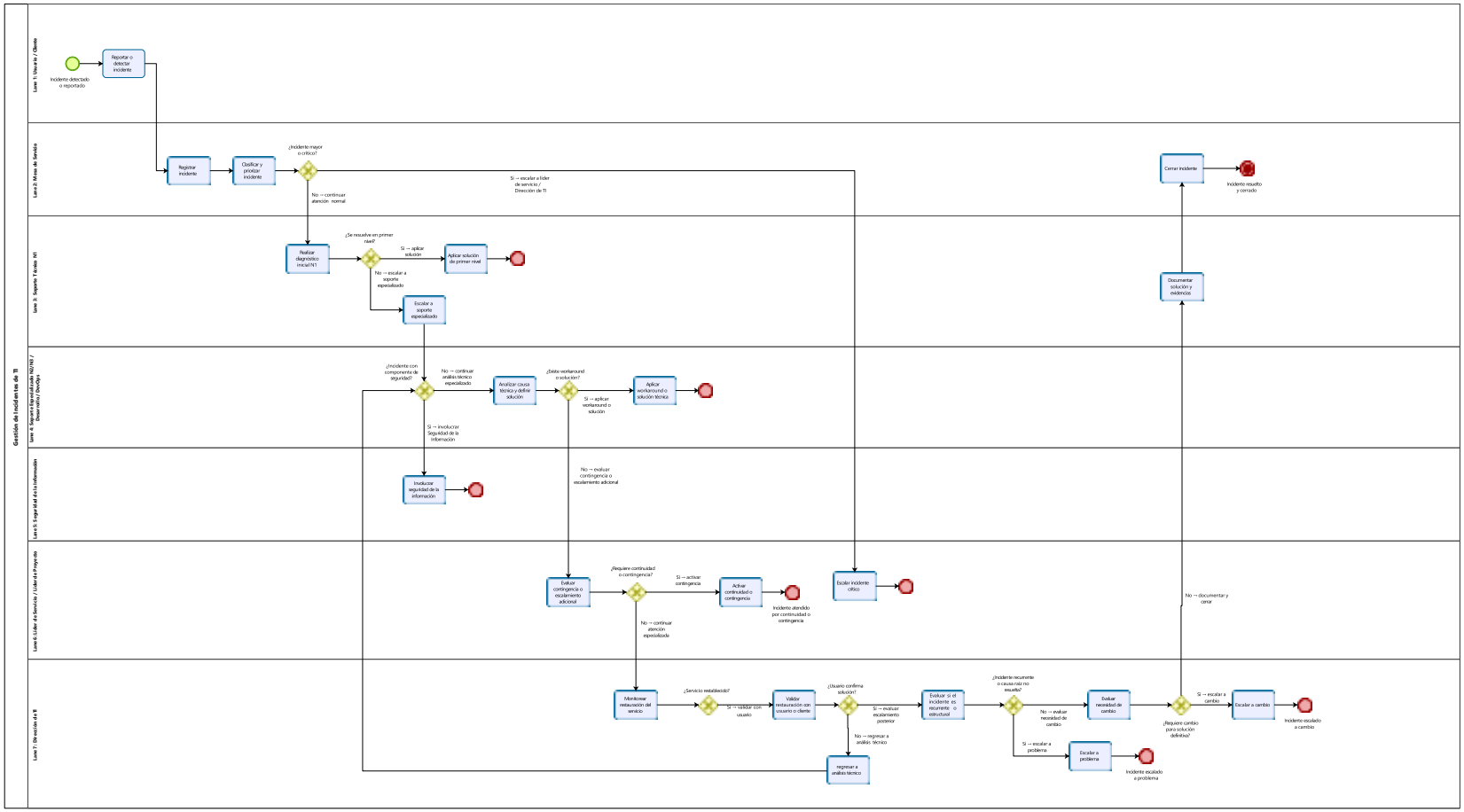
Gestión de Incidentes de TI - TO BE

Bizagi Modeler

Tabla de Contenidos

1 DIAGRAMA 1


Gestión de Incidentes de TI
Lane 1: Usuario / Cliente
Lane 2: Mesa de Servicio
Lane 3: Soporte Técnico N1
Lane 4: Soporte Especializado N2/N3 / Desarrollo / DevOps
Lane 5: Seguridad de la Información
Lane 6: Líder de Servicio / Líder de Proyecto
Lane 7: Dirección de TI
Incidente detectado o reportado
Reportar o detectar incidente
Registrar incidente
Clasificar y priorizar incidente
¿Incidente mayor o crítico?
No → continuar atención normal
Si → escalar a líder de servicio / Dirección de TI
Realizar diagnóstico inicial N1
¿Se resuelve en primer nivel?
Si → aplicar solución
Aplicar solución de primer nivel
No → escalar a soporte especializado
Escalar a soporte especializado
¿Incidente con componente de seguridad?
No → continuar análisis técnico especializado
Analizar causa técnica y definir solución
¿Existe workaround o solución?
Si → aplicar workaround o solución
Aplicar workaround o solución técnica
Si → involucrar Seguridad de la Información
Involucrar seguridad de la información
No → evaluar contingencia o escalamiento adicional
Evaluar contingencia o escalamiento adicional
¿Requiere continuidad o contingencia?
Si → activar contingencia
Activar continuidad o contingencia
Incidente atendido por continuidad o contingencia
No → continuar atención especializada
Escalar incidente crítico
Monitorear restauración del servicio
¿Servicio restablecido?
Si → validar con usuario
Validar restauración con usuario o cliente
¿Usuario confirma solución?
Si → evaluar escalamiento posterior
No → regresar a análisis técnico
regresar a análisis técnico
Evaluar si el incidente es recurrente o estructural
¿Incidente recurrente o causa raíz no resuelta?
No → evaluar necesidad de cambio
Si → escalar a problema
Escalar a problema
Incidente escalado a problema
Evaluar necesidad de cambio
¿Requiere cambio para solución definitiva?
Si → escalar a cambio
No → documentar y cerrar
Escalar a cambio
Incidente escalado a cambio
Documentar solución y evidencias
Cerrar incidente
Incidente resuelto y cerrado

Versión:

1.0

Autor:

Suad Salcedo

1.1 GESTIÓN DE INCIDENTES DE TI

1.1.1 ELEMENTOS DEL PROCESO

1.1.1.1 ☐ Reportar o detectar incidente

Descripción
Se reporta o detecta una afectación sobre un servicio, aplicación, acceso, integración, plataforma o componente tecnológico.

1.1.1.2 ☐ Registrar incidente

Descripción
Se crea el ticket o registro formal del incidente con la información mínima disponible.

Objeto de datos asociado:

- Ticket de incidente
- Registro del incidente

1.1.1.3 ☐ Clasificar y priorizar incidente

Descripción
Se determina categoría, impacto, urgencia y prioridad del incidente conforme a la matriz definida por TICSOFT.

Objeto de datos asociado:

- Clasificación del incidente

Prioridad del incidente

1.1.1.4 ☐ Realizar diagnóstico inicial N1

Descripción

Se revisan síntomas, alcance, base de conocimiento, configuración visible y posibles causas conocidas.

1.1.1.5 ☐ Escalar a soporte especializado

Descripción
Se asigna el incidente al equipo técnico especializado según naturaleza de la afectación.

1.1.1.6 ☐ Analizar causa técnica y definir solución

Descripción
Se revisan logs, infraestructura, código, integraciones, bases de datos o configuraciones para identificar causa y definir solución o workaround.

Objeto de datos asociado:

- Diagnóstico técnico
- Evidencias técnicas
- Plan de atención

1.1.1.7 ☐ Evaluar contingencia o escalamiento adicional

Descripción
Se analiza si debe activarse continuidad, proveedor, gestión de cambio o una ruta extraordinaria.

1.1.1.8 ☐ Monitorear restauración del servicio

Descripción
Se verifica que el servicio, aplicación o componente vuelva a operar con estabilidad.

1.1.1.9 ☐ Validar restauración con usuario o cliente

Descripción
Se confirma con el usuario o cliente que el servicio fue restablecido o que la afectación se encuentra controlada.

1.1.1.10 ☐Evaluar si el incidente es recurrente o estructural

Descripción
Se determina si el incidente requiere remisión a gestión de problemas o a gestión de cambios para una solución definitiva.

1.1.1.11 ☐Documentar solución y evidencias

Descripción
Descripción:
Se registran acciones ejecutadas, tiempos, causa identificada, validaciones, comunicaciones y evidencias del caso.

Objeto de datos asociado:

- Bitácora de atención
- Evidencias
- Registro técnico

1.1.1.12 ☐Cerrar incidente

Descripción
Descripción:
Se formaliza el cierre del incidente una vez resuelto, validado y documentado.

1.1.1.13 ☐Aplicar workaround o solución técnica

Descripción
Se implementa solución temporal o definitiva para restaurar el servicio.

1.1.1.14 ☐Involucrar seguridad de la información

Descripción

Se analiza el incidente desde la perspectiva de integridad, confidencialidad, disponibilidad y riesgo de información.

1.1.1.15 ☐Aplicar solución de primer nivel

Descripción
Se ejecuta corrección básica o solución conocida para restablecer el servicio.

1.1.1.16 ☐Escalar incidente crítico

Descripción
Se activa atención prioritaria, coordinación reforzada y, si aplica, comunicación ejecutiva o contingencia.