**Ejemplo de plantilla de matriz de derivación
de mesa de servicio de TI/ITIL**



Falla en la instalación de software

Como punto inicial de contacto para todos los problemas de TI , la mesa de ayuda maneja las consultas generales y la resolución de problemas básicos.

El nivel 2 se ocupa de problemas más complejos que requieren conocimientos especializados o habilidades técnicas adicionales.

El nivel 3 aborda dificultades técnicas de alto nivel que involucran infraestructura del sistema o problemas profundos de software.

**Mesa de servicio de TI (nivel 1)**

El nivel X representa el soporte externo o la asistencia específica de proveedores para problemas altamente especializados.

**Soporte de nivel 2**

**Soporte de nivel 3**

**Soporte de nivel X**

Tiempo de inactividad de la red

Vulneración de seguridad de datos

Interrupción de servicios de la nube

Confirmar los requisitos del sistema e intentar procedimientos básicos de reinstalación.

Realizar un diagnóstico detallado para identificar conflictos o archivos dañados. Probar sistemas alternativos, si es necesario.

Revisar y rectificar ajustes del sistema o conflictos de registros profundos que podrían perjudicar la función del sistema de seguridad.

Consultar al proveedor de software por problemas de instalación de software propio o para recibir parches.

Controlar los informes iniciales y confirmar si el problema está extendido o localizado. Volver a configurar los enrutadores o interruptores, si corresponde.

Analizar los registros de red y coordinar con los proveedores de servicio o equipos de red interna para identificar las interrupciones.

Implementar procedimientos avanzados de recuperación de la red y volver a configurar los protocolos centrales de enrutamiento.

Involucrar a los proveedores de equipos de red para las actualizaciones críticas de firmware o diagnósticos especializados.

Registrar el incidente, alertar a los equipos de seguridad e iniciar un procedimiento preliminar de bloqueo de datos.

Realizar un análisis forense inicial para evaluar el alcance de la vulneración e identificar los sistemas comprometidos.

Conducir auditorías integrales de seguridad e implementar estrategias de remediación para asegurar todos los puntos de datos.

Trabajar con las empresas de ciberseguridad para obtener soluciones avanzadas de detección de amenazas y técnicas de mitigación.

Comprobar el estado de servicio con los proveedores de nube e informar los detalles de la interrupción a los usuarios.

Evaluar las integraciones en las API y realizar comprobaciones en los servicios relacionados para asegurar la conectividad.

Coordinar con los ingenieros de nube para restablecer el servicio y gestionar comprobaciones de la integridad de los datos.

Comunicarse con los proveedores de servicio de nube para obtener un análisis de causa de origen y evitar futuras interrupciones.

|  |
| --- |
| **DESCARGO DE RESPONSABILIDAD**Todos los artículos, las plantillas o la información que proporcione Smartsheet en el sitio web son solo de referencia. Si bien nos esforzamos por mantener la información actualizada y correcta, no hacemos declaraciones ni garantías de ningún tipo, explícitas o implícitas, sobre la integridad, precisión, confiabilidad, idoneidad o disponibilidad con respecto al sitio web o la información, los artículos, las plantillas o los gráficos relacionados que figuran en el sitio web. Por lo tanto, la confianza que usted deposite en dicha información es estrictamente bajo su propio riesgo. |