 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	1 de 21

	ELABORADO POR		REVISADO POR		APROBADO POR	
Nombre/ Cargo	Elizenda Quispe Castillo	Responsable de la Unidad de Integridad	María Dolores Peche Becerra	Gerente de Modernización, Planeamiento y Presupuesto	Claudett Katerina Delgado Llanos	Gerente General
Firma						
Nombre/ Cargo	Guillermo Pérez Silva	Gerente de Tecnologías de Información				
Firma						

1. OBJETIVO


Establecer las actividades para identificar, analizar, evaluar y gestionar las conductas, operaciones, y/o acciones en las cuales podrían materializarse riesgos de soborno y de seguridad de la información, considerando el contexto institucional del Poder Judicial, así como identificar y gestionar las oportunidades en estas materias, estableciendo un proceso sistemático, planificado y coherente.

2. ALCANCE

La presente guía es de obligatorio cumplimiento por todas las unidades de organización y funcionales del Poder Judicial a cargo de los procesos que se encuentran comprendidos dentro del alcance del SGA y del SGSI, del Poder Judicial, conforme con los requisitos propios de la Entidad y los requisitos de la NTP ISO 37001 y de la NTP ISO/IEC 27001, respectivamente.

3. BASE NORMATIVA


- 3.1. Resolución Directoral N.º 012-2017- INACAL/DN, que aprueba la Norma Técnica Peruana - NTP- ISO 37001:2017. Sistema de Gestión Antisoborno. Requisitos con orientación para su uso.
- 3.2. Resolución Directoral N.º 022-2022-INACAL /DN que aprueba la Norma Técnica Peruana NTP-ISO/IEC 27001:2022; Norma Técnica Peruana NTP-ISO/IEC 27005:2022 y la Norma Técnica Peruana NTP ISO/IEC 27002:2022
- 3.3. Norma Técnica Peruana NTP-ISO/IEC 27005:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3a Edición
- 3.4. Decreto Supremo N.º 092-2017-PCM, que aprueba la Política Nacional de Integridad y Lucha contra la Corrupción
- 3.5. Decreto Supremo N.º 180-2021-PCM que, en la Única Disposición Complementaria Transitoria, dispone la vigencia de la Tabla N.º 11 del Plan Nacional de Integridad y Lucha contra la Corrupción 2018-2021, aprobado por Decreto Supremo N.º 044-2018-PCM, se mantiene vigente hasta la actualización de la Política Nacional de Integridad y Lucha contra la Corrupción.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO	UI/GUI-006	
	GUÍA	Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Página:	2 de 21

- 3.6. Resolución de secretaría de Gobierno y Transformación Digital N.º 003-2023-PCM/SGTD: Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.
- 3.7. Resolución de secretaría de Gobierno y Transformación Digital N.º 002-2023-PCM/SGTD: Aprueban la Directiva N.º 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
- 3.8. Resolución Administrativa N.º 247-2023-CE-PJ, que aprobó la Directiva N.º 004-2023-CE-PJ, denominada “Disposiciones para el Desarrollo de Documentos Normativos del Poder Judicial” – Versión 003.
- 3.9. Resolución Administrativa de Sala Plena N.º 050-2024-SP-CS-PJ, que aprueba la Política Sistema de Gestión del Poder Judicial.
- 3.10. Directiva “Sistema de Gestión antisoborno del Poder Judicial”
- 3.11. Resolución de Secretaría de Integridad Pública N.º 001-2023-PCM/SIP, que aprueba la Guía para la gestión de riesgos que afectan la Integridad Pública, aprobada mediante

4. DEFINICIONES

- 4.1. **Amenaza:** Causa potencial de un incidente de seguridad de la información que puede resultar en daño a un sistema o daño a una organización.
- 4.2. **Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.
- 4.3. **Control:** Actividad que tiene como finalidad reducir la criticidad de un riesgo. Medida que mantiene y/o modifica el riesgo.
- 4.4. **Efecto:** Es una desviación de lo esperado, ya sea positivo o negativo.
- 4.5. **Evaluación de riesgo:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su importancia es aceptable o tolerable.
- 4.6. **Fuente de riesgo:** elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.
- 4.7. **Identificación de riesgo:** Proceso de encontrar, reconocer y describir los riesgos.
- 4.8. **Impacto:** Grado en que el riesgo, de materializarse, impactará en la entidad. Es decir, la pérdida cuantitativa (factores financieros o monetarios) o cualitativa (reputación o imagen, incumplimiento de normas o regulaciones).
- 4.9. **Incertidumbre:** Estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su probabilidad.
- 4.10. **Incidente de seguridad de la información:** Un evento único o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- 4.11. **Nivel de riesgo:** Importancia de un riesgo, expresada en términos de la combinación de consecuencias y su probabilidad.
- 4.12. **Oficial de Cumplimiento del SGA:** Persona con responsabilidad y autoridad para la operación del Sistema de Gestión Antisoborno del Poder Judicial.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	3 de 21


- 4.13. Responsable de Seguridad y Confianza Digital:** Personal designado por la Corte Superior de Justicia que coordina, apoya y articula con el Oficial de Seguridad y Confianza Digital la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información en la Corte Superior de Justicia.
- 4.14. Parte Interesada:** persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
- 4.15. Plan de acción:** Conjunto de acciones enfocadas a reducir el nivel de riesgo, formuladas de acuerdo con la estrategia de tratamiento al riesgo seleccionada.
- 4.16. Probabilidad:** Posibilidad de ocurrencia de un riesgo en un periodo de tiempo determinado. Puede ser calculada en función a cuántas veces históricamente ha ocurrido o se prevé que pueda suceder en el futuro.
- 4.17. Proceso:** Conjunto de actividades relacionadas de manera lógica que utilizan elementos de entrada para proporcionar un resultado previsto o elementos de salida determinados
- 4.18. Propietario del riesgo:** Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
- 4.19. Riesgo y Oportunidades:** Efecto de la incertidumbre en la consecución de los objetivos. Estos efectos pueden ser desviaciones negativas o adversas (riesgos) y/o desviaciones positivas o beneficiosas (oportunidades).
- 4.20. Riesgo inherente:** Es el riesgo en su forma natural sin el efecto mitigante de los controles.
- 4.21. Riesgo residual:** Nivel resultante del riesgo después de aplicar los controles.
- 4.22. Soborno:** Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directa o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.
- 4.23. Vulnerabilidad (V):** Estado producido por la inexistencia o ineficacia de las medidas específicas (jurídicas, técnicas u organizativas) encaminadas a eliminar el riesgo en su origen o, en su caso, mitigarlo mediante una adecuada gestión. La vulnerabilidad es el factor reductor considerado una vez aplicadas las medidas y que nos permite estimar el riesgo residual. Inicialmente, en el caso de que no existan medidas implementadas, se considerará como 1.

5. RESPONSABLES

Son responsables del cumplimiento de las disposiciones contenidas en la presente guía, conforme al detalle siguiente:

5.1 El/La funcionario/a responsable de la Unidad de Integridad

Es responsable de supervisar y velar por el cumplimiento de las actividades contenidas en la presente guía, para lo cual cuenta con el apoyo del equipo que conforma la Unidad de Integridad.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO	UI/GUI-006	
	GUÍA	Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Página:	4 de 21

Asimismo, lidera, organiza y conduce las reuniones de identificación y revisión de los potenciales riesgos de soborno; y, de las oportunidades del SGA, para su posterior evaluación y establecimiento de medidas de tratamiento o acciones de mejora que correspondan.

5.2 El responsable que ejerce el rol de la función de Integridad en las Cortes Superiores de Justicia

Se encarga de la implementación, mantenimiento, seguimiento y mejora del Sistema de Gestión Antisoborno (SGA) en su respectiva jurisdicción y realiza actividades en coordinación con la Unidad de Integridad.

5.3 El Oficial de Seguridad y Confianza Digital

Es responsable de conducir el proceso de identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información, en coordinación y con el apoyo de los dueños de los procesos, propietarios de riesgos y responsables de las unidades de organización del Poder Judicial.

Asimismo, es responsable de coordinar con los dueños de procesos, propietarios de riesgos y responsables de las unidades de organización del Poder Judicial su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia.


5.4 El responsable de Seguridad y Confianza Digital:

Es el responsable de la gestión de riesgos de seguridad de la información de la Corte Superior de Justicia a la cual pertenece; desde la identificación, el análisis, la evaluación, el tratamiento y seguimiento de los riesgos identificados.

Asimismo, es responsable de coordinar con los dueños de procesos, propietarios de riesgos y titulares de las unidades de organización su apoyo y participación activa en la gestión de riesgos e implementación de los controles de seguridad de la información identificados, en los ámbitos de competencia de la Corte Superior de Justicia a la cual pertenece.

5.5 Las unidades de organización y funcionales del Poder Judicial, a cargo de los procesos que se encuentran bajo el alcance del SGSI y SGA

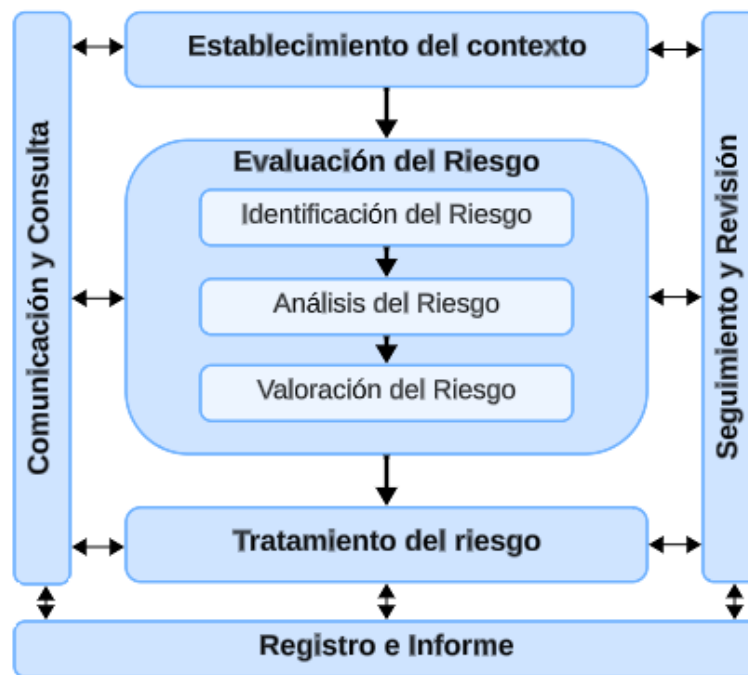
Son responsables de participar activamente en las reuniones de identificación y revisión de los potenciales riesgos de soborno y seguridad de la información, así como, de las oportunidades de mejora, según corresponda, proponiendo medidas de tratamiento para la mitigación de los riesgos o acciones de mejora para las oportunidades; y cuando aplique, son responsables de su implementación.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO	UI/GUI-006	
	GUÍA	Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Página:	5 de 21

6. DISPOSICIONES GENERALES Y ESPECÍFICAS

6.1. Actividades del Proceso

El proceso de la gestión de riesgos implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto, evaluación, tratamiento, seguimiento, registro e informe del riesgo, a continuación, se muestra el proceso:




En el Poder Judicial se busca reducir todos los riesgos de soborno y seguridad de la información en la medida de lo posible y somete a tratamiento todas aquellas conductas, operaciones y/o actividades que obtengan una evaluación de riesgo residual (riesgo final evaluado) superior a “Bajo”.

6.2. Establecimiento del contexto

La base para aplicar y mantener un SGA y un SGSI es la identificación, el análisis, evaluación y el tratamiento de los riesgos de soborno y de seguridad de la información respectivamente, que pueden darse en la entidad, con el objetivo de prevenirlos y gestionarlos de manera alineada a los objetivos institucionales. Asimismo, resulta fundamental identificar las oportunidades que permitan implementar acciones de mejora continua.

Para tal fin, se ha definido e identificado el contexto del Poder Judicial, así como los criterios de revisión periódica, conforme a lo establecido en la **Directiva del “Sistema de Gestión Antisoborno del Poder Judicial”** y en el documento normativo que regule la implementación del SGSI; de igual modo, se han definido e identificado los procesos comprendidos dentro del alcance del SGA y del SGSI, asegurando su actualización permanente.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	6 de 21

6.3. Evaluación del riesgo de soborno y de seguridad de la información

El/La funcionario/a responsable de la Unidad de Integridad, el responsable que ejerce el rol de la función de Integridad en las Cortes Superiores de Justicia, el Oficial de Seguridad y Confianza Digital, el Responsable de Seguridad y Confianza Digital, respectivamente; conjuntamente con los responsables de los procesos, realizan la identificación, el análisis y la valoración de los riesgos de soborno y de seguridad de la información identificados, siguiendo lo indicado en el **Instructivo “Evaluación y Tratamiento de los Riesgos de Soborno”** y **normas que regulen la materia**.

El mencionado instructivo detalla el procedimiento a emplear para la identificación, el análisis y la valoración de los riesgos, con el fin de evaluar objetivamente el nivel de **probabilidad** de ocurrencia y **el impacto** que dicho riesgo tendría en la entidad.


Asimismo, es responsabilidad del funcionario responsable de la Unidad de Integridad, del Oficial de Seguridad y Confianza Digital, del Responsable de Seguridad y Confianza Digital, respectivamente; conservar el detalle y la evidencia de esta actividad periódica en el formato denominado **“Ficha N°2: Evaluación del riesgo que afecta la integridad pública”** (Anexo 02) para el SGA y en la Matriz de Evaluación de Riesgos de Seguridad de la Información (Anexo 6) correspondiente al SGSI.

6.3.1. Identificación de los riesgos de soborno y de seguridad de la información

La identificación de los riesgos de soborno y de seguridad de la información en las actividades y servicios del Poder Judicial se realiza a partir del análisis de los procesos previamente identificados en el contexto institucional.

En este proceso participan los responsables de los procesos comprendidos en el alcance del SGA y del SGSI, con el objetivo de identificar situaciones, operaciones o actuaciones que pueden suponer un riesgo de soborno o de seguridad de la información. Esta identificación se realiza mediante reuniones de trabajo organizadas bajo la técnica de “tormenta de ideas” y participan personal seleccionado en función a sus responsabilidades, conocimiento y experiencia.

El/La funcionario/a responsable de la Unidad de Integridad, el responsable que ejerce el rol de la función de Integridad en las Cortes Superiores de Justicia, el Oficial de Seguridad y Confianza Digital, el Responsable de Seguridad y Confianza Digital, respectivamente; lideran esta actividad, garantizando la adecuada coordinación y recopilación de la información. Asimismo, para la identificación de riesgos se consideran otras fuentes relevantes como: recomendaciones y guías sectoriales sobre riesgos de corrupción, datos y experiencias propias de la entidad (incluyendo no conformidades, resultados de auditorías internas y externas, actividad de evaluación de eficacia de los controles, denuncias, investigaciones, entre otros), así como aportes de expertos externos.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO	UI/GUI-006	
	GUÍA	Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Página:	7 de 21

La identificación de los riesgos en los procesos implica analizar, en cada caso, la posible concurrencia de las fuentes de riesgo descritas a continuación:

- **Operacional:** Actividades y procesos legalmente autorizados que el Poder Judicial realiza para la consecución de sus objetivos institucionales y que pudieran ser sensibles a los riesgos de soborno y seguridad de la información.

En el SGA: conductas delictivas vinculadas al soborno por deficiencias u omisiones en los procesos de gestión, recursos humanos, tecnológicos o de infraestructura y similares.

En el SGSI: amenazas que podrían explotar las vulnerabilidades de los activos de información (inexistencia de controles de seguridad, sistemas y aplicaciones desactualizadas, falta de copias de respaldo, ausencia de sistemas de identificación y autenticación, falta de formación y conciencia sobre seguridad de la información, contraseñas poco seguras, entre otras).

- **Usuarios:** Justiciables, persona natural o jurídica, usuaria de la administración de justicia; y, abogado defensor, profesional que ejerce la defensa técnica en representación de su patrocinado en un proceso judicial o administrativo.

En el SGA: Quienes pueden aprovechar la prestación del servicio público para la comisión de actos de soborno a beneficio propio.


En el SGSI: Quienes pueden aprovechar la prestación del servicio público para la vulneración de los activos de información. Asimismo, se considera a quienes tengan o hagan uso de la información de la entidad como parte de la prestación del servicio o de las funciones que realicen dentro del Poder Judicial.

- **Socios de negocio:** Aquellas personas naturales o jurídicas con las cuales la entidad mantiene o planifica mantener una relación.

En el SGA: Aquellos que utilizan dicha relación para la comisión de delitos relacionados con el soborno. Esta fuente incluye a modo de referencia a proveedores, contrapartes de convenios o similar, etc.

En el SGSI: Aquellos que utilizan dicha relación para la comisión de delitos informáticos o quienes tengan o hagan uso de la información del Poder Judicial. Esta fuente incluye a modo de referencia a proveedores, contrapartes de convenios o similar, etc.

- **Transacciones y operaciones:** Son aquellas transacciones y operaciones específicas que realiza la entidad que dada su naturaleza pueden estar más expuestas al riesgo de soborno, como podrían ser actividades y operaciones que impliquen a modo de referencia, contrataciones o licitaciones, realización de actividades/procesos que pueden generar interés o impacto en terceros o usuarios del sistema y de los servicios del Poder Judicial, etc.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO	UI/GUI-006	
	GUÍA	Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Página:	8 de 21

En la identificación de riesgos de soborno y de seguridad de la información se revisan todos los procesos de la entidad definidos en el alcance del SGA y del SGSI, respectivamente; analizando para cada uno de ellos los posibles riesgos (entendidos como incertidumbres o conductas de riesgo). Este análisis considera las diferentes fuentes de riesgos, de modo que para cada proceso o subproceso se estudia el posible impacto asociado a cada fuente de riesgo de soborno y en consecuencia la forma, conducta, acción u omisión mediante la cual podría materializarse el riesgo.

Es responsabilidad del Oficial de Cumplimiento del SGA, del Oficial de Seguridad y Confianza Digital del SGSI y del Responsable de Seguridad y Confianza Digital, respectivamente; conservar el detalle y la evidencia de esta actividad periódica de identificación de riesgos, registrándose, en el formato denominado “**Ficha N°1: Identificación de riesgo que afecta la integridad pública**” (Anexo 01) del SGA. Para el caso del SGSI la identificación del riesgo se documenta a través de la Matriz de Evaluación de Riesgos de Seguridad de la Información (Anexo 6).


6.3.2. Análisis del riesgo

El Oficial de Cumplimiento del SGA, el responsable que ejerce el rol de la función de Integridad en las Cortes Superiores de Justicia, el Oficial de Seguridad y Confianza Digital del SGSI, el Responsable de Seguridad y Confianza Digital, respectivamente; conjuntamente con los responsables de los procesos, efectúan el análisis de los riesgos identificados en sus respectivos ámbitos. Este análisis permite comprender los riesgos, identificando las causas que podrían propiciar su materialización y sus posibles efectos, más allá de las consecuencias administrativas, civiles o penales para los agentes involucrados. En esa línea, el análisis considera:

- **Las causas personales**, referidas a los potenciales agentes de riesgo al interior de la institución.
- **Las causas organizacionales**, referidas a la entidad.
- **Los efectos**, referidos a sus implicancias en la sociedad y en la entidad.

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Se determina mediante la aplicación de la siguiente relación:

$$\text{Probabilidad X Impacto} = \text{Nivel del Riesgo}$$

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO	UI/GUI-006	
	GUÍA	Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Página:	9 de 21

El análisis del riesgo debería considerar factores tales como, entre otros:

- La probabilidad de los eventos y de las consecuencias;
- La naturaleza y la magnitud de las consecuencias;
- La eficacia de los controles existentes;
- Los niveles de sensibilidad y de confianza.

6.3.3. Valoración del riesgo

El Oficial de Cumplimiento del SGA, el responsable que ejerce el rol de la función de Integridad en las Cortes Superiores de Justicia, el Oficial de Seguridad y Confianza Digital y el Responsable de Seguridad y Confianza Digital, respectivamente; conjuntamente con los responsables de los procesos, efectúa la valoración de los riesgos identificados de sus respectivos procesos.

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios de riesgo establecidos para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de:

- No hacer nada más;
- Considerar opciones para el tratamiento del riesgo;
- Realizar un análisis adicional para comprender mejor el riesgo;
- Mantener los controles existentes;
- Reconsiderar objetivos.


6.4. Tratamiento de riesgos de soborno y de seguridad de la información

En el Poder Judicial se ha determinado que todo riesgo de soborno y de seguridad de la información, debe ser objeto de tratamiento, mediante la definición de planes de acción orientados a su mitigación, priorizando la asignación de atención y recursos.

En esta etapa se determinan las medidas necesarias para prevenir y mitigar los riesgos identificados, elaborando el correspondiente plan de acción que detalla dichas medidas.

La implementación de dicho plan corresponde a las unidades orgánicas responsables de los procesos en los que se identificaron riesgos.

Los responsables de los procesos, proponen al Oficial de Cumplimiento del SGA, al responsable que ejerce el rol de la función de Integridad en las Cortes Superiores de Justicia, al Oficial de Seguridad y Confianza Digital, y al Responsable de Seguridad y Confianza Digital, respectivamente; las medidas de prevención y de mitigación aplicables a sus respectivos procesos.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	10 de 21

La validación de las medidas de prevención y mitigación propuestas corresponde exclusivamente al Oficial de Cumplimiento del SGA, al responsable que ejerce el rol de la función de Integridad en las Cortes Superiores de Justicia, al Oficial de Seguridad y Confianza Digital, al Responsable de Seguridad y Confianza Digital, respectivamente. De ser necesario, este último puede convocar a los servidores con rol consultivo que correspondan, según sus competencias y experiencia, para aportar elementos de análisis que fortalezcan dicha evaluación.

Es responsabilidad de los dueños de los procesos, conservar el detalle y la evidencia de esta actividad periódica de tratamiento de riesgos, registrándose en el denominado **“Ficha N°3: Tratamiento del riesgo que afecta la integridad pública”** (Anexo 03) del SGA, en el caso del SGSI se deberá registrar en la Matriz de Tratamiento y Seguimiento de Riesgos de Seguridad de la Información (Anexo 7).

6.5. Conservación y disposición de la matriz de riesgos

Culminada las etapas de identificación, análisis, valoración y tratamiento del riesgo, se elabora la **“Matriz de Riesgos de Soborno”** (Anexo 04). Esta matriz es conservada por el/la Funcionario/a Responsable de la Unidad de Integridad, y puesta a disposición de los responsables de los procesos, a través de la Unidad de Integridad, garantizando así que la información se mantenga actualizada y disponible en todo momento.


Para el caso del SGSI, el Oficial de Seguridad y Confianza Digital o el Responsable de Seguridad y Confianza Digital, según corresponda, es el responsable de la conservación de la Matriz de Evaluación de Riesgos de Seguridad de la Información y de la Matriz de Tratamiento y Seguimiento de los Riesgos de Seguridad de la Información; así mismo los dueños de los procesos comprendidos en el alcance del SGSI o a quien designen, son los responsables de la conservación de las referidas matrices.

6.6. Gestión de oportunidades

6.6.1. Identificación de oportunidades

La identificación de oportunidades de mejora se lleva a cabo a través de reuniones en las que se identifican las oportunidades como un elemento fundamental para la mejora del SGA y del SGSI. El Oficial de Cumplimiento del Sistema de Gestión Antisoborno, el Oficial de Seguridad y Confianza Digital, el Responsable de Seguridad y Confianza Digital, respectivamente; conjuntamente con los dueños o los responsables de los procesos comprendidos en el alcance del SGA y del SGSI, proponen las oportunidades de mejora identificadas. Asimismo, deben de garantizar la conservación del detalle y la evidencia de esta actividad periódica, registrándose en el formato denominado **“Listado de Oportunidades de Mejora”** (Anexo 05).

Las oportunidades de mejora pueden ser identificadas tomando en cuenta los siguientes elementos:

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO	UI/GUI-006	
	GUÍA	Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Página:	11 de 21

- Análisis de Contexto, desarrollado en el “**Análisis FODA del Poder Judicial en materia de Prevención del Soborno**”.
- Requisitos de las Partes Interesadas, desarrollado en la “**Matriz de Partes Interesadas del Poder Judicial en materia de prevención del soborno**”.
- Resultados de Auditorías.
- Resultados de Revisión por el Oficial de Cumplimiento o por el Oficial de Seguridad y Confianza Digital o por el Responsable de Seguridad y Confianza Digital.
- Resultados de Revisión por la Alta Dirección.
- Resultados de Revisión por el órgano de Gobierno.
- Desempeño del Sistema de Gestión Antisoborno o del Sistema de Gestión de Seguridad de la Información.

6.6.2. Análisis y tratamiento de oportunidades

En el Poder Judicial, el análisis de oportunidades se realiza a través del funcionario/a responsable de la Unidad de Integridad, el responsable que ejerce el rol de la función de Integridad en las Cortes Superiores de Justicia, del Oficial de Seguridad y Confianza Digital o del Responsable de Seguridad y Confianza Digital, respectivamente; con el apoyo de los responsables de los procesos incluidos en el alcance del SGA y SGSI, según se estimen pertinentes. Este análisis permite identificar las oportunidades, evaluar su impacto y determinar su viabilidad para ser incorporadas en el plan de actuación.


Asimismo, se deciden cuáles oportunidades son priorizadas para su ejecución, definiendo el correspondiente plan de acción y las actividades de seguimiento, conforme a lo registrado en el “**Listado de Oportunidades de Mejora**” (Anexo 05).

6.7. Etapa de seguimiento y monitoreo

6.7.1. Actualización de la matriz de riesgos / listado de oportunidades de mejora

La matriz de riesgos de soborno y de seguridad de la información debe ser actualizada periódicamente, con la finalidad de generar controles que reduzcan la probabilidad de ocurrencia e impacto en caso de materialización.

El/La funcionario/a responsable de la Unidad de Integridad, el responsable que ejerce el rol de la función de integridad en las Cortes Superiores de Justicia, el Oficial de Seguridad y Confianza Digital o el Responsable de Seguridad y Confianza Digital, respectivamente; conjuntamente con los responsables de los procesos comprendidos en el alcance del sistema, son responsables de actualizar las fichas (Anexo 01, 02 y 03) y la matriz de riesgos de los procesos (Anexo 04); así como las matrices correspondientes del SGSI. La actualización se realiza semestralmente o, en su defecto, cuando se produzcan cambios significativos en el contexto, en los procesos o en las responsabilidades asignadas.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	12 de 21

Para ello, coordina con los responsables de los procesos, las acciones necesarias que comprenden la incorporación de nuevos riesgos, la reevaluación de los niveles de riesgos existentes, la definición de nuevas actividades de control, y, cuando corresponda, la formulación de planes de acción.

En cuanto a las oportunidades de mejora, estas también son revisadas con una frecuencia semestral, o en respuesta a cambios relevantes en el contexto, así como a sugerencias y recomendaciones derivadas del personal o de los propios procesos.


6.7.2. Seguimiento de las medidas de tratamiento / acciones de mejora

El cumplimiento de las medidas de tratamiento y acciones de mejora debe ser revisado de manera continua por el funcionario responsable de la Unidad de Integridad, el responsable que ejerce el rol de la función de integridad en las Cortes Superiores de Justicia, el Oficial de Seguridad y Confianza Digital o por el Responsable de Seguridad y Confianza Digital, respectivamente; quienes son los responsables de operativizar el seguimiento.

En caso de presentarse una situación de emergencia o fuerza mayor que dificulte la implementación o el cumplimiento de las medidas de tratamiento en los plazos establecidos, los responsables de los procesos deben reportarlo al Oficial de Cumplimiento del SGA, al Oficial de Seguridad y Confianza Digital o al Responsable de Seguridad y Confianza Digital, según corresponda; indicando los motivos y las medidas y las acciones adoptadas. Esta información debe registrarse en la Matriz de Riesgos.

El/La funcionario/a responsable de la Unidad de Integridad, el responsable que ejerce el rol de la función de integridad en las Cortes Superiores de Justicia, el Oficial de Seguridad y Confianza Digital, el Responsable de Seguridad y Confianza Digital; según corresponda, evalúan si la falta o retraso de la implementación de la medida tratamiento constituye un posible incumplimiento legal para la entidad. De ser el caso, emiten un informe al presidente del Poder Judicial (en calidad de Alta Dirección del SGA), para solicitar la aprobación de las medidas de acción respectivas y la eventual reprogramación de fechas de implementación de las medidas de tratamiento. Para el caso del SGSI el informe en mención debe ser remitido al Comité de Gobierno y Transformación Digital a través del Oficial de Seguridad y Confianza Digital, de considerarlo pertinente.

Las medidas de tratamiento son consolidadas y monitoreadas mediante un seguimiento continuo a cargo del Oficial de Integridad y Oficial de Seguridad y Confianza Digital, del Responsable de Seguridad y Confianza Digital, respectivamente. Asimismo, la Unidad de Integridad del Poder Judicial, debe revisar con los responsables de los procesos el avance y seguimiento de la ejecución de las medidas de tratamiento y acciones de mejora.

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	13 de 21

El seguimiento de las medidas de tratamiento y acciones de mejora tiene los siguientes objetivos:

- Realizar seguimiento de los compromisos adquiridos por los responsables de la ejecución e implementación de las medidas de tratamiento y acciones de mejora.
- Determinar el nivel de avance de la implementación de las medidas de tratamiento y acciones de mejora definidos.
- Identificar las causas de posibles retrasos en la implementación de las medidas de tratamiento y acciones de mejora.

6.7.3. Evaluación de la eficacia de las medidas de tratamiento

La eficacia de las medidas de tratamiento implementadas para mitigar, reducir o eliminar los riesgos de soborno debe ser evaluada transcurrido un periodo razonable, que no exceda los 12 meses desde implantadas las medidas.

Esta evaluación debe abarcar todas las medidas de tratamiento implementadas y es realizada por el Oficial de Cumplimiento del SGA, el Oficial de Seguridad y Confianza Digital, o por el Responsable de Seguridad y Confianza Digital, respectivamente, conjuntamente con los responsables de los procesos involucrados.


6.7.4. Evaluación de la eficacia de las acciones de mejora

La evaluación de la eficacia de las acciones de mejora implementadas para aprovechar las oportunidades de mejora identificadas, se realiza mediante el establecimiento de objetivos, a cargo del funcionario/a Responsable de la Unidad de Integridad, el responsable que ejerce el rol de la función de integridad en las Cortes Superiores de Justicia, el Oficial de Seguridad y Confianza Digital, el Responsable de Seguridad y Confianza Digital, respectivamente; con el apoyo de los responsables de los procesos.

Se considera que las acciones han sido eficaces cuando los objetivos planteados hayan sido alcanzados. Las conclusiones obtenidas, quedarán registradas en el “Listado de Oportunidades de Mejora” (Anexo 05).

7. CONTROL DE CAMBIOS

Versión	Fecha de actualización	Actualización	Responsable/ Cargo	Proceso
001	28/12/2020	Creación del documento	Carlos Arias Lazarte / Presidente de la Comisión de Integridad Judicial	Mejora Institucional
002	24/11/2021	a) Eliminación de términos en numeral 1.0. b) Cambio de término Directiva del Sistema de Gestión Antisoborno en Lugar de Manual del Sistema de Gestión Antisoborno en el numeral 2.0	Mariem Vicky de la Rosa Bebríana / Presidenta de la Comisión de Integridad Judicial	Mejora Institucional

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	14 de 21

Versión	Fecha de actualización	Actualización	Responsable/ Cargo	Proceso
		c) Actualización a Resolución 370-2020-CE-PJ que aprueba la Directiva denominada "Disposiciones para el Desarrollo de Documentos Normativos en el Poder Judicial en numeral 3 base normativa. d) Inclusión de Resolución Administrativa de Sala Plena N.º 000014-2020-SP CS-PJ en numeral 3 base normativa. e) Modificación a "Norma NTP -ISO 37001 -2017. Norma Técnica Peruana. Sistema de Gestión Antisoborno. Requisitos con orientación para su uso" y "Resolución Administrativa N.º 140-2021 CE-PJ" en numeral 3 base normativa. f) Inclusión de tiempos que toma el desarrollo de documentos normativos y medidas adoptadas para abordar cualquier situación de emergencia en el numeral 6.8. Tratamiento de riesgos de soborno.		
003	11/07/2025	a) Definiciones relacionadas con la gestión de riesgos de seguridad de la información b) Incorporación de las actividades para la identificación, el análisis, valoración y tratamiento de los riesgos de seguridad de la información en el marco de la implementación del SGSI. c) Incorporación de las actividades para el tratamiento de los riesgos de seguridad de la información en el marco de la implementación del SGSI d) Incorporación de las actividades de identificación, análisis y tratamiento de las oportunidades de mejoras en el marco de la implementación del SGSI. e) Identificación de las actividades de seguimiento y monitoreo de los riesgos de seguridad de la información en el marco de la implementación del SGSI.	Guillermo Pérez Silva/ Gerente de Tecnologías de Información Elizenda Quispe Castillo / Funcionaria Responsable de la Unidad de Integridad	Mejora Institucional

8. ANEXOS

Anexo 01: Ficha N°1: Identificación de riesgo que afecta la integridad pública

Anexo 02: Ficha N°2: Evaluación del riesgo que afecta la integridad pública


Anexo 03: Ficha N°3: Tratamiento del riesgo que afecta la integridad pública

Anexo 04: Matriz de Riesgos de Soborno

Anexo 05: Listado de Oportunidades de Mejora


Anexo 06: Matriz de Evaluación de Riesgos de Seguridad de la Información

Anexo 07: Matriz de Tratamiento y Seguimiento de Riesgos de Seguridad de la Información

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO			UI/GUI-006	
	GUÍA			Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN			Página:	15 de 21


Anexo 01:
Ficha N°1: Identificación de riesgo que afecta la integridad pública

Ficha N°1: Identificación de riesgo que afecta la integridad pública						
Proceso analizado				Ubicación del riesgo	<input type="checkbox"/> Proceso operativo o misional <input type="checkbox"/> Proceso de soporte	
Unidad orgánica responsable del proceso analizado						
Contexto de riesgo	<input type="checkbox"/>	Compra de bienes	<input type="checkbox"/>	Contratación y gestión de personal	<input type="checkbox"/>	Elaboración o aprobación de normas
	<input type="checkbox"/>	Contratación de obras	<input type="checkbox"/>	Prestación directa de servicios a los usuarios	<input type="checkbox"/>	Emisión de autorizaciones
	<input type="checkbox"/>	Contratación de servicios	<input type="checkbox"/>	Fiscalización, supervisión o monitoreo	<input type="checkbox"/>	Gestión de dinero entregado a servidores de la entidad
	<input type="checkbox"/>	Pago a proveedores	<input type="checkbox"/>	Recaudación directa de ingresos	<input type="checkbox"/>	Servicios administrativos
	<input type="checkbox"/>	Otro contexto				
Posible comportamiento irregular	<input type="checkbox"/>	Apropiación o uso indebido de recursos, bienes o información del Estado			<input type="checkbox"/>	Mantener intereses en conflicto
	<input type="checkbox"/>	Favorecimiento indebido			<input type="checkbox"/>	Abuso de autoridad
	<input type="checkbox"/>	Acceso a ventajas indebidas			<input type="checkbox"/>	Invocación de influencias en el Estado
	<input type="checkbox"/>	Obstrucción al acceso a la información pública			<input type="checkbox"/>	Otro comportamiento
Potencial agente primario				Potenciales agentes internos		
				Potenciales agentes externos		
Redacción del riesgo						
Preguntas de validación	<input type="checkbox"/>	Ejercicio inadecuado de la función asignada al cargo	<input type="checkbox"/>	Abuso del poder público	<input type="checkbox"/>	Obtención de beneficio irregular para sí o para terceros
Tipo de riesgo identificado	<input type="checkbox"/>	Inconducta funcional Posible infracción administrativa				
	<input type="checkbox"/>	Corrupción Posible(s) delito(s)				

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	16 de 21


Anexo 02:
Ficha N°2: Evaluación del riesgo que afecta la integridad pública

Ficha N°2: Evaluación del riesgo que afecta la integridad pública									
Formulación del riesgo que afecta la integridad pública							Código		
Tipo de riesgo	Riesgo de inconducta funcional			Unidad orgánica responsable					
	Riesgo de corrupción								
Análisis de causas (Seleccionar 3 causas en orden de importancia)							En caso se identifiquen procesos ineficientes como causa relevante, precisar:		
Causas personales	Predisposición por relación personal								
	Falta o deterioro de carácter ético								
	Percepción de impunidad								
	Desconocimiento								
Causas organizacionales	Presión jerárquica o de pares								
	Procesos ineficientes								
	Alta discrecionalidad								
	Prácticas normalizadas								
Análisis de efectos (Seleccionar los efectos correspondientes en orden de importancia)							En caso se identifique afectación de derechos o servicios como efecto relevante, precisar:		
Posibles efectos	Afectación de derechos								
	Afectación de servicios								
	Pérdida o desvío de recursos de la entidad								
	Afectación de recursos de los usuarios								
	Afectación de la continuidad de la actual gestión								
Probabilidad de ocurrencia del riesgo							Análisis del impacto del riesgo		
Nivel		Media		Alta		Muy Alta			
Valor		6		8		10			
Cálculo del Nivel del riesgo									
Nivel		Medio		Alto		Muy alto			
Valor		36		48, 60 o 64		80—100			
Decisión del tratamiento (considerando el nivel de tolerancia al riesgo de la entidad)							Sí		No


 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	17 de 21

Anexo 03:
Ficha N°3: Tratamiento del riesgo que afecta la integridad pública

Ficha N°3: Tratamiento del riesgo que afecta la integridad pública						
Formulación del riesgo que afecta la integridad pública						Código
Tipo de riesgo	Riesgo de inconducta funcional		Unidad orgánica responsable			
	Riesgo de corrupción					
Medidas para prevenir las causas del riesgo						
Detalle de la(s) medida(s) de prevención (máximo 3, una por causa)						
Medidas de prevención	1	Estrategia	Incrementar consciencia sobre las consecuencias		Optimizar el diseño organizacional	Producir ajustes de comportamiento
		Medida				
	2	Estrategia	Incrementar consciencia sobre las consecuencias		Optimizar el diseño organizacional	Producir ajustes de comportamiento
		Medida				
	3	Estrategia	Incrementar consciencia sobre las consecuencias		Optimizar el diseño organizacional	Producir ajustes de comportamiento
		Medida				
Detalle de la(s) medida(s) de mitigación (máximo 2, una por efecto)						
Medidas de mitigación	1	Estrategia	Contener posibles efectos de mediano y largo plazo		Activar respuesta inmediata	Demostrar acciones de debida diligencia
		Medida				
	2	Estrategia	Contener posibles efectos de mediano y largo plazo		Activar respuesta inmediata	Demostrar acciones de debida diligencia
		Medida				

 PODER JUDICIAL DEL PERÚ	DOCUMENTO INTERNO		UI/GUI-006	
	GUÍA		Versión:	003
	GESTIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN ANTISOBORNO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		Página:	18 de 21

**Anexo 04:
Matriz de Riesgos de Soborno**

 PODER JUDICIAL DEL PERÚ										MATRIZ DE RIESGOS DE SOBORNO										Versión		3	
Nombre del Proceso										Fecha de Revisión			May-24										
Unidad Orgánica / Subárea / Área / Comisión:										Responsable de Unidad Orgánica / Subárea / Área / Comisión:													
Órgano										Responsable de Órgano													
<i>FICHA 01</i>			<i>FICHA 01</i>			<i>FICHA 02</i>																	
Código de riesgo	Unidad Orgánica responsable del riesgo	Riesgo Identificado	Valor del riesgo	Tratamiento del Riesgo				Seguimiento y Verificación				Comentarios u Observaciones											
				Medidas de Control	Plazos de Implementación			Estado de Ejecución de	Fecha de Verificación	Evidencias o Medios de Verificación	¿Eficaz? SÍ/NO												
					1.-- 2.-- 3.--	1. Permanente 2. cada 6 meses 3.	1. Implementada 2. Implementada 3. Implementada					1/05/2024	1. 2. 3.	SI									
			Alto																				
			Alto																				
			Alto																				
			Alto																				
			Alto																				
			Alto																				

Elaborado por:	
Nombre	

