**Esempio di modello di matrice per escalation
per l’IT Service Desk / ITIL**



Problema di installazione del software

Essendo il punto di contatto iniziale per tutti i problemi IT, il service desk gestisce le richieste generali e la risoluzione dei problemi di base.

Il Livello 2 ha a che fare con problemi più complessi che richiedono conoscenze specialistiche o competenze tecniche aggiuntive.

Il Livello 3 risponde a sfide tecniche di alto livello che coinvolgono l’infrastruttura del sistema o problemi profondi del software.

**IT Service Desk (Livello 1)**

Il Livello X rappresenta il supporto esterno specialistico o l’assistenza specifica del vendor per problemi estremamente particolari.

**Assistenza di Livello 2**

**Assistenza di Livello 3**

**Assistenza di Livello X**

Inattività della rete

Violazione della sicurezza dei dati

Interruzioni del servizio cloud

Conferma i requisiti del
sistema e prova le
procedure di reinstallazione
di base.

Esegui una diagnostica dettagliata per identificare i conflitti o i file corrotti. Prova su sistemi alternativi, se necessario.

Rivedi e rettifica le impostazioni avanzate del sistema o registra i conflitti che possono compromettere la funzione di sicurezza del sistema.

Consulta il vendor del
software per problemi di installazioni proprietarie o
per ricevere patch.

Controlla i report iniziali e conferma se il problema è diffuso o localizzato. Reimposta i router o gli interruttori, se opportuno.

Analizza i registri di rete e coordinati con i provider del servizio internet o i team interni addetti alla rete per individuare le interruzioni.

Implementa le procedure avanzate di recupero della rete e riconfigura i principali protocolli di routing.

Coinvolgi i vendor delle apparecchiature di rete per aggiornamenti critici del firmware o diagnostica specialistica.

Registra l’incidente, allerta i team di sicurezza e avvia una procedura preliminare di blocco dei dati.

Conduci un’analisi forense iniziale per valutare l’estensione della violazione e identificare i sistemi compromessi.

Conduci audit di sicurezza completi e implementa strategie di correzione per mettere in sicurezza tutti i punti dati.

Lavora con aziende di cybersecurity per soluzioni avanzate di rilevamento delle minacce e tecniche di mitigazione.

Verifica lo stato del servizio con provider cloud e segnala i dettagli dell’interruzione agli utenti.

Valuta le integrazioni API e conduci controlli sui servizi correlati per garantire la connettività.

Coordinati con i tecnici del cloud per ripristinare i servizi e gestire i controlli sull’integrità dei dati.

Collabora con i provider dei servizi cloud per l’analisi dettagliata delle cause principali e per prevenire interruzioni future.

|  |
| --- |
| **DICHIARAZIONE DI NON RESPONSABILITÀ**Qualsiasi articolo, modello o informazione è fornito da Smartsheet sul sito web solo come riferimento. Pur adoperandoci per mantenere le informazioni aggiornate e corrette, non offriamo alcuna garanzia o dichiarazione di alcun tipo, esplicita o implicita, relativamente alla completezza, l’accuratezza, l’affidabilità, l’idoneità o la disponibilità rispetto al sito web o le informazioni, gli articoli, i modelli o della relativa grafica contenuti nel sito. Qualsiasi affidamento si faccia su tali informazioni è pertanto strettamente a proprio rischio. |