ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

ADMINISTRACIÓN DE RIESGOS Y OPORTUNIDADES INSTITUCIONALES

PRO-GPE-GSI-003

Coordinación General de Planificación Estratégica
Versión 7.0
Diciembre – 2025

ÍNDICE

ÍNDICE DE ILUSTRACIONES:

ÍNDICE DE TABLAS:

1. CUADRO DE FIRMAS DE RESPONSABILIDAD

CÓDIGO: PRO-GPE-GSI-003		**VERSIÓN:** 7.0
ROL	**NOMBRE/CARGO**	**FIRMA**
APROBADO POR:	Mgtr. David Alejandro Totoy Moreno **Coordinador General de Planificación Estratégica** **Representante de Alta Dirección**	Firmado electrónicamente por: DAVID ALEJANDRO TOTOY MORENO Validar únicamente con FirmaEC
REVISADO POR:	Mgtr. Carlos Gustavo Quinatoa Basantes **Líder del Cambio y Procesos**	Firmado electrónicamente por: CARLOS GUSTAVO QUINATOA BASANTES Validar únicamente con FirmaEC
	Mgtr. Sandra Elizabeth Prado Córdova **Líder de Planificación y Evaluación**	Firmado electrónicamente por: SANDRA ELIZABETH PRADO CORDOVA Validar únicamente con FirmaEC
	Lcdo. Jonathan Fernando Lozano Loor **Líder de Sistemas Integrados y Calidad**	Firmado electrónicamente por: JONATHAN FERNANDO LOZANO LOOR Validar únicamente con FirmaEC
ELABORADO POR:	Mgtr. Víctor Andrés Chumanía Lárraga **Especialista Junior de Procesos y Calidad**	Firmado electrónicamente por: VICTOR ANDRES CHUMANIA LARRAGA Validar únicamente con FirmaEC
	Ing. Gabriel David Quinteros Cárdenas **Especialista Junior de Procesos y Calidad**	Gabriel David Quinteros Cardenas Time Stamping Security Data
	Ing. María Belén Castro Ruales **Especialista Junior de Sistemas Integrados y Calidad**	Firmado electrónicamente por: MARIA BELEN CASTRO RUALES Validar únicamente con FirmaEC
	Mgtr. Jenny Alexandra Almeida Toapanta **Analista Legislativa**	Firmado electrónicamente por: JENNY ALEXANDRA ALMEIDA TOAPANTA Validar únicamente con FirmaEC

2. IDENTIFICACIÓN DEL DOCUMENTO

Proceso Nivel 1:	Gestión de Planificación Estratégica		
Proceso Nivel 2:	Gestión de Sistemas Integrados y Calidad		
Proceso Nivel 3:	No Aplica		
Versión del documento:	7.0	**Frecuencia de Ejecución:**	Bajo demanda / Planificación
Responsable:	Líder de Gestión de Sistemas Integrados y Calidad		

3. TRAZABILIDAD DEL DOCUMENTO

Versión	**Descripción de la versión** *(motivos y cambios)*	**Realizado / Autorizado por**	**Fecha de elaboración** *(mmm-aaaa)*	**Documentos que se dan de baja con la vigencia de este documento**
1	**Creación**	Ing. Alexandra Espinosa **SERVIDORA LEGISLATIVA ADMINISTRACIÓN GENERAL** / Ing. Jorge Troya Fuertes **ADMINISTRADOR GENERAL**	Oct-2019	No aplica

Versión	**Descripción de la versión** *(motivos y cambios)*	**Realizado / Autorizado por**	**Fecha de elaboración** *(mmm-aaaa)*	**Documentos que se dan de baja con la vigencia de este documento**
2	**Actualización:** - Modificación en normas generales - Modificación de la descripción de actividades. - Modificación del Diagrama de - Caracterización - Modificación del Diagrama de Flujo - Modificación de formatos	Ing. Alexandra Espinosa **SERVIDORA LEGISLATIVA ADMINISTRACIÓN GENERAL** / Ing. Jorge Troya Fuertes **ADMINISTRADOR GENERAL**	Ene-2020	PRO-GPP-GPC-002 V1.0
2.1	**Actualización:** - Inclusión de nuevas categorías de riesgos	Ing. Andrés Chanabá **LIDER DE PROCESOS Y CALIDAD** Econ. Mariuxi Vera Briones **SERVIDORA LEGISLATIVA** / Ing. Mauricio Sarabia **COORDINADOR GENERAL DE PLANIFICACIÓN**	Jul-2020	PRO-GPP-ARI-001 V2.0
3.0	**Actualización:** - Criterios de valoración de riesgos de soborno	Ing. Andrés Chanabá **LIDER DE PROCESOS Y CALIDAD** Ab. Andrea Segarra **SERVIDORA LEGISLATIVA** Econ. Mariuxi Vera Briones **SERVIDORA LEGISLATIVA** / Ing. Mauricio Sarabia **COORDINADOR GENERAL DE PLANIFICACIÓN**	Sep-2020	PRO-GPP-ARI-001 V2.1
4.0	**Actualización:** - Objetivo del proceso - Alcance - Normas internas y externas - Políticas internas y específicas del proceso - Diagrama de caracterización - Diagrama de flujo - Descripción de actividades - Indicador del proceso - Formatos - Definiciones - Control de registros.	Ing. Gabriel Quinteros **SERVIDOR LEGISLATIVO DE LA UNIDAD DE PROCESOS Y CALIDAD** / Ing. Mauricio Galarza **COORDINADOR GENERAL DE PLANIFICACIÓN Y PROCESOS**	Jul-2024	PRO-GPP-ARI-001 V3.0

Versión	**Descripción de la versión** *(motivos y cambios)*	**Realizado / Autorizado por**	**Fecha de elaboración** *(mmm-aaaa)*	**Documentos que se dan de baja con la vigencia de este documento**
5.0	**Actualización:** - Actualización del código del procedimiento - Normas internas y externas - Políticas internas y específicas del proceso - Inclusión de metodología de administración de riesgos de seguridad de la información. - Formatos - Control de registros	Ing. Gabriel Quinteros **SERVIDOR LEGISLATIVO DE LA GESTIÓN DE SISTEMAS INTEGRADOS Y CALIDAD** / Dr. Carlos Ordóñez **COORDINADOR GENERAL DE PLANIFICACIÓN ESTRATÉGICA (ALTA DIRECCIÓN)**	Mar-2025	PRO-GPE-GSC-004 V4.0
6.0	**Actualización:** - Actualización semántica de objetivo del procedimiento - Inclusión de normas para cargos críticos o riesgos antisoborno - Inclusión de normas generales para la evaluación del comportamiento éticos. - Actualización de actividades del procedimiento. - Cambio de imagen institucional y formato del procedimiento - Actualización de formato de matriz de riesgos y mapa de calor	Ing. Gabriel Quinteros **ESPECIALISTA JUNIOR DE SISTEMAS INTEGRADOS Y CALIDAD** / Mgtr. David Totoy **COORDINADOR GENERAL DE PLANIFICACIÓN ESTRATÉGICA (ALTA DIRECCIÓN)**	Oct-2025	PRO-GPE-GSI-003 V5.0
7.0	**Actualización:** - Actualización semántica de objetivo y alcance - Estructura de normas generales del proceso - Inclusión de actividades del procedimiento 9 y 10 - Actualización del diagrama de flujo - Actualización de formatos - Matriz de Riesgos - Matriz de oportunidades - Plan de mitigación de riesgos - Declaración de aplicabilidad de controles de seguridad de la información - Creación de formatos • Mapa de riesgos • Matriz de activos de información de la Asamblea Nacional	Ing. Gabriel Quinteros **ESPECIALISTA JUNIOR DE PROCESOS Y CALIDAD** Ing. María Castro **ESPECIALISTA JUNIOR DE SISTEMAS INTEGRADOS Y CALIDAD** Mgtr. Jenny Almeida **ANALISTA LEGISLATIVA** Mgtr. Víctor Chumanía **ESPECIALISTA JUNIOR DE PROCESOS Y CALIDAD** / Mgtr. David Totoy **COORDINADOR GENERAL DE PLANIFICACIÓN ESTRATÉGICA REPRESENTANTE DE ALTA DIRECCIÓN**	Dic-2025	PRO-GPE-GSI-003 V6.0

4. OBJETIVO

Implementar una metodología para identificar, analizar, evaluar y gestionar los riesgos a los que se encuentra expuesta la Asamblea Nacional del Ecuador, con el fin de comunicar los resultados a la Alta Dirección y facilitar la toma de decisiones de forma oportuna.

5. ALCANCE

Desde la identificación y valoración de los riesgos hasta la definición del plan de acción para mitigar su posible ocurrencia y evaluación de la eficacia de las acciones realizadas.

6. MARCO NORMATIVO

6.1 DOCUMENTOS EXTERNOS

- Norma ISO 31000-2018
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, NTE INEN-ISO 9001 y NTE INEN-ISO 37001
- Acuerdo Ministerial 003-2024 (MINTEL) - Esquema Gubernamental de Seguridad de la Información (EGSI v3.0).

6.2 DOCUMENTOS INTERNOS

- Reglamento Orgánico Funcional de la Asamblea Nacional – ROFAN y sus reformas.

6.3 NORMAS RELACIONADAS PARA LA EJECUCIÓN DEL PROCESO

a) Las normas de este documento son de aplicación obligatoria para todos los servidores de la Asamblea Nacional, en el ámbito de su competencia, en tanto guarden conformidad con las disposiciones constitucionales, legales, reglamentarias y resoluciones vigentes al momento de su ejecución.

b) El servidor legislativo que incumpliere sus obligaciones o contraviniere las disposiciones de este documento, así como las leyes y normativa conexa, incurrirá en responsabilidad administrativa que será sancionada disciplinariamente, acorde al reglamento interno de talento humano. Sin perjuicio de lo que establezca el ente de control en materia de riesgos.

c) La Coordinación General de Planificación Estratégica será la encargada de planificar y coordinar las acciones para aplicar esta metodología, así también será la encargada de unificar las respectivas matrices generadas para realizar comparaciones que se conviertan en respaldo técnico y funcional de un efectivo sistema integral de la administración del riesgo institucional.

d) El proceso de administración del riesgo requiere la activa participación de las Unidades Administrativas de la Asamblea Nacional para cumplir su propósito, en ese sentido, esta metodología será impartida al personal delegado de cada Unidad, quien será el responsable de reportar las respectivas evidencias de la aplicación de medidas de control de acuerdo a la frecuencia establecida a la Coordinación General de Planificación Estratégica.

e) Las Unidades Administrativas junto con el apoyo de la Coordinación General de Planificación Estratégica, deberán identificar los riesgos que puedan afectar al logro de los objetivos institucionales debido a factores internos o externos e identificarán las medidas pertinentes para afrontar exitosamente tales riesgos, a través del plan de mitigación correspondiente.

f) La administración del riesgo institucional identifica dentro de su estructura los siguientes tipos de riesgo:

Ilustración 1. Tipos de riesgo

En donde:

TIPO DE RIESGO INSTITUCIONAL	DESCRIPCIÓN	OBJETO DEL RIESGO
Riesgos Estratégicos	Probabilidad de ocurrencia de eventos adversos externos o internos que pudieran afectar el propósito y la dirección estratégica de la institución.	Objetivos Estratégicos Institucionales
Riesgos Operativos	Probabilidad de ocurrencia de eventos adversos que pudieren afectar el cumplimiento de los objetivos operativos institucionales.	Objetivos operativos de cada Unidad Administrativa
Riesgo Antisoborno	Es la posibilidad de que, por acción u omisión, se use el poder derivado del ejercicio de un cargo público para desviar la gestión a fin de obtener una ventaja indebida para sí mismo o para terceros.	Procesos sustantivos y adjetivos que forman parte del alcance del sistema de gestión antisoborno
Riesgo de Calidad	Es la probabilidad de ocurrencia de eventos adversos que afectan a los procesos institucionales.	Procesos sustantivos y adjetivos que forman parte del alcance del sistema de gestión de la calidad
Riesgo de Seguridad de la información	Es la probabilidad de ocurrencia de eventos internos o externos que pudieren afectar a la confidencialidad, integridad, y disponibilidad de la información.	Activos de seguridad de la información de los procesos que forman parte del alcance del sistema de gestión antisoborno
Riesgos Institucionales (Procesos)	Es la probabilidad de ocurrencia de eventos adversos que pudieren afectar a los procesos institucionales.	Procesos que no son parte de ningún alcance de los sistemas de gestión.
Riesgos de Proyectos Institucionales	Probabilidad de ocurrencia de eventos adversos, que podrían afectar el cumplimiento de las fases de los proyectos, el logro de los objetivos institucionales y su impacto.	Proyectos institucionales

Tabla 1. Tipos de riesgos

g) La Asamblea Nacional ha establecido como responsables de gestionar cada tipo de riesgo, según su ámbito de competencia, en función del siguiente detalle:

TIPO DE RIESGO	RESPONSABLE DE LA IDENTIFICACIÓN Y ANÁLISIS	RESPONSABLE DEL TRATAMIENTO	RESPONSABLE DEL SEGUIMIENTO
Riesgos Estratégicos	Secretario, Coordinador, líder o responsable de las Unidades de Gestión ejecutoras de procesos con el acompañamiento del Analista/Especialista de la Gestión de Planificación y	Secretarios, Coordinadores, Líderes/Responsables delegados del área	• Coordinador/a General de Planificación Estratégica • Líder/Responsable de la gestión de sistemas integrados y calidad

TIPO DE RIESGO	RESPONSABLE DE LA IDENTIFICACIÓN Y ANÁLISIS	RESPONSABLE DEL TRATAMIENTO	RESPONSABLE DEL SEGUIMIENTO
	Evaluación		
Riesgos Operativos	Secretario, Coordinador, líder o responsable de las Unidades de Gestión ejecutoras de procesos con el acompañamiento del Analista/Especialista de la Gestión de Planificación y Evaluación	Secretarios, Coordinadores, Líderes/Responsables/ Delegados del área	• Coordinador/a General de Planificación Estratégica • Líder/Responsable de la gestión de sistemas integrados y calidad
Riesgos de Calidad	Coordinador, líder o responsable de las Unidades de Gestión ejecutoras de procesos con el acompañamiento del Analista/Especialista de la Gestión de Sistemas Integrados y Calidad.	Secretarios, Coordinadores, Líderes o delegados del área	• Coordinador/a General de Planificación Estratégica • Líder/Responsable de la gestión de sistemas integrados y calidad.} • Especialista responsable del sistema de gestión de calidad
Riesgos Antisoborno	Coordinador, líder o responsable de las Unidades de Gestión ejecutoras de procesos con el acompañamiento del Analista/Especialista de la Gestión de Sistemas Integrados y Calidad.	Secretarios, Coordinadores, Líderes o delegados del área	• Coordinador/a General de Planificación Estratégica • Líder/Responsable de la gestión de sistemas integrados y calidad • Función de Cumplimiento.
Riesgos de Seguridad de la Información	Coordinador, líder o responsable de las Unidades de Gestión ejecutoras de procesos con el acompañamiento del Analista/Especialista de la Gestión de Sistemas Integrados y Calidad.	Secretarios, Coordinadores, Líderes o delegados del área	• Coordinador/a General de Planificación Estratégica • Líder/Responsable de la gestión de sistemas integrados y calidad • Oficial de Seguridad de la Información.
Riesgos de Procesos	Secretarios, Coordinador, o responsable del proyecto con el acompañamiento del Analista/Especialista de la Gestión de cambio y procesos	Secretarios, Coordinador, o responsable del proceso	• Coordinador/a General de Planificación Estratégica • Líder/Responsable de la gestión de sistemas integrados y calidad
Riesgos de Proyectos Institucionales	Secretarios, Coordinador, o responsable del proyecto con el acompañamiento del Analista/Especialista responsable del proyecto	Secretarios, Coordinador, o responsable del proyecto	• Responsable del proyecto • Líder/Responsable de la gestión de sistemas integrados y calidad

Tabla 2. Responsables para la administración del riesgo

h) La Gestión de Planificación y Evaluación será la responsable de analizar y/o actualizar los Riesgos Estratégicos y Operativos, así como la definición de las medidas de control a implementarse y su respectivo responsable con las Unidades Administrativas, con frecuencia anual, así como también de remitir la matriz de riesgos y el plan de mitigación propuesto a la Gestión de Sistemas Integrados y Calidad, para su respectivo seguimiento.

i) El responsable del proyecto será el responsable de analizar y/o actualizar los riesgos de proyectos institucionales, así como la definición de las medidas de control a implementarse con su respectivo responsable. Este ejercicio se realizará como parte de la documentación de inicio del proyecto y será entregada a la Gestión de Sistemas Integrados y Calidad, una vez termine el mismo.

j) En el caso que una Unidad Administrativa requiera incluir, eliminar (cambiar a estado pasivo) o modificar algún riesgo; se deberá solicitar mediante memorando a la Gestión de Sistemas Integrados y Calidad dicho cambio, para lo cual deberá sustentar su requerimiento con información que la respalde a fin de ser revisada y aprobada por la Gestión de Sistemas Integrados y Calidad.

k) Las evidencias de las acciones de control implementadas, deben ser remitidas a través de correo electrónico a la Gestión de Sistemas Integrados y Calidad, conforme la frecuencia establecida en el plan de mitigación de los riesgos, para más adelante ser evaluadas en conjunto, en conformidad con la metodología establecida.

l) La identificación de los riesgos se lo realizará al inicio del año/proyecto, con la finalidad de que las unidades administrativas tengan el conocimiento del riesgo.

m) En el caso de Oportunidades, serán gestionadas mediante el uso del formato "*F02-PRO-GPE-GSI-003 Matriz de Oportunidades*", tomando como referencia el análisis FODA.

n) Para el caso de los riesgos de seguridad de la información, se requiere de manera previa llenar la matriz de *"Activos de Información de la Asamblea Nacional - F03-PRO-GPE-GSI-003*" ya que se evaluarán los riesgos de aquellos activos que sean considerados con criticidad media hacia arriba y que formen parte del alcance del sistema de gestión. Así también, una vez se hayan establecido los riesgos de seguridad, se levantará el plan de tratamiento respectivo y la matriz de "Declaración de aplicabilidad - *F04-PRO-GPE-GSI-003*".

o) En cuanto al manejo de las matrices a utilizar para el levantamiento de información de riesgos, se establece el *"Instructivo para la Administración de riesgos y Oportunidades Institucionales – INS-PRO-GPE-GSI-001".*

p) Los controles existentes dentro del sistema de gestión de seguridad de la información corresponden a medidas que se han implementado como apoyo a las medidas de seguridad de un activo.

q) Las Unidades Administrativas serán responsables de remitir las evidencias de las medidas de control establecidas en el plan de mitigación. En el caso de no ser una acción recurrente, la entrega de evidencias corresponderá a la fecha establecida, caso contrario, esta será entregada hasta los primeros 7 días del mes siguiente según la frecuencia definida.

r) Todos los aspectos que no se encuentren normados de forma expresa en este documento deben ser complementados o suplidos por las disposiciones del marco normativo vigente.

6.3.1 METODOLOGÍA

La metodología presentada se basa en un ciclo de mejora continua, conforme al siguiente detalle:

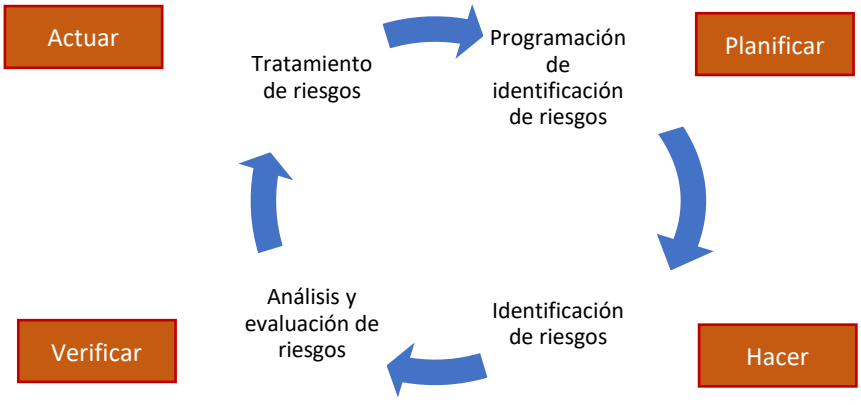


Ilustración 2. Ciclo de la administración de riesgos

Para el efecto, se deberá utilizar el instructivo "*Riesgos Institucionales*" en el cual se detalla los aspectos principales para completar la Matriz de riesgos y el plan de mitigación correspondiente.

6.3.2 MATRIZ DE ADMINISTRACIÓN DE RIESGOS

6.3.2.1 MATRIZ DE ADMINISTRACIÓN DE RIESGOS

La matriz de administración de riesgos institucional está conformada por las siguientes secciones, distribuidas de manera horizontal:

1. Generalidades.
2. Identificación y análisis de riesgos.
3. Valoración del Riesgo

6.3.2.2 GENERALIDADES

Dentro de la matriz de riesgos se encuentra establecido el campo macro generalidades, el cual, entre otros temas, identifica el tipo de riesgo, alineación con objetivos y determinación de factores internos y externos atados a la identificación del riesgo. Esto será identificado con las Unidades Administrativas dueñas del riesgo.

Entre los factores de riesgos externos e internos se tiene los siguientes:

FACTORES EXTERNOS		
FACTORES	**DESCRIPCION**	**EJEMPLOS**
ECONÓMICO	Evento o suceso externo no deseado, el cual, afecta de manera negativa a la disponibilidad de recursos económicos y por ende al desarrollo de las actividades de la Institución.	• Cambio de condiciones económicas. • Desembolso los Recursos Financieros. Inestabilidad del sistema financiero.
POLÍTICO	Evento causado por las resoluciones externas de las autoridades del país que afectan a la Institución	• Incumplimiento de leyes - políticas; o evasión de regulaciones. • Cambio de condiciones gubernamentales y regulatorias. • Continuidad en la Gestión Político - Estratégico.
TECNOLÓGICO	La ocurrencia de un evento externo no deseado que proviene del conjunto de conocimientos específicos de un determinado sector, oficio o arte industrial y que afectan al desenvolvimiento normal de la institución.	• Tecnología inapropiada / incompatible. • Vigencia Tecnológica / Grado de obsolescencia. • Incompatibilidad con la infraestructura y equipos.
SOCIAL	La ocurrencia de un evento externo no deseado que proviene de los problemas de la sociedad y que afectan al desenvolvimiento normal de la institución.	• Atentado, vandalismo o tentativa de agresión. • Intervenciones inapropiadas, mala manipulación o falta de información externa. (Suplantación). • Derechos Humanos.
LEGAL	La posibilidad de que la institución enfrente consecuencias adversas derivadas del incumplimiento de leyes, normas, reglamentos, directrices, contratos, obligaciones regulatorias o disposiciones emitidas por organismos de control.	• Incumplimiento normativo • Interpretación incorrecta de la normativa vigente. • Incumplimiento de obligaciones contractuales. • Incumplimiento de plazos legales.

FACTORES EXTERNOS		
FACTORES	**DESCRIPCION**	**EJEMPLOS**
AMBIENTAL ANTRÓPICO O SISTÉMICO	Evento o catástrofe causado en el medio ambiente; bien sea, por un fenómeno propio de la naturaleza o por la acción del hombre que lo genere.	• Insuficiencia en los Servicios Públicos requeridos. • Riesgos Naturales: derrumbes, erupciones volcánicas, deslaves, terremotos. • Alteración de la calidad de aire.

Tabla 3. Factores externos

FACTORES INTERNOS		
FACTORES	**DESCRIPCION**	**EJEMPLOS**
INFRAESTRUCTURA	Acontecimientos negativos en cuanto a: -Infraestructura y demás que tengan relación directa con las condiciones laborales.	• Control físico y aseguramiento de la Infraestructura requerida.
RECURSO HUMANO	Acontecimientos negativos que provengan de los funcionarios de la Institución. Estos pueden ser por: -Conocimiento insuficiente para el cargo a cubrir, -Poca experiencia, -Sobrecarga laboral, -Rotación de personal u otros factores.	• Rotación de Personal. • Competencia del Personal: Educación, Formación, Habilidades y Experiencia. Riesgo Laboral – • Factor de Riesgo Psicosocial, Ergonómico.
CULTURA ORGANIZACIONAL	Se refiere al conjunto de valores, principios, creencias, actitudes, comportamientos y prácticas compartidas por los servidores y funcionarios de la institución, que influyen directamente en la forma en que se toman decisiones, se ejecutan los procesos, se cumplen las normas y se gestionan los riesgos.	• Resistencia del personal al cumplimiento de procedimientos y controles establecidos. • Tolerancia a prácticas informales que no cumplen la normativa interna. • Falta de compromiso con los sistemas de gestión (calidad, antisoborno, seguridad de la información). • Escasa cultura de control interno y gestión de riesgos. • Normalización de incumplimientos de plazos o requisitos. • Baja sensibilización en ética, integridad y prevención del soborno. • Falta de reporte oportuno de incidentes o irregularidades.
CUMPLIMIENTO DE OBJETIVOS	Se refiere a la capacidad de la institución y de sus Unidades Administrativas para alcanzar las metas estratégicas, operativas y de gestión, de acuerdo con los plazos, recursos y lineamientos establecidos. Este factor de riesgo se presenta cuando existen debilidades en la planificación, ejecución, seguimiento o control de los objetivos institucionales, lo que puede generar desviaciones, incumplimientos, uso ineficiente de recursos y afectación al desempeño institucional.	• Definición inadecuada o poco clara de objetivos institucionales o de unidad. • Falta de alineación entre objetivos estratégicos, operativos y de proyectos. • Ausencia de indicadores de desempeño para medir el avance de los objetivos. • Insuficiente seguimiento y evaluación del cumplimiento de metas. • Retrasos en la ejecución de actividades planificadas. • Asignación inadecuada de recursos humanos, financieros o tecnológicos. • Cambios frecuentes de prioridades sin una adecuada gestión del impacto.

FACTORES INTERNOS		
FACTORES	**DESCRIPCION**	**EJEMPLOS**
TECNOLOGÍA	Incluyen vulnerabilidades en la seguridad cibernética, obsolescencia tecnológica, dependencia de sistemas crítico	• Soporte a las operaciones actuales y futuras. • Salvaguarda, invulnerabilidad y fiabilidad de las Tics. • Integración de los Sistemas de Información.
PROCESOS	El factor procesos se refiere al conjunto de actividades, procedimientos y flujos de trabajo internos mediante los cuales la institución cumple sus funciones y alcanza sus objetivos.	• Procesos no documentados o desactualizados. • Falta de estandarización en la ejecución de actividades. • Duplicidad de funciones o actividades entre unidades administrativas. • Procesos con excesivos puntos de control o trámites innecesarios. • Falta de indicadores para medir el desempeño de los procesos. • Deficiente coordinación entre procesos o áreas involucradas. • Dependencia excesiva de procesos manuales. • Ausencia de mecanismos de seguimiento y mejora continua. • Alineamiento Estratégico en los diversos niveles de Gestión. • Exceso de Información; • Información innecesaria; • Información a destiempo. • Procesos y/o procesamientos innecesarios; • Reprocesos y/o correcciones.

Tabla 4. Factores internos

6.3.2.3 IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

Es el proceso sistemático mediante el cual la institución reconoce, describe y evalúa los eventos que pueden afectar el logro de sus objetivos estratégicos, operativos, de calidad, de seguridad de la información, antisoborno y de proyectos.

Este proceso permite determinar los eventos/amenazas, así como también el impacto/ vulnerabilidad, probabilidad de ocurrencia e impacto, así como el nivel de riesgo inherente sobre el objeto evaluado.

En cuanto al análisis de riesgos se ha determinado lo siguiente:

Probabilidad: La evaluación de la probabilidad se realizará en función de los siguientes parámetros:

Calificación y Valoración de la Probabilidad	Descripción
Alto (3)	El evento es **muy probable que ocurra** en las condiciones actuales. Su materialización se espera o es casi segura a corto/mediano plazo.
Medio (2)	El evento **podría ocurrir** en algún momento bajo las condiciones actuales. Existe una posibilidad razonable de materialización.
Bajo (1)	El evento es **poco probable que ocurra** en las condiciones normales actuales. Su materialización sería inusual o excepcional.

Tabla 5. Valoración de la Probabilidad

Para decidir sobre la asignación de la probabilidad de alguno de los tres niveles citados, se debe responder a la pregunta: ¿Qué tan probable es que suceda el riesgo? y registrar el valor en el campo que corresponda.

Impacto: Para la identificación del impacto (Efecto) del riesgo, al igual que en el caso anterior, existen tres posibles opciones para categorizarlo, como se muestra en la siguiente tabla descriptiva:

Calificación y Valoración del Impacto	Descripción
Alto (3)	La materialización del riesgo causa **consecuencias graves o catastróficas** que comprometen la viabilidad estratégica, legal u operativa de la organización
Medio (2)	La materialización del riesgo causa **consecuencias significativas** que afectan objetivos operativos o de cumplimiento, requiriendo acción de gestión dedicada
Bajo (1)	La materialización del riesgo causa **consecuencias menores y localizadas**, fácilmente absorbibles por la operación normal

Tabla 6. Valoración del Impacto

Para asignar un nivel determinado de Impacto se debe responder a la pregunta: ¿Cuál es el impacto en el caso de que suceda el riesgo?, registrar el valor en el campo que corresponda.

En cuanto al valor del riesgo, estará dado por la siguiente fórmula:

$$\boldsymbol{Riesgo = Probabilidad * Impacto}$$

El resultado obtenido del riesgo en una escala de tres colores: Rojo, Amarillo y Verde, de acuerdo con el siguiente detalle:

Probabilidad: Impacto		Nivel de Riego	Rango Porcentual
1-2	1:1	BAJO	11%
	1:2	BAJO	22%
	2:1	BAJO	22%
3-4	1:3	MEDIO	33%
	2:2	MEDIO	44%
	3:1	MEDIO	33%
6-9	3:2	ALTO	67%
	3:3	ALTO	100%
	2:3	ALTO	67%

Tabla 7. Niveles de riesgo

6.3.2.4 PLAN DE MITIGACIÓN DE RIESGOS

El plan de mitigación de riesgos, constituirá la ejecución de actividades para reducir la probabilidad y/o el impacto de los riesgos identificados, de manera controlada y planificada.

Para el tratamiento del riesgo se debe realizar un análisis para determinar un conjunto de acciones o controles que la Unidad Administrativa decida ejecutar para evitar, transferir, aceptar, reducir las consecuencias y medidas para disminuir la probabilidad de los riesgos identificados, en base a la siguiente tabla:

TIPOS DE MEDIDAS	ACCIÓN
Medidas para transferir un riesgo	Consiste en que un tercero soporte o comparta, parcial o totalmente, la responsabilidad y/o las consecuencias potenciales de que un riesgo se materialice.

TIPOS DE MEDIDAS	ACCIÓN
Medidas para aceptar un riesgo	Consisten en no aplicar otros tipos de medidas y estar en disposición de enfrentar las eventuales consecuencias.
Medidas para reducir la probabilidad de un riesgo	Consiste en identificar el peligro del proyecto, función o actividad y controlarlo, para que logre su objetivo sin verse afectado por el riesgo.
Medidas para evitar la probabilidad de un riesgo	Consiste en eliminar la causa del riesgo o dejar de realizar la actividad que lo genera.

Tabla 8. Medidas de riesgos

Con respecto al sistema de gestión de seguridad de la información, es indispensable determinar los controles que se aplican en función de la norma ISO/IEC 27001:2022. Esto servirá como insumo para obtener la Declaración de Aplicabilidad de Controles de Seguridad de la Información.

6.3.2.5 DE LA EFICACIA DE LAS ACCIONES Y RIESGO RESIDUAL

A fin de medir objetivamente si las acciones y controles implementados están cumpliendo con su propósito, se realizará una evaluación anual por parte de la Gestión de Sistemas Integrados y Calidad de la Coordinación General de Planificación Estratégica, aplicando los siguientes criterios:

A: Grado de aplicación
B: Frecuencia en su ejecución y seguimiento
C: Determinación y definición del responsable/s del mismo.
D: Carácter preventivo.
E: Grado de documentación o evidencia

$$\boldsymbol{Eficacia\ de\ la\ acci\acute{o}n} = \frac{A + B + C + D + E}{5}$$

Variables	Grado de aplicación	Calificación
A	Nada aplicable	0
	Aplicación parcial	0,5
	Aplicable	1
	Frecuencia en ejecución	**Calificación**
B	No se ejecuta	0
	Ejecución parcial	0,5
	Acción ejecutada	1
	Definición del responsable	**Calificación**
C	Sin responsable	0
	Sin definición clara	0,5
	Responsable definido	1
	Carácter preventivo	**Calificación**
D	Nada preventivo	0
	Medio preventivo	0,5
	Preventivo	1
	Grado de documentación	**Calificación**
E	Sin evidencia	0
	Evidencia parcial	0,5
	Evidencia total	1

Tabla 9. Factores de evaluación de la eficacia de la acción

En cuanto al riesgo residual está dado por:

Riesgo residual = Riesgo Inherente * (1 – Eficacia de la Acción**)**

Porcentaje del Riesgo Residual: Valor del Riesgo Residual / 9

El resultado obtenido será identificado de manera gráfica en alguno de estos tres niveles:

Valoración de Riesgo Residual	Descripción
Alto (6-9)	Los controles son insuficientes o ineficaces. Requiere acciones inmediatas de fortalecimiento de controles. • Ejemplo antisoborno: manejo de contratos de alto valor por una sola persona sin revisión independiente. • Ejemplo calidad: producto crítico que llega defectuoso al cliente sin mecanismos de detección previa.
Medio (3-4)	Aun con controles, persisten vulnerabilidades que hacen posible su materialización. El impacto puede ser moderado y requerir acciones adiciona-les de mitigación. • Ejemplo antisoborno: contratación de proveedores donde existe debida diligencia parcial pero no continua. • Ejemplo calidad: reprocesos frecuentes en producción por fallas de control en etapas intermedias.
Bajo (0-1)	Después de aplicar los controles, la posibilidad de que ocurra el riesgo es mínima. El impacto, en caso de ocurrir, sería menor y manejable. • Ejemplo antisoborno: proceso de pagos con segregación de funciones, autorizaciones múltiples y auditoría frecuente. • Ejemplo calidad: un proceso automatizado con inspección final y verificación continua.

Tabla 10. Valoración de riesgo residual

Categoría de Riesgo Residual: Representa el valor del resultado obtenido del riesgo en una escala de tres colores: Rojo, Amarillo y Verde, de acuerdo con el siguiente detalle:

Residual	Nivel de Riego	Rango Porcentual
1:1	BAJO	11%
1:2	BAJO	22%
2:1	BAJO	22%
1:3	MEDIO	33%
2:2	MEDIO	44%
3:1	MEDIO	33%
3:2	ALTO	67%
3:3	ALTO	100%
2:3	ALTO	67%

Tabla 11. Medidas de riesgos

Finalmente, se determina que un riesgo residual es aceptable cuando el riesgo residual es menor a 6.

6.3.2.6 LINEAMIENTOS PARA EL SISTEMA DE GESTIÓN ANTISOBORNO

Para el Sistema de Gestión Antisoborno se aplicarán los siguientes controles:

Control operacional: Los controles operacionales en materia antisoborno son medidas, procedimientos o prácticas implementadas dentro de los procesos de la organización para prevenir, detectar y mitigar riesgos de soborno, asegurando que las actividades se ejecuten conforme a la política antisoborno y los requisitos legales y normativos aplicables. (Aplica para ISO 37001:2016)

Para los criterios de identificación de cargos críticos, considerando no solo el nivel jerárquico o acceso a recursos financieros, sino también el grado de influencia en decisiones estratégicas, la participación en procesos de contratación, la gestión de presupuesto, y la interacción con terceros (proveedores), se establece lo siguiente:

Cargos críticos	Definición
Nivel jerárquico	• Carta de compromiso de los sistemas de gestión.
Coordinación General Financiera	• Carta de compromiso de los sistemas de gestión.
Interacción con terceros	• Resolución de inicio de proceso de delegación de administrador de contrato. • Carta compromiso de los sistemas de gestión.

Tabla 12. Control operacional

La evaluación de comportamiento ético se realizará con la evaluación del control de los riesgos y mediante las auditorías internas del sistema de gestión antisoborno.

Se realizará retroalimentación continua de los resultados de riesgos y de las auditorías a las unidades administrativas por medio de la Alta Dirección.

6.3.2.7 DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los activos de información son todos aquellos elementos que contienen, procesan, almacenan o transmiten información de la Asamblea Nacional y que tienen valor para la institución, por lo que deben ser protegidos adecuadamente para garantizar su confidencialidad, integridad y disponibilidad.

Se consideran activos de información, entre otros:

- Información en formato físico y digital (documentos legislativos, resoluciones, bases de datos, expedientes, correos electrónicos).
- Sistemas de información y aplicaciones institucionales.
- Infraestructura tecnológica (servidores, redes, equipos de cómputo).
- Servicios de tecnología de la información.
- Recursos humanos que gestionan o acceden a la información.
- Proveedores y terceros con acceso a información institucional.

Cada activo de información se lo registrará en el formato: ***"F03-PRO-GPE-GSI-003 Activos de información de la Asamblea Nacional".***

6.3.2.8 DE LA DECLARACIÓN DE APLICABILIDAD DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

La Declaración de Aplicabilidad (SoA) es el documento mediante el cual la Asamblea Nacional determina y justifica los controles de seguridad de la información que son aplicables, no aplicables o implementados parcialmente, en función de los riesgos identificados y evaluados sobre sus activos de información.

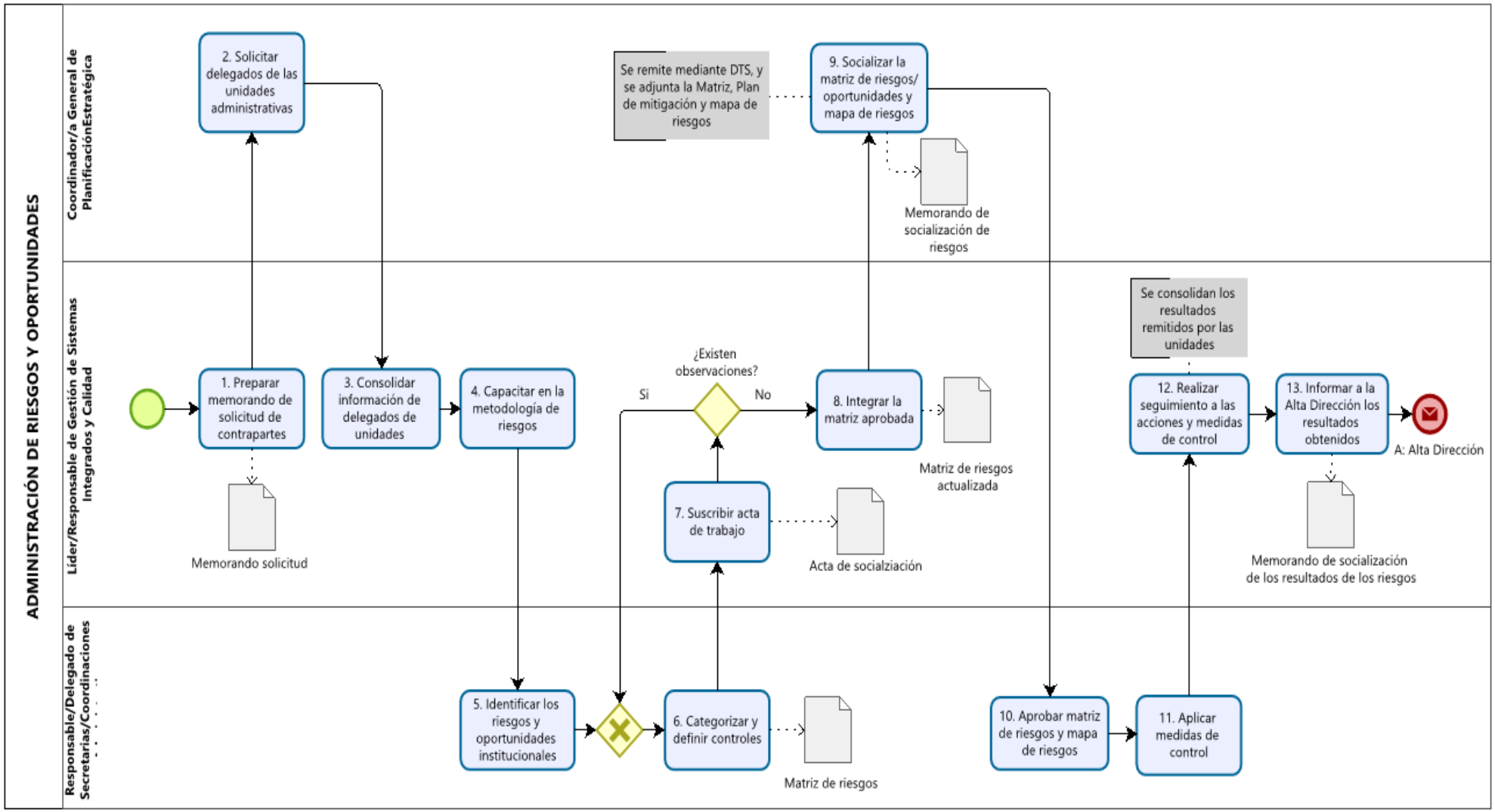
La (SoA) permite asegurar que los controles seleccionados son proporcionales al nivel de riesgo y están alineados con los objetivos institucionales y los requisitos legales, normativos y regulatorios aplicables.

La justificación de aplicabilidad se lo desarrollará en el formato: ***"F05V02-PRO-GPE-GSI-004 Declaración de aplicabilidad de controles de seguridad de la información".***

7. FICHA DE CARACTERIZACIÓN DEL PROCESO

Gestión de Desarrollo Metodológico De Procesos e Instrumentos Técnicos		
Tipo de Proceso	Asesoría	
Responsable del Proceso	Líder/Responsable de Gestión de Sistemas Integrados y Calidad	
Objetivo	Implementar una metodología eficaz para identificar, analizar, evaluar y gestionar los riesgos a los que se encuentra expuesta la Asamblea Nacional del Ecuador, con el fin de comunicar los resultados a la Alta Dirección y facilitar la toma de decisiones de forma oportuna.	
Objetivo Estratégico	OE4: Fortalecer y modernizar la gestión de la Asamblea Nacional.	
Proveedor	Evaluación de los Sistemas de Gestión y Acciones Correctivas Alta Dirección Comité de Calidad	
Entradas	Documentación del Sistema de Gestión Identificación de riesgos	
Actividades	Actividad Inicial 1. Preparar memorando de solicitud de contrapartes Actividad final: 12. Informar a la Alta Dirección los resultados obtenidos	
Controles	**5.** Construir matriz de riesgos **CONTROL:** Equipo metodológico de riesgos categorizará el riesgo "alto, medio o bajo" **RESPONSABLE:** Equipo metodológico de riesgos **11.** Aplicar medidas de control a los riesgos **CONTROL:** Inspección de evidencias de las acciones implementadas. **RESPONSABLE:** Equipo metodológico de riesgos	
Salidas	Matriz de riesgos institucional Acta de socialización de riesgos y medidas de control a aplicar	
Usuarios	Unidades Administrativas de la Asamblea Nacional Alta Dirección Documentos del Sistema de Gestión	
Recursos	**1. Software** Utilitarios de office o software libre **2. Hardware** Equipo de computo **3. Infraestructura** Estaciones de Trabajo **4. Recursos Humanos** Descritos en diagrama de flujo	
Indicador 1	**Nombre**	Porcentaje de reducción de riesgos residuales respecto a riesgos inherentes
	Fórmula	(Riesgo Inherente −Riesgo Residual) /Riesgo Inherente × 100
Riesgo	Descrito en Matriz de Riesgos Institucionales	

8. DIAGRAMA DE FLUJO



9. DESCRIPCIÓN DE ACTIVIDADES

#	Actividad	Responsable de ejecución de la actividad	Descripción	Registro
1.	Preparar memorando de solicitud de contrapartes	Líder/ delegado de la Gestión de Sistemas Integrados y Calidad	Preparará memorando de solicitud de contrapartes para el levantamiento, actualización o seguimiento de los riesgos y oportunidades institucionales.	
2.	Solicitar delegados de las Unidades Administrativas	Coordinador/a General de Planificación Estratégica	La Coordinación General de Planificación Estratégica con apoyo de la unidad de Sistemas integrados y Calidad, solicitará delegados de las Unidades Administrativas, los cuales participarán en el levantamiento de riesgos y oportunidades de acuerdo a su competencia.	
3.	Consolidar información de delegados de unidades administrativas	Líder/ delegado de la Gestión de Sistemas Integrados y Calidad	Recibirá la información de las contrapartes y consolida la misma.	
4.	Capacitar en la metodología	Líder/ delegado de la Gestión de Sistemas Integrados y Calidad	El Líder/ delegado de la Unidad de Sistemas Integrados y Calidad forma grupos integrados por los delegados de cada Unidad Administrativa, a los que se capacitará sobre la metodología y herramientas a utilizarse para la administración de riesgos y oportunidades institucionales en función al ***"Instructivo para la Administración de Riesgos y Oportunidades"***	
5.	Identificar los riesgos y oportunidades institucionales	Responsables de la Unidades Administrativas	Los responsables de la Unidad Administrativa serán los encargados de identificar los riesgos, así como también su correspondiente evaluación y establecimiento de medidas/control, bajo la coordinación metodológica de la Unidad de Sistemas Integrados y Calidad. **CONTROL:** Equipo metodológico de riesgos categorizará el riesgo "alto, medio o bajo" **RESPONSABLE:** Equipo metodológico de riesgos	• Matriz de riesgos F01-PRO-GPE-GSI-003 • Matriz oportunidades F02-PRO-GPE-GSI-003 • Plan de mitigación de riesgos F04-PRO-GPE-GSI-003
6.	Categorizar y definir controles	Responsables de la Unidades Administrativas	Los responsables de la Unidad Administrativa, definirán los controles y las evidencias a aplicar para que las mismas sea reportadas a la Gestión de Sistemas Integrados y Calidad, conforme las frecuencias definidas en las matrices.	• Plan de mitigación de riesgos F04-PRO-GPE-GSI-003

#	Actividad	Responsable de ejecución de la actividad	Descripción	Registro
7.	Suscribir acta de trabajo	Líder/ delegado de la Gestión de Sistemas Integrados y Calidad	El Líder/ delegado de la Unidad de Sistemas Integrados y Calidad junto con él o delegados de las unidades administrativas, suscribirán acta de conformidad de los riesgos y oportunidades identificados. ¿Existen observaciones? En caso que existan observaciones, deberá volver a la actividad 6 de este procedimiento. Si no existe observaciones, continuará con la actividad 8 de este procedimiento.	• Acta de reunión F01-PRO-GPE-GCP-001
8.	Integrar la matriz aprobada	Líder/ delegado de la Gestión de Sistemas Integrados y Calidad	Se consolidará la matriz y se genera el mapa de riesgos.	• Mapa de riesgos
9.	Socializar la matriz de riesgos/oportunidades y mapa de riesgos	Coordinador/a General de Planificación Estratégica	Mediante DTS *"Sistema de Gestión Documental"* se enviará a las unidades administrativas la socialización de la matriz de riesgos, mapa de riesgos y plan de mitigación de riesgos.	• Matriz de riesgos F01-PRO-GPE-GSI-003 • Matriz oportunidades F02-PRO-GPE-GSI-003 • Plan de mitigación de riesgos F04-PRO-GPE-GSI-003 • Mapa de riesgos
10.	Aprobar matriz de riesgos y mapa de riesgos	Responsable/Delegado de Secretarias/Coordinaciones Administrativas	Cada Unidad Administrativa deberá suscribir el mapa de riesgos aprobado, en el cual expresa el resumen de riesgos inherente y residual y remitir a la Coordinación General de Planificación Estratégica.	• Mapa de riesgos
11.	Aplicar medidas de control	Responsable/Delegado de Secretarias/Coordinaciones Administrativas	Cada Unidad Administrativa ejecutará las medidas de control conforme la frecuencia establecida en el "*Plan de mitigación de riesgos*"**.** **CONTROL:** Inspección de evidencias de las acciones implementadas. **RESPONSABLE:** Equipo metodológico de riesgos	• Plan de mitigación de riesgos F04-PRO-GPE-GSI-003
12.	Realizar seguimiento a las acciones y medidas de control	Líder/ delegado de la Gestión de Sistemas Integrados y Calidad	El Líder/ delegado de la Unidad de Sistemas Integrados y Calidad realizará seguimientos a las Unidades Administrativas para evaluar los avances de las medidas de control de los riesgos identificados.	• Plan de mitigación de riesgos F04-PRO-GPE-GSI-003
13.	Informar a la Alta Dirección los resultados obtenidos	Líder/ delegado de la Gestión de Sistemas Integrados y Calidad	El Líder/ delegado de la Unidad de Sistemas Integrados y Calidad reportará los resultados de mapa de calor a la Alta Dirección de los Sistemas de Gestión.	
FIN				

10. MEDICIÓN DEL PROCESO

N°	Indicador	Definición	Fórmula de Cálculo	Unidad de Medida	Responsable de Medición	Meta	Fuente de la Información	Frecuencia de Medición
1	Porcentaje de reducción del riesgo	Medir el porcentaje de reducción del riesgo inherente una de conformidad con la implementación de las acciones control imple entadas por parte de las unidades administrativas responsables	(Riesgo Inherente−Riesgo Residual) / RiesgoInherente×100	Porcentaje	Líder de Gestión de Sistemas Integrados y Calidad	Alcanzar al menos 75% de reducción del riesgo residual respecto al riesgo inherente.	Matriz de riesgos	Semestral

11. TERMINOS Y DEFINICIONES

- **Activo de información:** Cualquier cosa que tenga valor para la organización y por lo tanto debe ser protegida. Entre los activos primarios se encuentran la información, procesos y actividades.
- **Administración de Riesgo:** Proceso sistemático que deben realizar las instituciones para evaluar y dar seguimiento al comportamiento de los riesgos a que están expuestas en el desarrollo de sus actividades, mediante el análisis de los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias y acciones que permitan controlarlos y asegurar el logro de los objetivos y metas de una manera razonable.
- **Amenaza:** Causa potencial de la ocurrencia de un incidente no deseado, que puede ocasionar daños a un sistema o a la organización.
- **Alta Dirección:** Es aquella con la responsabilidad de demostrar liderazgo y compromiso con respecto a la implementación de los sistemas de gestión de la Asamblea Nacional.
- **Base de conocimiento:** Es un repositorio de documentos técnicos, manuales y preguntas frecuentes que se encuentran alojadas en el área de la Dirección de Tecnologías de la Información y Comunicaciones.
- **Catálogo de servicios tecnológicos informáticos:** Corresponde al listado de servicios tecnológicos.
- **Causa del Riesgo:** Manifestación, características o variable mensurable u observable que indica la presencia de un riesgo, lo provoca, o modifica su nivel. Condición que origina un evento riesgoso y que provoca incertidumbre.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible; ni sea revelada a individuos, instituciones o procesos no autorizados.
- **Conflicto de Intereses:** Situación donde los intereses de negocios, financieros, familiares, políticos o personales podrían interferir con el juicio de valor del personal en el desempeño de sus obligaciones hacia la organización.
- **Control:** Medida que mantiene y/o modifica el riesgo
- **Consecuencias:** Conjunto de efectos derivado de la ocurrencia de una situación identificada como riesgosa expresada cualitativa o cuantitativamente, sean pérdidas, perjuicios, desventajas o ganancias.
- **Debida diligencia**: Proceso para evaluar con mayor detalle la naturaleza y el alcance del riesgo de soborno y para ayudar a las organizaciones a tomar decisiones en relación con transacciones, proyectos, actividades, socios de negocios y personal específico.
- **Disponibilidad**: Propiedad de que la información sea accesible, utilizable y/o disponible a los usuarios autorizados cuando estos lo requieran.
- **Equipo metodológico:** Es el equipo conformado por el personal de la Unidad Administrativa/Legislativa y el personal de la Unidad de Sistemas Integrados y de Calidad.

- **Evento externo:** Son aquellos sobre los cuales la entidad no tiene control, por ejemplo, desastres naturales, actos terroristas, etc.
- **Evento:** Incidente o situación que podría ocurrir en un lugar específico, en un intervalo de tiempo particular."
- **Factor de Riesgo:** Circunstancia o situación interna y/o externa que aumenta la probabilidad de que un riesgo se materialice.
- **Integridad:** Propiedad de salvaguardar la integridad de las aplicaciones e información preservando la información completa y exacta.
- **Magnitud de Impacto**: Representación del efecto o de las consecuencias negativas que se generarían en la Institución, en el supuesto de materializarse el riesgo.
- **Objeto del Riesgo:** Es el servicio y/o producto al cual se realizará el análisis de riesgos institucionales.
- **Oportunidad:** Hace referencia a lo conveniente de un contexto y a la confluencia de un espacio y un periodo temporal apropiada para obtener un provecho o cumplir un objetivo. Las oportunidades, por lo tanto, son los instantes o plazos que resultan propicios para realizar una acción.
- **Organización:** Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus objetivos.
- **Parte interesada:** Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
- **Plan de Acción:** Un plan de acción es un tipo de plan que prioriza las iniciativas más importantes para cumplir con ciertos objetivos y metas. De esta manera, un plan de acción se constituye como una especie de guía que brinda un marco o una estructura a la hora de llevar a cabo un proyecto.
- **Probabilidad de ocurrencia:** Posibilidad o estimación de que ocurra un evento, en un periodo determinado.
- **Riesgo:** es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o su entorno, representan una amenaza para el cumplimiento de un plan con posibles eventos en el futuro, con incertidumbre en su ocurrencia, que pueden tener una o más causas raíz, y que, si ocurren pueden tener uno o más impactos negativos.
- **Riesgo residual:** Riesgo después de la aplicación del método de tratamiento
- **Seguridad de la información:** Es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción.
- **Soborno:** Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera) directamente o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actué o deje de actuar en relación con el desempeño de las obligaciones de esa persona.
- **Socio de negocios**: Parte externa con la que la organización, tiene o planifica establecer, algún tipo de relación comercial.
- **Vulnerabilidad**: Debilidad de un activo o control, que puede ser explotado por una o más amenazas.

12. FORMATOS, REGISTROS Y ANEXOS

12.1FORMATOS Y ANEXOS

Código	Nombre del documento
F01v03-PRO-GPE-GSI-003	Matriz de administración de riesgos de la Asamblea Nacional
F02V03-PRO-GPE-GSI-003	Matriz administración de oportunidades
F03V02-PRO-GPE-GSI-003	Activos de información de la Asamblea Nacional
F04V01-PRO-GPE-GSI-003	Plan de mitigación de riesgos
F05V02-PRO-GPE-GSI-003	Declaración de aplicabilidad de controles de seguridad de la información
INS-PRO-GPE-GSI-001	Instructivo para la Administración de riesgos y Oportunidades Institucionales

13. TABLA DE CONTROL DE DOCUMENTOS DEL PROCEDIMIENTO

Tipo	Código	Nombre de documento	Responsable de resguardo	Almacenamiento	Indexación	Control de acceso	Tiempo de retención
				Ubicación física y/o electrónica	Criterio de ordenación		
Matriz	F01- PRO-GPE-GSC-003	Matriz de Riesgos	Responsable de Sistemas Integrados y Calidad	**Digital:** ***Alfresco - Sistema de Gestión de la Asamblea Nacional***	Cronológico	Servidores de las unidades administrativas dueñas de los riesgos Personal de la Coordinación General de Planificación Estratégica	**Digital**: 7 años
Matriz	F02- PRO-GPE-GSC-003	Matriz de oportunidades	Responsable de Sistemas Integrados y Calidad	**Digital:** ***Alfresco - Sistema de Gestión de la Asamblea Nacional***	Cronológico	Servidores de las unidades administrativas dueñas de las oportunidades Personal de la Coordinación General de Planificación Estratégica	**Digital**: 7 años
Matriz	F03- PRO-GPE-GSC-003	Activos de información	Responsable de Sistemas Integrados y Calidad Oficial de Seguridad de la Información	**Digital:** ***Alfresco - Sistema de Gestión de la Asamblea Nacional***	Cronológico	Servidores de las unidades administrativas dueñas de los riesgos Personal de la Coordinación General de Planificación Estratégica	**Digital**: 7 años
Matriz	F04- PRO-GPE-GSC-003	Plan de mitigación de riesgos	Personal de la Sistemas Integrados y Calidad	**Digital:** ***Alfresco - Sistema de Gestión de la Asamblea Nacional***	Cronológico	Servidores de las unidades administrativas dueñas de los riesgos Personal de la Coordinación General de Planificación Estratégica	**Digital**: 7 años

Tipo	Código	Nombre de documento	Responsable de resguardo	Almacenamiento	Indexación	Control de acceso	Tiempo de retención
				Ubicación física y/o electrónica	Criterio de ordenación		
Matriz	F05- PRO-GPE-GSC-003	Declaración de aplicabilidad de controles de seguridad de la información	Responsable de Sistemas Integrados y Calidad Oficial de Seguridad de la Información	**Digital:** ***Alfresco - Sistema de Gestión de la Asamblea Nacional***	Cronológico	Servidores de las unidades administrativas dueñas de los riesgos Personal de la Coordinación General de Planificación Estratégica	**Digital**: 7 años
Matriz	No aplica	Mapa de riesgos	Responsable de Sistemas Integrados y Calidad	**Digital:** ***Alfresco - Sistema de Gestión de la Asamblea Nacional***	Cronológico	Personal de la Sistemas Integrados y Calidad	**Digital**: 7 años
Evidencias	No aplica	Carpeta de evidencia de unidades administrativas riesgos inherentes	Responsable de Sistemas Integrados y Calidad	**Digital:** ***Alfresco - Sistema de Gestión de la Asamblea Nacional***	Cronológico	Servidores de las unidades administrativas dueñas de los riesgos Personal de la Coordinación General de Planificación Estratégica	**Digital**: 7 años