www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Appunti libro Cesare Gallotti

Analisi E Gestione Del Rischio (Università degli Studi di Milano)

Studocu non è sponsorizzato o supportato da nessuna università o ateneo.
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Appunti libro Cesare Gallotti-Sicurezza delle informazioni

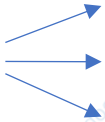
Definizioni della vecchia ISO 27000
Informazione (Information data): conoscenza o insieme di dati che hanno valore per un individuo o un'organizzazione
Sicurezza delle informazioni (Information security): preservazione della riservatezza, integrità e disponibilità delle informazioni.
Riservatezza (Confidentiality): proprietà di un'informazione di non essere disponibile o rivelata a individui, entità o processi non autorizzati;
Integrità (Integrity): proprietà di accuratezza e completezza;
Disponibilità (Availability): proprietà di essere accessibile e utilizzabile [entro i tempi previsti] su richiesta di un'entità autorizzata.
Processo: insieme di attività fra di loro interrelate o interagenti che trasformano elementi in ingresso (input) in elementi in uscita (output).
Sistema di gestione (management system): Insieme di elementi interrelati e interagenti di un'organizzazione per stabilire politiche e obiettivi e [insieme di] processi [interrelati e interagenti] per raggiungere tali obiettivi.
Rischio: effetto dell'incertezza sugli obiettivi
Livello di rischio: grandezza di un rischio espresso come combinazione delle sue conseguenze e della loro verosimiglianza
Valutazione del rischio (risk assessment): processo complessivo di identificazione, analisi e ponderazione del rischio.
Responsabile del rischio (risk owner): persona o entità con la responsabilità e con il potere per gestire un rischio.
Identificazione del rischio: processo di individuazione, riconoscimento e descrizione del rischio.
Asset (bene): qualsiasi cosa cha abbia valore per l'organizzazione.
Evento relativo alla sicurezza delle informazioni: Occorrenza identificata [...] e indicante una possibile violazione delle politiche di sicurezza delle informazioni, un funzionamento scorretto delle misure di sicurezza o una situazione precedentemente sconosciuta che potrebbe interessare la sicurezza delle informazioni.
Incidente relativo alla sicurezza delle informazioni: Evento o serie di eventi, non voluti e/o inattesi, relativi alla sicurezza delle informazioni, che hanno una probabilità significativa di compromettere le attività e di minacciare la sicurezza delle informazioni.
Minaccia: causa potenziale di un incidente, che può comportare danni ad un sistema o all'organizzazione.
Vulnerabilità: debolezza di un asset o di un controllo di sicurezza che può essere sfruttata da una o più minacce.
Analisi del rischio: processo di comprensione della natura del rischio e di determinazione del livello di rischio.
Ponderazione del rischio (risk evaluation): processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio è accettabile o tollerabile.
Criteri di rischio: valori di riferimento rispetto ai quali è ponderato il rischio.
Controllo: misura che modifica il rischio.
Politica: intenzioni e indirizzi di un'organizzazione espressi formalmente da parte della Direzione.
Direzione [con la "D" maiuscola, o alta direzione o top management]: persona o gruppo di persone che dirigono e tengono sotto controllo un'organizzazione al più alto livello.
Efficacia: grado rispetto al quale le attività pianificate sono realizzate e i risultati pianificati raggiunti.
Obiettivo: risultato da raggiungere.
Monitoraggio: Determinazione dello stato di un sistema, di un processo o di un'attività.
Nota: per la determinazione dello stato, potrebbe essere necessario verificare, sovrintendere o osservare.

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Misurazione: processo per determinare un valore.
Metodo di misurazione: sequenza logica di operazioni [...] usate per quantificare un attributo rispetto ad una scala specificata.
Non conformità: mancato soddisfacimento di un requisito.
Azione correttiva: azione per eliminare la causa di una non conformità e prevenirne il ripetersi.
Azione preventiva: azione per eliminare la causa di una potenziale non conformità o altre situazioni indesiderabili.

Definizione derivante dalla ISO 9000:2015:
Sistema di gestione per la sicurezza delle informazioni (SGSI): la parte del sistema di gestione di un'organizzazione che si occupa della sicurezza delle informazioni. O ISMS (information security management system).

Le informazioni sono archiviate e messe su dei supporti 

Quando si parla di sicurezza delle informazioni non ci si limita alla sicurezza informatica ma ad ogni sistema usato per raccogliere, conservare, modificare, trasmettere e distruggere le informazioni.
La sicurezza informatica è invece solo la parte di sicurezza delle informazioni che si riferisce ai sistemi informatici.

- dati: insieme di singoli fatti, immagini e impressioni;
- informazioni: dati organizzati e significativi;
- conoscenza: informazioni recepite e comprese da un singolo individuo;
- sapienza: conoscenze tra loro connesse che permettono di prendere decisioni

Principi:
Esistono altre proprietà importanti per la sicurezza delle informazioni oltre alla triade CIA:
Autenticità: le informazioni sono autentiche quando attestano la verità
Non ripudio: l'autore delle informazioni non può smentirle
Completezza: un'informazione che non ha carenze 
Ulteriore elemento è il diritto all'oblio, che prevede che le informazioni siano eliminate dopo quanto affermato nel momento di raccolta dei dati oppure, a meno che questo non vada contro le normative, quando richiesto dal possessore delle informazioni.

Processi:
I processi vanno tenuti sotto controllo, questo va verificato misurando l'efficacia e l'efficienza di quest'ultimo. Si forniscono le seguenti definizioni, derivanti dalla norma ISO 9000:2015:
Efficacia: grado rispetto al quale le attività pianificate sono realizzate e i risultati pianificati raggiunti.
Efficienza: relazione tra risultati ottenuti e risorse utilizzate.
Caratteristiche di un processo:

È necessario conoscere due termini: si mappano i processi così come sono e si modellano così come si desidera modificarli.
I processi non sono indipendenti ma sono tra loro interrelati e interagenti.

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Il sistema di gestione prevede di stabilire politiche, obiettivi e processi e poi fare in modo che gli obiettivi siano raggiunti.
In sintesi possiamo affermare che:

- ogni organizzazione ha uno scopo (missione)
- il sistema di gestione di un'organizzazione è il suo insieme pratiche organizzative (processi) e di strumenti atti a raggiungere il suo scopo;
- tali processi e strumenti sono tra loro interrelati;
- ciascun cambiamento organizzativo, anche se potenzialmente piccolo, può avere degli impatti su molte aree dell'organizzazione e sui clienti e fornitori, derivanti delle interrelazioni dei processi;
- quando si operano cambiamenti va prestata attenzione ai loro impatti sin da quando sono pianificati.

Funzioni:
Un'organizzazione è strutturata in funzioni, ossia gruppi di persone. I processi descrivono come le funzioni interagiscono tra loro per portare a termine gli obiettivi dell'organizzazione.
Le comunicazioni tra funzioni o tra persone della stessa funzione devono avvenire in maniera concordata.

Le 3 P:
Per la realizzazione di un sistema di gestione della sicurezza delle informazioni sono fondamentali questi tre elementi, tutti in egual misura: prodotti, processi e persone.

Valutazioni sulla gestione del rischio:
Le valutazioni necessarie per accertare che i metodi utilizzati stiano avendo dei risultati positivi devono essere eseguite da enti terzi e indipendenti, a loro volta controllati da appositi organismi.
Le valutazioni prevedono la raccolta e l'analisi degli elementi di prova secondo criteri stabiliti e il risultato finale può dare luogo ad una certificazione.
Nell'ambito della sicurezza delle informazioni esistono schemi per la certificazione dei processi, delle persone e dei prodotti.

Risk assessment:
La valutazione del rischio è divisa in tre fasi:

- identificazione del rischio
- analisi del rischio
- ponderazione del rischio (valutazione)

Questa fase deve essere preceduta da un'analisi del contesto e dell'ambito in cui applicare il rischio e seguita da un trattamento del rischio.
Il rischio è l'effetto dell'incertezza sugli obiettivi, l'incertezza è dovuta ad eventi che possono portare a impatti positivi o negativi. Gli impatti positivi portano ad opportunità mentre quelli negativi portano a danni.
Per comprendere come agire di fronte ad un rischio è importante stabilire il livello di rischio che si corre, ovvero la combinazione della probabilità o verosimiglianza e delle sue conseguenze. Si usa il termine verosimiglianza perché "probabilità" fa intendere che il rischio vada obbligatoriamente calcolato con metodi quantitativi.

Risk treatment:
Una volta calcolato il livello di rischio, è necessario prendere delle decisioni per affrontarlo o trattarlo (scelta di una o più opzioni: prevenire, ridurre, evitare, condividere, accettare).

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Qui a fianco abbiamo la rappresentazione dell'organizzazione attraverso la piramide di Anthony:

A livello strategico sono richiesti dati stimati e approssimati, utili per dare indirizzi con prospettive a lungo termine.

A livello tatti sono richiesti dati consultivi, arrotondati, utili per prospettive a medio termine.

A livello operativo i dati sono esatti e in tempo reale, servono a tenere sotto controllo le attività in corso.

Il livello di dettaglio nell'analisi del rischio deve essere basso poiché la situazione è in continuo cambiamento e non si riusciranno mai ad avere dati esatti perché è un'analisi basata sul futuro.

Un metodo valido di valutazione del rischio deve avere le seguenti caratteristiche:

- completezza: devono essere considerati, al giusto livello di sintesi, tutti gli asset, tutte le minacce e tutte le vulnerabilità;
- ripetibilità: valutazioni condotte nello stesso contesto e nelle stesse condizioni devono dare gli stessi risultati;
- comparabilità: valutazioni condotte in tempi diversi nello stesso contesto devono permettere di comprendere se il rischio è cambiato e come;
- coerenza: a fronte di valori di asset, minacce e vulnerabilità più elevati di altri, il livello di rischio deve essere più elevato.

Programmi software per la valutazione del rischio:
Si trovano in commercio molti programmi software per la valutazione del rischio, questi presentano numerosi difetti. Il primo difetto consiste nella quantità di dati da inserire: spesso sono moltissimi e richiedono molto tempo. Questo non garantisce affatto risultati precisi, utili o validi.
Il secondo difetto, comune a molti prodotti, consiste nella segretezza dell'algoritmo di calcolo. In questo modo, a fronte di risultati non accettabili, non ne è possibile comprendere l'origine per correggerla o per convincersi della validità dei risultati.
Il terzo difetto consiste nella configurazione iniziale del prodotto, che viene fatta non seguendo una situazione personalizzata.
Il quarto difetto è la difficoltà di riconfigurazione di questi strumenti.
Il quinto difetto è che gli utilizzatori di un software commerciale tendono ad adottarlo in modo meccanico, quando invece dovrebbero adattare il metodo al proprio contesto.
Alcune metodologie invitano ad avvalersi di facilitatori per la conduzione degli incontri tra le parti interessate e per coordinare le diverse attività, spesso questo lavoro è fatto da uno o più consulenti esterni.

1. Il contesto e l'ambito:

In questo capitolo si descrivono le fasi preliminari alla valutazione del rischio. Queste prevedono un'analisi del contesto in cui si vuole operare in modo da decidere in quale ambito valutare il rischio.
La definizione della ISO 9000:2015 fornisce una prima indicazione:
Contesto di un'organizzazione: combinazione di fattori interni ed esterni che possono avere degli effetti sullo sviluppo e raggiungimento degli obiettivi di un'organizzazione.
Dopo aver individuato il contesto, è possibile decidere l'ambito in cui effettuare la valutazione del rischio relativo alla sicurezza delle informazioni. Esso può comprendere tutta l'organizzazione o una parte di essa.

2. Inizio del risk assessment:

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

a) Identificazione del rischio: questo processo richiede l'identificazione degli asset, delle minacce, delle vulnerabilità e le relazioni tra questi.
I primi asset da identificare sono le informazioni per poi correlarle a tutti gli asset che le contengono o le trattano. Per individuarle conviene partire dai processi dell'organizzazione.
Dopo aver individuato le informazioni è necessario individuare gli altri asset utilizzati per trattarle o conservarle. Il dettaglio degli asset è importante per la gestione operativa, non per la valutazione del rischio, pertanto non bisogna fare un'analisi a granularità molto fine.
Per meglio individuare le minacce, si inizia dall'individuazione degli agenti di minaccia (persone malintenzionate, la natura, gli strumenti tecnici), per poi individuare le tecniche di minaccia.
Le minacce dovrebbero essere inizialmente individuate dai referenti delle informazioni, ma spesso non hanno le competenze per farlo quindi vengono chiamati i responsabili dei diversi sistemi.
Bisogna poi associare le minacce agli asset per valutarne la verosimiglianza (probabilità con cui la minaccia si piò trasformare in evento o incidente).
Deve poi essere individuate le vulnerabilità e di conseguenza le relazioni tra questi tre elementi.

b) Analisi del rischio:
Si tratta di un'attività di stima del rischio senza alcun tipo di giudizio. Per determinare il livello di rischio bisogna assegnare dei valori agli asset, alle minacce e alle vulnerabilità. Questi valori devono essere il più possibile oggettivi e ripetibili.
Per garantire la ripetibilità dei risultati, ossia la capacità di ottenere risultati uguali se le analisi sono effettuate nel medesimo contesto, una buona tecnica consiste nel giustificare per iscritto le motivazioni dei valori assegnati; così si migliora anche l'oggettività dell'analisi perché la documentazione rende le scelte più prudenti e permette di effettuare affinamenti futuri.
I metodi di analisi possono essere quantitativi e qualitativi (esistono metodologie semi-quantitative).

Il valore degli asset:
Come metodo pratico è utile determinare inizialmente il valore dell'asset i(a) in termini di riservatezza, integrità e disponibilità:

In termini economici, i costi per il ripristino e le sanzioni sono detti costi diretti, quelli dovuti ai mancati ricavi sono detti costi indiretti e gli altri costi consequenziali. Anche qui esistono metodi qualitativi o quantitativi per l'assegnazione di valori alle tre proprietà collegate ai beni.
Il risultato, sia che si adottino metodologie quantitative che qualitative, potrebbe essere riesaminato e modificato considerando gli effetti delle interdipendenze:

- distribuzione: i valori di uno o più parametri dell'asset possono essere diminuiti se l'asset è marginale rispetto ad altri asset
- dipendenza: i valori di uno o più parametri dell'asset possono essere aumentati se l'asset è fondamentale per altri asset
- cumulo: i valori di uno o più parametri dell'asset possono essere aumentati se l'asset è collegato a tante informazioni

Si valuta poi la verosimiglianza o probabilità delle minacce. Anche qui si può decidere se utilizzare metodi qualitativi o quantitativi.
Per dare maggiore senso di oggettività, si fa riferimento a delle statistiche pubblicate da diversi enti anche se queste non sono propriamente affidabili (chi riceve attacchi non li denuncia..).

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

La combinazione tra il valore degli asset e la probabilità di accadimento di una minaccia, senza considerare le vulnerabilità o le misure di sicurezza in atto è considerato rischio intrinseco o rischio puro.

Il rischio intrinseco può essere quantitativo o qualitativo:

Segue una valutazione delle vulnerabilità e dei controlli di sicurezza, bisogna prima individuare i controlli ideali sul rischio intrinseco e valutare quanto si discostano da quelli attivi. I controlli possono essere ideali nell'ambito in cui si effettua l'analisi (proporzionali al rischio intrinseco specifico per l'ambito in cui si valuta il rischio) o in generale controlli ideali assoluti (stabilire a priori quali controlli di sicurezza prevedere per i diversi livelli di rischio intrinseco indipendentemente dalla realtà osservata, e poi verificare se le misure previste sono attuate, parzialmente attuate o non attuate.
I controlli attuati per ciascun asset devono essere confrontati con quelli ideali, in modo da attribuire un valore rispetto all'adeguatezza e conformità.
Quando un controllo non è progettato come quello ideale, si dice che non è adeguato o sufficiente.
Quando un controllo di sicurezza è adeguato ma non è attuato correttamente e come previsto, si dice che è non conforme o non corretto.
In tutti e due i casi, si può parlare di inefficacia: inefficacia di progettazione o inefficacia di attuazione.
Quando si valuta l'adeguatezza dei controlli, bisognerebbe valutare anche la loro uniformità e, nel caso in cui a seguito di non conformità o inadeguatezze siano presenti controlli compensativi.
Per calcolare il livello di rischio si possono utilizzare le medesime formule di calcolo del rischio intrinseco, aggiungendo il parametro di vulnerabilità.
Al termine dei calcoli, il livello di rischio deve essere riesaminato ed eventualmente modificato per gli effetti di distribuzione, dipendenza e cumulo.
Il livello di rischio può essere quantitativo o qualitativo:

c) Ponderazione del rischio:
La ponderazione del rischio è il processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio è accettabile o tollerabile.
In altre parole, consiste nell'accettare o non accettare un rischio in base a dei criteri prestabiliti.
È quindi necessario ordinare i rischi dal più elevato al meno elevato e cominciare a ponderarli (ossia, giudicarli) uno ad uno.
Il fatto di accettare un rischio o meno è una questione soggettiva e non è possibile renderla oggettiva.
In questa fase si effettua uno studio di fattibilità preliminare relativo ai possibili controlli di sicurezza da introdurre o alle modifiche a quelli esistenti, in modo da comprendere se avviare dei progetti di miglioramento. Lo studio di fattibilità andrà approfondito nel processo di trattamento del rischio.

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

3. Trattamento del rischio: processo per modificare il rischio
   il trattamento può comportare: evitare il rischio decidendo di non iniziare o continuare un'attività; prendere o aumentare il rischio per cogliere un'opportunità; rimuovere la sorgente del rischio [ossia la minaccia]; modificare la probabilità [della minaccia]; modificare le conseguenze; condividere il rischio con altri soggetti (anche attraverso contratti e finanziamenti); mantenere il rischio con una scelta informata. il trattamento del rischio può creare nuovi rischi o
   modificare quelli esistenti.
   Alla fine di questo processo di trattamento si stende un piano di trattamento del rischio, il rischio successivo al trattamento è detto rischio residuo.
   - Evitare o eliminare il rischio: quando decide di non iniziare o di interrompere un'attività. Questa scelta è di tipo strategico e legata al posizionamento sul mercato dell'organizzazione quindi è raro vederla se collegata strettamente alla sicurezza delle informazioni
   - Aumentare il rischio: Il rischio potrebbe essere aumentato inconsapevolmente e questo è molto pericoloso. si può aumentare consapevolmente il rischio quando si modificano delle procedure, anche a fronte di controlli di sicurezza ritenuti eccessivamente onerosi (ritenuto come una vulnerabilità).
   - Prevenire il rischio: Questa opzione prevede quindi di aggiungere o migliorare i controlli di prevenzione e di rilevazione
   - Mitigare il rischio: Questa opzione è collegata ai controlli di recupero, come ad esempio i backup.
   - Condividere il rischio: La condivisione del rischio si attua attraverso il ricorso a fornitori e a polizze assicurative
   - Accettare il rischio: si decide di non far nulla, si accetta il rischio

   L'insieme di tutte le decisioni prese, rischio per rischio, prende il nome di piano di trattamento del rischio (risk treatment plan). Solitamente la maggioranza delle scelte sono di accettazione del rischio ma nel caso non si decida di accettarlo, per ognuna delle altre scelte dovranno essere identificati i benefici attesi.
   Prima di approvare il piano delle azioni, vanno accertarti i loro benefici, la loro reciproca coerenza, la loro fattibilità e che non introducano nuovi rischi inaccettabili.
   Per valutare se un'azione possa portare ad una riduzione del rischio, si può effettuare una what-if analysis, vale a dire la determinazione dei valori previsti per asset, minacce e vulnerabilità a seguito della conclusione dell'azione, in modo da calcolare il livello di rischio che si otterrebbe.
   Il miglioramento continuo deve essere interpretato come una costante capacità di analisi del contesto, in modo da individuare i rischi e controllarli in modo che siano accettabili, e di completamento delle azioni pianificate. Bisogna assicurarsi la coerenza delle azioni e la loro fattibilità.
   Dopo aver concluso l'azione, è necessario verificare se è stata realizzata correttamente e ha avuto gli effetti desiderati. In altre parole, è necessario verificarne e valutarne l'efficacia.
   Nel tempo dovrebbero essere analizzati gli avanzamenti delle azioni da parte dei responsabili dei rischi, in modo che eventuali ritardi o altri problemi siano gestiti.
4. Monitoraggio e riesame del rischio:
   Gli asset e le informazioni e il loro valore, le minacce e la loro verosimiglianza e le vulnerabilità e la loro gravità cambiano ne tempo oppure sono percepite diversamente nel tempo.
   Bisogna quindi tenere sotto controllo il contesto di riferimento affinché i cambiamenti siano identificati e bisogna mantenere attiva la comunicazione tra tutti gli stakeholder.

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Bisogna effettuare nuovamente la valutazione del rischio a intervalli periodici oppure a seguito di cambiamenti rilevanti.

Tecniche di minaccia:

- Intrusione nella sede o nei locali da parte di malintenzionati
- Intrusione nei sistemi informatici da parte di malintenzionati
- Social engineering
- Furto d'identità
- Danneggiamento di apparecchiature fisiche
- Danneggiamenti dei programmi informatici
- Furto di apparecchiature informatiche o di impianti fisici
- Lettura, furto, copia o alterazione di documenti in formato fisico
- Intercettazioni di emissioni elettromagnetiche
- Interferenze da emissioni elettromagnetiche
- Lettura e copia non autorizzata di documenti informatici
- Modifica non autorizzata di documenti informatici
- Trattamento scorretto delle informazioni rispetto alla normativa
- Malware
- Copia e uso illegale di software
- Uso non autorizzato di sistemi e servizi informatici esterni
- Uso non autorizzato di sistemi e servizi informatici offerti dall'organizzazione
- Recupero di informazioni
- Esaurimento o riduzione delle risorse
- Intercettazione delle comunicazioni
- Invio di dati a persone non autorizzate
- Invio e ricezione di dati non accurati
- Ripudio di invio di messaggi e documenti da parte del mittente

I controlli di sicurezza:
I controlli di sicurezza delle informazioni sono spesso indicati con il termine misure o contromisure.
i controlli possono essere processi, politiche, strumenti, pratiche o altre azioni che modificano il rischio e non sempre ottengono il risultato aspettato.
Controlli di sicurezza delle informazioni:

- Documenti: Per garantire la sicurezza delle informazioni vanno fornite al personale regole e istruzioni su come comportarsi, come trattare le informazioni e come gestire gli strumenti in uso.
  Sono previsti tre tipi di documenti
  - Politiche, che danno le regole generali. Vi sono due tipi di politiche: quelle generali (per esempio, la "politica per la sicurezza delle informazioni") e quelle specifiche per un determinato argomento, dette politiche di dettaglio.
    Deve riportare:
    - cosa si intende per "sicurezza delle informazioni", perché è importante per l'organizzazione, cosa è più e cosa è meno importante;
    - quali sono i principi generali da seguire, incluso l'impegno a rispettare i requisiti legali e quelli dei clienti in materia di sicurezza delle informazioni e l'impegno a migliorare continuamente la sicurezza delle informazioni;
    - come sono state assegnate le responsabilità a più alto livello.

    Le politiche vanno periodicamente riesaminate.
  - Procedure: un modo specifico per effettuare un'attività o un processo. Può essere documentata (procedura scritta/documentata) o meno (prassi).

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Il termine linee guida fa riferimento a documenti le cui indicazioni, a differenza delle procedure, non sono da attuare obbligatoriamente.

- Registrazioni: documento che riporta i risultati ottenuti o fornisce evidenza delle attività svolte. Possono essere di due tipi: con approvazione e senza approvazione.

Organizzazione per la sicurezza delle informazioni:
Uno dei principi di organizzazione aziendale richiede di assegnare esplicitamente le responsabilità per ciascuna attività e processo.

- La direzione: Direzione [con la "D" maiuscola, o alta direzione o top management]: persona o gruppo di persone che dirigono e tengono sotto controllo un'organizzazione al più alto livello.
  La Direzione ha la responsabilità ultima della sicurezza delle informazioni, così come di tutto il resto. Essa deve stabilire le politiche di sicurezza delle informazioni, assegnare le responsabilità, effettuare o far effettuare verifiche sulla corretta attuazione delle disposizioni date e dare l'esempio. La Direzione ha anche la responsabilità di fornire le risorse necessarie a garantire l'efficacia del sistema di gestione.
- Governance e management: la governance si occupa di attività direzionali e di fornire politiche e linee guida, mentre il management si occupa di garantire operativamente il loro rispetto. La direzione è la prima responsabile della governance e deve stabilire i ruoli e le responsabilità per l'attività di management.
- Il responsabile della sicurezza: non è richiesto dalle normative ma molto spesso viene assegnato questo ruolo Considerando quanto previsto dal Regolamento europeo in materia di privacy, ulteriore figura da prevedere è il Data protection officer o DPO o, in italiano, Responsabile della protezione dei dati personali. Questa figura, non sempre obbligatoria, può coincidere con il Responsabile per la sicurezza delle informazioni.
- Altri:
  Alcuni ruoli di primo livello, importanti per la sicurezza delle informazioni e da avere chiaramente visibili sull'organigramma riguardano i responsabili di: sistemi e reti IT (infrastruttura informatica), sviluppo dei programmi informatici, gestione del personale, acquisti, logistica e sicurezza fisica, audit interni.

I vari ruoli devono coordinarsi tra loro e a tal fine vanno istituite commissioni da riunire periodicamente per: analizzare eventi incidenti occorsi dopo la riunione precedente, riesaminare l'avanzamento delle attività concordate in precedenza e stabilire come migliorare i processi, le procedure e le misure di sicurezza con impatto su più funzioni.
Una commissione composta dai dirigenti di più alto livello è anche chiamata forum per la sicurezza delle informazioni.

Il termine progetto indica un insieme di attività con termini di tempo obiettivi definiti, Il risultato di un progetto è spesso indicato con il termine prodotto, anche se si tratta di un servizio o di un'organizzazione.
In particolare, è opportuno ricordare che ogni progetto prevede le seguenti fasi, importanti per la sicurezza delle informazioni:

1) pianificazione: all'avvio del progetto le attività sono pianificate e le responsabilità assegnate
2) definizione dei requisiti del prodotto
3) momenti di incontro tra le parti interessate, anche nell'ambito dei coordinamenti periodici
4) attività di verifica e test, inclusi quelli relativi alla sicurezza delle informazioni, come i penetration test

Gestione del personale:
Prima di inserire qualcuno nell'organizzazione bisogna verificare se le competenze dichiarate dal candidato corrispondano a quelle effettive richiedendo copie dei certificati di studio e professionali.

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Nel caso queste persone non abbiano le competenze auspicate bisogna predisporre un piano di formazione. Una volta selezionata la persona, si redige il contratto. Esso deve prevedere un accordo di riservatezza per cui la persona si impegna a non comunicare informazioni dell'organizzazione a persone non autorizzate o a farne uso senza autorizzazione. Questo accordo deve rimanere valido anche dopo la conclusione del rapporto di lavoro. Le persone vanno formate e sensibilizzate, bisogna fare in modo che siano consapevoli dei rischi che incombono sull'organizzazione e su loro stessi.

Gestione degli asset

Le informazioni vanno classificate, attribuendo loro i pertinenti livelli di riservatezza, ha il fine di stabilire chi è autorizzato ad accedere alle singole informazioni e modificarle.

In Italia, la normativa sul segreto di Stato prevede quattro livelli crescenti: riservato, riservatissimo, segreto e segretissimo.

Purtroppo, tranne un Regio Decreto del 194162, non sono disponibili linee guida per l'assegnazione di tali valori.

Una volta classificate, le informazioni possono essere etichettate. La scritta deve riportare il livello di classificazione e le aree il cui personale è autorizzato ad accedervi.

A seconda del livello di classificazione, vanno previste delle diverse modalità di trattamento. Esse riguardano:

- la conservazione delle informazioni a seconda del loro supporto
- la copia totale o parziale delle informazioni, in alcuni casi da vietare;
- la trasmissione delle informazioni
- la distruzione delle informazioni
- lo scambio delle informazioni con entità esterne

Nell'ambito della sicurezza delle informazioni, è necessario identificare gli asset al corretto livello di dettaglio.

Per effettuare la valutazione del rischio relativo alla sicurezza delle informazioni non è necessario identificare gli asset ad un elevato livello di dettaglio, mentre per finalità operative è necessario.

A ciascun asset va assegnato un proprietario, ossia la funzione organizzativa o la persona con la responsabilità della sua corretta gestione e manutenzione.

Controllo degli accessi:

Con il termine credenziali si indicano i parametri forniti ad una persona per poterla riconoscere. Il riconoscimento avviene in due fasi:

- identificazione: ad una persona viene assegnato un codice identificativo;
- autenticazione: si accerta che la persona sia effettivamente chi dichiara di essere.

Le autorizzazioni corrispondono alle operazioni che può effettuare una persona su un sistema informatico o su dei dati.

I principi relativi alle autorizzazioni sono spesso riassunti in tre espressioni:

- minimum privilege: a ciascuno devono essere date solo le autorizzazioni minime di cui ha bisogno
- need to know (to use): l'accesso a informazioni, programmi software, strumenti e archivi deve essere concesso solo a quanti hanno la necessità di accedere a quelle informazioni
- separation of duties (separazione dei ruoli): alcune operazioni vanno iniziate, controllate e approvate da persone distinte

Ci sono diversi modelli per assegnare le autorizzazioni, anche sulla base della classificazione delle informazioni. I due modelli generali più noti sono indicati dai termini discretionary access control (DAC) e mandatory access control (MAC), mentre i due modelli specifici più noti sono il modello Bell-LaPadula (policy confidenzialità) e il modello Biba (policy integrità).

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Crittografia:
Il termine crittografia indica gli strumenti che permettono di rendere cifrati i messaggi in modo tale che siano comprensibili solo a persone designate (che li possono quindi decrittare o decifrare).
Per cifrare un messaggio occorre un algoritmo crittografico, ossia una funzione matematica, e una chiave crittografica, ossia una variabile. Un messaggio viene cifrato utilizzando l'algoritmo insieme alla chiave; per decifrare il messaggio, il destinatario deve conoscere l'algoritmo e la chiave per decifrarlo.
Il principio di Kerckoff stabilisce che la sicurezza della crittografia non è garantita dalla segretezza dell'algoritmo, ma della chiave;
Conoscendo l'algoritmo, se un malintenzionato intercetta un messaggio cifrato, potrebbe cercare di decifrarlo provando tutte le possibili combinazioni di chiavi (attacco brute force). Ovviamente, più lunga è la chiave utilizzata, più tempo è richiesto all'attaccante per individuarla. La lunghezza della chiave è quindi un parametro molto importante.
Nel 1976 sono stati scoperti algoritmi che permettono agli interlocutori di cifrare con una chiave (la chiave pubblica) e di decifrare con un'altra chiave (la chiave privata): chi vuole inviare un messaggio cifrato ad una persona deve conoscere la sua chiave pubblica e glielo invia: il destinatario sarà l'unico a poter decifrare il messaggio con la propria chiave privata. Questi algoritmi sono detti algoritmi crittografici a chiave pubblica o algoritmi crittografici asimmetrici.
In precedenza, venivano usati solo algoritmi per i quali è necessario usare la medesima chiave per cifrare e decifrare. Questi algoritmi sono detti algoritmi crittografici a chiave privata o algoritmi crittografici simmetrici.
L'insieme degli algoritmi da utilizzare per le diverse finalità e dei requisiti di lunghezza delle chiavi prende il nome di protocollo crittografico.
Alcuni Paesi limitano l'uso della crittografia arrivando a considerarla come arma; ciò non si applica all'Italia.
Più complesso è il tema delle firme digitali. Quando queste sono legalmente riconosciute, anche in sostituzione della firma autografa, devono essere conformi a specifiche normative e standard tecnici, in continua evoluzione. I protocolli richiedono il coinvolgimento di almeno tre entità: l'utente, un'organizzazione che emette il dispositivo di firma (autorità di registrazione) e una che ne attesta la validità (certificatore di firma digitale).

Sicurezza fisica:

- Sicurezza della sede
  - Controllo degli accessi alla sede e ai locali
  - Visitatori
  - Controllo del materiale in uscita
  - Antintrusione e videosorveglianza
  - Aree speciali
- Sicurezza delle apparecchiature
  - Cablaggio
  - Apparecchiature e impianti fuori sede
  - Dismissione delle apparecchiature
  - Schermatura magnetica
  - Impianti
- Archivi fisici

Conduzione dei sistemi informatici:

- Documentazione
- Gestione dei cambiamenti
- Malware

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

- Backup
- Monitoraggio e logging
- Dispositivi portatili e personali

Sicurezza delle comunicazioni:

- Servizi autorizzati
  - Social network
  - Servizi di configurazione
  - Reti wi-fi
  - Accesso alla rete dei visitatori
- Segmentazione della rete
  - Separazione da Internet (firewall)
  - Segmentazione della rete interna
  - Connessioni esterne
  - Segmentazione e privilegi minimi
- Protezione degli apparati di rete
- Scambi di informazioni

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Gestione dei fornitori:
Il ricorso a fornitori è una forma di condivisione del rischio: una parte di esso resta sempre al cliente perché dovrà sostenere parte dei costi e affrontare i danni all'immagine conseguenti ad un incidente.
È possibile distinguere tre tipi di fornitori con impatto sulla sicurezza delle informazioni:

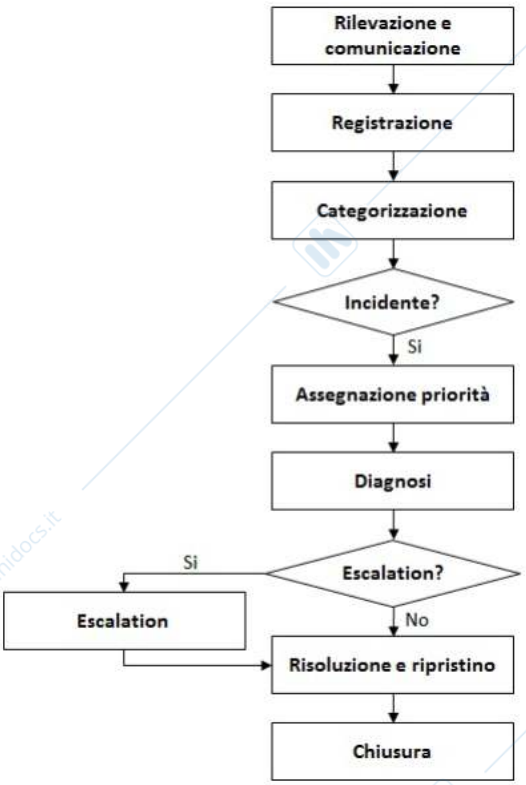
- quelli con accesso diretto alle informazioni
- quelli che svolgono attività necessarie alla sicurezza delle informazioni ma ai quali non è richiesto di accedere alle informazioni
- quelli ai quali non è richiesto di accedere alle informazioni ma possono introdurre dei rischi

Tra cliente e fornitore si stipula sempre un contratto, se appartengono alla stessa organizzazione questo si definisce contratto interno.

Gestione degli incidenti:

1. Processo di gestione degli incidenti

È importante stabilire un processo ben strutturato di gestione degli incidenti affinché siano rilevati e trattati efficientemente ed efficacemente, con eventuali effetti negativi ridotti al minimo, e attuato il piano di gestione della crisi se necessario.



Rilevazione e comunicazione:
La rilevazione riguarda eventi, incidenti e vulnerabilità. Può essere effettuata da: sistemi automatici di monitoraggio, analisi o verifiche manuali da parte degli operatori, segnalazioni da parte del personale, dei clienti o dei fornitori, mezzi di informazione.
È importante stabilire a chi segnalare un incidente o vulnerabilità, affinché venga convenientemente trattato.
Per gli utenti, si consiglia sempre di istituire un unico punto di contatto (SPOC o single point of contact), con un unico numero di telefono e indirizzo e-mail, ad evitare confusioni.
Quando si tratta della gestione di servizi informatici, questo punto di contatto viene chiamato service desk e si occupa di tutte le richieste e segnalazioni degli utenti.

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Registrazione:
Gli eventi devono essere registrati, in modo che sia noto chi li ha segnalati, chi li sta trattando e per conservarne una storia, utile se un caso simile si dovesse ancora verificare e se il trattamento richiede molto tempo e deve essere monitorato. Esistono molti tipi di sistemi di registrazione degli eventi detti sistemi di ticketing.

Categorizzazione:
Consiste in poche analisi, con l'obiettivo di comprendere:

- se la segnalazione riguarda effettivamente un incidente o una vulnerabilità;
- l'impatto attuale o potenziale dell'incidente o della vulnerabilità
- quale funzione tecnica è la più adeguata a trattare l'incidente o la vulnerabilità

Assegnazione delle priorità:
La categorizzazione consente di stabilire la priorità di trattamento: incidenti con impatti elevati hanno la priorità più elevata. Nell'assegnazione della priorità è anche necessario considerare altri parametri, come eventuali scadenze da rispettare o la possibilità che gli impatti dell'incidente possano aumentare rapidamente.

Diagnosi:
Secondo la priorità assegnata, la funzione tecnica coinvolta dal service desk procede ad una diagnosi più approfondita, le prime cose da individuare sono:

- L'ambito di origine dell'incidente, in modo tale da contattare gli esperti
- se incidenti simili si siano già verificati in precedenza

Escalation:
Se la funzione tecnica che ha svolto la diagnosi non può affrontare da sola l'incidente, deve coinvolgere ulteriori strutture, ossia effettuare una escalation. Se coinvolti i fornitori, può essere utilizzato il termine dispatching.
Tutte queste escalation devono essere regolamentate: il service desk inizialmente coinvolge il proprio responsabile che a sua volta, dopo aver valutato gli impatti e gli effetti previsti dell'evento, potrà contattare i livelli gerarchici superiori o il business continuity manager.

Risoluzione e ripristino:
A questo punto, le persone più adeguate a trattare l'incidente sono state coinvolte e provvedono alla sua risoluzione e a documentarla sul sistema di ticketing.

Chiusura:
Prima di chiudere definitivamente un incidente è opportuno verificare dopo qualche tempo l'efficacia della soluzione.

2. Processo di controllo vulnerabilità:

Nessun sistema è immune alle vulnerabilità, ogni segnalazione di vulnerabilità deve essere trattata come segnalazione di incidente.

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

3. Gestione dei problemi:

Nell'ambito dell'informatica, il termine problema è usato per indicare la causa di uno o più incidenti. In altri ambiti si utilizza l'espressione root cause e si dicono azioni correttive o preventive le attività per risolverla. Un'organizzazione deve attivare un processo di gestione dei problemi per prevenire il verificarsi o il ripetersi di incidenti. Infatti, normalmente, quando si chiude un incidente, si usa un workaround, ossia una veloce soluzione temporanea, per poi, con maggiore calma, cercare la causa ultima dell'incidente e risolverla in maniera definitiva.

4. Gestione delle crisi

Il crisis management si occupa degli aspetti strategici conseguenti ad un incidente grave.

5. Digital forensics:

Una definizione di digital forensics, seppure limitata al contesto penale e non civile, è la seguente.
Digital forensics: L'uso di metodi scientifici e provati per preservare, raccogliere, validare, identificare, analizzare, interpretare, documentare e presentare i mezzi di prova digitali derivati da dispositivi digitali, allo scopo di facilitare o portare avanti la ricostruzione di eventi criminali o aiutare ad anticipare azioni non autorizzate.

Continuità operativa:
Business continuity (Continuità operativa): capacità di un'organizzazione di continuare a fornire prodotti o servizi ad un livello accettabile predefinito, dopo un incidente di disturbo.
La business impact analysis (BIA) ha la finalità di individuare i tempi massimi accettabili di interruzione delle attività dell'organizzazione (maximum tolerable period of disruption o MTPD) e delle risorse ad esse collegate (incluse le informazioni).
Obiettivi e strategie di ripristino:
In base alle analisi, chi si occupa della sicurezza delle informazioni si dà degli obiettivi, di cui seguono le definizioni più diffuse accompagnate da alcune considerazioni.

- Recovery time objective (RTO): tempo massimo per ripristinare la disponibilità delle informazioni; deve essere minore o uguale al MTPD dei processi che le utilizzano.
- Recovery point objective (RPO): il punto nel tempo nel quale i dati sono coerenti e devono essere ripristinati;
- Minimum business continuity objective (MBCO): le risorse minime necessarie nella fase di emergenza.

Il termine contingenza locale non è ufficialmente condiviso e riguarda guasti locali. I termini alta affidabilità, alta disponibilità sono utilizzati se le strategie sono tali da garantire una disponibilità dei servizi informatici molto elevata, generalmente del 99,999%.
Hanno tempi di ripristino diversi:

- molto brevi se per le normali attività e per distribuire il carico di lavoro sono usati più sistemi contemporaneamente
- lunghi, se l'hardware è disponibile ma deve essere configurato
- molto lunghi, se si prevede di avere delle copie di backup dei dati e dei programmi software e di acquistare solo in caso di necessità le risorse hardware su cui caricarle.

Il sito di disaster recovery (o sito di DR) è un sito per i sistemi informatici, alternativo a quello primario e può anche essere usato per ospitare copie della documentazione in formato non digitale.

Dopo aver deciso come garantire la continuità dei servizi informatici, la disponibilità delle informazioni e la loro sicurezza, occorre redigere procedure semplici e schematiche, utilizzabili anche da personale poco preparato o in condizioni di tensione, che descrivano cosa fare in caso di incidente con impatti sulla continuità. Queste procedure sono denominate piani di continuità.

This document is available free of charge on studocu

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

Una parte del piano di continuità, detto piano di disaster recovery, riporta le azioni tecniche informatiche da compiere nei siti di disaster recovery.

Conformità:
Ogni organizzazione deve agire in conformità alla normativa vigente, alle procedure interne, ai contratti stipulati con i clienti, a standard nazionali o internazionali adottati volontariamente.
Per verificare la propria conformità a procedure, requisiti o norme, un'organizzazione deve condurre degli audit che possono essere svolti da personale interno o da organizzazioni esterne. Particolare caso di verifiche sono i vulnerability assessment.

- Standard volontari: Tra di essi vi sono gli standard con requisiti relativi ai sistemi di gestione come la ISO/IEC 27001, la ISO 9001, la ISO/IEC 20000-1 e la ISO 22301.
- Normativa sulla criminalità informatica: Codice Penale, D. Lgs. 373 del 2000 e la Legge 48 del 2008 (che regolamenta anche la digital forensics).
- Normativa sul diritto d'autore: Legge 633 del 1941, Codice di Proprietà Industriale, Codice civile in materia di brevetti.
- Responsabilità amministrativa delle imprese: Il Decreto Legislativo 231 del 2001, Le misure nel loro complesso sono indicate come modello organizzativo 231.
- Normativa sul commercio elettronico: La normativa applicabile al commercio elettronico (e-commerce) è riportata dai D. Lgs. 70 del 2003, D. Lgs. 206 del 2005 (Codice del consumo) e D. Lgs. 69 del 2012. La Direttiva Europea 2011/83 sui diritti dei consumatori ha introdotto ulteriori modifiche nell'ordinamento italiano.
- Codice dell'amministrazione digitale: Il riferimento principale è il D. Lgs. 82 del 2005
- Regolamento eIDAS: Nel 2014 è stato approvato il Regolamento UE 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari. Questo regolamento è in vigore dal 2016.
- Normativa sui dati personali: Il riferimento principale in materia di trattamento dei dati personali in Italia è il Regolamento europeo 2016/679 (detto General data protection regulation o GDPR). Alcune specifiche italiane sono oggetto del D. Lgs. 196 del 2003, aggiornato con il D. Lgs. 101 del 2018 a seguito dell'entrata in vigore del GDPR.
  La normativa distingue tra dati personali, dati personali appartenenti a categorie particolari (in precedenza dati personali sensibili) e dati personali relativi a condanne penali e reati (dati personali giudiziari). Per una migliore interpretazione del GDPR, sono da considerare le opinioni dell'European Data Protection Board o EDPB98. In Italia hanno inoltre valore le linee guida, le autorizzazioni e i provvedimenti generali del Garante per la protezione dei dati personali (Garante privacy), in particolare quelli sulla gestione degli Amministratori di sistema e sulla videosorveglianza.
  Il GDPR richiede che l'organizzazione attui misure di sicurezza "adeguate", considerando i rischi. Va quindi condotta una valutazione del rischio relativo alla privacy, che potrebbe essere integrata con quella relativa alla sicurezza delle informazioni.
  Una misura importante riguarda l'obbligo di comunicare violazioni ai dati personali al Garante e, nei casi in cui l'impatto potrebbe essere elevato per i diritti e le libertà delle persone fisiche, agli interessati. Un'altra riguarda il diritto all'oblio.

Audit:
Processo sistematico, indipendente e documentato volto all'ottenimento di prove, al fine di valutarle per determinare quanto i criteri di audit sono soddisfatti.

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

I criteri di audit sono l'insieme di politiche, procedure e requisiti su cui basare l'audit. È necessario definire i tre tipi di audit e i relativi criteri:

- interni o di prima parte: sono svolti dall'organizzazione stessa (con personale interno o esterno) e i criteri di audit sono le procedure interne;
- esterni o di seconda parte: sono svolti da una parte interessata(solitamente un cliente) presso un'organizzazione (solitamente un proprio fornitore) e i criteri di audit sono gli accordi o i contratti tra le parti;
- di certificazione o di terza parte: sono svolti da organismi indipendenti e i criteri di audit sono gli standard concordati dall'organizzazione con l'organismo di certificazione.

Il termine audit differisce da quello di assessment perché l'audit è orientato a verificare se sono soddisfatti requisiti completamente stabiliti a priori, mentre l'assessment può fare riferimento a requisiti non completamente predeterminati.

Vulnerability assessment:
Il vulnerability assessment consiste nell'analisi dei sistemi informatici e nella ricerca e valutazione di possibili vulnerabilità.
I vulnerability assessment possono essere condotti in diverse modalità: si può simulare un attaccante con conoscenza dei sistemi (white box) o senza alcuna conoscenza (black box);
può essere condotto da personale dell'organizzazione o da esterni (normalmente detti ethical hacker o white hat).
L'attività complessiva di identificazione e valutazione delle vulnerabilità è quindi suddivisa in due parti: una teorica (il vulnerability assessment) e una sperimentale (il penetration test).

- Vulnerability assessment (VA): attività volta a determinare l'esistenza e la possibilità di sfruttare security flaws e debolezze dell'oggetto sottoposto a valutazione nel suo ambiente operativo (simulato);
- Penetration test (PT): tecnica di test volta a determinare se le potenziali vulnerabilità identificate sono effettivamente sfruttabili nell'ambiente operativo in cui opera l'oggetto sottoposto a valutazione.

I requisiti di un sistema di gestione per la sicurezza delle informazioni:
Specifiche e linee guida:
si distingue tra diversi tipi di norme:

- Standard verificabili: norme con specifiche rispetto alle quali può essere condotto un audit da parte di personale indipendente; si DEVE fare
- Linee guida: manuali o raccolte di best practice disponibili per una loro selezione al fine di raggiungere un certo obiettivo; si PUO' fare, DOVREBBE, POTREBBE.

Le norme spesso nascono dalle cosiddette best practice.

Le norme della famiglia ISO 27000
La ISO/IEC 27001 è uno standard verificabile; Possono essere condotti audit di un sistema di gestione per la sicurezza delle informazioni di un'organizzazione e, se questo è ritenuto conforme ai requisiti della ISO/IEC 27001, può essere emesso un certificato di conformità.
La ISO/IEC 27001 è affiancata da altre linee guida che forniscono supporto all'attuazione dei suoi requisiti o delle indicazioni per la sua applicazione in settori specifici. L'insieme di queste norme è detto famiglia delle norme ISO/IEC 27000 (ISMS standard family o famiglia di norme dei SGSI) e ne fanno parte:

- ISO/IEC 27002, guida per la scelta dei controlli di sicurezza; non è possibile dichiarare una conformità rispetto ad essa, ma alcune organizzazioni lo fanno e dimostrano quanto poco conoscano questo standard;
- ISO/IEC 27003, guida all'interpretazione dei requisiti della ISO/IEC 27001;

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

- ISO/IEC 27004, guida per la misurazione e il monitoraggio di un sistema di gestione per la sicurezza delle informazioni;
- ISO/IEC 27005, guida per la valutazione e gestione del rischio relativo alla sicurezza delle informazioni (purtroppo, anche per questo alcuni chiedono la certificazione o attestati di conformità).

Altre norme della famiglia sono quelle che estendono i controlli della ISO/IEC 27001:

- ISO/IEC 27011 con controlli di sicurezza attuabili dai fornitori di servizi di telecomunicazione;
- ISO/IEC 27017 con controlli di sicurezza attuabili dai fornitori e dagli utilizzatori di servizi cloud;
- ISO/IEC 27018 con controlli privacy attuabili dai fornitori di servizi cloud;
- ISO/IEC 27019 con controlli di sicurezza attuabili nel settore dell'energia;
- ISO 27799 con controlli di sicurezza attuabili nel settore della sanità;
- ISO/IEC 29151 per i titolari dei trattamenti di dati personali.
- ISO/IEC 27552 riguarda infine la certificazione del sistema di gestione per la protezione dei dati personali, ispirato al Regolamento europeo sulla protezione dei dati personali (GDPR).

L'HLS (High level structure) contiene il testo di base da adottare per ciascun standard sui sistemi di gestione.

Come funziona la normazione:
La ISO/IEC 27001 è scritta da un gruppo di lavoro che fa riferimento alla ISO e alla IEC. La ISO (International organization for standardization) si occupa della standardizzazione in tutti i settori, mentre la IEC (International electrotechnical committee) è specializzata nell'ambito elettrotecnico. Fanno parte della ISO e della IEC gli Organismi nazionali (National bodies), uno per ciascuna nazione rappresentata.
Ogni norma passa diversi stadi: working draft (WD), committee draft (CD), draft of international standard (DIS), final draft of international standard (FDIS) e può essere pubblicata come International standard (IS), Technical specification (TS) o Technical report (TR) a seconda del consenso necessario per la sua approvazione. La ISO/IEC 27001 è un International Standard ed è stato approvato da almeno il 75% degli organismi nazionali aventi diritto.
In Italia, gli organismi nazionali corrispondenti all'ISO e all'IEC sono l'UNI (Ente nazionale per l'uniformazione) e la CEI (Comitato elettrotecnico italiano).

Le norme ISO sui sistemi di gestione, tra cui quindi la ISO/IEC 27001, impongono alle organizzazioni che li adottano il miglioramento continuo. Lo strumento per eseguire questo miglioramento è il processo PDCA (Plan-Do-Check-Act).
Il ciclo PDCA non è un metodo per gestire i cambiamenti, ma uno schema per identificarli e tenerli sotto controllo.
Il ciclo PDCA o Plan-Do-Check-Act è uno strumento per conseguire il miglioramento e si può applicare a tutte le organizzazioni, processi e attività. È noto come ciclo di Deming, dal nome della persona che lo ha reso noto e popolare prima in Giappone e poi nel mondo.

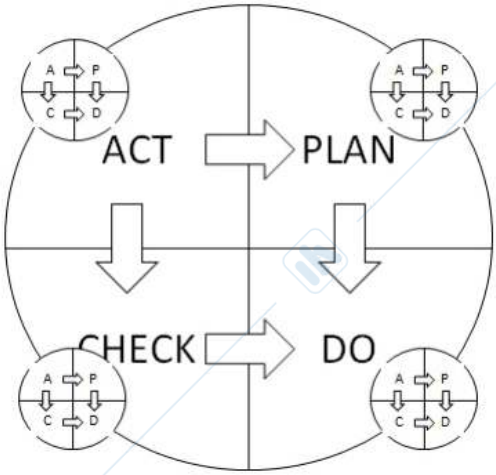
1. pianificare (plan): individuare le attività, i processi e gli strumenti da utilizzare per conseguire i risultati previsti;
    - a livello strategico si pianificano le attività a lungo termine e le caratteristiche generali dei prodotti e dei processi;
    - a livello tattico si pianificano i miglioramenti di dettaglio dei processi;
    - a livello operativo si pianificano le attività quotidiane necessarie alla produzione o all'erogazione dei servizi.

2. realizzare (do) quanto pianificato;
3. verificare (check) quanto realizzato rispetto a quanto pianificato; si verifica l'efficacia di quanto fatto.
4. intervenire (act) se a fronte delle verifiche si individuano carenze.

La natura frattale del ciclo PDCA:
Ognuna delle quattro fasi del ciclo PDCA deve essere a sua volta oggetto di un ciclo PDCA

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari



Accanto ad essa bisogna considerare la natura "frattale gerarchica" del ciclo PDCA lungo i livelli della piramide di Anthony: l'attuazione (Do) di una strategia richiede di pianificare (Plan) la modifica dei processi a livello tattico, la cui attuazione (Do) richiede di pianificare (Plan) quanto necessario a livello operativo.

I requisiti di sistema:
Il primo capitolo della ISO/IEC 27001, dopo un'introduzione, chiarisce che i requisiti dello standard sono applicabili a tutte le organizzazioni. Inoltre, per potersi dichiarare conformi allo standard e certificarsi rispetto ad esso, è necessario soddisfare tutti i requisiti esposti.
La ISO/IEC 27000 riporta le definizioni dei termini tecnici utilizzati dalle norme della famiglia ISO/IEC 27000.

La norma richiede di identificare il contesto dell'organizzazione, ossia:

- i fattori interni ed esterni
- le parti interessate e le loro aspettative, peraltro esse stesse fattori interni ed esterni.

La norma non richiede di documentare il contesto, ma andrebbe fatto.
Dal contesto è possibile stabilire l'ambito del sistema di gestione per la sicurezza delle informazioni: ricordando che esso può essere tutta l'organizzazione o parte di essa.
L'ambito deve essere descritto in un documento riportando quanto è necessario per capire: a cosa si applicano i requisiti e i controlli di sicurezza della ISO/IEC 27001, a cosa si riferisce la valutazione del rischio, quali sono le informazioni da proteggere e gli strumenti che le trattano.
Leadership:
La ISO/IEC 27001, anche sulla base di quanto previsto dall'HLS, utilizza il termine leadership, per sottolineare il ruolo della Direzione: non solo di appoggio, ma anche di esempio e guida.
Importante è la politica per la gestione delle informazioni: la politica deve essere documentata, comunicata all'interno dell'organizzazione e, per quanto appropriato, disponibile alle parti interessate.

Il capitolo 6 dello standard riguarda la pianificazione del sistema di gestione per la sicurezza delle informazioni da un punto di vista strategico e tattico. È quindi opportuno distinguere tra diversi tipi di pianificazione, facendo riferimento alla piramide di Anthony:

- pianificazione strategica: comprende le scelte generali relative al sistema di gestione, la preparazione e pubblicazione della politica per la sicurezza delle informazioni, la scelta degli obiettivi strategici, l'individuazione dei processi e dei controlli del sistema di gestione, le loro caratteristiche generali e le loro relazioni
- pianificazione tattica: stabilisce i dettagli dei processi e dei controlli di sicurezza da attuare, i loro obiettivi, le risorse necessarie per realizzare quanto pianificato, le attività che compongono i processi e la loro frequenza o scadenza

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

- pianificazione operativa: stabilisce esattamente quando effettuare le attività. Un ulteriore requisito riportato nell'ambito delle attività operative, più pertinente alla pianificazione del sistema di gestione, richiede di individuare, determinare e tenere sotto controllo i processi affidati all'esterno. Tra questi vi sono quelli affidati ai fornitori e agli outsourcer

I rischi, originati dai fattori interni ed esterni che compongono il contesto dell'organizzazione, devono essere identificati e valutati dall'organizzazione per decidere come impostare o migliorare il proprio sistema di gestione per la sicurezza delle informazioni.
La norma richiede di pianificare delle azioni per affrontare i rischi relativi al sistema di gestione e sottolinea la necessità di integrare gli elementi del sistema di gestione per la sicurezza delle informazioni nei processi e nelle attività dell'organizzazione.

Nella ISO/IEC 27001 i requisiti sulla valutazione del rischio relativo alla sicurezza delle informazioni sono riportati nel capitolo 6, dedicato alla pianificazione del sistema di gestione. Questo perché la valutazione dei rischi relativi alla sicurezza delle informazioni serve a stabilire e pianificare i requisiti dei processi del sistema di gestione.
La norma richiede di documentare in una procedura il processo di valutazione del rischio adottato. Tale processo deve essere composto dalle fasi di identificazione, analisi e ponderazione.
La norma richiede di stabilire i criteri da seguire per ripetere la valutazione del rischio, Si raccomanda di rivalutare completamente il rischio almeno una volta all'anno per collegare il piano di trattamento al processo di budgeting e al riesame di Direzione.

La norma richiede di documentare in una procedura, anche la stessa in cui è descritto il processo di valutazione del rischio, il processo di trattamento del rischio. Questo processo deve prevedere come input i risultati della valutazione del rischio (fine risk assessment) e come output la scelta delle opzioni di trattamento per ciascun rischio, dei controlli per attuarle, da descrivere nel piano di trattamento del rischio. I responsabili del rischio, infine, devono approvare le opzioni scelte e le azioni di trattamento proposte.

La norma richiede di preparare un documento in cui riportare un elenco esaustivo di controlli di sicurezza e, per ognuno di essi, indicare se è attuato o meno nell'ambito del sistema di gestione, insieme alle motivazioni della scelta o dell'esclusione.
I 114 controlli di sicurezza dell'Appendice A della norma stessa è ritenuto un elenco "esaustivo" e pertanto quasi tutti usano quello. È comunque necessario indicare quali controlli dell'Appendice A della ISO/IEC 27001 sono esclusi e la giustificazione per questa scelta.
Questo documento è denominato Dichiarazione di applicabilità in italiano o Statement of Applicability (SoA) in inglese.

La ISO/IEC 27001 non fornisce esplicitamente requisiti relativi alle azioni, malgrado richieda di pianificarle per trattare i rischi, acquisire le competenze necessarie, mitigare effetti indesiderati dei cambiamenti, correggere le non conformità e prevenire il ripetersi di non conformità. Non esiste quindi un paragrafo dedicato alle azioni, ma ad ogni azione deve essere collegato almeno un obiettivo (in caso contrario non si avrebbe la necessità di agire), per il quale devono essere soddisfatti dei requisiti precisi.
Quindi per ogni azione bisogna pianificare: le risorse necessarie, le persone responsabili dell'azione, le scadenze e le modalità con cui ne verrà valutata l'efficacia. Devono essere inoltre indicate le minacce o le opportunità per cui si è stabilita l'azione.
La valutazione dell'efficacia di un'azione prevede di analizzare se è stata realizzata come pianificato e ha raggiunto i risultati previsti. L'efficacia non dovrebbe essere valutata al completamento dell'azione ma, se possibile, ad intervalli pianificati durante le fasi di Plan e Do oppure dopo qualche tempo dal suo completamento, per poterne verificare i benefici o gli eventuali effetti indesiderati.

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

È opportuno, anche se non richiesto dallo standard, creare un registro delle azioni di miglioramento, dove descrivere le azioni in fase di pianificazione e in corso. Questo permetterebbe di tenere informate tutte le parti interessate.

Obiettivi:
Tutti gli obiettivi devono seguire il principio cosiddetto SMART, ossia:

- Specifici: riguardare un ambito preciso ed essere coerenti con la politica di sicurezza delle informazioni;
- Misurabili
- Raggiungibili (Achievable): l'organizzazione e le risorse assegnate sono tali da permetterne il conseguimento;
- Pertinenti (Relevant): applicabili all'ambito di lavoro della persona o funzione o processo a cui sono assegnati;
- Con scadenza (Time-bound): relativi ad un periodo di tempo specificato.

La norma richiede di stabilire gli obiettivi relativi alla sicurezza delle informazioni ai diversi livelli funzionali, di documentarli, di comunicarli alle parti interessate secondo necessità e aggiornarli come appropriato.
Le norme ISO richiedono di fissare obiettivi e tenerli sotto controllo ed esplicitamente alla Direzione di fornire supporto e risorse e adeguarli in base al contesto.

Processi di supporto:
I processi di supporto richiesti dallo standard sono quelli di gestione delle risorse, delle competenze, della consapevolezza, della comunicazione e dei documenti.

Processo di supporto: gestione risorse
Il requisito relativo alle risorse si riduce alla richiesta di garantire le risorse necessarie per soddisfare l'obiettivo di stabilire, attuare, mantenere e migliorare il sistema di gestione per la sicurezza delle informazioni. Questo requisito deve essere attuato seguendo un ciclo PDCA: stabilire quali sono le risorse necessarie, reperirle, monitorarne l'adeguatezza e intervenire quando sono insufficienti.

Processo di supporto: competenze e consapevolezza
La norma richiede di:

- documentare le competenze necessarie per garantire l'efficacia del sistema di gestione per la sicurezza delle informazioni;
- documentare le competenze in possesso delle persone impiegate dall'organizzazione, inclusi eventuali consulenti, considerando l'istruzione, la formazione, l'addestramento e l'esperienza.
- Pianificare e realizzare azioni per disporre delle competenze mancanti (corsi di formazione, affiancamenti, assunzioni o inserimento di consulenti);
- valutare l'efficacia delle azioni intraprese

Bisogna sensibilizzare il personale dell'organizzazione alla conoscenza della politica di sicurezza delle informazioni e alla sua importanza.

Processo di supporto: comunicazione
La norma richiede di individuare quando è necessario comunicare verso l'interno o verso l'esterno e di stabilire, per ogni tipo di comunicazione:

- cosa comunicare;

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

- quando comunicare;
- chi deve comunicare;
- chi sono gli interlocutori interni ed esterni all'organizzazione con cui comunicare.

Valutazione delle prestazioni:
La norma richiede di valutare le prestazioni della sicurezza delle informazioni e l'efficacia del sistema di gestione per la sicurezza delle informazioni mediante monitoraggi e misurazioni relativi a processi e controlli di sicurezza.

La norma richiede di garantire:

- la ripetibilità delle misurazioni: in condizioni uguali, i risultati delle misurazioni devono essere uguali;
- la comparabilità delle misurazioni: misurazioni condotte in momenti diversi devono permettere una valutazione di tendenze o cambiamenti.

Anche il processo relativo ai monitoraggi è eseguito con il processo PDCA.
La ISO/IEC 27001 richiede di documentare i monitoraggi e le misurazioni, conservando, per un tempo adeguato, le presentazioni dei risultati e le loro valutazioni.

Gli audit interni dovrebbero essere condotti secondo quanto previsto dalla norma ISO 19011. La prima cosa da fare è predisporre un programma di audit, individuando le aree da sottoporre ad audit.
Una volta stabilite le aree da verificare, deve essere inviato un piano di dettaglio alle persone da coinvolgere o al loro responsabile.

Riesame di direzione:
Il riesame di direzione è un'attività tra le più importanti per un sistema di gestione, dovrebbe presentare una previsione di spesa per la sicurezza delle informazioni e quindi dovrebbe costituire parte del budget annuale complessivo dell'organizzazione.
Più nel dettaglio, la norma richiede di analizzare:

- lo stato di avanzamento dei progetti e delle azioni stabilite nel riesame precedente
- i fattori interni ed esterni del contesto cambiati rispetto al riesame precedente
- le non conformità emerse dal riesame precedente e le azioni correttive avviate nello stesso periodo
- i risultati dei monitoraggi e delle misurazioni
- i risultati degli audit interni o condotti da parti esterne
- lo stato di completamento degli obiettivi di sicurezza delle informazioni;
- le segnalazioni dalle parti interessate
- i risultati della valutazione del rischio e lo stato del piano di trattamento del rischio relativo alla sicurezza delle informazioni;
- le opportunità di miglioramento

Miglioramento:
Il capitolo 10 dello standard è dedicato al miglioramento e si occupa delle non conformità, delle azioni correttive e del miglioramento continuo.

Non conformità:
Un requisito non completamente soddisfatto è pertanto una non conformità.

- mancato rispetto delle procedure e della ISO/IEC 27001, spesso rilevate durante un audit (non conformità di processo);

Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari

- prodotti e servizi non realizzati come previsto o progetti che non rispettano la pianificazione o gli obiettivi prefissati (non conformità di produzione o progettazione);
- prodotti e servizi consegnati ai clienti non in linea con quanto concordato (reclami e segnalazioni dei clienti);
- prodotti e servizi consegnati dai fornitori non in linea con quanto concordato (non conformità di fornitura).

La norma richiede di reagire alle non conformità e, se applicabile, eliminarle con una correzione e affrontarne le conseguenze. L'organizzazione deve anche valutare se intraprendere delle azioni correttive per evitare che la non conformità si ripeta.
Un'azione preventiva riguarda non conformità non ancora manifestate, ma potenziali.
È opportuno sottolineare la differenza tra azioni correttive e preventive: le prime sono finalizzate alla prevenzione del ripetersi di una non conformità, le seconde alla prevenzione del loro manifestarsi.

La norma si conclude con un breve paragrafo: "L'organizzazione deve migliorare continuamente l'idoneità, l'adeguatezza e l'efficacia del sistema di gestione per la sicurezza delle informazioni".

L'appendice A della norma ISO 27001:
L'Appendice A della ISO/IEC 27001 riporta 114 controlli di sicurezza a cui fare riferimento quando si realizza un sistema di gestione per la sicurezza delle informazioni.
chi intende certificarsi rispetto alla norma ISO/IEC 27001 deve compilare una Dichiarazione di applicabilità, ossia un'analisi dei controlli attuati. Solitamente questa analisi si basa sui controlli dell'Appendice A. Nel caso in cui alcuni controlli dell'Appendice A non siano attuati, la Dichiarazione di applicabilità deve riportarne la giustificazione.

This document is available free of charge on studocu
Scaricato da Stefano Giardina (giardina.stefano98@gmail.com)
www.unidocs.it - Appunti e dispense per superare i tuoi esami universitari