**System Management**

Il system management gestisce oltre la parte tecnica esecutiva guarda anche la parte strategica e di supporto.

**System management**: significa avere dei sistemi scalati in base alle necessita dell’azienda.

Benefici del S. M.

* Raccogliere dati del business a livello tecnologico
* Crea le condizioni per garantire un supporto continuo
* Crea una base per il BCP (Business Continuity Planning)
* Ruoli e responsabilità
* Coinvolgimento del supporto esecutivo nelle procedure a livello esecutivo

**CIO**: Chief Information Officer

Il Chief Information Officer (CIO) è un dirigente di alto livello responsabile della gestione e della supervisione delle strategie e delle operazioni informatiche (IT) di un'organizzazione. Il CIO è responsabile dell'allineamento degli obiettivi IT con gli obiettivi aziendali generali dell'organizzazione, nonché dell'implementazione e della manutenzione dei sistemi, delle infrastrutture e delle politiche IT che supportano tali obiettivi.

Fattori da considerare nella progettazione di infrastrutture IT

* Conoscere l'azienda (KYB)
* Individuare i reparti, le infrastrutture e le risorse disponibili.
* Identificare i proprietari dei processi

**Importanza dello staff**

* Valutazione dei livelli di competenza dell'attuale personale di bordo
* Identificazione dei set di competenze e dei livelli di abilità richiesti
* Identificazione di fonti alternative di reclutamento del personale
* Reclutamento del personale dell'infrastruttura dall'esterno (operativo, consultivo)
* Selezione del candidato più qualificato
* Mantenimento del personale chiave
* Utilizzo di consulenti e appaltatori per integrare il personale
* Vantaggi dell'utilizzo di consulenti e appaltatori (accesso a competenze specializzate, flessibilità)
* Svantaggi dell'utilizzo di consulenti e appaltatori (mancanza di conoscenza della cultura aziendale, dipendenza da risorse esterne)
* Fasi per lo sviluppo di percorsi di carriera per i membri del personale (identificazione delle competenze richieste, creazione di programmi di formazione e sviluppo)

**Servizio Clienti**

L'evoluzione dell'IT in un'organizzazione di servizi implica l'adozione di un approccio incentrato sul cliente e la fornitura di un buon servizio al cliente. Quattro elementi chiave di un buon servizio clienti sono:

* **Identificazione dei clienti chiave**: L'IT deve identificare i propri clienti e comprendere le loro esigenze e aspettative.
* **Identificare i servizi chiave dei clienti chiave**: Una volta identificati i clienti chiave, l'IT deve capire quali sono i servizi chiave richiesti da questi clienti e stabilirne la priorità.
* **Identificare i processi chiave che supportano i servizi chiave**: L'IT deve identificare i processi che supportano i servizi chiave richiesti dai clienti chiave e assicurarsi che siano ottimizzati in termini di efficienza ed efficacia.
* **Identificare i fornitori chiave che supportano i processi chiave**: L'IT deve identificare i fornitori che supportano i processi chiave necessari per fornire i servizi chiave ai clienti chiave e garantire che siano affidabili e conformi agli standard di qualità.

L'integrazione di questi quattro elementi chiave aiuterà l'IT a trasformarsi in un'organizzazione di servizi incentrata sul cliente. Mettendo il cliente al primo posto e fornendo un servizio eccellente, l'IT può migliorare la soddisfazione dei clienti, aumentare l'efficienza e guidare il successo aziendale.

I 9 peccati capitali del servizio clienti e dell'assistenza:

1. Mancanza di empatia
2. Non offrire soluzioni alternative
3. Atteggiamento di servizio freddo
4. Mancanza di ascolto attivo
5. Servizio clienti robotizzato
6. Trattamento da manuale
7. Trasferimento da agente ad agente
8. Ignorare le preferenze del cliente
9. Non riconoscere gli errori

**Disponibilità**

**UP time**= somma del tempo di disponibilità

**Responsività**: risposte in caso di problemi

Sistemi che rispondono lenti sono diversi da sistemi completamente down

**Disponibilità**: sistema disponibile basato su elementi unici, alta disponibilità: si basa su elementi multipli, clustering.

I 7 R dell'alta disponibilità sono:

* **Ridondanza**: avere componenti di backup in caso di guasto di quelli primari per garantire la continuità del servizio.
* **Reputazione**: l'immagine dell'organizzazione presso i clienti, i dipendenti e gli stakeholder in generale.
* **Affidabilità (Reliability)**: la probabilità che un sistema funzioni correttamente senza guasti per un certo periodo di tempo.
* **Riparabilità**: il tempo necessario per riparare un sistema in caso di guasto.
* **Recuperabilità**: la capacità di recuperare i dati e le applicazioni in caso di disastro o interruzione del servizio.
* **Reattività**: la capacità di rispondere rapidamente a situazioni di emergenza o di criticità.
* **Robustezza**: la capacità di mantenere un servizio o un'applicazione in funzione anche in presenza di situazioni anomale o di attacchi esterni.

Per misurare e monitorare la disponibilità dell'infrastruttura, è necessario definire un processo che tenga conto delle ore di disponibilità impegnate (A) e delle ore di interruzione (B). La formula per calcolare la disponibilità raggiunta è:

**Disponibilità raggiunta = ((A-B)/A)\*100%**

In questo modo, si può tenere traccia della disponibilità del servizio e intervenire in modo tempestivo per migliorare le prestazioni dell'infrastruttura e garantire un'alta disponibilità del servizio.

**SMART: Specific Measurable Achievable Relevant Timely**

viene comunemente usato per definire gli obiettivi in modo chiaro e preciso

Immagine che contiene testo

Descrizione generata automaticamente**Process Owner**: pianifica investimenti per evitare il down time.

Il processo di prestazioni e messa a punto è un processo fondamentale dell'infrastruttura IT che si occupa di misurare e ottimizzare le prestazioni dei vari ambienti di risorse.

Il proprietario di un processo di prestazioni e messa a punto deve avere competenze specifiche e conoscenze approfondite dei sistemi, delle applicazioni e dei servizi dell'infrastruttura.

I cinque principali ambienti di risorse che richiedono prestazioni e messa a punto sono: server, archiviazione su disco, database, rete e client.

La valutazione delle prestazioni e del processo di tuning dell'infrastruttura richiede una misurazione accurata delle prestazioni e la definizione di obiettivi chiari per il miglioramento delle prestazioni.

Il processo di prestazioni e messa a punto deve essere continuamente monitorato, misurato e ottimizzato per garantire il corretto funzionamento dell'infrastruttura IT e la soddisfazione degli utenti.

* **Ambiente server:** includono server fisici e virtuali, con un'attenzione particolare alle prestazioni del processore, della memoria e del disco.
* **Ambiente di archiviazione su disco**: include la gestione dell'archiviazione dei dati, la protezione dei dati, la velocità di accesso ai dati e la riproduzione di dati.
* **Ambiente del database**: si concentra sull'ottimizzazione delle query, la gestione dell'indice e la progettazione del database.
* **Ambiente di rete**: include la velocità di trasmissione dei dati, la larghezza di banda, la latenza e la disponibilità.
* **Ambiente client** (computer desktop, tablet, smartphone, ...): include la velocità del processore, la memoria, la connettività di rete e le prestazioni delle applicazioni.

**Stakeholders ruoli e regole**

* **Responsible**: persona o stakeholder che svolge il lavoro e deve completare il compito o l'obiettivo o prendere la decisione
* **Accountable**: persona o stakeholder che è il "proprietario" del lavoro e deve firmare o approvare il completamento del compito, dell'obiettivo o della decisione; deve assicurarsi che le responsabilità siano assegnate nella matrice per tutte le attività correlate
* **Consultato**: chi deve dare un contributo prima che il lavoro possa essere fatto e firmare il lavoro; partecipa attivamente
* **Informati**: persone o parti interessate che devono essere tenute "al corrente"; hanno bisogno di aggiornamenti sui progressi o sulle decisioni, ma non hanno bisogno di essere consultati formalmente, né contribuiscono direttamente al compito o alla decisione
* Il successo richiede che ci sia una sola persona responsabile, il che significa che "la responsabilità si ferma qui".

.

**Production Acceptance**

Definizione di accettazione della produzione: processo che permette di verificare che il prodotto software soddisfi i requisiti e le specifiche richiesti. I vantaggi di un processo di accettazione della produzione includono la riduzione del rischio di fallimento del progetto e l'incremento della qualità del prodotto.

Implementazione di un processo di accettazione della produzione

1. Fase 1: identificare uno sponsor esecutivo
2. Fase 2: selezionare un proprietario del processo
3. Fase 3: sollecitare il supporto dei dirigenti
4. Fase 4: Creare un team di accettazione della produzione
5. Fase 5: Identificare e dare priorità ai requisiti
6. Fase 6: Sviluppare dichiarazioni di politica
7. Fase 7: Nominare un sistema pilota
8. Fase 8: Progettazione di moduli appropriati
9. Fase 9: Documentare gli aggiornamenti, le estensioni e le nuove procedure.
10. Fase 10: Eseguire test sul campo e una solida fase pilota
11. Fase 11: revisione di politiche, procedure e moduli
12. Fase 12: Definizione di un'adeguata strategia di marketing (se applicabile)
13. Fase 13: condurre una sessione di lezioni apprese
14. Fase 14: Seguire le revisioni e i miglioramenti continui.

Distribuzione completa di una nuova applicazione

L'accettazione della produzione non è Change Management; Nuove applicazioni vs. nuove versioni di applicazioni esistenti

**Change Management**

si riferisce all'insieme di processi, strumenti e tecniche utilizzati per gestire e controllare i cambiamenti in un'organizzazione, in modo che possano essere implementati in modo efficace e senza causare interruzioni o problemi.

Le fasi fondamentali per lo sviluppo di un processo di change managment includono: **l'identificazione di uno sponsor esecutivo** e di un proprietario del processo, **la formazione di un team interfunzionale** di progettazione, **l'assegnazione di ruoli e responsabilità**, **l'identificazione e la priorizzazione** dei requisiti, **lo sviluppo di definizioni dei termini** chiave**, la progettazione del processo** e l'utilizzo di un comitato consultivo per migliorare continuamente il processo di gestione del cambiamento. Inoltre, vengono menzionate alcune metriche del cambiamento, come la valutazione dell'infrastruttura e la semplificazione del processo di gestione del cambiamento.

Il processo amministrativo quotidiano non fa parte del processo del change managment, poiché si riferisce alle attività di routine, come il ripristino delle password, l'aggiunta/eliminazione di utenti, la modifica degli utenti e dei gruppi di sicurezza, e il riavvio delle macchine senza modifiche alla configurazione del sistema o dei permessi dei file. Al contrario, il processo di change managment si occupa di modifiche a elementi o risorse di produzione e di attività correlate al BCM.

**BCM** è l'acronimo di Business Continuity Management, ovvero la gestione della continuità del business. Si tratta di un approccio olistico alla pianificazione e alla preparazione di un'organizzazione per affrontare e superare le situazioni di crisi e di emergenza, in modo da garantire la continuità delle attività aziendali.

**La gestione dei problemi** consiste nel gestire in modo efficace i problemi di un'infrastruttura IT, rilevando e risolvendo le cause sottostanti dei problemi per prevenirne la ricorrenza.

**La gestione dei problemi** si distingue dalla **gestione degli incidenti, dei cambiamenti e delle richieste**, ed è composta da fasi come la selezione dello sponsor esecutivo, l'assegnazione di un proprietario del processo, la creazione di un team interfunzionale, l'identificazione dei requisiti, lo schema di priorità e di escalation, la progettazione del processo di gestione delle chiamate e la valutazione del processo di gestione dei problemi di un'infrastruttura. Il Service Desk gioca un ruolo importante nella gestione dei problemi, mentre la segregazione e l'integrazione dei service desk sono elementi importanti da considerare.

**La gestione dello storage** riguarda la gestione dei dati su dispositivi di storage come dischi rigidi, unità a stato solido e archivi di backup. Il Process Owner della gestione dello storage è responsabile della pianificazione, dell'implementazione e del mantenimento della soluzione di storage dell'organizzazione.

Le attività principali della gestione dello storage sono **la capacità, la prestazione, l'affidabilità e la recuperabilità**. La capacità si riferisce alla quantità di spazio di storage disponibile e alla pianificazione futura. La prestazione riguarda la velocità e la capacità di elaborazione dei dati. L'affidabilità si riferisce alla capacità di ripristinare i dati in caso di guasti hardware o software, mentre la recuperabilità si riferisce alla capacità di ripristinare i dati in caso di perdita o cancellazione accidentale.

Per valutare il processo di gestione dello storage, si possono utilizzare indicatori di prestazione chiave come la percentuale di spazio di storage utilizzato e la velocità di lettura e scrittura dei dati. Inoltre, è possibile misurare e convalidare il processo di gestione dello storage attraverso la definizione di procedure standard, il monitoraggio dell'utilizzo dello storage e la verifica della conformità con le normative di sicurezza e privacy dei dati.

**La gestione della rete** è l'insieme di attività che riguardano la pianificazione, la configurazione, il monitoraggio e la gestione della rete di un'organizzazione. Le decisioni chiave riguardano la definizione dei servizi da offrire, la definizione dei livelli di servizio, la scelta degli strumenti e del supporto necessari, nonché l'integrazione con gli altri processi IT.

Il processo di gestione della rete sarà gestito da un Network Management Process Owner, che avrà l'autorità di prendere decisioni riguardanti la pianificazione, la configurazione e il monitoraggio della rete. Saranno forniti strumenti e supporto adeguati per garantire un'efficace gestione della rete.

Gli altri processi IT saranno integrati con il processo di gestione della rete al fine di garantire una gestione efficiente e coordinata della rete. I livelli di servizio e di qualità attesi dipenderanno dalle esigenze dell'organizzazione e dalle specifiche della rete.

Per valutare il processo di gestione della rete di un'infrastruttura, è possibile utilizzare indicatori di prestazione chiave come la disponibilità della rete, la velocità di trasmissione dei dati e il tempo di risposta del sistema. È inoltre possibile misurare e ottimizzare il processo di gestione della rete attraverso la definizione di procedure standard, il monitoraggio delle prestazioni della rete e la verifica della conformità con le normative di sicurezza e privacy dei dati.

**La gestione della configurazione** riguarda l'identificazione e il controllo di tutti gli elementi di configurazione di un sistema IT. Per migliorarla, è importante avere un process owner qualificato, coinvolgere i fornitori di hardware e software, valutare la documentazione esistente e coordinare gli sforzi di documentazione prima di importanti aggiornamenti. È inoltre utile coinvolgere il gruppo di gestione delle risorse per l'inventario delle apparecchiature desktop. Per valutare e ottimizzare il processo, è possibile misurare la qualità della documentazione di configurazione, il grado di conformità alle normative e l'efficacia del processo di controllo dei cambiamenti.

**Servizi cloud:**

**Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente**

- **Il pooling delle risorse** è la caratteristica fondamentale, dove il fornitore astrae le risorse e le raccoglie in un pool che può essere assegnato a diversi consumatori sulla base di politiche.

**- I consumatori gestiscono le loro risorse** dal pool attraverso self-service on-demand, senza dover parlare con un amministratore umano.

**- L'ampio accesso alla rete rende tutte le risorse disponibili** senza bisogno di un accesso fisico diretto, la rete non fa necessariamente parte del servizio.

- **L'elasticità rapida consente agli utenti di espandere o contrarre le risorse** utilizzate dal pool in modo completamente automatico, permettendo di far coincidere il consumo di risorse con la domanda.

- **Il servizio misurato misura ciò che viene fornito**, per garantire che i consumatori utilizzino solo ciò che viene loro assegnato e di addebitarne il costo.

**Il software come servizio (SaaS)** è un'applicazione completa gestita e ospitata dal fornitore, a cui i consumatori accedono tramite browser web, mobile o app client leggera.

**Il Platform as a Service (PaaS)** fornisce piattaforme applicative come database, piattaforme per l'esecuzione di codice e archiviazione di file, mentre **l'Infrastruttura come servizio (IaaS)** offre l'accesso a un pool di risorse di infrastrutture informatiche fondamentali, come l'elaborazione, la rete o lo storage. La differenza fondamentale tra PaaS e SaaS è che con il PaaS non si gestiscono i server, le reti o altre infrastrutture sottostanti.

**La pianificazione della capacità** si riferisce alla gestione della capacità delle risorse informatiche in modo da soddisfare la domanda futura. Tuttavia, spesso non viene fatta bene perché gli analisti sono troppo impegnati nelle attività quotidiane, gli utenti non sono in grado di prevedere i carichi di lavoro futuri, i pianificatori possono essere riluttanti ad usare strumenti di misurazione efficaci, la pianificazione non fa parte della cultura dell'infrastruttura, e i manager confondono la gestione con la pianificazione della capacità.

Sviluppare una pianificazione delle capacità

* Selezionare un responsabile per la pianificazione della capacità
* Identificare le risorse critiche da misurare
* Monitorare l'utilizzo o le prestazioni delle risorse
* Confrontare utilizzo e capacità massima
* Raccogliere le previsioni di carico di lavoro da sviluppatori e utenti
* Trasformare le previsioni in requisiti di risorse IT
* Mappare i requisiti sull'utilizzo esistente
* Prevedere quando l'azienda sarà fuori capacità
* Aggiornare previsioni e utilizzi.

**La sicurezza strategica** è l'approccio di lungo termine per la gestione della sicurezza dell'infrastruttura IT e delle informazioni dell'azienda. Un processo di sicurezza strategica ben strutturato aiuta a identificare e mitigare i rischi di sicurezza, proteggere le informazioni sensibili e mantenere la continuità del business.

Per sviluppare un processo di sicurezza strategica efficace, si possono seguire le seguenti fasi:

1. Identificare uno sponsor esecutivo
2. Selezionare un proprietario del processo di sicurezza
3. Definire gli obiettivi della sicurezza strategica
4. Creare comitati di revisione
5. Identificare, classificare e dare priorità ai requisiti
6. Effettuare un inventario dello stato attuale della sicurezza
7. Definire l'organizzazione della sicurezza
8. Sviluppare le politiche di sicurezza
9. Creare gruppi di pianificazione
10. Revisione e approvazione dei piani
11. Valutare la fattibilità tecnica dei piani
12. Assegnare e programmare l'attuazione dei piani.

Per valutare l'efficacia del processo strategico di sicurezza di un'infrastruttura, è possibile effettuare un'analisi dei rischi, delle minacce e delle vulnerabilità dell'infrastruttura e delle informazioni. Questo aiuta a identificare eventuali lacune nella sicurezza e a sviluppare piani per mitigare i rischi.

**La continuità aziendale** si riferisce alla capacità di un'organizzazione di mantenere le sue operazioni in caso di interruzioni o di eventi catastrofici. Un processo di continuità aziendale efficace può aiutare un'organizzazione a recuperare rapidamente da un'interruzione e minimizzare gli effetti negativi sulle sue operazioni.

Le fasi dello sviluppo di un processo di continuità aziendale efficace includono:

* Fase 1: **Acquisire il supporto dei dirigenti:** è importante ottenere il sostegno dei dirigenti dell'organizzazione per garantire che il processo di continuità aziendale abbia le risorse necessarie per essere efficace.
* Fase 2**: Selezionare un responsabile del processo**: un responsabile del processo di continuità aziendale dovrebbe essere selezionato per coordinare l'implementazione del processo.
* Fase 3: **Creare un team interfunzionale**: il team di continuità aziendale dovrebbe includere rappresentanti di tutte le funzioni aziendali per garantire che le esigenze di ogni area dell'organizzazione siano considerate.
* Fase 4: **Conduzione di un'analisi dell'impatto aziendale**: identificare i rischi e gli impatti che potrebbero derivare da eventi catastrofici.
* Fase 5**: Identificare e dare priorità ai requisiti**: in base ai risultati dell'analisi dell'impatto aziendale, identificare e stabilire le priorità per le esigenze di continuità aziendale dell'organizzazione.
* Fase 6: **Valutare le possibili strategie di ripristino della continuità operativa**: esaminare le opzioni disponibili per ripristinare la continuità operativa in caso di interruzione, come ad esempio il ripristino di dati da backup o la migrazione delle applicazioni in un centro di elaborazione dati alternativo.
* Fase 7: **elaborazione di una richiesta di offerta (RFP) per i servizi esterni**
* Fase 8: **valutazione delle proposte e selezione dell'offerta migliore**
* Fase 9: **Scegliere i partecipanti e chiarire i loro ruoli nel team di recupero.**
* Fase 10: **Documentare il piano di continuità operativa**
* Fase 11**: pianificare ed eseguire test periodici del piano**
* Fase 12: **condurre un'autopsia delle lezioni apprese dopo ogni test.**
* Fase 13: **Mantenere, aggiornare e migliorare continuamente il piano.**

**La gestione delle strutture** si riferisce alla pianificazione, al coordinamento e alla supervisione delle attività necessarie per mantenere e migliorare le infrastrutture fisiche di un'organizzazione, come ad esempio i data center, gli edifici, gli impianti e le apparecchiature. Ciò include anche la valutazione dei rischi, la gestione delle esposizioni fisiche comuni e l'ottimizzazione dell'ambiente fisico per garantire l'efficienza e l'efficacia del processo. Il responsabile del processo di gestione delle strutture deve garantire che siano presenti layout fisici efficienti ed efficaci e che il processo sia continuamente valutato e migliorato.

**Il monitoraggio IT** prevede la priorità di gestione dei sistemi, come la prestazione e la disponibilità del sistema operativo, lo stato dell'hardware del server, la disponibilità dei dati e dello storage, i servizi di directory, le patch e gli aggiornamenti, le prestazioni dell'infrastruttura di virtualizzazione, l'allarme e la segnalazione di problemi e incidenti, il rilevamento delle modifiche e l'analisi del comportamento, la pianificazione della capacità e il monitoraggio del server email. È importante seguire la regola dell'80% e verificare continuamente l'adeguatezza del monitoraggio. **COBIT (Control Objectives for Information and Related Technology)** è un framework sviluppato dall'ISACA (Information Systems Audit and Control Association) per la gestione dell'IT. Ecco alcuni punti salienti del COBIT:

* Definisce obiettivi di controllo e buone pratiche per la gestione dell'IT, focalizzandosi sulla governance, la gestione dei processi e la sicurezza.
* Aiuta le organizzazioni a stabilire un sistema di controllo per l'IT, a gestire i rischi e a garantire la conformità alle normative.
* Fornisce una struttura per la valutazione della maturità dei processi IT e per l'identificazione dei gap.
* È diviso in cinque domini: Pianificazione e organizzazione, Acquisizione e implementazione, Consegna e supporto, Monitoraggio e valutazione, e Informazioni.
* Ogni dominio è suddiviso in processi specifici, che sono descritti dettagliatamente e accompagnati da obiettivi di controllo e metriche di performance.
* Il COBIT è integrabile con altri framework e standard, come ITIL, ISO 27001 e COSO.
* È regolarmente aggiornato per riflettere i cambiamenti nell'ambiente IT e nelle esigenze delle organizzazioni.

Immagine che contiene testo, biglietto da visita, schermata, cerchio

Descrizione generata automaticamenteIl COBIT 5 distingue **la governance dalla gestione e definisce la governance come il processo attraverso il quale gli stakeholder definiscono gli obiettivi aziendali equilibrati e concordati da raggiungere**, stabiliscono le priorità e monitorano le prestazioni e la conformità rispetto agli obiettivi e alla direzione stabilita dall'organo di governo**. La gestione, d'altra parte, si riferisce al processo attraverso il quale le attività vengono pianificate, costruite, gestite e monitorate in linea con la direzione stabilita dall'organo di governo per raggiungere gli obiettivi dell'impresa**. In breve, **la governance definisce la direzione, le priorità e la conformità**, mentre **la gestione pianifica e gestisce le attività per raggiungere gli obiettivi stabiliti.**

**La governance** è il processo di presa e applicazione delle decisioni all'interno di un'organizzazione o di una società. È il processo di interazione attraverso le leggi, le norme sociali, il potere o il linguaggio strutturato nella comunicazione di una società organizzata su un sistema sociale.

**Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamenteLa gestione delle informazioni e degli eventi di sicurezza (SIEM)** è una soluzione che consente ai professionisti della sicurezza aziendale di monitorare le attività all'interno del loro ambiente IT. Essa fornisce analisi in tempo reale dei dati di log ed eventi, consentendo il monitoraggio delle minacce, la correlazione degli eventi e la risposta agli incidenti. La SIEM raccoglie e aggrega i dati di log generati da diversi componenti dell'infrastruttura tecnologica dell'organizzazione, tra cui server, sistemi host, applicazioni, rete e dispositivi di sicurezza come firewall e filtri antivirus.

Il SIEM (Security Information and Event Management) è una soluzione software o hardware che consente ai professionisti della sicurezza aziendale di monitorare e analizzare in tempo reale i dati di log ed eventi generati nella infrastruttura tecnologica dell'organizzazione, al fine di individuare eventuali minacce o attività anomale e di rispondere prontamente agli incidenti.

* **Retention**: Il SIEM conserva i dati per lunghi periodi di tempo, in modo da poter prendere decisioni basate su una serie di dati completi.
* **Dashboards**: Vengono utilizzati per analizzare (e visualizzare) i dati, nel tentativo di riconoscere modelli o di individuare attività o dati che non rientrano in un modello normale.
* **Correlation**: Il SIEM ordina i dati in pacchetti significativi, simili e con caratteristiche comuni, trasformando i dati in informazioni utili.
* **Alerting**: Quando vengono raccolti o identificati dati che innescano determinate risposte, come ad esempio avvisi o potenziali problemi di sicurezza, gli strumenti SIEM possono attivare determinati protocolli per avvisare gli utenti, come notifiche inviate al dashboard, e-mail automatiche o messaggi di testo.
* **Data Aggregation**: Una volta introdotto il SIEM, i dati possono essere raccolti da un numero qualsiasi di siti, tra cui server, reti, database, software e sistemi di posta elettronica. L'aggregatore funge anche da risorsa di consolidamento prima che i dati vengano inviati per essere correlati o conservati.
* **Compliance**: In un SIEM è possibile stabilire dei protocolli che raccolgono automaticamente i dati necessari per la conformità alle politiche aziendali, organizzative o governative.

**Il team SOC (Security Operations Center**) gestisce e previene i problemi di sicurezza e definisce tutte le istruzioni/linee guida sulla sicurezza per i team IT, richiedendo un livello di competenze diversificato e molto elevato, suddiviso in quattro aree distinte di competenza:

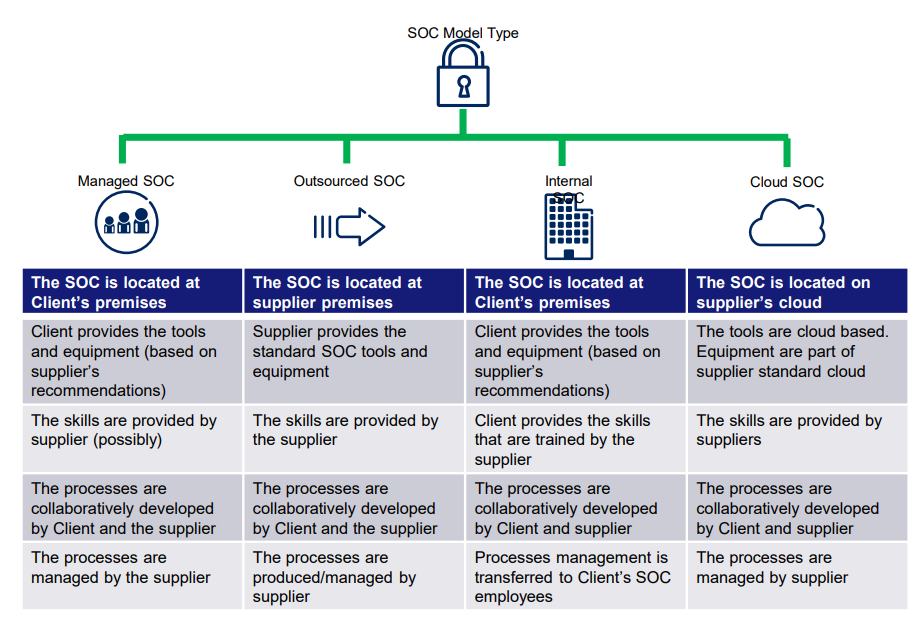
* Competenze di sicurezza
* Competenze di rete
* Competenze infrastrutturali
* Competenze di governance e conformità.

Alcuni nomi:

* Splunk
* IBM QRadar
* LogRhythm

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente



Gli elementi fondamentali di una **privacy policy** includono:

1. Tipi di dati raccolti: descrizione dei tipi di dati personali che vengono raccolti, ad esempio nome, indirizzo, numero di telefono, indirizzo email, informazioni di pagamento, dati di navigazione web, ecc.
2. Finalità della raccolta dati: indicazione delle finalità per cui i dati vengono raccolti, ad esempio per fornire un servizio specifico, per migliorare l'esperienza dell'utente, per inviare comunicazioni di marketing, ecc.
3. Modalità di raccolta dati: descrizione dei metodi utilizzati per raccogliere i dati personali, ad esempio attraverso un form online, attraverso l'utilizzo di cookie o attraverso l'accesso ai dati dal profilo social dell'utente.
4. Diritti dell'utente: elenco dei diritti dell'utente, come il diritto di accedere ai propri dati personali, di richiedere la cancellazione dei propri dati o di esercitare il diritto all'oblio.
5. Protezione dei dati: descrizione delle misure di sicurezza adottate per proteggere i dati personali, ad esempio l'uso di crittografia, la gestione degli accessi, la sicurezza delle reti e dei sistemi, ecc.
6. Condivisione dei dati: descrizione delle situazioni in cui i dati personali possono essere condivisi con terze parti, ad esempio per fornire un servizio o per rispettare le leggi applicabili.
7. Politica sui cookie: descrizione della politica sui cookie e dei tipi di cookie utilizzati, ad esempio cookie di sessione, cookie di tracciamento, cookie di terze parti, ecc.
8. Contatti e informazioni: indicazione dei contatti dell'azienda responsabile della raccolta dei dati e delle modalità per contattarla in caso di richieste o domande relative alla privacy policy.

La struttura di un documento di **policy aziendale** può variare a seconda dell'argomento e della specificità dell'azienda, ma in generale può includere le seguenti sezioni:

1. **Introduzione**: una breve descrizione del motivo per cui è stata creata la policy e del suo scopo.
2. **Scopo**: una descrizione dettagliata dell'obiettivo della policy, includendo una spiegazione di come verrà implementata e monitorata.
3. **Definizioni**: una sezione che definisce i termini utilizzati nella policy in modo chiaro e preciso, in modo da evitare malintesi o interpretazioni errate.
4. **Responsabilità**: una sezione che descrive le responsabilità dei vari membri dell'azienda, inclusi i manager e i dipendenti, riguardo all'implementazione della policy.
5. **Procedura di attuazione**: una descrizione dettagliata delle procedure da seguire per attuare la policy, inclusi i tempi di implementazione e le attività specifiche da svolgere.
6. **Monitoraggio e revisione**: una descrizione di come la policy verrà monitorata e rivista per garantire che sia efficace e aggiornata.
7. **Sanzioni**: una sezione che elenca le sanzioni che verranno applicate nel caso in cui i dipendenti non rispettino la policy.
8. **Allegati**: se necessario, potrebbero essere inclusi allegati che forniscono ulteriori informazioni o istruzioni relative alla policy.

È importante che la policy sia scritta in modo chiaro e conciso, in modo che sia facilmente comprensibile per tutti i membri dell'azienda. Inoltre, è essenziale che la policy sia conforme alle leggi e ai regolamenti in vigore nel paese in cui l'azienda opera.

Immagine che contiene testo, schermata, documento, Carattere

Descrizione generata automaticamente

**Thick Provision Eager Zeroed:** è un tipo di disco virtuale spesso che supporta funzionalità di clustering come Fault Tolerance. Lo spazio richiesto per il disco virtuale viene allocato al momento della creazione e i dati rimanenti sul dispositivo fisico vengono cancellati. La creazione di dischi virtuali in questo formato potrebbe richiedere più tempo rispetto ad altri tipi di dischi. Aumentare la dimensione di un disco virtuale Thick Eager Zeroed causa un significativo ritardo per la macchina virtuale.

**Thick Provision Lazy Zeroed:** crea un disco virtuale in un formato spesso predefinito. Lo spazio richiesto per il disco virtuale viene allocato al momento della creazione, ma i dati rimanenti sul dispositivo fisico non vengono cancellati durante la creazione, ma vengono cancellati a richiesta quando la macchina virtuale scrive per la prima volta. La macchina virtuale non legge dati obsoleti dal dispositivo fisico. Non backup-friendly.

**Thin Provision**: è un formato che consente di risparmiare spazio di archiviazione. Si assegna allo spazio del datastore solo quanto il disco virtuale richiederebbe in base alla dimensione virtuale inserita. Il disco virtuale inizia piccolo e utilizza solo lo spazio del datastore necessario per le sue operazioni iniziali. Se il disco virtuale ha bisogno di più spazio in seguito, può crescere fino alla sua capacità massima e occupare tutto lo spazio del datastore assegnato. La thin provisioning è il metodo più veloce per creare un disco virtuale perché crea un disco solo con le informazioni dell'header. Non alloca o cancella blocchi di archiviazione. I blocchi di archiviazione vengono allocati e cancellati solo quando vengono utilizzati per la prima volta. Backup-friendly.

Immagine che contiene testo, schermata, Carattere, design

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, diagramma

Descrizione generata automaticamenteiSCSI (Internet Small Computer System Interface) è un protocollo di rete che consente di trasferire dati tra server e dispositivi di storage su una rete IP. In pratica, iSCSI consente di creare un dispositivo di storage virtuale all'interno della rete, rendendolo accessibile ai server come se fosse un dispositivo di storage locale. Ciò consente di sfruttare l'infrastruttura di rete esistente per trasferire i dati, senza dover utilizzare hardware costoso e specifico per la connessione tra server e dispositivi di storage. iSCSI può essere utilizzato per il backup, la replica dei dati e il clustering ad alta disponibilità.

Immagine che contiene testo, schermata, diagramma, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, diagramma, Piano, linea

Descrizione generata automaticamente