppo ottimistiche rispetto alla reale situazione di sicurezza riscontrata.

4. **Mission Rate.** Questo parametro riguarda l'Analisi costi benefici quantitativa. La funzione ha come input tutti dati quantitativi inseriti nel tab "Controlli", con in più un input qualitativo/ semiquantitativo che deriva dai valori di Rischio effettivo RLE delle varie minacce del Risk Assessment. I risultati si ottengono considerando un valore ipotetico standard di Mission. (Il Valore di Mission è rappresentato dalla somma dei valori monetari di tutti gli asset del Caso, anche intangibili). Il valore reale di Mission del caso corrente potrà essere in realtà diverso, perciò è necessaria una calibrazione fatta tramite il parametro "Mission rate". Il valore di tale rapporto "Mission del Caso/Mission std" si potrà dedurre valutando per alcuni casi conosciuti i risultati ottenuti con quelli poi verificati.

   Tale costante di "Mission rate" permetterà di avere stime più vicine alla realtà per le analisi che successivamente riguarderanno tale ambito di analisi.

   Si ricorda che vista la modalità comunque qualitativo/quantitativa complessiva i risultati devono essere presi per valutare la priorità/convenienza tra le varie tipologie di intervento e non come valori monetari assoluti.

5. **No link in mappe rischio.** Questo parametro permette di "non" creare link associati al numero di Criticità che facciano saltare alla lista delle relative descrizioni. Con questa opzione si ottiene una riduzione dei tempi di elaborazione dei Report, specie nelle fasi intermedie del processo, prima della loro generazione finale.

3.4.1 DEFINIRE LE SOGLIE DEI CRITERI PER L'ACCETTAZIONE DEL RISCHIO

È importante che la Direzione indichi il "**Livello di rischio accettabile**" in modo da riuscire a definire i "**CRITERI PER L'ACCETTAZIONE DEL RISCHIO**" e poter effettuare una valutazione del rischio una volta ottenuti i risultati.

Lo strumento richiede l'indicazione di una "**Soglia Target di Rischio**" da inserire nelle **OPZIONI** utilizzata dallo strumento per fornire le sue valutazioni sui rischi riscontrati. Tale soglia Target di Rischio deve essere **uguale o inferiore alla Soglia di Rischio accettata** dalla Direzione.

Se inferiore vuol dire che altre entità rilevanti come Enti di certificazione, Autorità per la sicurezza pongono limiti più stringenti rispetto a quelli derivati dalla Soglia accettata dalla Direzione, ma che è necessario soddisfare per ottenere gli obiettivi strategici comunque definiti dalla Direzione stessa.

E' auspicabile, per un miglioramento virtuoso della sicurezza verso livelli più allineati allo stato dell'arte come richiesto dalle norme nazionali ed internazionali, abbassare il livello di rischio accettato nel tempo al fine di essere pronti sempre ad un eventuale mutamento del contesto di rischio. Sempre salvaguardando un livello equilibrato e giustificabile degli investimenti.

La Direzione è libera di definire la soglia che ritiene opportuna anche per considerazioni proprie non necessariamente tecniche.

In prima istanza lo strumento indica che è **NECESSARIO** un intervento in un'Area rilevante per la Sicurezza (Area di vulnerabilità) quando l'area influisce su un rischio di valore più alto della **Soglia Target di Rischio**.

Se la Soglia Target di Rischio è superiore al massimo livello di rischio riscontrato nel Caso, lo strumento conclude che abbiamo una situazione sotto controllo, perciò non è necessario un intervento nell'area, con indicazione **NESSUNO**.

Se si osserva che vi sono Aree rilevanti per la Sicurezza che comunque hanno un grado di attuazione ed efficacia troppo carente, sotto la "**Soglia media DA VALUTARE**", allora si passa all'indicazione di **intervento DA VALUTARE**.

Dai Criteri per l'accettazione del Rischio si derivano i Criteri di Intervento sulle Aree di vulnerabilità al fine di ridurre il rischio per tutte le minacce al livello accettabile dalla Direzione. Sono definiti 3 livelli di "**Necessità di intervento**":

1. **NECESSARIO**
2. **DA VALUTARE**
3. **NESSUNO**

Nelle OPZIONI si trovano 4 soglie che esprimono i "**CRITERI PER L'ACCETTAZIONE DEL RISCHIO**" e le relative politiche di intervento:

6. La "**Soglia Target di Rischio**". Con la possibilità di scegliere tale livello tra il Livello 1 fino al livello 3 di dieci, in cui il livello standard è il Livello 2.

7. La "**Soglia Media NECESSARIO**" che è la soglia di attuazione media di un'Area di vulnerabilità sotto la quale si ritiene NECESSARIO intervenire se correlata ad una minaccia con rischio sopra la "Soglia Target di Rischio".

8. La "**Soglia media DA VALUTARE**" che è la soglia di attuazione media di un'Area di vulnerabilità sotto la quale si ritiene DA VALUTARE l'intervento se correlata con una minaccia con rischio pur sotto la "Soglia Target di Rischio".

9. La soglia "**Soglia esclusione Area Vuln**" che indica la % di apporto al rischio sotto la quale le Aree non vengono considerate.

La logica è la presente:

4. La **SOGLIA DI RISCHIO effettivo RLE accettato dalla Direzione** può essere:

   a. Livello 2 – livello di sicurezza medio standard adeguato per ambiti civili

   b. Livello 1 – livello di alta sicurezza o per organizzazioni virtuose

   c. Livello 3 – livello di sicurezza per organizzazioni con minore criticità.

Valori accettati superiori non sono ritenuti congruenti con un adeguata gestione della sicurezza di un organizzazione.

LOGICA DELLE SOGLIE

1. Se ho una Minaccia che ha un **LIVELLO DI RISCHIO RLE sopra o uguale alla "Soglia Target di Rischio"**, allora lo strumento identifica **le AREE DI VULNERABILITA'** che provocano tale rischio critico.

   a. Di queste, viene stabilito come **NECESSARIO** un Intervento solo in quelle Aree che hanno un apporto al rischio in % sopra la "**Soglia esclusione Aree Vuln" (default 10%, personalizzabile)**, escludendo così le aree "irrilevanti" per il rischio.

   b. Tra le aree individuate si indica però **DA VALUTARE,** cioè di minore rilevanza per la riduzione del rischio rispetto a "NECESSARIO", quelle aree aventi una media di attuazione

superiore alla **"Soglia media NECESSARIO" (default "80"),** perché hanno già, **un buon livello di attuazione** e perciò meno margine di miglioramento.

2. Se invece ho una Minaccia che ha un **LIVELLO DI RISCHIO RLE sotto la "Soglia Target di Rischio"** allora lo strumento identifica **le AREE DI VULNERABILITA'** che provocano tale rischio.

3. Tra queste, se la MEDIA DI ATTUAZIONE dei controlli è sotto il valore di "**Soglia media DA VALUTARE**" allora l'intervento in tale area è indicato come **DA VALUTARE**, altrimenti l'intervento viene indicato come nessun intervento: **NESSUNO,** perché l'area non provoca rischi critici e ha già un buon livello di attuazione.

3.4.2 CALIBRARE LE SOGLIE DEI LIVELLI DI IRI

L'IRI misura la vulnerabilità nei confronti delle minacce ed è misurata con valori da 0 a 100. Nel calcolo del livello di rischio effettivo RLE abbiamo come input il livello di rischio potenziale massimo RMLE e il valore di IRI.

Per poter utilizzare una tabella di verità che esprima la logica implementata occorre trasfomare il valore continuo dell'IRI in 6 livelli. Questo viene fatto stabilendo 6 intervalli di valori identificati da 5 soglie del valore superiore (la più alta è 100).

Nelle Opzioni vi è la possibilità per l'analista di personalizzare i valori di tali soglie e perciò del sistema di valutazione del rischio.

3.4.3 CALIBRAZIONE DEL BIAS RISPOSTE

E' esperienza comune per gli analisti di risk assessment verificare in base alla tipologia di intervistati messi a disposizione dall'organizzazione una certa deriva (Bias) delle risposte ai questionari, dovuta ai vari interessi di ciascun intervistato.

Una scelta oculata del campione da utilizzare per il risk assessment assicura l'equilibrio delle risposte, in particolare se si scelgono persone con interessi e responsabilità diverse. Purtroppo nella realtà vi sono scelte, come ad esempio avere a disposizione solo i responsabili degli uffici, ma non gli operativi, che portano inevitabilmente ad un giudizio mediamente più positivo rispetto alla realtà.

Se l'analista dai risultati capisce come la modellazione risente di questa deriva, può utilizzare lo strumento di calibrazione dell'input che agisce sul valore medio delle risposte. Tale strumento si trova nel tab OPZIONI. Il

parametro è “Riduzione BIAS Risposte”, il valore deve essere una “differenza di risposta” valore intero in genere da 1 a 10.

4. INSTALLAZIONE DELL'APPLICAZIONE RISKXRSTUDIO"

4.1 PREREQUISITI

La suite del prodotto "RiskXRStudio™ 2021" è composta da più applicazioni 64 bit, in particolare dalla applicazione base identificata con nome file "RXRSTUDIO" con l'applicazione associata RXRASSESSX. Inoltre, si può installare l'applicazione WEB per il risk assessment tramite intranet di nome file RXRASSESSAPP, come descritto più avanti.

Possono essere fatte sia installazioni server, sia installazioni desktop/laptop. I prerequisiti del sistema per l'utilizzo di RiskXRStudio™ 2021 server/desktop sono i seguenti:

1. RAM: minima 8 GByte
2. HD o SSD: 125 GByte minimo, spazio libero 50 GByte
3. CPU: potenza equivalente consigliata di 4 vcpu Xeon 5600 / I7 a 2.00 Ghz.
4. O.S.: Windows server 2012 R2, Windows 10, Windows 8.1,
5. OFFICE: Microsoft Office 2019/2016/2013, Microsoft Office 365 business.
6. SOFTWARE da installare: Microsoft Access Database Engine 2010 64 bit redistributable scaricabile da internet.

4.2 INSTALLAZIONE

L'applicazione **RiskXRStudio™ 2021** base viene installata tramite il relativo setup effettuando il "download" dal sito internet del fornitore accedendo all'area riservata clienti con il proprio login.

Il setup una volta lanciato e inserita la password di accesso chiede l'accettazione delle condizioni di licenza, il proprio user-id, la società e alcune indicazioni di preferenza e di configurazione a seconda se l'installazione è in un server o in un desktop/laptop. Al termine riavviare il sistema.

4.2.1 CONFIGURARE PERCORSO ATTENDIBILE IN EXCEL E ACCESS

È necessario che **la directory di lavoro dei "Casi"** sia considerata in **OFFICE sia per EXCEL che per ACCESS** un "**Percorso attendibile**" secondo la indicazione di Microsoft, pena il non corretto calcolo dei risultati. Per ottenere tale impostazione procedere nel seguente modo.

1. Aprire un **Nuovo** file di Excel
2. Premere il **simbolo di Office** in alto a sinistra.
3. Aprire il bottone in basso a destra **Opzioni di Excel**.
4. Selezionare **Centro Protezione** a sinistra
5. Premere **Impostazioni Centro protezione** a destra
6. Selezionare "**Percorsi attendibili**" a sinistra in alto
7. Premere **Aggiungi percorso attendibile**
8. Inserire il **Percorso/Path della directory dei Casi** scelta: es. Documenti\Casi
9. Selezionare il flag **Considera attendibili anche le sottocartelle del percorso**.
10. Premere i vari **OK** fino ad uscire.

La procedura è completata.

Stessa procedura è da seguire per **ACCESS**.

5. INSTALLAZIONE DELL'APPLICAZIONE "RXRASSESSAPP"

5.1 PREREQUISITI

Se si desidera gestire da Web la fase di assessment in intranet occorre installare anche l'applicazione "RiskXRAssess Web" (RXRASSESSAPP) con l'apposito setup facente parte del prodotto. Per installare l'applicazione RXRASSESSAPP in un Web Server o altro sistema occorre che nel sistema operativo tra le funzionalità di Windows sia stata installata la funzione "**Internet Information Services (IIS)** di release Microsoft Internet Information Services (IIS) 10 o 8.5 o 7.5/7. Inoltre, occorre installare i moduli di IIS legati ad ISAPI: **ISAPI Extentions e ISAPI Filters**.
Al fine di verificare che non vi siano ostacoli al funzionamento di IIS lanciare "localhost" nel browser e verificare che sia mostrato il sito di default di IIS o altro sito che sia stato già installato al suo posto.
Soddisfatti i prerequisiti procedere poi all'installazione di "RXRAssessApp".

5.2 INSTALLAZIONE

L'applicazione "RXRAssessApp" è una applicazione ISAPI che permette l'acquisizione tramite web delle risposte e commenti ai questionari della fase di Assessment, nonché il monitoraggio di tutto il processo di assessment.

L'installazione di tale Applicazione nel "Web server" avviene tramite un "setup" che predispone il software sotto la directory "C:\web\RXRAssessApp\" come radice dell'applicazione.

Al fine di coprire tutte le esigenze dell'utente sono forniti: un setup di installazione STANDARD e un setup alternativo.

Il SETUP standard installa l'Applicazione nel Default Web Site (ID 1) associato alla porta standard HTTP (porta 80), usando il setup con denominazione del tipo "setupRiskXRAssessAPP1.0.x.xxx_Standard 80_xxx.exe".

In alternativa:

Se l'installazione standard, per ragioni legate a "constrains" di configurazione relative allo stesso sito o a "deny" nel file di configurazione generale di IIS, avesse difficoltà di funzionamento, allora si può richiedere e installare l'Applicazione in un NUOVO SITO del Web Server, associato alla porta 8876, lanciando il setup denominato:

"setupRiskXRAssessAPP1.0.x.xxx_8876_xxx.exe".

Occorrerà abilitare la porta 8876 nelle impostazioni avanzate del Firewall se presente. Questo setup consente di continuare ad utilizzare in

contemporanea anche altre applicazioni installate sul sito associato alla porta 80 standard.

La cartella in cui generare con l'Applicazione base "RXRStudio" e i file dei Questionari con la relativa autenticazione degli intervistati è "C:\web\rxrdata".
Occorre che la directory "rxrdata" possa essere scritta dagli utenti che accedono all'applicazione. Per questo "abilitare" in tale directory in "SCRITTURA" gli utenti di "RiskXRAccessAPP", altrimenti al "Salva" o "Salva ed Esci" l'applicazione non può scrivere.

Il software dell'applicazione RXRASSESSAPP, le risorse, le librerie, i dati e le immagini necessarie sono condensate in un unico file ISAPI di tipo ".dll" posto nella root. Insieme a tale file nella stessa directory è presente anche il file "web.config" di configurazione.

Nella directory "c:\web\Manuali" è disponibile il manuale relativo sia all'installazione sia alla fase operativa.

Per completare l'installazione occorre seguire anche le seguenti istruzioni e verifiche di configurazione:

a) Nel FIREWALL abilitare i Servizi Web (HTTP/HTTPS) per l'intranet, che è l'ambito di utilizzo dell'applicazione.

b) Solo nel caso alternativo abilitare nel firewall (sezione Impostazioni avanzate) anche la "porta 8876" da cui accederemo all'applicazione installata.

c) Selezionando in IIS il "Nome del web server" (al top), andare all'icona "ISAPI e CGI restrictions" e aggiungere (ADD) il percorso dell'applicazione (c:\web\rxrassessapp\RiskXRAssessAPP.dll) tramite il tasto "browse" ai percorsi file ISAPI eseguibili, settando anche il relativo "flag" di "eseguibile".

I setup sono installabili con Windows server 2012 R2 e IIS 8.5 o per desktop in Windows 7 e IIS 7.5, con Windows 8.1 e IIS 8.5 o Windows 10 e IIS 10.

Per utilizzare l'applicazione occorre seguire 2 fasi:

a) Effettuare lo "start" dell'applicazione RXRASSESSAPP eseguendo in un browser: http://localhost/rxrassessapp/$/Start,

b) A questo punto si potrà lanciare l'applicazione digitando il seguente indirizzo http://indirizzo_web_server/rxrassessapp dalla rete intranet o con un link nel sito intranet dell'organizzazione, ottenendo la schermata di LOGIN.

c) Solo per il caso alternativo occorre sostituire “rxrassessapp” con “rxrassessapp:8876”.

Nella schermata del Login in alto a sinistra è possibile avere il LOGO della società. Per inserirlo basta posizionare il file che deve essere di tipo .png ed avere il nome esatto “logo.png” nella cartella “C:\web\rxrdata”. Le dimensioni sono indicativamente, ma non necessariamente 200x50 pixel circa.

ALLEGATO 1

VALORI DELLE RISPOSTE AI QUESTIONARI

VALORI DI RIFERIMENTO PER LE RISPOSTE SULLA ATTUAZIONE DEI CONTROLLI

I valori possibili sono:

10 ATTUATO SEMPRE E IN MODO EFFICACE

9 ATTUATO OTTIMAMENTE

8 ATTUATO/CONFORME

7 ATTUATO IN BUONA PARTE

6 ATTUAZIONE APPENA SUFFICIENTE

5 ATTUAZIONE QUASI SUFFICIENTE

4 ATTUAZIONE INSUFFICIENTE

3 ATTUATO POCO E INEFFICACE

2 ATTUATO RARAMENTE

1 ATTUATO QUASI MAI

0 NON ATTUATO

NON APP NON APPLICABILE

NON SO NON SO

ALLEGATO 2
FORMATO NOMI BENE/ASSET

Formato NOME Asset

nnn NomeAsset #mm

nnn (opzionale)= se il NOME dell'Asset inizia con **3 CARATTERI NUMERICI "nnn"** allora se esiste un **Questionario/Intervistato** che inizia con **"nnn"** viene associato a questo Asset e le "**segnalazioni di non conformità**" del questionario saranno inserite nelle Mappe di rischio XR.

#mm (opzionale)= se in fondo al NOME dell'Asset vi sono **2 CARATTERI NUMERICI "mm" preceduti da #**, allora la valutazione del rischio viene effettuata usando il Profilo di Protezione XR **"mm"**

Tutti gli ASSET e AMBITI nel Modeldatacollection DEVONO avere **NOMI UNIVOCI**, eccetto gli **AMBITI RIFERITI** che hanno il **nome esatto** dell'Ambito che rappresentano come istanza.

ALLEGATO 3

FORMATO NOMI QUESTIONARI/INTERVISTATI

Formato NOMI Questionari/Intervistati

nnn NomeQuestionarioIntervistato

nnn (opzionale) = SE IL NOME del QUESTIONARIO/INTERVISTATO inizia con 3 CARATTERI NUMERICI "nnn" allora viene associato a tutti gli ASSET aventi un nome che inizia con lo stesso "nnn" e il numero delle sue segnalazioni di NON CONFORMITA' per Controlli critici è poi inserito nelle MAPPE DI RISCHIO XR vicino a tali ASSET (CRITICITA').

ALLEGATO 4
CATEGORIE DI ASSET

DEFINIZIONI DELLE CATEGORIE DI ASSET

La metodologia definisce ASSET una risorsa di cui sono identificate con esattezza le caratteristiche di sicurezza. Si definisce AMBITO un "Sistema", cioè un "insieme di ASSET" di cui l'AMBITO è un contenitore. Le sue caratteristiche di sicurezza sono date dalle caratteristiche molto varie dei suoi "figli" di cui l'AMBITO è il "Padre".

AMBITI - Questa categoria di beni comprende gli "elementi non caratterizzati" del modello che fanno da contenitori di altri beni/asset come "padri" di elementi "figli". Questi ultimi possono essere sia componenti interni dell'AMBITO sia ASSET o altri AMBITI esterni, da cui ereditano i rischi. Si utilizza questa categoria anche per processi e servizi erogati, nonché per rappresentare U.O. Essa può rappresentare comunque qualunque elemento tangibile o intangibile.

PERSONE - Questa categoria comprende tutte le persone di supporto dell'organizzazione incluso amministratori, persone di supporto ai sistemi, operatori, utenti e qualsiasi persona che abbia a che fare con il sistema sotto valutazione anche persone esterne.

APPLICAZIONI - Si riferisce a programmi applicativi specifici: Word processing, Spreadsheet, CAD/CAM, gestione paghe, inventario, ecc.

BASI DI DATI - Tutti i file di dati (elettronici e cartacei), sia organizzati in una base dati sia non organizzati, anche singoli, utilizzati da programmi e classificabili, come i file dati relativi a listini paga, i dati personali di un'anagrafe, i dati inseriti in un inventario, ecc.

DOCUMENTAZIONE - Questa categoria include i manuali degli apparati e le stampe di programmi e procedure operative riguardanti il sistema informativo.

EDIFICI E SERVIZI - Questa categoria di beni include gli edifici, i siti dei CED ed eventuali servizi quali la mensa e locali accessori, ecc.

HW COMMUNICATION - Hardware per i collegamenti remoti, include i modem, i multiplexer, i cavi, le schede di linea, antenne, antenne paraboliche e relativo firmware specifico.

HW SISTEMI IT - Questa categoria comprende l'hardware dei computer delle postazioni client, i server e gli apparati computerizzati coinvolti nella elaborazione dei dati o nelle funzioni di comunicazione.

INTANGIBILI - Questa categoria di beni comprende elementi non materiali come la reputazione dell'organizzazione, la sua credibilità, tutto ciò che è intangibile.

SW COMMUNICATION - Questa categoria include il software di rete relativo alla gestione delle comunicazioni tra computer in internet o in altre reti non compreso nel sistema operativo.

SW SISTEMI IT - Questa categoria di beni comprende tipicamente il sistema operativo, come windows, linux e le system utilities.

SISTEMI ANTINCENDIO - I sistemi considerati in questa categoria comprendono rivelatori di calore e di fumo, allarmi antincendio, sensori di umidità, sistemi di soppressione degli incendi.

SISTEMI DI SICUREZZA - Include i rivelatori di presenza, le videocamere, i sistemi di controllo degli accessi, i sistemi utilizzanti badge, cancelli, dispositivi crittografici, software di sicurezza e di audit.

SISTEMI DI SUPPORTO - Questa categoria comprende i sistemi di aria condizionata e di riscaldamento e umidificazione che gestiscono l'ambiente ottimale per l'utilizzo dei locali da parte del personale, dei sistemi computerizzati e degli apparati in genere, sistemi per il combustibile, sistemi di raffreddamento per macchinari e sistemi di messa a terra.

UTENZE - Questa categoria comprende i dispositivi che assicurano dentro l'organizzazione le utenze elettriche, telefoniche, del gas, del combustibile e dell'acqua, quali ad esempio eventuali trasformatori in cabine elettriche non del fornitore di elettricità e generatori elettrici.