Standard per la gestione della sicurezza ISO/IEC 27001/27002

Indice

- Introduzione
- ISO/IEC-27001
- Ciclo di Deming
- Rischio e valutazione dei costi di un incidente informatico
- ISO/IEC-27002
- Conclusioni

Introduzione: La serie ISO/IEC 27000

ISO/IEC 27001

- specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni (ISMS).
- Si basa su un approccio risk-based: *identificazione-analisi-valutazione-trattamento-revisione*

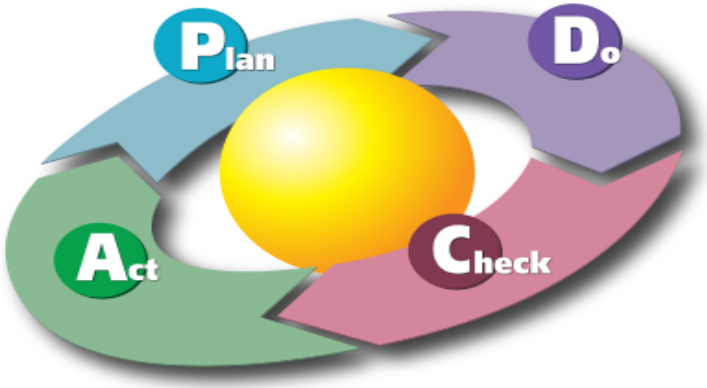
ISO/IEC 27002

- E' uno standard operativo*
- Identifica i *controlli* nell'ambito del processo di implementazione di un sistema di gestione della sicurezza delle informazioni basato su ISO/IEC 27001
- Supporta lo sviluppo di proprie linee guida per la gestione della sicurezza delle informazioni.

***per tale motivo la presentazione si concentra principalmente su questo standard**

ISO/IEC 27001

- Il modello di un ISMS è basato sul ciclo di Deming PDCA: *Plan Do Check Act*



PDCA in un ISMS: Plan

- Politiche di alto livello
- Definizione dell'approccio da usare per la gestione del rischio
- Identificazione del rischio
- Valutazione del rischio (viene prodotto un rapporto di Risk Assessment)
- Gestione del rischio (riduzione, trasferimento)
- Identificazione dei controlli
- Redazione di un SOA (Statement of Applicability) che dimostri l'idoneità e la compliance con ISO/IEC 27002 dei controlli scelti

PDCA in un ISMS: Do

In contesti limitati dell’organizzazione

- Implementazione del piano di gestione del rischio
- Implementazione dei controlli
- Comunicazione e piani di formazione
- Gestionde di task e delle risorse
- Procedure per l’incident response

PDCA in un ISMS: Check

- 1. Monitoring
- 2. Revisione del rischio residuo (verifica dell'efficacia dell'ISMS)
- Esecuzione di AUDIT (interni ed esterni)
- Azioni di revisione al livello del top-management
- Registrazione di ogni evento rilevante per l'ISMS

PDCA in un ISMS: Act

Implementazione finale

- Implementazione delle correzioni e check
- Notifica dei risultati alle parti appropriate
- Estensione a tutta l'organizzazione

Il concetto basilare di Rischio

- **Rischio: R = G x P**
- La quantificazione del rischio è un task complesso.
- Il framework FAIR (Factor analysis of information risk)è una metodologia usata per la risk quantification

Costi tangibili legati ad un incidente informatico

- perdite di materiale (danno fisico);
- perdite dovute alla non disponibilità delle informazioni;
- perdite dovute alla clientela che nel frattempo si rivolge ai concorrenti;
- perdita di produttività del personale (non IT) che si trova a lavorare in condizioni degradate durante le operazioni di ripristino;
- lavoro e materiali per il rilevamento, il contenimento, la riparazione e la ricostruzione dei danni ai dati;

Costi tangibili legati ad un incidente informatico

- lavoro per la corretta raccolta dei dati
- preparazione delle comunicazioni in relazione all'accaduto (per esempio comunicati stampa, posizione nei confronti della clientela e così via);
- difesa legale qualora possa essere ravvisata una qualsiasi responsabilità dell'azienda relativa alle conseguenze di quanto accaduto;
- eventuali aumenti del premio assicurativo.

Costi intangibili legati ad un incidente informatico

- perdite per svantaggio competitivo;
- perdita di fiducia dei clienti;
- Peggioramento della propria posizione di mercato, in seguito a cattiva pubblicità;
- accesso dei concorrenti a informazioni confidenziali o riservate.

Risk Management

- Parte del rischio può essere ceduto a soggetti esterni (assicurazioni, outsourcing)
- Hosting e Housing sono possibili soluzioni convenienti principalmente per le piccole organizzazioni (non sempre attuabile nel caso di PA)
- Per controllare il rischio si deve operare operare mediante controlli su impatto e probabilità.

ISO/IEC 27002: 2013

- 14 clausole (aree) di controlli di sicurezza
- Ogni clausola contiene una o più categorie di controlli di sicurezza (per un totale di 35 categorie)
- Ogni categoria contiene un insieme di controlli per un totale di 114 controlli.

1. Politiche di sicurezza

- 1. Le politiche devono fornire indicazioni di direzione e supporto per la sicurezza delle informazioni in conformità con requisiti dell'organizzazione, leggi e regolamenti pertinenti
  - Politiche di alto e basso livello
  - Le politiche dovrebbero essere riviste con cadenza pianificata o in caso di cambiamenti significativi, allo scopo di garantirne continua idoneità, adeguatezza ed efficacia.

2. Organizzazione della sicurezza

- 2. Organizzazione Interna della sicurezza:
  - Ruoli e Responsabilità
  - Separazione dei compiti

- 3. Sicurezza dei dispositivi portatili e accessi da remoto (telelavoro).

3. Risorse Umane

- 4. Azioni precedenti all'assunzione
- 5. Azioni applicabili al personale in servizio
- 6. Azioni relative al termine dell'impiego o al trasferimento presso altra organizzazione

4. Asset Management

- 7. Responsabilità degli asset
- 8. Classificazione dell’informazione
- 9. Gestione degli apparti di memorizzazione

5. Controllo dell’Accesso

- 10. Requisiti funzionali per il controllo dell’accesso
- 11. Gestione degli utenti e delle autorizzazioni
- 12. Accountability
- 13. Controllo dell’accesso ad applicazioni e sistemi operativi

6. Crittografia

- 14. Politiche ed utilizzo dei controlli crittografici
  - Gestione delle chiavi e dei certificati di firma e autenticazione
  - Procedure in caso di perdita delle chiavi

7. Sicurezza Fisica

- 15. Gestione della protezione delle aree critiche
- 16. Gestione della protezione delle attrezzature

8. Sicurezza delle operazioni

- 17. Procedure operazionali e responsabilità
- 18. Protezione dal malware
- 19. Backup
- 20. Logging e monitoring
- 21. Controllo del Software
- 22. Gestione delle vulnerabilità tecniche
- 23. Audit del sistema informativo

9. Sicurezza delle Comunicazioni

- 23. Gestione della sicurezza della rete
- 24. Trasferimento dell’informazione

10. Acquisizione dei sistemi, sviluppo e manutenzione

- 25. Requisiti di sicurezza del sistema informativo
- 26. Sicurezza nei processi di sviluppo e supporto
- 27. Protezione dei dati usati per gli ambienti di test

11. Relazione con i fornitori

- 28. Protezione degli asset a cui accedono i fornitori
- 29. Gestione delle forniture relativamente ai livelli di servizio e di sicurezza concordati

12. Gestione degli incidenti

- 30. Garantire un approccio efficace alla gestione degli incidenti di sicurezza, inclusa la comunicazione su eventi di sicurezza.

  - Compliance con ISO/IEC 27035 (Information security incident management) – verrà trattato successivamente

13. Aspetti di sicurezza della gestione della Business Continuity

- 32. Continuità dei servizi di sicurezza
- 33. Ridondanza

14. Compliance

- 34. Conformità ai requisiti legali e contrattuali

- 35. Aderenza alle policy e alle procedure

Conclusioni: vantaggi derivanti dall'adozione degli standard ISO-27000

- Vantaggi organizzativi
- Vantaggi legali (osservanza di leggi)
- Vantaggi operazionali (qualità di dati, servizi e hardware)
- Vantaggi finanziari (analisi dei costi migliorata)
- Vantaggi relativi alle risorse umane (migliore organizzazione di ruoli e awareness)

Approfondimento 1: rischio

G: gravità dell'impatto

P: probabilità dell'evento

- Esempio: supponiamo che un'intrusione comporti un danno di
  - Impact: 50.000 Euro
  - E che la probabilità di questo evento (in un anno) sia 0.2
  - Il rischio è R = 50.000 x 0.2= 10.000 Euro
  - Supponiamo che il costo della protezione sia 1000 Euro e che questa protezione abbassi la probabilità dell'evento a 0.1
  - Il rischio dopo la protezione sarà: R= 50.000 X 0.1 = 5.000
  - Il valore della protezione è quindi: 10.000-5.000-1.000= 4.000 Euro (ovviamente deve essere positiva>0)

Approfondimento 2: Politiche di sicurezza

- **Politiche per la sicurezza delle informazioni**
  - Deve essere definito un insieme di politiche per la sicurezza delle informazioni, approvato dal management, pubblicato e comunicato ai dipendenti e alle parti esterne pertinenti. Se le politiche di sicurezza sono divulgate al di fuori dell'organizzazione, **è necessario prestare attenzione non divulgare informazioni riservate**.
  - **Politiche di alto livello**: Devono riguardare a) strategia aziendale; b) regolamenti, legislazione e contratti; c) la minaccia cyber. Le politica di sicurezza dovrebbero contenere dichiarazioni riguardanti: a) definizione della sicurezza delle informazioni, obiettivi e principi per guidare tutte le attività relative alle informazioni di sicurezza; b) assegnazione di responsabilità generali e specifiche per la gestione della sicurezza delle informazioni a ruoli definiti; c) processi per la gestione di deviazioni ed eccezioni.
  - **Politiche di basso livello**: A un livello inferiore, le politica di sicurezza di fatto impongono controlli di sicurezza e sono progettate per rispondere a specifici obietti. Quindi sono politiche legate alle altre clausole (es. politiche di controllo dell'accesso, politiche per la crittografia, politiche per l'asset management, etc.
- **Revisione delle politiche**
  - Ogni politica dovrebbe avere un proprietario che abbia la responsabilità per lo sviluppo, la revisione e la valutazione della politica. La revisione dovrebbe includere la valutazione di opportunità di miglioramento in risposta alle modifiche dell'ambiente organizzativo, delle circostanze, delle condizioni legali e dell'ambiente tecnico.

Approfondimento 3: responsabilità

- L'assegnazione delle responsabilità in materia di sicurezza delle informazioni dovrebbe essere effettuata conformemente alle politiche di sicurezza. Devono essere identificate responsabilità per la protezione dei singoli beni e per la implementazione dei processi e delle procedure di sicurezza. Devono essere identificate le responsabilità per le attività di gestione del rischio e per l'accettazione dei rischi residui.
- Le responsabilità devono essere separate più possibile (**segregation of duties**) per ridurre le possibilità di modifiche non autorizzate per errore o per uso improprio degli asset dell'organizzazione.
- Le organizzazioni dovrebbero disporre di procedure che specifichino quando e da chi devono essere contattate organismi e autorità esterne in occasione di incidenti di sicurezza (es. Garante della Privacy).
- Simili responsabilità devono essere assegnate per mantenere appropriati contatti con gruppi di interesse speciali o altri forum di sicurezza specializzati e associazioni di professionisti.
- La sicurezza delle informazioni dovrebbe essere affrontata nella gestione dei progetti, indipendentemente dal tipo di progetto.

Approfondimento 4: dispositivi mobili

- Quando si utilizzano dispositivi mobili, è necessario prestare particolare attenzione per garantire che le informazioni dell'organizzazione non siano compromesse. La politica sui dispositivi mobili dovrebbe tenere conto dei rischi derivanti dal fatto che essi potrebbero operare in ambienti non protetti.
- La politica del dispositivo mobile dovrebbe considerare: a) registrazione di dispositivi mobili; b) requisiti di protezione fisica; c) limitazione dell'installazione del software; d) requisiti per le versioni del software del dispositivo mobile e per l'applicazione di patch; e) limitazione della connessione ai servizi di informazione; f) controllo dell'accesso; g) tecniche crittografiche; h) protezione da malware; i) disabilitazione, cancellazione o blocco a distanza; j) backup; k) utilizzo di servizi web e app web. I dispositivi mobili dovrebbero inoltre essere protetti fisicamente dal furto, soprattutto se lasciati, ad esempio, nelle automobili e altri mezzi di trasporto, camere d'albergo, centri congressi e luoghi di incontro. Deve esistere una procedura specifica che tenga conto dei requisiti legali, assicurativi e di sicurezza dell'organizzazione per i casi di furto o smarrimento di dispositivi mobili.
- Laddove la politica sui dispositivi mobili consenta l'uso di dispositivi mobili di proprietà privata, la politica e le relative le misure di sicurezza dovrebbero anche considerare: a) separazione dell'uso privato e commerciale dei dispositivi, compreso l'uso di software a supporto tale da separare e proteggere i dati dell'organizzazione; b) fornire accesso alle informazioni commerciali solo dopo che gli utenti hanno firmato un accordo per l'utente finale riconoscendo i loro doveri (protezione fisica, aggiornamento del software, ecc.), rinunciando alla proprietà di dati dell'organizzazione, che consente la cancellazione remota dei dati da parte dell'organizzazione in caso di furto o smarrimento del dispositivo o quando il dipendente non è più autorizzato a utilizzare il servizio.

Approfondimento 5: telelavoro

- Le organizzazioni che consentono attività di telelavoro dovrebbero emettere una politica che definisce le condizioni e le restrizioni per l'utilizzo del telelavoro. Laddove ritenuto applicabile e consentito dalla legge, devono essere considerati i seguenti aspetti:
  - a) la sicurezza fisica esistente sul sito di telelavoro
  - b) l'ambiente di telelavoro fisico proposto;
  - c) i requisiti di sicurezza delle comunicazioni, tenendo conto della necessità di un accesso remoto a sistemi interni dell'organizzazione
  - d) la fornitura di accesso a desktop virtuale che impedisca l'elaborazione e la memorizzazione delle informazioni su attrezzature di proprietà privata;
  - e) la minaccia di accesso non autorizzato a informazioni o risorse da parte di altre persone che utilizzano lo stesso luogo, ad es. famiglia e amici;
  - f) l'uso di reti domestiche e i requisiti o le restrizioni sulla configurazione della rete wireless e dei servizi di rete;
  - g) politiche e procedure per prevenire controversie relative ai diritti di proprietà intellettuale relativi a sviluppo su attrezzature di proprietà privata;
  - h) accesso alle apparecchiature di proprietà privata (per verificare la sicurezza della macchina o durante un'indagine), in relazione alla legislazione esistente;
  - i) accordi di licenza software tali da consentire alle organizzazioni di essere responsabili per la licenza software client su workstation di proprietà privata di dipendenti o utenti esterni;
  - j) requisiti di protezione da malware e firewall.

Approfondimento 6: Azioni precedenti all’assunzione

- **Verifiche**. Le verifiche suii candidati ad un certo impiego devono essere effettuate conformemente alle leggi, i regolamenti e l'etica pertinenti e dovrebbero essere proporzionati ai requisiti dell’organizzazione, laclassificazione delle informazioni a cui accedere e dei rischi percepiti. Laddove un lavoro una certa mansione comporta accesso ad informazioni riservate, ad es. informazioni finanziarie o informazioni altamente riservate, l'organizzazione dovrebbe anche considerare ulteriormente, verifiche particolarmente dettagliate.
- **Aspetti Contrattuali**. I ruoli e le responsabilità in materia di sicurezza delle informazioni devono essere comunicati ai candidati durante il processo di pre-assunzione. L'organizzazione dovrebbe garantire che dipendenti e appaltatori accettino termini e condizioni in merito alla sicurezza delle informazioni adeguata alla natura e alla portata dell'accesso che dovranno avere a risorse dell'organizzazione associate a sistemi e servizi di informazione. Se del caso, le responsabilità contenute nei termini e nelle condizioni di lavoro dovrebbero continuare per un periodo definito dopo la fine del rapporto di lavoro

Approfondimento 7: durante l’incarico

- Le responsabilità di gestione dovrebbero includere la garanzia che dipendenti e appaltatori:
  - a) siano adeguatamente informati sui loro ruoli e responsabilità in materia di sicurezza delle informazioni prima di essere abilitati all’accesso ad informazioni o sistemi di informazione riservati;
  - b) siano fornite linee guida per indicare le aspettative di sicurezza delle informazioni sul loro ruolo all'interno del organizzazione;
  - c) siano motivati a soddisfare le politiche di sicurezza delle informazioni dell'organizzazione;
  - d) abbiano un livello di consapevolezza sulla sicurezza delle informazioni pertinenti ai loro ruoli e responsabilità all'interno dell'organizzazione;
  - e) si adeguino ai termini e alle condizioni di impiego, inluse le politiche di sicurezza
  - f) garantiscano continuità temporale in relazione ai requisiti richiesti
  - g) siano dotati di un canale di segnalazione anonimo per segnalare violazioni delle politiche o delle proceduree di sicurezza
- Deve essere assicurato un piano di formazione continuo sulla sicurezza a tutto il personale, anche quello non direttamente coinvolto in servizi di sicurezza
- Devono essere previste azioni disciplinari in caso di violazioni di sicurezza (eventualmente anche incentivi per indurre buone pratiche e aderenza alle politiche/procedure)

Approfondimento 8: dopo l’incarico

- Devono essere definiti responsabilità e doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la risoluzione o il cambiamento di occupazione.
- La comunicazione delle responsabilità di risoluzione dovrebbero riferirsi (attraverso anche stipule di accordi di riservatezza in fase di assunzione) ad periodo ben definito dopo la fine del rapporto di lavoro.
- I cambiamenti di responsabilità o di impiego dovrebbero essere gestiti come la cessazione della corrente responsabilità o occupazione combinate con l'avvio della nuova responsabilità o occupazione.

Approfondimento 9: responsabilità degli asset

- Un'organizzazione dovrebbe identificare le risorse rilevanti nel ciclo di vita delle informazioni e documentarne l'importanza. Il ciclo di vita delle informazioni dovrebbe includere la creazione, l'elaborazione, la conservazione, la trasmissione e la cancellazione e distruzione. La documentazione deve essere conservata in inventari dedicati o esistenti, a seconda dei casi. L'inventario delle attività deve essere accurato, aggiornato, coerente e allineato con altri inventari.
- Deve essere implementato un processo per garantire l'assegnazione tempestiva della proprietà patrimoniale. La proprietà dovrebbe essere assegnata quando gli asset vengono creati o quando gli asset vengono trasferiti all'organizzazione. Il proprietario dell'asset dovrebbe essere responsabile della corretta gestione di un bene durante l'intero ciclo di vita del bene.
- I dipendenti e gli utenti di terze parti che utilizzano o hanno accesso alle risorse dell'organizzazione devono essere resi consapevoli dei requisiti di sicurezza delle informazioni delle risorse dell'organizzazione associate alle informazioni e alle infrastrutture e risorse per l'elaborazione delle informazioni. Dovrebbero essere responsabili del loro uso di qualsiasi risorsa di elaborazione delle informazioni e di tale uso effettuato sotto la loro responsabilità.
- Il processo di risoluzione deve essere formalizzato in modo da includere la restituzione di tutto il materiale fisico precedentemente consegnato e i beni elettronici di proprietà o affidati all'organizzazione. Nei casi di uso di dispositivi privati, devono essere seguite procedure per garantire che tutte le informazioni pertinenti siano trasferite all'organizzazione e rimosse in modo sicuro dall'apparecchiatura

Approfondimento 10: Classificazione dell’informazione

- Le classificazioni e i relativi controlli di protezione per le informazioni dovrebbero tener conto delle esigenze dell’organizzazione in relazione alla condivisione o alla limitazione di informazioni, nonché i requisiti legali.
- I proprietari delle risorse informative dovrebbero essere responsabili della loro classificazione. Lo schema di classificazione dovrebbe includere convenzioni per la classificazione e criteri per la revisione di la classificazione nel tempo.
- Il livello di protezione nel sistema dovrebbe essere valutato analizzando riservatezza, integrità e disponibilità e qualsiasi altro requisito per le informazioni considerate.
- Lo schema dovrebbe essere allineato alla politica di controllo degli accessi. A ciascun livello dovrebbe essere assegnato un nome che abbia senso nel contesto dell'applicazione dello schema di classificazione. Lo schema dovrebbe essere coerente in tutta l'organizzazione in modo che tutti classifichino le informazioni e le risorse correlate allo stesso modo.
- La classificazione dovrebbe essere inclusa nei processi dell'organizzazione ed essere coerente in tutta l'organizzazione. I risultati della classificazione dovrebbero indicare il valore delle attività in base alla loro sensibilità e criticità per l'organizzazione, ad es. in termini di riservatezza, integrità e disponibilità, e essere aggiornati in funzione dei precedenti attributi.
- È necessario sviluppare e attuare una serie adeguata di procedure per l'etichettatura delle informazioni in conformità con lo schema di classificazione delle informazioni adottato dall'organizzazione.
- È necessario elaborare procedure per la gestione, l'elaborazione, l'archiviazione e la comunicazione di informazioni coerente con la sua classificazione

Approfondimento 11: Gestione degli apparti di memorizzazione

- Dovrebbero essere implementate procedure per la gestione dei supporti rimovibili conformemente al schema di classificazione adottato dall'organizzazione.
- Dovrebbero essere stabilite procedure formali per lo smaltimento sicuro degli apparati di storage per ridurre al minimo il rischio di perdita di informazioni riservate a persone non autorizzate. Le procedure per lo smaltimento sicuro degli apparati contenenti informazioni riservate dovrebbe essere proporzionali alla sensibilità di tali informazioni.
- I supporti contenenti informazioni devono essere protetti da accesso non autorizzato, uso improprio o corruzione durante il trasporto.

Approfondimento 12: Requisiti funzionali per il controllo dell’accesso

- Devono essere definite opportune politiche di controllo degli accessi, documentate e riviste in base ai compiti dell’organizzazione e requisiti di sicurezza delle informazioni.
- I proprietari di beni dovrebbero stabilire adeguate regole di controllo dell'accesso, diritti di accesso e restrizioni per ruoli specifici dell'utente nei confronti delle proprie risorse, tenuto conto dei rischi associati alla sicurezza delle informazioni. Il controllo dell’accesso deve essere sia logico che fisico (vedere la clausola 11) e le politiche e i meccanismi devono essere coordinati. Agli utenti e ai fornitori di servizi dovrebbe essere fornita una chiara dichiarazione dei requisiti dell’organizzazione da soddisfare in relazione al controllo dell’accesso.
- Agli utenti dovrebbe essere fornito solo l'accesso alla rete e ai servizi di rete che sono stati specificamente autorizzati ad usare.

Approfondimento 13: gestione degli accessi

- È necessario implementare un processo di registrazione e annullamento della registrazione formale per consentire l'assegnazione di diritti di accesso.
- È necessario implementare un processo formale di provisioning dell'accesso utente per assegnare o revocare i diritti di accesso per tutti i tipi di utenti a tutti i sistemi e i servizi.
- L'assegnazione di diritti di accesso privilegiati dovrebbe essere controllata attraverso un processo di autorizzazione formale conformemente alla pertinente politica di controllo degli accessi
- L'allocazione di informazioni segrete di autenticazione dovrebbe essere controllata attraverso una procedura formale per il processo di gestione.
- I proprietari delle risorse dovrebbero revisionare i diritti di accesso degli utenti a intervalli regolari.
- I diritti di accesso di tutti i dipendenti e degli utenti di terze parti all'informazione e alle infrastrutture di elaborazione delle informazioni dovrebbero essere rimossi al termine del rapporto di lavoro, contratto o accordo, oppure adattati ad eventuali modifiche di mansione.

Approfondimento 14: Accountability

- Al fine di rendere gli utenti responsabili della protezione delle informazioni di autenticazione gli utenti dovrebbero essere tenuti a seguire le pratiche dell'organizzazione nell'uso delle informazioni segrete di autenticazione.
- Tutti gli utenti dovrebbero essere avvisati di:
  - a) mantenere riservate le informazioni di autenticazione segreta, garantendo che non vengano divulgate a nessun altro parti, compresi persone con ruoli di management, o tecnici;
  - b) evitare di memorizzare (ad es. su supporto cartaceo, software o palmare) le informazioni segrete, a meno che non possano essere archiviate in modo sicuro e il metodo di archiviazione sia stato approvato
  - c) modificare le informazioni segrete ogni qualvolta vi siano indicazioni della loro possibile compromissione;
  - d) usare password robuste
  - e) non condividere le informazioni di autenticazione segreta dei singoli utenti;
  - f) garantire un'adeguata protezione delle password quando le password vengono utilizzate come autenticazione segreta in procedure di accesso automatizzate;
  - g) non utilizzare le stesse informazioni di autenticazione segrete per scopi lavorativi e non commerciali.

Approfondimento 15: Controllo dell’accesso ad applicazioni e sistemi operativi

- L'accesso alle informazioni e alle funzioni degli applicativi dovrebbe essere limitato in conformità a politica di controllo accessi.
- Laddove richiesto dalla politica di controllo degli accessi, l'accesso ai sistemi e alle applicazioni dovrebbe essere controllato da una procedura di accesso sicuro.
- I sistemi di gestione delle password dovrebbero essere interattivi e garantire password di qualità.
- L'uso di programmi di utilità che potrebbero essere in grado di sovrascrivere i controlli di sistema e delle applicazioni dovrebbe essere limitato e strettamente controllato.
- L'accesso al codice sorgente dei programmi dovrebbe essere limitato.

Approfondimento 16: Crittografia

- Dovrebbe essere sviluppata una politica sull'uso dei controlli crittografici per la protezione delle informazioni.
- Prendere una decisione sull'opportunità di una soluzione crittografica dovrebbe essere vista come parte di il più ampio processo di valutazione del rischio e selezione dei controlli. Questa valutazione può quindi essere utilizzata per determinare se un controllo crittografico è appropriato, quale tipo di controllo dovrebbe essere applicato e per quale scopo e processi dell'organizzazione. È necessaria una politica sull'uso dei controlli crittografici per massimizzare i benefici e minimizzare il rischi di utilizzare tecniche crittografiche ed evitare usi inappropriati o non corretti.

- È necessario sviluppare e attuare una politica sull'uso, la protezione e la durata delle chiavi crittografiche durante l'intero ciclo di vita. La politica dovrebbe includere i requisiti per la gestione delle chiavi crittografiche durante l'intero ciclo di vita tra cui generazione, archiviazione, archiviazione, recupero, distribuzione, ritiro e distruzione di chiavi.
- Gli algoritmi crittografici, le lunghezze delle chiavi e le pratiche di utilizzo dovrebbero essere selezionati in base alle migliori pratiche. Una gestione delle chiavi appropriata richiede processi sicuri per la generazione, l'archiviazione, il recupero, la distribuzione, l revoca e la distruzione di chiavi crittografiche. Tutte le chiavi crittografiche devono essere protette da modifiche e perdite. Inoltre, chiavi segrete e private necessitano di protezione contro l'uso non autorizzato e la divulgazione. Le attrezzature utilizzate per generare, archiviare e le chiavi dell'archivio dovrebbero essere fisicamente protette.

Approfondimento 17: Gestione della protezione delle aree critiche

- I perimetri di sicurezza devono essere definiti e utilizzati per proteggere le aree che contengono informazioni sensibili e critiche o servizi di elaborazione delle informazioni correlati.
- Le aree sicure devono essere protette da adeguati controlli d'ingresso per garantire che solo al personale autorizzato è consentito l'accesso.
- La sicurezza fisica di uffici, locali e strutture deve essere progettata e applicata.
- È necessario progettare e applicare la protezione fisica contro catastrofi naturali, attacchi dolosi o incidenti.
- Devono essere progettate e applicate procedure per il lavoro in aree sicure.
- L’accesso a punti come aree di consegna e carico e altri punti in cui persone non autorizzate potrebbero entrare nei locali dovrebbe essere controllato e, se possibile, isolato dalle strutture di elaborazione delle informazioni per evitare accessi non autorizzati.

Approfondimento 18: protezione delle attrezzature

- Le apparecchiature devono essere collocate e protette per ridurre i rischi derivanti da minacce e pericoli per l'ambiente, e possibilità di accesso non autorizzato.
- Le apparecchiature devono essere protette da interruzioni di corrente e altre interruzioni causate da guasti.
- Icavi di alimentazione e di telecomunicazione che trasportano dati o supportano i servizi di informazione devono essere protetti da intercettazione, interferenza o danno.
- Le attrezzature devono essere mantenute correttamente per garantirne la continua disponibilità e integrità.
- Attrezzature, informazioni o software non devono essere portati fuori sede senza previa autorizzazione.
- La sicurezza dovrebbe essere applicata ai beni fuori sede tenendo conto dei diversi rischi connessi al lavoro effettuato all'esterno dei locali dell'organizzazione.
- Tutti gli elementi delle apparecchiature contenenti supporti di archiviazione devono essere verificati per garantire che tutti i dati sensibili e il software concesso in licenza sia stato rimosso o sovrascritto in modo sicuro prima dello smaltimento o del riutilizzo.
- Gli utenti devono garantire che le apparecchiature incustodite abbiano una protezione adeguata.
- Devono essere adottate politiche di scrivania per documenti cartacei e supporti di archiviazione rimovibili e politiche per il locking dello schermo.

Approfondimento 19: Procedure operazionali e responsabilità

- Dovrebbero essere preparate procedure per le attività operative associate alle informazioni e alle infrastrutture di elaborazione e comunicazione, come procedure di avvio e chiusura del computer, backup, manutenzione dell'attrezzatura, gestione dei supporti, gestione e sicurezza della sala computer e della posta.

- Le modifiche all'organizzazione, ai processi aziendali, alle strutture e ai sistemi di elaborazione delle informazioni che possono influenzare la sicurezza delle informazioni dovrebbe essere controllata.
- L'uso delle risorse dovrebbe essere monitorato, messo a punto e dovrebbero essere prodotte proiezioni sui futuri requisiti di capacità per garantire le prestazioni richieste.
- Gli ambienti di sviluppo, test e operativi devono essere separati per ridurre i rischi di accesso non autorizzato o modifiche all'ambiente operativo.

Approfondimento 20: Malware

- Dovrebbero essere implementati controlli di rilevamento, prevenzione e recupero per proteggere dai malware, combinati con un'adeguata consapevolezza dell'utente.
- La protezione da malware dovrebbe essere basata su software di rilevamento e remediation di malware, programmi si awareness e appropriati controlli di accesso al sistema e gestione delle modifiche. Si dovrebbe:
  - a) stabilire una politica formale che vieti l'uso di software non autorizzato;
  - b) implementare controlli che impediscano o rilevano l'uso di software non autorizzato (ad es. applicazione whitelisting);
  - c) implementare controlli che impediscono o rilevano l'uso di siti Web dannosi noti o sospetti (ad es. blacklist);
  - d) stabilire una politica formale di protezione contro i rischi associati all'ottenimento di file e software da o tramite reti esterne o su qualsiasi altro supporto, indicando quali misure di protezione dovrebbe essere adottate;
  - e) ridurre le vulnerabilità che potrebbero essere sfruttate da malware
  - f) condurre revisioni periodiche del software e del contenuto dei dati dei sistemi a supporto delle attività di processi critici; la presenza di file non approvati o di modifiche non autorizzate dovrebbe essere formalmente indagata;
  - g) installare e aggiornare regolarmente software di rilevamento e recupero da malware
  - h) definire procedure e responsabilità per la gestione della protezione da malware sui sistemi, per la formazione circa il loro uso, e la segnalazione e il recupero da attacchi di malware;
  - i) preparare piani di continuità aziendale adeguati per il recupero da attacchi di malware, inclusi tutte le disposizioni necessarie per il backup e il ripristino di dati e software;
  - j) attuare procedure per raccogliere regolarmente informazioni su nuovi malware;
  - l) isolare gli ambienti in cui possono verificarsi impatti catastrofici.

Approfondimento 21: backup

- Copie di backup di informazioni, immagini di software e di sistema devono essere prodotte e testate regolarmente in conformità con una politica di backup concordata.
- È necessario stabilire una politica di backup per definire i requisiti dell'organizzazione per il backup delle informazioni e dei software . La politica di backup dovrebbe definire i requisiti di conservazione e protezione. Dovrebbero essere fornite adeguate strutture di backup per garantire che tutte le informazioni e i software essenziali possano essere recuperati a seguito di un disastro o un guasto.

Approfondimento 22: logging

- Gli event logs che registrano le attività dell'utente, le eccezioni, i guasti e gli eventi di sicurezza dovrebbero essere prodotti, conservati e regolarmente rivisti.
- Le strutture di registrazione e le informazioni di registro devono essere protette da manomissioni e accessi non autorizzati.
- Le attività dell'amministratore di sistema e dell'operatore di sistema devono essere registrate e i registri protetti e regolarmente riviste.
- Gli orologi di tutti i pertinenti sistemi di elaborazione delle informazioni all'interno di un'organizzazione o di un dominio di sicurezza dovrebbe essere sincronizzati con una singola sorgente temporale di riferimento.

Approfondimento 23: Gestione della sicurezza della rete

- Le reti dovrebbero essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni. Dovrebbero essere attuati controlli per garantire la sicurezza delle informazioni nelle reti e la protezione di servizi connessi da accesso non autorizzato.
- Dovrebbero esserci meccanismi di sicurezza, livelli di servizio e requisiti di gestione di tutti i servizi di rete identificati e incluso nei contratti sui servizi di rete, indipendentemente dal fatto che tali servizi siano forniti internamente o esternalizzati.
- Gruppi di servizi, utenti e sistemi di informazione dovrebbero essere segregati sulle reti.

Approfondimento 24: trasferimento dell’informazione

- Politiche, procedure e controlli formali di trasferimento dovrebbero essere in atto per proteggere il trasferimento di informazioni attraverso l'uso di tutti i tipi di strutture di comunicazione.
- Gli accordi dovrebbero riguardare il trasferimento sicuro di informazioni commerciali tra l'organizzazione e le parti esterne.
- Le informazioni relative alla messaggistica elettronica devono essere adeguatamente protette.
- Dovrebbero essere identificati requisiti per accordi di riservatezza o di non divulgazione che riflettono le esigenze dell'organizzazione per la protezione delle informazioni, regolarmente revisionati e documentati.

Approfondimento 25: Acquisizione dei sistemi, sviluppo e manutenzione

- I requisiti di sicurezza delle informazioni dovrebbero essere identificati usando vari metodi come la derivazione da requisiti di conformità da politiche e normative, threat modeling, review su incidenti o uso delle soglie di vulnerabilità. I risultati dell'identificazione dovrebbero essere documentati e revisionati da tutti le parti interessate.
- Le informazioni relative ai servizi applicativi che passano attraverso reti pubbliche dovrebbero essere protette da attività fraudolenta, controversie contrattuali e divulgazione e modifiche non autorizzate.
- Le informazioni coinvolte nelle transazioni dei servizi applicativi devono essere protette per evitare che incomplete trasmissioni, instradamenti errati, modifiche non autorizzate dei messaggi, divulgazione non autorizzata, duplicazione o riproduzione dei messaggi non autorizzate.
- Le regole per lo sviluppo di software e sistemi dovrebbero essere stabilite e applicate agli sviluppi all'interno dell'organizzazione.
- Le modifiche ai sistemi all'interno del ciclo di vita dello sviluppo dovrebbero essere controllate mediante l'uso di procedure formali.
- Quando si cambiano le piattaforme operative, è necessario rivedere e testare le applicazioni business-critical e assicurarsi che non vi siano effetti negativi sulle operazioni organizzative o sulla sicurezza.
- Le modifiche ai pacchetti software dovrebbero essere scoraggiate, limitate alle modifiche necessarie e tutte le modifiche dovrebbe essere rigorosamente controllate.
- I principi per la progettazione di sistemi sicuri dovrebbero essere stabiliti, documentati, mantenuti e applicati a qualsiasi attività di implementazione del sistema informativo. Gli ambienti di sviluppo dovrebbero essere adeguatamente protetti.
- L'organizzazione dovrebbe supervisionare e monitorare l'attività di sviluppo del sistema esternalizzate.
- I test sulle funzionalità di sicurezza devono essere eseguiti durante le attività di sviluppo.
- I dati di test devono essere selezionati con cura, protetti e controllati.

Approfondimeno 26: relazione con i fornitori

- Requisiti di sicurezza per mitigare i rischi associati all'accesso del fornitore al le risorse dell'organizzazione devono essere concordati con il fornitore e documentati.
- Tutti i pertinenti requisiti di sicurezza delle informazioni devono essere stabiliti e concordati con ciascun fornitore che possono accedere, elaborare, archiviare, comunicare o fornire componenti di infrastruttura IT
- È necessario stabilire e documentare accordi con i fornitori per garantire che non vi siano equivoci tra l'organizzazione e il fornitore in merito agli obblighi di entrambe le parti di adempiere ai pertinenti requisiti di sicurezza delle informazioni.
- Le organizzazioni dovrebbero monitorare, rivedere e controllare regolarmente la fornitura del servizio ai fornitori
- Modifiche alla fornitura di servizi da parte dei fornitori, incluso il mantenimento e il miglioramento delle politiche, procedure e controlli esistenti in materia di sicurezza delle informazioni dovrebbero essere gestiti tenendo conto del criticità delle informazioni delle organizzazioni, dei sistemi e dei processi coinvolti e nuova valutazione dei rischi.

Approfondimento 27: business continuity

- L'organizzazione dovrebbe determinare i suoi requisiti per la sicurezza delle informazioni e la continuità di gestione della sicurezza delle informazioni in situazioni avverse, ad es. durante una crisi o un disastro.
- L'organizzazione dovrebbe stabilire, documentare, attuare e mantenere processi, procedure e controlli per garantire il livello richiesto di continuità per la sicurezza delle informazioni durante una situazione avversa.
- L'organizzazione dovrebbe verificare la continuità dei controlli di sicurezza stabiliti e implementati. Le verifiche devono avvenire a intervalli regolari al fine di garantire che siano validi ed efficaci in situazioni avverse.
- Le strutture di elaborazione delle informazioni dovrebbero essere implementate con ridondanza sufficiente per soddisfare la disponibilità requisiti.

Approfondimento 28: Compliance

- Tutti i pertinenti requisiti legislativi, regolamentari, contrattuali e l'approccio dell'organizzazione per soddisfare questi requisiti dovrebbero essere esplicitamente identificati, documentati e tenuti aggiornati per ciascun sistema informativo dell' organizzazione.
- Dovrebbero essere attuate procedure appropriate per garantire la conformità alle disposizioni legislative, regolamentari e ai requisiti contrattuali relativi ai diritti di proprietà intellettuale e all'uso di prodotti software proprietari.
- I registri devono essere protetti da perdita, distruzione, falsificazione, accesso o rilascio non autorizzato, in conformità con i requisiti legislativi, regolamentari, contrattuali e commerciali.
- La privacy e la protezione delle informazioni di identificazione personale devono essere garantite come richiesto dalle pertinenti legislazioni e la regolamentazione applicabile (in EU, GDPR).
- I controlli crittografici dovrebbero essere utilizzati in conformità con tutti gli accordi, la legislazione e regolamenti.
- L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e alla sua attuazione (ad es. Controllo obiettivi, controlli, politiche, processi e procedure per la sicurezza delle informazioni) dovrebbero essere rivisti indipendentemente a intervalli pianificati o quando si verificano cambiamenti significativi.
- I manager dovrebbero rivedere periodicamente la conformità delle procedure e del trattamento delle informazioni all'interno la loro area di responsabilità con le politiche di sicurezza appropriate, gli standard e ogni altro requisito di sicurezza.