concorsi superiori

Concorso RIPAM

Presidenza del Consiglio dei Ministri

130 Specialisti

80 Settore scientifico-tecnologico

MANUALE di TEORIA e QUIZ per tutte le prove

NLD CONCORSI

2. ISO 20000: la gestione dei servizi IT

► 2.1 Posizionamento di ISO 20000 nel panorama degli standard

Mentre ISO 27001 e gli standard ISO 27000 si concentrano specificamente sulla sicurezza delle informazioni, ISO 20000 fornisce un framework per la gestione complessiva dei servizi IT. ISO 20000 è uno standard internazionale che specifica i requisiti per un service provider IT per pianificare, fornire, e migliorare continuamente i servizi IT che soddisfanno le esigenze dei clienti.
La differenza tra ISO 27001 e ISO 20000 è importante. ISO 27001 si concentra su "come proteggere le informazioni?". Esso fornisce un framework per implementare controlli di sicurezza che proteggono la confidenzialità, l'integrità, e la disponibilità delle informazioni. ISO 20000, d'altro canto, si concentra su "come fornire servizi IT di qualità?". Esso fornisce un framework per implementare processi che assicurano che i servizi IT sono forniti in modo affidabile, che i clienti sono soddisfatti, che i servizi sono disponibili quando necessario.
Tuttavia, c'è una sovrapposizione significativa tra i due standard. La sicurezza è un aspetto importante della qualità dei servizi IT. Un servizio IT che non è sicuro non è di qualità, perché mette a rischio i dati e i sistemi del cliente. Per questo motivo, ISO 20000 include requisiti per la gestione della sicurezza dei servizi IT, e una organizzazione che è conforme a ISO 20000 implementa anche molti dei controlli di sicurezza richiesti da ISO 27001.
Molte organizzazioni implementano sia ISO 27001 che ISO 20000 come standard di riferimento per la loro gestione della sicurezza e della qualità dei servizi IT. ISO 27001 fornisce il framework per la gestione della sicurezza, mentre ISO 20000 fornisce il framework per la gestione complessiva dei servizi.

► 2.2 Requisiti chiave di ISO 20000-1: un approccio processuale

ISO 20000-1 specifica i requisiti per un Sistema di Gestione dei Servizi IT (Service Management System). Come ISO 27001, è basato sul ciclo PDCA, enfatizzando il miglioramento continuo.
La struttura di ISO 20000-1 include diverse aree critiche che ogni service provider IT dovrebbe implementare:
Pianificazione dei Servizi IT: Questa è la fondazione di un buon service management. L'organizzazione deve pianificare i servizi IT che fornirà, inclusa la definizione chiara di cosa è il servizio, come sarà fornito, quale livello di qualità può essere aspettato. Parte di questa pianificazione è lo sviluppo di Service Level Agreements (SLA) - documenti che specificano il livello di servizio che il service provider si impegna a fornire. Un SLA potrebbe specificare, ad esempio, che il servizio sarà disponibile il 99.9% del tempo (permettendo solo 43 minuti di downtime al mese), che il tempo medio di risoluzione di un incident critico sarà di 1 ora, che il tempo medio di risoluzione di un incident non critico sarà di 8 ore. Queste metriche devono essere realistiche (ottenibili dal service provider) ma anche soddisfare le esigenze dei clienti. Se i clienti hanno bisogno di 99.99% di disponibilità ma il service provider può fornire solo 99.9%, c'è un disallineamento che porterà a insoddisfazione del cliente.
Gestione della Relazione con il Cliente: Fornire un servizio IT di qualità non significa solo assicurare che i sistemi funzionano correttamente. Significa anche gestire la relazione con il cliente, assicurare che il cliente è soddisfatto, capire le esigenze del cliente, comunicare efficacemente. Un aspetto importante della gestione della relazione è ottenere il feedback dal cliente sulla qualità del servizio e utilizzare questo feedback per migliorare il servizio.
Gestione della Capacità e della Disponibilità: Una organizzazione deve assicurare di avere la capacità (hardware, software, personale) di fornire i servizi ai livelli di servizio concordati. Questo richiede pianificazione della capacità (prevedere la domanda futura e pianificare gli investimenti di infrastruttura necessari) e monitoraggio continuo della capacità per identificare i colli di bottiglia. La disponibilità è strettamente legata alla capacità: se un sistema è sovraccarico, la sua disponibilità diminuisce. Un buon service provider monitora continuamente la disponibilità e agisce proattivamente per migliorarla.
Gestione della Continuità e del Disaster Recovery: Nel caso di un disastro (incendio, attacco informatico, perdita di dati), l'organizzazione deve avere un piano per ripristinare rapidamente i servizi

critici. Questo non è solo una questione di sicurezza (proteggersi dagli attacchi), ma anche di continuità di business (proteggersi da disastri naturali, guasti di hardware, ecc.). Un buon business continuity plan identifica i servizi critici, stima il tempo massimo accettabile di downtime (Recovery Time Objective - RTO) e la quantità massima di dati che l'organizzazione è disposta a perdere (Recovery Point Objective - RPO), e ha un piano per ripristinare questi servizi entro questi parametri. Questo potrebbe richiedere la replica dei dati a un'altra ubicazione geografica, la manutenzione di server di backup, la pratica regolare del ripristino per assicurare che il piano funziona effettivamente.

Gestione della Sicurezza dei Servizi: Come già menzionato, la sicurezza è un aspetto critico della gestione dei servizi IT. L'organizzazione deve implementare misure per proteggere i servizi IT da accessi non autorizzati, modifiche malintenzionate, o interruzioni. Questo include misure tecniche (crittografia, firewall, intrusion detection), misure procedurali (controllo dell'accesso, gestione delle configurazioni), e misure organizzative (policy di sicurezza, training dei dipendenti).

Gestione dei Cambiamenti: Quando un'organizzazione cambia qualcosa nella sua infrastruttura IT (ad esempio, aggiorna un server, implementa una nuova applicazione, cambia la configurazione di un firewall), il cambiamento potrebbe avere conseguenze indesiderate. Un cambiamento sconsiderato potrebbe causare un'interruzione di servizio, la perdita di dati, o l'introduzione di una vulnerabilità di sicurezza. Un buon change management process richiede che tutti i cambiamenti significativi siano formalmente richiesti, approvati, testati, e implementati in modo controllato. Un piano di rollback dovrebbe essere preparato nel caso il cambiamento cause problemi.

Gestione degli Incidenti: Un incidente è un evento che causa un'interruzione di servizio o una degradazione della qualità del servizio. Un incident management process assicura che gli incidenti sono rilevati rapidamente, segnalati, e risolti nel più breve tempo possibile. Un buon incident management process include la categorizzazione degli incidenti per gravità (critico, alto, medio, basso) e la definizione di tempi di risoluzione target (Service Level Indicators - SLI) per ogni categoria.

Gestione della Configurazione: Un'organizzazione deve mantenere un inventario accurato di tutti i componenti IT (server, applicazioni, database, dispositivi di rete) e delle relazioni tra di essi. Questo è noto come Configuration Management Database (CMDB). Il CMDB è utilizzato da molti altri processi di service management: quando si verifica un incidente, è importante conoscere quali altre componenti potrebbero essere colpite; quando si implementa un cambiamento, è importante conoscere tutte le componenti che potrebbero essere colpite dal cambiamento.

Misurazione e Reporting: Infine, un'organizzazione deve misurare il performance del servizio IT e rapportare i risultati ai clienti e alla dirigenza. Questo include la misurazione delle metriche definite negli SLA (ad esempio, la disponibilità, il tempo di risoluzione), nonché metriche aggiuntive che riflettono la qualità complessiva del servizio (ad esempio, la soddisfazione del cliente, la percentuale di incidenti risolti al primo contatto). I rapporti regolari sulla performance assicurano che sia il *service provider* che il cliente comprendano se il livello di servizio concordato è stato raggiunto e se ci sono aree che necessitano di miglioramento.

5. Le tutele previste dall'AI *Act*

Nel 2024 l'Unione Europea si è data un insieme di principi e norme nuove, complementari al quadro di tutele previste in materia di protezione dei dati personali, che si applicano allo sviluppo e all'implementazione di sistemi di intelligenza artificiale. Lo strumento normativo adottato è il Regolamento UE 2024/1689, che prende il nome di AI Act.
L'AI Act è stato concepito per imporre alle organizzazioni che usano sistemi di intelligenza artificiale requisiti e obblighi specifici in relazione ai vari impieghi di queste tecnologie. Le norme proposte intendono gestire i rischi derivanti da tali impieghi, vietare le pratiche che comportano rischi inaccettabili e identificare chiaramente le applicazioni considerate ad alto rischio, per le quali valgono obblighi *ad hoc*. L'approccio normativo adottato si basa su una valutazione del rischio articolata in quattro livelli: rischio inaccettabile, alto rischio, rischio limitato e rischio minimo.
I sistemi che determinano un rischio inaccettabile per i diritti e le libertà individuali sono proibiti (ad esempio, pratiche come il *social scoring* da parte di governi o pubbliche amministrazioni, la vendita di dispositivi dotati di assistenza vocale che promuovono comportamenti pericolosi, ecc).
I sistemi di intelligenza artificiale ad alto rischio includono tecnologie utilizzate in settori come le infrastrutture critiche, in cui può essere messa a rischio la vita e la salute dei cittadini, l'istruzione, in cui può essere condizionato l'accesso alla formazione, l'amministrazione della giustizia, la sicurezza (*safety*) dei prodotti. I sistemi ad alto rischio devono rispettare obblighi rigorosi prima della loro commercializzazione, tra i quali la selezione dei dati per prevenire risultati discriminatori, la tracciabilità dei risultati e la supervisione umana sui risultati. Inoltre, gli utenti devono ricevere informazioni chiare sul loro funzionamento.
La mancanza di trasparenza è invece considerata fonte di rischi limitati e induce obblighi specifici per garantire che gli utenti siano adeguatamente informati sul funzionamento dei sistemi con cui interagiscono. Ad esempio, quando si utilizzano sistemi come le chatbots, le persone devono essere consapevoli di interagire con una macchina, permettendo loro di decidere consapevolmente se continuare o meno l'interazione. Inoltre, i fornitori devono garantire che i contenuti generati da sistemi di intelligenza artificiale siano distinguibili da quelli generati dall'uomo. L'AI Act consente l'uso libero di sistemi a rischio minimo, come nei casi di videogiochi o filtri antispam.
L'adozione diffusa delle tecnologie di intelligenza artificiale, come visto, presenta rischi significativi per la privacy e i diritti riconosciuti alla persona. Le norme esistenti, tanto in materia di protezione dei dati quanto quelle di regolamentazione del mercato di nuova adozione avranno nei prossimi anni il compito di trovare un equilibrio tra esigenze diverse e di difficile composizione: da una parte garantire il rispetto di tali diritti, dall'altra promuovere un'innovazione tecnologica responsabile, etica e sostenibile per il beneficio della società nel suo complesso.

Sezione II - Quesiti situazionali relativi a problematiche tecniche nell'ambito dei progetti o processi di trasformazione digitale.

- **Sei il responsabile di un progetto di migrazione al cloud di alcuni servizi digitali di un'amministrazione comunale. Durante la fase di analisi emerge che gli uffici coinvolti hanno fornito informazioni incomplete sui dati trattati, sui livelli di criticità dei servizi e sulle integrazioni con altre piattaforme. Il fornitore propone di procedere comunque alla migrazione, rinviando le verifiche di dettaglio a una fase successiva, per rispettare la scadenza prevista dal cronoprogramma.**

	Più efficace	Risposta neutra	Meno efficace
A. Accetti la proposta del fornitore e autorizzi la migrazione, poiché il rispetto della scadenza è l'obiettivo prioritario del progetto.			
B. Convochi gli uffici interessati e il fornitore, completi la ricognizione dei dati, dei servizi e delle integrazioni, aggiorni il piano di migrazione e valuti eventuali impatti su tempi, rischi e responsabilità.			
C. Sospendi definitivamente il progetto, segnalando che l'incompletezza delle informazioni rende impossibile qualsiasi attività di trasformazione digitale.			
D. Lasci che sia il solo fornitore a classificare dati e servizi, poiché dispone delle competenze tecniche necessarie per decidere autonomamente la soluzione cloud più adeguata.			

Commento
La risposta **più efficace** è la **B**, perché consente di procedere in modo ordinato, completando la ricognizione preliminare e coinvolgendo gli uffici titolari delle informazioni e il fornitore. In una migrazione al cloud, dati trattati, criticità dei servizi e integrazioni devono essere valutati prima dell'avvio operativo.
La risposta **meno efficace** è la **A**, perché privilegia il rispetto formale della scadenza senza considerare i rischi tecnici e organizzativi di una migrazione fondata su informazioni incomplete.
Le risposte **C** e **D** sono **neutre**: la **C** coglie la gravità dell'incompletezza informativa, ma adotta una soluzione eccessiva e non proporzionata; la **D** valorizza la competenza tecnica del fornitore, ma gli attribuisce una decisione che deve restare presidiata dall'amministrazione.

- **Sei il referente operativo di un progetto di digitalizzazione dei servizi online di un ente locale. A pochi giorni dal rilascio, l'ufficio comunicazione segnala che alcune pagine del nuovo portale risultano poco comprensibili per gli utenti e che i cittadini potrebbero non capire quali documenti allegare alle istanze. Il team tecnico sostiene che il portale funziona correttamente e propone di andare comunque online, rinviando eventuali modifiche a una fase successiva.**

	Più efficace	Risposta neutra	Meno efficace
A. Procedi al rilascio senza modifiche, perché il funzionamento tecnico del portale è sufficiente a considerare concluso il progetto.			
B. Chiedi all'ufficio comunicazione di predisporre autonomamente una guida esterna al portale, senza coinvolgere il team tecnico.			