|  |  |  |
| --- | --- | --- |
| TITOLO: Gestione degli Incidenti IT | | |
| Gestione | Funzione | Riferimento |
| REDATTO: | Progetti Speciali di Gruppo - Information Technology - Governance - Process & Procedures Design | Paola Celletti |
| VERIFICATO: | Progetti Speciali di Gruppo - Information Technology - Governance - Process & Procedures Design  Progetti Speciali di Gruppo - Information Technology - IT  Infrastructure - Control Room & Technical Management  Progetti Speciali di Gruppo - Information Technology - IT  Infrastructure - Service Management  Progetti Speciali di Gruppo - Information Technology  Application Development & Management – Integration & Testing – Industrial Monitoring & Tools  Security - Enterprise Risk Management & Process and Monitoring - Enterprise Risk Management & Business Continuity  Security - Enterprise Risk Management & Process and Monitoring - Enterprise Risk Management & Business Continuity  Security - Cyber Security  Administration, Finance & Control - Planning & Control and Revenue Assurance -  Planning & Control Business Units and Revenue Assurance  Technology - Processess & Service Creation - Processes & Procedures Design  Human Resources & Organizational Development - Organization & Processes - Business Process Framework | Ivo Della Valle  Alberto Chiesa  Stefano Santi  Antonio Di Bari  Domenico Fumai  Carlo Renato Gaspare Casertano  Fabio Zamparelli  Pierpaolo Taccini  Paolo Ravera  Giampiero Camporesi |
| APPROVATO: | Progetti Speciali di Gruppo - Information Technology - Application Development & Management  Progetti Speciali di Gruppo - Information Technology - IT Infrastructure  Progetti Speciali di Gruppo - Information Technology  Governance - Process & Procedures Design | Stefano Gigli  Carmine D'Acierno  Giampiero Mucci |
| N° allegati: |  |  |
| *Il presente documento è stato redatto in coerenza con il Codice Etico e di Condotta ed*  *il Modello Organizzativo 231 del Gruppo Telecom Italia* | | |

**REGISTRO DELLE MODIFICHE**

|  |  |  |
| --- | --- | --- |
| **N° Rev.** | **Descrizione** | **Data emissione** |
| 1 | Prima emissione a seguito della modellazione del processo in esame nella piattaforma di Business Process Management Tommy.  Il documento sostituisce la procedura "2015-00104 Gestione degli Incidenti", v 1 del 06/05/2015 (Codice TIIT: TIIT\_SGI\_PRO\_P105) | 18/12/2015 |
| 2 | Seconda emissione.  Il documento sostituisce la Procedura Operativa "2015-00229 Gestione degli Incidenti IT", v 1 del 18/12/2015 (Codice TIIT: TIIT\_SGI\_PRO\_P105) che risulta, dunque, superata.  Rispetto alla versione precedente sono stati apportati gli aggiornamenti utili per l'adeguamento a:  \* la nuova Classificazione dei "Major Incident";  \* la nuova struttura organizzativa TIM;  \* la Procedura Organizzativa "Comunicazione Eventi Rilevanti".  Non sono state apportate ulteriori modifiche a seguito di normative vigenti. | 07/03/2017 |

**INDICE**

[1. PREMESSA 5](#_Toc256000000)

[2. DESTINATARI 5](#_Toc256000001)

[3. SCOPO E CAMPO DI APPLICAZIONE 5](#_Toc256000002)

[4. RIFERIMENTI 6](#_Toc256000003)

[5. DESCRIZIONE PROCESSO E RESPONSABILITÀ 7](#_Toc256000004)

[5.1. Scopo e descrizione breve del processo 7](#_Toc256000005)

[5.2. Input/output e fornitori/clienti del processo 8](#_Toc256000006)

[5.3. Obiettivi (KPO / KPI / SLA) 8](#_Toc256000007)

[5.4. Vincoli sul processo 8](#_Toc256000008)

[5.5. Gestione degli Incidenti IT 9](#_Toc256000009)

[5.5.1. Contesto del processo 9](#_Toc256000010)

[5.5.2. Flow del processo 10](#_Toc256000011)

[5.5.3. Attività del processo 11](#_Toc256000012)

[5.5.3.1. 01 / Analisi tipologia segnalazione/ticket 11](#_Toc256000013)

[5.5.3.2. 02 / Classificazione Incidente 12](#_Toc256000014)

[5.5.3.3. 03 / Escalation 15](#_Toc256000015)

[5.5.3.4. 04 / Analisi Incidente 16](#_Toc256000016)

[5.5.3.5. 05 / Riassegnazione Ticket ad altro Gruppo Risolutore 17](#_Toc256000017)

[5.5.3.6. 06 / Registrazione Problema 17](#_Toc256000018)

[5.5.3.7. 07 / Risoluzione Incidente 18](#_Toc256000019)

[5.5.3.8. 08 / Certificazione intervento (incidente) 19](#_Toc256000020)

[5.5.3.9. 09 / Chiusura Incidente (ticket) 19](#_Toc256000021)

[5.5.3.10. 10 / Valutazione Incidenti 20](#_Toc256000022)

[5.5.4. Matrice RACI delle attività/attori del processo 22](#_Toc256000023)

[6. GLOSSARIO 24](#_Toc256000024)

# PREMESSA

La presente Procedura Operativa descrive il processo di “Gestione degli Incidenti” attuato nell'ambito della funzione IT di TIM.

Il documento sostituisce la procedura "2015 - 00229 Gestione degli Incidenti IT”, v 1 del 18/12/2015 (Codice TIIT: TIIT\_SGI\_PRO\_P105).

Rispetto alla versione precedente sono stati apportati gli aggiornamenti utili per l'adeguamento a:

* la nuova Classificazione dei "Major Incident".
* la nuova struttura organizzativa TIM;
* la Procedura Organizzativa "Comunicazione Eventi Rilevanti" (nuova versione della Procedura Organizzativa "Comunicazione Trasversale degli Eventi classificati Critici" Cod. 2015-00130);

Il processo in esame si correla ai seguenti processi TIM:

* Comunicazione Eventi Rilevanti
* Gestione eventi di Sicurezza Informatica

Tutte le precedenti versioni e documentazioni di riferimento sono reperibili sul Sistema Documentale Integrato dei Processi della funzione IT di TIM (consultabile sulla intranet TIM IT alla voce SDIP). La versione precedente della procedura è pubblicata anche sul Sistema Documentale Integrato (SDI) di TIM.

# DESTINATARI

La Procedura Operativa si applica alla funzione IT di TIM ed ha validità aziendale.

# SCOPO E CAMPO DI APPLICAZIONE

Lo scopo della presente Procedura Operativa è di definire la sequenza di attività e le responsabilità per la Gestione degli Incidenti IT.

Per **Incidente** si intende un evento non pianificato che causa una interruzione del servizio, oppure una riduzione della qualità del servizio. Anche un malfunzionamento di un configuration item che non ha ancora impattato il servizio è un incidente (ITIL v3).

Nel caso di incidente, finalità del processo è assicurare il ripristino del servizio il più rapidamente possibile, in modo coerente con quanto previsto dagli accordi di servizio.

La presente procedura, per completezza, comprende la gestione degli incidenti di sicurezza riscontrati nei Data Center al fine di proteggere i processi operativi ed il patrimonio informativo in accordo con la Politica della Sicurezza definita nel Manuale Integrato ed in conformità allo standard ISO 27001 e alle Linee Guida di Gruppo (vedi Linee Guida di Gruppo per la gestione degli incidenti ICT).

Rientrano nel campo di applicabilità della procedura di Gestione degli Incidenti IT:

· Incidenti di Servizio IT (di natura applicativa/infrastrutturale/gestionale);

· Reclami specifici;

· Incidenti di Sicurezza dei Data Center.

Per l’elenco dettagliato dei Servizi IT si faccia riferimento al Catalogo Servizi Base (rif. TIIT\_SGI\_CAT\_002) ed al Catalogo Servizi Telecom Specifiche Tecniche (rif. TIIT\_SGI\_CAT\_003\_ST).

Le segnalazioni provenienti da Utenti, Service Desk, ecc. sono preventivamente filtrate dal processo di "Gestione Operativa dei Servizi IT" (rif.: Cod. 2015 -00225) e, da quest'ultimo, sono inoltrate al processo di "Gestione degli Incidenti IT" le segnalazioni che riguardano le anomalie del servizio.

Non rientrano nel campo di applicabilità della procedura gli incidenti su aree applicative non in carico, in altre parole non riportate nell’elenco delle applicazioni gestite, censite nel Catalogo ITMC, e gli incidenti che occorrono su aree non in ambito di competenza di IT Infrastructure.

Per la gestione degli incidenti e/o situazioni di emergenza di carattere ambientale fare riferimento a quanto riportato nella Procedura Operativa "Gestione delle emergenze relative all'Ambiente" (rif.: TIIT\_SGI\_PRO\_P436).

# RIFERIMENTI

[1] Cod. 2016-00125 - Definizione del Budget/Forecast e del Piano delle Commesse

[2] Cod. 2015-00080 - Controllo dei Prodotti Non Conformi

[3] Cod. 2016-00073 - Gestione della Configurazione IT

[4] Cod. 2016-00005 - Azioni Correttive, Preventive e Migliorative

[5] Cod. 2016-00196 - Gestione dei Problemi

[6] Cod. 2015-00225 - Gestione Operativa dei Servizi IT

[7] Cod. 2015-00082 - Gestione dei Rilasci

[8] Cod. 2016-00084 - Gestione dei Cambiamenti IT

[9] TIIT\_SGI\_PRO\_ P206 - Operations Data Center

[10] Cod. 2016-00015 - Service Management

[11] Cod. 2016-00239 - Program Management Integrato IT

[12] TIIT\_SGI\_PRO\_P414 - Progettazione, Realizzazione e Delivery del Servizio

[13] Cod. 2016-00259 - Incidenti con Disservizio

[14] Cod. 2016-00069 - One Minute Escalation

[15] TIIT\_SGI\_QIO\_P105\_D - Istruzione Operativa per la Gestione delle Issue in ambito TIIT con impatti sui ricavi di TI

[16] TIIT\_SGI\_CAT\_002 - Catalogo Servizi Base

[17] TIIT\_SGI\_CAT\_003\_ST - Catalogo Servizi Telecom Specifiche Tecniche

[18] TIIT\_SGI\_TMP\_IRP - Report Incidente DC

[19] TIIT\_SGI\_TMP\_RIN - Registro Incidenti di Servizio

[20] TIIT\_SGI\_TMP\_SP - Scheda Problem

[21] TIIT\_SGI\_TMP\_TCK - Incidente

[22] TIIT\_SGI\_PRO\_P436 - Gestione delle emergenze relative all'Ambiente

[23] Cod. 2008-00054 - Linee Guida di Gruppo per la gestione degli incidenti ICT

[24] Cod. 2017-000nn - Comunicazione Eventi Rilevanti (codice in via di definizione)

[25] Cod. 2015-00170 - Gestione eventi di Sicurezza Informatica

[26] Cod. 2014-00151 - Policy di Gruppo Business Process Management

[27] Cod. 2014-00152 - Definizione e Formalizzazione di Policy, Procedure ed Istruzioni Operative di Gruppo

[28] Cod. 2015-00155 - Sviluppo dell'Identità Organizzativa - I nuovi Valori di Telecom Italia

[29] Modello Organizzativo 231 del Gruppo Telecom Italia (comprensivo del Codice Etico e di Condotta)

I documenti con codice TIIT\_SGI\_TMP costituiscono i template che possono essere utilizzati nell'esecuzione del processo.

I documenti SDI del processo sono:

- Definizione e Formalizzazione di Policy, Procedure ed Istruzioni Operative di Gruppo nota come Norma delle Norme che regolamenta la formalizzazione dei processi e dei relativi documenti procedurali ne stabilisce i criteri di classificazione, le regole per l’emissione delle procedure, nonché i ruoli e le responsabilità delle funzioni coinvolte nel processo di redazione e di approvazione

- Policy di Gruppo Business Process Management definisce un quadro normativo di riferimento per la definizione e gestione dei processi aziendali, i ruoli che agiscono, il Business Process Framework, i criteri, le modalità e gli strumenti per. process modeling

- Sviluppo dell’Identità Organizzativa - I nuovi Valori di Telecom Italia #ivaloridiTIM

# DESCRIZIONE PROCESSO E RESPONSABILITÀ

## Scopo e descrizione breve del processo

La procedura descrive le attività di presa in carico dell'incidente (generalmente il Trouble Ticket), la sua valutazione, in termini di severità dell’incidente, l’attivazione per i Major Incident del processo di escalation e, nel caso di errore non noto, l’indirizzamento alla gestione dei problemi per l’analisi delle cause dell’incidente.

La procedura gestisce inoltre i reclami specifici del Cliente/Utente. Poiché il trattamento di tale tipologia di reclamo è analogo a quello applicato per la gestione degli incidenti, laddove indicato (nel flusso e nel testo) “gestione incidenti”, si legga correntemente “gestione incidenti/reclami”. Per i reclami importanti (Reclami Major) si applica il medesimo processo di escalation dei MI.

## Input/output e fornitori/clienti del processo

I fornitori del processo sono:

- Enterprise Risk Management

- Operations Support & Readiness

Gli input del processo sono:

- Comunicazione gestione standard

- Incident Report

- Segnalazione Evento di Sicurezza DC

- Segnalazione Incidente

- Ticket Malfunzionamento/Reclamo/Disservizio

Gli output del processo sono:

- Comunicazione Evento Rilevante

- Notifica possibile Incidente di sicurezza Logica

- Problema

- Registro degli Incidenti di Servizio

- Report Incidente DC

- Report mensile per Service Manager

- Ticket Malfunzionamento/Reclamo/Disservizio

I clienti del processo sono:

- Assurance

- Enterprise Risk Management

## Obiettivi (KPO / KPI / SLA)

Gli obiettivi di performance sono legati a :

* Disponibilità delle applicazioni IT "Mission Critical" in base alla finestra temporale prevista per ciascuna di esse. L'indicatore Disponibilità delle Applicazioni IT, il valore soglia e la regolamentazione dello SLA sono definiti negli accordi di servizio.
* Distribuzione, per fasce di durata, degli Incident con Disservizio chiusi negli ultimi 12 mesi.
* Volume di tutti gli Incident con Disservizio chiusi negli ultimi 12 mesi

I KPI del processo sono:

- Disponibilità delle applicazioni IT

- Numero Incidenti con disservizio

- Tempestività nella chiusura dei disservizi

## Vincoli sul processo

Le normative cogenti sul processo sono:

- ISO 20000

- ISO 27001

## Gestione degli Incidenti IT

### **Contesto del processo**



### **Flow del processo**



### **Attività del processo**

#### **01 / Analisi tipologia segnalazione/ticket**

Descrizione attività

Il Gruppo Risolutore attivato esegue l’analisi della tipologia di segnalazione/ticket. La segnalazione/ticket può anche essere generata da parte del Service Owner (o suo Delegato) a valle dell’evidenza di anomalie riscontrate in fase di analisi del trend del servizio sui report operativi periodici.

Il Gruppo Risolutore verificherà la completezza del record d’incidente (Trouble Ticket) che dovrà contenere almeno:

· Un identificativo univoco

· Una descrizione dell’oggetto/disservizio provocato dall’incidente

· Il/i servizio/i impattato/i (\*)

· Il contesto in cui si è verificato (Cliente, Area del Business, Applicazioni)

· la severità/gravità dell’incidente

· uno stato (aperto/preso in carico/..., etc.)

· Una data di apertura

· L’intervento effettuato (workaround o problema associato)

· Eventuali riferimenti a ticket di segnalazione del malfunzionamento/disservizio

(\*) generalmente nel Trouble Ticket il campo “servizio impattato” contiene la funzionalità dell’applicazione (es.: attivazioni linee, servizio di post vendita, etc.); il servizio IT (es.: il servizio di Job Scheduling di GA) è trattato di norma in altro file (es.: Registro degli Incidenti di Servizio).

Le segnalazioni di eventi di sicurezza dei Data Center (Incidenti di sicurezza logica, incidenti di sicurezza fisica, incidenti infrastrutturali) vanno registrate nel "Report Incidente DC".

* Nel caso in cui l’evento segnalato faccia riferimento ad incidenti di sicurezza logica viene coinvolto, in qualità di Gruppo Risolutore, il Security Operation Center a cui viene inviata via mail una "Notifica di possibile incidente di sicurezza logica", in accordo al processo di “Gestione eventi di Sicurezza Informatica”, oppure vengono fornite telefonicamente le informazioni rilevate e già registrate nel "Report Incidente DC". Per conoscenza deve essere altresì informato il Responsabile del DC.
* Gli incidenti di sicurezza fisica vengono segnalati alle figure di riferimento per i Data Center, che in ambito locale sono rappresentate dal Responsabile DC a dal Local Security, e come coordinamento centrale sono rappresentate dal gruppo DC Sicurezza Fisica. Le attività di contenimento/contrasto agli incidenti di sicurezza fisica riguardano il perimetro interno dei Data Center, ovvero le sale sistemi. Sulla base della criticità dell'incidente occorso, possono essere richiesti interventi della Vigilanza e/o delle Forze dell'Ordine, nonché di fornitori degli impianti di sicurezza fisica al fine di ripristinare il livello di sicurezza degli apprestamenti impattati.
* Gli incidenti infrastrutturali vengono gestiti a livello operativo come previsto dalle attività di Fault Management Sistemi e Facilities descritte nella procedura "Operations Data Center", pertanto la notifica dell'incidente occorso viene effettuata attraverso l'apertura di un Trouble Ticket (TT DC).

Dal processo "Gestione eventi di Sicurezza Informatica" può pervenire, attraverso mail, il risultato dell'analisi effettuata a fronte di una precedente "Notifica di possibile incidente di Sicurezza Logica", in cui si dichiara che l'incidente in esame non è un incidente di Sicurezza Logica. In tal caso, l'incidente, deve essere nuovamente analizzato per comprenderne la vera natura.

Input/output dell’attività

Input attività:

- Incident Report

- Registro degli Incidenti di Servizio

- Segnalazione Evento di Sicurezza DC

- Segnalazione Incidente

- Ticket Malfunzionamento/Reclamo/Disservizio

- Trouble Ticket/mail

Output attività:

- Incidente

- Notifica possibile Incidente di sicurezza Logica

Processi aziendali in output all'attività

- Gestione eventi di sicurezza informatica

Risorse IT utilizzate (opzionale)

Le risorse IT utilizzate dall'attività sono:

- TSSC-TM Piattaforma Integrata per la gestione di Trouble Ticket Management, provisioning di richieste, SLA concordati. --Il sistema prevede le seguenti funzionalitÃ : -Â·Inserimento di una segnalazione, -Â·Attribuzione automatica del reclamo alla struttura competente, -Â·Evoluzione del reclamo, -Â·Monitoraggio dei reclami, -.Inoltro delle segnalazioni ad altri sistemi/procedure.

#### **02 / Classificazione Incidente**

Descrizione attività

Pur essendo sempre necessario risolvere ciascun incidente nel tempo più breve possibile, a ciascuno di essi viene assegnata una priorità di intervento, con le stesse regole previste per la gestione delle richieste di servizio (rif.: “Gestione Operativa dei Servizi IT” Cod. 2015 - 00225).

In particolare l’incidente viene classificato “**Major Incident**” nel caso in cui rientra in uno degli 11 criteri riportati di seguito:

1° Criterio)

* Criticità Applicazione: Mission Critical
* Tipologia Incidente: Interruzione o forte degrado nella finestra di erogazione del Servizio
* Soglia: Durata > 1 ora, ovvero Ripetizioni > 3 nell'arco temporale della finestra di erogazione del Servizio

2° Criterio)

* Criticità Applicazione: Mission Critical / Alta Criticità
* Tipologia Incidente: Grave anomalia applicativa con impatto sulle funzionalità principali dell'Applicazione
* Soglia: Nessuna

3° Criterio)

* Criticità Applicazione: Mission Critical / Alta Criticità
* Tipologia Incidente: Anomalia applicativa di qualunque natura e durata che determina un errato addebito o una errata fatturazione nei confronti dei Clienti (Business, Consumer e Wholesale)
* Soglia: > 5.000 Linee

4° Criterio)

* Criticità Applicazione: Alta / Media / Bassa Criticità
* Tipologia Incidente: Interruzione o forte degrado nella finestra di erogazione del Servizio
* Soglia: Durata > 4 ore (Alta Criticità) oppure durata > 8 ore (Media / Bassa Criticità) nell'arco temporale della finestra di erogazione del Servizio (escluse le Applicazioni ad uso interno IT)

5° Criterio)

* Criticità Applicazione: Tutte
* Tipologia Incidente: Disservizi di cui ha avuto evidenza diretta il CIO, soprattutto se oggetto di comunicazione in escalation (es. Portali)
* Soglia: Nessuna

6° Criterio)

* Criticità Applicazione: Tutte
* Tipologia Incidente: Disservizi di qualsiasi durata e natura che provochino mancata raccolta dei file di traffico, mancato rating o billing, blocco delle ricariche prepagate, blocco dei Servizi On Demand che comportino perdite economiche per l'Azienda
* Soglia: Nessuna

7° Criterio)

* Criticità Applicazione: Tutte
* Tipologia Incidente: Disservizi di qualsiasi durata e natura in concomitanza di eventi aziendali rilevanti (CdA, Assemblea con gli Azionisti, Incontro con la Comunità Finanziaria, etc.) che impattano le Applicazioni normalmente utilizzate durante tali eventi
* Soglia: Qualsiasi durata disservizio

8° Criterio)

* Criticità Applicazione: Mission Critical / Alta Criticità
* Tipologia Incidente: Disservizi di qualsiasi durata e natura nella finestra di erogazione su GUI (Graphical User Interface) di Applicazioni con impatti su utilizzatori
* Soglia: Impatto > 100 utilizzatori per Applicazioni Mission Critical oppure Impatto > 500 utilizzatori per Applicazioni con Alta Criticità AND durata disservizio > 1 ora

9° Criterio)

* Criticità Applicazione: Tutte
* Tipologia Incidente: Disservizi/anomalie di qualsiasi durata che hanno comportato un rilevante incremento di reclami al Customer Care rispetto al pianificato e la conseguente escalation di Regia Nazionale (Segnalazione "Alto Impatto")
* Soglia: accertata causa IT

10° Criterio)

* Criticità Applicazione: Tutte
* Tipologia Incidente: Disservizi/anomalie di qualsiasi durata che hanno comportato un impatto sull'operatività di intere sedi del Customer Care (almeno due) o intere sedi operative
* Soglia: Oltre due sedi disservite del CC o una intera sede operativa TIM

11° Criterio)

* Criticità Applicazione: Tutte
* Tipologia Incidente: Disservizi / anomalie di qualsiasi durata che possono comportare violazioni o escalation (lettere, richieste di danni, etc.) relative a OLO/AOM/MVNO, Regolatorio o AGCOM (MNP, etc.)
* Soglia: Nessuna

Il livello di criticità di una applicazione è definito internamente al catalogo IT Master Catalog ITMC, nel campo “Criticità Business”.

Nel caso in cui si è in presenza di un Major Incident viene attivato il processo di escalation (vedi dettaglio nell’attività corrispondente).

Nel caso in cui la segnalazione/ticket faccia riferimento ad un evento critico che ha impatti sui ricavi di TIM si attivano le funzioni di Revenue Assurance e si effettua tutto quanto indicato nella “ Istruzione Operativa per la gestione delle issue in ambito TIIT con impatti sui ricavi di Telecom Italia” (rif.: TIIT\_SGI\_QIO\_P105\_D).

Nel caso di eventi di sicurezza riscontrati nei Data Center la classificazione dell'incidente di sicurezza si effettua, in accordo alla procedura "Gestione eventi di Sicurezza Informatica", secondo i seguenti 4 livelli di severità:

* Crisi
* Emergenza
* Incidente Rilevante
* Business as Usual

Input/output dell’attività

Input attività:

- Incidente

Output attività:

- Incidente

- Major Incident

Processi aziendali in output all'attività

- Issue con impatti sui Ricavi di TI

Risorse IT utilizzate (opzionale)

Le risorse IT utilizzate dall'attività sono:

- ITMC Catalogo Unificato dei Sistemi e delle Applicazioni TIIT

- TSSC-TM Piattaforma Integrata per la gestione di Trouble Ticket Management, provisioning di richieste, SLA concordati. --Il sistema prevede le seguenti funzionalitÃ : -Â·Inserimento di una segnalazione, -Â·Attribuzione automatica del reclamo alla struttura competente, -Â·Evoluzione del reclamo, -Â·Monitoraggio dei reclami, -.Inoltro delle segnalazioni ad altri sistemi/procedure.

#### **03 / Escalation**

Descrizione attività

L'iter di escalation viene attivato, in coerenza con gli accordi presi con il Cliente, sui “Major Incident”.

Per questo tipo di incidenti è necessario attivare tempestivamente quanto necessario ad individuare una soluzione (workaround o soluzione definitiva) e rimuovere il disservizio in tempi rapidissimi.

Per i Major Incident” viene innescato il processo di “One Minute Escalation” (rif.: Cod. 2016 - 00069) per la segnalazione tempestiva del disservizio, o dell'evento rilevante, ad una lista di nominativi predefiniti e per una eventuale escalation verso TIM (rif.: "Comunicazione Eventi Rilevanti"). Dal processo di "Comunicazione Eventi Rilevanti" può pervenire una "Comunicazione gestione standard" che sancisce che, a fronte delle analisi effettuate su un evento rilevante, non è ritenuto necessario avviare una Comunicazione Trasversale e che, quindi, si procede con la normale gestione dell'evento.

Nel caso di Major Incident, in qualunque fase del suo processo di gestione, può verificarsi la necessità/opportunità di azioni gestionali o di escalation nei confronti dei vendor a vario titolo coinvolti/responsabili del MI in esame.

Azioni tipiche possono essere finalizzate a coinvolgere il vendor affinché rispetti gli accordi e gli SLA contrattuali. In questo caso il processo prevede di scalare l’azione verso il responsabile di primo livello della struttura di esercizio owner del MI che si avvarrà (con eventuale supporto delle strutture legali e della funzione Acquisti) di tutte le leve contrattualmente previste per ottenere dal vendor la risposta/risoluzione del problema secondo gli accordi e gli SLA previsti.

Nel caso di Major Incident viene data indicazione, da parte dell'owner dell'incidente, di Fornitori esterni potenzialmente coinvolti; viene effettuata anche una valutazione dell'impatto di business, questa attività è descritta nel processo di "Service Management"(rif.: Cod. 2016 - 00015).

Input/output dell’attività

Input attività:

- Comunicazione gestione standard

- Major Incident

Output attività:

- Major Incident

Processi aziendali in output all'attività

- One Minute Escalation

#### **04 / Analisi Incidente**

Descrizione attività

Il Gruppo Risolutore, a seconda della natura:

* controlla la competenza sul CI(Servizio)
* utilizza le informazioni presenti nel CMDB, che rappresenta l'insieme delle informazioni sul contesto operativo che supportano l'attività di analisi. Sono ad es. informazioni su:
* Applicazione
* Ticket
* Contratti (Livelli di Servizio)
* Individua la soluzione utilizzata in un incidente simile già occorso precedentemente o un workaround. In questa attività è supportato dalle informazioni relative agli Errori Noti presenti nel KEDB (Known Error Data Base), che rappresenta l’elenco degli errori noti che hanno una soluzione già individuata, oppure dalle informazioni del CMDB attraverso il quale può controllare se l'incidente ha gli stessi sintomi di un problema o di un errore noto presentatosi in altri contesti applicativi simili a quello in corso di analisi per applicare le medesime soluzioni.

Input/output dell’attività

Input attività:

- CMDB Configuration Management Data Base - è un DB virtuale federato dei DB aziendali e rappresenta l'insieme delle informazioni sul contesto operativo che supportano prevalentemente l'attività di analisi e sono, dunque, utili a poter gestire un incidente. Sono ad esempio informazioni relative alle Applicazioni coinvolte, ai Ticket correlati, ai Piani di Rilascio e agli esiti del rilascio, al Catalogo dei Servizi Base ed ai contratti (Livelli di Servizio), Nel caso della funzione di IT Infrastructure costituisce un vero e proprio applicativo a supporto della gestione dei Configuration Item infrastrutturali.

- Incidente

- KEDB Known Error Data Base - rappresenta l'elenco degli errori noti che hanno una soluzione già individuata

Output attività:

- Incidente

- Soluzione nota

Risorse IT utilizzate (opzionale)

Le risorse IT utilizzate dall'attività sono:

- TSSC-TM Piattaforma Integrata per la gestione di Trouble Ticket Management, provisioning di richieste, SLA concordati. --Il sistema prevede le seguenti funzionalitÃ : -Â·Inserimento di una segnalazione, -Â·Attribuzione automatica del reclamo alla struttura competente, -Â·Evoluzione del reclamo, -Â·Monitoraggio dei reclami, -.Inoltro delle segnalazioni ad altri sistemi/procedure.

#### **05 / Riassegnazione Ticket ad altro Gruppo Risolutore**

Descrizione attività

Il Gruppo Risolutore reindirizza il ticket ad altri gruppi di risoluzione o ad enti di competenza oppure li coinvolge direttamente per la risoluzione. Nel primo caso se si è in presenza di un Major Incident notifica al Service Manager/Revenue Assurance il cambio di gruppo.

Risorse IT utilizzate (opzionale)

Le risorse IT utilizzate dall'attività sono:

- TSSC-TM Piattaforma Integrata per la gestione di Trouble Ticket Management, provisioning di richieste, SLA concordati. --Il sistema prevede le seguenti funzionalitÃ : -Â·Inserimento di una segnalazione, -Â·Attribuzione automatica del reclamo alla struttura competente, -Â·Evoluzione del reclamo, -Â·Monitoraggio dei reclami, -.Inoltro delle segnalazioni ad altri sistemi/procedure.

#### **06 / Registrazione Problema**

Descrizione attività

Se non esistono soluzioni immediate, per risolvere l’Incidente, il Gruppo che lo ha in carico attiva il processo di “Gestione dei Problemi” (rif.: Cod. 2016 - 00196) con l’apertura di un Problema per la rimozione della causa che l’ha generato. L’Incidente e il Problema sono collegati fra di loro, un Problema potrà far riferimento a più Incidenti.

L'apertura di un Problema può avvenire anche in seguito all’analisi del trend di servizio (vedi attività “Valutazione incidenti”).

Ai fini della rimozione del problema e quindi della causa radice sono trattati in maniera dettagliata nella istruzione operativa “Incidenti con disservizio” (rif.: Cod. 2016 - 00259) gli incidenti che provocano malfunzionamento e non sono circoscritti a singole utenze.

Input/output dell’attività

Input attività:

- Incidente

- Registro degli Incidenti di Servizio

Output attività:

- Problema

Processi aziendali in output all'attività

- Gestione dei Problemi

Risorse IT utilizzate (opzionale)

Le risorse IT utilizzate dall'attività sono:

- TSSC-TM Piattaforma Integrata per la gestione di Trouble Ticket Management, provisioning di richieste, SLA concordati. --Il sistema prevede le seguenti funzionalitÃ : -Â·Inserimento di una segnalazione, -Â·Attribuzione automatica del reclamo alla struttura competente, -Â·Evoluzione del reclamo, -Â·Monitoraggio dei reclami, -.Inoltro delle segnalazioni ad altri sistemi/procedure.

#### **07 / Risoluzione Incidente**

Descrizione attività

Il Gruppo Risolutore rimuove il disservizio e completa la documentazione dell’intervento allegandola all’incidente. Come descritto nella istruzione operativa “Incidenti con disservizio” una sintetica descrizione della soluzione implementata o dell’intervento effettuato deve essere riportata nel campo “Soluzione strutturale” del record relativo all’incidente in analisi, o problema correlato, nel sito Sharepoint di ADM.IT PM, rintracciabile a l link

http://grfwww026rm001.griffon.local:8080/sites/ADM-operations/Major%20Incident/SitePages/Menu.aspx,

nella cartella “Incident & Problem”. Tale documentazione dovrà consentire una chiara interpretazione dell’intervento eseguito.

Se si è in presenza di un Major Incident, viene inviata notifica al Service Manager/Revenue Assurance.

In caso di soluzione non idonea e di compromissione del servizio si attiverà il processo di “Controllo dei prodotti non conformi”.

Nel caso di Incidente di Sicurezza DC vengono integrate nel "Report Incidente DC" le informazioni relative alle precedenti fasi di gestione, compresi gli Incident Report provenienti dal processo di "Gestione eventi di Sicurezza Informatica", ed inserite le eventuali azioni, proposte dalle funzioni che hanno gestito l'incidente, per impedire il ripetersi dell'incidente di sicurezza. Se tali azioni hanno un notevole impatto su risorse, budget e servizi erogati viene attivato il processo di "Definizione del budget/forecast e del Piano delle Commesse".

Input/output dell’attività

Input attività:

- Soluzione nota

- Soluzione Strutturale

- Workaround

Processi aziendali in output all'attività

- Definizione del Budget/Forecast e del Piano delle Commesse TIIT

#### **08 / Certificazione intervento (incidente)**

Descrizione attività

Se necessario, una volta ripristinato il servizio, il Gruppo Risolutore coinvolge il Cliente/Utente (il relativo TT viene posto in stato “Risolto” e parte la mail di notifica all’utente che ha aperto il TT), eventualmente anche attraverso il supporto del Service Manager/Revenue Assurance, per una verifica finale e per comunicargli le azioni intraprese a valle della segnalazione ricevuta. Se la verifica ha esito negativo si ritorna alla fase di analisi dell’incidente.

#### **09 / Chiusura Incidente (ticket)**

Descrizione attività

La chiusura del ticket è obbligatoria. Deve essere registrata nel tool di Trouble Ticket Management, confermando obbligatoriamente la tipologia dell’incidente ed il relativo motivo, in base alla Tassonomia condivisa.

Il Gruppo Risolutore può chiudere autonomamente un incidente aperto proattivamente.

In alternativa, effettuerà la chiusura del ticket a valle dell’esito positivo della verifica da parte del Cliente/Utente. Nel caso di mancata risposta da parte di quest’ultimo, una volta trascorsi cinque giorni da quando il TT è stato posto in “Risolto” ed è partita la mail di notifica all’utente (cfr.: Certificazione intervento), un automatismo pone il TT nello stato definitivo di “Chiuso”. Solo in alcuni casi particolari il tempo di attesa, per chiudere il TT, può essere più lungo, come ad esempio per i TT di Fatturazione per i quali il tempo di attesa è fino alla fatturazione successiva.

In caso di Incidente di Sicurezza DC viene congelato il "Report Incidente DC" ed archiviato sia nel sistema "Reporting DC" del Data Center che in SDIP. La versione finale del report conterrà le seguenti informazioni.

* Data e ora di compilazione
* Descrizione dell'evento
* Descrizione dei sistemi informativi e/o dei servizi impattati
* Classificazione dell'incidente
* Indicazione delle persone che eseguono l'attività di gestione dell'incidente (ruolo, nominativo)
* Resoconto delle attività eseguite durante le fasi di gestione
* Proposte/osservazioni emerse in fase di fallow up.

Nel report sono altresì formalizzate le informazioni scambiate mediante comunicazione telefonica durante le attività di escalation, nei casi in cui sia prevista tale modalità di notifica dell'incidente di sicurezza.

Input/output dell’attività

Output attività:

- Report Incidente DC

Risorse IT utilizzate (opzionale)

Le risorse IT utilizzate dall'attività sono:

- TSSC-TM Piattaforma Integrata per la gestione di Trouble Ticket Management, provisioning di richieste, SLA concordati. --Il sistema prevede le seguenti funzionalitÃ : -Â·Inserimento di una segnalazione, -Â·Attribuzione automatica del reclamo alla struttura competente, -Â·Evoluzione del reclamo, -Â·Monitoraggio dei reclami, -.Inoltro delle segnalazioni ad altri sistemi/procedure.

#### **10 / Valutazione Incidenti**

Descrizione attività

Il Service Owner, o suo delegato, verifica se le attività messe in atto dalla funzione di Application Management, o Control Room corrispondente, per la gestione dei servizi di competenza e per la gestione dei relativi Incidenti, non siano a loro volta gravate da inconvenienti di tipo tecnico e/o organizzativo, tali da non poter garantire la normale erogazione del servizio o, in caso di disservizio, il rispetto degli SLA contrattuali definiti per il ripristino del servizio. In tal caso il Service Owner, registra quanto occorso in uno specifico file di tracciamento (Registro degli Incidenti di Servizio) da sottoporre a trattamento in maniera analoga a quanto visto in precedenza. Inoltre, nel caso di problematiche occorse a livello organizzativo, innesca il processo di Program Management Integrato.

Se dall’analisi dei trend emergono opportunità di miglioramento per ridurre in modo proattivo il verificarsi di alcuni incidenti viene aperto un Problema corrispondente.

Inoltre le informazioni riguardanti gli Incidenti con disservizio sono valutate settimanalmente secondo quanto previsto dalla Istruzione Operativa “Incidenti con Disservizio”, ponendo particolare attenzione ai Major Incident.

Mensilmente viene inviato per condivisione ai Service Manager un report sugli incidenti più devastanti che saranno, successivamente, oggetto di pubblicazione nella Business Review.

Una reportistica sugli incidenti di maggior rilievo sarà inviata alla funzione di Business Continuity di TIM.

Le informazioni riguardanti gli incidenti di sicurezza dei DC sono valutate periodicamente da IT Infrastructure che attiva, eventualmente, il processo di "Azioni Correttive, Preventive e Migliorative".

Input/output dell’attività

Output attività:

- Registro degli Incidenti di Servizio

- Report mensile per Service Manager

Processi aziendali in output all'attività

- Service Management

### **Matrice RACI delle attività/attori del processo**

| **Ruoli (Job)** |  |  | **PRODUCTION & DATA ENGINEER** | **RESPONSABILE AFC.PC.BU** | **RESPONSABILE I.SM.BS** | **Responsabile I.SM.C** | **RESPONSABILE I.SM.WT** |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ruoli logici** | **GRUPPO RISOLUTORE** | **IT SERVICE OWNER** |  |  |  |  |  | **Utente** |
| **Strutture** | **Vedi elenco\*** | **Vedi elenco\*** | **ADM.IT.IMT** | **AFC.PC.BU** | **I.SM.BS** | **I.SM.C** | **I.SM.WT** |  |
| **01 Analisi tipologia segnalazione/ticket** | **R A** | **I** |  |  |  |  |  |  |
| **02 Classificazione Incidente** | **R A** |  |  |  |  |  |  |  |
| **03 Escalation** | **I** | **R A** | **C** | **R** | **R** | **R** | **R** |  |
| **04 Analisi Incidente** | **R A** | **C** |  |  |  |  |  |  |
| **05 Riassegnazione Ticket ad altro Gruppo Risolutore** | **R A** | **I** | **I** | **I** | **I** | **I** | **I** |  |
| **06 Registrazione Problema** | **R** | **A** | **I** |  |  |  |  |  |
| **07 Risoluzione Incidente** | **R** | **A** | **I** | **I** | **I** | **I** | **I** |  |
| **08 Certificazione intervento (incidente)** | **R** | **C** |  | **C** | **C** | **C** | **C** | **R A** |
| **09 Chiusura Incidente (ticket)** | **R A** |  | **I** |  |  |  |  |  |
| **10 Valutazione Incidenti** | **C** | **R A** | **R** |  |  |  |  |  |

**\*Ruolo logico / Strutture organizzative**

**GRUPPO RISOLUTORE**

- ADM.AE ANALYTICS & ESS

- ADM.B BILLING

- ADM.BB EX BSS BUSINESS

- ADM.BSS BSS

- ADM.D EX DATAWAREHOUSE

- ADM.IT INTEGRATION & TESTING

- ADM.O OSS

- I.CT CONTROL ROOM & TECHNICAL MANAGEMENT

- I.DC/CS DATA CENTER CENTRO SUD

- I.DC/N DATA CENTER NORD

- I.UC END USER COMPUTING

- SEC SECURITY

- T.N EX NETWORK

- TS.SA SECURITY APPLICATION MANAGEMENT

- TS.SE SECURITY ENGINEERING

**IT SERVICE OWNER**

- ADM.AE.AM APPLICATION MANAGEMENT ANALYTICS & ESS

- ADM.B.AM APPLICATION MANAGEMENT BILLING

- ADM.BM.DV EX DIGITAL CHANNEL&VAS SERVICE MNGT

- ADM.BM.SM EX DIGITAL CORE SERVICE MANAGEMENT

- ADM.BSS.AM APPLICATION MANAGEMENT BSS

- ADM.D.AM EX DATAWAREHOUSE APPLICATION MANAG.

- ADM.IT.SD.AM EX APPLICATION MANAGEMENT MIDDLEWARE

- ADM.O.AM APPLICATION MANAGEMENT OSS

- I.CT CONTROL ROOM & TECHNICAL MANAGEMENT

- I.CT.CA CAPACITY & ASSET MANAGEMENT

- I.UC END USER COMPUTING

- TS.SA SECURITY APPLICATION MANAGEMENT

# GLOSSARIO

**CI**

Configuration Item. È un qualsiasi Componente che necessita di essere gestito per poter erogare un Sevizio IT. I CI sono sotto il controllo del Change Management. Tipicamente fra i CI sono inclusi i Servizi IT, hardware, software, edifici, persone e documentazione formale quale la documentazione del Processo e di SLA (def. ITIL V3).

**Evento Rilevante**

Evento/disservizio/incidente con impatto diretto o indiretto sul business e/o sui Clienti strategici e/o sulla Reputation e/o immagine dell'azienda e/o sulla sicurezza di beni materiali ed immateriali che è classificato rilevante in coerenza con i criteri definiti per le singole tipologie di disservizio (come dalla Procedura Organizzativa "Comunicazione Eventi Rilevanti").

**Incidente**

Un evento non pianificato che causa una interruzione del servizio, oppure una riduzione della qualità del servizio. Anche un malfunzionamento di un configuration item che non ha ancora impattato il servizio è un incidente

**Incidente applicativo**

Quando si verifica un disservizio applicativo e viene registrato dalle strutture di Application Management, o Control Room, per tracciare gli interventi atti a ripristinare il corretto funzionamento dell’applicativo e del servizio supportato

**Incidente con disservizio**

Un evento non pianificato che determina una interruzione del servizio, oppure una riduzione della qualità del servizio.

Un incidente con disservizio può essere o può determinare anche un incidente applicativo

**Incidente di Sicurezza Logica**

Incidente originato da eventi informatici, legati a malfunzionamenti hardware e/o software o mirati a sfruttare le vulnerabilità dell'infrastruttura informatica (Denial of Service, Malicious Code, Accesso non autorizzato, Furto di informazioni o risorse aziendali, Traffico Anomalo, Impersonificazione di soggetti, Acquisizione di privilegi appartenenti a soggetti autorizzati, Frode, Incidente generico)

**Incidente di Sicurezza Fisica**

Incidente riconducibile a fattori umani, sia di tipo accidentale che di tipo premeditato, che insiste sugli asset aziendali (in particolare accesso fisico non autorizzato, furto, sabotaggio, danneggiamento volontario,, danneggiamento accidentale, comportamento non conforme alle norme aziendali e/o codice etico, azioni vandaliche, azioni terroristiche) sul perimetro interno dei Data Center (sale sistemi).

**Incidente di Sicurezza Infrastrutturale**

Incidente causato da guasti degli impianti industriali dei Data Center (mancata erogazione energia elettrica, guasto ai sistemi di condizionamento, errori di manutenzione) o legati a fenomeni di generazione di incendi, a fuoriuscite di liquidi dalle tubature idriche (allagamenti), che impattano sale sistemi, server, ed altri apparati IT.

**Major Incident**

Vedi la classificazione riportata nel testo del documento nell'attività "Classificazione Incidente" (pag. 12)

**Problema**

Costituisce la “root cause” di uno o più incidenti.

La root cause in genere non è nota inizialmente, quindi viene creato un problem record ed il processo di problem management è responsabile dell’ulteriore fase investigativa.

**Reclamo**

E’ un reclamo indefinito che prevede approfondimenti con il cliente sulla sua percezione del servizio fornito, nel rispetto dei livelli di servizio concordati

**Reclamo specifico**

E’ un reclamo puntuale su un disservizio reale segnalato soprattutto dall’utente finale; viene veicolato dal Service Desk con un sistema di Trouble Ticketing