

MINISTÈRO DELLA PRESIDENZA

MAGERIT - versione 2

Metodologia di analisi e gestione dei rischi dei sistemi informativi

I - Metodo

Catàlogo generale delle publicazióni ufficiali:
http://www.060.es
© Governo della Spagna. Ministèro della Presidenza
Pubblicato da: Ministèro della Presidenza. Segretaria Generale Tècnica
Publlicato in Dicèmbre de 2009
NIPO: 000-09-070-4

GRUPPO RESPONSABILE DEL PROGETTO MAGERIT versione 2

Direttore:
Francisco López Crespo
Ministero della Pubblica Amministrazione

Miguel Angel Amutio Gómez
Ministero della Pubblica Amministrazione

Javier Candau
Centro Crittografico Nazionale

Consulente esterno:
José Antonio Mañas
Professore
Università Politecnica di Madrid

Traduzione in italiano:
Fabio Guasconi
@ Mediaservice.net

Sommario

1. Introduzione a Magerit 5
1.1. Obiettivi di Magerit 5
1.2. Introduzione all'analisi e alla gestione dei rischi 6
1.3. L'analisi e gestione dei rischi nel suo contesto 7
1.4. Organizzazione delle guide 8
1.5. Per chi ha lavorato con Magerit v1.0 11
1.6. Valutazione, certificazione, audit e accreditamento 11
1.7. Quando occorre analizzare e gestire i rischi? 13
2. Realizzazione dell'analisi e della gestione 16
2.1. Analisi dei rischi 16
2.2. Gestione dei rischi 26
3. Strutturazione del progetto 32
3.1. Partecipanti 32
3.2. Sviluppo del progetto 34
3.3. Processo P1: Pianificazione 37
3.4. Processo P2: Analisi dei rischi 50
3.5. Processo P3: Gestione dei rischi 61
4. Sviluppo di sistemi informativi 69
4.1. Inizializzazione dei processi 69
4.2. Ciclo di vita delle applicazioni 70
4.3. Analisi dei rischi 71
4.4. Gestione dei rischi 72
4.5. "Metrica" versione 3 74
4.6. Riferimenti 82
5. Consigli pratici 83
5.1. Per identificare gli asset 83
5.2. Per individuare e modellizzare le dipendenze tra asset 84
5.3. Per valorizzare gli asset 86
5.4. Per identificare le minacce 87
5.5. Per valorizzare le minacce 87
5.6. Per selezionare le contromisure 88
5.7. Approssimazioni successive 88
5.8. Riferimenti 90
Appendice 1. Glossario 91
1.1. Termini in italiano 91
1.2. Termini anglosassoni 97
1.3. ISO/IEC Guide 73:2002 98
1.4. Riferimenti 99
Appendice 2. Riferimenti 101
Appendice 3. Ambito legale 102
Appendice 4. Ambito di valutazione e certificazione 103
4.1. Sistemi di gestione della sicurezza delle informazioni (SGSI) 103
4.2. Common Criteria (CC) 109
Appendice 5. Strumenti 115
5.1. PILAR 116

5.2. Riferimenti 117
Appendice 6. Evoluzione rispetto a Magerit versione 1.0 118
Appendice 7. Caso pratico 119
7.1. La storia 119
7.2. Processo P2: Analisi dei rischi 120
7.3. Processo P3: Gestione dei rischi 135

1. Introduzione a Magerit

Il CSAE[1] ha elaborato e promuove Magerit in risposta alla consapevolezza che l'amministrazione (ed in genere tutta la società) dipende in modo crescente dalla tecnologie informatiche per il raggiungimento dei suoi obiettivi di servizio. La ragion d'essere di Magerit è direttamente legata alla generalizzazione dell'uso dei mezzi elettronici, informatici e telematici, che comporta benefici evidenti per i cittadini; ma dà anche luogo a rischi che si devono ridurre a proporzioni minime con misure di sicurezza che contribuiscano a generare fiducia nell'uso di tali mezzi.

Nel periodo trascorso dalla pubblicazione della prima versione di Magerit (1997) fino alla data odierna, l'analisi dei rischi si è venuta consolidando come un passaggio necessario per la gestione della sicurezza. Così afferma chiaramente la guida dell'OCDE che, nel suo principio 6 riporta:

> *6) Valutazioni del rischio. I partecipanti devono portare a termine valutazioni del rischio.*

Questa metodologia interessa tutti quelli che impiegano informazioni trattate in modo automatizzato ed i sistemi informatici ad esse legati. Se tali informazioni o i servizi prestati grazie ad esse sono preziosi, questa metodologia permetterà di sapere quanto di questo valore è a rischio ed aiuterà a proteggerlo.

Conoscere il rischio a cui sono sottoposti gli elementi utilizzati è, semplicemente, indispensabile per poterli gestire ed è per questo motivo che sono comparse una moltitudine di guide informali, approssimazioni metodiche e strumenti di supporto, tutti mirati ad oggettivare l'analisi per determinare quanto sicuri (o insicuri) si è in maniera certa. La grande sfida di tutte queste approssimazioni è la complessità del problema che affrontano; complessità nel senso che ci sono molti elementi da considerare e, se non si è rigorosi, le conclusioni di tale esame saranno inevitabilmente poco affidabili. È per ciò che è necessario seguire un'approssimazione metodica che non lasci luogo all'improvvisazione, né dipenda dell'arbitrarietà dell'analista.

Malgrado si siano messe nelle mani dei sistemi informativi gravi responsabilità per raggiungere gli obiettivi delle organizzazioni, la preoccupazione per la loro sicurezza non cessa di essere un argomento ricorrente. Gli interessati, che spesso non sono tecnici, si domandano se questi sistemi meritano la loro fiducia, fiducia che diminuisce ad ogni inconveniente e, soprattutto, quando gli investimenti in misure di difesa del mezzo di lavoro non si traducono nell'assenza completa di inconvenienti. L'ideale sarebbe che i sistemi non avessero mai alcun problema ma è ovvio che si accetta di convivere con sistemi che ne hanno. Il punto non è tanto l'assenza di incidenti quanto la fiducia che essi siano sotto controllo: si sa che può succedere e si sa che cosa fare quando succede. Il timore di ciò che è ignoto è la principale origine della sfiducia e, in conseguenza, in questa sede l'approccio è di conoscere per avere fiducia: conoscere i rischi per poterli affrontare e controllare.

1.1. Obiettivi di Magerit

Magerit mira ai seguenti obiettivi:

Diretti:

1. rendere consapevole il responsabile dei sistemi informativi dell'esistenza dei rischi e del bisogno di considerarli in tempo;
2. offrire un metodo sistematico per analizzare tali rischi;
3. aiutare a scoprire e a pianificare le misure opportune per mantenere i rischi sotto controllo.

[1] CSAE: Consiglio Superiore dell'Amministrazione Elettronica.

Indiretti:

4. preparare l'organizzazione per processi di valutazione, audit, certificazione o accreditamento, a seconda dell'esigenza

Si è anche cercata l'uniformità delle relazioni che raccolgono le scoperte e le conclusioni di un progetto di analisi e gestione dei rischi:

Modello dei valori

Caratterizzazione del valore che hanno gli asset per l'organizzazione così come le dipendenze tra i differenti asset.

Mappa dei rischi

Relazione delle minacce a cui sono esposti gli asset.

Valutazione delle contromisure

Valutazione dell'efficacia delle contromisure esistenti in relazione al rischio che affrontano.

Stato di rischio

Caratterizzazione degli asset per il loro rischio residuo; cioè, per quello che può succedere avendo già preso in considerazione le contromisure realizzate.

Relazione delle debolezze

Assenza o debolezza delle contromisure che appaiono come opportune per ridurre i rischi verso il sistema.

Piano di sicurezza

Insieme di programmi di sicurezza che permettono di concretizzare le decisioni di gestione dei rischi

1.2. Introduzione all'analisi e alla gestione dei rischi

La sicurezza è la capacità delle reti o dei sistemi informativi di resistere, con un determinato livello di confidenza, agli incidenti o alle azioni illecite oppure ai malintenzionati che compromettano disponibilità, autenticità, integrità e riservatezza dei dati immagazzinati o trasmessi e dei servizi che dette reti e sistemi offrono o rendono accessibili.

L'obiettivo da proteggere è la missione dell'organizzazione, tenendo in considerazione le differenti dimensioni della sicurezza:

Disponibilità:

o disposizione dei servizi ad essere utilizzati quando sia necessario. La carenza di disponibilità può causare un'interruzione del servizio. La disponibilità riguarda direttamente la produttività delle organizzazioni.

Integrità:

o mantenimento delle caratteristiche di completezza e correttezza dei dati. Considerando l'integrità, le informazioni possono apparire manipolate, corrotte o incomplete. L'integrità riguarda direttamente il corretto svolgimento delle funzioni di un'organizzazione.

Riservatezza:

o che le informazioni arrivino solamente alle persone autorizzate. In detrimento alla riservatezza o al segreto possono esserci fughe e perdite di informazioni, così come accessi non autorizzati. La riservatezza è una proprietà difficile da ripristinare, potendosi compromettere la fiducia di altri nell'organizzazione non diligente nel mantenimento del segreto, e può causare l'inadempimento di leggi e requisiti contrattuali relativi alla custodia dei dati.

Autenticità (di chi fa uso di dati o servizi):

o che non esista dubbio di chi è responsabile di una informazione o della prestazione di un servizio, tanto al fine di avere fiducia di lui come di poterlo perseguire dopo eventuali inadempimenti o errori. In detrimento all'autenticità possono esserci sostituzioni ed inganni mirati a realizzare una frode. L'autenticità è la base per poter lottare contro il ripudio e, in quanto tale, fondamento per il commercio elettronico o per l'amministrazione elettronica, permettendo di avere fiducia senza bisogno di documenti cartacei né di presenzia fisica.

Tutte queste caratteristiche possono essere richieste o meno a seconda del caso. Quando sono richieste, non è evidente che si conseguano immediatamente. E' normale che siano necessari mezzi e tempo per conseguirle. A razionalizzare questo sforzo si dedicano le metodologie di analisi e gestione dei rischi che cominciano da una definizione:

Rischio:

stima del grado di esposizione per cui una minaccia si concretizza su uno o più asset causando danni o problemi all'organizzazione.

Il rischio indica quello che può accadere agli asset se non si proteggono adeguatamente. È importante sapere quali caratteristiche sono di interesse in ogni asset, così come sapere in che misura queste caratteristiche sono a rischio, in altre parole è importante analizzare il sistema:

Analisi dei rischi:

processo sistematico per stimare la grandezza dei rischi ai quali è esposta un'organizzazione.

Sapendo quello che potrebbe succedere, si devono prendere delle decisioni:

Gestione dei rischi:

selezione e realizzazione di contromisure per individuare, prevenire, impedire, ridurre o controllare i rischi identificati.

Si noti che un'opzione legittima è quella di accettare il rischio. È frequente sentir dire che la sicurezza assoluta non esiste; infatti si deve sempre accettare un rischio che però deve essere noto e subordinato al livello di qualità che si richiede al servizio.

Siccome tutto questo è molto delicato, non è meramente tecnico ed include la decisione di accettare un certo livello di rischio. Diviene quindi necessario sapere in che condizioni si lavora così da poter conoscere la fiducia che merita il sistema. Perciò cosa c'è di meglio che un'approssimazione metodica la quale permetta di prendere decisioni motivate e di spiegare razionalmente le decisioni prese?

1.3. L'analisi e gestione dei rischi nel suo contesto

Le attività di analisi e gestione dei rischi non sono fini a sé stesse ma fanno parte della gestione continua della sicurezza.

L'analisi dei rischi permette di determinare quali sono, quanto valgono e come sono protetti gli asset. In combinazione con gli obiettivi, la strategia e le politiche dell'organizzazione, le attività di gestione dei rischi permettono di elaborare un piano di sicurezza che, impostato e realizzato, soddisfi gli obiettivi impostati attraverso il livello di rischio accettato dalla direzione.

La realizzazione delle contromisure di sicurezza richiede un'organizzazione gestita e la partecipazione informata di tutto il personale che lavora con i sistemi informativi. È questo personale il responsabile dell'operatività giornaliera, della reazione agli incidenti e del monitoraggio in genere del sistema per determinare se soddisfa con efficacia ed efficienza gli obiettivi preposti.

Questo schema di lavoro deve essere ciclico perché i sistemi informativi sono raramente immutabili; sono piuttosto soggetti ad evoluzione continua tanto propria (nuovi asset) quanto dell'ambiente (nuove minacce), cosa che esige una revisione periodica di ciò che si impara dall'esperienza e si adatta al

nuovo contesto.

L'analisi dei rischi fornisce un modello del sistema in termini di asset, minacce e contromisure, ed è fondamentale per controllare tutte le attività con un fondamento. La gestione dei rischi è l'organizzazione delle azioni di sicurezza per soddisfare le necessità evidenziate dall'analisi.

1.3.1. Consapevolezza e formazione

Il migliore piano di sicurezza si vedrebbe seriamente compromesso senza una collaborazione attiva delle persone preposte ai sistemi informativi, specialmente se l'atteggiamento è negativo, contrario o di "lottare contro le misure di sicurezza". È per ciò che si richiede la creazione di una "cultura della sicurezza" che, emanandosi dall'Alta direzione, consapevolizzi tutti gli interessati della sua necessarietà e pertinenza.

Sono due i pilastri fondamentali per la creazione di questa cultura:

- una politica di sicurezza aziendale comprensibile (emanata da coloro i quali non sono esperti della materia), che sia diffusa e che sia mantenuta aggiornata
- una formazione continua a tutti i livelli, ricordando le misure di cautela abitudinarie e le attività specialistiche, secondo la responsabilità associata ad ogni posto di lavoro

al fine che queste attività riescano nell'organizzazione, è necessario che la sicurezza sia

- minimamente intrusiva: che non renda inutilmente difficile l'attività giornaliera né comprometta il raggiungimento degli obiettivi di produttività proposti,
- "naturale": che non dia origine ad errori gratuiti, che faciliti l'adempimento delle buone prassi proposte,
- praticata dalla direzione: che dia esempio nell'attività giornaliera e reagisca con sollecitudine a cambiamenti ed incidenti.

1.3.2. Incidenti e ripristino

Allo stesso tempo, le persone interessate devono essere consce del loro ruolo e della sua rilevanza continua per prevenire problemi e per reagire quando capitino. È importante creare una cultura di responsabilità dove i potenziali problemi, scoperti da quelli che stanno vicini all'asset interessato, possono essere incanalati verso i punti di decisione. In questo modo il sistema di contromisure risponderà alla realtà.

Quando capita un incidente, il tempo comincia a correre a sfavore del sistema: la sua sopravvivenza dipende della tempestività e dalla correttezza delle attività di notifica e reazione. Qualsiasi errore, imprecisione o ambiguità in questi momenti critici, si vede amplificato trasformando quello che poteva essere un semplice incidente in un disastro.

E' conveniente imparare tanto dai successi come dai fallimenti ed incorporarli al processo di analisi e gestione dei rischi. La maturità di un'organizzazione si riflette nell'accuratezza e nel realismo del suo modello di valorizzazione e, di conseguenza, nell'idoneità delle contromisure di ogni tipo, dalle misure tecniche fino ad un'ottima organizzazione.

1.4. Organizzazione delle guide

Questa versione 2 di Magerit è strutturata in tre libri: il presente, che descrive "il metodo", un "catalogo degli elementi" ed una "guida alle tecniche".

Questa guida descrive la metodologia da tre punti di vista:

- Il capitolo 2 descrive i passi per realizzare un'analisi dello stato del rischio e per gestire la

sua mitigazione. È una presentazione chiaramente concettuale.

- Il capitolo 3 descrive i compiti basilari per realizzare un progetto di analisi e gestione dei rischi, sottolineando che non basta avere chiari i concetti, ma che è opportuno definire ruoli, attività, milestones e documentazione affinché la realizzazione del progetto di analisi e gestione dei rischi sia sotto controllo in ogni momento.
- Il capitolo 4 applica la metodologia a un caso di sviluppo di sistemi informativi, nella prospettiva in cui i progetti di sviluppo dei sistemi devono tenere in considerazione i rischi dal primo momento, tanto quelli ai quali sono esposti direttamente, quanto quelli che le stesse applicazioni introducono nel sistema.

Come conclusione, il capitolo 5 tratta una serie di aspetti pratici, derivati dell'esperienza accumulata nel tempo, per la realizzazione di un'analisi ed una gestione realmente efficaci.

Le appendici raccolgono materiale di consultazione:

1. un glossario,
2. riferimenti bibliografici considerati per lo sviluppo di questa metodologia,
3. riferimenti alla cornice legale che inquadra i compiti di analisi e gestione dei rischi,
4. la cornice normativa di valorizzazione e certificazione,
5. le caratteristiche che si richiedono agli strumenti, presenti o futuri, per supportare il processo di analisi e gestione dei rischi,
6. una guida comparativa di come Magerit versione 1 si è evoluta in questa versione 2.

Infine, si sviluppa un caso pratico come esempio.

1.4.1. Modo di impiego

I lettori nuovi alla materia sono invitati a cominciare dal capitolo 2.

Se si ha già una familiarità dei concetti, l'esempio aiuta ad inquadrare idee e terminologia.

Se si sta iniziando un progetto di analisi e gestione dei rischi, il capitolo 3 aiuta a strutturarlo e a pianificarlo. Se il sistema informativo è semplice e ridotto oppure se si richiede solo una prima approssimazione, può bastare un'impostazione informale; ma quando il progetto prende importanza è opportuno essere metodici.

Se si sta realizzando un progetto di analisi e gestione dei rischi, il capitolo 5 aiuta ad inquadrare l'attività immediatamente.

Se si collabora ad un progetto di sviluppo di un nuovo sistema informativo, o ad un ciclo di manutenzione, è opportuno ricorrere al capitolo 4.

Se si prevede di lavorare con sistemi omologati, sia perché interessa come meccanismo per specificare quello di cui si ha bisogno, sia perché interessa come meccanismo per specificare quello che si ha, è opportuno ricorrere all'appendice 4.

Nell'impostazione di queste guide si è seguito un criterio "di massima", considerando tutti i tipi di asset, tutti gli aspetti di sicurezza, tutti i tipi di situazioni definitivamente parlando. Nella pratica, l'utente può trovarsi davanti a situazioni dove l'analisi è più ristretta. Seguono alcuni casi pratici frequenti:

- si richiede solo uno studio degli archivi elettronici interessati dalla legislazione sui dati di carattere personale;
- si richiede solo uno studio delle garanzie di riservatezza delle informazioni;

- si richiede solo uno studio sulla disponibilità dei servizi (tipico perché si cerca lo sviluppo di un piano di continuità);
- etc.

Queste situazioni, frequentemente, si raccolgono formalmente nell'attività A1.2, mentre informalmente si considera che è costruttivo concentrarsi in un ambito ridotto e procedere con il suo ampliamento a seconda dei requisiti, anziché affrontare subito tutto insieme.

1.4.2. Il catalogo degli elementi

In un libro a parte, si propone un catalogo, aperto ad ampliamenti, che individua alcune linee guida circa:

- tipi di asset;
- dimensioni di valorizzazione degli asset;
- criteri di valorizzazione degli asset;
- minacce tipiche sui sistemi informativi;
- contromisure da considerare per proteggere i sistemi informativi.

Si perseguono due obiettivi:

1. Facilitare il lavoro delle persone che lavorano al progetto, offrendo loro elementi standard con cui si possa familiarizzare rapidamente, concentrandosi nello specifico del sistema oggetto dell'analisi.
2. Omogeneizzare i risultati dell'analisi, promuovendo una terminologia ed alcuni criteri uniformi che permettano di paragonare ed integrare analisi realizzate per differenti sistemi.

Ogni sezione include una notazione XML che si utilizzerà per pubblicare regolarmente gli elementi in un formato standard capace di essere elaborato automaticamente da strumenti di analisi e gestione.

Se il lettore usa uno strumento di analisi e gestione dei rischi, questo catalogo sarà parte dello stesso; se l'analisi si realizza a mano, questo catalogo fornirà un'amplia base di partenza per avanzare rapidamente senza distrazioni né dimenticanze.

1.4.3. La guida alle tecniche

In un libro a parte, si apporta maggiore chiarezza e guida su alcune tecniche che si impiegano abitualmente per portare a termine progetti di analisi e gestione dei rischi:

- tecniche specifiche per l'analisi dei rischi;
  - analisi mediante tavole;
  - analisi algoritmica;
  - alberi di attacco.
- tecniche generali;
  - analisi di costi-benefici;
  - diagrammi di flusso di dati;
  - diagrammi di processi;
  - tecniche grafiche;
  - pianificazione di progetti;

- sessioni di lavoro: interviste, riunioni e presentazioni;
- valorizzazione Delphi.

Si tratta di una guida per la consultazione. Mano a mano che il lettore avanza per le attività del progetto, si gli raccomanderà l'uso di certe tecniche specifiche, delle quali questa guida cerca di essere un'introduzione, così come di fornire riferimenti affinché il lettore approfondisca autonomamente le tecniche presentate.

1.5. Per chi ha lavorato con Magerit v1.0

A coloro i quali hanno lavorato con Magerit v1.0, tutti i concetti risulteranno familiari, sebbene ci sia una certa evoluzione. In particolare si riconoscerà quello che si chiamava sottomodello di elementi: asset, minacce, vulnerabilità, impatti, rischi e contromisure. Questa parte concettuale è stata aggiornata a causa del trascorrere del tempo e continua ad essere l'asse intorno al quale si articolano le fasi fondamentali di analisi e gestione. Si è corretto ed ampliato ciò che si chiamava "sottostati di sicurezza" dandogli il nuovo nome di "dimensioni" ed introducendo nuove unità di misura per dare un valore agli aspetti di interesse degli asset. Il sottomodello di processi appare sotto l'epigrafe di "strutturazione del progetto di analisi e gestione dei rischi".

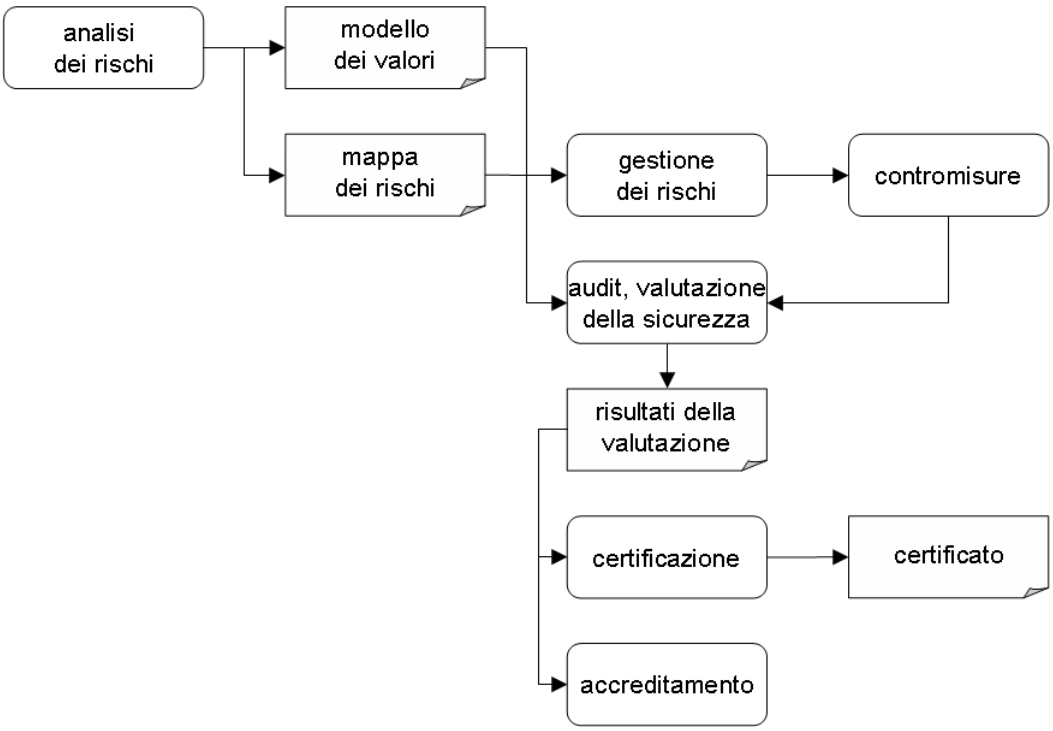
Sebbene Magerit v1.0 abbia resistito bene al passare del tempo dal lato concettuale, non si può dire lo stesso dei dettagli tecnici dei sistemi informativi con i quali si lavora. Si effettua un aggiornamento ma innanzi tutto si vuole differenziare quello che è essenziale (e permanente) da quello che è congiunturale e cambierà con il tempo. Questo si traduce in una parametrizzazione del metodo di lavoro, collegandolo a cataloghi esterni di minacce e contromisure che si potranno aggiornare, adattandosi al passare del tempo, tanto per il progresso tecnologico quanto per il progredire dell'ambiente, perché è certo tanto che i sistemi cambino quanto che lo facciano le entità al loro intorno, in meglio e in peggio. Inoltre, quanto più successo hanno i sistemi, tanti più utenti avranno anche simultaneamente, quindi tanti più soggetti saranno interessati nel loro abuso o, semplicemente, nella loro distruzione. Così quindi, resta il metodo: aperto. In modo che, restando chiaro che cosa si deve fare e come, si possano adattare i dettagli ad ogni momento.

In pratica, il paragrafo precedente si traduce nel fatto che si sono isolati in un libro allegato, il "catalogo degli elementi", i tipi di asset, le dimensioni e i criteri di valorizzazione, il catalogo delle minacce ed il catalogo delle contromisure, in modo che possono evolvere.

L'appendice 6 è più precisa stabilendo le corrispondenze tra la versione 1.0 e questa.

1.6. Valutazione, certificazione, audit e accreditamento

L'analisi dei rischi è un punto focale dei processi di valutazione, certificazione, audit ed accreditamento che danno forma ufficiale alla fiducia che merita un sistema informativo. Dato che non esistono due sistemi informativi uguali, la valutazione di ogni sistema concreto richiede di adattarsi ai componenti che lo costituiscono. Un'analisi dei rischi fornisce una visione singolare di com'è ogni sistema, che valore possiede, a quali minacce è esposto e di che contromisure è dotato. L'analisi dei rischi è quindi un passaggio obbligato per potere portare a termine tutti i compiti menzionati, messi in relazione secondo il seguente schema:



In questa sezione si presentano concettualmente le attività citate. Il lettore troverà nell'appendice 4 un trattamento specifico degli ambiti normativi relativi ai sistemi di gestione ed ai prodotti di sicurezza.

Valutazione

È sempre più frequente la valutazione della sicurezza dei sistemi informativi, tanto internamente come parte dei processi di gestione, quanto attraverso periti indipendenti esterni. Le valutazioni permettono di misurare il grado di fiducia che un sistema informativo merita.

Certificazione

La valutazione può portare ad una certificazione ufficiale della sicurezza del sistema. Nella pratica si certificano prodotti e si certificano sistemi di gestione della sicurezza. La certificazione di prodotti è, in un certo senso, impersonale: "questo ha queste caratteristiche tecniche". Tuttavia, la certificazione di sistemi di gestione ha a che vedere con il "componente umano" delle organizzazioni cercando l'analisi di come si utilizzano i sistemi.

Certificare è assicurare in modo responsabile e per iscritto un comportamento. Quello che si certifica, prodotto o sistema, è sottoposto ad una serie di valutazioni orientate verso un obiettivo individuabile dal quesito "perché lo si vuole?". Un certificato dice che un sistema è capace di proteggere alcuni dati di alcune minacce con una certa qualità (capacità di protezione), affermandolo in base all'osservazione dell'esistenza e del funzionamento di una serie di contromisure. Il tutto per dire che dietro ad un certificato non vi sono altro che gli stessi concetti di un'analisi dei rischi.

Prima di procedere alla certificazione, deve essersi realizzata un'analisi dei rischi a fine di conoscere i rischi e di controllarli mediante l'adozione di contromisure adeguate. Questa, inoltre, rappresenta un punto di controllo importante della gestione del prodotto o sistema.

Accreditamento

Alcune certificazioni hanno come oggetto l'accreditamento del prodotto o del sistema.

L'accreditamento è un processo specifico il cui obiettivo è legittimare il sistema a essere parte di sistemi più ampi. Lo si può vedere come una certificazione per un proposito specifico.

Audit

Sebbene non sia la stessa cosa, non sono molto lontani da questo mondo gli audit, interni o esterni, a cui si sottopongono i sistemi informativi:

- alcune volte richiesti dalla legge per poter operare in un certo settore,
- altre volte richiesti dalla stessa direzione dell'organizzazione,
- altre volte richiesti da entità con cui si collabora che hanno il proprio livello di rischio legato al nostro.

Un'audit può servirsi di un'analisi dei rischi che gli permetta (1) di sapere che cosa c'è in gioco, (2) sapere a che cosa è esposto il sistema e (3) valutare l'efficacia e l'efficienza delle contromisure.

Frequentemente gli auditor partono da un'analisi dei rischi, implicita o esplicita, che o realizzano loro stessi o sottopongono ad audit. Nelle prime fasi dell'audit è sempre difficile discorrere di quello che non si conosce. A partire dall'analisi dei rischi si può analizzare il sistema ed informare la direzione se il sistema è sotto controllo; cioè, se le misure di sicurezza adottate sono giustificate, realizzate e monitorate in modo che si possa avere fiducia nel sistema di indicatori di cui dispone la direzione per gestire la sicurezza dei sistemi.

La conclusione dell'audit è una relazione di debolezze scoperte, che non sono altro che le inconsistenze tra le necessità individuate nell'analisi dei rischi e la realtà scoperte durante l'ispezione del sistema durante l'operatività quotidiana.

> Il rapporto di audit dovrà dare un parere sull'adeguatezza delle misure e dei controlli del presente regolamento, identificare le sue deficienze e proporre le misure correttive o complementari necessarie. Dovrà, ugualmente, includere i dati, fatti oggettivi e le osservazioni su cui si fondino i dettami raggiunti e le raccomandazioni proposte. [RD 994/1999, articolo 17.2]

Nel caso della pubblica amministrazione spagnola, esistono alcuni riferimenti fondamentali rispetto ai quali si può e si deve realizzare un audit:

- Real Decreto 994/1999, dell' 11 di giugno, per il quale si approva il regolamento di misure di sicurezza dei file automatizzati che contengano dati di carattere personale.
- "Criteri di sicurezza, normalizzazione e conservazione delle applicazioni utilizzate per l'esercizio di potestà", MAP, 2004

Gli audit devono ripetersi regolarmente tanto per seguire l'evoluzione dell'analisi dei rischi (che si deve aggiornare regolarmente) quanto per seguire lo sviluppo del piano di sicurezza determinato dalle attività di gestione dei rischi.

1.7. Quando occorre analizzare e gestire i rischi?

Realizzare un'analisi dei rischi è laborioso e costoso. Creare una mappa degli asset e valorizzarli richiede la collaborazione di molti profili all'interno dell'organizzazione, dai livelli di direzione fino a quelli tecnici. E non è solo necessario coinvolgere molte persone, ma si deve ottenere un'uniformità di criterio tra tutti perché, se è importante quantificare i rischi, più importante ancora è renderli comparabili. Questo perché è normale che in un'analisi dei rischi appaiano una moltitudine di dati. L'unico modo di affrontare la complessità è concentrarsi sui più importanti (massimo impatto, massimo rischio) ed ovviare quello che è secondario o addirittura trascurabile. Ma se i dati non sono bene ordinati in termini relativi, la loro interpretazione è impossibile.

Riassumendo, un'analisi dei rischi non è un compito secondario che realizza chiunque nei suoi

momenti liberi. È un'attività primaria che richiede impegno e coordinazione. Pertanto deve essere adeguatamente pianificata e giustificata.

Un'analisi dei rischi è raccomandabile in qualsiasi organizzazione che dipenda da sistemi informativi e di comunicazioni per il raggiungimento dei suoi obiettivi. In particolare in qualsiasi ambiente dove si effettuino trasmissioni elettroniche di beni e servizi, sia in ambito pubblico che privato. L'analisi dei rischi permette di prendere decisioni su investimenti in tecnologia, dall'acquisto di apparecchiature di produzione fino all'allestimento di un centro alternativo per assicurare la continuità operativa, passando per le decisioni di acquisto di contromisure tecniche e di selezione ed abilitazione del personale.

L'analisi dei rischi è uno strumento di gestione che permette di prendere decisioni. Le decisioni possono essere prese prima di realizzare un servizio o prima di metterlo in funzione. È molto desiderabile farlo prima, in modo che le misure da prendere si incorporino nel disegno del servizio, nella scelta di componenti, nello sviluppo delle applicazioni e nei manuali utente. Tutto quello che è correggere rischi imprevisti è costoso sia in tempo proprio che altrui, il che può andare a danno dell'immagine dell'organizzazione e può comportare, in casi estremi, la perdita di fiducia nelle sue capacità. Si è sempre detto che è meglio prevenire che curare e qui si applica in modo diretto: non si aspetti che un servizio faccia acqua; lo si deve prevenire ed essere preparati.

Per motivi legali

L'analisi dei rischi può venire richiesta per motivi legali. Questo è il caso del Real Decreto 263/1996, del 16 di febbraio, per quello che riguarda l'utilizzazione di tecniche elettroniche, informatiche e telematiche per l'amministrazione generale dello stato. Nel suo articolo 4 (garanzie generali dell'utilizzazione di supporti, mezzi ed applicazioni elettroniche, informatiche e telematiche) dice così:

2. Quando si utilizzino supporti, mezzi ed applicazioni riferiti nel paragrafo precedente, si adotteranno le misure tecniche ed organizzative necessarie ad assicurare autenticità, riservatezza, integrità, disponibilità e conservazione delle informazioni. Tali misure di sicurezza dovranno tenere in considerazione lo stato della tecnologia ed essere proporzionate alla natura dei dati e dei trattamenti ed *ai rischi a cui sono esposti*.

In forma simile, la Legge Organica 15/1999, di 13 di dicembre, di protezione di dati di carattere personale, nel suo articolo 9 (sicurezza dei dati) dice così:

1. Il responsabile dei file, e, nel suo caso, l'incaricato del trattamento, dovranno adottare le misure di natura tecnica ed organizzativa necessarie a garantire la sicurezza dei dati di carattere personale ed evitare la loro alterazione, perdita, trattamento o accesso non autorizzato, considerando lo stato della tecnologia, la natura dei dati immagazzinati e *i rischi a cui sono esposti,* che provengono dall'azione umana o da agenti fisici oppure naturali.

Testo che si riprende ancora nel preambolo al Real Decreto 994/1999, dell'11 di giugno, per il quale si approva il regolamento di misure di sicurezza dei file automatizzati che contengono dati di carattere personale. In questo decreto si raccoglie l'obbligo di elaborare un documento di sicurezza:

1. Il responsabile del file elaborerà e realizzerà la normativa di sicurezza mediante un documento di rispetto obbligatorio per il personale con accesso ai dati automatizzati di carattere personale ed ai sistemi informativi.

Difficilmente si può sviluppare detto documento senza un'analisi previa dei rischi sui dati, analisi che porti a determinare le misure di sicurezza pertinenti.

N.d.T.: In ambito italiano si fa riferimento al comma 3 dell'art.19 dell'allegato B al d.lgs 196/2003 per la protezione dei dati personali, il quale richiede "l'analisi dei rischi che incombono sui dati".

Certificazione ed accreditamento

Se il sistema aspira ad una certificazione, l'analisi dei rischi è un requisito preventivo che sarà richiesto dal valutatore. È la fonte di informazioni per determinare la relazione di contromisure rilevanti per il sistema e che quindi devono essere esaminate. Si veda l'appendice 4.1 sulle certificazione dei sistemi di gestione della sicurezza delle informazioni (SGSI).

L'analisi dei rischi è essa stessa un requisito nei processi di accreditamento di sistemi. Questi processi sono necessari quando si va a trattare un sistema informativo militare classificato su base nazionale, UE, NATO o di altri organismi internazionali. Il primo passo del processo è la realizzazione dell'analisi dei rischi che identifichi minacce e contromisure e gestisca in modo soddisfacente i rischi del sistema.

Infine, è rilevante menzionare l'impiego di profili di protezione come meccanismo di contrattazione. I profili di protezione (ISO/IEC-15408) nascono con la doppia missione di poter definire a priori i requisiti di sicurezza di un sistema (per il suo acquisto o per il suo sviluppo) e di poter sfruttare il valore internazionale del significato di una certificazione. Nell'uno o nell'altro caso, stabilisce l'unità di misura rispetto a cui si qualificherà l'idoneità della sicurezza del sistema. Si veda l'appendice 4.2 sui Common Criteria.

In conclusione

Occorre analizzare e gestire i rischi quando questo sia stabilito direttamente o indirettamente da un requisito legale ed ogni volta che lo richieda un’attività di protezione responsabile degli asset di un'organizzazione.

2. Realizzazione dell'analisi e della gestione

Questo capitolo espone concettualmente in che cosa consiste l'analisi dei rischi e la sua gestione, che cosa si ricerca in ogni suo momento e quali conclusioni si derivano.

Ci sono due compiti principali da realizzare:

I. analisi dei rischi,

che permette di determinare ciò che l'organizzazione possiede e di stimare quello che potrebbe succedere.

Elementi:

1. asset, che sono gli elementi dei sistemi informativi (o strettamente relazionati con questi) che danno valore all'organizzazione
2. minacce, che sono ciò che può succedere all'asset causando un danno all'organizzazione
3. contromisure (o controlli), che sono gli elementi di difesa realizzati affinché le minacce non causino [tanto] danno.

Con questi elementi si può stimare:

1. l'impatto: quello che potrebbe succedere
2. il rischio: quello che probabilmente succederà

L'analisi dei rischi permette di analizzare questi elementi in modo metodico per giungere a conclusioni fondate

II. gestione dei rischi,

che permette di organizzare la difesa in modo coscienzioso e prudente, operando affinché non succeda niente di negativo ed al tempo contribuendo ad affrontare le emergenze, a sopravvivere agli incidenti e a continuare ad operare nelle migliori condizioni; dato che niente è perfetto, si dichiara che il rischio è ridotto ad un livello residuo che la direzione accetta.

Informalmente, si può dire che la gestione della sicurezza di un sistema informativo è la gestione dei suoi rischi e che l'analisi permette di razionalizzare detta gestione.

2.1. Analisi dei rischi

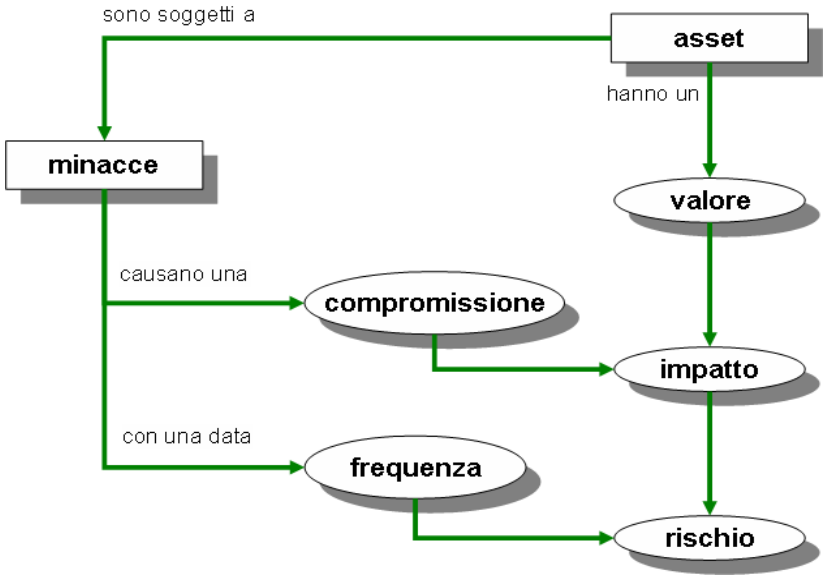
L'analisi dei rischi è un'approssimazione metodica per determinare il rischio seguendo alcuni passi programmati:

1. determinare gli asset rilevanti per l'organizzazione, le loro interrelazioni ed il loro valore, nel senso del danno (costo) che causa una loro compromissione;
2. determinare a quali minacce sono esposti quegli asset;
3. determinare o quali contromisure sono implementate e quanto sono efficaci rispetto al rischio
4. stimare l'impatto, definito come il danno sull'asset derivante dalla concretizzazione della minaccia;
5. stimare il rischio, definito come l'impatto ponderato con la frequenza di occorrenza (o aspettativa di concretizzazione) della minaccia.

Con l'obiettivo di organizzare la presentazione degli argomenti si considerano prima i passi 1, 2, 4 e 5, considerando quindi che le stime di impatto e rischio siano "potenziali": casi in cui non si ha contromisura alcuna dispiegata. Una volta ottenuto questo scenario teorico, si aggiungono le

contromisure del passo 3, derivando stime realistiche di impatto e rischio.

La seguente figura riassume questo primo percorso, i cui passi sono dettagliati nelle seguenti sezioni:



2.1.1. Passo 1: Asset

Sono definiti asset le **risorse proprie del sistema informativo o ad esso collegate, necessarie affinché l'organizzazione operi correttamente e raggiunga gli obiettivi preposti dalla sua direzione.**

L'asset centrale sono le informazioni trattate dal sistema; cioè i dati. Intorno ad essi si possono identificare altri asset rilevanti:

I servizi che si possono prestare grazie ai dati, ed i servizi di cui si ha bisogno per poter gestire detti dati.

Le applicazioni informatiche *(software)* che permettono di trattare i dati.

Le apparecchiature informatiche *(hardware)* che permettono di memorizzare e impiegare dati, applicazioni e servizi.

I supporti di memorizzazione che sono dispositivi di immagazzinamento di dati.

Le apparecchiature ausiliarie che supportano il materiale informatico.

Le reti di comunicazioni che permettono di scambiare dati.

I siti che accolgono le apparecchiature informatiche e di comunicazione.

Il personale che impiega od opera gli elementi precedentemente citati.

Tipi di asset

Non tutti gli asset sono dello stesso tipo. A seconda del tipo di asset, le minacce e le contromisure sono differenti. Il capitolo 2 del "catalogo degli elementi" presenta uno schema dei tipi di asset.

Se il sistema tratta dati di carattere personale, questi solgono essere importanti di per sé stessi e richiedono una serie di contromisure, spesso definite per legge. Per questi asset interessa determinare che modalità di trattamento si devono imporre. Il fatto che un dato sia di carattere personale impatta tutti gli asset coinvolti nel suo trattamento.

Lo stesso avviene con i dati sottoposti ad una classificazione di riservatezza. Quando si dice che un certo documento è classificato come *"riservato",* nel senso che le copie sono numerate, possono solo arrivare a certe persone, non devono uscire dall'azienda e devono essere distrutte in modo controllato etc. si stanno imponendo una serie di contromisure perché lo richiede il regolamento, settoriale o specifico dell'organizzazione.

Dipendenze

Gli asset che richiamano più immediatamente l'attenzione solgono essere le informazioni ed i servizi; ma questi asset dipendono di altri più tradizionali come possono essere le apparecchiature, le comunicazioni o le frequentemente dimenticate persone che lavorano con essi. Per questo è importante il concetto di "dipendenze tra asset" o la misura in cui un asset *superiore* si vede influenzato da un incidente di sicurezza in un asset *inferiore.*

Si dice che un "asset superiore" dipende da un altro "asset inferiore" quando i requisiti di sicurezza del superiore si riflettono nei requisiti di sicurezza dell'inferiore. Detto con altre parole, quando la concretizzazione di una minaccia sull'asset inferiore ha come conseguenza un danno sull'asset superiore. Informalmente si può considerare che gli asset inferiori sono i piloni su cui si appoggia la sicurezza degli asset superiori.

Sebbene in ogni caso ci si deve adattare all'organizzazione oggetto dell'analisi, spesso si può strutturare l'insieme degli asset in livelli, dove i livelli superiori dipendono dagli inferiori, secondo quanto segue:

- livello 1: **l'ambiente**: asset che operano a garanzia dei seguenti livelli
  - servizi infrastrutturali: energia, climatizzazione, comunicazioni
  - personale: di direzione, operativo, di sviluppo, etc.
  - altri: edifici, mobilio, etc.
- livello 2: **il sistema informativo** propriamente detto
  - apparecchiature informatiche (hardware)
  - applicazioni (software)
  - comunicazioni
  - supporti di memorizzazione: dischi, nastri, etc.
- livello 3: **le informazioni**
  - dati
  - meta-dati: strutture, indici, chiavi di cifratura, etc.
- livello 4: **le funzioni dell'organizzazione**, che giustificano l'esistenza del sistema informativo e gli danno un fine
  - obiettivi e missione
  - beni e servizi prodotti
- livello 5: **altri** asset
  - credibilità e buona immagine
  - conoscenza accumulata
  - indipendenza di giudizio o di azione
  - privacy delle persone

- incolumità delle persone

Valorizzazione

Perché interessa un asset? Per quello che vale.

Non si sta parlando di quello che costano gli asset, ma di quello che valgono. Se qualcosa non serve a nulla lo si può trascurare. Se non si può fare a meno di un asset senza incorrere in conseguenze è perché esso ha un valore. Si deve verificare questo aspetto in quanto un asset con valore è ciò che si deve proteggere.

Il valore può essere proprio, o può essere cumulativo. Si può affermare che gli asset inferiori in uno schema di dipendenze accumulano il valore degli asset che si appoggiano su di loro.

Il valore centrale è solito stare nelle informazioni (o dati) che il sistema tratta, lasciando gli altri asset relegati allo sfruttamento e alla protezione delle informazioni. D'altronde, i sistemi informativi sfruttano i dati per fornire servizi, interni all'organizzazione o destinati a terzi, basandosi su di una serie di informazioni necessarie. Senza entrare in dettagli tecnici di come si fa qualcosa, l'insieme di informazioni e servizi finali permette di caratterizzare funzionalmente un'organizzazione. Le dipendenze tra asset permettono di mettere in relazione gli altri asset con informazioni e servizi.

Dimensioni

Di un asset può essere d'interesse considerare differenti dimensioni:

- la sua **autenticità:** che danno causerebbe non sapere esattamente chi fa o ha fatto ogni azione?

  Questa valorizzazione è tipica dei servizi (autenticità dell'utente) e dei dati (autenticità di chi accede ai dati in scrittura o, semplicemente, in lettura)

- la sua **riservatezza**: che danno causerebbe il fatto che lo conoscesse chi non dovrebbe?

  Questa valorizzazione è tipica dei dati.

- la sua **integrità**: che danno causerebbe il suo danneggiamento o corruzione?

  Questa valorizzazione è tipica dei dati, che possono essere manipolati, essere totalmente o parzialmente falsi o incompleti.

- la sua **disponibilità**: che danno causerebbe non averlo più o non poterlo utilizzare?

  Questa valorizzazione è tipica dei servizi.

In sistemi dedicati all'amministrazione o al commercio elettronico, la conoscenza degli attori in gioco è fondamentale per poter prestare il servizio correttamente e poter ricostruire gli errori (casuali o deliberati) che potrebbero verificarsi. In questi asset, oltre all'autenticità, interessa considerare:

- la **tracciabilità** dell'uso del servizio: che danno causerebbe non sapere a chi si presta tale servizio? cioè, chi fa che cosa e quando?
- i **tracciabilità** dell'accesso ai dati: che danno causerebbe non sapere chi accede a quali dati e che cosa fa con essi?

Si riconoscono abitualmente le dimensioni basilari di: autenticità, riservatezza, integrità e disponibilità. In questa metodologia si è raffinato il concetto di autenticità per distinguere tra l'uso di un servizio e l'accesso ai dati. Si è inoltre introdotto il concetto di tracciabilità (dall'inglese *accountability)* preso delle guide ISO/IEC 13335, ugualmente diviso tra la tracciabilità del servizio e dei dati. Gli aspetti di autenticità e tracciabilità dei dati sono critici per soddisfare le misure regolamentari su archivi elettronici che contengano dati di carattere personale.

Il capitolo 3 del "catalogo degli elementi" presenta una relazione delle dimensioni di sicurezza.

In un albero di dipendenze, dove gli asset superiori dipendono da quelli inferiori, è irrinunciabile valutare gli asset superiori, quelli che sono importanti di per sé stessi. Questo valore si accumula automaticamente sugli inferiori, il che non è un impedimento al fatto che possano avere, in aggiunta, una loro valorizzazione propria.

quanto vale la "salute" degli asset?

Una volta determinato quali dimensioni (di sicurezza) sono rilevanti per un asset si deve procedere a valorizzarle. La valorizzazione è legata alla determinazione del costo necessario al recupero da un incidente che comprometta l'asset. Ci sono molti fattori da considerare:

- costo di rimpiazzamento: acquisto ed installazione;
- costo di mano d'opera (specializzata) impiegata per recuperare (il valore) dell'asset;
- cessazione di profitto: perdita di entrate;
- capacità operativa: fiducia degli utenti e dei fornitori che si traduce in una perdita di attività o in peggiori condizioni economiche;
- sanzioni per inadempimento della legge o obblighi contrattuali;
- danni ad altri asset, propri o altrui;
- danni a persone;
- danni ambientali;

La valorizzazione può essere quantitativa (con una quantità pecuniaria) o qualitativa (con una scala di livelli). I criteri più importanti da rispettare sono:

- **omogeneità**: è importante poter paragonare i valori sebbene siano associati a differenti dimensioni al fine di poter combinare valori propri e valori cumulativi, così come per poter determinare se il danno è più grave in una dimensione o in un'altra
- **relatività**: è importante poter normalizzare il valore di un asset rispetto ad altri asset

Tutti questi criteri si soddisfano usando valutazioni economiche (costo pecuniario richiesto per "curare" l'asset) ed è frequente la tentazione di dare un valore a tutto. Se si riesce, eccellente. E' facile associare un prezzo agli aspetti più tangibili (apparecchiature, ore di lavoro, etc.); ma entrando in valutazioni più astratte (asset intangibili come la credibilità dell'organizzazione) la valorizzazione economica esatta può essere ingannevole e motivo di disputa tra esperti.

Il capitolo 4 del "catalogo degli elementi" presenta alcune linee guida per la valorizzazione sistematica degli asset.

Valorizzazione qualitativa

Le scale qualitative permettono di avanzare con rapidità, posizionando il valore di ogni asset in un ordine relativo rispetto ad altri. È frequente impostare queste scale come "ordini di grandezza" e, di conseguenza, derivarne stime sull'ordine di grandezza del rischio.

La limitazione delle valorizzazioni qualitative è che non permettono di paragonare valori più in là del loro ordine relativo. Non si possono sommare valori.

Il capitolo 8.1 del "guida alle tecniche" presenta un modello di analisi basato su valorizzazioni qualitative.

Valorizzazione quantitativa

Le valorizzazioni numeriche assolute necessitano molto impegno, ma non soffrono dei problemi delle valorizzazioni qualitative. Sommare valori numerici è assolutamente "naturale" e l'interpretazione delle somme non è mai motivo di controversia.

Se la valorizzazione è pecuniaria, inoltre si possono fare studi economici paragonando quello che si rischia con quello che costa la soluzione rispondendo quindi alle domande:

- vale la pena investire tanto denaro in questa contromisura?
- che insieme di contromisure ottimizza l'investimento?
- in quanto tempo si ricupera l'investimento?
- quanto è ragionevole che costi il premio di un'assicurazione?

Il capitolo 8.2 del "guida alle tecniche" presenta un modello di analisi basato su valorizzazioni quantitative.

Il valore dell'interruzione del servizio

Quasi tutte le dimensioni menzionate precedentemente permettono una valorizzazione semplice, qualitativa o quantitativa ma c'è un'eccezione: la disponibilità.

Non è lo stesso interrompere un servizio per un'ora, per un giorno o per un mese. Può darsi che un'ora di interruzione sia irrilevante, mentre un giorno senza servizio causi un danno moderato; ma un mese di blocco potrebbe comportare la chiusura dell'attività. Il fattore negativo è che non esiste una proporzionalità tra il tempo di interruzione e le conseguenze.

Conseguentemente, per valutare l'interruzione della disponibilità di un asset si deve usare una struttura più complessa che si può riassumere visivamente come segue:



Nel grafo sono evidenti una serie di soglie di interruzione che terminano con la distruzione totale o permanente dell'asset. Nell'esempio illustrato, interruzioni fino a 6 ore si possono sostenere senza conseguenze. Alle 6 ore però si diramano allarmi che aumentano se il fermo supera i 2 giorni. e se questo supera il mese, si può dire che l'organizzazione ha perduto la sua capacità operativa: è finita. Dal punto di vista dei rimedi, la grafica dice direttamente che non si deve spendere nemmeno un euro per evitare fermi di meno di 6 ore. Vale invece una certa spesa impedire che un fermo superi le 6 ore o i 2 giorni. Quando si valuta quello che costa impedire che il fermo superi il mese, si deve mettere sulla bilancia tutto il valore dell'organizzazione a fronte del costo delle contromisure. Potrebbe anche essere che non ne valga la pena.

2.1.2. Passo 2: Minacce

Il seguente passo consiste nel determinare le minacce che possono interessare ogni asset. Le minacce sono "cose che accadono", e, di tutto quello che può accadere, è rilevante solo quello che può succedere al nostro asset e causargli un danno.

Esistono incidenti naturali (terremoti, inondazioni ...) e disastri industriali (contaminazione, sbalzi di tensione elettrica ...) a fronte dei quali il sistema informativo è una vittima passiva; non per questo si deve però rimanere indifesi. Ci sono minacce causate dalle persone, errori, attacchi intenzionali.

Il capitolo 5 del "catalogo degli elementi" presenta una relazione delle minacce tipiche.

Non tutte le minacce riguardano tutti gli asset, ma c'è una certa relazione tra il tipo di asset e quello che gli può accadere.

Valorizzazione delle minacce

Quando un asset è vittima di una minaccia, non si vede influenzato in tutte le sue dimensioni, né nello stesso modo all'interno di esse.

Una volta determinato che una minaccia può danneggiare un asset, si deve stimare quanto è vulnerabile l'asset, sotto due aspetti:

compromissione: come risulta danneggiato l'asset

frequenza: ogni quanto si concretizza la minaccia

La compromissione misura il danno causato da un incidente supponendo che accada.

La compromissione suole essere rappresentata come una frazione del valore dell'asset e in questo modo appaiono espressioni del tipo che un asset si è visto "totalmente compromesso", o "compromesso in minima parte". Quando le minacce non sono intenzionali, basta conoscere la frazione fisicamente danneggiata di un asset per calcolare la perdita proporzionale di valore. Ma quando la minaccia è intenzionale, non si può pensare in termini di proporzionalità alcuna perché l'attaccante può causare molti danni in modo selettivo.

La frequenza pone in prospettiva una compromissione, perché una minaccia può avere terribili conseguenze ma essere di improbabile concretizzazione; mentre un'altra minaccia può avere conseguenze molto basse, ma essere tanto frequente da finire per creare un danno considerevole.

La frequenza si rappresenta come un tasso annuale di occorrenza, con i seguenti valori tipici

100	molto frequente	ogni giorno
10	frequente	Mensile
1	normale	una volta all'anno
1/10	poco frequente	ogni vari anni

2.1.3. Passo 4: Determinazione dell'impatto

Si denomina impatto la misura del danno sull'asset derivato della concretizzazione di una minaccia. Conoscendo il valore dell'asset (in svariate dimensioni) e la compromissione che gli può causare una minaccia, è immediato derivare l'impatto che questa può avere sul sistema. L'unica considerazione che resta da fare è relativa alle dipendenze tra asset. È frequente che il valore del sistema informativo sia incentrato sui servizi che presta e sui dati che tratta, e al tempo stesso che le minacce si materializzino sui mezzi.

Impatto cumulativo

È calcolato su di un asset tenendo in considerazione

- il suo valore cumulativo (il proprio più quello degli asset che dipendono da lui)
- le minacce a cui è esposto

L'impatto cumulativo si calcola per ogni asset, per ogni minaccia ed in ogni dimensione di valorizzazione, essendo una funzione del valore cumulativo e della compromissione causata.

L'impatto è tanto più grande quanto maggiore è il valore proprio o cumulativo di un asset.

L'impatto è tanto più grande quanto maggiore è la compromissione dell'asset attaccato.

L'impatto cumulativo, calcolato sugli asset che sostengono il peso del sistema informativo, permette di determinare le contromisure di cui gli strumenti di lavoro devono essere dotati: protezione delle apparecchiature, copie di backup, etc.

Impatto riflesso

È calcolato su di un asset tenendo in considerazione

- il suo valore proprio
- le minacce a cui sono esposti gli asset dai quali dipende

L'impatto riflesso si calcola per ogni asset, per ogni minaccia ed in ogni dimensione di valorizzazione, essendo una funzione del valore proprio e della compromissione causata.

L'impatto è tanto più grande quanto maggiore è il valore proprio di un asset.

L'impatto è tanto più grande quanto maggiore è la compromissione dell'asset attaccato.

L'impatto è tanto più grande quanto maggiore è la dipendenza dell'asset attaccato.

L'impatto riflesso, calcolato sugli asset che hanno valore proprio, permette di determinare le conseguenze degli incidenti tecnici sulla missione del sistema informativo. Offre quindi una visione gestionale che aiuta a prendere una delle decisioni più critiche di un'analisi dei rischi: accettare un certo livello di rischio.

Aggregazione di valori di impatto

I paragrafi precedenti determinano l'impatto che una minaccia ha su un asset in una certa dimensione. Questi impatti singolari possono essere aggregati sotto certi condizioni:

- si può aggregare l'impatto riflesso su differenti asset,
- si può aggregare l'impatto cumulativo su asset che non sono dipendenti tra di loro, né dipendono da nessun asset superiore comune,
- non si deve aggregare l'impatto cumulativo su asset a meno che siano indipendenti, perché ciò porterebbe a sopravvalutare l'impatto includendo svariate volte il valore cumulativo di asset superiori,
- si può aggregare l'impatto di differenti minacce su di uno stesso asset, sebbene sia opportuno considerare in che misura le differenti minacce siano indipendenti e possano essere concorrenti,
- si può aggregare l'impatto di una minaccia in differenti dimensioni.

2.1.4. Passo 5: Determinazione del rischio

Si denomina rischio la misura del danno probabile su un sistema. Conoscendo l'impatto delle minacce sull'asset, è immediato derivare il rischio senza considerare altro che la frequenza di occorrenza.

Il rischio cresce con l'impatto e con la frequenza.

Rischio cumulativo

È calcolato su di un asset tenendo in considerazione

- l'impatto cumulativo su di un asset dovuto ad una minaccia e
- la frequenza della minaccia.

Il rischio cumulativo si calcola per ogni asset, per ogni minaccia ed in ogni dimensione di valorizzazione, essendo una funzione del valore cumulativo, della compromissione causata e della frequenza della minaccia.

Il rischio cumulativo, calcolato sugli asset che sostengono il peso del sistema informativo, permette di determinare le contromisure di cui gli strumenti di lavoro devono essere dotati: protezione delle apparecchiature, copie di backup, etc.

Rischio riflesso

È calcolato su di un asset tenendo in considerazione

- l'impatto riflesso su di un asset dovuto ad una minaccia e
- la frequenza della minaccia.

Il rischio riflesso si calcola per ogni asset, per ogni minaccia ed in ogni dimensione di valorizzazione, essendo una funzione del valore proprio, la compromissione causata e la frequenza della minaccia.

Il rischio riflesso, calcolato sugli asset che hanno valore proprio, permette di determinare le conseguenze degli incidenti tecnici sulla missione del sistema informativo. Offre quindi una visione gestionale che aiuta a prendere una delle decisioni più critiche di un'analisi dei rischi: accettare un certo livello di rischio.

Aggregazione di rischi

I paragrafi precedenti determinano il rischio che una minaccia genera su di un asset in una certa dimensione. Questi rischi singoli possono aggregare si sotto certi condizioni:

- si può aggregare il rischio riflesso su differenti asset,
- si può aggregare il rischio cumulativo su asset che non sono dipendenti tra loro, né dipendono da nessun asset superiore comune,
- non si deve aggregare il rischio cumulativo su asset a meno che siano indipendenti, perché ciò porterebbe a sopravvalutare il rischio, includendo svariate volte il valore cumulativo di asset superiori,
- si può aggregare il rischio di differenti minacce su di uno stesso asset, sebbene sia opportuno considerare in che misura le differenti minacce siano indipendenti e possano essere concorrenti,
- si può aggregare il rischio di una minaccia in differenti dimensioni.

2.1.5. Passo 3: Contromisure

Nei passi precedenti non sono tenute in considerazione le contromisure dispiegate. Si misurano,

pertanto, gli impatti e i rischi a cui sono esposti gli asset se non si proteggessero affatto. In pratica non è frequente trovare sistemi senza protezione: i valori calcolati finora indicano quello che accadrebbe se si disattivassero le contromisure presenti.

Si definiscono le contromisure o controlli le procedure e i mezzi tecnologici che riducono il rischio. Esistono minacce che possono essere scongiurate semplicemente organizzandosi adeguatamente, altre richiedono elementi tecnici (programmi o apparecchiature), altre sicurezza fisica e, infine, c'è la formazione del personale.

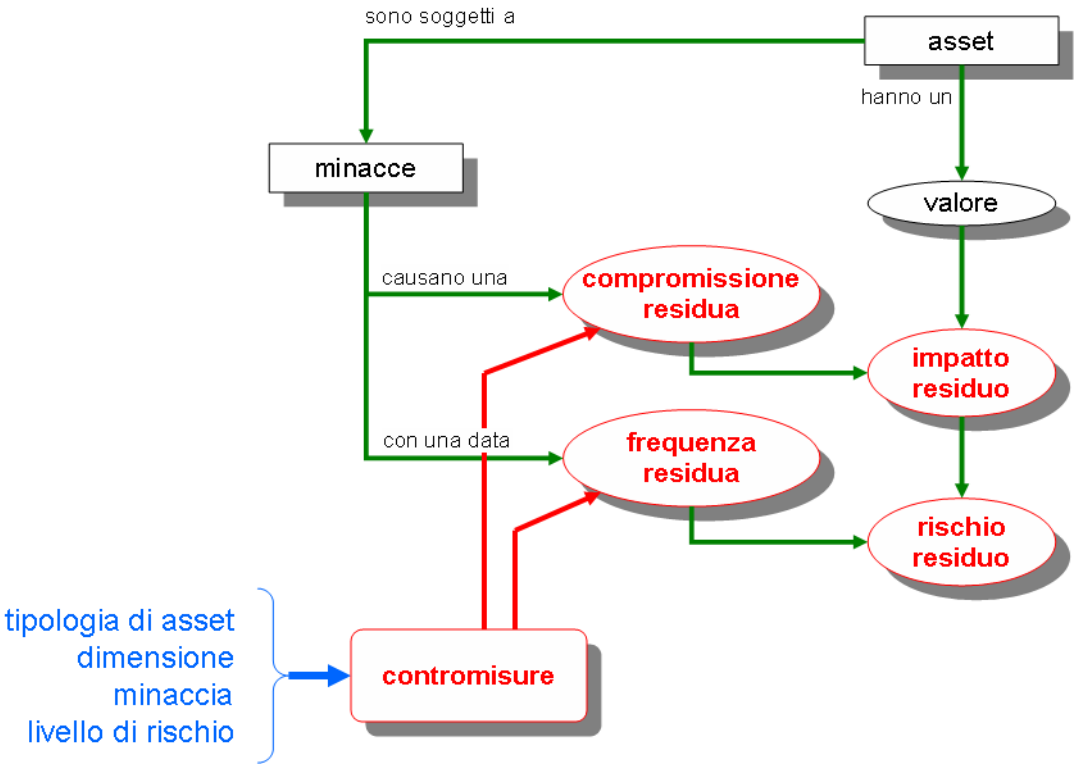
Il capitolo 6 del "catalogo degli elementi" presenta una serie di contromisure adeguate per ogni tipo di asset. Le contromisure rientrano nel calcolo del rischio in due modi:

Riducendo la frequenza delle minacce

Si chiamano contromisure preventive. Idealmente arrivano ad impedire completamente che la minaccia si concretizzi.

Limitando il danno causato

Esistono contromisure che limitano direttamente la possibile compromissione, mentre altre permettono di scoprire immediatamente l'attacco per frenare l'avanzamento della compromissione. Alcune contromisure si limitano a permettere il rapido ripristino del sistema quando la minaccia lo distrugge. In tutti i casi precedenti, la minaccia si materializza ma le conseguenze sono limitate.



Le contromisure sono caratterizzate, oltre che dalla loro esistenza, dalla loro efficacia a fronte del rischio che mirano a scongiurare. La contromisura ideale è efficace al 100%, ovvero:

- è teoricamente idonea;
- è perfettamente documentata, configurata e mantenuta;

- viene impiegata sempre;
- esistono procedure chiare di uso normale ed in caso di incidenti;
- gli utenti sono formati e consapevolizzati;
- esistono controlli che avvisano dei possibili errori.

Tra un'efficacia dello 0% per quelle di carattere "decorativo" e del 100% per quelle che sono perfette, si stimerà un grado di efficacia reale della contromisura in ogni caso concreto.

2.1.6. Revisione del passo 4: impatto residuo

Se si sono eseguite tutte le operazioni alla perfezione, l'impatto residuo deve essere trascurabile.

Se si sono fatte le cose a metà (norme imprecise, procedure incomplete, contromisure inadeguate o insufficienti, o controlli che non controllano) allora si dice che il sistema rimane soggetto ad un impatto residuo.

Il calcolo dell'impatto residuo è semplice. Visto che non è cambiato l'asset, né le sue dipendenze, ma solamente l'entità della compromissione, si ripetono i calcoli di impatto con questo nuovo livello di compromissione.

L'entità della compromissione prendendo in considerazione l'efficacia delle contromisure è la differenza che resta tra l'efficacia perfetta e l'efficacia reale.

L'impatto residuo può essere calcolato in modo cumulativo sull'asset inferiore, o riflesso sugli asset superiori.

2.1.7. Revisione del passo 5: rischio residuo

Se si sono eseguite tutte le operazioni alla perfezione, il rischio residuo deve essere trascurabile.

Se si sono fatte le cose a metà (norme imprecise, procedure incomplete, contromisure inadeguate o insufficienti, o controlli che non controllano) allora si dice che il sistema rimane soggetto ad un rischio residuo.

Il calcolo del rischio residuo è semplice. Visto che non è cambiato l'asset, né le sue dipendenze, ma solamente l'entità della compromissione e la frequenza di accadimento, si ripetono i calcoli di rischio con questi due nuovi dati.

L'entità della compromissione si prende in considerazione nel calcolo dell'impatto residuo.

L'entità della frequenza prendendo in considerazione l'efficacia delle contromisure è la differenza che resta tra l'efficacia perfetta e l'efficacia reale.

Il rischio residuo può essere calcolato in modo cumulativo sull'asset inferiore, o riflesso sugli asset superiori.

2.2. Gestione dei rischi

L'analisi dei rischi definisce impatti e rischi. Gli impatti includono danni assoluti, indipendentemente da ciò che è più o meno probabile che accada. Invece il rischio pondera la probabilità per cui questo accada. L'impatto riflette il danno possibile, mentre il rischio il danno probabile.

Se l'impatto ed il rischio residuo risultano trascurabili, si ha terminato. Se no, si deve procedere ulteriormente.

2.2.1. L'interpretazione dei valori di impatto e rischio residui

Impatto e rischio residuo sono una misura dello stato presente, tra l'insicurezza potenziale (senza

contromisura alcuna) e le misure adeguate che riducono impatto e rischio a valori trascurabili. Rappresentano quindi una misurazione delle carenze.

I paragrafi seguenti si riferiscono contemporaneamente ad impatti e rischi.

Se il valore residuo è uguale al valore potenziale, le contromisure esistenti non servono a nulla, tipicamente non perché non ci sia niente di fatto, ma perché ci sono elementi fondamentali trascurati.

Se il valore residuo è trascurabile, ecco fatto. Questo non vuole dire abbassare il livello di guardia; ma poter affrontare la giornata con una certa fiducia.

Infine, se il valore residuo è più alto rispetto alla soglia di trascurabilità, esiste una certa esposizione.

È importante capire che un valore residuo è solo un numero. Per la sua corretta interpretazione deve venire accompagnato della relazione di quello che si deve fare e non si è fatto. I responsabili della presa di decisioni dovranno prestare molta attenzione a questa relazione di compiti pendenti, denominata **relazione delle debolezze**.

2.2.2. Selezione di contromisure

Le minacce devono essere scongiurate, per principio e nel caso che non si giustifichi il contrario.

Si deve pianificare l'insieme di contromisure rilevanti per mitigare tanto l'impatto quanto il rischio, riducendo sia la compromissione dell'asset (minimizzando il danno), sia riducendo la frequenza della minaccia (minimizzando l'occorrenza).

Qualsiasi minaccia deve essere scongiurata in modo professionale, il che vuole dire che si deve:

1. stabilire una politica dell'organizzazione a riguardo; ovvero norme generali che definiscono chi è responsabile di che cosa;
2. stabilire una norma; ovvero alcuni obiettivi da soddisfare per potere dire a ragion veduta che la minaccia è stata scongiurata;
3. stabilire alcune procedure; ovvero istruzioni passo a passo di cosa si deve fare
4. realizzando contromisure tecniche che effettivamente facciano fronte verso le minacce con possibilità di scongiurarle;
5. realizzando controlli che permettano di sapere che tutto quanto definito in precedenza stia funzionando secondo le previsioni.

Questo insieme di elementi si individua abitualmente sotto il nome di sistema di gestione della sicurezza delle informazioni (SGSI), sebbene si stia operando non solo gestendo ma anche agendo.

Il paragrafo precedente può trarre in inganno se il lettore interpreta che si devono portare a termine tutti i punti per ogni minaccia. No. Nella pratica quanto detto si traduce nello sviluppo di una politica, di alcune norme ed alcune procedure assieme alla realizzazione di una serie di contromisure e controlli e, a questo punto sì, verificare che tutte le minacce abbiano avuto una risposta adeguata.

Dei punti precedenti, il più "aperto" è quello di determinazione delle contromisure appropriate. È realmente un'arte che richiede personale specializzato, sebbene in pratica le situazioni più abituali siano perfettamente documentate nella letteratura e sia sufficiente scegliere tra un catalogo in funzione della grandezza del rischio.

Tipi di contromisure

Un sistema deve considerare prioritarie le contromisure di tipo preventivo mirate a fare in modo che la minaccia non accada o da rendere il suo danno trascurabile. Ovvero impedire incidenti o attacchi.

In pratica non tutto è prevedibile, né tutto quello che è prevedibile è economicamente ragionevole da

mitigare sul nascere. Sia per prepararsi ad affrontare l'ignoto che per proteggersi da ciò a cui si rimane esposti, bisogna disporre di elementi che individuino il principio di un incidente e permettano di reagire con sollecitudine impedendo che esso si trasformi in un disastro.

Tanto le misure preventive quanto quelle di emergenza ammettono una certa compromissione degli asset, quindi si dovrà disporre infine di misure di ripristino che restituiscano il valore perduto dagli asset.

E' buon senso comune tentare di agire in modo preventivo affinché le cose possano non accadere o possano non causare molto danno; ma non sempre è possibile e si deve essere preparati a quando queste accadono. Quello che non deve succedere assolutamente è che un attacco passi inosservato: è necessario individuarlo, esaminarlo e reagire prima con un piano di emergenza (che blocchi e limiti l'incidente) e dopo con un piano di continuità e ripristino per ritornare ad uno stato di normalità.

Infine, senza volontà di annoiare il lettore, ci si deve ricordare che è opportuno arrivare ad un certo equilibrio tra:

contromisure tecniche: in applicazioni, apparecchiature e comunicazioni;

contromisure fisiche: di protezione per l'ambiente di lavoro, per le persone e per le apparecchiature;

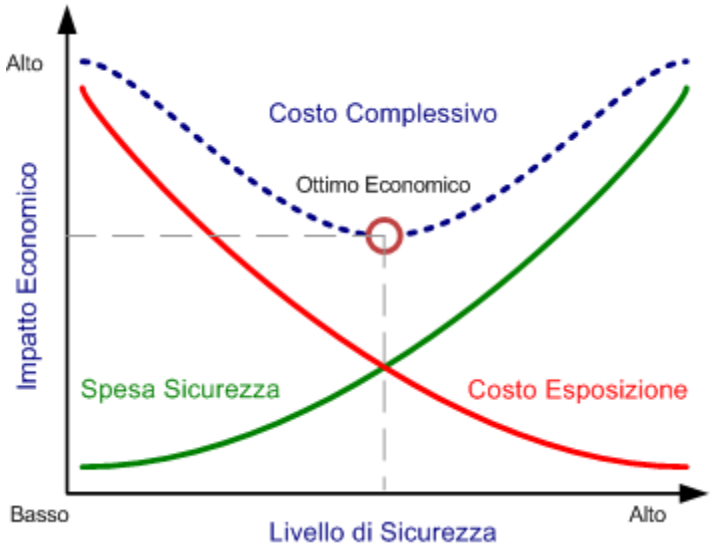
misure organizzative: di prevenzione e gestione delle incidenti;

politica del personale: che, a fine di conti, è un anello indispensabile e molto delicato: politica di assunzione, formazione permanente, organizzazione di risposta agli incidenti, piano di reazione e misure disciplinari.

2.2.3. Perdite e guadagni

Fa parte del buon senso l'idea di non investire in contromisure oltre il valore dei propri asset da proteggere.

Grafici come il seguente appaiono in pratica, mettendo una fronte all'altro il costo dell'insicurezza (quello che costerebbe non sta protetti) ed il costo delle contromisure.



Questo tipo di rappresentazioni grafiche tentano di riflettere come superare un grado di sicurezza

dello 0% verso un grado di sicurezza del 100%, il costo dell'insicurezza (il rischio) diminuisce, mentre il costo dell'investimento in contromisure aumenta. È intenzionale la rappresentazione che il rischio si abbatta di molto con piccoli investimenti e che il costo cresca in modo esponenziale per raggiungere livelli di sicurezza vicini al 100%. La curva centrale somma il costo per l'organizzazione, derivato dal rischio (sicurezza) e dall'investimento in protezione. In una certa forma esiste un punto di equilibrio tra quello che si rischia e quello che si investe in difesa, punto a cui si deve tendere se l'unico vincolo è economico.

Portare il senso comune alla pratica non però così è evidente, né per la parte del calcolo del rischio, né per la parte del calcolo del costo delle contromisure. In altri parole, la curva precedente è concettuale e non si può disegnare a partire da un caso reale.

In pratica, quando ci si deve proteggere da un rischio che si considera significativo, appaiono vari scenari ipotetici:

E0: se non si è fatto niente;

E1: se si applica un certo insieme di contromisure;

E2: se si applica un altro insieme di contromisure;

e così N scenari con differenti combinazioni di contromisure.

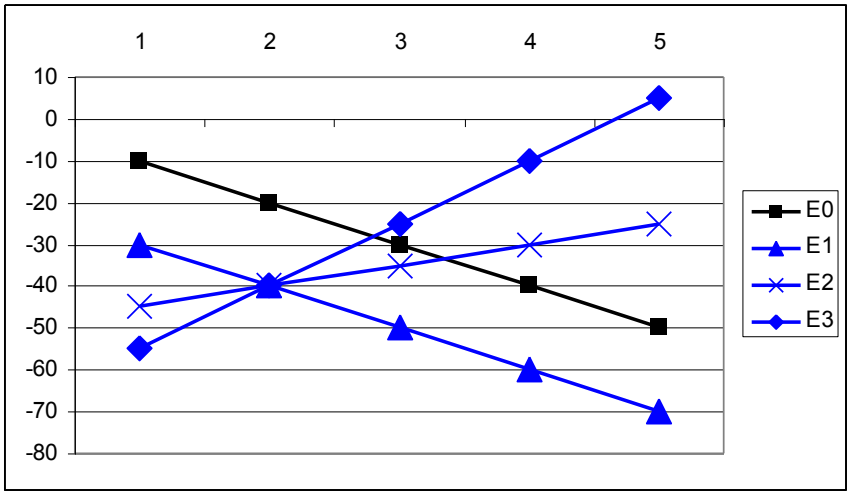
L'analisi economica avrà come missione decidere tra queste opzioni, essendo E0 (non fare niente) un'opzione possibile, che potrebbe essere giustificata economicamente.

In ogni scenario si deve stimare nel tempo i costi annessi. Per potere aggregare i costi, si registrano come valori negativi le perdite di denaro e come valori positivi le entrate di denaro. Considerando i seguenti componenti:

- (ricorrente) rischio residuo;
- (una volta) costo delle contromisure;
- (ricorrente) costo annuale di manutenzione delle contromisure;
- \+ (ricorrente) miglioramento nella produttività;
- \+ (ricorrente) miglioramento nella capacità dell'organizzazione di prestare nuovi servizi, conseguire condizioni più favorevoli dai fornitori, entrare in società con altre organizzazioni, etc.

Lo scenario E0 è molto semplice: tutti gli anni si affronta una spesa definita per il rischio, che si accumula anno dopo anno.

Negli altri scenari, ci sono cose che si sommano e cose che si sottraggono, dando luogo a differenti situazioni:



- In E0 si sa (o si stima) quello che ogni anno si perde.
- Lo scenario E1 sembra una cattiva idea, perché comporta una spesa aggiuntiva il primo anno; ma questa spesa non si recupera in anni successivi.
- Non è così nello scenario E2 che, pur comportando un esborso iniziale, comincia ad essere redditizio a partire dal quarto anno.
- Più attraente ancora è lo scenario E3 nel quale, a fronte di un maggiore esborso iniziale, si comincia a risparmiare al terzo anno e si arrivano ad ottenere benefici operativi a partire del quinto anno. Si può dire che nello scenario E3 si è fatto un buon investimento.

2.2.4. L'atteggiamento della direzione

La direzione dell'organizzazione sottoposta all'analisi dei rischi deve determinare i livelli di impatto e rischio accettabili. Detto più precisamente, accettare la responsabilità delle insufficienze. Questa decisione non è tecnica. Può essere una decisione politica o gestionale o può venire determinata per legge o da requisiti contrattuali con fornitori o utenti. Questi livelli di accettabilità si possono stabilire per asset o per gruppi di asset (in un determinato dipartimento, in un determinato servizio, in una determinata dimensione...)

Qualsiasi livello di impatto e/o rischio è accettabile se lo conosce e lo accetta formalmente la direzione.

Se l'impatto e/o il rischio sono al di sopra di quanto accettabile, si può:

1. eliminare l'asset; suona molto forte, ma alle volte ci sono asset che, semplicemente, non vale la pena mantenere;
2. introdurre nuove contromisure o migliorare l'efficacia di quelle presenti.

2.2.5. Revisione del passo 1: asset

Alcune contromisure, in particolar modo quelle di tipo tecnico, si traducono nel dispiegamento di più apparecchiature che si trasformano alla loro volta in asset del sistema. Questi asset supportano parte del valore del sistema e sono a loro volta soggetti a minacce che possono danneggiare gli asset di valore.

C'è quindi da ripetere l'analisi dei rischi, ampliandola con il nuovo spiegamento di mezzi e, naturalmente, accertarsi che il rischio del sistema ampliato sia minore di quello del sistema originale; cioè, che le contromisure diminuiscano effettivamente lo stato di rischio dell'organizzazione.

3. Strutturazione del progetto

Se nel capitolo precedente si è esposto in modo teorico come portare a termine l'analisi e la gestione dei rischi, in questo capitolo si definiscono gli stessi concetti calati nelle componenti di un progetto di analisi e gestione dei rischi (AGR). I passi si organizzano in tre grandi processi (preparazione, analisi e gestione). Ogni processo si organizza in attività che, alla fine, si strutturano in compiti da realizzare. In ogni compito si indica quello che si deve fare così come le possibili difficoltà per espletarlo nonché il modo di affrontarle con successo. In ogni processo si indicano i traguardi che vanno segnando il progresso del progetto fino alla sua conclusione.

Magerit copre uno spettro molto ampio degli interessi dei suoi utenti. Nell'impostazione di queste guide si è seguito un criterio "di massima", considerando tutti i tipi di asset, tutti i tipi di aspetti di sicurezza, tutti i tipi di situazioni.. Nella pratica, l'utente può trovarsi di fronte a situazioni dove l'analisi è più ristretta. Seguono alcuni casi pratici frequenti:

- si richiede solo uno studio dei file di soggetti alla legislazione sui dati di carattere personale;
- si richiede solo uno studio delle garanzie di riservatezza delle informazioni;
- si richiede solo uno studio della sicurezza delle comunicazioni;
- si richiede solo uno studio della sicurezza perimetrale;
- si richiede solo uno studio del disponibilità dei servizi (tipico perché si cerca lo sviluppo di un piano di continuità);
- si cerca un'omologazione o accreditamento del sistema o di un prodotto;
- si cerca di lanciare un progetto di metriche di sicurezza, dovendo identificare quali punti interessa controllare e con che grado di periodicità e dettaglio;
- etc.

Queste situazioni, frequentemente, sono raccolte in modo formale nei compiti dell'attività A1.2 e in modo informale commentando che è costruttivo concentrarsi su un ambito ridotto, ampliandolo successivamente a seconda della necessità, invece di affrontare subito la totalità del problema.

Oltre a coprire un ambito più o meno esteso, possono capitare situazioni in cui si richiedono analisi in ottiche differenti:

- un'analisi urgente per determinare gli asset critici;
- un'analisi globale per determinare le misure generali;
- un'analisi di dettaglio per determinare contromisure specifiche per certi elementi del sistema informativo;
- un'analisi quantitativa di dettaglio per determinare l'opportunità di una spesa elevata;
- ...

Riassumendo, i compiti che si dettagliano nel seguito devono essere adattati:

1. orizzontalmente all'obiettivo che si richiede (attività A1.2);
2. verticalmente alla profondità opportuna.

3.1. Partecipanti

Durante lo sviluppo del progetto di AGR, dal suo inizio alla sua conclusione, si identificano i seguenti

organi collegiali:

Comitato di direzione

Il profilo richiesto per questo gruppo di partecipanti include persone con un alto livello nella direzione dell'organizzazione, conoscenza degli obiettivi strategici e di business che si perseguono ed autorità per convalidare ed approvare ognuno dei processi realizzati durante lo sviluppo del progetto.

Le responsabilità di questo comitato consistono in

- assegnare le risorse necessarie per l'esecuzione del progetto;
- approvare i risultati finali di ogni processo.

Il comitato di direzione ha le sue funzioni formalizzate nel compito T1.3.2.

Comitato di attenzione

E' costituito dal responsabile delle unità operative incluse nel progetto, così come dai responsabili dell'informatica e della gestione all'interno di tali unità. Sarà anche importante la partecipazione dei servizi interni all'organizzazione (pianificazione, contabilità, personale, amministrazione, etc.) In ogni caso la composizione del comitato dipende delle caratteristiche delle unità operative interessate.

Le responsabilità di questo comitato consistono in:

- risolvere gli incidenti durante lo sviluppo del progetto;
- assicurare la disponibilità di personale con i profili adeguati e la sua partecipazione nelle attività dove è necessaria la sua collaborazione;
- approvare le relazioni provvisorie e finali di ogni processo;
- elaborare le relazioni finali per il comitato di direzione;

Il comitato di attenzione è creato nel compito T1.1.1 e le sue funzioni sono definite in T1.3.2.

Gruppo di progetto

E’ formato da personale esperto in tecnologie e sistemi informativi e personale tecnico qualificato sull’ambito interessato, con nozioni sulla gestione della sicurezza in generale e sull'applicazione della metodologia di analisi e gestione dei rischi in particolare. Se il progetto è eseguito con assistenza tecnica esterna, tale personale specializzato in sicurezza di sistemi informativi si integrerà in questo gruppo di progetto.

Le responsabilità di questo gruppo consistono in:

- portare a termine i compiti del progetto;
- compilare, elaborare e consolidare i dati;
- elaborare le relazioni.

Il gruppo di progetto è definito nel compito T1.3.2.

Gruppi di interlocutori

Sono formati da utenti rappresentativi delle unità operative interessate dal progetto. Li costituiscono vari possibili sottogruppi:

- responsabili di servizi, coscienti della missione dell'organizzazione e le sue strategie a medio e lungo termine;
- responsabili di servizi interni;
- personale di erogazione ed operazione dei servizi informatici, coscienti dei mezzi

impiegati (di produzione e contromisure) e degli incidenti abituali.

Le unità operative interessate si determinano nei compiti T1.2.2 e T1.2.3. Gli interlocutori si identificano nel compito T1.3.1.

Oltre a detti organi, si devono identificare alcuni ruoli puntuali:

Promotore

È una figura individuale che conduce i primi compiti del progetto, definendo la sua opportunità e l'ambito su cui lanciare il progetto di AGR propriamente detto.

Deve essere una persona con visione globale dei sistemi informativi e del loro ruolo nelle attività dell'organizzazione, senza necessità di conoscere i dettagli tecnici, ma possibilmente quelli relativi agli incidenti.

Il promotore ha il suo ruolo definito nel compito T1.1.1.

Direttore del progetto

Deve essere un dirigente di alto livello, con responsabilità in sicurezza all'interno dell'organizzazione, di sistemi informativi o di pianificazione, di coordinazione o di risorse, servizi o aree somiglianti.

È il capo visibile del gruppo di progetto.

Il direttore del progetto è designato nel compito T1.2.2.

Collegamento operativo

Sarà una persona dell'organizzazione con buona conoscenza delle persone e delle unità coinvolte nel progetto di AGR, che abbia capacità per collegare il gruppo di progetto con il gruppo di utenti.

È l'interlocutore visibile del comitato di attenzione.

Il collegamento operativo è designato nel compito T1.3.2.

È opportuno ricordare che un progetto di AGR è sempre misto per la sua propria natura; richiede cioè la collaborazione permanente di specialisti ed utenti tanto nelle fasi preparatorie come nel suo sviluppo. La figura del collegamento operativo acquista una rilevanza permanente che non è abituale in altri tipi di progetti più tecnici.

3.2. Sviluppo del progetto

In questa sezione si ordinano e formalizzano le azioni da realizzare durante un progetto di AGR, stabilendo una traccia normalizzata per il suo sviluppo. Questa traccia di lavoro definisce:

1. una strutturazione del progetto che serva da guida al gruppo di lavoro e che permetta di inserirvi il responsabile e gli utenti;
2. un insieme di prodotti da ottenere;
3. un insieme di tecniche per ottenere i prodotti;
4. le funzioni e le responsabilità dei diversi partecipanti.

Il progetto si divide in tre grandi processi, organizzati a loro volta in una serie di attività che contengono un insieme di compiti con il grado di dettaglio opportuno.

Ogni compito specifica i seguenti concetti:

- azioni da realizzare;

- dati in ingresso;
- dati in uscita: prodotti e documenti da ottenere come risultato delle azioni;
- tecniche raccomandate per portare a buon fine gli obiettivi del compito;
- partecipanti che intervengono o sono interessati nel compimento delle attività.

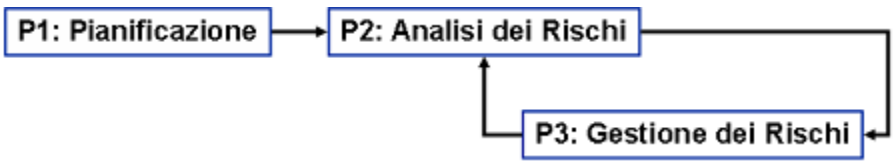
Un progetto di AGR si compone di tre processi principali:

Processo P1: Pianificazione
▪ Si stabiliscono le considerazioni necessarie per iniziare il progetto AGR. ▪ Si investiga l'opportunità di realizzarlo. ▪ Si definiscono gli obiettivi che deve compiere ed l'ambito (ambito) che includerà. ▪ Si pianificano le risorse materiali ed umane per la sua realizzazione. ▪ Si procede al lancio del progetto.

Processo P2: Analisi dei rischi
▪ Si identificano gli asset interessati, le relazioni tra di essi e la valorizzazione che gli compete. ▪ Si identificano le minacce significative sugli asset e si valorizzano in termini di frequenza di occorrenza e di compromissione causata rispetto al valore dell'asset interessato. ▪ Si identificano le contromisure esistenti e si valuta l'efficacia della loro realizzazione. ▪ Si stimano l'impatto ed il rischio a cui sono esposti gli asset del sistema. ▪ Si interpreta il significato dell'impatto e del rischio.

Processo P3: Gestione dei rischi
▪ Si sceglie una strategia per mitigare impatto e rischio. ▪ Si determinano le contromisure opportune per raggiungere l'obiettivo precedente. ▪ Si determina la qualità necessaria di dette contromisure. ▪ Si definisce un piano di sicurezza (piano di azione o piano maestro) per portare l'impatto ed il rischio a livelli accettabili. ▪ Si porta a termine il piano di sicurezza.

Questi tre processi non sono necessariamente sequenziali. Il processo P1 è chiaramente l'iniziatore del progetto. Il processo P2 funziona come sostegno del processo P3 nel senso che la gestione dei rischi (P3) è un compito continuo sopportato dalle tecniche di analisi (P2). La gestione dei rischi suppone sempre l'alterazione dell'insieme delle contromisure, sia perché appaiono nuove contromisure, sia perché si sostituiscono alcune di esse per altre, sia perché si migliorano quelle esistenti. La gestione dei rischi può supporre l'alterazione dell'insieme di asset, tanto perché appaiono nuovi asset (elementi di contromisura che vengono a far parte del sistema) quanto perché sono eliminati asset dal sistema. In definitiva, durante il processo P3 si ricorrerà a compiti del processo P2.



Durante questi processi si generano una serie di documenti di interesse generale:

P1: Pianificazione

- Tipologia degli asset
- Dimensioni di sicurezza rilevanti
- Criteri di valorizzazione

P2: Analisi dei rischi

- Modello dei valori
- Mappa dei rischi
- Valorizzazione delle contromisure
- Stato del rischio
- Relazione delle debolezze

P3: Gestione dei rischi

- Piano di sicurezza

3.2.1. Visione globale

Senza precludere un'esposizione dettagliata successiva, si mostra nel seguito l'albero completo di processi, attività e compiti che formano un progetto di AGR.

Processi, attività e compiti
Processo P1: Pianificazione
Attività A1.1: Studio dell'opportunità
Compito T1.1.1: Determinazione dell'opportunità
Attività A1.2: Determinazione dell'ambito del progetto
Compito T1.2.1: Obiettivi e restrizioni generali
Compito T1.2.2: Determinazione dell'ambito e dei limiti
Compito T1.2.3: Identificazione dell'ambiente
Compito T1.2.4: Stima di dimensioni e costi
Attività A1.3: Pianificazione del progetto
Compito T1.3.1: Valorizzazione dei ruoli e pianificazione delle interviste
Compito T1.3.2: Organizzazione dei partecipanti
Compito T1.3.3: Pianificazione del lavoro
Attività A1.4: Lancio del progetto
Compito T1.4.1: Adattamento dei questionari
Compito T1.4.2: Criteri di valorizzazione
Compito T1.4.3: Risorse necessarie
Compito T1.4.4: Sensibilizzazione
Processo P2: Analisi dei rischi
Attività A2.1: Caratterizzazione degli asset
Compito T2.1.1: Identificazione degli asset
Compito T2.1.2: Dipendenze tra asset
Compito T2.1.3: Valorizzazione degli asset
Attività A2.2: Caratterizzazione delle minacce
Compito T2.2.1: Identificazione delle minacce
Compito T2.2.2: Valorizzazione delle minacce
Attività A2.3: Caratterizzazione delle contromisure
Compito T2.3.1: Identificazione delle contromisure esistenti
Compito T2.3.2: Valorizzazione delle contromisure esistenti

Attività A2.4: Stima dello stato di rischio Compito T2.4.1: Stima dell'impatto Compito T2.4.2: Stima del rischio Compito T2.4.3: Interpretazione dei risultati
Processo P3: Gestione dei rischi Attività A3.1: Presa di decisioni Compito T3.1.1: Qualificazione dei rischi Attività A3.2: Piano di sicurezza Compito T3.2.1: Programmi di sicurezza Compito T3.2.2: Piano di esecuzione Attività A3.3: Esecuzione del piano Compito T3.3.*: Esecuzione di ogni programma di sicurezza

3.3. Processo P1: Pianificazione

L'obiettivo principale di questo processo è stabilire la traccia generale di riferimento per tutto il progetto.

Come obiettivi complementari si possono identificare i seguenti:

- Motivare, consapevolizzare ed inserire la direzione o gerenza dell'organizzazione.
- Ragionare sull'opportunità di realizzare un progetto di AGR.
- Affermare e far conoscere la volontà della direzione della sua realizzazione.
- Creare le condizioni umane e materiali per il buono sviluppo del progetto.

Questo processo si sviluppa attraverso le seguenti attività e compiti:

Attività A1.1: Studio dell'opportunità

Si dà un fondamento all'opportunità della realizzazione, in questo momento, del progetto di AGR, inquadrandolo nello sviluppo delle altre attività dell'organizzazione.

Il risultato di questa attività è la relazione cosiddetta "preliminare".

Compiti:

Compito T1.1.1: Determinazione dell'opportunità

Attività A1.2: Determinazione dell'ambito del progetto

Si definiscono gli obiettivi finali del progetto, il suo ambito ed i suoi limiti. Si realizza una prima identificazione dell'ambiente e delle restrizioni generali da considerare. Si stima infine il costo che il progetto va a comportare.

Il risultato di questa attività è un profilo di progetto AGR.

Compiti:

Compito T1.2.1: Obiettivi e restrizioni generali

Compito T1.2.2: Determinazione dell'ambito e dei limiti

Compito T1.2.3: Identificazione dell'ambiente

Compito T1.2.4: Stima di dimensioni e costi

Attività A1.3: Pianificazione del progetto

Si determinano i carichi di lavoro necessari per la realizzazione del progetto. Si pianificano le intervistate che si vanno a realizzare per la raccolto di informazioni e chi deve essere intervistato. Si elabora il piano di lavoro per la realizzazione del progetto.

In questa attività si determinano i partecipanti e si strutturano i differenti gruppi e comitati per portare a termine il progetto.

Il risultato di questa attività è costituito da:

- un piano di lavoro per il progetto di AGR;
- procedure di gestione delle informazioni create.

Compiti:

Compito T1.3.1: Valorizzazione dei ruoli e pianificazione delle interviste

Compito T1.3.2: Organizzazione dei partecipanti

Compito T1.3.3: Pianificazione del lavoro

Attività A1.4: Lancio del progetto

Si adattano i questionari per la raccolta di informazioni al progetto presente. Si scelgono le tecniche principali di valorizzazione di rischio da utilizzare e si assegnano le risorse necessarie per l'inizio del progetto. Si realizza inoltre una campagna informativa di sensibilizzazione per gli interessati sulle finalità e sui requisiti della loro partecipazione.

Il risultato di questa attività è costituito da:

- i questionari per le interviste;
- il piano delle interviste;
- il catalogo dei tipi di asset;
- la relazione delle dimensioni di sicurezza e;
- i criteri di valorizzazione.

Compiti:

Compito T1.4.1: Adattamento dei questionari

Compito T1.4.2: Criteri di valorizzazione

Compito T1.4.3: Risorse necessarie

Compito T1.4.4: Sensibilizzazione

3.3.1. Attività A1.1: Studio dell'opportunità

Consta di un unico compito:

T1.1.1: Determinazione dell'opportunità

P1: Pianificazione
A1.1: Studio dell'opportunità
T1.1.1: Determinazione dell'opportunità

Obiettivi ▪ Identificare o suscitare l'interesse della direzione dell'organizzazione nella realizzazione di un progetto di AGR
Elementi in ingresso
Elementi in uscita **Relazione preliminare** che raccomanda l'elaborazione del progetto di AGR ▪ Sensibilizzazione ed appoggio della direzione alla realizzazione del progetto di AGR ▪ Creazione del comitato di attenzione
Tecniche, consuetudini e linee guida ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2)
Partecipanti ▪ Il promotore

La direzione è di norma molto cosciente dei vantaggi che apportano le tecnologie elettroniche, informatiche e telematiche al suo funzionamento, ma non altrettanto dei nuovi problemi di sicurezza che queste tecnologie implicano, oppure degli obblighi legali o regolamentari che le riguardano.

In tutte le organizzazioni, pubbliche o private, è importante trasformare in misure concrete la crescente attenzione verso la mancanza di sicurezza dei sistemi informativi, direttamente e nell'ambiente che li include, poiché i suoi effetti non riguardano solo tali sistemi, ma l'intero funzionamento dell'organizzazione e, nelle situazioni critiche, la sua stessa missione o capacità di sopravvivenza.

Sviluppo

L'iniziativa per la realizzazione di un progetto di AGR parte da un promotore interno o esterno all'organizzazione, cosciente dei problemi legati alla sicurezza dei sistemi informativi, come per esempio:

- Incidenti continui legati alla sicurezza.
- Inesistenza di previsioni sulla valutazione di necessità e mezzi per raggiungere un livello accettabile di sicurezza dei sistemi informativi compatibile con l'adempimento corretto della missione e delle funzioni dell'organizzazione.
- Ristrutturazioni nei prodotti o nei servizi forniti.
- Cambiamenti nella tecnologia utilizzata.
- Sviluppo di nuovi sistemi informativi.

Il promotore può elaborare un **questionario-traccia** (documentare poco generalizzabile che dovrà creare per ogni caso concreto) per provocare la riflessione su aspetti della sicurezza dei sistemi informativi da parte di:

Responsabili delle unità operative (responsabili di servizi).

Il questionario permette di condurre un esame informale della situazione per quanto concerne la sicurezza dei suoi sistemi informativi; i responsabili devono potere esprimere la loro opinione sui progetti di sicurezza finora realizzati (con il loro grado di soddisfazione o con le limitazioni di questi), così come le loro aspettative a fronte dell'elaborazione di un progetto AGR. Questa approssimazione di alto livello permette di ottenere una prima visione degli obiettivi concreti e delle opzioni che devono sottostare all'elaborazione del progetto.

Responsabile dei servizi informativi.

Il questionario permette di ottenere una panoramica tecnica per l'elaborazione del progetto e

semplifica l'approccio allo studio dell'opportunità di realizzazione, dopo aver integrato le opzioni precedenti.

Dalle risposte al questionario-traccia e dalle interviste tenute con il responsabile e i suoi colleghi anteriormente, il promotore ottiene una prima approssimazione sulle funzioni, i servizi ed i prodotti implicati in questioni di sicurezza dei sistemi informativi, l'ubicazione geografica degli stessi, i mezzi tecnologici, le risorse umane, etc.

Con questi elementi il promotore realizza la **relazione preliminare** raccomandando l'elaborazione del progetto di AGR e includendo in essa questi elementi:

- Esposizione degli argomenti di base.
- Relazione su antecedenti sulla sicurezza dei sistemi informativi (piano strategico, piano d'azione, etc.).
- Prima approssimazione all'ambito da includere nel progetto in funzione di:
  - finalità delle unità o dei dipartimenti;
  - orientamenti direttivi e tecnici;
  - struttura dell'organizzazione;
  - ambiente tecnologico.
- Prima approssimazione delle risorse, tanto umane quanto materiali, per la realizzazione del progetto di AGR.

Il promotore presenta questa relazione preliminare alla direzione che può decidere se:

- approvare il progetto, oppure
- modificare il suo ambito e/o i suoi obiettivi, oppure
- ritardare il progetto.

3.3.2. Attività A1.2: Determinazione dell'ambito del progetto

Una volta che si è constatata l'opportunità di realizzare il progetto di AGR e si è ottenuto l'appoggio della direzione, questa attività prende in carico la stima degli elementi di pianificazione del progetto, cioè i partecipanti ed i carichi di lavoro.

In detta stima si deve tenere in considerazione la possibile esistenza di altri piani (per esempio un piano strategico dei sistemi informativi o di sicurezza generale nelle unità operative interessate o nell'organizzazione) ed il termine di tempo stimato per la conclusione del progetto di AGR. In particolare, l'esistenza di un piano strategico dei sistemi informativi per le unità operative può determinare in grande misura l'ambito e l'estensione delle attività che si realizzino in questa attività.

Questa attività consta di quattro compiti:

T1.2.1: Obiettivi e restrizioni generali

T1.2.2: Determinazione dell'ambito e dei limiti

T1.2.3: Identificazione dell'ambiente

T1.2.4: Stima di dimensioni e costi

P1: Pianificazione
A1.2: Determinazione dell'ambito del progetto
T1.2.1: Obiettivi e restrizioni generali

Obiettivi ▪ Determinare gli obiettivi del progetto, differenziati secondo orizzonti temporali a corto e medio termine ▪ Determinare le restrizioni generali che si impongono sul progetto
Elementi in ingresso ▪ Raccolta della documentazione pertinente dell'organizzazione
Elementi in uscita ▪ Specifica dettagliata degli obiettivi del progetto ▪ Relazione sulle restrizioni generali
Tecniche, consuetudini e linee guida ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2)
Partecipanti ▪ Il comitato di attenzione

Un progetto di AGR può perseguire obiettivi a molto breve termine come l'assicurazione di un certo sistema o di un certo processo di business o può includere obiettivi più ampi quali l'analisi globale della sicurezza dell'organizzazione. In ogni caso questo punto deve essere definito.

Soprattutto al momento di intraprendere azioni correttive, si deve tenere in considerazione che non "tutto va bene", ma che il progetto avrà a che fare con una serie di restrizioni, non necessariamente tecniche, che tracciano dei confini. Per incorporare le restrizioni all'analisi e gestione dei rischi, queste si raggruppano per diversi concetti tipici:

Restrizioni politiche o direttive

Tipiche di organizzazioni governative o molto relazionate con organismi governativi, sia come fornitori che come erogatori di servizi.

Restrizioni strategiche

Derivanti dall'evoluzione prevista della struttura o dagli obiettivi dell'organizzazione.

Restrizioni geografiche

Derivanti dell'ubicazione fisica dell'organizzazione o dalla sua dipendenza da mezzi fisici di comunicazioni. Isole, sedi fuori delle frontiere, etc.

Restrizioni temporali

Che prendono in considerazione situazioni congiunturali: conflittualità lavorativa, crisi internazionali, cambi della proprietà, reingegnerizzazione dei processi, etc.

Restrizioni strutturali

Prendendo in considerazione l'organizzazione interna: procedure di presa di decisioni, dipendenza da società di controllo internazionali, etc.

Restrizioni funzionali

Che tengono in considerazione gli obiettivi dell'organizzazione.

Restrizioni legali

Leggi, regolamenti, normative settoriali, contratti esterni ed interni, etc.

Restrizioni relative al personale

Profili lavorativi, accordi contrattuali, accordi sindacali, carriere professionali, etc.

Restrizioni metodologiche

Derivanti dalla natura dell'organizzazione ed dalle sue abitudini o abilità di lavoro che possono imporre un certo modo di fare le cose.

Restrizioni culturali

La "cultura" o modo interno di lavoro può essere incompatibile con certe contromisure teoricamente ideali.

Restrizioni pecuniarie

La quantità di denaro è importante; ma anche il modo di pianificare la spesa e di usare tale budget.

P1: Pianificazione ***A1.2: Determinazione dell'ambito del progetto*** ***T1.2.2: Determinazione dell'ambito e dei limiti***
Obiettivi ▪ Determinare l'ambito o perimetro del progetto di AGR
Elementi in ingresso ▪ Risultati del compito T1.2.1, obiettivi e restrizioni generali ▪ Profilo generale delle unità comprese nell'ambito del progetto
Elementi in uscita ▪ Relazione di unità dell'organizzazione che si vedranno coinvolte come parte del'ambito del progetto ▪ Lista di ruoli rilevanti nelle unità comprese nell'ambito ▪ Designazione del direttore del progetto
Tecniche, consuetudini e linee guida ▪ Diagrammi dei processi (vedere "guida alle tecniche" 3.3)
Partecipanti ▪ Responsabili delle unità operative dell'organizzazione ▪ Il comitato di attenzione

Questo compito identifica le unità operative oggetto del progetto di AGR e specifica le caratteristiche generali di suddette di unità in quanto a responsabili, servizi erogati ed ubicazioni geografiche. Identifica inoltre le principali relazioni delle unità oggetto del progetto con altre entità, per esempio lo scambio di informazioni su diversi supporti, l'accesso a strumenti informatici comuni, etc.

Il compito presume un principio basilare: l'analisi e la gestione dei rischi devono essere concentrate su un ambito limitato, che può includere svariate unità o mantenersi all'interno di una sola unità (a seconda della complessità e del tipo di problematiche in questione), giacché un progetto dall'ambito troppo ampio o indeterminato può risultare infattibile, ovvero eccessivamente generico oppure troppo esteso nel tempo, con ripercussioni sulle stime degli elementi dell'analisi.

P1: Pianificazione ***A1.2: Determinazione dell'ambito del progetto*** ***T1.2.3: Identificazione dell'ambiente esterno***
Obiettivi ▪ Definire il perimetro dell'ambito ▪ Definire le relazioni tra l'interno dell'ambito e l'ambiente esterno
Elementi in ingresso

▪ Risultati del compito T1.2.1, obiettivi e restrizioni generali ▪ Risultati del compito T1.2.2, determinazione dell'ambito e limiti ▪ Schema delle relazioni delle unità dell'ambito con l'ambiente esterno ▪ Diagrammi di flusso dei dati
Elementi in uscita ▪ Relazione delle unità dell'organizzazione che si vedranno incluse nel perimetro dell'ambito ▪ Lista dei ruoli rilevanti in altre unità, da considerare per la definizione dell'ambiente
Tecniche, consuetudini e linee guida ▪ Diagrammi di flusso dei dati (vedere "guida alle tecniche" 3.2) ▪ Diagrammi di processo (vedere "guida alle tecniche" 3.3) ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2)
Partecipanti ▪ Responsabili delle unità incluse nell'ambito ▪ Il comitato di attenzione

Questo compito realizza uno studio globale dei sistemi informativi delle unità comprese nell'ambito del progetto, per identificare le loro funzioni e le loro finalità principali nonché le loro relazioni con l'ambiente esterno, così come le loro tendenze evolutive. Il profilo generale delle unità, ottenuto nel compito precedente, si amplia in questo compito con le informazioni fornite dal responsabile delle diverse aree di tali unità.

P1: Pianificazione ***A1.2: Determinazione dell'ambito del progetto*** ***T1.2.4: Stima di dimensioni e costi***
Obiettivi ▪ Determinare la quantità di risorse necessarie per l'esecuzione del progetto di AGR: umane, temporali e finanziarie
Elementi in ingresso ▪ Risultati del compito T1.2.1, obiettivi e restrizioni generali ▪ Risultati del compito T1.2.2, determinazione dell'ambito e limiti ▪ Risultati del compito T1.2.3, identificazione dell'ambiente esterno
Elementi in uscita ▪ Dimensione del progetto ▪ Costi e benefici del progetto
Tecniche, consuetudini e linee guida ▪ Analisi dei costi-benefici (vedere "guida alle tecniche" 3.1) ▪ Pianificazione di progetto (vedere "guida alle tecniche" 3.5)
Partecipanti ▪ Il direttore di progetto

Il compito facilita il dimensionamento (estensione, complessità, aree di incertezza) del progetto a partire della conoscenza degli obiettivi del progetto, dell'ambito e del profilo delle unità operative comprese nello studio. In funzione della dimensione stimata e degli obiettivi del progetto si scelgono alcune delle tecniche da utilizzare nel progetto. Per esempio, se il progetto ha come obiettivo la realizzazione di un'analisi iniziale generica, la tecnica di calcolo del rischio si orienta ad una discriminazione dicotomica (in due blocchi) dei rischi, a seconda che esigano o meno altri cicli più dettagliati di analisi.

D'altronde questo compito dimensiona anche il progetto nel suo costo e nei ritorni o benefici che può comportare, affinché la direzione possa valutare fondatamente la decisione di intraprenderlo ed assegnare il mezzi necessari per il suo eventuale sviluppo.

- Lo studio del costo del progetto si realizza stimando i tempi e i profili del personale assegnato alle tappe del progetto dimensionate precedentemente.
- Lo studio dei benefici può non essere molto preciso in questo processo iniziale, perché non può tenere in considerazione ancora il vero ritorno di un progetto di sicurezza, che è precisamente il costo di non avere tale sicurezza nell'ambito interessato ovvero il risultato finale del progetto di AGR.

3.3.3. Attività A1.3: Pianificazione del progetto

In questa attività si determinano i partecipanti al progetto, definendo la distribuzione del lavoro, la loro organizzazione in gruppi ed le modalità di azione.

Questa attività consta di tre compiti:

T1.3.1: Valutare la distribuzione del lavoro e pianificare le interviste

T1.3.2: Organizzare i partecipanti

T1.3.3: Pianificare il lavoro

P1: Pianificazione ***A1.3: Pianificazione del progetto*** ***T1.3.1: Valutare la distribuzione del lavoro e pianificare interviste***
Obiettivi ▪ Definire i gruppi di interlocutori: utenti interessati in ogni unità operativa ▪ Pianificare le interviste di raccolta delle informazioni
Elementi in ingresso ▪ Risultati dell'attività A1.2, determinazione dell'ambito del progetto
Elementi in uscita ▪ Relazione dei partecipanti nei gruppi di interlocutori ▪ Piano di interviste ▪ Relazione di distribuzione del lavoro
Tecniche, consuetudini e linee guida ▪ Pianificazione di progetti (vedere "guida alle tecniche" 3.5)
Partecipanti ▪ Il direttore di progetto ▪ Il comitato di attenzione

Il piano di interviste deve riportare chi si va ad intervistare, quando e con che obiettivo. Questo piano permette di determinare il carico di lavoro che il progetto va a comportare per le unità interessate, sia appartenenti all'ambito, sia esterne.

Il piano di interviste è particolarmente importante quando i soggetti da intervistare si trovano in differenti locazioni geografiche e l'intervista richiede lo spostamento di una o di ambedue le parti.

È opportuno anche ordinare le interviste in modo che si ottengano prima le informazioni più tecniche e successivamente quelle gestionali, in modo che l'intervistatore possa far evolvere le domandate prendendo in considerazione fatti (esperienza storica) anziché valutazioni e prospettive di terzi.

P1: Pianificazione ***A1.3: Pianificazione del progetto*** ***T1.3.2: Organizzare i partecipanti***
Obiettivi ▪ Determinare gli organismi partecipanti alla gestione, alla realizzazione e alla manutenzione del progetto ▪ Definire le funzionati e responsabilità degli organismi partecipanti ▪ Stabilire le regole e le modalità operative ▪ Stabilire la classificazione delle informazioni generate
Elementi in ingresso ▪ Risultati dell'attività A1.2, determinazione dell'ambito del progetto
Elementi in uscita ▪ Formalizzazione del comitato di direzione ▪ Formalizzazione del comitato di attenzione ▪ Criteri e procedure di classificazione e gestione delle informazioni generate ▪ Designazione del collegamento operativo ▪ Creazione del gruppo di lavoro
Tecniche, consuetudini e linee guida non applicabile
Partecipanti ▪ Comitato di attenzione ▪ Direttore del progetto

Sebbene tutti i progetti di AGR incorporino fondamentalmente gli stessi comitati, in questo compito si avvicina l'approccio generico al caso particolare, potendosi attenere al caso generale o particolare.

È particolarmente rilevante determinare la classificazione dei documenti che si producano durante il progetto. Se esiste una norma di classificazione, è opportuno attenersi ad essa per approfittare delle procedure già stabilite di trattamento dei documenti. Se non esiste, bisogna elaborare tanto i criteri di classificazione quanto le procedure di trattamento. La classificazione di default sarà "confidenziale", essendo di particolare importanza preservare la riservatezza dei documenti di valorizzazione delle contromisure e delle debolezze.

P1: Pianificazione ***A1.3: Pianificazione del progetto*** ***T1.3.3: Pianificare il lavoro***
Obiettivi ▪ Elaborare il calendario concreto di realizzazione delle diverse tappe, attività e compiti del progetto ▪ Stabilire un calendario di attenzione che raccolga le date di riunione proposte del comitato di direzione, il piano di consegna dei prodotti del progetto, le possibili modifiche negli obiettivi selezionati, etc.
Elementi in ingresso ▪ Risultati dell'attività A1.2, determinazione dell'ambito del progetto ▪ Risultati del compito T1.3.1, valutare la distribuzione del lavoro e pianificare interviste ▪ Risultati del compito T1.3.2, organizzare i partecipanti
Elementi in uscita ▪ Cronologia del progetto ▪ Compiti dei partecipanti ▪ Specifica dettagliata delle risorse materiali necessarie

▪ Descrizione dei punti di controllo
Tecniche, consuetudini e linee guida ▪ Pianificazione di progetti (vedere "guida alle tecniche" 3.5)
Partecipanti ▪ Il gruppo di progetto

3.3.4. Attività A1.4: Lancio del progetto

Questa attività completa i compiti propedeutici al lancio del progetto: cominciando dalla selezione e adattamento dei questionari da utilizzare nella raccolta di dati, proseguendo con la specifica dei criteri e delle tecniche pratiche da impiegare; terminando con l'assegnazione delle risorse necessarie per la realizzazione del progetto e per il completamento della campagna informativa di sensibilizzazione verso gli interessati.

Questa attività consta di quattro compiti:

T1.4.1: Adattare i questionari

T1.4.2: Criteri di valorizzazione

T1.4.3: Risorse necessarie

T1.4.4: Sensibilizzazione

P1: Pianificazione ***A1.4: Lancio del progetto*** ***T1.4.1: Adattare i questionari***
Obiettivi ▪ Identificare le informazioni rilevanti da ottenere, raggruppate coerentemente alla struttura delle unità operative e ai ruoli dei partecipanti
Elementi in ingresso ▪ Risultati dell'attività A1.3, Pianificazione del progetto
Elementi in uscita ▪ Questionari adattati
Tecniche, consuetudini e linee guida ▪ Questionari (vedere "catalogo degli elementi" in generale e l'appendice 2 in particolare)
Partecipanti ▪ Il gruppo di progetto

Il compito adatta i questionari da utilizzare nella raccolta di informazioni all'interno del processo P1 in funzione degli obiettivi del progetto, dell'ambito e dei temi da approfondire con gli utenti.

I questionari devono essere adattati con l'obiettivo di identificare correttamente gli elementi di lavoro: asset, minacce, vulnerabilità, impatti, contromisure esistenti, restrizioni generali, etc. in previsione dei requisiti delle attività A2.1 (caratterizzazione degli asset), A2.2 (caratterizzazione delle minacce) e A2.3 (caratterizzazione delle contromisure).

Il bisogno di un qualche adattamento esiste sempre (dovuto all'ampio spettro dei problemi di sicurezza che Magerit può e deve trattare). Un grado maggiore o minore di adattamento dipende però dalle condizioni in cui si realizza l'impiego di detti questionari. Non ci sarà la stessa profondità di adattamento nelle interviste guidate dallo specialista in sicurezza rispetto ai questionari autogestiti dal responsabile dell'ambito o dagli utenti dei suoi sistemi informativi.

P1: Pianificazione ***A1.4: Lancio del progetto*** ***T1.4.2: Criteri di valorizzazione***
Obiettivi ▪ Determinare il catalogo dei tipi di asset ▪ Determinare le dimensioni di valorizzazione degli asset ▪ Determinare i livelli di valorizzazione degli asset, includendo una guida unificatrice di criteri per assegnare un certo livello ad un certo asset ▪ Determinare i livelli di valorizzazione delle minacce: frequenza e compromissione
Elementi in ingresso ▪ Catalogo degli elementi ▪ Risultati dell'attività A1.3, pianificazione del progetto
Elementi in uscita ▪ Catalogo dei tipi di asset ▪ Relazione delle dimensioni di sicurezza ▪ Criteri di valorizzazione
Tecniche, consuetudini e linee guida ▪ Vedere "catalogo degli elementi" capitoli 2, 3 e 4
Partecipanti ▪ Il gruppo di progetto

Questo compito, preparatorio del processo P2 (analisi dei rischi), stabilisce la selezione dei criteri e delle tecniche che si manterranno per tutta la durata del processo. In effetti, la gestione dei rischi del processo P3 sarà condizionata dal tipo di analisi realizzato nel processo P2: se si sono scelti criteri e tecniche per valutare i rischi, è raccomandabile applicare gli stessi per valutare la riduzione dei rischi e per realizzare le contromisure proposte. La scelta di questi criteri e tecniche è in funzione:

- degli obiettivi del progetto (T1.2.1)
- dell'ambito del progetto (T1.2.2)

Si raccomanda di attenersi a quanto suggerito nel libro "catalogo degli elementi" allegato a questa guida.

P1: Pianificazione ***A1.4: Lancio del progetto*** ***T1.4.3: Risorse necessarie***
Obiettivi ▪ Assegnare le risorse necessarie (umane, organizzative, tecniche, etc.) per la realizzazione del progetto di AGR
Elementi in ingresso ▪ Risultati dell'attività A1.3, pianificazione del progetto
Elementi in uscita ▪ Comunicazione di assegnazione al progetto rivolta al personale partecipante ▪ Disponibilità delle risorse materiali necessarie
Tecniche, consuetudini e linee guida ▪ Pianificazione dei progetti (vedere "guida alle tecniche" 3.5)
Partecipanti ▪ Il comitato di attenzione

P1: Pianificazione ***A1.4: Lancio del progetto*** ***T1.4.4: Sensibilizzazione***
Obiettivi ▪ Informare le unità interessate ▪ Creare una consapevolezza generale sugli obiettivi, sui responsabili del progetto e sui termini
Elementi in ingresso ▪ Risultati dell'attività A1.3, pianificazione del progetto
Elementi in uscita ▪ Nota informativa della direzione ▪ Materiale e relazione di presentazione del progetto
Tecniche, consuetudini e linee guida ▪ Presentazioni (vedere "guida alle tecniche" 3.6.3)
Partecipanti ▪ Il direttore del progetto ▪ Il comitato di attenzione ▪ Il collegamento operativo ▪ Il gruppo di progetto

Questo compito informa le unità operative interessate del lancio del progetto di AGR attraverso diversi mezzi, ma come minimo tramite:

- Una nota informativa della direzione, diretta alle unità operative interessate e dichiarativa del suo appoggio alla realizzazione del progetto.
- La presentazione del progetto, dei suoi obiettivi e della metodologia da impiegare, realizzata nelle unità implicate da parte del gruppo di progetto.

3.3.5. Sintesi del processo P1

3.3.5.1. Punto di controllo

Punto di controllo H1.1:

La direzione procederà all'approvazione o meno della realizzazione del progetto di AGR, basandosi sullo studio di opportunità realizzato dal promotore.

Punto di controllo H1.2:

Il comitato di direzione del progetto convaliderà la relazione di "pianificazione del progetto di analisi e gestione dei rischi" che conterrà una sintesi dei prodotti ottenuti nelle attività realizzate nel processo P1.

3.3.5.2. Risultati

Documentazione intermedia

- Risultati delle interviste.
- Documentazione da altri fonti: statistiche, osservazioni di esperti ed osservazioni degli analisti.

- Documentazione ausiliaria: piani, organigrammi, requisiti, specifiche tecniche, analisi funzionali, quaderni di allocazione, manuali utente, manuali d'uso, diagrammi di flusso delle informazioni e dei processi, modelli di dati, etc.
- Analisi dei risultati, con il rilevamento delle aree critiche chiave.
- Informazioni esistenti utilizzabili per il progetto (per esempio un inventario di asset)
- Risultati possibili dell'applicazione di metodi di analisi e gestione dei rischi realizzati precedentemente (per esempio catalogazione, raggruppamento e valorizzazione di asset, minacce, vulnerabilità, impatti, rischio, meccanismi di protezione, etc.).

Documentazione finale

- Tipologie degli asset
- Dimensioni di sicurezza rilevanti
- Criteri di valorizzazione
- Relazione di "pianificazione del progetto di analisi e gestione dei rischi" che conterrà una sintesi dei prodotti ottenuti dalle attività realizzate nel processo P1.

3.3.6. Lista di controllo del processo P1

Organizzazione del progetto:

- ✓ Approvazione della direzione (P1)
- ✓ Impegno esplicito della direzione (P1)
- ✓ Appoggio della direzione (P1)
- ✓ Comitato di attenzione (T1.3.2)
- ✓ Gruppo di progetto (T1.3.2)
- ✓ Direttore del progetto (T1.2.2)
- ✓ Collegamento operativo (T1.3.2)
- ✓ Gruppi di interlocutori (T1.3.1)
- ✓ Funzioni e metodo di lavoro (T1.3.2)
- ✓ Criteri di classificazione della documentazione e procedure per trattarla (T1.3.2)

Pianificazione del progetto:

- ✓ Relazione preliminare di raccomandazione e giustificazione dell'opportunità di lanciare un progetto di AGR (T1.1.1)
- ✓ Obiettivi espressi e non ambigui (T1.2.1)
- ✓ Stima di dimensioni e costi (T1.2.4)
- ✓ Piano di interviste: persone e date (T1.4.3)
- ✓ Piano di lavoro: punti di controllo (T1.3.3)
- ✓ Assegnazione delle risorse (T1.4.3)
- ✓ Sensibilizzazione dell'organizzazione (T1.4.4)
- ✓ Piano di progetto di Analisi e Gestione dei Rischi (P1)

Aspetti tecnici:

- ✓ Limitazioni generali del progetto (T1.2.1)
- ✓ Ambito del progetto: unità operative comprese nell'analisi (T1.2.2)
- ✓ Ambiente del progetto: altre unità operative collegate in qualche modo (T1.2.3)
- ✓ Questionari adattati (T1.4.1)
- ✓ Catalogo dei tipi di asset (T1.4.2)
- ✓ Relazione delle dimensioni di sicurezza rilevanti (T1.4.2)
- ✓ Criteri di valorizzazione (T1.4.2)

3.4. Processo P2: Analisi dei rischi

Questo processo costituisce il nucleo centrale di Magerit e la sua corretta applicazione condiziona la validità e l'utilità di tutto il progetto. L'identificazione e la stima degli asset e delle possibili minacce che li interessano rappresenta una compito complesso.

Questo processo ha i seguenti obiettivi:

- Creare un modello dei valori del sistema, identificando e valutando gli asset rilevanti.
- Creare una mappa dei rischi del sistema, identificando e valutando le minacce sugli asset.
- Creare una base di conoscenza dello stato attuale delle contromisure.
- Valutare l'impatto possibile sul sistema in esame, tanto l'impatto potenziale (senza contromisure), quanto l'impatto residuo (includendo l'effetto delle contromisure implementate se si tratta di un sistema reale, non di un sistema previsto).
- Valutare il rischio del sistema in esame, tanto il rischio potenziale (senza contromisure), quanto il rischio residuo (includendo l'effetto delle contromisure implementate se si tratta di un sistema reale, non di un sistema previsto).
- Mostrare al comitato di direzione le aree del sistema con maggiore impatto e/o rischio.

Il punto di partenza di questo processo è la documentazione di quello precedente relativamente agli obiettivi del progetto, ai piani di interviste, alla valorizzazione dei carichi di lavoro, alla composizione e alle regole di azione del gruppo dei partecipanti, al piano di lavoro e alla relazione di presentazione del progetto.

Questo processo si sviluppa attraverso le seguenti attività e compiti:

Attività 2.1: Caratterizzazione degli asset

Questa attività mira ad identificare gli asset rilevanti all'interno del sistema da analizzare, caratterizzandoli per tipo, identificando le relazioni tra loro, determinando in che dimensioni di sicurezza sono importanti e valorizzando tale importanza.

Il risultato di questa attività è la relazione denominata "Modello dei valori".

Compiti:

Compito T2.1.1: Identificazione degli asset

Compito T2.2.2: Dipendenze tra asset

Compito T2.3.3: Valorizzazione degli asset

Attività 2.2: Caratterizzazione delle minacce

Questa attività mira ad identificare le minacce rilevanti per il sistema da analizzare,

caratterizzandole con la frequenza stimata di occorrenza e con la stima del danno (compromissione) che causerebbero sugli asset.

Il risultato di questa attività è la relazione denominata "Mappa dei rischi".

Compiti:

Compito T2.2.1: Identificazione delle minacce

Compito T2.2.2: Valorizzazione delle minacce

Attività 2.3: Caratterizzazione delle contromisure

Questa attività mira ad identificare le contromisure dispiegate nel sistema da analizzare, qualificandole per la loro efficacia di fronte alle minacce che sono volte a mitigare.

Il risultato di questa attività è la relazione denominata "Valorizzazione delle contromisure".

Compiti:

Compito T2.3.1: Identificazione delle contromisure esistenti

Compito T2.3.2: Valorizzazione delle contromisure esistenti

Attività 2.4: Stima dello stato di rischio

Questa attività elabora tutti i dati raccolti nelle attività precedenti per

- realizzare un relazione dello stato di rischio: stima di impatto e rischio;
- realizzare un relazione delle debolezze: mancanze o debolezze nel sistema di contromisure.

Compiti:

Compito T2.4.1: Stima dell'impatto

Compito T2.4.2: Stima del rischio

Compito T2.4.3: Interpretazione dei risultati

Questa attività consta di tre compiti:

T2.1.1: Identificazione degli asset

T2.1.2: Dipendenze tra asset

T2.1.3: Valorizzazione degli asset

3.4.1. Attività A2.1: Caratterizzazione degli asset

L'obiettivo di questi compiti è di riconoscere gli asset che compongono i processi e di definire le dipendenze tra di essi. A partire da questo e dalle informazioni compilate nell'attività precedente, l'attività approfondisce lo studio degli asset mirando ad ottenere le informazioni necessarie per realizzare le stime di rischio.

È frequente che i compiti relazionati con gli asset si realizzino parallelamente ai compiti relazionati con le minacce su detti asset (A2.2) e con l'identificazione delle contromisure attuali (A2.3), semplicemente perché le persone rilevanti solgono coincidere ed è difficile che l'interlocutore non tenda in modo naturale a trattare ogni asset "verticalmente", vedendo tutto quello che lo riguarda prima di passare al seguente.

P2: Analisi dei rischi ***A2.1: Caratterizzazione degli asset*** ***T2.1.1: Identificazione degli asset***
Obiettivi ▪ Identificare gli asset che compongono l'ambito, determinandone le caratteristiche, gli attributi e la classificazione nei tipi determinati
Elementi in ingresso ▪ Inventari dei dati trattati dall'organizzazione ▪ Processi di business ▪ Diagrammi di utilizzo ▪ Diagrammi di flusso di dati ▪ Inventari di apparecchiature logiche ▪ Inventari di apparecchiature fisiche ▪ Caratterizzazione funzionale dei posti di lavoro ▪ Locali e sedi dell'organizzazione
Elementi in uscita ▪ Relazione degli asset da considerare ▪ Caratterizzazione degli asset
Tecniche, consuetudini e linee guida ▪ Diagrammi di flusso di dati (vedere "guida alle tecniche" 3.2) ▪ Diagrammi dei processi (vedere "guida alle tecniche" 3.3) ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Vedere anche la sezione 2.1.1.
Partecipanti ▪ Il gruppo di progetto ▪ I gruppi di interlocutori

Questo compito è critico. Una buona identificazione è importante sotto vari punti di vista:

- concretizza con precisione l'ambito del progetto;
- permette l'interazione con i gruppi di utenti: tutti parlano lo stesso linguaggio;
- permette di determinare le dipendenze precise tra gli asset;
- permette di valutare gli asset con precisione;
- permette di identificare e valorizzare le minacce con precisione.

Caratterizzazione degli asset

Per ogni asset si devono determinare una serie di caratteristiche che lo definiscono:

- codice, tipicamente proveniente dall'inventario;
- nome (corto);
- descrizione (lunga);
- tipo (o tipi) che caratterizzano l'asset;
- unità operativa responsabile. Alle volte c'è più di un'unità. Per esempio, nel caso di applicazioni è possibile distinguere tra l'unità che la mantiene e quella che la impiega;

- persona responsabile. Particolarmente rilevante nel caso dei dati. Alle volte c'è più di un responsabile. Per esempio, in caso di dati personali c'è da differenziare tra il responsabile del dato e l'operatore o gli operatori che lo trattano;
- ubicazione, tecnica (asset intangibili) o geografica (asset materiali);
- quantità, come può essere nel caso dell'informatica personale (per esempio 350 elaboratori desktop);
- altre caratteristiche specifiche del tipo di asset.

P2: Analisi dei rischi ***A2.1: Caratterizzazione degli asset*** ***T2.1.2: Dipendenze tra asset***
Obiettivi ▪ Identificare e valorizzare le dipendenze tra asset, cioè la misura in cui un asset di ordine superiore si può vedere danneggiato per una minaccia concretizzatasi su di un asset di ordine inferiore
Elementi in ingresso ▪ Risultati del compito T1.2.1, identificazione ▪ Processi di business ▪ Diagrammi di flusso di dati ▪ Diagrammi di utilizzo
Elementi in uscita ▪ Diagramma delle dipendenze tra asset
Tecniche, consuetudini e linee guida ▪ Diagrammi di flusso di dati (vedere "guida alle tecniche" 3.2) ▪ Diagrammi dei processi (vedere "guida alle tecniche" 3.3) ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Valorizzazione Delphi (vedere "guida alle tecniche" 3.7) ▪ Vedere anche la sezione 2.1.1.
Partecipanti ▪ Il gruppo di progetto ▪ I gruppi di interlocutori

Per ogni dipendenza è conveniente annotare le seguenti informazioni:

- stima del grado di dipendenza: fino ad un massimo del 100%;
- spiegazione della valorizzazione della dipendenza;
- interviste realizzate da cui si sono dedotte le stime precedenti.

P2: Analisi dei rischi ***A2.1: Caratterizzazione degli asset*** ***T2.1.3: Valorizzazione degli asset***
Obiettivi ▪ Identificare in che dimensione ha valore l'asset ▪ Valutare il costo che comporta la distruzione dell'asset per l'organizzazione
Elementi in ingresso ▪ Risultati del compito T1.4.2, criteri di valorizzazione

▪ Risultati del compito T2.1.1, identificazione degli asset ▪ Risultati del compito T2.1.2, dipendenze tra asset
Elementi in uscita ▪ Modello dei valori: relazione dei valori degli asset
Tecniche, consuetudini e linee guida ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Valorizzazione Delphi (vedere "guida alle tecniche" 3.7) ▪ Vedere anche la sezione 2.1.1.
Partecipanti ▪ Il gruppo di progetto ▪ I gruppi di interlocutori ▪ Il comitato di attenzione ▪ La direzione

Per acquisire queste conoscenze può essere necessario intervistare differenti gruppi all'interno dell'organizzazione:

- direzione o gerenza, che conoscono le conseguenze rispetto alla missione dell'organizzazione;
- responsabili dei servizi, che conoscono le conseguenze della non prestazione del servizio o di una sua prestazione degradata;
- responsabili dei dati, che conoscono le conseguenze della compromissione dei dati;
- responsabili dei sistemi informativi e responsabili operativi, che conoscono le conseguenze di un incidente.

Per ogni valorizzazione è opportuno esaminare le seguenti informazioni:

- dimensioni in cui l'asset è rilevante;
- stima della valorizzazione in ogni dimensione;
- spiegazione della valorizzazione;
- interviste realizzate da cui si sono dedotte le stime precedenti.

3.4.2. Attività A2.2: Caratterizzazione delle minacce

Questa attività è solitamente svolta parallelamente alle attività A2.1 e A.2.3 dato che i responsabili da intervistare sono gli stessi.

Questa attività consta di due compiti:

T2.2.1: Identificazione delle minacce

T2.2.2: Valorizzazione delle minacce

P2: Analisi dei rischi ***A2.2: Caratterizzazione delle minacce*** ***T2.2.1: Identificazione delle minacce***
Obiettivi ▪ Identificare le minacce rilevanti per ogni asset
Elementi in ingresso

▪ Risultati del compito T1.4.2, criteri di valorizzazione ▪ Risultati dell'attività A2.1, caratterizzazione degli asset
Elementi in uscita ▪ Relazione delle minacce possibili
Tecniche, consuetudini e linee guida ▪ Cataloghi di minacce (vedere "catalogo degli elementi", capitolo 5) ▪ Alberi di attacco (vedere "guida alle tecniche" 2.3) ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Valorizzazione Delphi (vedere "guida alle tecniche" 3.7) ▪ Vedere anche la sezione 2.1.2.
Partecipanti ▪ Il gruppo di progetto ▪ i gruppi di interlocutori

In questo compito si identificano le minacce significative per gli asset identificati, prendendo in considerazione:

- il tipo di asset;
- le dimensioni in cui l'asset è valorizzato;
- l'esperienza dell'organizzazione.

Per ogni minaccia su ogni asset occorre registrare le seguenti informazioni:

- spiegazione degli effetti della minaccia;
- interviste realizzate da cui si sono dedotte le stime precedenti;
- precedenti, se li si ha, sia nella propria organizzazione, sia in altre organizzazioni che siano considerate rilevanti.

P2: Analisi dei rischi ***A2.2: Caratterizzazione delle minacce*** ***T2.2.2: Valorizzazione delle minacce***
Obiettivi ▪ Stimare la frequenza di concretizzazione di ogni minaccia su ogni asset ▪ Stimare la compromissione che causerebbe la minaccia per ogni dimensione dell'asset, se dovesse concretizzarsi
Elementi in ingresso ▪ Risultati del compito T1.4.2, criteri di valorizzazione ▪ Risultati del compito T2.2.1, identificazione delle minacce ▪ Serie storiche di incidenti ▪ Precedenti: incidenti nell'organizzazione
Elementi in uscita ▪ **Mappa dei rischi**: relazione delle minacce possibili, caratterizzate dalla loro frequenza di concretizzazione e dalla compromissione che causerebbero negli asset
Tecniche, consuetudini e linee guida ▪ Alberi di attacco (vedere "guida alle tecniche" 2.3) ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Valorizzazione Delphi (vedere "guida alle tecniche" 3.7)

▪ Vedere anche la sezione 2.1.2.
Partecipanti ▪ Il gruppo di progetto ▪ I gruppi di interlocutori

In questo compito si valorizzano le minacce identificate nel compito precedente, prendendo in considerazione:

- l'esperienza (storica) universale;
- l'esperienza (storica) del settore di attività;
- l'esperienza (storica) dell'ambiente sono ubicati sistemi;
- l'esperienza (storica) propria dell'organizzazione.

Considerando che esistono una serie di possibili aggravanti, come si descrive nella sezione X.

Per ogni minaccia su ogni asset è opportuno esaminare le seguenti informazioni:

- stima della frequenza della minaccia;
- stima del danno (compromissione) che causerebbe la sua concretizzazione;
- spiegazione delle stime di frequenza e di compromissione;
- interviste realizzate da cui si sono dedotte le stime precedenti.

3.4.3. Attività A2.3: Caratterizzazione delle contromisure

Questa attività è solitamente svolta in parallelo alle attività A2.1 e A.2.2 dato che i responsabili da intervistare sono gli stessi.

L'attività consta di due compiti:

T2.3.1: Identificazione delle contromisure esistenti

T2.3.2: Valorizzazione delle contromisure esistenti

P2: Analisi dei rischi ***A2.3: Caratterizzazione delle contromisure*** ***T2.3.1: Identificazione delle contromisure esistenti***
Obiettivi ▪ Identificare le contromisure, di qualsiasi tipo, che risultano previste o dispiegate alla data di realizzazione dello studio
Elementi in ingresso ▪ Inventario delle procedure operative ▪ Inventario di prodotti e/o progetti di sviluppo di hardware o software a sostegno alla sicurezza dei sistemi ▪ Piano di formazione ▪ Definizione dei posti di lavoro ▪ Contratti ▪ Accordi di outsourcing di servizi
Elementi in uscita ▪ Relazione delle contromisure dispiegate
Tecniche, consuetudini e linee guida ▪ Cataloghi di contromisure (vedere "catalogo degli elementi" capitolo 6)

▪ Alberi di attacco (vedere "guida alle tecniche" 2.3) ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Vedere anche la sezione 2.1.5.
Partecipanti ▪ Il gruppo di progetto ▪ I gruppi di interlocutori

Per ogni contromisura è opportuno esaminare le seguenti informazioni:

- descrizione della contromisura e del suo stato di realizzazione;
- descrizione delle minacce a cui la contromisura vuole far fronte;
- interviste realizzate da cui si sono dedotte le stime precedenti.

P2: Analisi dei rischi ***A2.3: Caratterizzazione delle contromisure*** ***T2.3.2: Valorizzazione delle contromisure esistenti***
Obiettivi ▪ Determinare l'efficacia delle contromisure dispiegate
Elementi in ingresso ▪ Inventario delle contromisure (catalogo degli elementi)
Elementi in uscita ▪ **Valorizzazione delle contromisure**: relazione delle contromisure dispiegate, caratterizzate dal loro grado di efficacia
Tecniche, consuetudini e linee guida ▪ Interviste (vedere "guida alle tecniche" 3.6.1) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Valorizzazione Delphi (vedere "guida alle tecniche" 3.7) ▪ Vedere anche la sezione 2.1.5.
Partecipanti ▪ Il gruppo di progetto ▪ I gruppi di interlocutori ▪ Specialisti in contromisure

In questo compito si valuta l'efficacia delle contromisure identificate nel compito precedente, prendendo in considerazione:

- l'idoneità della contromisura per il fine perseguito;
- la qualità della realizzazione;
- la formazione dei responsabili della loro configurazione ed operatività;
- la formazione degli utenti, se hanno un ruolo attivo;
- l'esistenza di controlli per la misura della sua efficacia;
- l'esistenza di procedure di revisione regolare.

Per ogni contromisura è opportuno esaminare le seguenti informazioni:

- stima della sua efficacia per affrontare le specifiche minacce;

- spiegazione della stima di efficacia;
- interviste realizzate da cui si sono dedotte le stime precedenti.

3.4.4. Attività A2.4: Stima dello stato di rischio

In questa attività si combina quanto individuato durante le attività precedenti (A2.1, A2.2 e A2.3) per derivare le stime dello stato di rischio dell'organizzazione.

Questa attività consta di tre compiti:

T2.4.1: Stima dell'impatto

T2.4.2: Stima del rischio

T2.4.3: Interpretazione dei risultati

P2: Analisi dei rischi ***A2.4: Stima dello stato di rischio*** ***T2.4.1: Stima dell'impatto***
Obiettivi ▪ Determinare l'impatto potenziale a cui è soggetto il sistema ▪ Determinare l'impatto residuo a cui è soggetto il sistema
Elementi in ingresso ▪ Risultati dell'attività A2.1, caratterizzazione degli asset ▪ Risultati dell'attività A2.2, caratterizzazione delle minacce ▪ Risultati dell'attività A2.3, caratterizzazione delle contromisure
Elementi in uscita ▪ Relazione di impatto (potenziale) per asset ▪ Relazione di impatto residuo per asset
Tecniche, consuetudini e linee guida ▪ Analisi mediante tavole (vedere "guida alle tecniche" 2.1) ▪ Analisi algoritmica (vedere "guida alle tecniche" 2.2) ▪ Vedere anche la sezione 2.1.3 e 2.1.6.
Partecipanti ▪ Il gruppo di progetto

In questo compito si stima l'impatto a cui sono esposti gli asset del sistema:

- l'impatto potenziale, a cui è esposto il sistema tenendo in considerazione il valore dell'asset e la valorizzazione delle minacce ma non le contromisure attualmente dispiegate;
- l'impatto residuo, a cui è esposto il sistema tenendo in considerazione il valore dell'asset e la valorizzazione delle minacce, così come l'efficacia delle contromisure attualmente dispiegate.

P2: Analisi dei rischi ***A2.4: Stima dello stato di rischio*** ***T2.4.2: Stima del rischio***
Obiettivi ▪ Determinare il rischio potenziale a cui è soggetto il sistema

▪ Determinare il rischio residuo a cui è soggetto il sistema
Elementi in ingresso ▪ Risultati dell'attività A2.1, caratterizzazione degli asset ▪ Risultati dell'attività A2.2, caratterizzazione delle minacce ▪ Risultati dell'attività A2.3, caratterizzazione delle contromisure
Elementi in uscita ▪ Relazione di rischio (potenziale) per asset ▪ Relazione di rischio residuo per asset
Tecniche, consuetudini e linee guida ▪ Analisi mediante tavole (vedere "guida alle tecniche" 2.1) ▪ Analisi algoritmico (vedere "guida alle tecniche" 2.2) ▪ Vedere anche la sezione 2.1.4 e 2.1.7.
Partecipanti ▪ Il gruppo di progetto

In questo compito si stima il rischio a cui sono soggetti gli asset del sistema:

- il rischio potenziale, a cui è soggetto il sistema tenendo in considerazione il valore dell'asset e la valorizzazione delle minacce ma non le contromisure attualmente dispiegate;
- il rischio residuo, a cui è soggetto il sistema tenendo in considerazione il valore dell'asset e la valorizzazione delle minacce, così come l'efficacia delle contromisure attualmente dispiegate.

P2: Analisi dei rischi ***A2.4: Stima dello stato di rischio*** ***T2.4.3: Interpretazione dei risultati***
Obiettivi ▪ Interpretare i risultati precedenti di impatto e di rischio ▪ Stabilire relazioni di priorità per asset o gruppi di asset, sia in ordine di impatto sia in ordine di rischio
Elementi in ingresso ▪ Risultati dell'attività A2.1, caratterizzazione degli asset ▪ Risultati dell'attività A2.2, caratterizzazione delle minacce ▪ Risultati dell'attività A2.3, caratterizzazione delle contromisure ▪ Risultati del compito T2.4.1, stima dell'impatto ▪ Risultati del compito T2.4.2, stima del rischio
Elementi in uscita ▪ Relazione prioritizzata degli asset soggetti a maggiore impatto ▪ Relazione prioritizzata degli asset soggetti a maggiore rischio ▪ **Stato del rischio**: relazione riassuntiva dell'impatto e del rischio potenziale e residuo a cui è soggetto ogni asset dell'ambito ▪ **Relazione delle debolezze**: relazione che sottolinea il divario tra le contromisure di cui si ha bisogno, quelle che esistono, le divergenze tra la grandezza del rischio e infine l'efficacia attuale delle contromisure
Tecniche, consuetudini e linee guida ▪ Tecniche grafiche (vedere "guida alle tecniche" 3.4) ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Presentazioni (vedere "guida alle tecniche" 3.6.3) ▪ Vedere anche la sezione 2.2.1.

Partecipanti
- Il gruppo di progetto
- Il comitato di attenzione

3.4.5. Sintesi del processo P2

3.4.5.1. Punto di controllo

Punto di controllo H2.1:

Accettazione della relazione "Modello dei valori ".

Punto di controllo H2.2:

Accettazione della relazione "Mappa dei rischi".

Punto di controllo H2.3:

Accettazione della relazione "Valorizzazione delle contromisure".

Punto di controllo H2.4:

Accettazione della relazione "Stato del rischio".

Punto di controllo H2.5:

Accettazione della relazione "Relazione delle debolezze".

3.4.5.2. Risultati

Documentazione intermedia

- Risultati delle interviste.
- Documentazione di altri fonti: statistiche, osservazioni di esperti ed osservazioni degli analisti.
- Informazioni esistenti utilizzabili per il progetto (per esempio l'inventario degli asset).
- Documentazione ausiliaria: piani, organigrammi, requisiti, specifiche tecniche, analisi funzionali, quaderni di allocazione, manuali utente, manuali d'uso, diagrammi di flusso delle informazioni e dei processi, modelli di dati, etc.

Documentazione finale

- **Modello dei valori**

Relazione che dettaglia gli asset, le loro dipendenze, le dimensioni in cui sono valorizzati e la stima del loro valore in ogni dimensione.

- **Mappa dei rischi**

Relazione che dettaglia le minacce significative su ogni asset, caratterizzandole per la loro frequenza di occorrenza e per la compromissione che causerebbe la loro concretizzazione sugli asset.

- **Valorizzazione delle contromisure**

Relazione che dettaglia le contromisure esistenti qualificandole nella loro efficacia nel ridurre il rischio a cui fanno fronte.

- **Stato del rischio**

Relazione che dettaglia per ogni asset l'impatto ed il rischio residuo a fronte ad ogni minaccia.

- **Relazione delle debolezze**

Relazione che dettaglia le contromisure necessarie ma assenti o insufficientemente efficaci.

Questa documentazione è un indice fedele dello stato di rischio e delle ragioni per cui questo rischio non è trascurabile. È fondamentale capire le ragioni che portano ad una determinata valorizzazione del rischio come passaggio preventivo al processo seguente, P3, che cercherà di eliminare il rischio o mitigarlo a livelli accettabili.

3.4.6. Lista di controllo del processo P2

- ✓ Identificazione di asset (T2.1.1)
- ✓ Caratterizzazione degli asset (T2.1.1)
- ✓ Dipendenze tra asset (T2.1.2)
- ✓ Dimensioni rilevanti di sicurezza per asset (T2.1.3)
- ✓ Valorizzazione degli asset (T2.1.3)
- ✓ Modello dei valori (A2.1)
- ✓ Identificazione delle minacce rilevanti (T2.2.1)
- ✓ Stima della frequenza di occorrenza (T2.2.2)
- ✓ Stima del danno (compromissione) derivato della concretizzazione di una minaccia (T2.2.2)
- ✓ Mappa dei rischi (A2.2)
- ✓ Identificazione delle contromisure esistenti (T2.3.1)
- ✓ Stima dell'efficacia delle contromisure esistenti (T2.3.2)
- ✓ Valorizzazione delle contromisure (A2.3)
- ✓ Stima dell'impatto e impatto residuo (T2.4.1)
- ✓ Stima del rischio e rischio residuo (T2.4.2)
- ✓ Stato del rischio (P2)
- ✓ Relazione delle debolezze (P2)

3.5. Processo P3: Gestione dei rischi

Si trattano gli impatti e rischi identificati nel processo precedente, sia accettandoli, sia affrontandoli. Per affrontare i rischi che si considerino inaccettabili si porterà a termine un piano di sicurezza che corregga la situazione attuale. Un piano di sicurezza si concretizza in un insieme di programmi di sicurezza. Alcuni programmi saranno semplici, mentre altri raggiungeranno un livello di complessità e di costo tale da comportare che la loro esecuzione si converta in un progetto vero e proprio. La serie di programmi (e progetti talvolta) si pianifica nel tempo per mezzo del cosiddetto Piano di Sicurezza che ordina ed organizza le azioni destinate a portare lo stato di rischio ad un punto accettabile ed accettato formalmente dalla direzione.

Questo processo si sviluppa attraverso le seguenti attività e compiti:

Attività A3.1: Presa di decisioni

In questa attività si trasformano le conclusioni tecniche del processo P2 in decisioni sul modo di agire.

Compiti:

Compito T3.1.1: Qualificazione dei rischi

Attività A3.2: Piano di sicurezza

In questa attività si trasformano le decisioni sul modo di agire in azioni concrete: progetti di miglioramento della sicurezza pianificati nel tempo.

Compiti:

Compito T3.2.1: Programmi di sicurezza

Compito T3.2.2: Piano di esecuzione

Attività A3.3: Esecuzione del piano

Questa attività raccoglie la serie di progetti che concretizzano il piano di sicurezza e che si vanno realizzando secondo tale piano.

Compiti:

Compito T3.3.*: Esecuzione di ogni programma di sicurezza

3.5.1. Attività A3.1: Presa di decisioni

Questa attività consta di una solo compito:

T3.1.1: Qualificazione dei rischi

P3: Gestione dei rischi ***A3.1: Presa di decisioni*** ***T3.1.1: Qualificazione dei rischi***
Obiettivi ▪ Qualificare i rischi secondo una scala: critico, grave, apprezzabile o accettabile
Elementi in ingresso ▪ Risultati del processo P2, analisi dei rischi ▪ Legislazione applicabile, leggi e giurisprudenza ▪ Regolamento settoriale ▪ Accordi e contratti ▪ Relazioni ambientali ▪ Studi di mercato
Elementi in uscita ▪ Relazione di qualificazione di impatti e rischi, includendo indicazioni riguardo al termine di tempo entro cui devono essere risolti
Tecniche, consuetudini e linee guida ▪ Riunioni (vedere "guida alle tecniche" 3.6.2) ▪ Valorizzazione Delphi (vedere "guida alle tecniche" 3.7) ▪ Vedere anche la sezione 2.2.1.
Partecipanti ▪ Il gruppo di progetto

- Il comitato di attenzione
- Il comitato di direzione

A fronte degli impatti e dei rischi a cui è esposto il sistema, si devono prendere una serie di decisioni di tipo direzionale, non tecnico, condizionate da diversi fattori:

- la gravità dell'impatto e/o del rischio;
- gli obblighi a cui per legge è soggetta l'organizzazione;
- gli obblighi a cui per regolamenti settoriali è soggetta l'organizzazione;
- gli obblighi a cui per contratto è soggetta l'organizzazione.

All'interno del margine di manovra che permette questo contesto, possono comparire considerazioni addizionali sulla capacità dell'organizzazione di accettare certi impatti di natura intangibile tale come:

- immagine pubblica della società;
- politica interna: rapporti con i propri impiegati, come la capacità di assumere personale idoneo, la capacità di trattenere i migliori, la capacità di effettuare rotazioni di personale, la capacità di offrire una carriera professionale attraente, etc.;
- rapporti con i fornitori, come la capacità di arrivare ad accordi vantaggiosi a breve, medio o lungo termine, la capacità di ottenere relazioni prioritarie, etc.;
- rapporti con clienti o utenti, come la capacità di mantenimento, la capacità di incremento dell'offerta e la capacità di differenziazione dalla concorrenza;
- rapporti con altre organizzazioni, come la capacità di raggiungimento di accordi strategici, alleanze, etc.;
- nuove di opportunità di business, come modalità di recupero dell'investimento in sicurezza;
- accesso a certificati o qualifiche riconosciute di sicurezza.

Tutte le considerazioni precedenti sboccano in una qualificazione di ogni rischio significativo, determinando se…

1. è **critico** nel senso che richiede attenzione urgente;
2. è **grave** nel senso che richiede attenzione;
3. è **apprezzabile** nel senso che può essere oggetto di studio per il suo trattamento;
4. è **accettabile** nel senso che non si intraprendono azioni per mitigarlo.

L'opzione 4, detta accettazione del rischio, è sempre rischiosa: si deve considerare con prudenza e giustificarla. I ragionamenti che possono condurre a questa accettazione sono:

- quando l'impatto residuo è trascurabile;
- quando il rischio residuo è trascurabile;
- quando il costo delle contromisure opportune è sproporzionato in confronto all'impatto e al rischio residuo.

Tutte le decisioni sono proposte dal comitato di attenzione, sentita l'opinione del direttore del progetto. Tutte le decisioni sono adottate dal comitato di direzione.

Questa qualificazione avrà conseguenze nei compiti susseguenti, essendo un fattore basilare per stabilire la priorità relativa delle differenti azioni.

3.5.2. Attività A3.2: Elaborazione del piano di sicurezza delle informazioni

Si traducono le decisioni sul modo di agire in azioni concrete.

Questa attività consta di due compiti:

T3.2.1: Programmi di sicurezza

T3.2.2: Piano di esecuzione

P3: Gestione dei rischi ***A3.2: Elaborazione del piano di sicurezza delle informazioni*** ***T3.2.1: Programmi di sicurezza***
Obiettivi ▪ Elaborare un insieme di programmi di sicurezza
Elementi in ingresso ▪ Risultati del compito T3.1.1, qualificazione dei rischi ▪ Nozioni di tecniche e prodotti di sicurezza ▪ Cataloghi di prodotti e servizi di sicurezza
Elementi in uscita ▪ Relazione di programmi di sicurezza
Tecniche, consuetudini e linee guida ▪ Analisi dei rischi (vedere processo P2) ▪ Analisi costi-benefici (vedere "guida alle tecniche" 3.1) ▪ Pianificazione dei progetti (vedere "guida alle tecniche" 3.5) ▪ Vedere anche la sezione 2.2.2 e 2.2.3.
Partecipanti ▪ Il gruppo di progetto ▪ Specialisti in sicurezza ▪ Specialisti in aree specifiche di sicurezza

Fondamentalmente, si portano a termine due passaggi:

1. Si prenderanno in considerazione tutti gli scenari d'impatto e di rischio che si considerino critici o gravi come risultato del compito precedente.
2. Si elaborerà un insieme di programmi di sicurezza che diano risposta ad ognuno degli scenari precedenti, sapendo che uno stesso programma può affrontare differenti scenari e che uno scenario può essere affrontato attraverso differenti programmi.

In ultima istanza si tratta di instaurare o migliorare l'instaurazione di una serie di contromisure che portino impatto e rischio a livelli residui decisi dalla direzione. Questo trattamento delle contromisure si concretizza in una serie di compiti da portare a termine.

Un programma di sicurezza è un insieme di compiti. Questo raggruppamento si realizza per convenienza: sia perché si tratta di compiti che singolarmente mancherebbero di efficacia, sia perché si tratta di compiti con un obiettivo comune, sia perché si tratta di compiti che competono ad un'unica unità operativa.

Ogni programma di sicurezza deve dettagliare:

- Il suo obiettivo generico.
- Le contromisure concrete, considerando i loro obiettivi di qualità, volte a instaurare o a migliorare efficacia ed efficienza

- Il rapporto con gli scenari di impatto e/o rischio che affronta: asset interessati, tipi di asset, minacce affrontate, valorizzazione di asset, minacce e livelli di impatto e rischio.
- L'unità operativa responsabile della sua esecuzione.
- Una stima dei costi, tanto economici quanto di impegno per la realizzazione, tenendo in considerazione:
  - costi di acquisto (di prodotti), o di appalto (di servizi), o di sviluppo (di soluzioni del tipo "chiavi in mano"), potendo essere necessario valutare differenti alternative;
  - costi di installazione iniziale e manutenzione nel tempo;
  - costi di formazione, tanto degli operatori come degli utenti, a seconda del caso;
  - costi di impiego;
  - impatto sulla produttività dell'organizzazione.
- Una relazione dei sottocompiti da affrontare, tenendo in considerazione:
  - cambiamenti normativi e sviluppo delle procedure;
  - soluzioni tecniche: programmi, apparecchiature, comunicazioni ed installazioni;
  - piano di dispiegamento (delle contromisure);
  - piano di formazione.
- Una stima del tempo di esecuzione dal suo avvio fino alla sua messa in funzione.
- Una stima dello stato di rischio (impatto e rischio residuo al suo completamento).
- Un sistema di indicatori di efficacia ed efficienza che permettano di conoscere in ogni momento la qualità dello svolgimento della funzione di sicurezza che si desidera e la sua evoluzione temporale.

Le stime precedenti possono essere molto precise nei programmi semplici ma possono essere semplicemente orientative nei programmi complessi che comportino la realizzazione di un progetto specifico di sicurezza. In quest' ultimo caso, ogni progetto svilupperà i dettagli per mezzo di una serie di compiti proprietari che, in linea generale, risponderanno ai seguenti punti:

- Studio dell'offerta del mercato: prodotti e servizi.
- Costo di uno sviluppo specifico, proprio o subappaltato.
- Se si stima di adeguare uno sviluppo specifico si deve determinare:
  - il conto dettagliato funzionale e non funzionale dello sviluppo;
  - il metodo di sviluppo che garantisca la sicurezza del nuovo componente;
  - i meccanismi di misura (controlli) che devono essere già integrati;
  - i criteri di accettazione;
  - il piano di manutenzione: incidenti ed evoluzione.

P3: Gestione dei rischi ***A3.2: Elaborazione del piano di sicurezza delle informazioni*** ***T3.2.2: Piano di esecuzione***
Obiettivi ▪ Ordinare cronologicamente i programmi di sicurezza

Elementi in ingresso ▪ Risultati del compito T3.1.1, qualificazione dei rischi ▪ Risultati del compito T3.2.1, programmi di sicurezza
Elementi in uscita ▪ Diagramma temporale di esecuzione del piano ▪ **Piano di sicurezza**
Tecniche, consuetudini e linee guida ▪ Analisi dei rischi (vedere processo P2) ▪ Pianificazione di progetti (vedere "guida alle tecniche" 3.5)
Partecipanti ▪ Divisione sviluppo ▪ Divisione acquisti

Si devono ordinare nel tempo i programmi di sicurezza tenendo in considerazione i seguenti fattori:

- la criticità, gravità o convenienza degli impatti e/o rischi che si affrontano, tenendo in massima considerazione i programmi che affrontino situazioni critiche;
- il costo del programma;
- la disponibilità del personale interno per acquisire responsabilità sulla direzione (ed eventualmente sull'esecuzione) dei compiti programmati;
- altri fattori: come possono essere l'elaborazione del budget annuale dell'organizzazione, le relazioni con altre organizzazioni, l'evoluzione del contesto legale, regolamentare o contrattuale, etc.

Tipicamente un piano di sicurezza è articolato su tre livelli di dettaglio:

Piano principale (uno).

Spesso denominato "piano di azione", lavora su un periodo lungo (tipicamente tra 3 e 5 anni), stabilendo le linee di azione principali.

Piano annuale (una serie di piani annuali).

Opera su un periodo medio (tipicamente tra 1 e 2 anni), stabilendo la pianificazione dei programmi di sicurezza.

Piano di progetto (un insieme di progetti con la loro pianificazione).

Lavora nel breve termine (tipicamente meno di 1 anno), stabilendo il piano dettagliato di esecuzione di ogni programma di sicurezza.

Si deve sviluppare un (1) piano principale unico, che è quello che dà prospettiva ed unità di obiettivi a ciascuna azione. Questo piano di principale permette di sviluppare piani annuali che, all'interno dell'ambito strategico, vanno strutturando l'assegnazione di risorse per l'esecuzione dei compiti, in particolare spese budgetarie. Ci sarà infine una serie di progetti che concretizzano i programmi di sicurezza.

3.5.3. Attività A3.3: Esecuzione del piano

Questa attività consta di un numero di compiti che dipende dal piano di sicurezza determinato nell'attività A3.2, perché si tratta eseguire i programmi ivi pianificati.

Questa attività consta di *n* compiti, tanti quanti sono previsti nel piano di sicurezza:

T3.3.*: Esecuzione di ogni programma di sicurezza

P3: Gestione dei rischi ***A3.3: Esecuzione del piano*** ***T3.3.*: Esecuzione di ogni programma di sicurezza***
Obiettivi ▪ Raggiungere gli obiettivi previsti nel piano di sicurezza per ogni programma pianificato
Elementi in ingresso ▪ Risultati dell'attività A3.2, piano di sicurezza ▪ Programma di sicurezza di cui ci si occupa ▪ Analisi dei rischi prima dell'esecuzione del piano
Elementi in uscita ▪ Contromisure dispiegate ▪ Norme d'uso e di operatività ▪ Sistema di indicatori di efficacia ed efficienza del raggiungimento degli obiettivi di sicurezza prefissati ▪ Modello dei valori aggiornato ▪ Mappa dei rischi aggiornata ▪ Stato del rischio aggiornato (impatto e rischio residui).
Tecniche, consuetudini e linee guida ▪ Analisi dei rischi (vedere processo P2) ▪ Pianificazione dei progetti (vedere "guida alle tecniche" 3.5)
Partecipanti ▪ Il gruppo di progetto: evoluzione dell'analisi dei rischi ▪ Personale specializzato nelle contromisure in questione

3.5.4. Sintesi del processo P3

3.5.4.1. Punto di controllo

Punto di controllo H3.1:

La direzione procederà all'approvazione o meno del piano di sicurezza, includendo la relazione dei programmi di sicurezza ed il diagramma temporale proposto per la sua esecuzione.

Punto di controllo H3.*:

Completamento di ogni programma di sicurezza, soddisfacendo i criteri di accettazione imposti nel Piano di Sicurezza.

3.5.4.2. Risultati

Documentazione intermedia

- Decisioni di qualificazione degli scenari di impatto e rischio

Documentazione finale

- Piano di sicurezza

3.5.5. Lista di controllo del processo P3

- ✓ Qualificazione dei rischi (T3.1.1)
- ✓ Identificazione dei programmi di sicurezza necessari (T3.2.1)
- ✓ Programmi di sicurezza

- ✓ obiettivi
- ✓ stima dell'impegno
- ✓ stima del costo
- ✓ piano di accettazione
- ✓ piano d'uso
- ✓ piano di manutenzione
- ✓ piano di formazione
- ✓ sistema di controlli di efficacia
- ✓ sistema di controlli di efficienza
- ✓ stima di impatto e rischio residuo

✓ Calendario di esecuzione (T3.2.2)

✓ Piano di sicurezza strategica: lungo termine (A3.2)

✓ Piano di sicurezza tattica: medio termine (A3.2)

✓ Piani operativi: progetti singoli (A3.2)

4. Sviluppo di sistemi informativi

Le applicazioni *(software)* costituiscono un tipo di asset frequente e di tipo atomico per quanto concerne il trattamento delle informazioni e per la prestazione di servizi basati su di esse. La presenza di applicazioni in un sistema informativo è sempre una fonte di rischio nel senso che costituisce un punto verso il quale si possono concretizzare minacce. Alle volte, inoltre, le applicazioni sono anche parte della soluzione nel senso che costituiscono una contromisura di fronte a rischi potenziali. In qualsiasi caso è necessario che il rischio derivato della presenza delle applicazioni sia sotto controllo.

L'analisi dei rischi costituisce una parte fondamentale del disegno e dello sviluppo di sistemi informativi sicuri. È possibile, ed imperativo, incorporare nella fase di sviluppo le funzioni e i meccanismi che rinforzano la sicurezza del nuovo sistema nonché quelle del proprio processo di sviluppo, assicurando la sua consistenza e la sua sicurezza, completando il piano di sicurezza vigente nell'organizzazione. È un fatto riconosciuto che prendere in considerazione la sicurezza del sistema prima e durante il suo sviluppo è più efficace ed economico che prenderla in considerazione a posteriori. La sicurezza deve essere parte integrante del sistema dalla sua prima concezione.

Si possono identificare due tipi di attività differenziate:

- **SSI**: attività relative alla propria sicurezza del sistema informativo.
- **SPD**: attività relative alla sicurezza del processo di sviluppo del sistema informativo.

Dietro una prima esposizione sullo sviluppo di applicazioni in genere, la sezione 4.5 approfondisce nella sua applicazione a "Metrica" versione 3. "Metrica" è stato sviluppato dal CSAE come la "Metodologia di Pianificazione, Sviluppo e Manutenzione dei sistemi informativi".

4.1. Inizializzazione dei processi

Ci sono svariate ragioni che possono portare ad iniziare lo sviluppo di una nuova applicazione o alla modifica di una già esistente:

Nuovi servizi e/o dati.

- Richiede lo sviluppo di nuove applicazioni o la modifica di applicazioni operative. Può implicare la scomparsa di applicazioni in produzione.
- L'iniziativa è presa dal responsabile di sviluppo, mentre il responsabile di sicurezza agisce come attore secondario.

Evoluzione tecnologica. Le tecnologie di TLC sono in continua evoluzione, possono presentarsi cambiamenti nelle tecniche di sviluppo di sistemi, nei linguaggi o nelle piattaforme di sviluppo, nelle piattaforme o nei servizi d'impiego, nei servizi di comunicazioni, etc.

- Richiede lo sviluppo di nuove di applicazioni o la modifica di applicazioni in produzione. Può implicare la scomparsa di applicazioni in produzione.
- L'iniziativa è presa dal responsabile di sviluppo, mentre il responsabile di sicurezza agisce come attore secondario.

Modifica della qualificazione di sicurezza di servizi o dati.

- Tipicamente richiede la modifica di applicazioni in produzione. Implica di rado lo sviluppo di nuove di applicazioni o la scomparsa di applicazioni in produzione.
- L'iniziativa è presa dal responsabile di sicurezza, il responsabile di sistemi agisce come attore secondario.

Considerazione di nuove minacce. L'evoluzione delle tecnologie e dei servizi di comunicazione

possono porre nuove minacce o trasformare minacce che erano trascurabili nel passato in minacce rilevanti nel futuro.

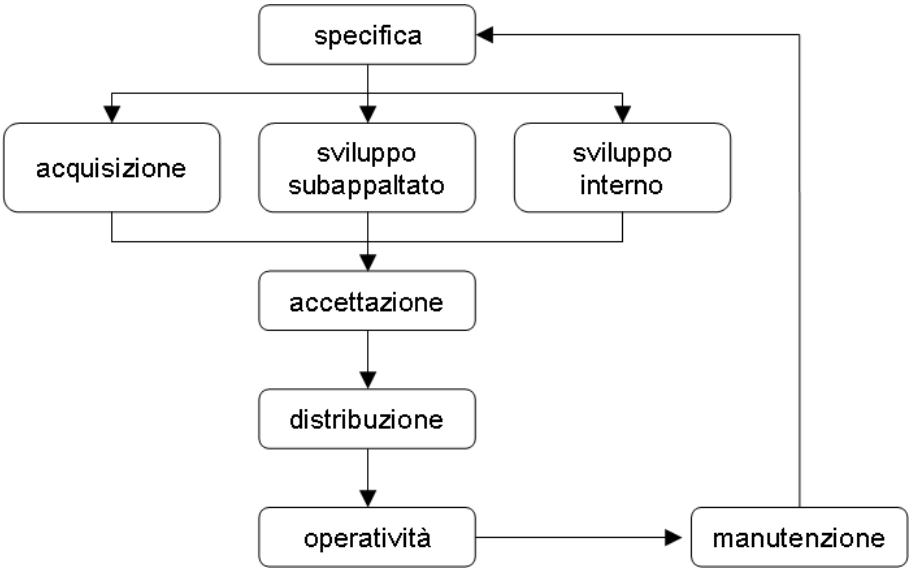
- Tipicamente richiede la modifica di applicazioni in produzione, sia nella loro codifica, sia, più frequentemente, nella loro condizione d'impiego. Implica di rado lo sviluppo di nuove di applicazioni o la scomparsa di applicazioni in produzione.
- L'iniziativa è presa dal responsabile di sicurezza, il responsabile di sistemi agisce come attore secondario.

Modifica dei criteri di qualificazione di rischi. Può venire indotta da criteri di qualità operativa, da novità nella legislazione applicabile, nel regolamento settoriale o da accordi o contratti con terzi.

- Tipicamente richiede la modifica di applicazioni in produzione. Implica di rado lo sviluppo di nuove applicazioni o la scomparsa di applicazioni in produzione.
- L'iniziativa è presa dal responsabile di sicurezza, il responsabile di sistemi agisce come attore secondario.

4.2. Ciclo di vita delle applicazioni

Tipicamente, un'applicazione segue un ciclo di vita composto da svariate fasi:



Specifica. In questa fase si determinano i requisiti che l'applicazione deve soddisfare e si elabora un piano per le seguenti fasi.

Acquisizione o sviluppo. Per trasformare delle specifiche in realtà, si può acquistare un prodotto, o se ne può sviluppare uno, internamente o per appalto esterno.

Accettazione. Che si tratti di un'applicazione nuova o della modifica di un'applicazione precedente, un'applicazione non deve mai entrare in produzione senza essere stata formalmente accettata.

Distribuzione. Consiste nell'installazione del codice nel sistema e nella sua configurazione per entrare in produzione.

Operatività. L'applicazione è usata da parte degli utenti, prestando attenzione agli incidenti rilevati

dagli utenti e/o dagli operatori.

Manutenzione. Sia perché appaiono nuovi requisiti, sia perché si è scoperto un errore, l'applicazione può richiedere un manutenzione che obblighi a ritornare a una qualsiasi delle tappe precedenti, in ultima istanza alla specifica iniziale.

4.2.1. Piano dei sistemi

Le applicazioni informatiche sono una componente dei sistemi informativi. Si prenda in considerazione il contesto di un sistema informativo dove le differenti applicazioni si intrecciano per farsi carico dei servizi richiesti. Un piano dei sistemi determina il contesto di sviluppo e sfruttamento delle applicazioni informatiche, e per la precisione:

I servizi richiesti, tanto dagli utenti interni, quanto i servizi di sostegno a utenti o applicazioni interne.

I dati funzionali che si utilizzano.

Le applicazioni che gestiscono detti dati.

Le apparecchiature: elaboratori e servizi di comunicazione.

Dal punto di vista di sicurezza, un piano dei sistemi permette

- identificare e valutare i servizi essenziali;
- identificare, classificare e valorizzare i dati essenziali;
- determinare la politica di sicurezza dell'organizzazione; cioè:
  - il contesto legale in cui opera l'organizzazione;
  - i criteri di eccellenza nella prestazione dei servizi;
  - i ruoli del personale relazionato ai sistemi informativi.

Il piano dei sistemi permette di stabilire il modello dei valori; cioè, i punti principali (asset) e le prime valutazioni di quello che finirà per essere un'analisi dei rischi dettagliata.

4.3. Analisi dei rischi

Come parte di un sistema informativo, i rischi associati ad un'applicazione devono essere noti e venire gestiti. Questo sia nel caso siano rischi che gravano sull'applicazione, sia nel caso siano rischi riflessi su asset superiori, o se sono rischi accumulati su asset inferiori.

Magerit permette di modellare direttamente l'applicazione come un asset, stabilendo le sue dipendenze, sia per asset superiori che dipendono di lei, sia per asset inferiori che la supportano. Il metodo permette di identificare e valutare minacce e contromisure, derivando informazioni di impatto e rischio sulla stessa applicazione e sugli asset relazionati ad essa.

AGR autocontenuta. Se l'organizzazione non ha ancora realizzato un progetto di AGR, sarà corretto portarlo a termine includendo gli asset direttamente o indirettamente relazionati con l'applicazione.

AGR marginale. Se l'organizzazione ha già realizzato un progetto di AGR, basta rivedere i risultati di tale progetto includendo i nuovi asset. L'apparizione di una nuova applicazione può implicare nuovi servizi, nuovi dati, nuove apparecchiature, nuovi locali e nuovo personale. Può anche implicare la scomparsa di vecchi asset che vengono superati dalla nuova applicazione e dalle sue funzionalità. In ogni caso concreto si deve determinare ciò che deve essere aggiunto e ciò che deve essere eliminato, seguendo le attività A2.1, A2.2 e A2.3 del processo P2, analisi dei rischi.

Che si sia seguito il primo approccio o il secondo, al termine si dispone di una relazione di impatti e rischi, sia sull'applicazione sia sul suo ambiente. Per derivare questi dati si seguono i passi dell'attività A2.4 del processo P2. Per interpretare i risultati si ricorre al compito A2.4.3 del processo P2, interpretazione dei risultati.

4.4. Gestione dei rischi

Il processo P3 di gestione dei rischi raccomanda le contromisure da dispiegare e valuta l'effetto delle contromisure già dispiegate sull'impatto e sul rischio. Le decisioni effettuate dipenderanno dei criteri stabiliti nella politica di sicurezza dell'organizzazione e da altre considerazioni specifiche per ogni caso. Sebbene la politica di sicurezza stabilisca un punto di riferimento che non può essere ignorato, è abituale che non preveda tutti i dettagli tecnici e organizzativi del servizio utili a prendere decisioni precise.

A causa dell'interrelazione tra gli elementi che costituiscono un sistema, non è sufficiente proteggere un certo tipo di asset per proteggere tutto l'insieme. Ciò nonostante, questo capitolo si concentra sulle contromisure che devono essere realizzate all'interno delle applicazioni affinché queste non diminuiscano la sicurezza del sistema.

Sempre condotti su iniziativa e sostegno del processo di gestione dei rischi, si devono tenere in considerazione i seguenti aspetti:

Durante la specifica:

- Dimensionamento.
- Profili degli utenti.
- Requisiti di identificazione ed autenticazione degli utenti.
- Requisiti di cifratura.
- Requisiti di monitoraggio (controllo) ed esame *(log)*:
  - di dati in ingresso;
  - di dati in uscita;
  - di dati intermedi;
  - di accesso all'applicazione;
  - di attività (uso).

Se si acquista *software* standard...

- Contratti di acquisto e manutenzione.

Se si subappalta lo sviluppo di *software*...

- Contratti di acquisto e manutenzione.
- Ambiente di sviluppo: locali, personale, piattaforma ed strumenti.
- Tecniche di programmazione sicura.
- Gestione del codice sorgente:
  - controllo degli accessi;
  - controllo delle versioni.

Se si sviluppa *software* in casa...

- Condizioni di manutenzione.

- Ambiente di sviluppo: locali, personale, piattaforma ed strumenti.
- Tecniche di programmazione sicura.
- Gestione del codice sorgente:
  - controllo degli accessi;
  - controllo delle versioni.

Per realizzare l'accettazione:

- Prove di accettazione
  - dati di prova;
  - se non sono reali, devono essere realistici;
  - se non si può evitare che siano reali, si devono controllare copie ed accesso;
  - prove funzionali (dei servizi di sicurezza);
  - simulazione di attacchi;
  - prove di carico;
  - intrusione controllata (ethical hacking);
  - ispezione di servizi/ispezione del codice;
  - fughe di informazioni: canali nascosti, attraverso i log, etc.;
  - "back door" di accesso;
  - scalata dei privilegi;
  - problemi di riempimento della memoria (buffer overflow);
  - accreditamenti.

Per realizzare la distribuzione:

- Inventario delle applicazioni in produzione;
- Gestione dei cambiamenti: normativa e procedure;
- Creazione di chiavi.

Durante l'operazione:

- Normativa e procedure di...
  - gestione degli utenti;
  - gestione delle chiavi;
  - gestione dei log;
  - gestione degli incidenti: registro delle evidenze, escalation, piano di emergenza e di ripristino.
- Analisi dei *log*: strumenti, criteri, procedure,...
- Manuali d'uso: amministratori, operatori ed utenti.
- Formazione: iniziale e continua per amministratori, operatori ed utenti

Nei cicli di manutenzione:

- Normativa e procedure di...

- richiesta di manutenzione;
- approvazione, includendo l'analisi differenziale dei rischi, approvazione nel caso di nuove contromisure.

Conclusione

- Distruzione dei dati di produzione.
- Copia e custodia dei dati, quando richiesta per legge o per politica interna.
- Eliminazione del codice: eseguibili, dati di configurazione e account degli utenti.
- Revisione delle copie di sicurezza.

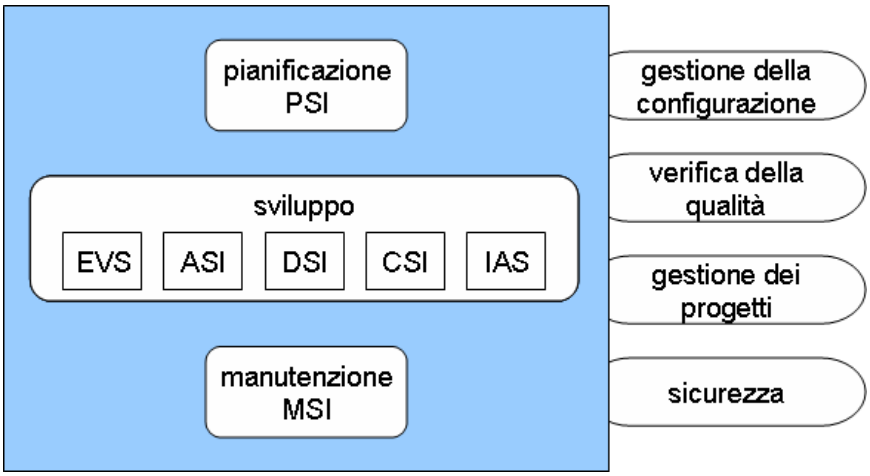
4.5. "Metrica" versione 3

La metodologia "Metrica" versione 3 offre alle organizzazioni uno strumento utile per rendere sistematiche le attività a supporto del ciclo di vita del *software* all'interno dell'ambito di analisi, permettendo di raggiungere i seguenti obiettivi:

- Fornire o definire sistemi informativi che aiutino a conseguire gli obiettivi dell'organizzazione mediante la definizione di un ambito strategico per lo sviluppo degli stessi.
- Dotare l'organizzazione di prodotti *software* che soddisfino i requisiti degli utenti dando una maggiore importanza all'analisi dei requisiti.
- Migliorare la produttività dei dipartimenti dei sistemi, delle tecnologie delle informazioni e delle comunicazioni, permettendo una maggiore capacità di adattamento ai cambiamenti e tenendo in considerazione quanto possibile il riuso.
- Facilitare la comunicazione e la comprensione tra i partecipanti nella produzione di *software* lungo il ciclo di vita del progetto, tenendo in considerazione il loro ruolo e le loro responsabilità, così come i requisiti di ognuno.
- Facilitare l'operatività, la manutenzione e l'uso dei prodotti *software* ottenuti.

Nel caso lo sviluppo dell'applicazione si attenga alla metodologia Metrica versione 3, gli aspetti precedentemente trattati per assicurare che la nuova applicazione non alteri in modo incontrollato lo stato di rischio dell'organizzazione dovranno essere tenuti in considerazione durante il processo di sviluppo.

"Metrica" versione 3 identifica 3 processi, 5 sottoprocessi e 4 interfacce:



PSI-pianificazione del sistema informativo

EVS-studio di fattibilità del sistema

ASI-analisi del sistema informativo

DSI-progettazione del sistema informativo.

CSI-costruzione del sistema informativo

IAS-installazione ed accettazione del sistema

MSI-manutenzione del sistema informativo

L'interfaccia di sicurezza permette la comunicazione tra i compiti di sviluppo ed i compiti di analisi e gestione dei rischi.

- La direzione apporta i servizi necessari e la qualità della sicurezza desiderata.
- Il gruppo di sviluppo apporta gli elementi tecnici che realizzano l'applicazione.
- Il gruppo di analisi dei rischi apporta un giudizio critico sulla sicurezza del sistema.

Ovvero si considerano simultaneamente differenti requisiti:

- di servizio, provenienti dalla direzione;
- tecnici, provenienti dal gruppo di sviluppo;
- di sicurezza, provenienti dal gruppo di analisi dei rischi.

Questo dà origine ad un'interrelazione continua tra il gruppo di sviluppo e il gruppo di sicurezza che, attraverso l'interfaccia della sicurezza, vanno eseguendo ogni passaggio presente in Metrica. È importante sottolineare che il conseguimento di un livello di sicurezza può richiedere modifiche nei componenti tecnici del sistema; allo stesso modo i dettagli tecnici possono alterare l'analisi di sicurezza. In qualsiasi caso, il punto di accordo tra i componenti (asset) e lo stato di sicurezza (impatto e rischio) deve essere approvato dalla direzione dell'organizzazione.

Come indicato precedentemente, si può distinguere tra la sicurezza del processo di sviluppo (compiti di SPD) e la sicurezza del sistema informativo (SSI). I compiti dell'interfaccia si organizzano secondo la sua pertinenza ad uno o all'altro obiettivo di sicurezza.

4.5.1. SPD-sicurezza del processo di sviluppo

Quello che si tratta in questa sezione riguarda a tutti i processi e sottoprocessi di Metrica: PSI, EVS, ASI, DSI, CSI, IAS e MSI.

L'interfaccia di sicurezza di Metrica identifica fino a 4 compiti che sono ripetuti in ogni processo. Qui di seguito sono trattati in modo compatto:

Compiti inclusi nell'interfaccia di sicurezza di Métrica v3
PSI: Pianificazione del sistema informativo SEG 1: Pianificazione della sicurezza richiesta nel processo di PSI PSI-SEG 1.1: Studio della sicurezza richiesta nel processo di PSI PSI-SEG 1.2: Organizzazione e pianificazione SEG 4: Catalogazione degli output generati durante il processo di PSI PSI-SEG 4.1: Classificazione e catalogazione degli output generati durante il processo di PSI
EVS: Studio di fattibilità del sistema SEG 1: Studio della sicurezza richiesta nel processo di EVS

EVS-SEG 1.1: Studio della sicurezza richiesta nel processo EVS SEG 2: Selezione del gruppo di sicurezza EVS-SEG 2.1: Selezione del gruppo di sicurezza SEG 6: Catalogazione degli output generati durante il processo di EVS SEG 6.1: Classificazione e catalogazione degli output generati durante il processo di EVS
ASI: Analisi del sistema informativo SEG 1: Studio della sicurezza richiesta nel processo di ASI ASI-SEG 1.1: Studio della sicurezza richiesta nel processo ASI SEG 4: Catalogazione degli output generati durante il processo di ASI ASI-SEG 4.1: Classificazione e catalogazione degli output generati durante il processo di ASI
DSI: Progettazione del sistema informativo SEG 1: Studio della sicurezza richiesta nel processo di DSI DSI-SEG 1.1: Studio della sicurezza richiesta nel processo DSI SEG 5: Catalogazione degli output generati durante il processo di DSI DSI-SEG 5.1: Classificazione e catalogazione degli output generati durante il processo di DSI
CSI: Costruzione del sistema informativo SEG 1: Studio della sicurezza richiesta nel processo di CSI CSI-SEG 1.1: Studio della sicurezza richiesta nel processo CSI CSI SEG 4: Classificazione degli output generati durante il processo di CSI CSI-SEG 4.1: Classificazione e catalogazione degli output generati durante il processo di CSI
IAS: Installazione ed accettazione del sistema SEG 1: Studio della sicurezza richiesta nel processo di IAS SEG 1.1: Studio della sicurezza richiesta nel processo IAS SEG 4: Catalogazione degli output generati durante il processo di IAS SEG 4.1: Classificazione e catalogazione degli output generati durante il processo di IAS
MSI: Manutenzione del sistema informativo SEG 1: Studio della sicurezza richiesta nel processo di MSI MSI-SEG 1.1: Studio della sicurezza richiesta nel processo MSI MSI-SEG 3: Catalogazione degli output generati durante questa fase SEG 3.1: Classificazione e catalogazione degli output generati durante questa fase

Asset da considerare

In ogni processo si richiede un'analisi dei rischi specifica che contempli:

- i dati trattati:
  - specifiche e documentazione dei sistemi;
  - codice sorgente;
  - manuali dell'operatore e dell'utente;
  - dati di prova.
- l'ambiente *software* di sviluppo:
  - strumenti di trattamento della documentazione: generazione, pubblicazione, controllo di documentazione, etc.;
  - strumenti di trattamento del codice: generazione, compilazione, controllo delle versioni, etc.
- l'ambiente *hardware* di sviluppo: apparecchiature centrali, posti di lavoro, apparecchiature di archiviazione, etc.

- l'ambiente di comunicazioni di sviluppo;
- i siti;
- il personale coinvolto: sviluppatori, personale di manutenzione ed utenti (di prove).

Attività

Si seguono questi passi:

1. il gruppo di sviluppo espone attraverso il capo progetto gli elementi coinvolti;
2. il gruppo di analisi dei rischi riceve attraverso il direttore di sicurezza le informazioni degli asset coinvolti;
3. il gruppo di analisi dei rischi realizza l'analisi;
4. il gruppo di analisi dei rischi espone attraverso il suo direttore lo stato di rischio, proponendo una serie di misure da prendere;
5. il gruppo di sviluppo elabora un relazione del costo che supporrebbero le misure raccomandate, includendo costi di sviluppo e deviazioni nei termini di consegna;
6. la direzione qualifica il rischio e decide le contromisure da instaurare sentendo la relazione congiunta di analisi dei rischi e il costo delle soluzioni di proposte;
7. il gruppo di analisi dei rischi elabora le relazioni corrispondenti alle soluzioni adottate;
8. il gruppo di sicurezza elabora la normativa di sicurezza pertinente;
9. la direzione approva il piano per eseguire il processo con la sicurezza richiesta.

Risultati dell'analisi e della gestione dei rischi

In tutti i casi:

- contromisure raccomandate;
- norme e procedure di trattamento delle informazioni.

Altre considerazioni

Sebbene ogni processo richieda la sua analisi dei rischi specifica, è certo che si tratta di modelli estremamente simili per cui il maggior impegno sarà richiesto nell'elaborare il primo, essendo gli altri adattamenti successivi.

Nei primi processi, particolarmente in PSI, possono apparire contribuzioni di alto livello che riguardano la normativa di sicurezza dell'organizzazione e finanche la politica di sicurezza aziendale.

Tra le norme e le procedure generate è da sottolineare la necessità di una normativa di classificazione della documentazione e delle procedure per il suo trattamento.

In tutti i processi si deve prestare una speciale attenzione al personale inserito. Di base è opportuno:

- identificare i ruoli e le persone;
- determinare i requisiti di sicurezza di ogni ruolo ed incorporarli ai criteri di selezione e alle condizioni contrattuali;
- limitare l'accesso alle informazioni: solo in base alla necessità;
- segregare i compiti; in particolare evitare la concentrazione in una sola persona di quelle applicazioni o parti di applicazioni soggette ad un forte rischio;

4.5.2. SSI-sicurezza del sistema informativo

Tutta la vita di un sistema informativo può essere vista come un'insieme di fasi di concretizzazione crescente, da una prospettiva molto globale durante i processi di pianificazione fino ad una visione in dettaglio durante lo sviluppo e l'impiego. Ciò nonostante, questo ciclo di vita non è lineare, ma frequentemente deve valutare opzioni alternative e rivedere decisioni prese.

L'analisi dei rischi deve fondare le sue stime di impatto e di rischio nella realtà dei sistemi, concretizzata nei suoi asset. Di conseguenza, si può concepire il modello dei valori come evolutivo, raccogliendo in ogni momento il livello di dettaglio di cui si dispone. Magerit, come metodologia, permette un trattamento sistematico ed omogeneo che è essenziale per poter paragonare opzioni alternative e per gestire l'evoluzione dei sistemi.

L'utilizzazione di strumenti di supporto deve permettere di:

1. definire un modello iniziale (PSI),
2. studiarne le variazioni (EVS e ASI),
3. passare dal generale al concreto, prevenendo minacce potenziali e preparando meccanismi di rilevamento e reazione (DSI e CSI),
4. dirigere la loro accettazione e i loro impiego (ASI),
5. rivedere periodicamente i cambiamenti che avvengono (MSI).

Uso dei compiti della metodologia Magerit

Processo P1: Pianificazione

Attività A1.1: Studio dell'opportunità

Compito T1.1.1: Determinazione dell'opportunità

Questo compito si riduce alla decisione, interna, di sviluppare il sistema informativo tenendo in considerazione la sicurezza.

Attività A1.2: Determinazione dell'ambito del progetto

Compito T1.2.1: Obiettivi e restrizioni generali

Quelli del sistema informativo in sviluppo.

Compito T1.2.2: Determinazione di ambito e limiti

Quelli del sistema informativo in sviluppo.

Compito T1.2.3: Identificazione dell'ambiente esterno

Quelli del sistema informativo in sviluppo.

Compito T1.2.4: Stima di dimensioni e costi

Parte di progetto (o dei progetti) di sviluppo del sistema informativo.

Attività A1.3: Pianificazione del progetto

Compito T1.3.1: Valutare la distribuzione del lavoro e pianificare le interviste

Questo compito è portato a termine come in qualsiasi progetto AGR. Questo compito si deve realizzare con il primo processo, PSI, conservando la relazione delle interviste per il resto dei processi, salvo aggiustamenti puntuali che emergano come necessari.

Compito T1.3.2: Organizzare i partecipanti

Questo compito è portato a termine come in qualsiasi progetto AGR. durante il primo processo, PSI, deve stabilirsi la relazione dei partecipanti da intervistare, senza precisare oltre il ruolo che svolgono. Con l'avanzare dello sviluppo del sistema, si andranno identificando le persone che svolgono i ruoli previsti.

Compito T1.3.3: Pianificare il lavoro

Parte di progetto (o dei progetti) di sviluppo del sistema informativo.

Attività A1.4: Lancio del progetto

Compito T1.4.1: Adattare i questionari

Questo compito è portato a termine come in qualsiasi progetto AGR. Si deve realizzare con il primo processo, PSI, mantenendolo fisso per il resto dei processi, salvo aggiustamenti puntuali.

Compito T1.4.2: Criteri di valorizzazione

Questo compito si porta a termine come in qualsiasi progetto AGR. Si deve realizzare con il primo processo, PSI, mantenendo i criteri stabiliti per il resto dei processi.

Compito T1.4.3: Mezzi necessari

Parte di progetto (o dei progetti) di sviluppo del sistema informativo.

Compito T1.4.4: Sensibilizzazione

Parte di progetto (o dei progetti) di sviluppo del sistema informativo.

Processo P2: Analisi dei rischi

Attività A2.1: Caratterizzazione degli asset

Compito T2.1.1: Identificazione degli asset

Nei primi processi, PSI, si identificano asset generici. Avanzando nello sviluppo, questa identificazione si fa più precisa in modo che gli l'asset generici si trasformano in asset concreti. La concretizzazione deve essere massima una volta giunti al processo di CSI.

Compito T2.1.2: Dipendenze tra asset

Nei primi processi, PSI, appaiono conoscenze generiche. Avanzando nello sviluppo, le dipendenze si vanno specificando mentre gli asset generici si trasformano in asset concreti. La concretizzazione deve essere massima una volta giunti al processo di CSI.

Compito T2.1.3: Valorizzazione degli asset

La valorizzazione dei servizi finali e dei dati essenziali si può realizzare praticamente dal primo processo di PSI, sebbene durante l'avanzamento i servizi e/o i dati possano frazionarsi, richiedendo una valorizzazione particolare che mai dovrà supporre il superamento della valorizzazione dei servizi o dei dati d'insieme. Si possono quindi disgregare i servizi e/o i dati in frazioni di minore valore.

Tipicamente la valorizzazione del resto degli asset si può analizzare come semplice valore cumulativo dagli asset superiori, sfruttando le relazioni di dipendenza.

Attività A2.2: Caratterizzazione delle minacce

Compito T2.2.1: Identificazione delle minacce

Le minacce su asset generici possono essere incluse dal primo processo di PSI; ma man mano che si va concretizzando l'insieme dettagliato dei componenti deve includere minacce specifiche della tecnologia che si impiega.

Compito T2.2.2: Valorizzazione delle minacce

Questo compito è portato a termine come in qualsiasi progetto AGR.

Attività A2.3: Caratterizzazione delle contromisure

Compito T2.3.1: Identificazione delle contromisure esistenti

Buona parte delle contromisure possono essere incluse fin dal primo processo di PSI.

Ciò nonostante, le contromisure di carattere tecnico dovranno farsi più precise con il concretizzarsi dell'insieme dettagliato dei componenti e delle tecnologie che si impiegano.

Compito T2.3.2: Valorizzazione delle contromisure esistenti

Questo compito è portato a termine come in qualsiasi progetto AGR.

Attività A2.4: Stima dello stato del rischio

Compito T2.4.1: Stima dell'impatto

Questo compito è portato a termine come in qualsiasi progetto AGR.

Compito T2.4.2: Stima del rischio

Questo compito è portato a termine come in qualsiasi progetto AGR.

Compito T2.4.3: Interpretazione dei risultati

Questo compito è portato a termine come in qualsiasi progetto AGR.

Processo P3: Gestione dei rischi

Attività A3.1: Presa di decisioni

Compito T3.1.1: Qualificazione dei rischi

Questo compito è portato a termine come in qualsiasi progetto AGR.

Alla presa di decisioni deve partecipare tanto il gruppo di sviluppo quanto il gruppo di analisi dei rischi.

Attività A3.2: Elaborazione del piano principale di sicurezza delle informazioni

Compito T3.2.1: Programmi di sicurezza

Questo compito resta incluso nei compiti di sviluppo.

Compito T3.2.2: Piano di esecuzione

Questo compito resta incluso nei compiti di sviluppo.

Attività A3.3: Esecuzione del piano

Compito T3.3.*: Esecuzione di ogni programma di sicurezza

Questi compiti restano inclusi nei compiti di sviluppo.

Altre considerazioni

È importante portare a termine le differenti analisi dei rischi in modo evolutivo, includendo maggiore dettaglio con l'avanzare dello sviluppo; ma mai ricominciando da zero.

Nei primi processi, particolarmente in PSI, possono apparire contribuzioni di alto livello che riguardino la normativa di sicurezza dell'organizzazione e persino la stessa politica di sicurezza aziendale.

Le norme e le procedure che sono derivate da ogni processo vanno costituendo l'insieme di norme e procedure che si impiegano durante l'uso del sistema.

- Tipicamente la normativa deve essere chiusa nei primi processi: PSI, EVS e ASI, essendo infrequente la sua modifica nei processi seguenti.
- Al contrario, le procedure non si possono ottenere fino a non aver concretizzato il dettaglio nei processi di DSI, CSI e IAS. Non si devono poi modificare, salvo aggiustamenti e correzioni, nei processi seguenti.
- Il processo IAS porta norme e procedure all'impiego pratico.
- Il processo di MSI può includere la modifica di norme o procedure erronee, o la cancellazione di norme o procedure incomplete che non abbiano contemplato tutte le circostanze pratiche.

Il conto dettagliato delle contromisure deve includere sia i meccanismi di azione sia i meccanismi di configurazione, monitoraggio e controllo della loro efficacia ed efficienza. È frequente che appaiano alcuni sviluppi specificamente destinati a configurare l'insieme di contromisure e a monitorare la loro operatività.

Compiti inclusi nell'interfaccia di sicurezza di Métrica v3
PSI: Pianificazione del sistema informativo SEG 2: Valutazione del rischio per l'architettura tecnologica PSI-SEG 2.1: Studio e valorizzazione del rischio delle alternative per l'architettura tecnologica PSI-SEG 2.2: Revisione della valorizzazione del rischio delle alternative per l'architettura tecnologica SEG 3: Determinazione della sicurezza nel piano di azione PSI-SEG 3.1: Determinazione della sicurezza nel piano di azione
EVS: Studio di fattibilità del sistema SEG 3: Raccomandazioni addizionali di sicurezza per il sistema informativo EVS-SEG 3.1: Elaborazione di raccomandazioni di sicurezza SEG 4: Valutazione della sicurezza delle soluzioni alternative EVS-SEG 4.1: Valorizzazione e valutazione della sicurezza delle soluzioni alternative SEG 5: Valutazione dettagliata della sicurezza della soluzione proposta EVS-SEG 5.1: Descrizione dettagliata della sicurezza della soluzione proposta
ASI: Analisi del sistema informativo SEG 2: Descrizione delle funzioni e dei meccanismi di sicurezza ASI-SEG 2.1: Studio delle funzioni e dei meccanismi di sicurezza da realizzare SEG 3: Definizione dei criteri di accettazione della sicurezza ASI-SEG 3.1: Aggiornamento del piano delle prove
DSI: Progettazione del sistema informativo SEG 2: Specifica dei requisiti di sicurezza dell'ambiente tecnologico DSI-SEG 2.1: Analisi dei rischi dell'ambiente tecnologico SEG 3: Requisiti di sicurezza dell'ambiente di sviluppo DSI-SEG 3.1: Identificazione dei requisiti di sicurezza dell'ambiente di sviluppo SEG 4: Progettazione delle prove di sicurezza DSI-SEG 4.1: Progettazione delle prove di sicurezza
CSI: Costruzione del sistema informativo SEG 2: Valutazione dei risultati delle prove di sicurezza CSI-SEG 2.1: Valutazione dei risultati delle prove di sicurezza SEG 3: Elaborazione del piano di formazione di sicurezza CSI-SEG 3.1: Elaborazione del piano di formazione di sicurezza
ASI: Installazione ed accettazione del sistema SEG 2: Revisione delle misure di sicurezza nell'ambiente operativo ASI-SEG 2.1: Revisione delle misure di sicurezza nell'ambiente operativo

SEG 3: Valutazione dei risultati delle prove di sicurezza di installazione del sistema ASI-SEG 3.1: Studio dei risultati delle prove di sicurezza di installazione del sistema SEG 5: Revisione delle misure di sicurezza nell'ambiente di produzione ASI-SEG 5.1: Revisione delle misure di sicurezza nell'ambiente di produzione
MSI: Manutenzione del sistema informativo SEG 2: Specifica e identificazione delle funzioni e dei meccanismi di sicurezza MSI-SEG 2.1: Studio delle necessità MSI-SEG 2.2: Analisi delle funzioni e di meccanismi di sicurezza interessati o nuovi

4.6. Riferimenti

- NIST Special Publication 800-64, "Security Considerations in the Information System Development Life Cycle", Rev.1. June 2004.
- NIST Special Publication 800-27 Rev. A, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)", Rev. A, June 2004.
- "Seguridad de las Tecnologías de la Información. La construcción de la confianza para una sociedad conectada" E.Fernández-Medina e R.Moya (editori). AENOR, 2003.
- Metodologia di Pianificazione, Sviluppo e Manutenzione dei sistemi informativi. Métrica v3. Consejo Superior de Informática y para el Impulso de la Administración Electrónica, 2000.

5. Consigli pratici

Tutta l'impostazione precedente può risultare alquanto astratta e non permettere all'analista di progredire con profitto attraverso i passi indicati. Per questo si è considerato opportuno includere alcuni commenti che possano servire come guida.

Si raccomanda anche la consultazione del "catalogo degli elementi" che raccoglie tipologie di asset, dimensioni di valorizzazione, guide di valutazione, cataloghi di minacce e di contromisure.

5.1. Per identificare gli asset

È opportuno ripetere che interessano solo le risorse dei sistemi informativi che hanno un valore per l'organizzazione, sia in sé stessi, sia perché su di loro si appoggiano asset di valore.

A titolo di esempio, un web server di presentazione è un asset con uno scarso valore proprio. Questo si può verificare perché non è normale che un'organizzazione dispieghi un server web di presentazione a meno che ne abbia bisogno per prestare un servizio. Tutto il suo valore è imputabile a:

- l'indisponibilità del server causa l'interruzione del servizio; il costo che comporta l'interruzione del servizio è il valore di disponibilità che si imputerà al server;
- l'accesso non controllato al server mette a rischio la segretezza dei dati che presenta; il costo che comporta la perdita di riservatezza dei dati è il valore di riservatezza che si imputerà al server;
- ... e così via per le differenti dimensioni prese in considerazione.

Gli intangibili

Certi elementi di valore per le organizzazioni sono di natura intangibile:

- credibilità o buona immagine;
- conoscenza accumulata;
- indipendenza di criterio o modo di agire;
- privacy delle persone;
- integrità fisica delle persone.

Questi elementi possono essere aggiunti all'analisi dei rischi come asset o come elementi di valorizzazione. La quantificazione di questi concetti è spesso difficile, ma in un modo o nell'altro non ci si può dimenticare che quello che si deve proteggere in ultima istanza è la missione dell'organizzazione ed il valore di questa risiede appunto negli asset intangibili, come già si considerava in Magerit versione 1.0.

Identificazione degli asset

Forse la migliore approssimazione per identificare gli asset è domandare direttamente:

- Quali asset sono fondamentali per raggiungere gli obiettivi?
- Esistono più asset da proteggere per obblighi di legge?
- Esistono asset collegati ai precedenti?

Non sempre è evidente che cosa un asset rappresenti singolarmente. Se per esempio in una unità ci sono 300 postazioni di lavoro basate su PC, tutte identiche agli effetti della configurazione e dati che

trattano, non è conveniente analizzare 300 asset identici. Basta analizzare un PC generico le cui problematiche rappresentano quelle di tutti. Raggruppare semplifica il modello.

Altre volte si presenta il caso contrario, un server centrale che assolve mille funzioni: file server, server di messaggistica, di intranet, del sistema di gestione documentale e... In questo caso è opportuno segregare i servizi prestati come servizi (interni) indipendenti. Solo quando si arriva al livello di gruppo fisico si devono far confluire in un unico gruppo tutti i servizi. Se nel futuro si riuscirà a separare i servizi tra più server, allora sarà facile rivedere il modello dei valori e delle dipendenze.

5.2. Per individuare e modellizzare le dipendenze tra asset

A volte è più difficile di quanto ci si aspetti perché i responsabili degli asset solgono essere più preoccupati per il collegamento funzionale tra asset che per la dipendenza nel senso di propagazione del valore.

Bisogna far capire all'interlocutore che non si cerca cosa serve affinché il sistema funzioni, ma, al contrario, si cerca dove può fallire il sistema o, più precisamente, dove può essere compromessa la sicurezza degli asset.

- Se alcuni dati sono importanti per la loro riservatezza, è necessario sapere in quali posti risiedono detti dati e per quali ambienti circolano: in questi punti possono essere rivelati.
- Se alcuni dati sono importanti per la loro integrità, è necessario sapere in quali posti risiedono detti dati e per quali ambienti circolano: in questi punti possono essere alterati.
- Se un servizio è importante per la sua disponibilità, è necessario sapere quali elementi si usano per prestare tale servizio: il fallimento di tali elementi può arrestare il servizio.

Queste considerazioni possono essere impostate attraverso argomenti del tipo:

- Volendo accedere a questi dati, dove si attaccherebbe?
- Volendo arrestare questo servizio, dove si attaccherebbe?

Questa impostazione di "mettersi al posto dell'attaccante" è quella che dà fondamento alle tecniche denominate "alberi di attacco" che sono collegate a quello che in questa metodologia sono le dipendenze. In effetti, un asset può essere attaccato direttamente o indirettamente attraverso un altro asset da cui dipenda.

Le precedenti considerazioni possono sfociare in un diagramma "piatto" di dipendenze che si può (ed è opportuno ad effetti pratici) convertire in un albero più compatto. Così, è normale dire che i servizi dipendono dal gruppo, che dipende a sua volta dai locali dove sono situate le apparecchiature, senza bisogno di esplicitare i servizi che dipendono dai locali. È frequente identificare "servizi interni" o "servizi orizzontali" quelli che sono insiemi di asset votati ad una certa funzione. Questi servizi intermedi sono efficaci per compattare il grafo di dipendenze, perché le dipendenze di detti di servizi si interpretano senza ambiguità come dipendenze di tutti gli elementi che prestano il servizio.

Quando si usino diagrammi di flusso di dati o diagrammi di processi, non deve preoccupare tanto il percorso che seguono i dati quanto l'insieme (disordinato) di elementi che intervengono. Un processo dipende da tutti gli asset che appaiono nel suo diagramma. Alcuni dati dipendono da tutti gli ambienti per cui transitano. Tanto in alcuni come in altri diagrammi è frequente trovare descrizioni gerarchizzate dove un processo si suddivide in livelli di maggior dettaglio. Queste gerarchie di diagrammi possono aiutare ad elaborare il grafo delle dipendenze.

Errori tipici

Non è corretto dire che un'applicazione dipende dai dati che tratta. Il ragionamento di coloro che affermano ciò è che "l'applicazione non funziona senza dati", che è corretto; ma non è quello che interessa considerare. Piuttosto è tutto il contrario: i dati dipendono dell'applicazione. In termini di

valore, si può assicurare che l'applicazione non vale niente senza dati. Siccome il valore è una proprietà dei dati, è codesto valore quello che l'applicazione eredita. Poi i dati dipendono dell'applicazione. Da un altro punto di vista, attraverso l'applicazione si può accedere ai dati, convertendo l'applicazione nella via di attacco ai dati.

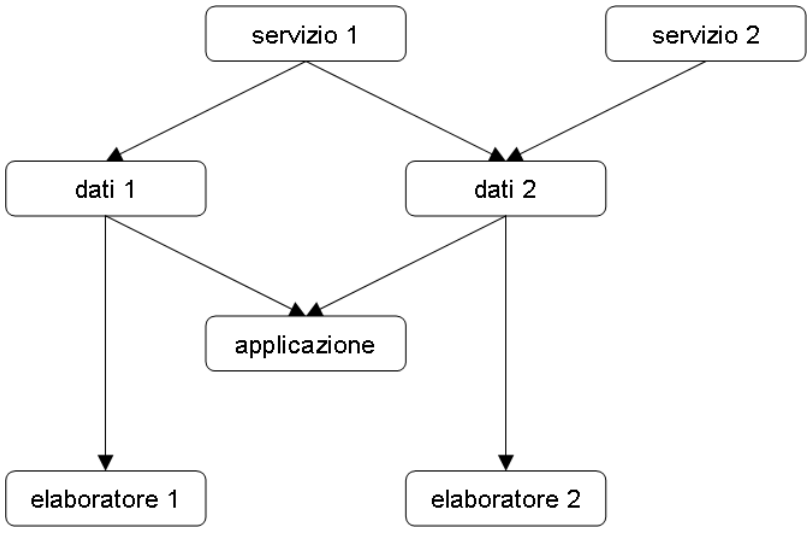
Dato che dati ed applicazioni solgono riunirsi per la prestazione di un servizio, il valore del servizio si trasmette tanto ai dati quanto alle applicazioni che intervengono.

male	***bene***
▪ servizio→ applicazione ▪ applicazione→ dati	▪ servizio→ dati ▪ dati→ applicazione ▪ servizio→ applicazione

Non è corretto dire che un'applicazione dipende dall'apparecchiatura su cui si esegue. Il ragionamento di coloro che affermano che "l'applicazione non funzionare senza apparecchiature" è corretto; ma non è quello che interessa considerare. Se tanto l'applicazione quanto le apparecchiature sono necessarie per prestare un servizio, lo si deve dire chiaramente, senza cercare cammini contorti.

male	***bene***
▪ servizio→ applicazione ▪ applicazione→ apparecchiatura	▪ servizio→ applicazione ▪ servizio→ apparecchiatura

Gli errori illustrati alle volte passano inosservati fintanto che il sistema è molto ridotto (se c'è solo un servizio, un'applicazione e un'apparecchiatura); ma appaiono immediatamente appena il sistema cresce. Per esempio, un'applicazione X può essere eseguita su differenti apparecchiature con differenti dati per prestare differenti servizi. Risulta allora impossibile mettere in relazione l'applicazione con uno o più apparecchiature, salvo considerare ogni caso.



sono ben modellizzate le dipendenze?

Stabilire le dipendenze è un compito delicato che può finire male. Prima di dare per buono un modello di dipendenze si devono individuare per ogni asset tutti gli asset da cui dipende direttamente o

indirettamente e si deve rispondere positivamente alle domande:

- Ci sono tutti quelli che devono? Cioè, si sono identificati tutti gli asset attraverso i quali può essere attaccato indirettamente l'asset in esame?
- Devono esserci tutti quelli che ci sono? Cioè, se realmente l'asset in esame può essere attaccato attraverso tutti questi asset da cui dipende?

Visto che la relazione di dipendenza propaga il valore cumulativo, trovare un asset senza valore cumulativo è sintomo che le dipendenze sono mal modellizzate o, semplicemente, che l'asset è irrilevante.

5.3. Per valorizzare gli asset

E' sempre opportuno valorizzare le informazioni o i dati che costituiscono la ragion d'essere del sistema informativo.

Se si sono modellizzati servizi finali (prestati ad utenti esterni all'ambito di analisi), è opportuno valutarli allo stesso modo.

È facile identificare asset di tipo dato o informazione e valorizzarli seguendo le classificazioni guidate in base alle loro caratteristiche individuali o alla loro classificazione di sicurezza. E' comunque molto più delicato valorizzare dati di tipo commerciale od operativo perché si deve guardare alle conseguenze del danno subito.

Il resto degli asset può frequentemente non essere valorizzato, perché il loro valore più importante è supportare i dati e/o i servizi e questo calcolo lo forniscono i valori delle dipendenze.

Nonostante ciò, si considera opportuno valorizzare altri tipi di asset...

Gli asset più semplici da valorizzare sono quelli che si acquistano in commercio. Se subisce un danno a uno di essi, se ne deve mettere un altro. Questo costa denaro e tempo (quindi, più denaro). Si parla di un costo di rimpiazzamento. Salvo eccezioni, frequentemente accade che il costo degli asset fisici risulti trascurabile a fronte di altri costi, potendo essere trascurato.

E' difficile valorizzare le persone, in genere; ma se un ruolo suppone una formazione lenta e faticosa, si deve tenere in considerazione che la si persona che si disimpegna da questo ruolo si converte in una risorsa molto preziosa, perché il suo "costo di rimpiazzamento" è notevole.

In qualsiasi caso, per valorizzare un asset, si deve identificare il responsabile, che sarà la persona adeguata per valorizzare l'asset. Si deve aiutare tale responsabile tramite tavole di valorizzazione come quelle del capitolo 4 del "catalogo degli elementi" che, adattate al caso concreto, permettono di tradurre la percezione del valore in una misura qualitativa o quantitativa dello stesso.

Spesso non esiste un responsabile unico e individuale di un asset e/o servizio, ma varie persone all'interno dell'organizzazione hanno un'opinione qualificata a riguardo. Le si deve ascoltare tutte ed arrivare ad un consenso. Se il consenso non è ovvio, è possibile richiedere:

un confronto: riunendo quelli che divergono tentando di farli arrivare ad un'opinione comune;

un Delphi: inviando questionari a quelli che divergono e fare in modo che convergano su di una posizione comune.

Nei processi di valorizzazione degli asset è frequente ricorrere a persone differenti per valorizzare asset differenti. E' frequente che ogni intervistato consideri il suo asset come della massima importanza; tanto più frequentemente quanto più specializzato è l'intervistato. Siccome molte valorizzazioni sono stime del valore, ci si deve assicurare che tutti usino la stessa scala di stima. Per questo è importante usare una tavola come quella del capitolo 4 del "catalogo degli elementi", direttamente o adattata al caso concreto. E' infine importante che, dopo aver domandato a quelli che si occupano di ogni asset, tutti ricevano una copia della valorizzazione globale del sistema affinché

stimino il valore relativo del "loro asset" e formulino delle opinioni a proposito.

Dati personali

I dati personali sono definiti da leggi e regolamenti, richiedendo che l'organizzazione adotti una serie di misure di protezione indipendenti dal valore dell'asset.

La forma più realistica di affrontare gli asset di carattere personale è caratterizzarli come tali nel livello che gli corrisponda e, inoltre, determinare il loro valore: il danno che comporterebbe la loro diffusione o alterazione indebita. Con questa approssimazione, l'analisi di impatti e rischi permetterà di proteggere i dati sia per obbligo di legge sia per il loro proprio valore.

5.4. Per identificare le minacce

Questo compito può sembrare impossibile: identificare le minacce per ogni asset, in ogni dimensione.

Si può partire dell'esperienza passata, propria o di organizzazioni simili. Quello che è accaduto può ripetersi e, in qualunque caso, è impensabile non tenerlo in considerazione.

Inoltre, un catalogo di minacce come quello presente nel "catalogo degli elementi" aiuta a circoscrivere quello che è opportuno considerare in funzione del tipo di asset e delle dimensioni in cui ha un valore proprio o cumulativo.

Spesso si finisce per ideare scenari di attacco che non sono altro che ipotesi di come un attaccante affronterebbe i nostri sistemi. Questa tecnica è quella che alle volte si denomina "alberi di attacco". Ci si mette nei panni dell'attaccante e si immagina che di agire con le sue nozioni e la sue capacità economiche. Può darsi che sia necessario impostare differenti situazioni a seconda del profilo tecnico dell'attaccante o dei suoi mezzi tecnici ed umani. Queste ipotesi sono interessanti per poter calcolare impatti e rischi, ma saranno anche molto utili all'ora di convincere l'alta direzione e gli utenti sul perché una minaccia non sia solo teorica ma ben reale. In più, quando si valutano le contromisure, questi scenari di attacco possono essere convenientemente riveduti.

5.5. Per valorizzare le minacce

Questo compito può sembrare scoraggiante: determinare la compromissione che causerebbero e la frequenza probabile di occorrenza delle minacce, per ogni asset e in ogni dimensione.

Ogni volta che sia possibile è opportuno partire da dati standard. Nel caso di disastri naturali o di incidenti industriali, si può disporre di serie storiche, generiche o del luogo in cui sono situate le apparecchiature del sistema informativo in esame. Probabilmente si dispone anche di una cronologia che riporti quello che è frequente e quello che "non succede mai".

Più complicato è qualificare gli errori umani; ma l'esperienza permette di andare approssimando valori realistici.

Il più difficile è qualificare gli attacchi intenzionali perché dipendono della sorte, buona o cattiva. Esistono molti motivi che acuiscono il pericolo di una minaccia:

- che non richieda grandi nozioni tecnica da parte dell'attaccante;
- che non richieda grandi investimenti in apparecchiature da parte dell'attaccante;
- che ci sia un enorme beneficio economico in gioco (l'attaccante può arricchirsi);
- che ci sia un enorme beneficio in gioco (l'attaccante può guadagnare fortemente nella sua reputazione, nella sua notorietà...); per questo motivo si evitino le sfide e non si faccia mai sfoggio che il sistema informativo è invulnerabile: non lo è e non si ha interesse che si lo dimostri;

- che ci sia un cattivo ambiente di lavoro, fomentatore di impiegati scontenti che si vendicano attraverso i sistemi, semplicemente per causare danno;
- che ci sia una cattiva relazione con gli utenti esterni, che si vendicano attraverso i nostri sistemi.

Partendo da un valore standard, si devono aumentare o diminuire le sue valorizzazioni di frequenza e di compromissione fino a riflettere il più fedelmente possibile il caso concreto. Spesso non è evidente determinare il valore corretto e bisogna ricorrere a simulazioni che diano un'indicazione. L'uso di certi tipi di strumenti è molto utile per studiare le conseguenze di un certo valore, quello che alcuni autori denominano la sensibilità del modello verso un certo dato. Se si stima che i risultati cambino radicalmente a fronte di piccole alterazioni di una stima di frequenza o compromissione, si deve (1) essere realisti e (2) prestare molta attenzione verso il motivo per cui il sistema è tanto sensibile a qualcosa di così poco concreto e prendere misure orientate a rendere indipendente il sistema, cioè, a non rendere critica una certa minaccia.

Si ricordi che la frequenza non riguarda l'impatto, motivo per cui studiando l'impatto si può modificare la compromissione e, successivamente, studiando il rischio, si può rivedere la frequenza. Non si deve mai accettare un valore ingiustificato di compromissione nella speranza di compensarlo con la frequenza, perché la stima dell'impatto è importante in sé stessa, oltre che per il rischio.

Quale che sia la decisione finale che si prenda per stimare un valore, la si deve documentare perché prima o poi saranno richieste spiegazioni, soprattutto se come conseguenza si raccomandano contromisure costose.

5.6. Per selezionare le contromisure

Probabilmente l'unico modo è quello di scegliere dal catalogo. Si usi un (sistema) esperto che aiuti a valutare quale soluzione è adeguata per ogni combinazione di:

- tipo di asset;
- minaccia a cui è esposto;
- dimensione del valore che è motivo di attenzione;
- livello di rischio.

Spesso si troveranno molte soluzioni per un singolo problema, con differenti livelli di qualità. In questi casi si deve scegliere una soluzione proporzionata ai livelli di impatto e di rischio calcolati.

Molte contromisure sono di basso costo, essendo sufficiente configurare adeguatamente i sistemi o organizzare regole affinché il personale faccia le cose in modo adeguato. Alcune contromisure sono invece realmente costose (per il loro acquisto, dispiegamento, manutenzione periodica, formazione del personale incaricato ...). In questi casi conviene ponderare se il costo della contromisura non supera il rischio potenziale; cioè, effettuare sempre decisioni di spesa che suppongano un risparmio netto.

Infine, e non meno importante, all'ora di dispiegare le contromisure si deve considerare la loro facilità d’uso. L'ideale è che la contromisura sia trasparente in modo che l'utente non debba fare niente o, nell’impossibilità di ciò, meno cose possibili. Questo semplicemente perché una contromisura di complesso impiego richiede personale specializzato ed aggiunge alle minacce che già aveva il sistema la minaccia derivante da un suo erroneo impiego.

5.7. Approssimazioni successive

Il lettore si sarà già reso conto che l'analisi dei rischi può essere molto laboriosa, richiedendo tempo e sforzi. Inoltre, si devono introdurre molti elementi che non sono obiettivi, ma stime dell'analista, il che

implica che ci sia da spiegare e da creare un consenso su quello che significa ogni cosa per non restare esposti ad impatti o rischi che si ignorano o si sottovalutano, né trasformare la paranoia in un dispendio di risorse ingiustificato.

Se si deve essere pratici ed efficaci, è opportuno realizzare approssimazioni successive. Si comincia da un'analisi sommaria, di alto livello, identificando rapidamente ciò che è più critico: asset di grande valore, vulnerabilità manifeste o, semplicemente, raccomandazioni da manuale perché non c'è niente di più prudente che imparare approfittando dell'esperienza di altri. Quest'analisi dei rischi è imperfetta, evidentemente, ma ha senso confidare nel fatto che porta nella direzione corretta. I paragrafi seguenti danno indicazioni di come orientarsi presto verso l'obiettivo finale: avere impatti e rischi sotto controllo.

Si noti che queste approssimazioni imperfette permettono di realizzare rapidamente sistemi ragionevolmente protetti quando non c'è tempo per un'analisi dei rischi in tutta la sua pienezza. Quando, con il tempo, si arriverà alla fase di gestione dei rischi dopo un'analisi esauriente, molto probabilmente accadrà che molte contromisure siano già realizzate, essendoci bisogno solo più dell'introduzione di alcune nuove e/o il miglioramento dell'efficacia di quelle esistenti. Non è quindi lavoro sprecato seguire queste approssimazioni informali.

5.7.1. Protezione di base

È frequente sentir parlare di misure basilari di protezione *(baseline)* che devono essere instaurate in tutti i sistemi, a meno che si dimostri che non sono pertinenti al caso particolare.

Non si discute né si dubita che ai sistemi informativi non può accedere chiunque in qualsiasi momento. Si possono proteggere dal lato fisico o logico, mettendoli in una sala dove non può entrare chiunque, o imponendo un'identificazione di accesso logico.

Questi tipi di ragionamenti si possono applicare con frequenza e portano a dispiegare un minimo di contromisure "di buonsenso comune". Una volta raggiunto quello che è ovvio e non si dovrebbe mai discutere, si possono raggiungere livelli più elaborati, specifici per ogni sistema.

Per applicare un trattamento di base è necessario un catalogo di contromisure. Esistono numerosi fonti, tra cui sono da segnalare:

- norme internazionali, per esempio ISO/IEC 27002:2005;
- norme nazionali;
- norme settoriali;
- norme aziendali, particolarmente frequenti in piccoli dipartimenti di grandi organizzazioni.

I vantaggi di proteggersi secondo un catalogo sono:

- è molto rapido;
- non comporta molto sforzo;
- si ottiene un livello omogeneo con altre organizzazioni simili.

Gli inconvenienti di proteggersi per catalogo sono:

- il sistema può essere protetto a fronte di minacce che non subisce, il che causa una spesa ingiustificata;
- il sistema può essere inadeguatamente protetto a fronte di minacce reali.

In genere, con la protezione di base non si sa quello che si è fatto e, sebbene probabilmente si sia ancora sulla giusta via, non c'è alcun indicatore di cosa manca o di cosa è sovrabbondante. Ciò nonostante, può essere un punto di partenza utile da raffinare in seguito.

La protezione per catalogo può essere raffinata molto considerando il valore degli asset o

quantificando le minacce.

In base alla tipologia degli asset

Se ci sono dati di carattere personale qualificato di alto livello, devono essere crittografati.

Se ci sono dati classificati come confidenziali, dono essere etichettati e crittografati.

A parte il rispetto di legislazione e norme specifiche, si è portata a termine una specie di "vaccinazione preventiva" di asset che di sicuro sono importanti.

Se c'è una rete locale connessa all'esterno, deve esserci un firewall nel punto di connessione.

In base al valore degli asset

Se ci sono tutti i dati operativi su sopporto informatico, devono essere fatte copie di sicurezza.

Se ci sono apparecchiature informatiche, devono essere mantenute allineate con gli aggiornamenti del produttore.

Quello che ha valore deve essere protetto, nel caso gli succedesse qualcosa, senza entrare nel dettaglio su ciò che può succedere esattamente.

In base alle minacce

Se si tratta di un sistema della cosiddetta amministrazione elettronica (una pratica amministrativa non cartacea) o se i sistemi si usano per commerciare elettronicamente (acquisti e vendite non cartacee), si registri accuratamente chi fa che cosa in ogni momento perché se messo di fronte a problemi con gli utenti, si deve poter determinare chi ha ragione e chi paga i danni. Ci sarà anche chi vuole usare i servizi senza avere diritto a ciò (frode).

Tutto ciò di cui si può avere bisogno è necessario, e parte delle responsabilità del responsabile della sicurezza è di disporre delle informazioni corrette quando sia il caso.

In base alle vulnerabilità

Se c'è una rete di apparecchiature datate e si connette ad Internet, devono essere installati dei firewall.

Se c'è un'applicazione in produzione, deve essere mantenuta aggiornata applicando migliorie e correggendo i difetti resi noti dal produttore.

Quando si viene a sapere che i sistemi informativi sono vulnerabili, è necessario proteggerli.

5.8. Riferimenti

- ISO/IEC 27002:2005, "Information technology - Security techniques - Code of practice for information security management", giugno 2005.
- " Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades", MAP, 2004
- C. Alberts and a Dorofee, "Managing information Security Risks. The OCTAVE Approach", Addison Wesley, 2003.
- United States General Accounting Office, Accounting and Information Management Division, "Information Security Risk Assessment - GAO Practices of Leading Organizations".
- Ministerio de Administraciones Públicas, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", MAP, versión 1.0, 1997.

Appendice 1. Glossario

Differenti autori od organizzazioni definiscono gli stessi termini in diverse forme e maniere. Le seguenti tavole riportano definizioni riguardanti l'accezione nella quale sono impiegati i termini in questa guida metodologica, sia in italiano sia in inglese. Delle molteplici definizioni si è selezionata quella preferita in Magerit v2, evidenziandola in grassetto. Quando la definizione proviene da qualche fonte, essa è citata. L'assenza di fonte indica che è definizione propria di questa guida. Salvo casi per cui sussistevano particolari ragioni avverse, si è sempre preferito mantenere la definizione proposta in Magerit v1 (1997).

1.1. Termini in italiano

Accreditamento	Azione di dare facoltà a un sistema o rete di informazioni affinché tratti dati sensibili, determinando il grado con cui la progettazione e la realizzazione di tale sistema soddisfa I requisiti di Sicurezza tecnica prestabiliti [CESID:1997] Accreditation: Formal declaration by the responsible management approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is based on the certification process as well as other management considerations. [15443-1:2005]
Asset	**Risorse del sistema informativo o collegate ad esso, necessarie affinché l'organizzazione operi correttamente e raggiunga gli obiettivi fissati dalla sua direzione. [Magerit:1997]** Asset: Anything that has value to the organization. [13335-1:2004] Asset: A component or part of the total system. Assets may be of four types: physical, application software, data, or end user services. [CRAMM:2003] Asset: Something of value to the enterprise. [Octave:2003] Asset: Any information resource with value that is worth protecting or preserving. [TDIR:2003] Assets: Information or resources to be protected by the countermeasures of a Target of Evaluation. [CC:1999]
AGR	Analisi e Gestione dei Rischi
Minaccia	**Evento che può causare un incidente nell'organizzazione, producendo danni materiali o d'immagine nei suoi asset. [Magerit:1997]** Threat: A potential cause of an incident which may result in harm to a system or organization. [17799:2005][13335-1:2004] Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [800-53:2004] Threat: Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. [CNSS:2003] Threat: An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity. [TDIR:2003] Threat: Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of

	service, or physical destruction or impairment. [CIAO:2000] A threat is an indication of a potential undesirable event. [NSTISSI:1998] Threat: A potential violation of security. [7498-2:1989]service, or physical destruction or impairment. [CIAO:2000] A threat is the indication of a potential undesirable event. [NSTISSI:1998] Threat: a potential violation of security. [7498-2:1989]
Analisi d'impatto	Studio delle conseguenze che avrebbe un fermo di x tempo sull'organizzazione.
Analisi dei rischi	**Processo sistematico per stimare la grandezza dei rischi a cui è esposta un'organizzazione.** Identificazione delle minacce che gravano sui diversi componenti appartenenti o collegati al sistema informativo (noti come 'asset'); per determinare la vulnerabilità del sistema rispetto a codeste minacce e per stimare l'impatto o il grado di compromissione che una sicurezza insufficiente può avere per l'organizzazione, ottenendo certa conoscenza del rischio che si corre. [Magerit:1997] Risk analysis: Systematic use of information to identify sources and to estimate the risk. [17799:2005][Guide 73:2002] Risk assessment: Process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity. [OPSEC] Risk analysis: The systematic process of estimating the magnitude of risks. [13335-1:2004] Risk Analysis: Examination of information to identify the risk to an information system. [CNSS:2003] Risk Assessment:: Process of analyzing threats to and vulnerabilities of an information system, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures. [CNSS:2003] Risk Analysis: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. [TDIR:2003] Risk Assessment: A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations. [TDIR:2003]
Attacco	Qualsiasi azione deliberata volta a violare i meccanismi di sicurezza di un sistema informativo. [CESID:1997]
Audit di sicurezza	Studio ed esame indipendente della storia ed attività di un sistema informativo, con il fine di valutare l'idoneità dei controlli del sistema, assicurare la sua conformità con la struttura di sicurezza e con le procedure operative stabiliti, al fine di scoprire falle nella sicurezza e di raccomandare cambiamenti nelle procedure, nei controlli e nelle strutture di sicurezza.
Autenticità	**Assicurazione dell'identità o della provenienza.** Autenticazione: Caratteristica che prevede il dare e il riconoscere l'autenticità degli asset dell'ambito (di tipo "informazione") e/o l'identificazione degli attori e/o l'autorizzazione da parte di chi autorizza, così come la verifica di questi tre punti. [Magerit:1997] Authenticity: Having an undisputed identity or origin. [OPSEC] Authenticity: The property of being genuine and being able to be verified

	and trusted; confidence in the validity of a transmission, a message, or message originator. [800-53:2004] Authenticity: The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems, and information. [13335-1:2004]
Certificazione	Conferma del risultato di una valorizzazione, e che i criteri di valorizzazione utilizzati sono stati correttamente applicati.
Compromissione	Perdita di valore di un asset come conseguenza della concretizzazione di una minaccia.
Controllo	Vedere contromisura.
Contromisura	**Procedura o meccanismo tecnologico che riduce il rischio.** Control: Means of managing risks, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature. [17799:2005] Countermeasure: Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities. [OPSEC] Safeguard: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [800-53:2004] Safeguard: a practice, procedure or mechanism that treats risk. [13335-1:2004] Countermeasure: Action, device, procedure, technique, or other measure that reduces the vulnerability of an information system. [CNSS:2003] Security safeguard: Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [CNSS:2003] Countermeasure: Any action, device, procedure, technique, or other measure that mitigates risk by reducing the vulnerability of, threat to, or impact on a system. [TDIR:2003]
Dimensione	**(di sicurezza) Un aspetto, differente da altri possibili aspetti, rispetto a cui si può misurare il valore di un asset per il danno che causerebbe la sua perdita di valore.**
Disponibilità	**Garanzia che gli utenti autorizzati abbiano accesso alle informazioni e agli asset associati quando lo richiedono. [17799:2002]** Caratteristica che previene la negazione non autorizzata di accesso ad asset dell'ambito. [Magerit:1997] Availability: The assurance that data transmissions, computer processing systems, and/or communications are not denied to those who are authorized to use them (JCS 1997) [OPSEC] Availability: Ensuring timely and reliable access to and use of information. [800-53:2004] Availability: The extent to which, or frequency with which, an asset must be present or ready for use. [Octave:2003] Availability: Timely, reliable access to data and information services for authorized users. [CNSS:2003] [TDIR:2003] [CIAO:2000] Availability: The property of being accessible and usable upon demand by an authorized entity. [7498-2:1989]
Documento di selezione di controlli	Documento formale in cui, per un insieme di contromisure, si indica se sono da applicare nel sistema informativo in esame o se, al contrario, non ne ha

	ragione.
Frequenza	**Tasso di occorrenza di una minaccia.**
Gestione dei rischi	**Selezione e realizzazione di contromisure per conoscere, prevenire, impedire, ridurre o controllare i rischi identificati.** Selezione e realizzazione delle misure o "contromisure" di sicurezza adeguate per conoscere, prevenire, impedire, ridurre o controllare i rischi identificati e così ridurre al minimo la loro potenzialità o i loro possibili danni. La gestione dei rischi si basa sui risultati ottenuti nell'analisi dei rischi. [Magerit:1997] Risk treatment: process of selection and implementation of measures to modify risk. [17799:2005][13335-1:2004][Guide 73:2002] Risk management: A security philosophy which considers actual threats, inherent vulnerabilities, and the availability and costs of countermeasures as the underlying basis for making security decisions (JSCR 1994). [OP-SEC] Risk management: Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment. [CNSS:2003] The identification, assessment, and mitigation of probabilistic security events (risks) in information systems to a level commensurate with the value of the assets protected. [CIAO:2000]
Impatto	**Conseguenza che la concretizzazione di una minaccia ha su di un asset. [Magerit:1997]** Impact: The result of an information security incident. [13335-1:2004] Impact: The effect of a threat on an organization's mission and business objectives. [Octave:2003] Impact: The effect on the organization of a breach in security. [CRAMM:2003]
Impatto residuo	**Impatto rimanente nel sistema dopo la realizzazione delle contromisure determinate nel piano di sicurezza delle informazioni.**
Incidente	**Evento con conseguenze dannose per la sicurezza del sistema informativo.** Information security event: An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. [17799:2005] Information security incident: Any unexpected or unwanted event that might cause a compromise of business activities or information security. [13335-1:2004] Incident: A successful or unsuccessful action attempting to circumvent technical controls, organizational policy or law. This is often called an attack. [TDIR:2003]
Integrità	**Garanzia dell'esattezza e della completezza delle informazioni e dei metodi impiegati nel loro trattamento. [17799:2002]** Caratteristica che previene la modifica o la distruzione non autorizzata di asset dell'ambito [Magerit:1997]. Information integrity: The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed (NSC EO 1995; JCS 1997). [OPSEC] Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [800-53:2004] Integrity: the property of safeguarding the accuracy and completeness of

	assets. [13335-1:2004] Integrity: the authenticity, accuracy, and completeness of an asset. [Octave:2003] Data integrity: A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [CNSS:2003] [TDIR:2003] [CIAO:2000] Data integrity: The data quality that exists as long as accidental or malicious destruction, alteration, or loss of data does not occur. [CRAMM:2003] Integrity: Condition existing when an information system operates without unauthorized modification, alteration, impairment, or destruction of any of its components. [CIAO:2000]
Mappa dei rischi	**Relazione: Relazione delle minacce a cui gli asset sono esposti.** Threat Analysis: The examination of all actions and events that might adversely affect a system or operation. [TDIR:2003] Threat Assessment: An evaluation of the nature, likelihood, and consequence of acts or events that could place sensitive information and assets as risk. [TDIR:2003]
Modello dei valori	**Relazione: Caratterizzazione del valore che gli asset rivestono per l'organizzazione così come delle dipendenze tra i differenti asset.**
Piano di sicurezza	**Insieme dei programmi di sicurezza che permettono di concretizzare le decisioni di gestione dei rischi.**
Programma di sicurezza	**Insieme di compiti orientati ad affrontare il rischio del sistema. Il raggruppamento si realizza per convenienza, sia perché si tratta di compiti che singolarmente sarebbero poco efficaci, sia perché si tratta di compiti con un obiettivo comune, sia perché si tratta di compiti che concorrono ad un'unicità di azione.**
Progetto di sicurezza	**Programma di sicurezza la cui importanza è tale da richiedere una pianificazione specifica.**
Relazione delle debolezze	**Relazione: Assenze o debolezze delle contromisure che appaiono come opportune per ridurre il rischio sul sistema.**
Rischio	**Stima del grado di esposizione alla concretizzazione di una minaccia su uno o più asset causando danni o problemi all'organizzazione.** Possibilità che si produca un impatto determinato in un asset, in un ambito o in tutta l'organizzazione. [Magerit:1997] Probabilità che una vulnerabilità propria di un sistema informativo sia sfruttata dalle minacce a tale sistema, con l'obiettivo di penetrarlo. [CESID:1997] Risk: combination of the probability of an event and its consequence. [17799:2005][Guide 73:2002] Risk: A measure of the potential degree to which protected information is subject to loss through adversary exploitation. [OPSEC] Risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. [13335-1:2004] Risk: Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. [CNSS:2003] Risk: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk. [TDIR:2003] Total risk: The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). [TDIR:2003]

	Risk: A measure of the exposure to which a system or potential system may be subjected. [CRAMM:2003]
Rischio residuo	**Rischio rimanente nel sistema dopo la realizzazione delle contromisure determinate nel piano di sicurezza delle informazioni.** Rischio che si definisce dopo l'applicazione delle contromisure disposte in uno scenario di simulazione o nel mondo reale. [Magerit:1997] Residual risk: The risk that remains after risk treatment. [13335-1:2004] Residual risk: Portion of risk remaining after security measures have been applied. [CNSS:2003] [CRAMM:2003] Residual Risk: The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards. [TDIR:2003]
Rischio cumulativo	Dato calcolato prendendo in considerazione il valore proprio di un asset ed il valore degli asset che dipendono da esso. Questo valore si combina con la compromissione causata da una minaccia e con la frequenza stimata della stessa.
Rischio riflesso	Dato calcolato prendendo in considerazione solo il valore proprio di un asset. Questo valore è combinato con la compromissione causata da una minaccia e dalla frequenza stimata della stessa, misurate ambedue sugli asset da cui dipende.
Riservatezza	**Garanzia che le informazioni sono accessibili solo dalle entità autorizzate ad avere accesso. [17799:2002]** Caratteristica che previene la divulgazione non autorizzata di asset dell'ambito. [Magerit:1997] Confidentiality: An assurance that information is not disclosed to unauthorized entities or processes (DOD JP 1994; JCS 1997) [OPSEC] Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [800-53:2004] Confidentiality: The requirement of keeping proprietary, sensitive, or personal information private and inaccessible to anyone that is not authorized to see it. [Octave:2003] Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices. [CNSS:2003] [TDIR:2003] Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [7498-2:1989]
Sicurezza	**La capacità delle reti o dei sistemi informativi di resistere, con un determinato livello di fiducia, agli incidenti o alle azioni illecite o malevole che compromettano la disponibilità, autenticità, integrità e riservatezza dei dati immagazzinati o trasmessi e dei servizi che detti reti e sistemi offrono o rendono accessibili.** Information System Security: Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [CNSS:2003]
Sistema informativo	**Gli elaboratori e le reti di comunicazioni elettroniche, così come i dati elettronici immagazzinati, trattati, recuperati o trasmessi dagli stessi nella loro operatività, uso, protezione e manutenzione.** Insieme di elementi fisici, logici, elementi di comunicazione, dati e personale che permettono l'immagazzinamento, trasmissione e trattamento delle informazioni. [Magerit:1997] Qualsiasi sistema o prodotto destinato ad immagazzinare, trattare o

	trasmettere informazioni. [CESID:1997] Information System: Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. [CNSS:2003] Information System: Any procedure or process, with or without IT support, that provides a way of acquiring, storing, processing or disseminating information. Information systems include applications and their supporting infrastructure. [CRAMM:2003]
Stato del rischio	**Relazione: Caratterizzazione degli asset per il loro rischio residuo; cioè quello che può succedere considerando le contromisure dispiegate.**
Tracciabilità	**Assicurazione del fatto che si potrà sempre determinare chi ha fatto cosa e in quale momento l'ha fatto.** Responsabilità: Caratteristica che permette che tutte le azioni realizzate su un sistema di tecnologia informatica siano associate in modo inequivocabile ad un individuo o entità. [CESID:1997] Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity. [13335-1:2004] Accountability: Process of tracing information system activities to a responsible source. [CNSS:2003]
Valore	**Di un asset. È una stima del costo indotto dalla concretizzazione di una minaccia.** Caratteristica che possiedono alcune realtà, considerate beni, per la quale possono essere valutate. [DRAE]
Valore cumulativo	**Considera tanto il valore proprio di un asset quanto il valore degli asset che dipendono da esso.**
Valorizzazione delle contromisure	**Relazione: Valorizzazione dell'efficacia delle contromisure esistenti in rapporto al rischio che mitigano.**
Vulnerabilità	**Stima dell'esposizione effettiva di un asset ad una minaccia. Si determina tramite due misurazioni: frequenza di occorrenza e compromissione causata.** La vulnerabilità di un'asset è la potenzialità o possibilità di occorrenza della concretizzazione di una minaccia su detto asset. [Magerit:1997] Debolezza nella sicurezza di un sistema informativo. [CESID:1997] Vulnerability: A weakness of an asset or group of assets that can be exploited by one or more threats. [17799:2005][13335-1:2004] Vulnerability: The susceptibility of information to exploitation by an adversary. [OPSEC] Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited. [CNSS:2003] Vulnerability: A weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. [CRAMM:2003]

1.2. Termini anglosassoni

Breve dizionario di inglese-italiano di termini abituali nell'analisi e gestione dei rischi:

Accountability	Tracciabilità
ALE	Annual Loss Expectancy
ARO	Annual Rate of Occurrence

Authenticity	Autenticità
Availability	Disponibilità
Asset	Asset
BIA	Business Impact Analysis
Business Impact Analysis	Analisi d'impatto
Confidentiality	Riservatezza
Countermeasure	Contromisura
Frequency	Frequenza
Impact	Impatto
Integrity	Integrità
Residual risk	Rischio residuo
Risk	Rischio
Risk analysis	Analisi dei rischi
Risk assessment	Valutazione dei rischi
Risk management	Gestione dei rischi
Risk map	Mappa dei rischi
Risk treatment	Trattamento dei rischi
Safeguard	Contromisura
Security	Sicurezza
Statement of applicability	Dichiarazione di applicabilità
Traceability	Tracciabilità
Threat	Minaccia
Value	Valore
Vulnerability	Vulnerabilità

1.3. ISO/IEC Guide 73:2002

La guida 73 della ISO [2002] organizza i concetti di gestione dei rischi nel seguente modo:

Risk management:
coordinated activities to direct and control an organization with regard to risk.

Risk assessment:
overall process of risk analysis and risk evaluation.

Risk analysis:
systematic use of information to identify sources and to estimate risk.

Source identification:
process to find, list and characterize sources[2].

Risk estimation:
process used to assign values to the probability[3] and consequences of a risk.

Risk evaluation:
process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

---

2 Source: item or activity having a potential for a consequence.
Consequence: outcome of an event.
Event: occurrence of a particular set of circumstances.

3 Probability: extend to which an event is likely to occur.

Risk treatment:
process of selection and implementation of measures to modify risk.

La seguente tabella riassume il rapporto tra la terminologia identificata nella Guida 73 e in Magerit:

Guide 73:2002	**Magerit v2**	
Risk management	Analisi e gestione dei rischi	P1 + P2 + P3
Risk assessment		
Risk analysis	Analisi dei rischi	P2
Source identification		
Risk estimation		
Risk evaluation		A3.1
Risk treatment	Gestione dei rischi	A3.2 + A3.3

1.4. Riferimenti

[DRAE]
Real Academia Española. Diccionario de la Lengua Española. 22.ª edición, 2001. http://buscon.rae.es/diccionario/drae.htm

[OPSEC]
OPSEC Glossary of Terms, http://www.ioss.gov/docs/definitions.html

[17799:2005]
ISO/IEC 17799:2005, “Information technology -- Code of practice for information security management”, 2005. (N.d.T. ora ISO/IEC 27002:2005)

[15443-1:2005]
ISO/IEC TR 15443:2005, “Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework”, 2005.

[800-53:2004]
NIST, “Recommended Security Controls for Federal Information Systems”, National Institute of Standards and Technology, special publication 800-53, 2004.

[13335-1:2004]
ISO/IEC 13335-1:2004, “Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management”, 2004.

[CRAMM:2003]
“CCTA Risk Analysis and Management Method (CRAMM)”, Version 5.0, 2003.

[Octave:2003]
C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.

[TDIR:2003]
Texas Department of Information Resources, “Practices for Protecting Information Resources Assets“, Revised September 2003.

[CNSS:2003]
Committee on National Security Systems, Instruction No. 4009, “National Information Assurance (IA) Glossary“, May 2003.

[Guide 73:2002]
ISO/IEC Guide 73:2002, “Risk management – Vocabulary – Guidelines for use in Standards”, 2002.

[17799:2002]
UNE ISO/IEC:2002, “Tecnología de la Información – Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”, 2002.

[CIAO:2000]
Critical Infrastructure Assurance Office, “Practices for Securing Critical Information Assets”, January 2000.

[CC:1999]
ISO/IEC 15408:1999, “Information technology — Security techniques — Evaluation criteria for IT security”, 1999.

[NSTISS:1998]
National Security Telecommunications and Information Systems Security Committee, “Index of National Security Telecommunications Information Systems Security Issuances”, NSTISSI no. 4014, NSTISSC Secretariat, 1998.

[CESID:1997]
Centro Superior de Información de la Defensa, “Glosario de Términos de Criptología”, Ministerio de Defensa, 3ª edición, 1997.

[Magerit:1997]
Ministerio de Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997.

[Ribagorda:1997]
A. Ribagorda, “Glosario de Términos de Seguridad de las T.I.”, Ediciones CODA, 1997.

[7498-2:1989]
ISO 7498-2:1989, “Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture”, 1989.

Appendice 2. Riferimenti

Sebbene i capitoli e le appendici includano riferimenti bibliografici specifici all'argomento che trattano, in quest'appendice si riportano i riferimenti a metodi e metodologie che affrontano l'analisi e la gestione dei rischi come attività integrale. I riferimenti sono ordinati temporalmente: dai più recenti ai più datati.

- Federal Office for Information Security (BSI). "IT Baseline Protection Manual", October 2003. Germany.
  http://www.bsi.de/gshb/english/etc/index.htm
- "The Vulnerability Assessment and Mitigation Methodology", P.S. Antón et al., RAND National Defense Research Institute, MR-1601-DARPA, 2003.
- "Managing Information Security Risks: The OCTAVE Approach", C.J. Alberts and A.J. Dorofee, Addison-Wesley Pub Co; 1st edition (July 9, 2002)
  http://www.cert.org/octave/
- "Information Security Risk Analysis", T.R. Peltier, Auerbach Pub; 1st edition (January 23, 2001)
- "Risk Management: Multiservice Tactics, Techniques, and Procedures for Risk Management", Air Land Sea Application Center, FM 3-100.12, MCRP 5-12.1C, NTTP 5-03.5, AFTTP(I) 3-2.30. February 2001.
- Air Force Pamphlet 90-902, "Operational Risk Management (ORM) Guidelines and Tools", December 2000.
- KPMG Peat Marwick LLP, "Vulnerability Assessment Framework 1.1", October 1998.
- Magerit, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", MAP, versión 1.0, 1997
  http://www.csi.map.es/csi/pg5m20.htm
- GMITS, ISO/IEC TR 13335-2:1997, "Information technology - Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security".

Infine si deve citare uno strumento che porta con sé implicitamente una metodologia. Essendo un prodotto, la data si limita ad indicare quella dell'ultima versione sul mercato al momento della pubblicazione del presente libro.

- CRAMM, "CCTA Risk Analysis and Management Method (CRAMM)", Version 5.0, 2003.

Appendice 3. Ambito legale

In quest'appendice si raccoglie la legislazione, nazionale ed internazionale, rilevante al caso dell'analisi e gestione dei rischi, sia per esigerla, sia per rispettarla, sia per essere di utilità in un progetto AGR. La relazione non pretende di essere completamente esauriente, essendo oltretutto riferita ad un processo legislativo in costante divenire, per cui resta un obbligo del responsabile mantenersi informato sulle novità.

La documentazione aggiornata si può trovare nelle pagine web del SSISTAD e del CSAE:

http://www.csi.map.es/

Infine, si sono inclusi alcuni riferimenti ad accordi di carattere politico o di altro natura che è opportuno tenere in considerazione. Ad esempio le guide dell'OCDE (Guide dell'OCDE per la sicurezza dei sistemi informativi e reti. Verso una cultura di sicurezza.)

N.d.T. Non si è ritenuto opportuno includere in questo documento i riferimenti alla legislazione spagnola in merito.

Appendice 4. Ambito di valutazione e certificazione

La complessità dei sistemi informativi comporta un grande sforzo per determinare la qualità delle misure di sicurezza di cui sono stati dotati e la fiducia che meritano. È frequente l'apparizione di terze parti che emettono giudizi indipendenti a proposito di tali aspetti, giudizi che arrivano dopo una valutazione rigorosa e che si concretizzano in un documento formale.

In questo capitolo si ripassano brevemente due ambiti all'interno dei quali è stato formalizzato il processo di valutazione e certificazione:

- nei sistemi di gestione per la sicurezza delle informazioni;
- nei prodotti di sicurezza.

Di ognuno di questi ambiti si indica l'opportunità, il modo di organizzarsi per raggiungere la certificazione e l'ambito amministrativo e normativo in cui si sviluppa l'attività.

4.1. Sistemi di gestione della sicurezza delle informazioni (SGSI)

I problemi di sicurezza dei sistemi informativi hanno un'origine tecnica ma sono tanto complessi che la soluzione non può essere soltanto su quel lato. La tecnologia è troppo ricca di opportunità e pertanto deve essere mantenuta sotto controllo garantendo che operi nella direzione degli obiettivi dell'organizzazione.

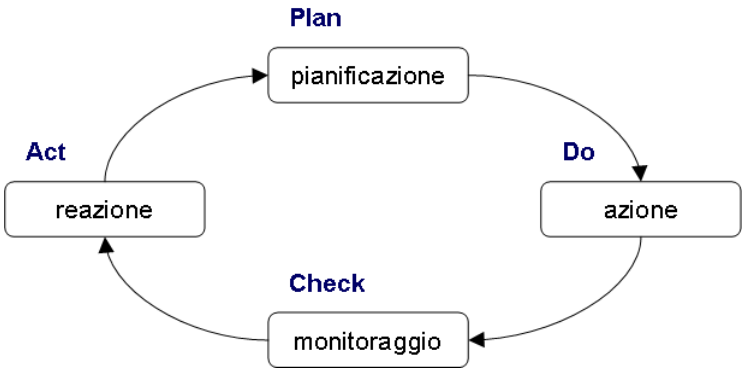
Sicurezza significa essere previdenti (prima); è essere preparati per reagire alle emergenze, previste o impreviste; ed è sapersi riprendere dopo il disastro. Tutto questo non è gratis: costa denaro, tempo e sforzo. Per questo motivo bisogna razionalizzare, con criterio economico, una soluzione equilibrata tra quello che si evita che accada, quello che si mette in piedi per individuare gli errori, e quello che si mantiene pronto per quando accade quello che, teoricamente, non sarebbe dovuto mai accadere. Tutto questo senza dimenticare la dimensione di tempo, perché si devono razionalizzare spese ed investimenti sia per quello che sappiamo oggi sia per quello che scopriremo domani.

Compare quindi una componente di gestione, tanto necessaria quanto le componenti tecniche.

Sistema di gestione per la sicurezza delle informazioni

> È un sistema di gestione che comprende le politiche, la struttura organizzativa, le procedure, i processi e le risorse necessarie per instaurare la gestione della sicurezza delle informazioni. Il sistema è lo strumento di cui la direzione delle organizzazioni dispone per portare a compimento le politiche e gli obiettivi di sicurezza (integrità, riservatezza e disponibilità, assegnazioni di responsabilità, autenticazione, etc.). Esso fornisce meccanismi per la salvaguardia degli asset informativi e dei sistemi che li trattano, in accordo con le politiche di sicurezza e con i piani strategici dell'organizzazione. [UNE 71502:2004]

Questa è l'essenza del modello PDCA (dall'inglese *Plan, Do, Check, Act)* che si usa anche nei modelli di gestione della qualità.



La pianificazione (p di *Plan)* deve includere una politica di sicurezza che definisca gli obiettivi ed un'analisi dei rischi che modellizzi il valore del sistema, la sua esposizione alle minacce e quello di cui si dispone (o che si necessita) per mantenere il rischio sotto controllo. È naturale che con queste basi si generi un piano di sicurezza pensato per la gestione dei rischi.

L'azione (d di *Do)* è l'esecuzione del piano, nei suoi aspetti tecnici e organizzativi, coinvolgendo le persone che si sono fatte carico del sistema o che sono legate ad esso. Un piano ha successo quando conduce ad ottenere un'operatività giornaliera senza sorprese.

Il monitoraggio (c di *Check)* delle operazioni del sistema parte dal fatto che non si può confidare ciecamente nell'efficacia delle contromisure, ma che si deve valutare continuamente se queste rispondano alle attese con l'efficacia desiderata. Si deve misurare sia quello che accade sia quello che accadrebbe se non si fossero realizzate contromisure. A volte si parla del "costo dell'insicurezza" come giustificazione del fatto che la spesa di denaro e la profusione di impegno hanno fondamento. Si deve inoltre prestare attenzione alle novità che si vengono a creare, tanto in merito alle modifiche al sistema informativo, quanto a nuove minacce.

La reazione (a di *Act)* è saper derivare considerazioni dall'esperienza, propria e di sistemi simili, ripetendo e migliorando il ciclo di PDCA.

La valutazione di un sistema di gestione della sicurezza parte dalla supposizione che lo schema precedente struttura le modalità di azione dell'organizzazione in materia di sicurezza e giudica l'efficacia dei controlli instaurati per raggiungere gli obiettivi preposti.

4.1.1. La certificazione

Certificare un sistema di gestione per la sicurezza consiste nel fatto che qualcuno, adeguatamente competente, affermi che un sistema sia sano e impegni in ciò la suo parola (per iscritto). Il tutto completata dalle cautele di conseguimento e di tempo che si considerino opportune e sapendo che quanto si garantisce oggi lo si deve rivedere a medio termine perché tutto evolve.

Per ottenere un certificato si devono seguire una serie di formalismi. Senza entrare in eccessivi dettagli ci si concentrerà su cosa viene valutato dal gruppo che invia l'organismo di certificazione a giudicare l'organizzazione.

La prima cosa che si deve fare è delimitare l'ambito di quello che si va a valutare come "sistema di gestione per la sicurezza delle informazioni". Questa è una delimitazione propria di ogni organizzazione, che riflette la sua missione e la sua struttura interna. È importante delimitare ciò con chiarezza. Se il perimetro è sfumato non rimarrà chiaro che cosa si deve fare nei passi seguenti; in particolare, non si saprà bene a quali persone e dipartimenti dirigersi per raccogliere le informazioni pertinenti; si noti che questo può non essere evidente. Attualmente è raro trovare un'organizzazione chiusa dal punto di vista dei suoi sistemi informativi: l'outsourcing di servizi, l'amministrazione elettronica ed il commercio elettronico hanno diluito le frontiere. D'altronde, l'organigramma interno raramente rispecchia le responsabilità di sicurezza.

Successivamente, ciò che deve essere chiaro, scritto e manutenuto è la politica di sicurezza aziendale. Spesso la politica di sicurezza include riferimenti alla legislazione che rispetta ed è assolutamente necessario delimitare l'ambito legislativo e regolamentare a cui attenersi.

Tutto deve essere scritto, e scritto bene: in modo comprensibile, coerente, opportunamente divulgato e noto agli interessati, oltre che mantenuto aggiornato. Un processo di certificazione ha sempre una forte componente di revisione della documentazione.

Prima che giunga il gruppo di valutazione, si deve avere una fotografia dello stato di rischio dell'organizzazione. Cioè, si deve fare un'analisi dei rischi identificando asset, valorizzandoli, identificandoli e valorizzando le minacce significative. In questo processo si determina quali contromisure e di che qualità le richiede il sistema. Ogni caso è un mondo a parte: né tutti hanno lo stesso asset, né hanno lo stesso valore, né sono ugualmente interconnessi, né tutti sono soggetti alle medesime minacce, né tutti adottano la stessa strategia per proteggersi. E' il caso di avere una strategia, definita dalla politica e il dettaglio della mappa di rischi.

L'analisi dei rischi è uno strumento (irrinunciabile) di gestione. Facendo o smettendo di fare un'analisi dei rischi non si è né più né meno sicuri: semplicemente, si sa o meno a che punto si è.

I risultati dell'analisi dei rischi permettono di elaborare un documento di selezione di controlli, così come una giustificazione della qualità che questi devono avere. Tutto ciò dovrà essere verificato dal gruppo di valutazione che, restando soddisfatto, avallerà il conferimento del certificato.

Il gruppo di valutazione ispeziona il sistema informativo che si desidera certificare confrontandolo con una riferimento riconosciuto che gli permette di oggettivare la valorizzazione con il fine di evitare qualsiasi tipo di arbitrarietà o soggettività e di permettere l'utilizzazione universale delle attestazioni emesse. Si utilizza per questo uno "schema di certificazione" (per esempio, in Spagna, si dispone della norma UNE 71502).

La norma UNE 71502:2004 ha come oggetto la specifica dei "requisiti per stabilire, instaurare, documentare e valutare un sistema di gestione della sicurezza delle informazioni in conformità con la norma UNE ISO/IEC 17799:2002 all'interno del contesto dei rischi identificati per le organizzazioni. Specifica i requisiti dei controlli di sicurezza rispetto ai requisiti delle organizzazioni indipendentemente dal suo tipo, dimensione o area di attività."

La norma UNE 71502:2004 parte da una relazione di controlli basati sulla norma UNE-ISO/IEC 17799:2002, relazione che si deve adattare all'organizzazione soggetta a valutazione, tralasciando gli elementi che non sono pertinenti. Se si considera necessario si possono selezionare controlli addizionali, fuori dall'UNE-ISO/IEC 17799, per ogni organizzazione, adeguati al suo modello particolare di business, così come gli obiettivi che si pretende di raggiungere con gli stessi, giustificando in questo modo la selezione.

La relazione di base è la seguente:

Politica di sicurezza

Revisione e valorizzazione periodica della politica di sicurezza

Controllo e gestione della documentazione

Aspetti organizzativi per la sicurezza

Assegnazione delle responsabilità per la sicurezza delle informazioni

Identificazione dei rischi derivanti dall'accesso di terzi

Contrattualizzazione dei servizi

Contrattualizzazione dell'outsourcing

Contrattualizzazione con imprese collaboratrici

Classificazione e controllo degli asset
- Inventario degli asset
- Classificazione degli asset
- Classificazione delle informazioni
- Revisione e classificazione periodica degli asset
- Revisione periodica dell'analisi dei rischi
- Etichettatura e trattamento delle informazioni

Sicurezza legata al personale
- Contrattualizzazione con il personale
- Formazione
- Comunicazione degli incidenti

Sicurezza fisica e dell'ambito
- Installazione e protezione delle apparecchiature
- Manutenzione delle apparecchiature

Gestione delle comunicazioni e dell'operatività
- Processi operativi
- Controllo dei cambiamenti
- Gestione degli incidenti
- Misure e controlli contro il software dannoso
- Ripristino delle informazioni
- Gestione dei supporti rimovibili
- Eliminazione dei supporti
- Sicurezza della posta elettronica
- Disponibilità dei sistemi pubblici
- Controllo di ingresso, immagazzinamento ed uscita di informazioni
- Analisi e gestione dei log
- Pianificazione della capacità del sistema
- Scambio fisico di informazioni
- Scambio logico di informazioni
- Autorizzazione di uscita di materiale e/o informazioni
- Copie di backup e ripristino

Controllo degli accessi
- Identificazione ed autenticazione degli utenti
- Restrizione dell'accesso alle informazioni
- Controllo degli accessi alla rete
- Controllo degli accessi ai sistemi operativi

Controllo degli accessi logici alle informazioni

Gestione delle password

Gestione remota delle apparecchiature

Sviluppo e manutenzione dei sistemi

Controllo del passaggio dallo sviluppo al test

Controllo del passaggio dal test alla produzione

Controllo dei cambiamenti ai sistemi operativi

Controllo dei cambiamenti nel software

Selezione, controllo ed approvazione di software esterno

Controllo della progettazione delle applicazioni

Specifica dei requisiti di sicurezza

Controllo del software operativo

Gestione della continuità operativa

Gestione della continuità operativa

Manutenzione e valutazione dei piani di continuità operativa

Conformità

Identificazione della legislazione applicabile

Revisione del rispetto della legislazione

Audit interni

4.1.2. L'accreditamento dell'ente certificatore

La credibilità del certificato è legata alla fiducia di cui gode il certificatore. Come si costruisce questa fiducia?

Un componente essenziale è la credibilità dello schema di certificazione. Un secondo componente è la credibilità dell'organizzazione che emette i certificati. Questa organizzazione è responsabile della competenza del gruppo di valutazione e dell'esecuzione del processo di valutazione stesso. Per certificare che queste responsabilità siano assolte si procede al "processo di accreditamento" dove una terza organizzazione valuta il valutatore stesso. In Spagna, l'organizzazione incaricata dell'accreditamento di organismi di valutazione è ENAC, che si attiene alle norme internazionali di mutuo riconoscimento dei certificati emessi da differenti enti in differenti paesi.

N.d.T. In Italia tale ruolo è assolto dal SINCERT.

4.1.3. Terminologia

Si raccolgono di seguito i termini impiegati nelle attività di certificazione dei sistemi informativi, cosi e come si intendono in questo contesto.

Accreditamento

Procedura mediante la quale un organismo autorizzato riconosca formalmente che un'organizzazione è competente per la realizzazione di una determinata attività di valutazione della conformità.

Audit

Vedere "valutazione".

Certificazione

L'obiettivo della certificazione è di "dichiarare pubblicamente che un prodotto, processo o servizio è conforme ai requisiti stabiliti".

Certification: A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST SP 800-37]

Documento di certificazione (o certificato)

Documento che afferma che il sistema di gestione per la sicurezza delle informazioni (SGSI) di un'organizzazione è conforme alla norma di riferimento adattata alla singolarità dell'organizzazione certificata.

Documento di selezione dei controlli

Documento che descrive gli obiettivi di controllo e i controlli rilevanti ed applicabili al sistema di gestione della sicurezza delle informazioni dell'organizzazione. Questo documento deve essere basato sui risultati e sulle conclusioni del processo di analisi e gestione dei rischi.

Schema di certificazione

Ambito tecnico ed amministrativo che stabilisce il riferimento a fronte del quale si verifica il grado di adempimento dell'organizzazione soggetta a valutazione, si emette il certificato e lo si mantiene aggiornato e valido.

Valutazione

Insieme di attività che permette di determinare se l'organizzazione soddisfa i criteri applicabili all'interno dello schema di certificazione. Include attività preparatorie, di revisione della documentazione, di ispezione del sistema informativo e la preparazione della documentazione pertinente per l'emissione del certificato di conformità, se opportuno.

Organismo di certificazione

Entità che, a fronte della relazione di valutazione, certifica per l'organizzazione il raggiungimento dei requisiti stabiliti nello schema di certificazione.

Organismi di valutazione della conformità

Sono incaricati di valutare e realizzare una dichiarazione obiettiva riguardo al fatto che i servizi e i prodotti soddisfino alcuni requisiti specifici, che siano del settore regolamentare o volontario.

Politica di sicurezza

Insieme di norme regolatrici, regole e prassi che determinano il modo in cui gli asset, incluse le informazioni identificate come sensibili, siamo gestiti, protetti e distribuiti all'interno di un'organizzazione.

4.1.4. Riferimenti

- ISO/IEC 17799:2005, *"Information technology - Code of practice for information security management",* 2005.
- UNE 71502:2004, *"Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)",* 2004.
- UNE-ISO/IEC 17799:2002, *"Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información",* 2002.

- ISO Guide 72:2001, *“Guidelines for the justification and development of management system standards”,* 2001.
- European Co-Operation for Accreditation, “Guidelines for the Accreditation of Bodies Operating Certification / Registration of Information Security Management Systems”, *EA-7/03, February 2000.*

4.2. Common Criteria (CC)

Il bisogno di valutare la sicurezza di un sistema informativo appare molto precocemente da parte dei processi di acquisto di apparecchiature del dipartimento della difesa degli Stati Uniti che, nel 1983, pubblica il "libro arancione" (TCSEC-*Trusted Computer System Evaluation Criteria)*. L'obiettivo è specificare senza ambiguità ciò di cui si ha bisogno da parte di chi richiede (e compara) e che si offre da parte del venditore, in modo che non ci siano fraintendimenti ma uno schema trasparente di valutazione, garantendo quindi l'oggettività degli acquisti.

Lo stesso bisogno porta all'apparizione di iniziative europee come ITSEC *(Information Technology Security Evaluation Criteria).* A metà degli anni 90, esiste nel mondo una proliferazione di criteri di valutazione che rende molto difficile il commercio internazionale, arrivando ad un accordo di convergenza che riceve il nome di *"Common Criteria for Information Technology Security Evaluation",* normalmente noti come "Common Criteria" o, in breve, CC.

I CC, oltre al bisogno di un intendimento universale, catturano la natura mutevole delle tecnologie delle informazioni che, nel periodo dal 1980, sono passate da essere concentrate sulle apparecchiature per l’elaborazione, ad includere sistemi informativi molto più complessi.

I CC permettono:

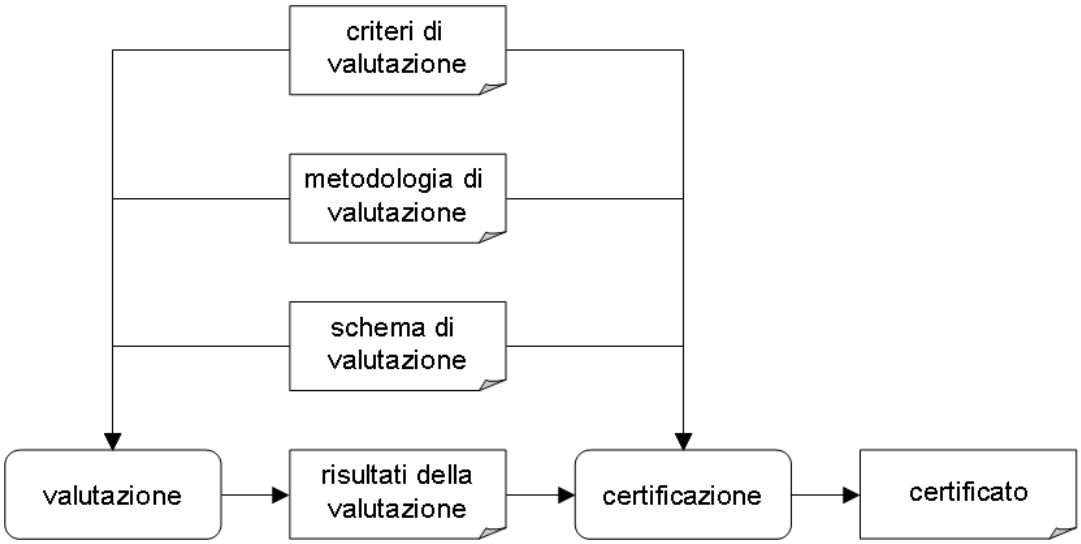
1. di definire le funzioni di sicurezza dei prodotti e dei sistemi (in tecnologie delle informazioni) e
2. di determinare i criteri per valutare la qualità di suddette funzioni.

È essenziale la possibilità che i CC aprono affinché la valutazione sia obiettiva e possa essere realizzata da una terza parte (né dal fornitore, né dall'utente) in modo che la scelta di contromisure adeguate si veda particolarmente semplificata per le organizzazioni che hanno bisogno di mitigare i loro rischi.

L'amministrazione spagnola, e molte altre, riconoscono le certificazioni di sicurezza emesse in altri paesi in base all’ "accordo sul riconoscimento dei certificati di CC nel campo della tecnologia delle informazioni".

La valutazione di un sistema è la base per la sua certificazione. Per certificare bisogna disporre di:

1. alcuni criteri, che definiscono il significato degli elementi che si vanno a valutare;
2. una metodologia, che indichi come portare a termine la valutazione;
3. uno schema di certificazione che fissi l’ambito amministrativo e regolamentare sotto il quale si realizza la certificazione.



In questo modo si può garantire l'oggettività del processo; costruire cioè la fiducia sul fatto che i risultati di un processo di certificazione sono validi universalmente, indipendentemente da dove è realizzata la certificazione.

Dato che la qualità della sicurezza richiesta a un sistema non è sempre la stessa, ma che dipende da per che cosa la si vuole impiegare, i CC stabiliscono una scala di livelli di assicurazione:

EAL0: senza garanzie.

EAL1: provato funzionalmente.

EAL2: provato strutturalmente.

EAL3: provato e verificato metodicamente.

EAL4: progettato, provato e riveduto metodicamente.

EAL5: progettato e provato semi-formalmente.

EAL6: progettato, provato e verificato semi-formalmente.

EAL7: progettato, provato e verificato formalmente.

I livelli superiori richiedono un maggior sforzo di sviluppo e di valutazione, offrendo in ritorno alcune grandi garanzie agli utenti. Per esempio, nell'ambito della firma elettronica, i dispositivi sicuri di firma solgono essere certificati con un profilo di livello EAL4+.

4.2.1. Beneficiari

I CC si dirigono ad un'amplia pletora di potenziali beneficiari della formalizzazione dei concetti e degli elementi di valutazione: i consumatori (utenti dei prodotti di sicurezza), gli sviluppatori e i valutatori. Un linguaggio comune tra tutti loro si traduce in vantaggi apprezzabili:

Per i consumatori

- che possono esprimere i loro requisiti, prima di acquistare i servizi o prodotti che li soddisfino; questo passaggio può risultare utile tanto per acquisti individuali, quanto nell'identificazione di requisiti per gruppi di utenti;
- che possono analizzare le caratteristiche dei servizi o dei prodotti che offre il mercato;
- che possono paragonare differenti offerte;

Per gli sviluppatori

- che sanno quello che verrà richiesto e come si valuteranno i loro prodotti;
- che sanno, obiettivamente, quello che richiedono gli utenti;
- che possono esprimere senza ambiguità quello che fanno i loro prodotti.

Per i valutatori

- che dispongono di un contesto formalizzato per sapere che cosa devono valutare e come devono qualificarlo.

Per tutti

- che dispongono di determinati criteri obiettivi che permettono di accettare le certificazioni realizzate in qualsiasi luogo.

Tutti questi partecipanti confluiscono su un oggetto da valutare denominato **TOE** *(Target Of Evaluation*)**,** che altro non è se non il servizio o il prodotto (di sicurezza) le cui caratteristiche (di sicurezza) si vogliono valutare.

Quando un'analisi dei rischi espone la relazione di contromisure adeguate, queste possono venire espresse usando la terminologia dei CC, il che permette di sfruttare i vantaggi citati, trasformandosi in una specifica formale normalizzata.

4.2.2. Requisiti di sicurezza

Dato un sistema si possono determinare, attraverso un'analisi dei rischi, quali contromisure sono richieste e con che qualità. Quest'analisi può essere effettuata su un sistema generico o su un sistema specifico. Nei CC, l'insieme dei requisiti che si richiedono ad un sistema generico si denomina **profilo di protezione** (**PP** - *Protection Profile)*. Se non si sta parlando di un sistema generico, ma di un sistema specifico, l'insieme di requisiti si definisce come **dichiarazione di sicurezza** (**ST** - *Security Target)*.

I PP, dato il loro carattere generico, coprono differenti prodotti concreti. Solgono essere preparati per gruppi di utenti o organismi internazionali che vogliono dar forma al mercato.

I ST, dato il loro carattere specifico, coprono un solo prodotto concreto. Solgono essere preparati dai propri produttori che in questa maniera danno forma legale alla loro offerta.

I CC determinano i punti su cui deve articolarsi un PP o un ST. L'indice di questi documenti è un buon indicatore del suo scopo:

PP - profilo di protezione	***ST - dichiarazione di sicurezza***
❑ Introduction ❑ TOE description ❑ Security environment • assumptions • threats • organizational security policies ❑ Security objectives • for the TOE • for the environment ❑ Security requirements • for the environment • TOE functional requirements	❑ Introduction ❑ TOE description ❑ Security environment • assumptions • threats • organizational security policies ❑ Security objectives • for the TOE • for the environment ❑ Security requirements • for the environment • TOE functional requirements

• TOE assurance requirements ❑ Application notes ❑ Rationale	• TOE assurance requirements ❑ TOE summary specification ❑ PP claims • PP reference • PP tailoring • PP additions ❑ Rationale

I PP e i ST possono essere a loro volta sottoposti ad una valutazione formale che verifichi la loro completezza ed integrità. I PP così valutati possono passare a registri pubblici per essere condivisi da differenti utenti.

Nell'elaborazione di un ST si fa riferimento ai PP su cui questo si basa.

4.2.3. Creazione di profili di protezione

La generazione di un PP o ST è fondamentalmente un processo di analisi dei rischi dove l'analista ha determinato l'ambito dell'analisi (il TOE nella terminologia dei CC), identifica minacce e determina, attraverso gli indicatori di impatto e rischio, le contromisure necessarie. Nella terminologia dei CC, le contromisure richieste sono denominate **requisiti di sicurezza** e sono suddivise in due grandi gruppi:

requisiti funzionali di sicurezza *(functional requirements)*

- che cosa si deve fare?
- definiscono il comportamento funzionale del TOE

requisiti di garanzia della funzione di sicurezza *(assurance requirements)*

- il TOE è ben costruito?
- è efficace? soddisfa l'obiettivo per ciò che si richiede?
- è efficiente? raggiunge i suoi obiettivi con un impiego ragionevole di risorse?

È importante sottolineare che i CC stabiliscono un linguaggio comune per esprimere gli obiettivi funzionali e di assicurazione. E' quindi necessario che l'analisi dei rischi utilizzi questa terminologia nella selezione delle contromisure. La norma dei CC fornisce nella sua parte 2 il catalogo standardizzato di obiettivi funzionali, mentre nella sua parte 3 fornisce il catalogo standardizzato di obiettivi di assicurazione.

Parte 2: Requisiti funzionali	***Parte 3: Requisiti di garanzia***
FAU: Security audit	ACM: Configuration management
FCO: Communication	ADO: Delivery and operation
FCS: Cryptographic support	ADV: Development
FDP: User data protection	AGD: Guidance documents
FIA: Identification and authentication	ALC: Life cycle support
FMT: Security management	ATE: Tests
FPR: Privacy	AVA: Vulnerability assessment
FPT: Protection of the TOE security functions	APE: PP evaluation
FRU: Resource utilisation	ASE: ST evaluation
FTA: TOE access	
FTP: Trusted path / channels	

4.2.4. Uso di prodotti certificati

Quando un TOE è stato certificato in accordo ad un PP o ad un ST, a seconda di quanto è opportuno in ogni caso, si può avere la certezza che detto TOE soddisfi i requisiti ed inoltre li soddisfi con la qualità richiesta (ad esempio, EAL4).

La certificazione di un sistema o di un prodotto non è una garanzia cieca di idoneità: bisogna accertarsi del fatto che il PP o il ST rispetto a cui è certificato soddisfi i requisiti del sistema. L'analisi dei rischi permette di elaborare il PP o il ST o, talvolta, di selezionare un insieme appropriato ad una mappa dei rischi. Ma l'essenziale è che dall'analisi dei rischi si siano ottenuti alcuni requisiti di sicurezza la cui soddisfazione permetterà di mantenere impatto e rischio residuo sotto controllo.

Nella misura in cui un prodotto certificato si attiene ad un PP o ST che soddisfa i requisiti, la gestione dei rischi si riduce ad acquistare il prodotto, installarlo ed impiegarlo nelle condizioni adeguate.

È importante sottolineare che tanto il PP quanto il ST includono una sezione cosiddetta di "ipotesi" *(assumptions)* in cui si stabiliscono una serie di prerequisiti che l'ambiente operativo in cui si installa il TOE deve soddisfare. Il migliore prodotto, inadeguatamente installato o impiegato, è incapace di garantire la soddisfazione degli obiettivi globali di sicurezza. Per questo i prodotti certificati sono componenti molto solidi di un sistema; ma si deve inoltre garantire loro un adeguato ambiente per assicurare il sistema nella sua completezza.

4.2.5. Terminologia

Visto che il loro obiettivo è quello di servire da riferimento internazionale e sostenere valutazioni e certificazioni, i CC devono essere molto precisi nella terminologia. Nel testo precedente si sono introdotti i termini a seconda della necessità; questi termini si raccolgono formalmente nel seguito:

Assurance (garanzia)

Base della fiducia in cui un'entità raggiunge i suoi obiettivi di sicurezza.

Evaluation (valutazione)

Valutazione di un PP, ST o TOE a fronte di criteri definiti.

Evaluation Assurance Level (EAL) (livello di garanzia di valutazione)

Pacchetto che consiste in componenti di garanzia della parte 3 e che rappresenta un livello nella scala di garanzia predefinita di CC.

Evaluation authority (autorità di valutazione)

Organismo che implementa i CC per un'area specifica mediante uno schema di valutazione attraverso il quale si stabiliscono le norme e si soprintende alla qualità delle valutazioni realizzate da organismi di tale area.

Evaluation scheme (schema di valutazione)

Ambito amministrativo e regolamentare attraverso il quale un'autorità di valutazione applica i CC in un'area specifica.

Formale

Espresso in un linguaggio dalla sintassi ristretta con una semantica definita basata su concetti matematici bene stabiliti.

Informale

Espresso in linguaggio naturale.

Organisational security policies (politiche di sicurezza organizzativa)

Una o più regole di sicurezza, procedure, prassi o norme di imposte da un'organizzazione sulle sue operazioni.

Product (prodotto)

Pacchetto *software*, *firmware* e/o *hardware* IT che fornisce una funzionalità, progettato per il suo impiego o per la sua incorporazione in una grande varietà di sistemi.

Protection Profile (PP) (profilo di protezione)

Insieme di requisiti di sicurezza, indipendente dell'implementazione, per una categoria di TOEs che soddisfano alcuni requisiti specifici del consumatore.

Security objective (obiettivo di sicurezza)

Dichiarazione dell'intenzione di contrastare le minacce identificate e/o di rispettare le politiche e ipotesi di sicurezza identificate dall'organizzazione.

Security Target (ST) (dichiarazione di sicurezza)

Insieme di requisiti di sicurezza e specifiche utilizzati come base della valorizzazione di un TOE identificato.

Semiformal

Espresso in un linguaggio dalla sintassi ristretta con una semantica definita.

System (sistema)

Installazione specifica IT con un proposito ed in un ambiente particolare.

Target of Evaluation (TOE) (oggetto da valutare)

Prodotto o sistema IT, unito ai suoi manuali dell'amministratore e dell'utente, che si sottopone a valutazione.

TOE Security Functions (TSF) (funzioni di sicurezza del TOE)

Insieme composto da tutto l'*hardware*, il *firmware* e il *software* del TOE sul quale si deve fare riferimento per la corretta applicazione del TSP.

TOE Security Policy (TSP) (politica di sicurezza del TOE)

Insieme di regole che regolano come si gestiscono, proteggono e distribuiscono gli asset nel TOE.

4.2.6. Riferimenti

- "Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de las Tecnologías de la Información", Mayo, 2000.
- CC, "Common Criteria for Information Technology Security Evaluation", Version 2.3, 2005.
  - Part 1: Introduction and general model
  - Part 2: Security functional requirements
  - Part 3: Security assurance requirements

  Anche pubblicati come norma ISO/IEC 15408:2005, parti 1, 2 e 3.
- ITSEC, European Commission, "Information Technology Security Evaluation Criteria", version 1.2, 1991.
- TCSEC, Department of Defence, "Trusted Computer System Evaluation Criteria", DOD 5200.28-STD, Dec. 1985.

Appendice 5. Strumenti

La realizzazione di un progetto di AGR comporta il dover lavorare con una quantità di asset che raramente è nell'ordine delle decine e più normalmente è in quello delle centinaia. Il numero di minacce tipicamente si colloca nell'ordine delle decine, mentre il numero di contromisure sta nelle migliaia. Tutto ciò ci indica che si deve trattare una moltitudine di dati e di combinazioni tra loro, il che porta logicamente a cercare appoggio in strumenti automatici.

Come requisiti generali, uno strumento di appoggio ai progetti di AGR deve:

- permettere di lavorare con un insieme ampio di asset, minacce e contromisure;
- permettere un trattamento flessibile dell'insieme di asset per raggiungere un modello vicino alla realtà dell'organizzazione;
- essere utilizzato durante i tre processi che costituiscono il progetto, specialmente come supporto al processo P2, analisi dei rischi e
- non nascondere all'analista il ragionamento che porta alle conclusioni.

Gli strumenti possono effettuare un trattamento qualitativo o quantitativo delle informazioni. La scelta tra l'una e l'altra impostazione è motivo di lunghi dibattiti. I modelli qualitativi offrono risultati utili prima dei modelli quantitativi, semplicemente perché la raccolta di dati qualitativi è più facile che quella di dati quantitativi. I modelli qualitativi sono efficaci relativizzando ciò che è più importante rispetto a quello che non è molto importante; ma raggruppano le conclusioni in grandi insiemi. I modelli quantitativi, al contrario, consentono un'ubicazione precisa di ogni aspetto.

Impatti e rischi residui possono essere qualitativi finché non si devono effettuare grandi investimenti e si deve determinare la loro razionalità su base economica: cos'è ciò che interessa di più? A questo punto si ha bisogno dei numeri.

Un'opzione mista fa comodo: un modello qualitativo per il sistema informativo completo, con capacità di entrare in un modello quantitativo per quelle componenti la cui protezione va a richiedere forti investimenti.

E' certo che il modello dei valori di un'organizzazione deve potersi impiegare per un tempo relativamente lungo, almeno per gli anni che dura il piano di sicurezza, per analizzare l'effetto dell'esecuzione dei programmi. È decisamente più difficoltoso generare un modello dei valori da zero che va adattando un modello esistente all'evoluzione degli asset del sistema e all'evoluzione dei servizi che fornisce l'organizzazione. In questa evoluzione continua si può affrontare la progressiva migrazione di un modello qualitativo iniziale verso un modello ogni volta più quantitativo.

E' da sottolineare che i dati di caratterizzazione delle possibili minacce saranno dei tentativi di approssimazione nei primi modelli; ma l'esperienza permetterà di andare avvicinando le valutazioni alla realtà.

Che siano strumenti qualitativi o quantitativi, devono:

- Trattare un catalogo ragionevolmente completo di tipi di asset. Su questa linea si orienta il capitolo 2 del "catalogo degli elementi".
- Trattare un catalogo ragionevolmente completo di dimensioni di valorizzazione. Su questa linea si orienta il capitolo 3 del "catalogo degli elementi".
- Aiutare a valorizzare gli asset offrendo dei criteri di valorizzazione. Su questa linea si orienta il capitolo 4 del "catalogo degli elementi".
- Trattare un catalogo ragionevolmente completo di minacce. Su questa linea si

incammina il capitolo 5 del "catalogo degli elementi".

- Trattare un catalogo ragionevolmente completo di contromisure. Su questa linea si orienta il capitolo 6 del "catalogo degli elementi".
- Valutare l'impatto ed il rischio residui.

È interessante che gli strumenti possano importare ed esportare i dati che trattano in formati facilmente processabili da altri strumenti, per esempio:

- XML - Extended Markup Language

che è l'opzione considerata in questa guida, la quale stabilisce formati XML di scambio.

- CSV - Comma Separated Values

5.1. PILAR

PILAR, acronimo di "Procedura Informatico Logica per l'Analisi dei Rischi" è uno strumento sviluppato dietro specifica del centro nazionale di intelligence per supportare l'analisi dei rischi di sistemi informativi seguendo la metodologia Magerit.

Lo strumento supporta tutte le fasi della metodologia Magerit:

- Caratterizzazione degli asset: identificazione, classificazione, dipendenze e valorizzazione.
- Caratterizzazione delle minacce.
- Valorizzazione delle contromisure.

Lo strumento incorpora i cataloghi del "catalogo degli elementi" permettendo un'omogeneità nei risultati dell'analisi:

- tipi di asset;
- dimensioni di valorizzazione;
- criteri di valorizzazione;
- catalogo delle minacce.

Per incorporare questo catalogo, PILAR differenzia tra il motore di calcolo dei rischi e la biblioteca degli elementi, che può essere sostituita per mantenere il passo con l'evoluzione nel tempo dei cataloghi di elementi.

Lo strumento valuta l'impatto ed il rischio, cumulativo e riflesso, potenziale e residuo, presentandoli in modo da permettere l'analisi del perché si assegna un certo impatto o un certo rischio.

Le contromisure sono valorizzate per fasi, permettendo l'incorporazione in uno stesso modello di differenti situazioni temporali. Tipicamente si può includere il risultato dei differenti programmi di sicurezza durante l'esecuzione del piano di sicurezza, monitorando il miglioramento del sistema.

I risultati sono presentati in vari formati: relazioni RTF, grafici e tabelle facilmente esportabili e fogli di calcolo. In questo modo è possibile elaborare differenti tipi di relazioni e presentazioni dei risultati.

Infine, lo strumento calcola le qualificazioni di sicurezza seguendo i punti di norme *de iure* o *de facto* di uso comune. Tra queste:

- Criteri di sicurezza, normalizzazione e conservazione.
- UNE-ISO/IEC 17799:2002: sistemi di gestione della sicurezza.
- RD 994/1999: dati di carattere personale.

Infine si deve sottolineare che PILAR include tanto i modelli qualitativi quanto quelli quantitativi, potendo alternare l'uno con l'altro per ottenere il massimo beneficio dalle possibilità teoriche di ognuno di essi.

5.2. Riferimenti

CARVER

"Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability", National Infrastructure Institute's Center for Infrastructure Expertise, USA.

COBRA

"Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance", C&A Systems Security Ltd, UK.

CRAMM

"CCTA Risk Analysis and Management Method". Insight Consulting. UK.

The CRAMM Risk Analysis and Management Method is owned, administered and maintained by the Security Service on behalf of the UK Government.

EBIOS

"Méthode pour l'Expression des Besoins et l'Identification des Objectifs de Sécurité". Service Central de la Sécurité des Systèmes d'Information. France.

RIS2K

Supporto a Magerit v1.0. Ministero della Pubblica Amministrazione. España.

PILAR

"Procedimiento Informático-Lógico para el Análisis de Riesgos". Centro Nazionale di Intelligence. Ministero della Difesa. Spagna.

Appendice 6. Evoluzione rispetto a Magerit versione 1.0

La versione 1.0 di Magerit, pubblicata nel 1997, ha resistito nella sua maggior parte al passare del tempo, modificandosi nelle parti fondamentali. Ciò nonostante, il tempo passato permette di migliorare particolarmente quella prima versione. Questa seconda versione non parte con volontà di rottura, ma si imposta con intenzioni di miglioramento, aggiornando la metodologia al presente ed aggiungendo l'esperienza di questi anni.

Le seguenti sezioni serviranno come guida nella versione 2 ai professionisti che hanno già familiarità con la versione 1.

N.d.T. Non si è ritenuto opportuno includere in questo documento la traduzione di questa appendice in quanto la versione 2.0 è la prima ad essere tradotta in italiano.

Appendice 7. Caso pratico

A titolo di esempio, quest'appendice analizza il caso di un'unità amministrativa che utilizza sistemi informativi propri e di terzi per i suoi compiti interni e per prestare servizi di attenzione ai cittadini (amministrazione elettronica).

L'esempio pretende solo di essere illustrativo, senza che il lettore debba derivarne conseguenze o conclusioni di natura vincolante. Anche davanti agli stessi impatti e rischi, le soluzioni possono essere differenti, senza poter essere estrapolate ciecamente dall'una all'altra circostanza. In particolare si sottolinea il ruolo della direzione dell'organizzazione come ultimo punto di decisione rispetto a quale politica adottare per mantenere impatti e rischi sotto controllo.

Buona parte del testo che segue presenta la situazione in parole "normali", cosi come può giungere nella realtà al gruppo di lavoro a seguito delle interviste. È la missione di questo gruppo tradurre la conoscenza acquistata nei termini formali definiti per questa metodologia.

7.1. La storia

L'unità oggetto di studio non è di nuova di creazione, ma è da anni che inoltra incartamenti in modo locale, dapprima a mano e adesso per mezzo di un sistema informatico proprio. A questo sistema informatico si è aggiunta recentemente una connessione ad un archivio centrale che funziona come "memoria storica": permette di recuperare dati e conservare gli incartamenti chiusi. L'ultima novità consiste nell'offrire un servizio proprio di amministrazione elettronica, all'interno del quale gli utenti possono realizzare le loro transazioni via web, usando il numero della loro CI per l'identificazione, più una password personale. Lo stesso sistema di trasmissione è usato localmente da un funzionario che presta assistenza ai cittadini che si presentano nei locali dell'unità.

Il responsabile del progetto di amministrazione elettronica, allarmato dalle notizie apparse sui mass media sull'insicurezza di Internet, e sapendo che un errore nel servizio comporterebbe un serio danno all'immagine della sua unità, assume il ruolo di promotore. In questo ruolo scrive una relazione interna, diretta al direttore dell'unità, in cui si tiene conto di:

- i mezzi informatici con cui si sta lavorando e quelli che si andranno ad installare;
- gli incidenti accaduti da quando l'unità esiste;
- le incertezze che causa l'uso di Internet per la prestazione del servizio.

In base a detta relazione sostiene la necessità di lanciare un progetto di AGR.

La direzione, convinta del bisogno di prendere contromisure prima che accada una disgrazia, crea un comitato di attenzione formato dal responsabile dei servizi interessati: assistenza agli utenti, consulenza giuridica, servizi informatici e sicurezza fisica.

Si determina che l'ambito del progetto (attività A1.2) sarà il servizio di trasmissione elettronica, locale e remota. Si studierà anche la sicurezza delle informazioni che si impiegano: gli incartamenti. Rispetto alle attrezzature, si analizzeranno apparecchiature e reti di comunicazioni. Si prende la decisione di lasciare fuori dello studio gli elementi che potrebbero essere rilevanti in un'analisi più dettagliata come i dati di identificazione ed autenticazione degli utenti dei sistemi, le aree di lavoro del personale che li impiega, la sala macchine (centro di elaborazione di dati) e le persone collegate al processo. E' previsto lanciare un futuro progetto di AGR più dettagliato che approfondisca detti aspetti.

Si escluderà esplicitamente la valorizzazione della sicurezza dei servizi sussidiari impiegati. L'analisi è locale, circoscritta all'unità che ci compete. Detti servizi remoti si considerano, agli effetti di questa analisi, "opachi"; non verrà analizzato come sono prestati.

Il lancio del progetto (attività A1.4) include una riunione della direzione con il comitato di attenzione in

cui si espongono i punti principali dell'analisi preliminare realizzata dal promotore che rimane incaricato come direttore del progetto di AGR, nel quale parteciperanno due persone del suo staff congiuntamente ad un consulente esterno. Uno dei membri dello staff interno avrà un profilo tecnico: ingegnere di sistemi. Al consulente esterno si richiede di identificare nominalmente le persone che parteciperanno e di firmare un accordo di riservatezza.

Il progetto si annuncia internamente mediante comunicazione generale a tutto il personale dell'unità e notifica personale alle persone che si vedranno direttamente coinvolte. In queste comunicazioni si identificano le persone responsabili del progetto.

7.2. Processo P2: Analisi dei rischi

La fase di analisi dei rischi si mette in moto con una serie di interviste ai responsabili designati dal comitato di attenzione, interviste in cui partecipano:

- la persona di collegamento, per introdurre le parti;
- il personale del consulente esterno come direttore dell'intervista;
- il personale interno nel ruolo di verbalizzante: relazione della riunione e raccolta di dati.

Servizio di trasmissione

Il servizio di trasmissione si presta attraverso un'applicazione informatica sviluppata in passato su alcune base di dati. A questa applicazione si accede attraverso un'identificazione locale dell'utente che controlla i suoi privilegi di accesso. Nell'ambito di una trasmissione locale, è la persona che sta prestando attenzione all'utente finale quella che si autentica al sistema. Nel caso di una trasmissione remota, è l'amministrazione che si identifica.

Tutte la trasmissioni includono una fase di richiesta (ed inserimento di dati) ed una fase di risposta (e consegna di dati). L'utente realizza la sua richiesta ed aspetta una notifica per ricevere la risposta. La notifica è per posta, raccomandata nel caso di trasmissione locale, ed elettronica nel caso di trasmissione remota.

Iniziare una trasmissione presuppone l'apertura di un incartamento che si immagazzina localmente nell'ufficio, oltre all'ottenimento di una serie di dati dall'archivio centrale di informazioni, dati che si copiano localmente. Alla chiusura dell'incartamento, i dati ed una relazione delle azioni intraprese sono spedite all'archivio centrale per la custodia, eliminando le informazioni dalle apparecchiature locali.

Il personale dell'unità si identifica attraverso il suo account, mentre gli utenti remoti si identificano con il loro numero di CI. In entrambi i casi il sistema richiede una password per autenticarli.

Infine, si deve sottolineare il ruolo che la messaggistica elettronica ricopre in tutto il processo di trasmissione, usata tanto come mezzo interno di comunicazione tra il personale, quanto come meccanismo di notifica agli utenti esterni. Di norma, non si deve impiegare la posta per il trasporto di documenti; questi saranno sempre serviti mediante accessi web.

Servizio di archivio centrale

Attraverso una intranet si presta un servizio centralizzato di archiviazione e ripristino di documenti. Gli utenti accedono attraverso un'interfaccia web locale, che si connette attraverso una rete privata virtuale con il server remoto, identificandosi con il suo numero di CI. Questo servizio è a disposizione solo del personale dell'unità e dell'impiegato virtuale che presta il servizio di trasmissione remota.

Apparecchiature informatiche

L'unità dispone di varie apparecchiature personali di tipo PC situate all'interno dei locali. Queste

macchine dispongono di un web browser, di un client di posta elettronica senza memorizzazione locale dei messaggi ed un pacchetto di applicazione di ufficio standard (editor di testi e fogli di calcolo).

Esiste una capacità di memorizzazione locale di informazioni sul disco del PC, del quale non sono realizzate copie di sicurezza; in più, esiste una procedura di installazione/aggiornamento che cancella il disco locale e reinstalla il sistema ex novo.

Le macchine non dispongono di unità disco rimovibili di nessun tipo: dischetti, cd,dvd, USB, etc.

Si dispone di un server mid-range, di impiego generico, dedicato ai compiti di:

- file server;
- server di messaggistica elettronica, con memorizzazione locale ed accesso via web;
- server di base di dati: incartamenti in corso ed identificazione di utenti;
- server web per la trasmissione remota e per l'intranet locale.

Comunicazioni

Si dispone di una rete locale che copre i locali di lavoro e la sala macchine. E' esplicitamente proibita l'installazione di modem di accesso remoto e di reti senza fili, ed è attiva una procedura regolare d'ispezione in materia.

Esiste una connessione ad Internet ADSL con un operatore commerciale. Su questo collegamento si prestano molteplici servizi:

- servizio (proprio) di trasmissione remota;
- servizio di posta elettronica (come parte del servizio di trasmissione remota);
- servizio (proprio) di accesso alle informazioni;
- rete privata virtuale con l'archivio centrale.

La connessione ad Internet si realizza unicamente ed esclusivamente attraverso un firewall che limita le comunicazioni a livello di rete, permettendo soltanto:

- lo scambio di posta elettronica con il server di posta;
- lo scambio di traffico web con il server web.

La rete privata virtuale con l'archivio centrale utilizza un'applicazione *software*. La rete si stabilisce all'inizio della giornata, chiudendosi automaticamente all'ora di chiusura. Durante la connessione i terminali si riconoscono reciprocamente e stabiliscono una chiave di sessione per la giornata. Non c'è intervento di nessuno operatore locale.

C'è la percezione che molti servizi dipendano dalla connessione ad Internet. Inoltre nel passato ci sono stati incidenti tali come caduta del servizio dovuta a lavori municipali o ad una carente prestazione del servizio per parte del fornitore. Per tutto ciò:

1. si è definito un contratto di servizio che stabilisce un certo livello di qualità, al di sotto del quale l'operatore deve accreditare alcuni indennizzi concordati anticipatamente in proporzione al periodo di interruzione o alla lentezza (insufficiente volume di dati trasmessi in periodi determinati di tempo) del collegamento.
2. si è contrattualizzato con un'altro fornitore un collegamento digitale (RDSI o ISDN) di backup, collegamento che abitualmente non è attivo, ma che si attiva automaticamente quando il l'ADSL si interrompe per più di 10 minuti

Durante l'intervista si è scoperto che questi collegamenti sono prestati sullo stesso segmento di rete

telefonica che supporta i servizi di voce dell'unità.

Sicurezza fisica

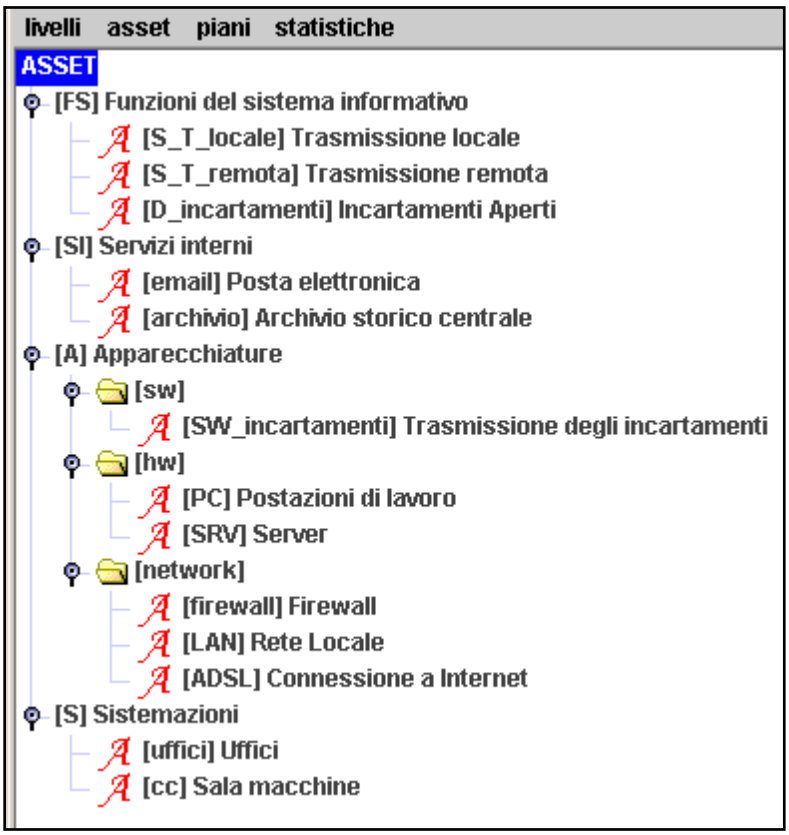
Il personale lavora nei locali dell'unità, principalmente in zone interne, salvo una serie di terminali nei punti di assistenza al pubblico. L'accesso alle zone interne è limitato alle ore di ufficio, restando chiuso a chiave al di fuori di detto orario. In orario di ufficio c'è un controllo di accesso che identifica gli impiegati e memorizza la loro ora di entrata e di uscita.

La sala macchine è semplicemente una stanza interna che rimane chiusa a chiave, la quale è custodita dall'amministratore dei sistemi. La sala dispone di un sistema di rilevamento ed estinzione di incendi che si revisiona annualmente. Questa sala dista 50 metri della canalizzazione di acqua più vicina.

I locali dell'unità occupano interamente il 4° piano di un edificio di uffici di 12 piani. I controlli di accesso sono propri dell'unità, non dell'edificio, che è di uso condiviso con altre attività. Non c'è nessun controllo su ciò che si trova nei locali al piano di sopra o di sotto.

7.2.1. Compito T2.1.1. Identificazione degli asset

A seguito delle precedenti interviste si decide di lavorare con il seguente insieme di asset:



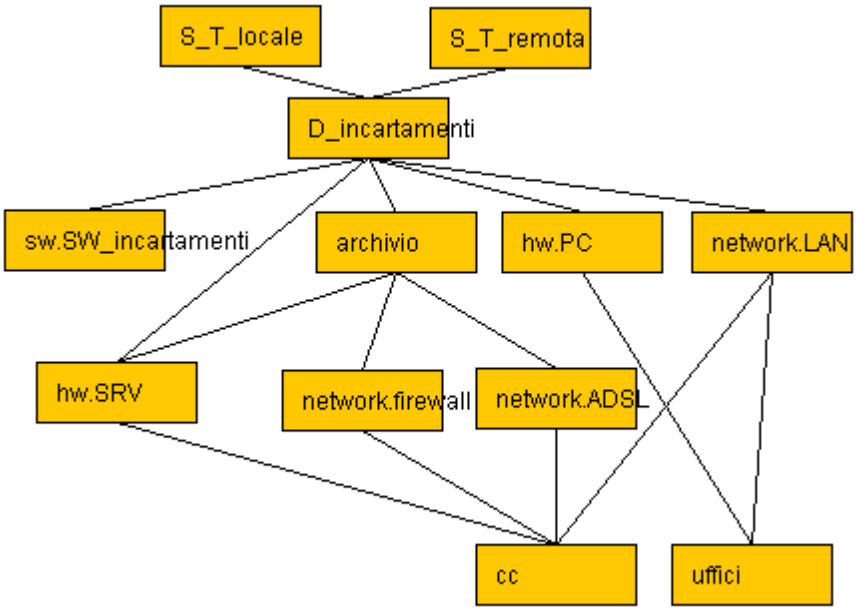
Il sistema descritto è, evidentemente, più complesso; ma il numero di asset significativi è stato ridotto drasticamente affinché l'esempio sia realmente semplice, centrato nella casistica tipica che si desidera illustrare.

7.2.2. Compito T2.1.2: Dipendenze

Tenendo in considerazione le dipendenze per operare (disponibilità) e di immagazzinamento di dati (integrità e riservatezza), si è determinata la seguente matrice di dipendenze tra asset:

	S_T_locale	S_T_remota	D_incartamenti	email	archivio	SW_exp	PC	SRV	firewall	LAN	ADSL
S_T_locale			√	√	√	√	√	√		√	
S_T_remota			√	√	√	√		√	√	√	√
D_ incartamenti					√	√	√	√		√	
email								√	√	√	√
archivio								√	√		√
SW_incartamenti											
PC											
SRV											
firewall											
LAN											
ADSL											

Queste tavole si possono rappresentare graficamente, facendo attenzione che non ci sia una saturazione di dipendenze; cioè, raramente si può rappresentare tutto il sistema in un solo grafo. Per il caso dei dati di incartamenti aperti, il grafo delle dipendenze è così:



7.2.3. Compito T2.1.3: Valorizzazione

La direzione è preoccupata per il potenziale abuso dei processi di trasmissione, alcuni dei quali possono includere l'accredito di quantità economiche importanti, sia a beneficio dell'organizzazione, sia a beneficio degli utenti. L'esistenza di un movente economico può incitare all'abuso tanto il personale interno quanto gli utenti remoti, poiché esiste una particolare difficoltà relazionata con l'impunibilità di attaccanti che possono perpetrare attacchi da qualsiasi punto del pianeta in remoto.

C'è una particolare sensibilità relativa alla disponibilità dei servizi: in particolare c'è preoccupazione che non si possa prestare assistenza ad una richiesta effettuata allo sportello.

I servizi web ad utenti esterni, si considerano "emblematici" e si vogliono fornire con precisione per dare un'immagine di modernità, efficacia e vocazione al servizio. Tutto quello che possa dare una brutta immagine, sia perché non è disponibile il servizio, sia perché si presta in modo erroneo, sia perché non si presta attenzione agli incidenti con sollecitudine,..., tutte queste situazioni si vogliono evitare quanto più possibile.

Le basi di dati di locali ospitano dati personali classificati ad un livello medio di riservatezza all'interno dello schema di classificazione per tali dati.

In vista di tutto ciò, si è raggiunta la seguente valorizzazione degli asset del sistema. Si sono soltanto valutati direttamente gli asset superiori dell'albero delle dipendenze, nella seguente maniera:

	dimensioni di sicurezza						
asset	D	I	R	A_S	A_D	T_S	T_D
[S_T_locale] Trasmissione locale	5(1)			7(2)		6(3)	
[S_T_remota] Trasmissione remota	3(4)			7(5)		6(6)	
[D_incartamenti] Incartamenti aperti		5(7)	6(8)		5(9)		5(10)

Concretamente, i livelli sono stati assegnati per le seguenti ragioni (richiamate nella tavola precedente):

(1) 5.da Può causare interruzioni delle attività proprie dell'Organizzazione con qualche ripercussione anche in altre organizzazioni
(2) 7.da Può causare interruzioni gravi delle attività proprie dell'Organizzazione con ripercussioni consistenti anche in altre organizzazioni
5.lro Requisiti legali e normativi: può causare la violazione di obblighi legali o normativi
(3) 6.pi2 Dati personali: può causare una violazione significativa dei requisiti legali per i dati personali
(4) 3.da Può causare interruzioni di attività interne all'Organizzazione
(5) 7.da Può causare interruzioni gravi delle attività proprie dell'Organizzazione con ripercussioni consistenti anche in altre organizzazioni
6.pi1 Dati personali: può interessare seriamente un gruppo di individui
5.lro Requisiti legali e normativi: può causare la violazione di obblighi legali o normativi
(6) 6.pi2 Dati personali: può causare una violazione significativa dei requisiti legali per i dati personali
(7) 5.da Può causare interruzioni delle attività proprie dell'Organizzazione con qualche ripercussione anche in altre organizzazioni
(8) 6.pi2 Dati personali: può causare una violazione significativa dei requisiti legali per i dati personali
(9) 5.lro Requisiti legali e normativi: può causare la violazione di obblighi legali o normativi
(10) 5.lro Requisiti legali e normativi: può causare la violazione di obblighi legali o normativi

Quando questa valorizzazione si propaga attraverso l'albero delle dipendenze, risulta la seguente

tavola di valori cumulativi in ognuno degli asset del sistema (si mostra su fondo bianco quello che è valore proprio, e su fondo colorato quello che è cumulativo):

	dimensioni di sicurezza						
asset	D	I	R	A_S	A_D	T_S	T_D
[S_T_locale] Trasmissione locale	5			7		6	
[S_T_remota] Trasmissione remota	3			7		6	
[D_incartamenti] Incartamenti aperti	5	5	6	7	5	6	5
[email] Posta elettronica	5			7		6	
[archivio] Archivo storico centrale	5	5	6	7	5	6	5
[SW_ trasmissione] Trasmissione degli incartamenti	5	5	6	7	5	6	5
[PC] Postazioni di lavoro	5	5	6	7	5	6	5
[SRV] Server	5	5	6	7	5	6	5
[firewall] Firewall	5	5	6	7	5	6	5
[LAN] Rete locale	5	5	6	7	5	6	5
[ADSL] Connessione ad Internet	5	5	6	7	5	6	5

A questo punto si ottiene il "Modello dei valori" dell'organizzazione.

7.2.4. Attività A2.2: Caratterizzazione delle minacce

Essendo difficile, per non dire impossibile, caratterizzare quello che può accadere gli all'asset se non ci fossero contromisure dispiegate, si ricorre ad una qualificazione standard delle minacce tipiche sull'asset tenendo in considerazione la sua natura ed il suo valore.

Con tutte queste considerazioni, ed a titolo illustrativo, la seguente tavola mostra le minacce che si sono considerate tipiche per il caso degli incartamenti amministrativi.

		dimensioni di sicurezza						
asset/minaccia	frequenza	D	LE	C	A_S	A_D	T_S	T_D
[D_incartamenti] Incartamenti aperti		50%	50%	100%	100%	100%	100%	100%
E.1 Errore lato utente	10	10%	10%					
E.2 Errore lato amministratore	1	20%	20%	10%	10%	10%	20%	20%
E.3 Errore di monitoraggio	1						50%	50%
E.4 Errore di configurazione	0,5	50%	10%	10%	50%	50%	50%	50%
E.14 Fuga di informazioni	1			1%				
E.15 Alterazione delle informazioni	10		1%					
E.16 Inserimento di false informazioni	100		1%					
E.17 Corruzione delle informazioni	10		1%					
E.18 Distruzione delle informazioni	10	1%						
E.19 Diffusione delle informazioni	1			10%				
A.4 Manipolazione della configurazione	0,1	50%	10%	50%	100%	100%	100%	100%
A.11 Accesso non autorizzato	100		10%	50%	50%			
A.14 Intercettazione delle informazioni	10			50%				
A.15 Alterazione delle informazioni	10		50%					
A.16 Inserimento di false informazioni	20		50%					
A.17 Corruzione delle informazioni	10		50%					
A.18 Distruzione delle informazioni	10	50%						
A.19 Diffusione delle informazioni	10			100%				

Si noti che c'è una differenza tra la percezione dell'utente e le minacce potenziali nel sistema. Questa differenza si deve all'esistenza di contromisure, che sono tenute in considerazione più avanti.

A questo punto si ottiene la "Mappa dei rischi " dell'organizzazione.

7.2.5. Attività A2.4: Stima di impatto e rischio

Senza ancora considerare le contromisure, si derivano le seguenti stime di impatto e rischio cumulativo sui differenti asset. Le tavole seguenti raccolgono per ogni asset (riga) la stima di impatto e di rischio in ogni dimensione di sicurezza (colonna).

Impatto cumulativo

asset	[D]	[I]	[R]	[A_S]	[A_D]	[T_S]	[T_D]
ASSET							
[FS] Funzioni del sistema informativo							
[S_T_locale] Trasmissione locale	[5]			[7]		[6]	
[S_T_remota] Trasmissione remota	[3]			[7]		[6]	
[D_incartamenti] Incartamenti aperti	[5]	[4]	[6]	[7]	[5]	[6]	[5]
[SI] Servizi interni							
[email] Posta elettronica	[5]			[7]		[6]	
[archivio] Archivio storico centrale	[5]	[4]	[5]	[7]	[5]	[6]	[5]
[A] Apparecchiature							
[sw]							
[SW_incartamenti] Trasmissione degli inca	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[hw]							
[PC] Postazioni di lavoro	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SRV] Server	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[network]							
[firewall] Firewall	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[LAN] Rete Locale	[5]	[2]	[6]	[7]	[5]	[6]	[5]
[ADSL] Connessione a Internet	[5]	[2]	[5]	[7]	[5]	[6]	[5]
[S] Sistemazioni							
[uffici] Uffici	[5]	[4]	[5]	[6]	[4]	[5]	[4]
[cc] Sala macchine	[5]	[4]	[5]	[6]	[4]	[5]	[4]

Rischio cumulativo

asset	[D]	[I]	[R]	[A_S]	[A_D]	[T_S]	[T_D]
ASSET							
[FS] Funzioni del sistema informativo							
[S_T_locale] Trasmissione locale	{4}			{5}		{5}	
[S_T_remota] Trasmissione remota	{3}			{5}		{5}	
[D_incartamenti] Incartamenti aperti	{5}	{4}	{5}	{5}	{3}	{3}	{3}
[SI] Servizi interni							
[email] Posta elettronica	{4}			{5}		{5}	
[archivio] Archivio storico centrale	{5}	{5}	{5}	{5}	{5}	{5}	{4}
[A] Apparecchiature							
[sw]							
[SW_incartamenti] Trasmissione degli i	{5}	{5}	{5}	{5}	{5}	{5}	{5}
[hw]							
[PC] Postazioni di lavoro	{5}	{5}	{5}	{5}	{5}	{5}	{5}
[SRV] Server	{5}	{5}	{5}	{5}	{5}	{5}	{5}
[network]							
[firewall] Firewall	{4}	{2}	{4}	{5}	{2}	{4}	{3}
[LAN] Rete Locale	{4}	{3}	{5}	{5}	{4}	{4}	{3}
[ADSL] Connessione a Internet	{4}	{3}	{4}	{5}	{4}	{4}	{3}
[S] Sistemazioni							
[uffici] Uffici	{5}	{5}	{5}	{5}	{5}	{5}	{5}
[cc] Sala macchine	{5}	{5}	{5}	{5}	{5}	{5}	{5}

Impatto riflesso

In queste tavole si analizza ogni asset (superiore) valorizzato per sè stesso (con valore proprio) e si considerano gli altri asset (inferiori) da cui dipende. Quando le minacce si materializzano sull'asset inferiore, il danno si ripercuote su quelli superiori.

asset	[D]	[I]	[R]	[A_S]	[A_D]	[T_S]	[T_D]
ASSET							
[S_T_locale] Trasmissione locale	[5]			[7]		[6]	
[D_incartamenti] Incartamenti aperti	[5]			[7]		[6]	
[E.1] Errore lato utente	[4]	[2]					
[E.2] Errore lato amministratore	[5]	[3]	[3]	[4]	[2]	[4]	[3]
[E.3] Errore di monitoraggio						[5]	[4]
[E.4] Errore di configurazione	[5]	[2]	[3]	[6]	[4]	[5]	[4]
[E.14] Fuga di informazioni							
[E.15] Alterazione delle informazioni							
[E.16] Inserimento di false informazioni							
[E.17] Corruzione delle informazioni							
[E.18] Distruzione delle informazioni	[4]						
[E.19] Diffusione delle informazioni			[3]				
[A.4] Manipolazione della configurazione	[4]	[2]	[5]	[7]	[5]	[6]	[5]
[A.11] Accesso non autorizzato	[5]	[2]	[5]	[6]			
[A.14] Intercettazione delle informazioni			[5]				
[A.15] Alterazione delle informazioni		[4]					
[A.16] Inserimento di false informazioni		[4]					
[A.17] Corruzione delle informazioni		[4]					
[A.18] Distruzione delle informazioni	[5]						
[A.19] Diffusione delle informazioni			[6]				
[email] Posta elettronica	[5]			[7]		[6]	

Rischio riflesso

asset	[D]	[I]	[R]	[A_S]	[A_D]	[T_S]	[T_D]
ASSET							
[S_T_locale] Trasmissione locale	{5}			{5}		{5}	
[D_incartamenti] Incartamenti aperti	{5}			{5}		{3}	
[E.1] Errore lato utente	{4}	{3}					
[E.2] Errore lato amministratore	{3}	{2}	{2}	{3}	{2}	{3}	{2}
[E.3] Errore di monitoraggio						{3}	{3}
[E.4] Errore di configurazione	{3}	{1}	{2}	{4}	{3}	{3}	{3}
[E.14] Fuga di informazioni							
[E.15] Alterazione delle informazioni							
[E.16] Inserimento di false informazioni							
[E.17] Corruzione delle informazioni							
[E.18] Distruzione delle informazioni	{4}						
[E.19] Diffusione delle informazioni			{2}				
[A.4] Manipolazione della configurazione	{2}	{1}	{3}	{4}	{3}	{3}	{3}
[A.11] Accesso non autorizzato	{5}	{3}	{5}	{5}			
[A.14] Intercettazione delle informazioni			{4}				
[A.15] Alterazione delle informazioni		{4}					
[A.16] Inserimento di false informazioni		{4}					
[A.17] Corruzione delle informazioni		{4}					
[A.18] Distruzione delle informazioni	{4}						
[A.19] Diffusione delle informazioni			{5}				
[email] Posta elettronica	{4}			{5}		{5}	

7.2.6. Attività A2.3: Caratterizzazione delle contromisure

AL momento di valutare lo stato di sicurezza dell'unità sotto studio, si devono considerare una serie di aspetti generali ed una serie di aspetti specifici di ogni asset. In questa indagine si deve tenere in considerazione tanto la natura dell'asset quanto il suo valore e le minacce a cui è esposto.

In termini generici si deve verificare

- come è organizzata la sicurezza: responsabili, presa di decisioni, contatti esterni, etc.;
- se c'è un'identificazione dei ruoli del personale, associati ai privilegi di accesso;
- se c'è segregazione effettiva dei compiti;
- se esiste una politica di sicurezza documentata e riveduta periodicamente;
- come si gestiscono gli incidenti;
- come si gestiscono le registrazioni di attività;
- se esiste un piano di continuità: gestione di emergenze, continuità e ripristino

Rispetto ai servizi prestati per l'organizzazione, si deve verificare

- se esistono normative e procedure d'uso, note ed impiegate;
- se esiste un capacity planning;
- se ci sono meccanismi di prevenzione del ripudio;
- se ci sono meccanismi di prevenzione di attacchi di denial of service;

- come si gestiscono gli utenti;
- che registrazioni restano di quello che si è fatto.

Rispetto ai dati trattati dall'organizzazione, si deve verificare:

- se c'è un inventario dei file, con identificazione dei responsabili;
- se esistono normative e procedure d'uso, note ed impiegate;
- se fanno copie di backup e con che qualità;
- se sono previsti meccanismi per garantire il segreto;
- se sono previsti meccanismi per garantire l'integrità;
- se sono previsti meccanismi di registrazione di accesso.

Rispetto agli applicativi in uso, si deve verificare

- come si gestisce la loro manutenzione;
- come si controlla la loro configurazione, in particolare di utenti e destri di accesso;
- se si è ispezionato il codice, specialmente a fronte di back door.

Rispetto al servizio di messaggeria (*email*), si deve verificare:

- se esistono normative e procedure d'uso, note ed impiegate;
- come si gestiscono gli utenti;
- come si controlla il contenuto dei messaggi e degli file allegati
  - dal punto di vista delle fughe di informazioni;
  - dal punto di vista delle iniezione di programmi dannosi (per esempio, virus);
  - dal punto di vista dell'autenticità dell'origine;
- come si assicura la disponibilità del servizio;

Rispetto al servizio di archivio, si deve verificare:

- se esistono normative e procedure d'uso, note ed impiegate;
- come si controlla chi accede al suo uso;
- come si garantisce il segreto dei dati in transito;
- come si garantisce la sua disponibilità.

Rispetto alle apparecchiature informatiche, si deve verificare:

- se esistono normative e procedure d'uso, note ed impiegate;
- come si gestisce la loro manutenzione;
- come si controlla la loro configurazione, in particolare riguardo ad utenti e diritti di accesso;
- come si garantisce il suo disponibilità.

Rispetto alle comunicazioni, si deve verificare:

- se esistono normative e procedure d'uso, note ed impiegate;
- come si controlla chi acconsente al loro uso;
- come si garantisce il segreto dei dati in transito;

- come si garantisce la sua disponibilità.

Il lettore tenga in considerazione che questo è solo un esempio che non pretende di essere esauriente. Ci si è riferiti agli aspetti più rilevanti; non a tutti. È in particolar modo da evidenziare l'assenza di un'analisi delle installazioni fisiche e del personale, che sono state tralasciate per mantenere l'esempio ridotto..

Indagando si verifica che:

- Esiste una politica di sicurezza ereditata dell'organizzazione madre dell'unità di cui ci si occupa. Essendo un'unità di piccole dimensioni, esiste un responsabile unico di sicurezza che riferisce direttamente alla direzione ed è il contatto a fronte di altre organizzazioni. Inoltre esiste una procedura locale di escalation di incidenti che può risalire più in là della propria unità.
- Il server centrale ospita una tavola per controllare quali privilegi di accesso ha ogni utente, differenziando in particolare la capacità amministrativa al fine di dare corso agli incartamenti lungo il suo processo. Tutta l'attività è registrata in un file a cui ha accesso solo l'operatore e che viene spedito quotidianamente all'archivio centrale.
- Le procedure di lavoro con i sistemi non sono scritte. Si fa affidamento sul fatto che le applicazioni web impostino le attività che si possono realizzare in ogni momento secondo lo stato dell'incartamento attivo e secondo i privilegi dell'utente. Si realizza comunque una registrazione di tutte le azioni intraprese dal personale sui servizi web. Per l'elaborazione manuale esiste una serie di stampe disponibili con istruzioni su quando usarle, su che dati fornire e su come inoltrarle.
- Una persona dell'unità ha le funzioni di operatore, incaricandosi di tutti i compiti di installazione, configurazione e risoluzione di incidenti. Questa persona dispone delle procedure scritte per le attività abitudinarie, ma deve improvvisare in situazioni atipiche, per le quali può ricorrere al sostegno tecnico dell'organizzazione madre.
- Non esiste nessuno piano di continuità (al di là della prosecuzione manuale delle attività).
- Esistono contratti di manutenzione con i fornitori delle apparecchiature e dei programmi di base: sistema operativo, di ufficio, posta e server web.
- Gli utenti interni sono amministrati dall'operatore, che necessita richieste per iscritto di entrata in servizio, uscita e cambi. Detta richiesta deve venire firmata dal gerente.
- Gli utenti esterni si registrano personalmente, indicando il loro numeri di CI. Per ottenere la loro password devono presentarsi fisicamente la prima volta. Una volta registrati non si effettua una manutenzione degli account, che durano a tempo indefinito.
- Tanto gli utenti interni come quelli esterni si identificano per accedere attraverso un nome di utente ed una password. Tutti ricevono sommarie istruzioni su come scegliere password; ma non si verifica che le seguano, né che le password siano cambiate regolarmente.
- Si è realizzato recentemente un'audit dei dati di carattere personale, superato completamente in tutti gli aspetti.
- I dati provenienti dall'archivio centrale si considerano corretti. I dati introdotti da i cittadini devono essere convalidati dal personale dell'unità. I dati introdotti dagli utenti interni devono essere convalidati da un secondo utente; normalmente li introduce una persona e li convalida chi firma il progresso dell'incartamento.
- L'applicativo di trasmissione è fornito dall'organizzazione madre, considerandosi "di qualità sufficiente".
- Si è installato un sistema di anti-virus e si è contrattualizzato un servizio di manutenzione

24x7 attraverso l'organizzazione madre con un tempo di risposta inferiore a 1 giorno.

- Il servizio di messaggistica si centralizza nel server in modo che l'accesso degli utenti interni avvenga attraverso un'interfaccia web. Si eliminano in modo sistematico tutti i tipi di allegati nella posta in uscita e si analizzano con l'anti-virus gli allegati della posta in entrata.
- Il servizio di archivio centrale è un servizio prestato esternamente che si considera "di qualità sufficiente". La prestazione di questo servizio dovrà rientrare in un'analisi più dettagliata.
- La comunicazione con Internet risponde ad un contratto ADSL standard, non essendosi realizzato uno studio di necessità, né essendosi prevista nessuna clausola contrattuale di qualità di servizio o ampliamento di capacità.
- La connessione all'archivio centrale si realizza tramite Internet, usando una rete privata virtuale che si stabilisce tra gli estremi. Questa rete è configurata e mantenuta dall'archivio centrale, senza capacità locale alcuna di configurazione. Si considererà "di qualità sufficiente".

In questo punto si ottiene la "Valorizzazione delle contromisure" dell'organizzazione.

Debolezze scoperte

Esaminato quanto raccolto, si stimano le seguenti insufficienze:

- La segregazione di compiti è adeguata tranne nel caso dell'amministratore di sistemi che dispone di ampie capacità di accesso a tutti i sistemi, installazioni e configurazioni.
- Deve esistere una gestione della continuità: gestione di emergenze, piano di continuità e piano di ripristino.
- Devono esistere procedure scritte per tutti i compiti ordinari e per gli incidenti prevedibili, includendo tutti quelli che si sono realizzati nel passato.
- Deve realizzarsi uno studio dell'uso della connessione ADSL e la sua evoluzione per potere pianificare un ampliamento di capacità. Deve inoltre essere stabilito con il fornitore un accordo sulla qualità di servizio.
- Devono stabilirsi meccanismi per scoprire e reagire ad un attacco di denial of service.
- Devono essere analizzati gli account degli utenti esterni, individuando almeno lunghi periodi di inattività, tentativi di penetrazione e comportamenti anomali in genere.
- L'uso di password come meccanismo di autenticazione si considera "debole", raccomandandosi l'uso di schede crittografiche di identificazione.

A questo punto si ottiene la "Relazione delle debolezze" dell'organizzazione.

7.2.7. Attività A2.4: Stima dello stato di rischio

Conosciuti il "Modello dei valori", la "Mappa dei rischi" e la "Valorizzazione delle contromisure", si procede alla stima degli indicatori di impatto e di rischio, tanto cumulativi (sull'asset inferiore) quanto riflessi (sugli asset superiori).

Impatto cumulativo residuo

asset	[D]	[I]	[R]	[A_S]	[A_D]	[T_S]	[T_D]
ASSET							
[FS] Funzioni del sistema informativo							
[S_T_locale] Trasmissione locale	[2]			[3]		[3]	
[S_T_remota] Trasmissione remota	[1]			[3]		[3]	
[D_incartamenti] Incartamenti aperti	[1]	[0]	[2]	[1]	[1]	[1]	[1]
[SI] Servizi interni							
[email] Posta elettronica	[4]			[6]		[5]	
[archivio] Archivio storico centrale	[4]	[3]	[4]	[5]	[4]	[4]	[4]
[A] Apparecchiature							
[sw]							
[SW_incartamenti] Trasmissione degli i	[2]	[2]	[3]	[3]	[2]	[3]	[2]
[hw]							
[PC] Postazioni di lavoro	[4]	[4]	[5]	[6]	[4]	[5]	[4]
[SRV] Server	[4]	[4]	[5]	[6]	[4]	[5]	[4]
[network]							
[firewall] Firewall	[4]	[2]	[4]	[5]	[2]	[5]	[4]
[LAN] Rete Locale	[4]	[2]	[5]	[6]	[5]	[5]	[5]
[ADSL] Connessione a Internet	[4]	[2]	[4]	[6]	[5]	[5]	[5]
[S] Sistemazioni							
[uffici] Uffici	[2]	[1]	[2]	[2]	[1]	[2]	[1]
[cc] Sala macchine	[2]	[1]	[2]	[2]	[1]	[2]	[1]

Rischio cumulativo residuo

asset	[D]	[I]	[R]	[A_S]	[A_D]	[T_S]	[T_D]
ASSET							
[FS] Funzioni del sistema informativo							
[S_T_locale] Trasmissione locale	{3}			{4}		{3}	
[S_T_remota] Trasmissione remota	{2}			{4}		{3}	
[D_incartamenti] Incartamenti aperti	{2}	{2}	{3}	{2}	{0}	{0}	{0}
[SI] Servizi interni							
[email] Posta elettronica	{4}			{5}		{4}	
[archivio] Archivio storico centrale	{4}	{4}	{4}	{5}	{4}	{4}	{3}
[A] Apparecchiature							
[sw]							
[SW_incartamenti] Trasmissione degli	{3}	{3}	{3}	{3}	{3}	{3}	{3}
[hw]							
[PC] Postazioni di lavoro	{5}	{4}	{5}	{5}	{4}	{5}	{4}
[SRV] Server	{5}	{4}	{5}	{5}	{4}	{5}	{4}
[network]							
[firewall] Firewall	{4}	{2}	{4}	{4}	{1}	{3}	{3}
[LAN] Rete Locale	{4}	{2}	{5}	{5}	{3}	{4}	{3}
[ADSL] Connessione a Internet	{4}	{2}	{4}	{5}	{3}	{4}	{3}
[S] Sistemazioni							
[uffici] Uffici	{3}	{3}	{3}	{3}	{3}	{3}	{3}
[cc] Sala macchine	{3}	{3}	{3}	{3}	{3}	{3}	{3}

Impatto riflesso residuo

asset	[D]	[I]	[R]	[A_S]	[A_D]	[T_S]	[T_D]
ASSET							
[S_T_locale] Trasmissione locale	[4]			[6]		[5]	
[D_incartamenti] Incartamenti aperti	[1]			[1]		[1]	
[E.1] Errore lato utente	[0]	[0]					
[E.2] Errore lato amministratore	[1]	[0]	[1]	[0]	[0]	[0]	[0]
[E.3] Errore di monitoraggio						[1]	[0]
[E.4] Errore di configurazione	[1]	[0]	[1]	[1]	[0]	[1]	[0]
[E.14] Fuga di informazioni							
[E.15] Alterazione delle informazioni							
[E.16] Inserimento di false informazioni							
[E.17] Corruzione delle informazioni							
[E.18] Distruzione delle informazioni	[0]						
[E.19] Diffusione delle informazioni			[1]				
[A.4] Manipolazione della configurazione	[0]	[0]	[2]	[1]	[1]	[1]	[1]
[A.11] Accesso non autorizzato	[1]	[0]	[2]	[1]			
[A.14] Intercettazione delle informazioni			[2]				
[A.15] Alterazione delle informazioni		[0]					
[A.16] Inserimento di false informazioni		[0]					
[A.17] Corruzione delle informazioni		[0]					
[A.18] Distruzione delle informazioni	[1]						
[A.19] Diffusione delle informazioni			[2]				
[email] Posta elettronica	[4]			[6]		[5]	

Rischio riflesso residuo

asset	[D]	[I]	[R]	[A_S]	[A_D]	[T_S]	[T_D]
ASSET							
[S_T_locale] Trasmissione locale	{5}			{5}		{5}	
[D_incartamenti] Incartamenti aperti	{2}			{2}		{0}	
[E.1] Errore lato utente	{1}	{1}					
[E.2] Errore lato amministratore	{0}	{0}	{1}	{0}	{0}	{0}	{0}
[E.3] Errore di monitoraggio						{0}	{0}
[E.4] Errore di configurazione	{0}	{0}	{1}	{0}	{0}	{0}	{0}
[E.14] Fuga di informazioni							
[E.15] Alterazione delle informazioni							
[E.16] Inserimento di false informazioni							
[E.17] Corruzione delle informazioni							
[E.18] Distruzione delle informazioni	{1}						
[E.19] Diffusione delle informazioni			{1}				
[A.4] Manipolazione della configurazione	{0}	{0}	{0}	{0}	{0}	{0}	{0}
[A.11] Accesso non autorizzato	{2}	{2}	{3}	{2}			
[A.14] Intercettazione delle informazioni			{2}				
[A.15] Alterazione delle informazioni		{1}					
[A.16] Inserimento di false informazioni		{1}					
[A.17] Corruzione delle informazioni		{1}					
[A.18] Distruzione delle informazioni	{1}						
[A.19] Diffusione delle informazioni			{2}				
[email] Posta elettronica	{4}			{5}		{4}	

A questo punto si ottiene lo "Stato di rischio" dell'organizzazione. Questo "Stato di rischio" viene documentato attraverso la relazione della "Valorizzazione delle contromisure" che sintetizza la realizzazione attuale delle misure di sicurezza, e la "Relazione delle debolezze" che raccoglie le debolezze individuate.

7.3. Processo P3: Gestione dei rischi

7.3.1. Attività A3.1: Presa di decisioni

Visti gli indicatori di rischio residuo e le insufficienze dell'unità, la direzione decide di classificare nei seguenti livelli i programmi di sicurezza da sviluppare:

Di carattere urgente
P1: Sviluppare un piano di continuità P2: Monitorare e gestire gli account degli utenti esterni
Considerazioni importanti
P3.1: Documentare tutti le procedure di lavoro, revisionando quelle attuali ed aggiungendo quelle che mancano P3.2: Segregare le funzioni dell'amministratore dei sistemi
Temi da considerare nel futuro
▪ Uso di schede di identificazione ▪ Contatto con il fornitore di comunicazioni per garantire la qualità del servizio ▪ Contrattazione di un servizio alternativo di comunicazione ▪ Misure a fronte di attacchi di denial of service

7.3.2. Attività A3.2: Piano di sicurezza

Tutte le considerazioni precedenti devono essere plasmate in un "piano di sicurezza" che organizzi le attività in modo pianificato e gestito.

Lo sviluppo del piano di continuità (programma P1) si traduce in un progetto specifico per il quale

1. quest'anno si realizzerà una stima di costi del progetto ed una richiesta di proposte che si completi con il conferimento d'incarico ad un appaltatore esterno;
2. vista l'offerta vincitrice si destineranno fondi nell'anno a venire per la realizzazione del piano; in questa realizzazione si includeranno tutti i compiti amministrativi (dimensionamento, scelta di soluzioni, procedure, etc.), eccettuandosi le possibili esecuzioni di opere civili o la contrattazione di servizi esternalizzati di continuità, che saranno oggetto di future gare.

Per il monitoraggio degli account (programma P2) si lancia un progetto per lo sviluppo di un sistema di gestione degli account che includa il rilevamento di intrusioni ed il lancio di allarmi. Si stima che questo progetto si possa lanciare immediatamente e che la sua durata sarà di un anno.

Per la documentazione di tutte le procedure (programma P3.1) si ricorrerà ad un ampliamento del contratto di consulenza ed assistenza che l'organizzazione madre ha attualmente. In questo ampliamento, consulenti esterni si incaricheranno di ottenendo le informazioni pertinenti, completando i manuali attuali. Questo compito non si affronterà fino al prossimo anno finanziario. Nell'elaborazione delle procedure si definiranno i compiti specifici di un operatore (locale) ed un amministratore (remoto) in modo che si raggiunga l'obiettivo del programma P3.2. Si negozia con l'archivio centrale la disposizione di un servizio centralizzato di amministrazione, lasciando a livello locale le mere funzioni di operatività.

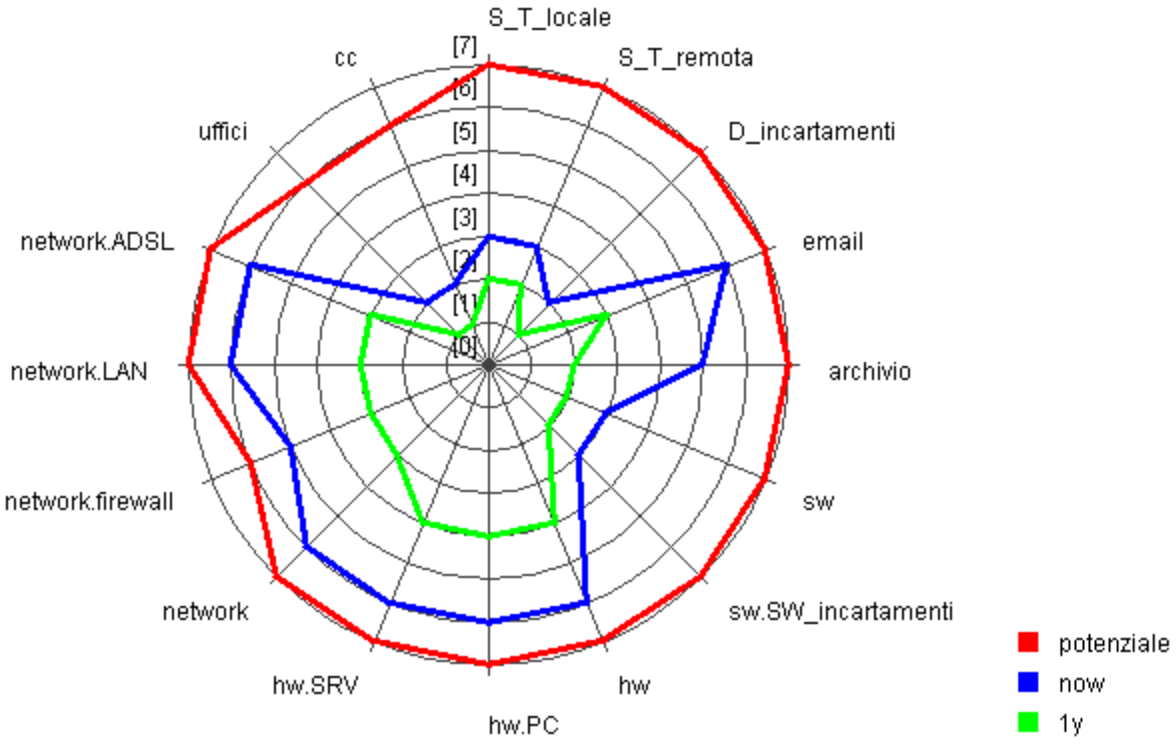
Infine si ottengono dall'organizzazione madre le informazioni sull'uso di schede di identificazione corporativa ed anche della carta di identità elettronica, come mezzi che potrebbero utilizzarsi nel futuro per migliorare l'autenticità degli utenti. Per il prossimo anno finanziario si contrattualizzerà uno studio delle modifiche richieste per incorporare detti meccanismi, tanto per gli utenti interni quanto per gli utenti esterni. Parte di questo studio sarà un piano dettagliato di realizzazione, che in nessun caso si affronterà prima di due anni.

7.3.3. Evoluzione degli indicatori di impatto e rischio

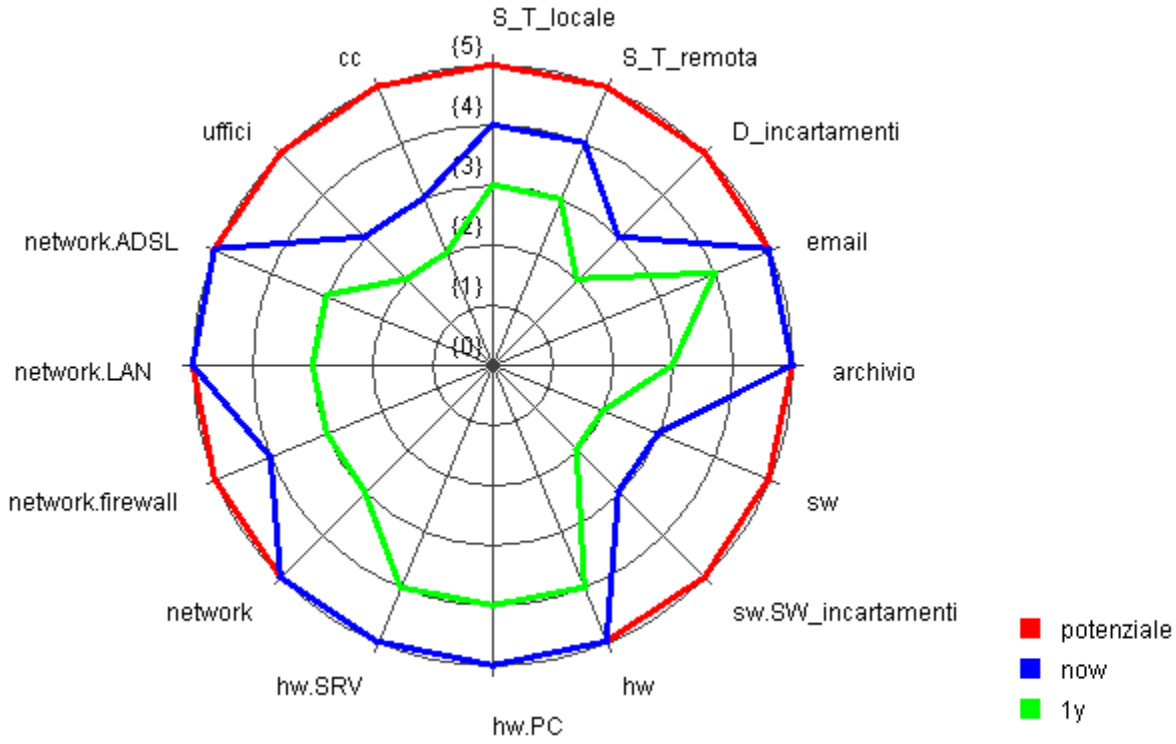
Le seguenti figure mostrano l'evoluzione degli indicatori di impatto e rischio, cumulativo e riflesso, in tre istanti della gestione del sistema informativo sottoposto a studio:

- senza contromisure;
- nel momento presente;
- a valle dell'esecuzione dei programmi P1, P2 e P3 del piano di sicurezza (1 anno).

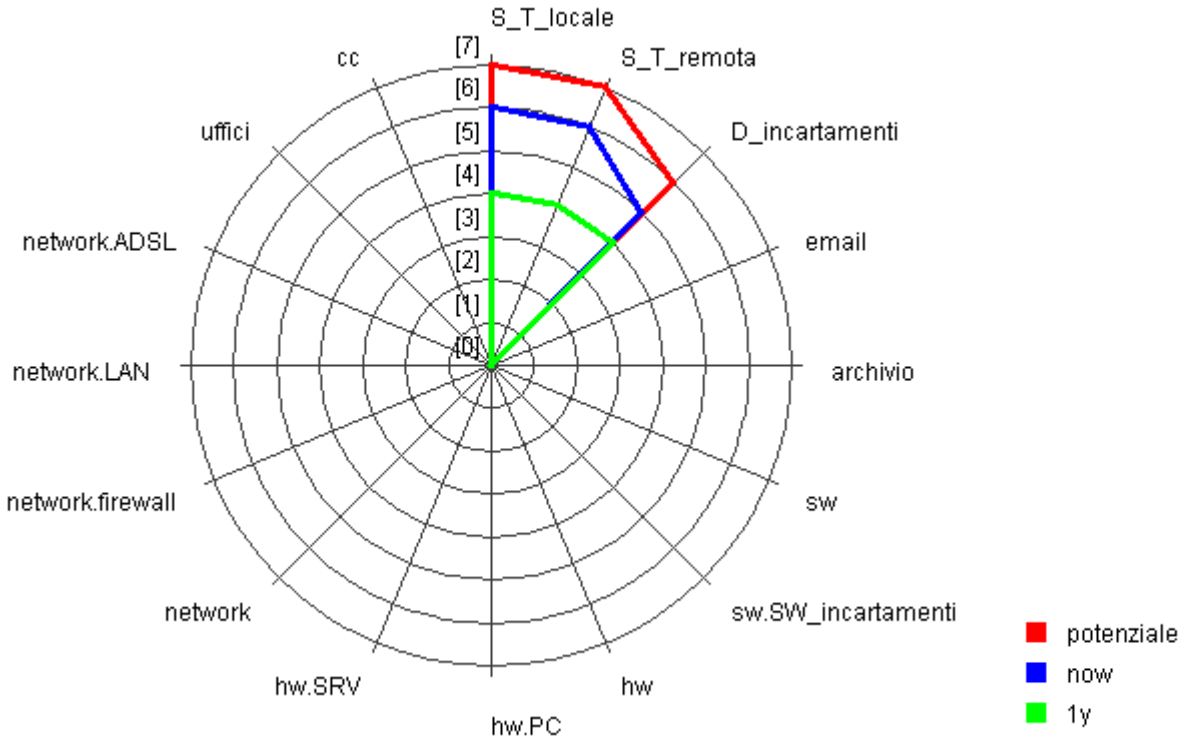
Impatto cumulativo



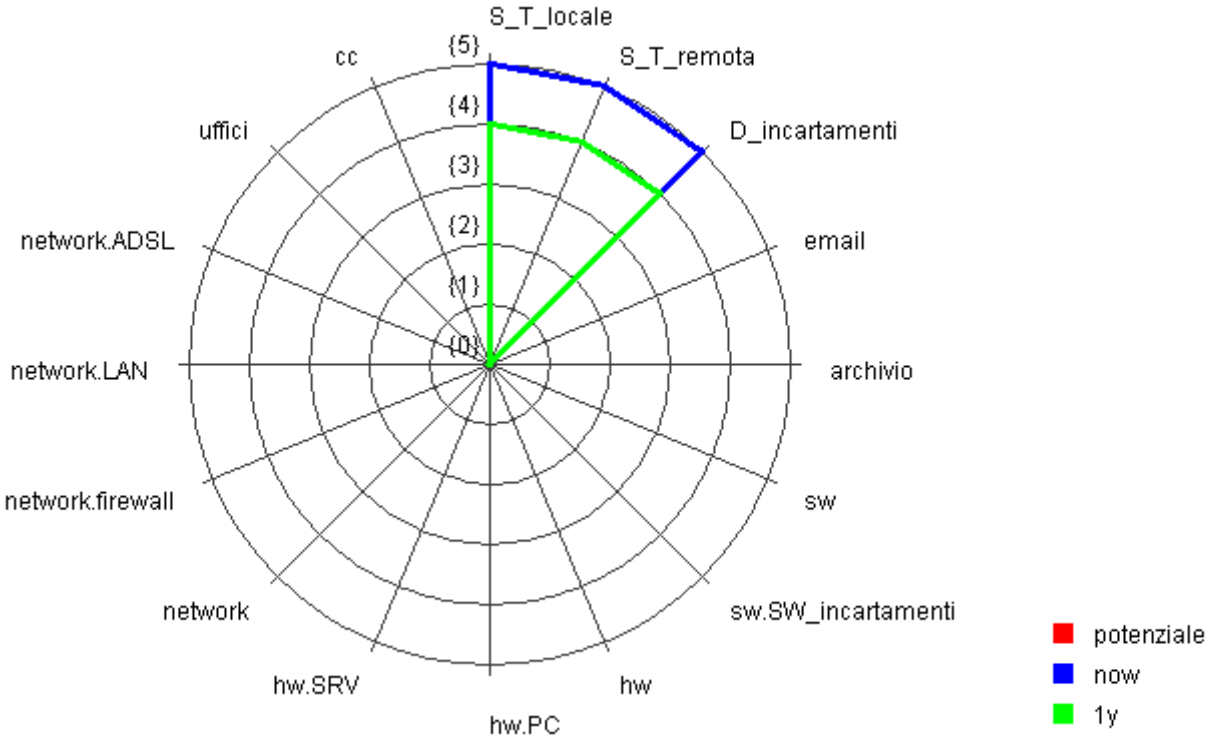
Rischio cumulativo



Impatto riflesso



Rischio riflesso



7.3.4. Qualificazione secondo la norma ISO/IEC 17799:2005

La norma ISO/IEC 17799:2005, "Code of pratice for information security management", definisce una serie di controlli raccomandabili per i sistemi di gestione della sicurezza delle informazioni (SGSI). La seguente grafica mostra il grado di soddisfazione di detti di criteri lungo lo sviluppo del piano di sicurezza:

