Corso di Amministrazione di Sistema
Parte I – ITIL 4

Francesco Clabot

Responsabile erogazione servizi tecnici

francesco.clabot@netcom-srl.it

Fondamenti di ITIL per la “Gestione dei Servizi Informatici”

IT Incident Management

IT Incident Management

Poiché l'IT Service Management è orientato all'erogazione di predeterminati livelli di servizio agli utenti finali, è importante creare un'organizzazione le cui direttive fondamentali siano:

- Monitorare l'ambiente IT in conformità con i suddetti livelli di servizio e scalare propriamente gli incidenti che si verificano nell'erogazione del servizio
- La funzione di IM ha la responsabilità di risolvere gli incidenti più in fretta possibile

Quando un utente incontra un incidente, il processo di IM farà sì che il servizio all'utente ritorni disponibile il prima possibile.

IT Incident Management: Obiettivi

I principali obiettivi sono:

- Risolvere gli incidenti del servizio prima possibile, o almeno entro il tempo stabilito nello SLA
- Mantenere un flusso costante di informazioni tra l'organizzazione IT e il suo cliente riguardo lo stato di un incidente (es. escalation, tempo stimato di risoluzione, etc.)
- Valutare un incidente per stabilire se è probabile che si ripresenti o se è sintomo di un problema cronico: in tal caso informare il PM a riguardo.

IT Incident Management: Responsabilità

Sono:

IT Incident Management: Responsabilità

Individuazione e registrazione di un incidente:

- Il SD è responsabile della registrazione e del monitoraggio della risoluzione di tutti gli incidenti; questo è un processo estremamente reattivo.
- Per consentire una reazione efficiente ed efficace deve essere implementato un metodo di lavoro formale. Essi tracciano i dettagli di base dell'Incidente, allertano i gruppi di supporto specializzato nella misura necessaria e danno avvio alle procedure per gestire la richiesta di servizio.

IT Incident Management: Responsabilità

Classificazione di tutti gli incidenti e supporto iniziale:

- Questo è il processo di identificazione delle ragioni che hanno portato all'incidente e di conseguenza della relativa azione risolutiva.
- In questo caso il CMDB può essere consultato per controllare l'esistenza di known errors e problemi; una valutazione dell'impatto e dell'urgenza deve essere fatta per poter definire la priorità e deve essere fornito un supporto iniziale.
- Tipicamente il supporto iniziale consiste nel fornire un work around.

IT Incident Management: Responsabilità

Investigazione e diagnosi:

- Dopo una valutazione iniziale di un incidente, vengono raccolte e analizzate ulteriori informazioni.
- L'investigazione e l'individuazione possono diventare un processo iterativo, iniziando con vari gruppi di supporto specializzato e proseguendo con la definitiva eliminazione della possibile causa.
- Ciò può coinvolgere un supporto distribuito o anche vendor esterni.
- Questo richiede rigore e un approccio disciplinato oltre a una dettagliata attività di registrazione delle azioni intraprese e dei corrispettivi risultati.

IT Incident Management: Responsabilità

Risoluzione e ripristino:

- L’incidente è stato risolto o aggirato con successo oppure viene creata una RFC.

IT Incident Management: Responsabilità

Chiusura di un incidente:

- Questa può avvenire una volta che l'utente è soddisfatto riguardo la risoluzione o il workaround.
- Il Service Desk garantisce che:
  - I dettagli sulle azioni intraprese per risolvere l'incidente siano concisi e leggibili
  - La classificazione è completa e accurata in base alla causa di origine
  - La risoluzione è concordata con il cliente/utente
  - Tutti i dettagli applicabili a questo incidente vengono registrati

IT Incident Management: Responsabilità

Incident control:

- Ne parliamo successivamente, nella parte dove si descrive il Life Cycle dell'Incidente

IT Incident Management: Terminologia

Incidente:

- Ogni evento che non rientra nel servizio concordato è chiamato incidente.
- Interruzione del servizio o riduzione del servizio.
- E se l'incidente è in arrivo?

Workaround:

- E' un metodo per aggirare l'incidente o un problema con l'utilizzo di una fix temporanea.
- E' solitamente la prima soluzione di ripristino del servizio.
- Non è una soluzione definitiva, ma un espediente per mantenere il servizio "up and running"
- Solitamente riduce il servizio.

IT Incident Management: Terminologia

Service Request:

- Può essere pensato come un incidente che non è dovuto ad un malfunzionamento dell'infrastruttura IT.
- Può essere una richiesta di informazioni (es. l'utente non sa come si utilizza una certa funzionalità di un applicativo) o una change request (es. richiesta di cambio password) legata ad uno dei servizi che si stanno erogando.

Il processo di Incident Management

Input:

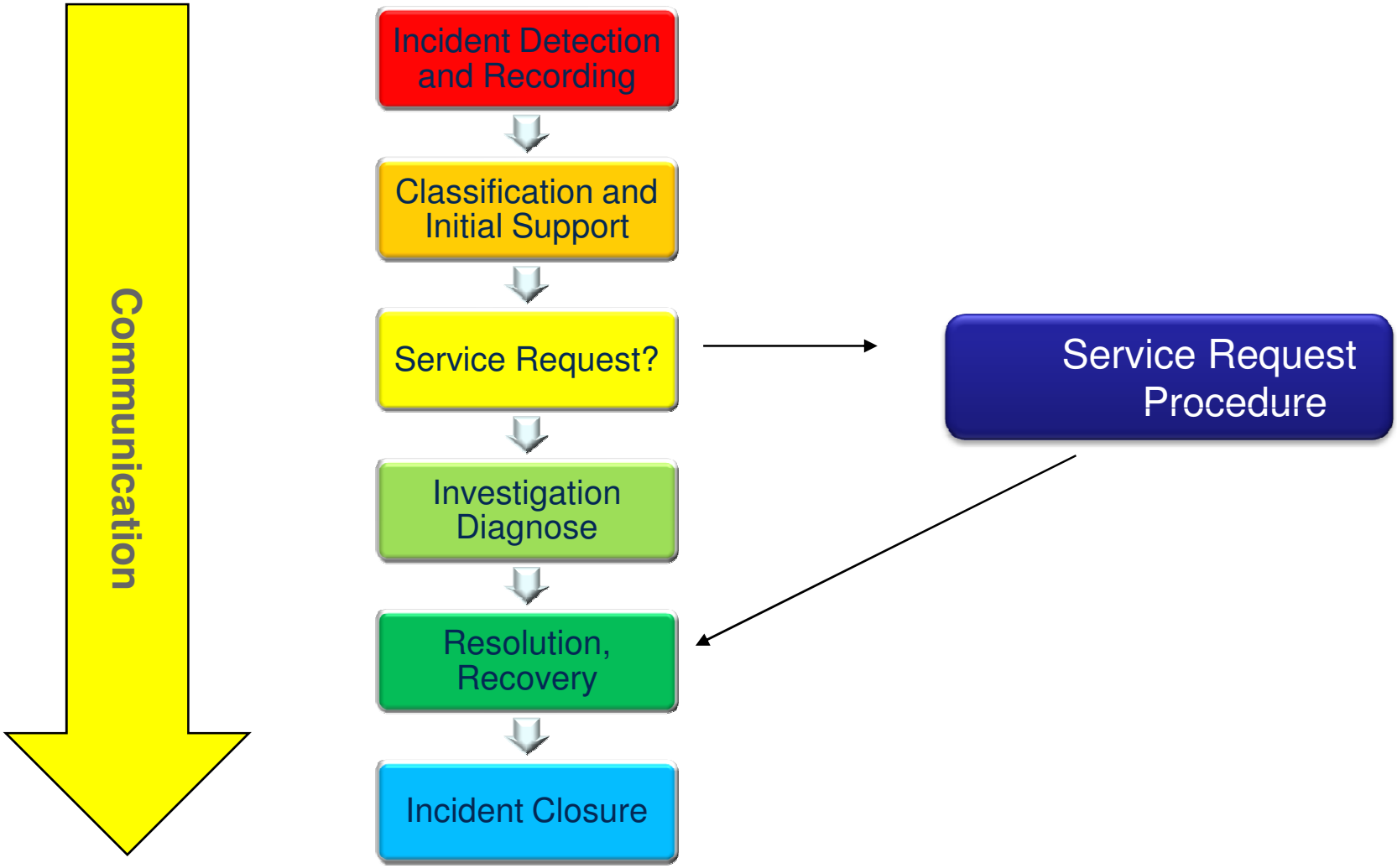
- Dettagli sull'incidente, forniti da più fonti
- Dettagli sulla Configurazione dal CMDB
- Esiti dei riscontri fatti fra incidente e problemi o known errors (Incident Matching)
- Dettagli sulla risoluzione
- Risposte a fronte di RFC

Il processo di Incident Management

Ouput:

- RFC per la risoluzione di un incidente; record sull'incidente aggiornato (inclusa soluzione e/o workaround)
- Incidenti risolti e chiusi
- Comunicazione ai clienti
- Informazione al management (reports)

Incident Life Cycle



Incident Life Cycle

Incident Detection and Recording:

- Tracciare l'incidente durante tutto il suo ciclo di vita
- Aggiungere utili informazioni che possono aiutare le organizzazioni di supporto a trovare una soluzione
- Registrare informazioni storiche per futuro utilizzo
- Raccogliere informazioni (es. per i reports)

Incident Life Cycle

Classification and Initial Support:

- L'SD determina la priorità degli incidenti appena li riceve
- Assegna una priorità in base all'impatto ed all'urgenza
- Viene assegnata una categoria alla chiamata (es. HW, SW) e l'operatore dell'SD procede con l'incident matching
- La consultazione del CMDB è necessaria per ottenere info riguardo il servizio che ha subito interruzione, i dati dell'SLA, i CIs legati al servizio, eventuali incidenti passati correlati, known errors e record di change

Incident Life Cycle

Service Request o Incident?:

- Se la chiamata è una SR l'operatore del SD segue una appropriata procedura di SR.
- Se è un incidente, dopo aver fornito un supporto iniziale, dovrà risolverlo o inoltrarlo al supporto di livello superiore per ulteriori investigazioni.

Incident Life Cycle

Investigation, Diagnose:

- Altri gruppi di supporto inizieranno ad analizzare l'incidente con l'unico scopo di trovare una soluzione permanente oppure, se ciò non fosse possibile, un workaround.

Incident Life Cycle

Resolution, Recovery:

- Dopo che la risoluzione od il workaround hanno avuto buon esito, può iniziare il ripristino del servizio, spesso svolto da uno staff specializzato (supporto di 2 e 3 livello).
- Il sistema di IM deve registrare eventi ed azioni intraprese durante la risoluzione ed il ripristino.

Incident Life Cycle

Incident Closure:

- Se viene trovate una soluzione permanente o un workaround, questi vengono implementati ed il servizio ripristinato. Il team che ha trovato la soluzione informerà l'SD che farà da intermediario con il cliente per verificare che la soluzione/workaround sia soddisfacente.
- In tal caso il SD potrà chiudere l'incidente.

Incident Life Cycle

- Nel corso di tutto il processo, l'IM ha la responsabilità di tracciare e monitorare i progressi e la qualità, oltre a fornire reports.
- Nella maggior parte dei casi il ruolo di Incident Manager sarà rivestito dal SD Manager.
- Il SD ha anche la responsabilità di tenere utente/cliente continuamente informati riguardo i progressi della chiamata.

Incident Management: Classificazione

PRIORITA':

- Il SD determina la priorità degli incidenti non appena li riceve.
- La priorità viene stabilita in base ai criteri descritti nello SLA.
- La priorità si calcola in base all'impatto ed all'urgenza.

- **IMPATTO:** effetto che l'incidente ha sulle attività del business
- **URGENZA:** velocità con cui l'incidente deve essere risolto

Incident Management: Classificazione

Nel determinare la priorità si deve considerare:

- I costi potenziali della non risoluzione
- La minaccia di danno per i clienti e per lo staff
- Le implicazioni legali
- Il “disturbo” arrecato ai clienti ed allo staff

- L’impatto non riguarda la complessità tecnica della risoluzione.

Incident Management: Priorità

- Se si assegna subito la priorità della chiamata, il supporto di 2 livello può ottimizzare il suo funzionamento.
- La priorità non consiste solo nel mettere in code gli incidenti, riguarda anche le risorse che saranno allocate per la risoluzione (tempo, staff, esperienza, ricerca, etc.)
- In pratica, può capitare che un incidente a bassa priorità venga risolto oltre il tempo target in modo da permettere ad un altro a priorità maggiore di essere risolto entro il tempo prestabilito.

Incident Management: Classificazione

CATEGORIZZAZIONE:

- Può fare muovere un primo passo verso la definizione.
- E' necessario che IM e PM utilizzino un linguaggio comune per la categorizzazione.
- 2 tipi di categorie: registrare gli incidenti riportati (linguaggio dell'utente) – registrare le cause finali individuate (linguaggio tecnico).
- Se fatta bene può rivelare una tendenza (trend) e condurre all'identificazione di aree specifiche di problemi che necessitano di ulteriore investigazione.

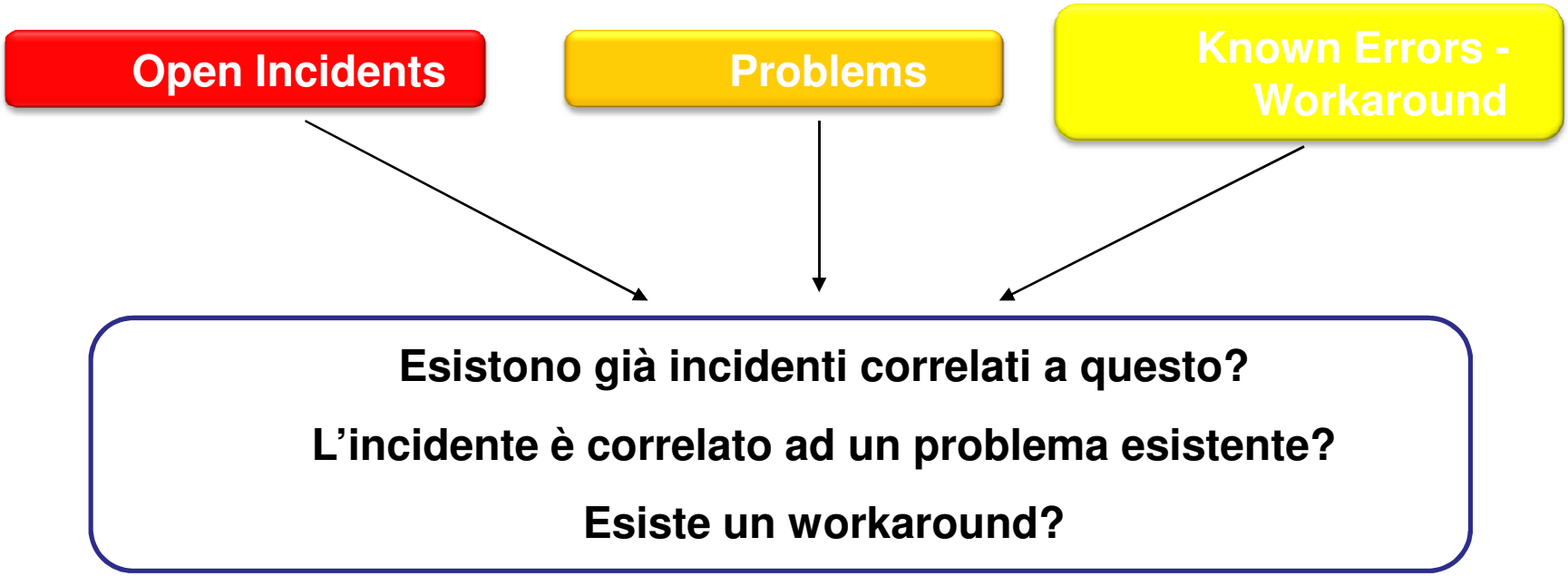
Incident Management: Categorizzazione

Esempi di categorie:

- Application:
  - Servizio non disponibile
  - Bug di applicazione
- Hardware:
  - Un'alert automatico
  - Una stampante che non stampa
- Service Request:
  - Password dimenticata
- Security Incident:
  - Virus

Incident Management: Classificazione

MATCHING:

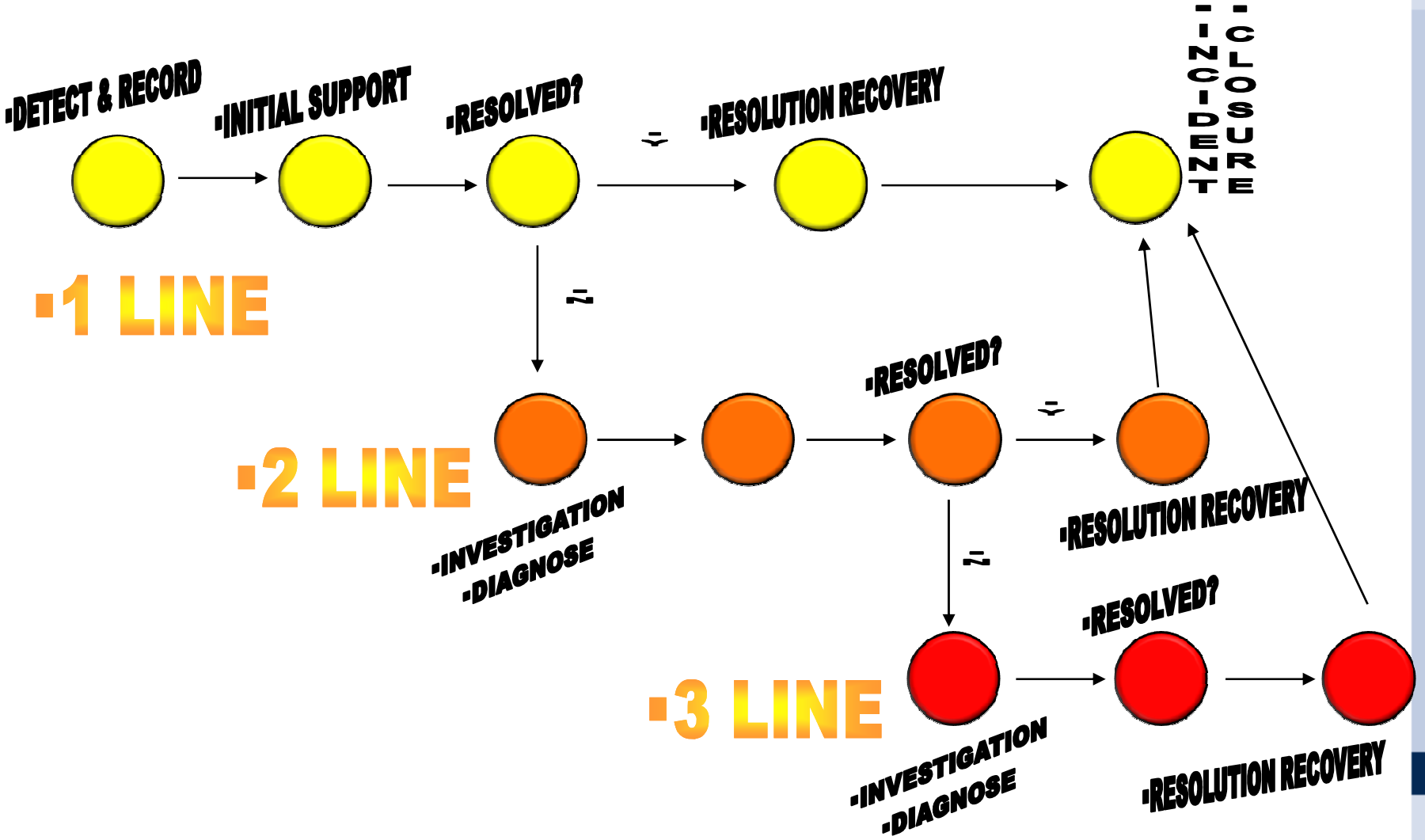


Incident Management: Classificazione

MATCHING:

- Un utente contatta il SD perché non gli funziona la posta elettronica
- Altri utenti chiamano con lo stesso problema
- Gli incidenti vanno messi in relazione
- Se l'incidente non trova un match allora è da considerarsi come un incident unico e deve essere registrato come tale.

Routing degli incidenti



Routing degli incidenti

- Il SD, in qualità di owner di tutti gli incidenti, deve coordinare il processo di Incident Management.
- Se vi sono discordanze di opinioni, il SD deve scalare il problema al PM.
- Da notare che il 2 e 3 livello di supporto possono comprendere anche fornitori esterni ai quali può essere dato accesso al tool di registrazione degli incidenti.

Escalation & Referral

- L'incident routing è chiamato escalation orizzontale o referral ed ha luogo principalmente quando non ci sono la conoscenza o l'esperienza necessarie. Quando si fa un referral di un incidente, il SD deve fare attenzione a non superare i tempi di risoluzione indicati nello SLA.
- L'escalation gerarchica o verticale può verificarsi in ogni momento durante l'ILC. Di solito avviene quando vengono riportati incidenti di grossa entità o quando diventa evidente che non si potranno rispettare gli SLA di risoluzione. Questo permette all'autorità competente di intraprendere le dovute azioni correttive.
- Hierarchical Escalation = Inform / Support
- Functional Escalation = Knowledge

Escalation & Referral

- L'Escalation ed il Referral non fanno MAI trasformare un incidente in un problema, anche quando l'ownership di un incidente parla al PM per ragioni amministrative, ed il PM dovesse procedere all'identificazione di un problema associato.
- I problemi NON sono incidenti seri.

Sommario

Obiettivi

- Ripristinare il servizio minimizzando l'impatto
- Garantire il rispetto degli SLA

Responsabilità

- Individuazione e tracciamento degli incidenti
- Classificazione e supporto iniziale
- Investigazione e diagnosi
- Risoluzione e ripristino, chiusura dell'incidente
- Incident Control
- Incident ownership, monitoraggio, tracciamento e comunicazione