autostrade per l'italia

ISTRUZIONE OPERATIVA

INCIDENT MANAGEMENT

	Struttura aziendale	Responsabile
Redatta da:	DIDT/SEO/ITC	Alessio Mugnai
Quality Gate:	na	
	na	
Approvata da:	DIDT/SEO	Pietro Mazzini
Verificata da:	DIDT	Danilo Gismondi

ONE PAGE LESSON

OBIETTIVO DEL DOCUMENTO

La presente procedura ha lo scopo di descrivere il processo di gestione degli incidenti di natura informatica che interessano le infrastrutture hardware e software di competenza della Direzione IT & Digital Transformation (di seguito “DIDT”).

Il documento descrive:

- il modello operativo per la rilevazione, la classificazione e la risoluzione degli incidenti di natura informatica;
- il modello di classificazione adottato per le segnalazioni di incidenti di natura informatica in ambito DIDT;
- i criteri di identificazione delle situazioni di “emergenza” e le modalità di gestione;
- le strutture operative, ed eventuali società esterne coinvolte nel processo di gestione degli incidenti;
- il modello di escalation per la gestione degli incidenti.

Obiettivi del processo di Incident Management sono principalmente:

- rilevare, registrare e acquisire un incidente IT
- classificare tra gli incidenti che si verificano quelli riconducibili ad una “emergenza” e/o ad un incidente di sicurezza informatica
- ripristinare, a fronte di un incidente, le normali operazioni di servizio nel più breve tempo possibile (e comunque entro gli SLA previsti) e con il minimo impatto sul business.
- 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)
- valutare un incidente per stabilire se è probabile che si ripresenti o se è sintomo di un problema cronico: in tal caso informare le strutture responsabili dei servizi a riguardo
- mantenere l’efficienza del servizio attraverso processi di comunicazione e di formazione tra i gruppi di lavoro, di presidio delle variazioni della baseline di esercizio garantendo l’aggiornamento della documentazione tecnica e la correttezza degli aggiornamenti.

FRAMEWORK

CAMPO DI APPLICAZIONE

PROCESSI ASPI IN SCOPE:

23. IT

DESTINATARI

- Tutto il personale operativo della DIDT
- Tutto il personale delle Società Controllate che hanno affidato ad ASPI, tramite appositi termini contrattuali, le attività di Service Informatico.
- tutto il personale operativo nell'ambito della Direzione IT and Digital Transformation (DIDT) e nell'ambito delle strutture o Società con responsabilità e competenza diretta o indiretta sui domini tecnologici coinvolti.

LINK UTILI

REVISIONI E PRINCIPALI MODIFICHE

#	Data	Principali Modifiche
00	03/12/2013	Prima emissione del documento
01	16/06/2014	Aggiornamento
02	10/06/2015	Aggiornamenti a seguito di: • Raccomandazione Certiquality N.16 (reati informatici secondo 231/01) – Rapporto di audit 27001 – 23, 24 Luglio 2014 • Dettaglio ruoli e responsabilità nel processo di Incident Management Recepimento requisiti dello standard ST_SG01 – Standard per la stesura della documentazione
03	09/12/2015	Aggiornamenti a seguito di: • Raccomandazione Certiquality N.04 (classificazione incidenti informatici secondo leggi 231 e 196) – Rapporto di audit 27001 del 6 Luglio 2015 • Introduzione processi per "Gestione emergenze" Modifiche organizzative (cfr . Istr. Serv 18/2015 e Istr. Serv. 22/2015)
04	03/04/2017	Aggiornamenti a seguito di: • Modifiche organizzative (cfr . Istr. Serv 5/2017 del 8 Marzo 2017) • Revisione annuale della documentazione Revisione cap.6 Incidenti di Sicurezza a

		seguito delle modifiche organizzative
05	21/05/2018	Aggiornamenti a seguito di: • Separazione flusso di gestione Incidenti di Sicurezza Revisione annuale della documentazione
06	20/05/2019	Aggiornamenti a seguito di: • Modifiche organizzative (cfr. IdS 22/2018 del: 17 dicembre 2018 Revisione annuale della documentazione
07	22/03/2021	Aggiornamenti a seguito di: • Modifiche organizzative Cambio sistema di ticketing
08	26/0372021	Aggiornamento tabelle delle priorità e correzioni formali
09	10/12/2023	Aggiornamenti a seguito di: • Modifiche organizzative Ids n.32/2022 Cambio sistema di ticketing Revisione casistiche di compilazione per incidente di servizio e introduzione di Escalation Time

•

APPROVAZIONI E CONTROLLI

Numero Approvazioni
2

Key control n(a

*** per Approvazioni si intendono Controlli di primo livello**

SISTEMI DI GESTIONE APPLICATI

- **SGSI – Sistema di gestione della sicurezza delle Informazioni (ISO 27001)**

Indice

1 SCOPO DEL DOCUMENTO

La presente procedura ha lo scopo di descrivere il processo di gestione degli incidenti di natura informatica che interessano le infrastrutture hardware e software di competenza della Direzione IT & Digital Transformation (di seguito "DIDT").

Il documento descrive:

1. il modello operativo per la rilevazione, la classificazione e la risoluzione degli incidenti di natura informatica;
2. il modello di classificazione adottato per le segnalazioni di incidenti di natura informatica in ambito DIDT;
3. i criteri di identificazione delle situazioni di "emergenza" e le modalità di gestione;
4. le strutture operative, ed eventuali società esterne coinvolte nel processo di gestione degli incidenti;
5. il modello di escalation per la gestione degli incidenti.

Obiettivi del processo di Incident Management sono principalmente:

- rilevare, registrare e acquisire un incidente IT
- classificare tra gli incidenti che si verificano quelli riconducibili ad una "emergenza" e/o ad un incidente di sicurezza informatica
- ripristinare, a fronte di un incidente, le normali operazioni di servizio nel più breve tempo possibile (e comunque entro gli SLA previsti) e con il minimo impatto sul business.
- 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)
- valutare un incidente per stabilire se è probabile che si ripresenti o se è sintomo di un problema cronico: in tal caso informare le strutture responsabili dei servizi a riguardo
- mantenere l'efficienza del servizio attraverso processi di comunicazione e di formazione tra i gruppi di lavoro, di presidio delle variazioni della baseline di esercizio garantendo l'aggiornamento della documentazione tecnica e la correttezza degli aggiornamenti.

2 CAMPO D'APPLICAZIONE

La procedura si applica nella fase di rilevazione e gestione degli incidenti, a tutto il personale operativo nell'ambito della DIDT e nell'ambito delle strutture o Società con responsabilità e competenza diretta o indiretta sui domini tecnologici coinvolti dall'evento.

Nel modello definito dal presente documento, Service Desk presidia la gestione degli incidenti. Il personale di Service Desk ha la responsabilità della corretta attuazione del processo di gestione degli incidenti con il supporto del personale specialistico sia per la classificazione che per le azioni di contenimento e ripristino.

Tutto il personale, interno o esterno è tenuto a prendere visione del presente documento e ad adoperarsi al fine di minimizzare gli impatti di eventuali incidenti sulle infrastrutture informatiche di competenza della DIDT.

Sono escluse dal presente documento tutte le attività successive alla risoluzione tecnica, ovvero le attività carattere organizzativo e disciplinare eventualmente finalizzate a:

- gestire la segnalazione in termini di abuso o frode informatica;
- avviare eventuali procedure legali o disciplinari.

Per quanto riguarda la gestione degli incidenti di sicurezza essa è regolata dalla Norma Operative "ASPI_NO_ITC11 - *Security Incident Management (Processo per la gestione degli incidenti di sicurezza informatica"*

3 ABBREVIAZIONI E DEFINIZIONI

TERMINE/SIGLA	DEFINIZIONE
CMDB	Configuration Management DataBase: database che contiene informazioni sugli elementi di configurazione (CI) e le loro relazioni all'interno dell'infrastruttura IT
Cruscotto di monitoraggio	Modalità principale di segnalazione di non disponibilità dell'hardware e del software di base; a fronte di ciascun allarme rilevato viene aperto un incident i cui tempi di risoluzione sono determinati anche dall'evidenza sulla disponibilità delle applicazioni
Emergenza	Classificazione di un incidente che causa la totale indisponibilità di un servizio IT , da risolvere nel più breve tempo possibile . L'elenco dei servizi IT soggetti a procedura di emergenza è riportato nella Norma Operativa ASPI_PR_VIA01_rev06_2022_Info Stati Emergenza
Escalation Time	Intervallo di tempo, definito nei sistemi di monitoraggio, trascorso il quale si attiva il processo di escalation per la risoluzione dell'incident , censito e registrato nel CMBD .
KEDB	Known Error Database. Informazioni e documenti di supporto ai servizi distribuiti attraverso lo strumento di trouble ticketing che permette la visualizzazione degli interventi già trattati
Impatto	Misura degli effetti di un incident sui processi di business . E' classificato come : Alto , Medio , Basso
Incident	Evento, o catena di eventi, che causa, o può causare, un'interruzione non pianificata e/o una riduzione della qualità di un servizio IT.
Incidente di sicurezza informatica	Evento, o catena di eventi, che causa, o può causare, un'interruzione non pianificata e/o una riduzione della qualità di un servizio IT, ed avere per conseguenza la perdita di riservatezza, integrità o disponibilità dei dati aziendali e dei servizi erogati dagli asset informatici protetti, nonché l'utilizzo di asset al fine di commettere illeciti o arrecare danni verso terzi, in violazione a disposizioni aziendali e/o legislative
Priorità	Ordine nel quale gli incidenti debbono essere risolti; viene determinata sulla base dell'urgenza e dell'impatto e in accordo con gli SLA. E' classificata come : Critico , Alto , Moderato , Pianificazione
Problem	Causa che ha determinato l'incident , per la risoluzione del quale può essere necessario una "Change"
Root cause	Causa principale di un evento.

Service Desk	Punto di contatto per gli utenti dei servizi IT per la gestione degli incidenti.
SLA disponibilità	Service Level Agreement. Livello di servizio concordato da associare ai servizi erogati attraverso la disponibilità delle applicazioni e delle loro componenti infrastrutturali . Le disponibilità sono concordate fra la DIDT e gli utenti del servizio.
SLA intervento	Livello di servizio dei tempi di presa in carico e risoluzione delle segnalazioni .
OLA	Operation level agreement. Livello di servizio concordato con le struttue interne per le attività necessarie alla fornitura dei servizi IT
Urgenza	Priorità di risoluzione richiesta dall'utente o definita dal processo di monitoraggio. E' classificato come : Alto , Medio , Basso
Workaround	Correzione temporanea ad un incidente o una sequenza di azioni alternativa a quella che produce l'incidente, utilizzabile dall'utente

Sigle Organizzative

DIDT	Direzione IT and Digital Transformation
DIDT/SEO	Service Operations
DIDT/SEO/ITC	IT Services
DIDT/SEO/SRM	Supporto Utenti Sede Roma
DIDT/ DTL	Direzione IT and Digital Transformation and Innovation
DIDT/CISO	Chief Information Security Officer
DIDT/CTO	Chief Technology Officer
DIDT/CTO/SCR	Sicurezza Sistemi
DIDT/CTO/ITO	IT Operations
DIDT/CTO/IEA	IT Enterprise Architecture
DIDT/CTO/ITA	IT Asset Monitoring
DIDT/CTO/RFI	Rete Fisica
DIDT/CTO/RLO	Rete Logica

4 RUOLI E RESPONSABILITA’

Le responsabilità delle funzioni coinvolte nel processo di gestione degli incident è sintetizzata nella seguente matrice RACI1*

		Service Desk (*)	IT Services	Resolver Group
Identificazione	Rilevamento e registrazione Incident	R/A	I	C
	Valutazione Impatto e determinazione severità	R/A	I	C
Presa in carico	Analisi e diagnosi	R/A	I	C
	Risoluzione Livello 0	R/A	I	C
	Smistamento/Escalation	R/A	I	C
Risoluzione	Risoluzione livelli 1, 2, 3	C	I	R/A
	Chiusura e verifica SLA	R/A	I/R	C
Post incident	Analisi delle cause	C	R/A	C
	Ricerca evidenze	C	R/A	C
	Emissione Rapporto Incidente	C	R/A	C

(*) Svolgono attività di Service Desk le U.O.:
DIDT/SEO/SRM per problemi di Office relativamente alla sede di Roma
DIDT/SEO/ITC per la gestione completa del Service Desk

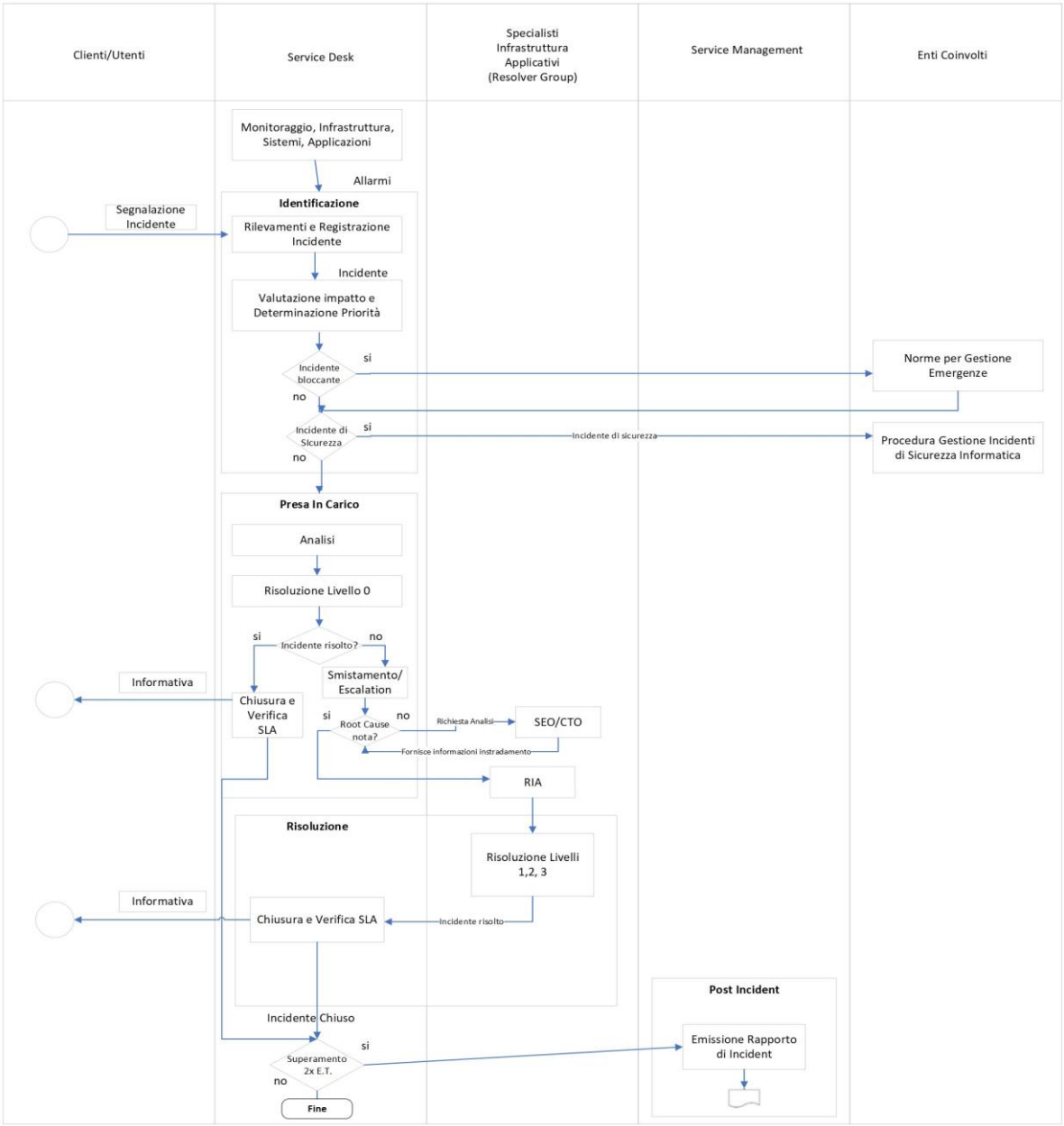
R - È responsabile dell’esecuzione di un’attività. Per un’attività deve esistere almeno un ente/ruolo responsabile A - Ha la responsabilità generale dei risultati di un’attività. Conseguentemente è tenuto a rispondere della misura in cui sono stati raggiunti gli obiettivi e di quali aspettative sono state soddisfatte. Per un’attività deve essere presente un unico ente/ruolo accountable.

C - Partecipa alla realizzazione di un’attività o contribuisce, a vario titolo, alla produzione di contributi informativi attesi. Può anche trattarsi di una persona consultata per un parere o per svolgere una specifica sotto-attività in qualità di esperto. In quest’ultimo caso, il suo coinvolgimento è generalmente limitato nel tempo. Per un’attività possono essere presenti più enti/ruoli che collaborano.

I - E’ informato dell’esecuzione di un’attività avendone un interesse specifico. Per un’attività possono essere presenti più enti/ruoli informati.

5 GESTIONE DEGLI INCIDENT

5.1 Flusso procedurale incidenti



5.2 Descrizione dei processi

I processi riportati nel precedente flusso sono applicabili a qualsiasi tipologia di incidente informatico.

Relativamente alla gestione delle “emergenze” per la fase di risoluzione le norme operative di dettaglio da seguire sono descritte nella Norma Operativa: ASPI_PR_VIA01_rev06_2022_Info Stati Emergenza

5.2.1 Identificazione

5.2.1.1 Rilevamento e registrazione Incident

La rilevazione degli incident può avvenire secondo le seguenti modalità:

- i clienti/utenti e le Strutture Organizzative erogatrici dei Servizi IT segnalano un incident attraverso lo strumento di trouble ticketing disponibile sulla intranet aziendale oppure attraverso il numero telefonico dedicato, definendone l’urgenza;

- gli Operatori di Service Desk registrano incident a fronte di segnalazioni telefoniche o di altro tipo ricevute;

- i cruscotti di monitoraggio e controllo a disposizione di Service Desk generano allarmi sulle componenti di infrastruttura;

Gli Operatori di Service Desk responsabili della registrazione e del monitoraggio della risoluzione degli incidenti, tracciano i dettagli di base dell’incidente, allertano i gruppi di supporto specializzato nella misura necessaria e danno avvio alle procedure per gestire la segnalazione. La registrazione avviene tramite lo strumento di trouble ticketing.

A valle della segnalazione, con gli strumenti a propria disposizione, gli Operatori di Service Desk sono in grado di reperire le seguenti informazioni:

- Dettagli dell’incidente, forniti da più fonti (strumenti di monitoraggio, segnalazioni degli utenti via web, telefonate su numeri dedicati, etc.)
- Form di riferimento per l’acquisizione delle informazioni tipiche del problema applicativo (data incident, screenshot dell’errore, ...)
- Dettagli sulla configurazione, forniti dai documenti contenuti nel CMDB
- *Incident matching* (verifica di preesistenti problematiche dello stesso tipo contenute nel KEDB
- Informazioni sulle recenti RFC implementate (deploy) come indizi sulle possibili cause di incidenti

- Workarounds o interventi risolutori come da procedure operative fornite dagli specialisti - SLA

5.2.1.2 Valutazione Impatto e determinazione Priorità

Si identificano le ragioni che hanno portato all'incidente e di conseguenza della relativa azione risolutiva. In questo caso lo strumento di KEDB può essere consultato per controllare l'esistenza di known errors e problemi analoghi oppure si applicano le procedure operative; viene effettuata una valutazione dell'impatto in modo che lo strumento di trouble ticketing possa calcolarne la Priorità. La valutazione dell'impatto viene proposta dallo strumento di Truble ticketing e l'operatore di SD può modificarla tenendo presente i seguenti criteri :

Alto

Un incidente che causa la **totale incapacità** di svolgere il normale funzionamento di qualsiasi attività di applicazioni/sistemi utilizzati all'interno degli SLA concordati.

Esempi:

- Tutti gli utenti non sono in grado di effettuare il login.
- Indisponibilità di applicazioni.
- Malfunzionamenti di rete, che incidono su una o più sedi.
- Incapacità di accedere alla posta elettronica o accesso a Internet per l'intera azienda.
- Diffusione di virus sui sistemi

Gli incidenti di impatto bloccante devono essere risolti con la massima tempestività seguendo le indicazioni della Norma Operativa ASPI_PR_VIA01_rev06_2022_Info Stati Emergenza

Medio

Problemi che limitano l'uso di un'applicazione, sistema, o una parte di hardware .
Il mancato contenimento di problemi di impatto *medio* può condurre a problemi di impatto alto.

Esempi:

- Fermo di un server o di un database

- Malfunzionamento Rete

Basso

Problemi che impattano un gruppo di utenti ristretto e che non sono critici .

Un problema di impatto *basso* è generalmente risolto in orario base in quanto non comporta una perdita significativa di operatività e non ha influenza su applicazioni. Ad esempio, si classificano a impatto *basso* le anomalie riscontrate su componenti hardware o software di

applicazioni, che però non provocano disservizi, grazie ad architetture ridondate.

Problema che impatta una sola persona o un gruppo molto ristretto di persone che non può eseguire una funzionalità non considerata critica per l'azienda

Esempi:

- Stampante condivisa inutilizzabile in un ufficio.
- Ripristino di file eliminati dalla rete.
- Impossibilità ad operare da parte di una figura aziendale con incarichi dirigenziali
- Richiesta di informazioni.
- Installazione di software
- Reset password
- Assegnazione abilitazioni

Lo strumento di trouble ticketing determina quindi la Priorità degli incidenti (1-Critico, 2-Alto, 3-Moderato, 4-Basso, 5-Pianificazione) in base all'Impatto ed all'Urgenza (1-Alto, 2-Medio,3-Basso) fornita dall'utente e seguendo la seguente matrice

		IMPATTO		
	PRIORITA'	3- Basso	2 - Media	1 - Alto
URGENZA	1 - Alta	3 - Moderata	2 - Alta	1 - Critica
	2 - Media	4 - Bassa	3 - Moderata	2 - Alta
	3 - Bassa	5 - Pianificazione	4 - Bassa	3 - Moderata

Sulla base della Priorità possono scattare controlli di rispetto degli SLA concordati o procedure specifiche di coinvolgimento di enti DIDT o di terze parti.

Classificata la chiamata gli Operatori di Service Desk procedono con l'incident matching. La consultazione del CMDB e dell'archivio degli Asset è necessaria per ottenere info riguardo il servizio che ha subito interruzione; i dati degli SLA sono visibili nello strumento di trouble ticketing.

Nel caso gli Operatori del Service Desk classifichino l'incidente come incidente di sicurezza la sua gestione è descritta nella Norma Operativa "ASPI_NO_ITC11 *Service Incident Management (Processo per la gestione degli incidenti di sicurezza informatica)*" cui si rimanda.

5.2.2 Presa in carico

5.2.2.1 Analisi

A seguito della valutazione iniziale di un incident, vengono raccolte e analizzate ulteriori informazioni. L'investigazione e l'individuazione possono diventare un processo iterativo, iniziando con la applicazione di procedure predefinite, e/o coinvolgendo i vari gruppi di supporto specializzato.

5.2.2.2 Risoluzione Livello 0

Se l'intervento degli Operatori di Service Desk anche attraverso l'utilizzo delle EventGuide relative al sistema IT oggetto dell'incident (livello 0) elimina gli effetti dello stesso, Service Desk verifica che il servizio sia ripristinato in maniera soddisfacente e secondo gli SLA richiesti e provvede alla chiusura del ticket indicando l'evento, le cause e la soluzione adottata per il ripristino. In caso di eventi ripetitivi il SEO/ITC può aprire un "Problem" per l'eventuale correzione delle cause .

5.2.2.3 Smistamento/Escalation

Se l'intervento non può essere effettuato a livello 0 e/o non risulta efficace entro il tempo di escalation (E.T.), il Service Desk smista l'incident ad un livello di competenza specialistica superiore (livelli 1, 2 e 3)

Livello 1 – E' costituito dagli specialisti di SEO

Livello 2 – E' costituito dagli specialisti delle strutture di gestione Infrastrutturale e CoE.

Livello 3 – E' costituito dagli specialisti degli applicativi

Se il Service Desk rileva una potenziale minaccia di sicurezza informatica, allerta tempestivamente l'incident al SOC/CSIRT secondo la procedura : "Istruzione Operativa Cyber Security Incident Handling - v0.2".

5.2.3 Risoluzione

5.2.3.1 Risoluzione Livelli 1, 2, 3

A fronte della risoluzione dell'incident, gli "Specialisti" descrivono nelle note la causa dell'incident e le soluzioni adottate per il ripristino.

Service Desk garantisce che:

- I dettagli sulle azioni intraprese per risolvere l'incident siano concisi e leggibili e registrati sullo strumento di Trouble Ticketing
- La classificazione sia completa e accurata in base alla causa di origine
- La risoluzione sia concordata con il cliente/utente

5.2.3.2 Chiusura e verifica SLA

Quando il ticket è risolto, Service Desk ,che opera da intermediario con il cliente, verifica che:

- il cliente/utente sia soddisfatto della soluzione adottata,
- il servizio sia stato ripristinato e la conformità rispetto agli SLA richiesti.

In tal caso provvede alla chiusura del ticket che determina la chiusura dell'incident, altrimenti procederà alla riapertura dello stesso.

Nel corso di tutto il processo vengono tracciati e monitorati i progressi e la qualità del servizio. Service Desk ha anche la responsabilità di tenere utente/cliente continuamente informati riguardo i progressi della chiamata e i previsti tempi di risoluzione.

5.2.4 Post incident

Nel caso di incidenti che provocano un indisponibilità dell'applicazione superiore a 2 volte E.T. l'Operation Manager predispone il Rapporto Incidente. Nella predisposizione del Rapporto di incidente, Operation Manager procede nel modo seguente.

5.2.4.1 Analisi delle cause e ricerca evidenze

- Identificazione di Problemi relativi all'infrastruttura
- Controllo dei dati sul CMDB ed eventuali feedback al Configuration Management per aumentare l'accuratezza delle informazioni
- Informazioni su eventuali incidenti che non sono stati risolti secondo i criteri stipulati negli SLA.

5.2.4.2 Emissione rapporto incidente

Successivamente alla chiusura dell'incidente OM, coordinandosi con gli enti responsabili dei servizi, predispone un rapporto sull'incidente contenente le seguenti informazioni:

- data dell'evento
- descrizione e durata dell'evento
- cause
- impatti
- tipologia di minaccia (Fisica, Logica, organizzativa)
- ambito di rischio (Fisico/ambientale, Organizzativo, Sistemistico, Network, Applicativo) - azioni di ripristino nel rispetto degli SLA
- pianificazione delle azioni correttive, concordate con le strutture di DIDT, da mettere in atto per ridurre il rischio che l'incidente si possa ripetere.

Il report di analisi post-incident è reso disponibile alle entità aziendali coinvolte affinché possano prendere atto delle azioni intraprese durante la gestione dell'incidente ed attuare quanto definito.

Per la gestione e il tracciamento di eventuali azioni correttive cfr. ASPI_NO_GST02_*Gestione Audit interni o a fornitori, Non conformità, Azioni Correttive o Preventive.*

6 GESTIONE INCIDENTI DI SICUREZZA

La gestione degli incidenti di sicurezza informatica viene effettuata dalle strutture del Security Operation Center (SOC) tramite le attività descritte nella procedura aziendale "*Gestione degli Incidenti di Sicurezza Informatica*", a cui si rimanda per ogni approfondimento.

RIFERIMENTI A LEGGI, NORME E REGOLAMENTI

All'interno del presente documento sono evidenziate tutte le norme e linee guida applicabili al processo di gestione degli incidenti di sicurezza, tra cui:

1. **ISO/IEC 27001:2022** – Information security, cybersecurity and privacy protection – Information security management systems – Requirements;
2. **ISO/IEC 27002:2022** – Information security, cybersecurity and privacy protection – Information security controls;
3. **D.lgs 231/01** – Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300
4. **D.Lgs 196/03** – come modificato dal decreto attuativo del GDPR n.101/2018 Codice in materia di protezione dei dati personali e s.m.i.;
5. **GDPR** – General Data Protection Regulation – Regolamento UE 2016/679;
6. **ASPI_IO_ITC06-01_rev08_2022 -** Metodologia di valutazione e gestione del rischio della sicurezza delle informazioni e protezione dei dati personal
7. **ASPI_PR_QLM06-03_rev00_2022 -** GestioneAudit NonConformità AzioniCorrettive
8. **ASPI_ PR_ITC01** – Gestione dei Cambiamenti dei Sistemi IT - Versione Applicabile
9. **ASPI_PR_VIA01** - Info Stati Emergenza
10. **ASPI_NO_ITC11** – Security Incident Management – Versione Applicabile