[logo de la organización]

[nombre de la organización]

PROCESO DE GESTIÓN DE INCIDENTES

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

Commented [20A1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

Commented [20A2]: Si desea ver más información sobre el proceso de gestión de incidentes, consulte https://advisera.com/20000academy/blog/2013/05/21/incident-management-itil-solid-foundations-operational-processes/

Commented [20A3]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1	20000Academy	Descripción básica del documento

Tabla de contenido

1. Objetivos, alcance y usuarios

El propósito de este documento es definir el objetivo, alcance, principios y actividades para el proceso de gestión de incidentes.

Este documento se aplica a todos los procesos y actividades del SGS.

Los usuarios de este documento son todos los empleados de [nombre de la organización], como también todos los participantes externos que cumplan algún rol en el SGS.

Commented [20A4]: Por favor, incluye el nombre de tu empresa.

2. Documentos de referencia

- ISO/IEC 20000-1:2018, apartado 7.5.4.e), 8.6.1.
- Proceso de gestión de cambios
- Proceso de gestión de problemas
- Proceso de gestión de configuración
- Proceso de gestión de entrega y despliegue
- Proceso de gestión de la seguridad de la información
- Proceso de gestión de nivel de servicios

Commented [20A5]: Puedes encontrar una plantilla para este documento en la carpeta "09_Procesos_Diseño_Construccion_y_Transicion_de_Servicios / 09.1_Gestion_de_cambios".

Commented [20A6]: Puedes encontrar una plantilla para este documento en la carpeta "10_Procesos_de_Resolucion_y_Ejecucion / 10.3_Gestion_de_problemas".

Commented [20A7]: Puedes encontrar una plantilla para este documento en la carpeta "06_Procesos_del_Catalogo_de_Servicios / 06.3_Gestion_de_configuracion".

Commented [20A8]: Puedes encontrar una plantilla para este documento en la carpeta "09_Procesos_Diseño_Construccion_y_Transicion_de_Servicios / 09.3_Gestion_de_Entrega_y_Despliegue".

Commented [20A9]: Puedes encontrar una plantilla para este documento en la carpeta "11_Procesos_Aseguramiento_del_Servicio / 11.3_Gestion_de_la_seguridad_de_la_informacion".

Commented [20A10]: Puedes encontrar una plantilla para este documento en la carpeta "07_Procesos_de_Relacion_y_Acuerdo / 07.2_Gestion_de_niveles_de_servicio".

3. Visión general del proceso

El propósito del proceso de gestión de incidentes es restaurar los servicios de TI lo más rápido posible, minimizar el impacto sobre las operaciones de negocio y asegurar que se mantengan los niveles de servicios (conforme al Acuerdo de Nivel de Servicio).

El alcance del proceso de gestión de incidentes incluye a todos los incidentes de los servicios operacionales incluidos en la Lista de Servicios, así como también los incidentes de seguridad.

Commented [20A11]: Puedes encontrar una plantilla para este documento en la carpeta "04_Plan_del_SGS".

Los objetivos del proceso de gestión de incidentes son los siguientes:

- [illegible]
- [illegible]
- [illegible]

Commented [20A12]: [illegible]

4. Actividades del proceso

La persona que tiene asignado el incidente es la responsable de asegurar que se registre cada actividad a medida que un incidente avanza camino a su resolución; es decir, que se actualice el registro del incidente para que esté disponible todo el historial de resolución.

4.1. Registro de incidentes

[Nombre de la organización] utiliza la herramienta [nombre de la herramienta / Plantilla Registro Incidente] para la gestión de incidentes. [Nombre de la herramienta] registra los incidentes con los datos relacionados que correspondan.

Los incidentes pueden ser registrados por:

a) [illegible]
   - [illegible]
   - [illegible]
   - [illegible]
     - [illegible]
     - [illegible]

b) Herramienta de eventos: [ingrese el nombre de la(s) herramienta(s)]

El personal del Service Desk es responsable de ingresar los datos de los incidentes en [nombre herramienta]/Plantilla Registro Incidentes cuando sean abiertos por teléfono.

Los datos obligatorios que se deben registrar son:

- Número de incidente - proporcionado automáticamente
- Nombre, departamento, ubicación del solicitante
- Nombre, departamento, ubicación del usuario (si es distinto al solicitante)
- Datos de fecha y hora
- [illegible]
- [illegible]
- [illegible]

4.2. Priorización de incidentes

El Analista de Primera Línea es responsable de asegurar que se priorice cada incidente. La prioridad consiste en el impacto y urgencia, tiene 5 niveles y está codificada en base a la siguiente tabla:

Impacto / Urgencia	Alta	Media	Baja
Alta	[illegible]	[illegible]	[illegible]
Media	[illegible]	[illegible]	[illegible]
Baja	[illegible]	[illegible]	[illegible]

El tiempo de resolución de un incidente depende de su código de prioridad y se calcula de la siguiente forma:

Código de prioridad	Descripción	Tiempo objetivo de resolución

Commented [20A13]: La persona encargada de trabajar sobre el incidente, registra las acciones que lleva a cabo para resolver el incidente.

Commented [20A14]: Ingrese el nombre de la herramienta de gestión de incidentes.

Commented [20A15]: Ingrese el nombre de la herramienta de gestión de incidentes.

Commented [20A16]: Eliminar si tu empresa no utiliza una herramienta para registra incidentes.

Commented [20A17]: Adapte a su propia situación.

Commented [20A18]: [illegible]

Commented [20A19]: [illegible]

Commented [20A20]: Ingrese la dirección de correo electrónico que se utiliza para abrir un incidente.

Commented [20A21]: [illegible]

Commented [20A22]: Incluye el número de teléfono en el formato adecuado, de acuerdo al horario establecido.

Commented [20A23]: Puedes adaptarlo de acuerdo a las prácticas de tu organización.

Commented [20A24]: Selecciona el que aplique.

Commented [20A25]: [illegible]

Commented [20A26]: Estos datos siempre son necesarios. [illegible]

Commented [20A27]: Esto sólo es una recomendación; puedes adaptar los niveles de prioridad de acuerdo a las prácticas de tu organización.

1	Crítico	1 hora
2	Alto	2 horas
3	Media	4 horas
4	Baja	8 horas
5	Planificada	24 horas

Impacto - impacto en el negocio que ocasiona un incidente:

[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

Urgencia - qué tan rápida es necesaria una resolución para el negocio

Alta	Media	Baja
Inmediatamente: sin solución temporal disponible	A mediano plazo: no existe solución temporal parcial	A largo plazo: existe solución temporal satisfactoria

Cambio de prioridad - la prioridad definida por un usuario puede/no puede ser modificada por el Service desk bajo las siguientes circunstancias [escribir descripción].

4.3. Clasificación de incidentes

Después de la priorización, los incidentes son clasificadas. Personal del Service Desk clasifica los incidentes iniciados por teléfono. El Service Desk verifica la clasificación de incidentes abiertos por otros medios, y si es necesario pueden ser re-categorizados.

[illegible]

Los incidentes podrán ser de los siguientes tipos:

- [illegible]
    - [illegible]
    - [illegible]
    - [illegible]
    - [illegible]
- [illegible]
    - [illegible]
    - [illegible]
- [illegible]
    - [illegible]
    - [illegible]

Commented [20A28]: Debe ser adaptado de acuerdo a 1) necesidades de la organización o 2) SLS con un cliente determinado.

Commented [20A29]: [illegible]

Commented [20A30]: [illegible]

Commented [20A31]: [illegible]

Commented [20A32]: Se debe escoger una de las afirmaciones, la otra debe ser eliminada.

Commented [20A33]: Selecciona lo que aplique a las prácticas de tu organización.

Commented [20A34]: [illegible]

Commented [20A35]: Elimina esta sección en el caso de que la prioridad no pueda ser modificada bajo ninguna circunstancia.

Commented [20A36]: [illegible]

Commented [20A37]: Modifique según su propia organización.

Commented [20A38]: [illegible]

Commented [20A39]: [illegible]

    - Estación de trabajo
    - Impresora
- [illegible]
    - [illegible]
    - [illegible]
    - [illegible]
- [illegible]

Los incidentes de seguridad de la información son clasificados como [Seguridad de la Información] y con una prioridad que se establece utilizando las siguientes directrices […].

El Gerente de cambios es el responsable de decidir qué cambios serán manejados a través del proceso de gestión de incidentes.

4.4. Escalado

Para resolver los incidentes tan pronto como sea posible y/o ahorrar tiempo a la hora de escalarlos, se utiliza una base de conocimiento. Por lo tanto, todos los empleados que tienen asignados roles en [illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]

Si los incidentes no pueden ser resueltas se ejecuta el procedimiento de escalado. Existen dos posibles escalados:

- Escalado funcional
- Escalado jerárquico

[illegible] del mismo.

4.4.1. Escalado funcional

[illegible] propietario del incidente es responsable de la coordinación si hay más de un grupo de soporte involucrado en la resolución.

4.4.2. Escalado jerárquico

El escalado jerárquico es iniciado por el [cargo] o la herramienta [nombre de la herramienta]. El escalado jerárquico se utiliza en las siguientes situaciones:

- Para incidentes de alta prioridad: se informa al Gerente de Incidentes y la Gerente de nivel de servicios acerca de ese incidente.

Commented [20A40]: [illegible]

Commented [20A41]: [illegible]

Commented [20A42]: Describe un manejo de prioridad para un incidente de seguridad. Ejemplo: "Incrementado por un alto impacto".

Commented [20A43]: Puedes encontrar una plantilla para este documento en la carpeta "10_Procesos_de_Resolucion_y_Ejecucion / 10.3_Gestion_de_problemas".

Commented [20A44]: Puedes encontrar una plantilla para este documento en la carpeta "10_Procesos_de_Resolucion_y_Ejecucion / 10.3_Gestion_de_problemas".

Commented [20A45]: Puedes encontrar una plantilla para este documento en la carpeta "06_Procesos_del_Catalogo_de_Servicios / 06.3_Gestion_de_configuracion".

Commented [20A46]: Sólo son ejemplos; puedes modificarlos, eliminarlos, o incluir información adicional de acuerdo a las prácticas de tu organización.

Commented [20A47]: Puedes encontrar una plantilla para este documento en la carpeta "09_Procesos_Diseño_Construccion_y_Transicion_de_Servicios / 09.3_Gestion_de_Entrega_y_Despliegue".

Commented [20A48]: [illegible]

Commented [20A49]: [illegible]

Commented [20A50]: [illegible]

Commented [20A51]: El SLA define las reglas y el manejo de [illegible]

Commented [20A52]: Modifique en caso que sea necesario.

Commented [20A53]: Elimine lo que no es necesario. Ejemplo de rol que escala un incidente: quien tiene asignado, gerente de incidentes, gerente de nivel de servicios.

Commented [20A54]: Modifique en caso que sea necesario.

- [illegible]
- [illegible]

El empleado que realiza el escalado es responsable de manejar este escalado y de informar al Gerente de Incidentes.

Si se ha acordado en el SLA, el Gerente de Incidentes informa al Gerente de Nivel de Servicio cuando un incidente alcanza el 90% de objetivo de resolución, y es obvio que no se va a cumplir el SLA. El Gerente de Nivel de Servicio debe informar al cliente sobre el incumplimiento del SLA.

4.5. Resolución

[illegible]

El Gerente de Incidentes es responsable de lo siguiente:

- Definir el personal responsable para la prueba y verificación de resolución.
- Asegurar que se actualice el registro del incidente.
- Coordinar las actividades entre los grupo de soporte o terceros.

[illegible]

El Analista de Primera Línea verifica que el incidente esté totalmente resuelto y que el usuario esté satisfecho y dispuesto a acordar que el incidente pueda se finalmente cerrado.

[illegible]

Si los incidentes son clasificados como incidentes de seguridad de la información, una vez que son cerrados, el Gerente de Serguridad de la Información es responsable de:

- Analizar el tipo, volumen e impacto del incidente de seguridad de la información.
- Informar el incidente al Gerente de Nivel de Servicio.
- [illegible]

4.6. Incidente grave

Los incidentes graves son incidentes con mayor impacto que implican una interrupción significativa de los servicios y que requieren atención especial para su resolución. Los incidentes graves son específicos del cliente, son definidos en función del cliente y son una parte obligatoria del SLA. El Gerente de Incidentes es responsable de:

- Informar a [cargo].

Commented [20A55]: [illegible]

Commented [20A56]: Modifique de acuerdo a la definición del OLA o UC.

Commented [20A57]: [illegible]

Commented [20A58]: Puedes encontrar una plantilla para este documento en la carpeta "07_Procesos_de_Relacion_y_Acuerdo / 07.2_Gestion_de_niveles_de_servicio".

Commented [20A59]: Sólo son ejemplos; puedes eliminarlos, o incluir elementos adicionales de acuerdo a las prácticas de tu organización.

Commented [20A60]: Modifique en caso que sea necesario. Por ejemplo: Gerente de incidentes, Gerente del grupo de resolución, etc.

Commented [20A61]: [illegible]

Commented [20A62]: [illegible]

Commented [20A63]: [illegible]

Commented [20A64]: Selecciona el que aplique de acuerdo a las prácticas de tu organización.

Commented [20A65]: Borre la parte redundante.

Commented [20A66]: Borre este párrafo si: [illegible]

Commented [20A67]: Debes escribir este párrafo de acuerdo a las condiciones acordadas en el SLA.

Commented [20A68]: [illegible]

Commented [20A69]: Por ej., Gerente de nivel de servicios, Gerente de mejora continua de servicios.

Commented [20A70]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo_ CEO, CIO, Director RI, Responsable TI, Responsable del Servicio, etc.

- La definición del procedimiento para incidente grave (como parte del SLA) debe incluir:
    - Declaración de incidente grave
    - Gestión (es decir, manejo de incidentes graves)
    - [illegible]
    - [illegible]
    - [illegible]

Commented [20A71]: [illegible]

Commented [20A72]: Por ejemplo, grupo de soporte.

Commented [20A73]: [illegible]

El Gerente de Relaciones de Negocio es responsable de comunicar el progreso, las actividades y los resultados al cliente tal como se haya documentado en el Informe de Incidentes Graves.

El [función de alta gerencia] nombra al Gerente de incidentes graves.

Commented [20A74]: Por ej., CIO, Junta directiva, etc.

5. Roles y responsabilidades

5.1. Gerente de incidentes

El [cargo] asigna el rol de Gerente de incidentes.

Commented [20A75]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo_ CEO, CIO, Director RI, Responsable TI, Responsable del Servicio, etc.

Responsabilidades del Gerente de incidentes son:

- Responsabilidad general de ejecutar las actividades dentro del alcance de la Gestión de incidentes.
- Coordinar con otros roles de gestión del servicio.
- Planificar y administrar las herramientas necesarias para respaldar el proceso de gestión de incidentes.
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Commented [20A76]: [illegible]

5.2. Analista de primera línea (1° nivel)

El [cargo] asigna el rol de Analista de primera línea.

Commented [20A77]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo_ CEO, CIO, Director RI, Responsable TI, Responsable del Servicio, etc.

Commented [20A78]: [illegible]

Responsabilidades del Analista de primera línea:

- Registrar incidentes
- Clasificación, priorización y escalado de incidentes
- Resolución y recuperación de incidentes
- Monitoreo del estado y progreso de incidentes asignados
- Cierre de incidentes
- Informar a usuarios sobre progreso de incidentes
- Actualizar el registro de incidentes

Commented [20A79]: Sólo son recomendaciones; puedes eliminar o incluir elementos adicionales de acuerdo a las prácticas de tu organización.

5.3. Analista de segunda línea (2° nivel)

Commented [20A80]: [illegible]

El [cargo] asigna el rol de Analista de segunda línea.

Commented [20A81]: Generalmente es un perfil con un conocimiento más técnico que el Analista de Primera Línea.

Responsabilidades del Analista de segunda línea:

- Igual que el Analista de primera línea pero con conocimientos técnicos mucho más profundos y mayor dedicación de tiempo a la resolución del incidente.

6. Medición y reporte

El Gerente de incidentes es responsable de:

- Definir y revisar [anualmente] los Factores Críticos de Éxito (CSFs) que soportan los actuales objetivos definidos para el SGS en el Plan del SGS, y los correspondientes KPIs que pueden ser utilizados para monitorizar el progreso de cumplimiento de los CSFs.
- [redacted]

Commented [20A82]: Puedes modificar la frecuencia de acuerdo a las prácticas empleadas por tu organización.

Commented [20A83]: Puedes encontrar una plantilla para este documento en la carpeta "13_Revision_por_parte_de_la_direccion".

Commented [20A84]: Puedes modificar la frecuencia de acuerdo a las prácticas empleadas por tu organización.

Commented [20A85]: Puedes encontrar algunos ejemplos de [redacted]

Commented [20A86]: Puedes modificar la frecuencia de acuerdo a las prácticas empleadas por tu organización.

Cuando se actualicen los objetivos del SGS en el Plan del SGS, el Gerente de incidentes revisa y actualiza los CSFs y los KPIs en la Matriz de Mediciones del Proceso, para reflejar los nuevos objetivos.

7. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Registro de incidentes (en formato electrónico)	[nombre de la herramienta]	Gerente de Incidentes	Analistas de Primera Línea y Segunda Línea tienen permiso para agregar o modificar el registro.	Los registros de incidentes se guardan para siempre.
Informe de Incidente Grave	[nombre de la herramienta]	Gerente de Incidentes	Gerente de Incidentes	Los Informes de Incidentes Graves se almacenan de manera permanente

Commented [20A87]: Modifique en caso que sea necesario.

Informes	[nombre de la herramienta]	Gerente de Incidentes	Gerente de incidentes	Los informes se guardan por un periodo de [3 años].

Commented [20A88]: Modifique en caso que sea necesario.

Commented [20A89]: Ajusta la frecuencia de acuerdo a las prácticas de tu organización.

8. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

El propietario de este documento es el Gerente de Incidentes, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Commented [20A90]: Sólo es una recomendación; puedes cambiar la frecuencia de acuerdo a las prácticas de tu organización.

9. Apéndices

- Apéndice 1 – Registro de incidentes
- Apéndice 2 – Informe de incidente grave

[cargo]
[nombre]

____
[firma]

Commented [20A91]: Sólo es necesario si el Procedimiento para control de documentos establece que los documentos en papel deben ser firmados.