[logo de la organización]

[nombre de la organización]

Commented [20A1]: All fields in this document marked by square brackets [ ] must be filled in.

POLÍTICA DE GESTIÓN DE RIESGOS

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

Commented [20A2]: 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 plantilla

Tabla de contenidos

1. Objetivo, alcance y usuarios

El propósito de esta política es garantizar que los riesgos y oportunidades de [nombre de la organización] son gestionados a través de un proceso establecido.

Este documento aplica a todas las actividades, procesos y documentos incluidos en el alcance del SGS.

Los usuarios de este documento son todos empleados de [nombre de la organización], así como todas las partes externas relevantes que tienen un rol en el SGS.

2. Documentos de referencia

- ISO/IEC 20000-1:2018, apartado 8.5.1
- Plan SGS
- Proceso de Gestión de Continuidad del Servicio TI
- Proceso de Gestión de Disponibilidad
- Proceso de Gestión de Seguridad de la Información
- Proceso de Gestión de Proveedores
- Proceso de Gestión de Cambios

3. Política

3.1. Alcance y metas de la gestión de riesgos

El alcance de la gestión de riesgos de [Nombre de la organización] cubre todos los riesgos y oportunidades que pueden tener un impacto en el SGS y los servicios proporcionados por la organización.

Los objetivos de la gestión de riesgos son:

- dar garantías de que el SGS puede lograr sus resultados previstos
- prevenir o reducir los efectos no deseados de los riesgos
- [redacted]

3.2. Guía del proceso

[redacted]

La descripción detallada del proceso se documenta a continuación:

3.2.1. Identificación y registro

Cualquier empleado puede identificar nuevos riesgos y oportunidades durante las siguientes fases:

Commented [20A3]: Por favor, incluye el nombre de tu organización

Commented [20A4]: Puedes encontrar una plantilla para este documento en la carpeta "04_Plan_de_SGS"

Commented [20A5]: Puedes encontrar una plantilla para este documento en la carpeta "11_Procesos_Aseguramiento_del_Servicio / 11.2_Gestion_de_continuidad_del_servicio_de_TI".

Commented [20A6]: Puedes encontrar una plantilla para este documento en la carpeta "11_Procesos_Aseguramiento_del_Servicio / 11.1_Gestion_de_disponibilidad"

Commented [20A7]: 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 [20A8]: Puedes encontrar una plantilla para este documento en la carpeta "07_Procesos_de_Relacion_y_Acuerdo / 07.3_Gestion_de_proveedores"

Commented [20A9]: Puedes encontrar una plantilla para este documento en la carpeta "09_Procesos_Diseño_Construccion_y_Transicion_de_Servicios/09.1_Gestion_de_cambios"

Commented [20A10]: [redacted]

- Planificación del SGS
- [illegible]
- [illegible]
- Realización de revisiones por parte de dirección
- Realización de auditorías internas
- Recibir comentarios de clientes y otras partes interesadas

Commented [20A11]: Ejemplo: Proceso de Gestión de la [illegible]

Siempre que un empleado identifique un nuevo riesgo en [nombre de la organización], el empleado debe informar al [cargo]. [cargo] crea una nueva entrada en el Registro de Riesgos y Oportunidades (en la hoja de cálculo "Riesgo").

Commented [20A12]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo: Gerente TI, Gerente Servicio, Gerente Riesgos, etc.

Cada vez que un empleado de [nombre de la organización] identifica una nueva oportunidad, el empleado debe informar al [cargo]. [cargo] crea una nueva entrada en el Registro de Riesgos y Oportunidades (en la hoja de cálculo "Oportunidad").

Commented [20A13]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo: Gerente TI, Gerente Servicio, Gerente Riesgos, etc.

3.2.2. Análisis

Una vez identificados los riesgos, el propietario del riesgo realizará una evaluación del impacto y la [illegible]

Análisis de impacto:

Impacto Bajo	0	[illegible]
[illegible]	1	Situaciones que pueden incurrir en costes adicionales y tienen un impacto bajo o moderado en las obligaciones legales o contractuales, o la reputación de la organización.
Impacto Alto	2	[illegible]

Análisis de probabilidad:

[illegible]	0	Los controles existentes son sólidos y hasta ahora han proporcionado un nivel adecuado de protección. No se esperan nuevos incidentes en el futuro.
Probabilidad Moderada	1	[illegible]
[illegible]	2	Los controles existentes son bajos o ineficaces. Estos incidentes tienen una alta probabilidad de ocurrir en el futuro.

El propietario del riesgo registra los resultados de la evaluación de riesgos en el Registro de Riesgos y Oportunidades (en la hoja de cálculo "Riesgo").

[illegible]

3.2.3. Evaluación

Los siguientes criterios de aceptación de riesgos deben ser utilizados por el propietario de riesgos para evaluar los riesgos: [Los valores 0, 1 y 2 indican riesgos aceptables, mientras que los valores iguales y/o mayores a 3 indican riesgos inaceptables].

3.2.4. Tratamiento

Cada riesgo no aceptable debe ser tratado. El propietario del riesgo debe decidir sobre una medida [illegible]

- Implementación de controles para reducir el nivel de riesgo
- Transferencia parcial de riesgos a terceros (a través de seguros o externalización)
- Evitar el riesgo (renunciar a ciertas actividades que introducen el riesgo, pero con la salvedad de perder cualquier oportunidad asociada con esas actividades)

Si la respuesta al riesgo implica la implementación de un control, [cargo] documentará los controles elegidos en el Registro de riesgos y oportunidades (hoja de cálculo "Controles").

El propietario de la oportunidad evaluará cualquier oportunidad identificada en función del coste estimado y los beneficios esperados de la oportunidad y decidirá sobre una medida de respuesta [illegible]

Commented [20A14]: Sólo son recomendaciones; puedes adaptarlo de acuerdo a las prácas de tu organización.

Commented [20A15]: [illegible]

Commented [20A16]: Puedes modificar el nivel de riesgo acceptable de acuerdo a las practices de tu organización.

Commented [20A17]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo: Gerente TI, Gerente Servicio, Gerente Riesgos, etc.

Commented [20A18]: [illegible]

3.2.5. Monitorización

Para cualquier nuevo riesgo y oportunidad documentado en el Registro de Riesgos y Oportunidades, [cargo] notificará a los propietarios de riesgos/oportunidades tan pronto como se actualice el Registro de Riesgos y Oportunidades.

[redacted]

Commented [20A19]: Modifica la frecuencia de acuerdo a las prácticas de tu organización

Commented [20A20]: [redacted]

4. Validez y gestión de documentos

Este documento es válido a partir de [fecha].

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

Commented [20A21]: [redacted]

Commented [20A22]: Sólo es una recomendación; por favor, ajusta la frecuencia de acuerdo a las prácticas de tu organización

5. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del almacenamiento	Controles para la protección del registro	Tiempo de retención
Registro de Riesgos y Oportunidades	[nombre herramienta]	[cargo]	[cargo]	[...]

Commented [20A23]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo: Gerente TI, Gerente Servicio, Gerente Riesgos, etc

Commented [20A24]: Añadir la descripción apropiada de acuerdo a las prácticas de tu organización. Ejemplo: Gerente TI, Gerente Servicio, Gerente Riesgos, etc

Commented [20A25]: Example: for current year (YTD) – in [tool name], otherwise archived in [tool name or place of archive].

6. Apéndices

- Apéndice 1 – Registro de Riesgos y Oportunidades

[cargo]
[nombre]

_____
[firma]

Commented [20A26]: Sólo es necesario si el Procedimiento para control de documentos establece que los documentos en papel deben ser firmados.