

Incident Management

Obiettivi

Obiettivo dell'Incident Management e' di ripristinare le normali operazioni di servizio nel piu' breve tempo possibile e con il minimo impatto sul business, garantendo il mantenimento dei livelli migliori di servizio.

Definizioni

Le seguenti definizioni sono usate nel processo di Incident Management:

- ✓ Un **incidente** e' qualsiasi evento che non fa parte dell'operativita' standard di un servizio e che causa, o puo' causare, un'interruzione e una riduzione della qualita' di tale servizio
- ✓ Un **workaround** e' una correzione temporanea ad un incidente o una sequenza di azioni alternativa a quella che produce l'incidente, utilizzabile dall'utente.

Responsabilità

Le responsabilità dell'Incident Management normalmente includono le seguenti:

- ✓ Registrazione degli Incidenti
- ✓ Classificazione e supporto iniziale degli Incidenti
- ✓ Anailisi dell'incidente e diagnosi
- ✓ Risoluzione e chiusura degli incidenti
- ✓ Comunicazioni con l'utente riguardo gli incidenti
- ✓ Ripristino dei normali livelli di servizio il prima possibile
- ✓ Verifica dell'aderenza ai criteri stipulati negli SLA

Attività

Input

Gli input alle funzioni effettuate dall'Incident Management includono le seguenti:

- ✓ Incident details
- ✓ CMDB (Configuration Management Database)
- ✓ KEDB (Known Error Database)
- ✓ Problem log
- ✓ FSC (Forward Schedule of changes)
- ✓ SLAs (Service Level Agreements)
- ✓ OLAs (Operating Level Agreements)
- ✓ Workarounds
- ✓ RFCs (Request for Change) implementate

Funzioni

Le funzioni effettuate dall'Incident Management includono le seguenti:

- ✓ Rilevamento e registrazione degli incidenti
- ✓ Classificazione e supporto iniziale
- ✓ Analisi dell'incidente e diagnosi
- ✓ Risoluzione e ripristino
- ✓ Chiusura dell'incidente
- ✓ Ownership, monitoraggio, tracciamento e comunicazione

Output

Gli output delle funzioni effettuate dall'Incident Management includono i seguenti:

- ✓ Chiusura degli incidenti
- ✓ Aggiornamento delle informazioni relative agli incidenti
- ✓ Reports per il management
- ✓ Identificazione di Problemi relativi all'infrastruttura
- ✓ Controllo dei dati sul CMDB
- ✓ Creazione di nuovi workaround (normalmente sono un prodotto del processo di problem management, pero' occasionalmente sono prodotti durante il processo di risoluzione degli incidenti)
- ✓ Informazioni su eventuali incidenti che non sono stati risolti secondo i criteri stipulati negli SLA (SLA Breaches)

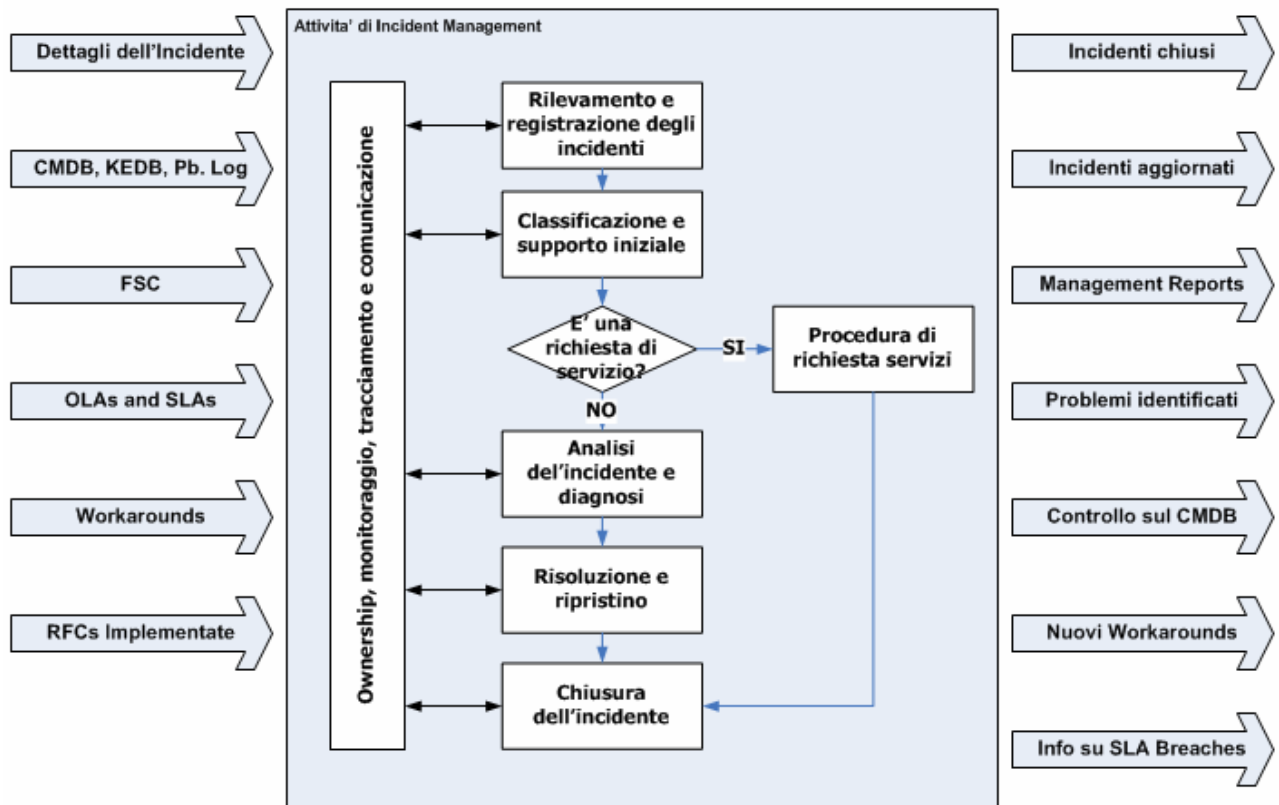


Figura 1 - Attivita' dell'Incident Management

Concetti

Relazione tra Incidenti, Problemi e Known errors

L'incidente è, normalmente, il risultato di un malfunzionamento di una parte dell'infrastruttura IT. In molti casi le cause possono essere ovvie e facilmente risolvibili con un workaround (per esempio riavviando il computer) oppure con un rapido cambiamento (per esempio un reset della password). In altri casi le cause possono essere ignote ed ha senso quindi creare un 'problema', che indichi che vi è una 'causa ignota' per uno o più incidenti che valga la pena analizzare più in profondità. Il processo di problem management si occupa di determinare le cause dei problemi. Non appena la causa del problema è nota ed una RFC (Request For Change o richiesta di cambiamento) viene creata per rettificare la situazione, oppure un workaround è disponibile, il problema viene marcato come 'known error' (errore noto).

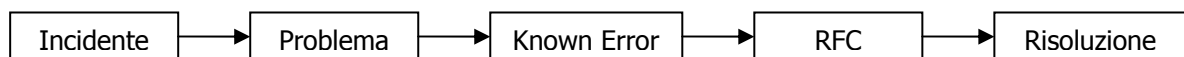


Figura 2 - Relazione tra incidenti, problemi e known errors

Incidenti significativi

In alcuni casi alcuni incidenti possono essere di una gravità tale che, a causa degli effetti negativi che hanno sul business, ha senso tralasciare le procedure standard e fare intervenire le persone che possano essere utili a risolvere l'incidente nel modo più rapido possibile, tra le quali anche problem management.

Riferimento ad altri gruppi di supporto (1° livello, 2° livello, etc...)

Oltre al gruppo di Service Desk, spesso ci sono altri gruppi di supporto, più specialistici, che hanno un ruolo nel processo di incident management.

Se un incidente non può essere risolto dal 1° livello di supporto perché richiede competenze specialistiche, può essere riferito a gruppi specialistici di 2° livello (e a sua volta a gruppi di 3° livello, etc...). Questo tipo di riassetto è definito funzionale, in quanto si basa sulle competenze e sulle funzioni.

Esiste anche un altro tipo di riassetto, definito gerarchico, che avviene quando un incidente non viene risolto in tempo, e viene riferito al manager del gruppo in questione.

Priorità

La priorità di un incidente deve essere determinata in un modo il più obiettivo possibile. Un metodo utile può essere quello di basarla sull'urgenza e sull'impatto di un incidente.

L'urgenza è una valutazione della rapidità con cui un incidente va risolto (entro quanto l'incidente va risolto).

L'impatto è una misura degli effetti che l'incidente ha sul business (quante e quali persone o processi aziendali ne risentono). La valutazione dell'impatto può essere valutata in base ai dati presenti sul CMDB (quali sono le relazioni che il componente che non funziona ha con altri componenti?).

La priorità può essere basata sulla combinazione delle due informazioni.

		<i>Impatto</i>		
		Alto	Medio	Basso
<i>Urgenza</i>	Alta	1	2	3
	Media	2	3	4
	Bassa	3	4	5

Figura 3 - Matrice delle priorità

Benefici

I benefici dell'Incident Management includono i seguenti:

- ✓ Riduzione dell'impatto negativo al business degli incidenti grazie ad una più rapida risoluzione
- ✓ Migliore utilizzo del personale, che si concentra sugli incidenti, migliorandone le prestazioni e l'efficienza
- ✓ Miglioramento della soddisfazione degli utenti
- ✓ Informazioni più accurate nel CMDB, in quanto vengono verificate continuamente a seguito dell'analisi degli incidenti
- ✓ Disponibilità di dati aziendali sugli incidenti (e sulla risoluzione di essi)
- ✓ Eliminazione degli incidenti e delle richieste di servizio perse

Possibili Problemi

I possibili problemi nell'implementazione del processo di Incident Management includono i seguenti:

- ✓ Mancanza di impegno da parte del management
- ✓ Mancanza di risorse sufficienti ad occuparsi degli incidenti
- ✓ Mancanza di competenze adeguate per la risoluzione degli incidenti
- ✓ Mancanza di strumenti adeguati (software o altro)
- ✓ Mancanza di conoscenza del processo da parte dei tecnici e/o degli utenti
- ✓ Mancanza di interazione con altri processi (Problem management per il KEDB, Configuration Management per il CMDB, etc...)
- ✓ Resistenza al cambiamento
- ✓ Mancanza di chiarezza sulle necessità del business
- ✓ Utenti e tecnici IT che bypassano il processo

Relazioni

L'Incident Management si relaziona con i seguenti processi/funzioni:

- ✓ Service Desk
 - Il Service Desk e' il punto di contatto per gli utenti che segnalano incidenti nell'utilizzo dei servizi IT
 - Il Service Desk fornisce una valutazione iniziale degli incidenti
 - Il Service Desk svolge attività di coordinamento e comunicazione rispetto al processo di Incident Management
 - Il Service Desk produce reports sul processo di Incident Management
- ✓ Problem Management
 - L'Incident Management utilizza il Problem log (la lista di problemi) gestita dal Problem Management
 - L'Incident Management utilizza il KEDB (Known Error Database) gestito dal Problem Management
 - L'incident management può rendersi conto di problemi all'infrastruttura e fornire le informazioni al Problem Management
 - L'incident management può sviluppare workarounds a problemi noti nel processo di risoluzione degli incidenti, e può passarli al Problem Management perché siano registrati nel KEDB
 - L'incident management genera informazioni che possono essere utilizzati dal problem management per la determinazione proattiva di problemi nell'infrastruttura.
- ✓ Configuration Management

- L'incident management utilizza i dati del CMDB nel processi di analisi degli incidenti. Può fornire feedback al Configuration Management se i dati presenti nel CMDB non sono accurati.
- ✓ Change Management
 - L'incident management utilizza le informazioni sulle RFC (Request for Change) implementate come indizi sulle possibili cause di incidenti
- ✓ Service Level Management
 - Il processo di incident management utilizza gli SLA (prodotti dal Service Level Management) per determinare i livelli di servizio da fornire agli utenti

Implementazione

Fattori Critici di Successo

I fattori critici di successo nell'implementazione dell'Incident Management includono i seguenti:

- ✓ Un CMDB aggiornato. Se il CMDB non è aggiornato la determinazione dell'impatto e dell'urgenza della soluzione diventa molto lenta e difficile.
- ✓ Strumenti software adeguati per la gestione degli incidenti. I processi manuali/cartacei sono ragionevoli solo per implementazioni molto ridotte, ed impossibili per implementazioni che includono più gruppi di lavoro.
- ✓ Una 'knowledge base', che comprenda al minimo:
 - Il Known Error Database
 - La lista dei problemi nell'infrastruttura
 - Uno storico degli incidenti risolti nel passato
 - Documentazione tecnica
- ✓ Una stretta connessione con il processo di Service Level Management per determinare le deadline per la risoluzione per ogni tipo di incidente.

Costi

I costi necessari per implementare e gestire il processo di Incident Management possono includere i seguenti:

- ✓ Costo del personale che lavora nell'incident management, sia come costo iniziale (costi di assunzione, etc..) che operativo (stipendi, etc...).
- ✓ Costo dei locali utilizzati per l'incident management, sia iniziali (arredamento, etc...) che operativi (affitto, luce, telefono, etc...)
- ✓ Costo degli strumenti software di gestione dell'incident management, sia iniziali (acquisto licenze software, etc...) che operativi (costi di assistenza, etc...)
- ✓ Costo dell'Hardware a supporto dell'incident management, principalmente come costo iniziale (acquisto e messa in opera) ma con possibile elementi di costo operativo (contratti di assistenza, etc...)
- ✓ Costi del training, sia iniziali (training iniziale, etc...) che operativi (corsi di perfezionamento, etc...)

- ✓ Costi per consulenza esterne, normalmente iniziali, per il set up dei processi, ma a volte anche operativi, nell'ottica di un miglioramento continuo dei processi

Metriche

Alcune metriche che possono essere utili per misurare le performance dei processi di Incident Management sono le seguenti:

- ✓ % di incidenti risolti al primo livello di supporto (non sono stati scalati) al mese, per misurare la bontà della knowledge base;
- ✓ % di incidenti risolti al momento del contatto, per misurare l'aderenza dell'incident management alla situazione ideale, cioè di poter risolvere tutte le chiamate "al volo";
- ✓ % di incidenti assegnati in modo non corretto al mese, per misurare la bontà dei processi di assegnamento;
- ✓ % di incidenti risolti nei livelli di servizio stipulati (SLAs) al mese, per misurare la capacità di risolvere gli incidenti secondo i livelli di servizio stipulati;
- ✓ tempo medio di risoluzione degli incidenti al mese, per misurare la bontà e l'efficienza del processo di incident management in generale;
- ✓ % di incidenti con categorizzazione non corretta al mese, per misurare l'accuratezza e l'utilizzabilità dei dati prodotti dall'incident management.
- ✓ % di richieste di servizio rispetto agli incidenti al mese, per misurare la maturità del servizio. Col tempo, gli incidenti dovrebbero diminuire e le richieste di servizio aumentare.
- ✓ % di incidenti risolti correttamente al primo tentativo, al mese, per misurare l'efficienza del processo.