<table>
<thead>
<tr>
<th>Código:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Versión:</td>
<td></td>
</tr>
<tr>
<td>Fecha de la versión:</td>
<td></td>
</tr>
<tr>
<td>Creado por:</td>
<td></td>
</tr>
<tr>
<td>Aprobado por:</td>
<td></td>
</tr>
<tr>
<td>Nivel de confidencialidad:</td>
<td></td>
</tr>
</tbody>
</table>

Comment [BV1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

Comment [BV2]: 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

<table>
<thead>
<tr>
<th>Fecha</th>
<th>Versión</th>
<th>Creado por</th>
<th>Descripción de la modificación</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx/xx/2013</td>
<td>0.1</td>
<td>Branimir Valentic</td>
<td>Plantilla básica del documento</td>
</tr>
</tbody>
</table>

Tabla de contenido

1. OBJETIVO, ALCANCE Y USUARIOS .................................................................................... 3
2. DOCUMENTOS DE REFERENCIA .................................................................................... 3
3. POLÍTICA .................................................................................................................... 3
   3.1. GESTIÓN DE INCIDENTES ...................................................................................... 3
   3.2. COMUNICACIÓN ...................................................................................................... 4
   3.3. PLAZO .................................................................................................................... 4
   3.4. SATISFACCIÓN DEL CLIENTE ................................................................................... 4
   3.5. REAPERTURA DE INCIDENTES ................................................................................. 4
   3.6. REGISTROS DE INCIDENTES .................................................................................... 5
   3.7. MEDICIÓN ............................................................................................................. 5
4. VALIDEZ Y GESTIÓN DE DOCUMENTOS ........................................................................ 5
1. Objetivo, alcance y usuarios

El objetivo de esta política es asegurar todo incidente que afecte las operaciones diarias de [nombre de la organización] sean tratados a través de un proceso establecido.

Esta política aplica a todos los empleados de tiempo completo, de media jornada y contratados de [nombre de la empresa]; como también a proveedores relacionados en actividades que utilizan o manejan soluciones tecnológicas dentro de [nombre de la empresa].

Los usuarios de este documento son empleados de [organización de gestión de servicios de TI].

2. Documentos de referencia

- Proceso de gestión de incidentes
- Proceso de gestión de niveles de servicios
- Medición y métricas
- Proceso de gestión de relaciones del negocio
- Proceso de gestión de la seguridad de la información
- Procedimiento de comunicación

3. Política

3.1. Gestión de incidentes

El propósito del proceso de gestión de incidentes es restaurar los servicios de TI lo más rápido posible, minimizar el impacto sobre los usuarios y asegurar que se mantengan los niveles de servicios (consultar el Proceso de gestión de incidentes).

Todos los incidentes de [nombre de la organización] son gestionados de acuerdo al proceso de gestión de incidentes.

El alcance del proceso de gestión de incidentes incluye a todos los incidentes de los servicios proporcionados. Se identifican incidentes en el diagnóstico del proceso de gestión del portafolio de servicios, como también los incidentes relacionados con seguridad de la información (consultar el proceso de gestión de la seguridad de la información).

El objetivo de la gestión de incidentes es:

- Aumentar la satisfacción del cliente con servicios brindados a través de una gestión eficiente de incidentes.
- Prevenir y gestionar un proceso estandarizado para identificar incidentes de ITSM y los usuarios y clientes.
3.2. Comunicación

El [descripción del rol] es responsable de definir las formas de comunicación y las responsabilidades entre los diferentes grupos de intereses, como clientes, hacia el servicio del departamento de TI, y los usuarios, las personas que utilizan diariamente el servicio. En adelante, serán denominados "usuarios".

Para asegurar que la información sea compartida a tiempo (cuando es necesaria, durante todo el año), se debe definir en los Acuerdos de niveles de servicio (SLA) el tipo de comunicación que se debe realizar con la persona que abre el incidente (el usuario interno, hacia el departamento de TI, como externa, hacia los usuarios), el [descripción del rol] es responsable de:

- Capacitar al personal del Service desk, soporte de 1° nivel, soporte de 2° nivel (consultar el Proceso de gestión de incidentes).
- Introducir soluciones tecnológicas:
  - Correo electrónico
  - [Opción]
  - [Opción]
  - [Opción]

El [descripción del rol] es el responsable de informar al incidente que ellos han abierto.

El procedimiento de comunicación está definido en el documento "Procedimiento de comunicación".

3.3. Plazo

Los plazos en los que se deben resolver los incidentes están definidos en los Acuerdos de niveles de servicio (SLA), el [descripción del rol] es el responsable de definir los plazos en la herramienta [nombre de la herramienta].

3.4. Satisfacción del cliente

La satisfacción del cliente se mide de la siguiente forma:

a) Una vez que se resolvió un incidente, el usuario puede enviar sus comentarios a través de un formulario de comentarios, que se recoge en el servicio de soporte del departamento de TI, el [descripción del rol] recibe los comentarios de los clientes e informa los resultados a [descripción del rol].

b) Una vez al año, el [descripción del rol] realizará una Encuesta de satisfacción del cliente (consultar en el Apéndice del proceso de gestión de relaciones del negocio). Los resultados de la encuesta serán informados a [descripción del rol].

3.5. Reapertura de incidentes
Los incidentes pueden ser reabiertos por [descripción del rol]. La reapertura de incidentes se puede producir, como máximo, tres (3) veces después que el incidente fue cerrado. Si la solicitud de cambio de estado de incidente debe informarse mensualmente, y utilizando [...], todos los incidentes reabiertos.

3.6. Registros de incidentes

Todos los registros de incidentes se guardan y gestionan en un único sistema de gestión. Para ello se utiliza [nombre de la herramienta]. Todos los registros de incidentes se documentan para su posterior análisis. Los servicios de TI están obligados a ingresar y actualizar todos los estados y datos detallados.

El [descripción del rol] es responsable de auditar la integridad de los incidentes [una vez por año].

La auditoría incluye la verificación de los siguientes parámetros:

- Todos los estados actualizados están ingresados.
- Se han registrado todas las actividades.
- Los incidentes están correctamente priorizados.

3.7. Medición

Los requerimientos de rendimiento y métricas están definidos en el documento “Medición y métricas”.

4. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

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

[cargo]

[nombre]

[firma]

Comment [BV17]: Modifique en caso que sea necesario.

Comment [BV18]: Los incidentes reabiertos son responsabilidad del Gerente rol delegado.

Comment [BV19]: Modifique en caso que sea necesario.

Comment [BV20]: Describa el método Ti o una hoja de cálculo.

Comment [BV21]: Ingrese el nombre de la herramienta o hoja de cálculo.

Comment [BV22]: Escriba la persona Gestión de servicios de TI (por ejemplo, alguien de gestión de calidad).

Comment [BV23]: Modifique en caso que sea necesario.

Comment [BV24]: Modifique según sus propios requerimientos.

Comment [BV25]: Esta es sólo una recomendación, ajustar la frecuencia según sea necesario.

Comment [BV26]: Sólo es necesario si el Procedimiento para control de documentos establece que los documentos en papel deben ser firmados.