Instituto Nacional Electoral

Dirección Ejecutiva de Administración

# Marco Normativo de Control Interno

del Instituto Nacional Electoral

## Contenido

# Contexto básico del Control Interno

El Control Interno es un proceso dinámico e iterativo efectuado por la alta dirección, en el que participa todo el personal de cualquier entidad pública o privada. En términos generales y en el caso del Instituto Nacional Electoral (INE), el control interno es impulsado por el Consejo General y la Junta General Ejecutiva, así como por los Titulares de las Unidades Responsables (UR), órganos delegacionales y las y los demás servidores públicos. Este proceso es acompañado por el Órgano Interno de Control (OIC), en el ámbito de su respectiva competencia y tiene como objeto el proporcionar una seguridad razonable sobre la consecución de los objetivos institucionales, vigilar la implementación y operación del control interno como apoyo en el logro de los objetivos vinculados con sus procesos y la salvaguarda de los recursos públicos, así como para prevenir la corrupción.

De esta manera, existe una relación directa entre los objetivos estratégicos, los procesos institucionales, los componentes o normas generales, principios y elementos de Control Interno, entendidos estos como el conjunto de requisitos necesarios que se deben cumplir para alcanzar dichos objetivos.

La implementación de un sistema de control interno efectivo incluye planes, uso de metodologías, definición de programas, políticas, procedimientos y sistemas que se orientan a dar cumplimiento al mandato constitucional, la Política Nacional Anticorrupción, la misión, la visión, el plan estratégico, los objetivos y las metas institucionales.

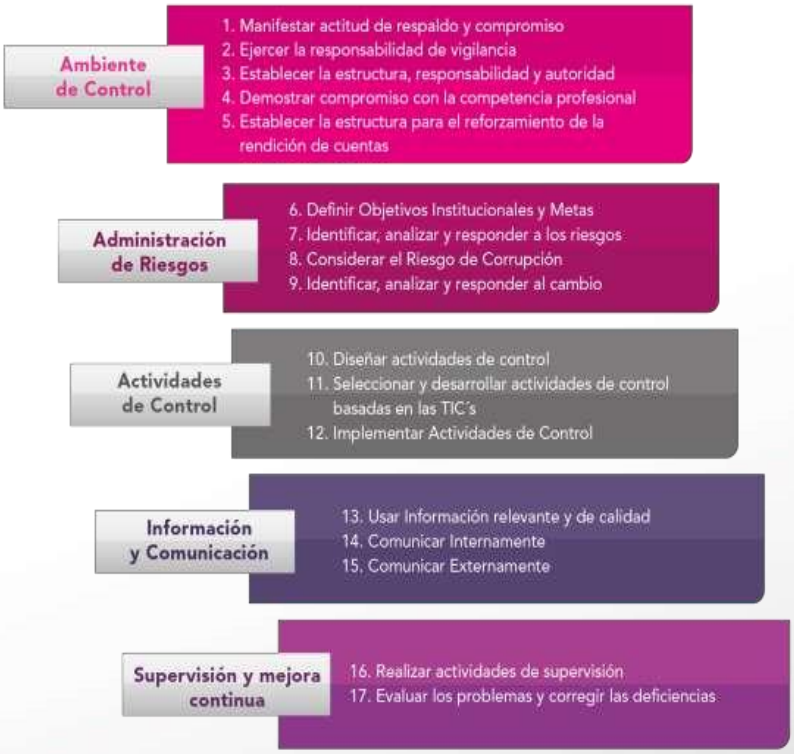
En México, la metodología adoptada para las instituciones públicas es la denominada COSO de amplia utilización a escala internacional y que se integra por los siguientes cinco componentes o normas generales (figura 1):

*Figura 1. Metodología COSO*


Fuente: Elaboración propia de acuerdo al Modelo Coso

Cada uno de estos componentes o normas generales se vincula estrechamente con determinados principios (figura 2) que, en su acepción más general, se entienden como el conjunto de valores que orientan y regulan la vida institucional:

*Figura 2. Principios COSO*




Fuente: Elaboración propia de acuerdo al Modelo Coso

Cuando se evalúa el nivel de cumplimiento de los componentes o normas generales se efectúa analizando los principios referidos, los cuales deben ser periódicamente evaluados en lo individual y como parte del componente al que están vinculados, con el objeto de fortalecer y optimizar el nivel de control interno.

Ciertamente es importante cumplir con todas las normas de control interno, pero la segunda, denominada evaluación de riesgos o administración de riesgos, es considerada por muchos como un elemento central del modelo, pues permite identificar con mayor precisión no solo el riesgo en sí mismo, sino la probabilidad de ocurrencia y su impacto en la consecución de los objetivos institucionales.

*Figura 3. Administración*


Fuente: Elaboración con base al Modelo COSO

Así, el hecho de documentar las situaciones que pueden impedir el logro de los objetivos institucionales permite diseñar estrategias preventivas con el fin de evitar la materialización del riesgo, mitigar su probabilidad de ocurrencia o una vez materializado, atender la situación con el objeto de regresar lo más pronto posible a la normalidad. Todo ello, para evitar o mitigar dichos eventos, ya que a través de la administración de esos riesgos se detecta cuándo, cómo, dónde y porqué los eventos pueden afectar los objetivos.

# Capítulo I. Disposiciones Generales

## Del objeto y ámbito de aplicación

**Artículo 1.** Estas Disposiciones tienen por objeto normar la implementación, fortalecimiento, coordinación, seguimiento y supervisión del Sistema de Control Interno Institucional que se ejecuta a través de los procedimientos de Gestión de Control Interno, en todos los procesos del INE, en el ejercicio de sus atribuciones conferidas en la Constitución Política de los Estados Unidos Mexicanos, en las obligaciones establecidas en la Política Nacional Anticorrupción, así como en el logro de su misión, visión, objetivos, proyectos estratégicos, valores organizacionales y principios rectores institucionales definidos en el Plan Estratégico del Instituto Nacional Electoral y sus metas.

## De las siglas, abreviaturas y definiciones

**Artículo 2.** Para efectos de las presentes disposiciones se entenderá por:

I. Siglas y abreviaturas:

a. **ASF:** Auditoría Superior de la Federación;
b. **Código de Conducta:** Código de Conducta del Instituto Nacional Electoral;
c. **Código de Ética:** Código de Ética de la Función Pública Electoral;
d. **CG:** Consejo General del Instituto;
e. **CP:** Coordinación de Planeación Institucional;
f. **CPI:** Comité de Planeación Institucional;
g. **DEA:** Dirección Ejecutiva de Administración;
h. **INSTITUTO:** Instituto Nacional Electoral;
i. **JGE:** Junta General Ejecutiva;
j. **MNCI:** Marco Normativo de Control Interno;
k. **OIC:** Órgano Interno de Control del Instituto;
l. **PTAR:** Programa de Trabajo de Administración de Riesgos;
m. **PTCI:** Programa de Trabajo de Control Interno;
n. **RICI:** Repositorio Institucional de Control Interno;
o. **SCII:** Sistema de Control Interno Institucional;
p. **SE:** Secretaría Ejecutiva;
q. **TIC:** Tecnologías de Información y Comunicaciones;
r. **UTSI:** Unidad Técnica de Servicios de Informática;
s. **UR:** Unidad (es) Responsable (s).

## II. Definiciones

a. **Acción (es) de control:** Las actividades definidas para ser implementadas por el personal del INSTITUTO para fortalecer los elementos, principios y componentes de control, así como prevenir y administrar los riesgos identificados en el ámbito de sus atribuciones, contribuyendo al logro de los objetivos estratégicos y metas institucionales. Este tipo de actividades pueden ser controles preventivos, detectivos o correctivos, incluidos los de corrupción y los de TIC.

b. **Acción(es) de mejora:** Las actividades determinadas e implantadas por el personal del INSTITUTO y prestadores de servicios para optimizar los procesos, y por lo tanto hacerlos más eficientes y eficaces.

c. **Actores externos:** Instancias independientes del INSTITUTO, involucradas o que pueden influir en el SCII.

d. **Administración:** Se refiere a las y los Titulares y Mandos Medios que participan en la operación de los procesos (estratégicos, sustantivos y de soporte) del INSTITUTO.

e. **Administración de riesgos:** La gestión efectuada por el personal del INSTITUTO y prestadores de servicios que participan en los procesos institucionales, para identificar eventos potenciales, evaluarlos, jerarquizarlos, controlarlos y darles seguimiento, ya que podrían obstaculizar o impedir el cumplimiento de los objetivos institucionales, lo que proporcionará una seguridad razonable para lograrlos, además de evitar posibles actos de corrupción.

f. **Actividades de control:** Son los mecanismos formalmente establecidos, ya sean manuales o automatizados, para mitigar los riesgos a que están expuestos los objetivos, así como a posibles actos de corrupción. Pueden ser de tipo preventivo, detectivo o correctivo.

g. **Área (s) de oportunidad:** Aspectos perfectibles del entorno institucional, bajo la forma de hechos, tendencias, cambios o nuevas necesidades que se pueden aprovechar para el fortalecimiento del SCII.

h. **Autocontrol:** La implantación de mecanismos, acciones y prácticas de supervisión o evaluación de cada sistema, actividad o proceso, que permitan identificar, evitar y, en su caso, corregir con oportunidad los riesgos o condiciones que limiten, impidan o hagan ineficiente el logro de objetivos y proyectos estratégicos institucionales y el cumplimiento de sus metas.

i. **Control Correctivo**: Mecanismo que opera una vez concluido el proceso con el objeto de subsanar eventos no deseados -como errores, omisiones o desviaciones-, que vulneran los objetivos.

j. **Control Detectivo:** Mecanismo que opera durante la ejecución de los procesos, esto es, antes de que concluyan, para identificar errores, omisiones o desviaciones con el fin de que estos se subsanen o se

reviertan antes de la conclusión del proceso y evitar que vulneren los objetivos.

k. **Control Interno:** Proceso compuesto por una serie de acciones y procedimientos concatenados que se realizan durante el desempeño de las funciones del INSTITUTO, que tiene como fin proporcionar un grado de seguridad razonable en la consecución de sus objetivos, así como la salvaguarda de los recursos públicos y la prevención de actos contrarios a la integridad del INSTITUTO o de corrupción.

l. **Control Preventivo:** Mecanismo de control establecido que opera anticipadamente a eventos no deseados, como errores, omisiones o desviaciones en los procesos, que vulneren los objetivos.

m. **Componentes del Proceso:** Todas aquellas partes integrantes de un proceso y que contribuyen a su ejecución para el logro de su objetivo.

n. **Corrupción:** Se entiende como el abuso del poder público encomendado para el beneficio propio o de terceros.

o. **Debilidad (es) de control:** La insuficiencia, deficiencia o inexistencia de controles, cuyo nivel de riesgo puede ser bajo, medio o alto. Esta situación no se detecta en el curso normal de las funciones, por lo que su persistencia podría permitir que ocurran incumplimientos o irregularidades.

p. **Disposiciones:** Marco Normativo de Control Interno del Instituto Nacional Electoral.

q. **Economía:** Los términos y condiciones bajo los cuales se adquieren recursos, en cantidad y calidad requeridos y al menor costo posible para realizar una actividad determinada.

r. **Eficacia:** cumplimiento de metas y objetivos establecidos, en lugar, tiempo, cantidad y calidad, con los recursos disponibles.

s. **Eficiencia:** Logro de metas y objetivos programados, por medio del uso racional de recursos y medios disponibles a fin de obtener el mayor beneficio a cambio del menor costo posible.

t. **Elemento:** Parte constitutiva o integrante de algo.

u. **Elementos de control:** Los elementos asociados a las normas generales o componentes o normas generales de control interno, que contribuyen a cumplir con los principios de cada uno de ellos; estos elementos son de diversa índole como por ejemplo, el establecimiento de una línea funcional de autoridad, la definición precisa de funciones y responsabilidades en la cadena de mando, un sistema contable que proporciona información completa y precisa de las operaciones, un mecanismo de información para la administración en los diversos niveles de la institución y mecanismos específicos para prevenir y proteger a la institución contra fraudes o actos de corrupción, entre otros.

v. **Elemento (s) vulnerable (s):** Debilidades o problemas potenciales que en caso de presentarse pueden afectar el cumplimiento de los objetivos del proceso o los objetivos estratégicos institucionales.

w. **Enlace de control interno**: Persona designada por la o el Titular de la Unidad Responsable como contacto para control interno y

administración de riesgos.

x. **Evaluación del Sistema de Control Interno:** Proceso mediante el cual se determina el grado de eficacia y de eficiencia con que se cumplen las normas generales o componentes o normas generales de control interno, para garantizar el objetivo del control interno en sus respectivas categorías;

y. **Factor de Riesgo:** La circunstancia, causa o situación interna y/o externa que aumenta la probabilidad de que un riesgo se materialice;

z. **Firma electrónica avanzada**: El conjunto de datos y caracteres que permite la identificación de la o el firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa; ésta podrá ser emitida por el INE o por alguna Autoridad Certificadora externa con la que el INE haya firmado algún convenio.

aa. **Gestión de riesgos de corrupción:** Proceso desarrollado para contextualizar, identificar, analizar, evaluar, atender, monitorear y comunicar los riesgos que por acción u omisión, mediante el abuso del poder y/o el uso indebido de recursos y/o de información, empleo, cargo o comisión, pueden dañar los intereses del INSTITUTO, para la obtención de un beneficio particular o de terceros, incluye soborno, apropiación indebida u otras formas de desviación de recursos por un funcionario público, nepotismo, extorsión, tráfico de influencias, uso indebido de información privilegiada, entre otras prácticas, en aquellos procesos o temáticas relacionados con áreas financieras, presupuestales, de contratación, de información y documentación, investigación y sanción, trámites y/o servicios internos y externos.

bb. **Impacto o efecto:** Las consecuencias negativas que se generarían en el INSTITUTO, en el supuesto de materializarse un riesgo.

cc. **Integridad:** Se refiere al comportamiento de un individuo correcto, atento, probo y basado en valores éticos. Se reconoce como una cualidad que le da, a quien la posee, la autoridad para decidir y resolver por sí misma, cuestiones relacionadas con sus propias acciones.

dd. **Mandos medios:** Para efectos de las presentes Disposiciones serán las y los directores de área, subdirectores, jefes de departamento u homólogos adscritos a las Direcciones Ejecutivas y Unidades Técnicas del INSTITUTO. Para el caso de los Órganos Delegacionales serán las y los vocales secretarios; de Organización Electoral; Registro Federal de Electores; Capacitación Electoral y Educación Cívica de las Juntas Locales.

ee. **Mapa de riesgos:** La representación gráfica de los riesgos en donde se puede visualizar la probabilidad de ocurrencia y su impacto en forma clara y objetiva.

ff. **Matriz de Administración de Riesgos:** Documento que concentra los riesgos (listado), su periodicidad, grado de impacto y probabilidad de ocurrencia en un proceso, y ayuda a identificar las acciones necesarias para mitigar dichos riesgos.

gg. **Mecanismo:** El conjunto de elementos que apoyan a los procesos en el logro de sus objetivos.

hh. **Mejora continua:** El proceso de optimización y perfeccionamiento del Sistema de Control Interno; de la eficacia, eficiencia y economía de su gestión; y de la mitigación de riesgos, a través de su evaluación periódica.

ii. **Meta:** Es un propósito que se prevé alcanzar en un periodo determinado (generalmente proyectado en un ejercicio fiscal), el cual debe ser concreto, medible, alcanzable y articulado a uno o varios objetivos y proyectos estratégicos institucionales.

jj. **Normas generales de control interno:** Las cinco normas que integran el control interno (ambiente de control, administración de riesgos, actividades de control, información y comunicación; así como a la supervisión y mejora continua), referidas también, como los cinco componentes o normas generales en el modelo COSO.

kk. **Objetivo estratégico:** Los objetivos incluidos en la planeación estratégica.

ll. **Principios de control interno o principios**: los 17 principios asociados a las Normas Generales de Control Interno o cinco componentes o normas generales de control interno, establecidos en estas disposiciones.

mm. **Probabilidad de ocurrencia:** La ponderación de la estimación de que se materialice un riesgo, en un periodo determinado.

nn. **Proceso (s) de soporte:** Conjunto de actividades que interactúan para la gestión interna de la institución y que no contribuyen directamente con su razón de ser, ya que dan apoyo a los procesos sustantivos.

oo. **Proceso(s) sustantivo(s):** Conjunto de actividades que interactúan directamente con las funciones sustantivas de la institución, es decir, con el cumplimiento de su misión, objetivos y proyectos estratégicos institucionales y el cumplimiento de sus metas.

pp. **Proceso(s) Estratégico(s**): Son procesos destinados a definir y controlar las metas de la Institución, sus políticas y estrategias. Están en relación muy directa con la misión/visión de la Institución.

qq. **Proyecto Específico:** Conjunto de actividades y recursos para el logro de objetivos específicos, únicos e irrepetibles, en un tiempo determinado.

rr. **Proyecto Estratégico Institucional**: Iniciativas de primer nivel que apoyan el cumplimiento de la misión, la visión, y de los objetivos estratégicos institucionales, y se traducen en un elemento importante del presupuesto del Instituto, facilitando la toma de decisiones en la asignación de recursos, la comunicación, la transparencia y la rendición de cuentas.

ss. **Programa de Trabajo de Administración de Riesgos:** Documento que incorpora las acciones de control comprometidas a implementar en determinado plazo para la administración de los riesgos, bajo un enfoque de procesos, con el objeto de gestionarlos para garantizar de manera razonable el logro de los objetivos estratégicos institucionales.

tt. **Programa de Trabajo de Control Interno:** Documento que incorpora las acciones de control comprometidas a ejecutar en determinado plazo para la implementación o fortalecimiento de los elementos de control vinculados a los principios y a las normas generales de control interno establecidas en estas disposiciones.

uu. **Relevancia:** Se refiere al efecto sobre el logro de los objetivos institucionales y metas.

vv. **Rendición de cuentas**: Proceso mediante el cual el personal del INSTITUTO o prestador de servicios está obligado a explicar e informar a la ciudadanía, de los logros alcanzados y de los recursos utilizados para alcanzar dichos logros.

ww. **Riesgo:** Posibilidad de que ocurra un acontecimiento o evento no deseado que impacte de forma negativa el logro de los objetivos institucionales.

xx. **Riesgo de corrupción:** La posibilidad de que, por acción u omisión, mediante el abuso del poder y/o el uso indebido de recursos y/o de información, empleo, cargo o comisión, se dañan los intereses de la institución, para la obtención de un beneficio particular o de terceros, incluye soborno, apropiación indebida u otras formas de desviación de recursos por un funcionario público, nepotismo, extorsión, tráfico de influencias, uso indebido de información privilegiada, entre otras prácticas.

yy. **Riesgo inherente:** Es el que enfrenta la institución cuando no cuenta con mecanismos de control establecidos, o estos no son suficientes, para responder al riesgo.

zz. **Riesgo materializado:** Es el que ha ocurrido o se ha presentado durante la operación de un proceso, dejando de ser una posibilidad, para convertirse en un hecho.

aaa. **Riesgo residual:** Es el que permanece después de la respuesta al riesgo inherente; es decir, después de la aplicación de mecanismos de control.

bbb. **Seguridad razonable:** El escenario en el que la posibilidad de materialización del riesgo disminuye, y la posibilidad de lograr los objetivos y proyectos estratégicos institucionales y el cumplimiento de sus metas se incrementa.

ccc. **Servidora o servidor público:** Toda persona que desempeñe un cargo o comisión de cualquier naturaleza en el INSTITUTO, quienes serán responsables por los actos u omisiones en que incurran en el desempeño de sus respectivas funciones.

ddd. **Sistema de Control Interno Institucional (SCII):** El conjunto de procesos, mecanismos y elementos organizados y relacionados que interactúan entre sí, y que se aplican de manera específica por el INSTITUTO a nivel de planeación, organización, ejecución, dirección, información y seguimiento de sus procesos, para dar certidumbre a la toma de decisiones y conducirla con una seguridad razonable al logro de los objetivos y proyectos estratégicos institucionales y el cumplimiento de sus metas en un ambiente ético e íntegro, de calidad,

de mejora continua y eficiencia.

eee. **Sistema de información:** El conjunto de procedimientos ordenados que, al ser ejecutados, proporcionan información para apoyar la toma de decisiones y el control de la Institución.

fff) **Titular(es):** Para efectos de las presentes Disposiciones serán todas y todos los Titulares de las Direcciones Ejecutivas y Unidades Técnicas. Para el caso de los Órganos Delegacionales serán las y los Vocales Ejecutivos de las Juntas Locales.

ggg) **Unidades Responsables o UR:** Son las áreas del INSTITUTO Nacional Electoral, identificadas como Direcciones Ejecutivas, Unidades Técnicas y Órganos Delegacionales.

## De las y los sujetos obligados

**Artículo 3.** Estas Disposiciones son de observancia obligatoria y general para todo el personal del INSTITUTO y prestadores de servicios en cuanto a lo siguiente:

I. Las y los Titulares de las UR y órganos delegacionales, así como el personal del INSTITUTO y prestadores de servicios que participa en los procesos institucionales.

II. La DEA, en la coordinación de la implementación, seguimiento y supervisión del control interno a nivel institucional.

III. El CPI, en cuanto al seguimiento y conocimiento de los avances en la implementación del control interno.

IV. La SE y la JGE en cuanto al impulso y la supervisión.

V. Presidencia del Consejo para su impulso, conocimiento y seguimiento.

VI. El OIC en su acompañamiento, en los términos previstos en el presente MNCI.

## De la interpretación

**Artículo 4**. La interpretación para efectos administrativos de las presentes disposiciones, así como la resolución de los casos no previstos en las mismas, corresponderá a la DEA.

### De la revisión y actualización

**Artículo 5**. Las presentes disposiciones deberán revisarse y actualizarse en los casos necesarios, a propuesta de la DEA con la opinión del CPI. Las propuestas de modificación que en su caso se realicen deberán someterse a consideración de la JGE para su aprobación.

El OIC, conforme a sus atribuciones, acompañará a la DEA en las revisiones de las propuestas de modificación, para tal efecto, deberá emitir sus comentarios y/o sugerencias con el propósito de fortalecer y promover el cumplimiento del presente Marco Normativo, para mantener un proceso de mejora continua dentro del SCII. Las propuestas se revisarán con la Dirección Jurídica y la Coordinación de Planeación Institucional a fin de fortalecer la propuesta, previo a someter a consideración del CPI y posteriormente de la JGE.

### Del uso de la firma electrónica avanzada

**Artículo 6.** Los documentos que deriven de la aplicación de las presentes Disposiciones y que requieran ser firmados por la Administración, Responsables de los Riesgos de los Procesos, Analistas de Riesgos, Responsables de las Acciones de Control, por la DEA o cualquier servidora o servidor público designado podrán utilizar de manera preferente la Firma Electrónica Avanzada utilizando el sistema que la DEA implemente para tales efectos.

# Capítulo II. SCII

## Sección I. Estructura del SCII

### Del enfoque

**Artículo 7.** Las presentes disposiciones se deberán aplicar con la finalidad de implementar y mejorar continuamente el SCII.

Inicialmente, derivado del levantamiento, modelado, análisis y mapeo de los

procesos, se identificarán los riesgos y sus controles existentes, debiendo de ser estos validados en función de sus atributos -de acuerdo a las fases de la metodología de administración de riesgos establecidas en el artículo 21 de las presentes disposiciones-, a fin de determinar los procesos en los que se implementará y fortalecerá el SCII.

En razón de lo anterior, las acciones de control previamente definidas, para los procesos modelados a través del componente de Modernización Administrativa, serán reevaluadas, conforme a lo dispuesto por el componente de Control Interno, ambos del Modelo de Planeación Institucional, en aquellos procesos que resulten pertinentes de acuerdo a la programación prevista en las acciones de control, a fin de mantener una valoración constante de la implementación y del fortalecimiento del control interno en estos, para asegurar razonablemente el logro de los objetivos estratégicos institucionales, considerando que el ciclo de control interno es dinámico e iterativo.

## De los objetivos del Control Interno

**Artículo 8**. El control interno tiene como objetivo proporcionar una seguridad razonable en el logro de los objetivos y proyectos estratégicos institucionales y el cumplimiento de sus metas dentro de las siguientes categorías:

I. Operación: Eficacia, eficiencia y economía de las operaciones;

II. Información: Confiabilidad, veracidad y oportunidad de la información financiera, presupuestaria y de operación;

III. Cumplimiento: Observancia del marco legal, reglamentario, normativo y administrativo aplicable al INSTITUTO, y

IV. Salvaguarda: prevención de actos de corrupción y la protección de recursos institucionales contra pérdidas, manteniéndolos en condiciones de integridad, transparencia, conservación y disponibilidad, para su utilización en los fines a que están asignados y autorizados.

## De las Normas generales, principios y elementos de control interno

**Artículo 9.** Para apoyar el logro de los objetivos vinculados con los procesos, se deberán observar los componentes o normas generales de control interno con sus principios y elementos de control siguientes:

I. Norma General Primera: Ambiente de Control.

El ambiente de control tiene como finalidad el que exista un entorno y clima organizacional de respeto, que se den las condiciones para promover la sensibilización con respecto a la igualdad de género, la integridad y el compromiso. Asimismo, se deberá contar con las disposiciones generales para fomentar la cultura de control interno; documentos rectores de la planeación institucional; mecanismos de supervisión en los niveles de la planeación institucional y el SCII.

El INSTITUTO deberá contar con una estructura organizacional, un reglamento interior, manuales de organización y de procedimientos autorizados, actualizados y que sean de conocimiento del personal que lo integra. Asimismo, se deberán instaurar procedimientos de administración de recursos humanos que permitan establecer y fortalecer el programa del servicio profesional de carrera con mecanismos de integridad bajo principios de igualdad de oportunidades, mérito, no discriminación, conocimientos necesarios, profesionalización continua, evaluación permanente, transparencia de los procedimientos, rendición de cuentas, paridad e igualdad de género, cultura democrática, ambiente laboral libre de violencia y respeto a los derechos humanos, eficiencia, consistencia estructural, capacidad funcional y ética, para garantizar la permanencia de los mejores elementos de la organización; todo ello, en congruencia con los objetivos estratégicos institucionales, la misión, la visión, los principios rectores, el Código de Ética, el Código de Conducta, el marco jurídico y el Plan Estratégico del Instituto Nacional Electoral vigente, lo que contribuirá a una mayor transparencia y rendición de cuentas.

Para la implementación del ambiente de control se deberán considerar los siguientes principios:

**Principio 1. Manifestar actitud de respaldo y compromiso**. – La Presidencia del CG, la JGE, la SE y la Administración en el ámbito de sus atribuciones deberán tener una actitud de compromiso, en lo general con la integridad, los valores éticos, las normas de conducta, así como la prevención de irregularidades administrativas y actos contrarios a la integridad:

1.1 Actitudes de Respaldo.

La Presidencia del CG, la JGE, la SE y la Administración en el ámbito de sus atribuciones deberán demostrar la importancia de la integridad, los valores éticos y las normas de conducta en sus directrices, actitudes y comportamiento.

La Presidencia del CG, la JGE, la SE y la Administración en el ámbito de sus atribuciones deberán guiar, a través del ejemplo, los valores, la filosofía organizacional y el estilo de gestión de la Institución.

Las directrices, actitudes y conductas de la Presidencia del CG, la JGE, la SE y la Administración deberán reflejar la integridad, los valores éticos y las normas de conducta que se esperan tener de todas y todos los servidores públicos de la institución.

1.2 Normas de Conducta.

El INSTITUTO cuenta con principios y valores establecidos en un Código de Ética de la Función Pública Electoral, emitido por el OIC y con estándares de comportamiento contenidos en un Código de Conducta, emitido por la JGE, a fin de guiar a las personas servidoras públicas en el desempeño de sus funciones. Ambos códigos deberán ser difundidos y verificar su cumplimiento.

El Instituto con respecto a su autonomía constitucional cuenta con un Comité de Ética que funge como órgano de consulta, recibe, da seguimiento y, en su

caso, emite recomendaciones derivado de las denuncias por posibles actos contrarios a la ética y conducta institucional, de conformidad con los Lineamientos que regulan el Comité de Ética del Instituto, el Manual de desahogo de Consultas y Denuncias ante el Comité de Ética del Instituto Nacional Electoral y demás normatividad aplicable.

### 1.3 Apego a las Normas de Conducta.

Las y los servidores públicos deberán realizar una declaración de conocimiento y aceptación de lo dispuesto en los Códigos de Ética y de Conducta, así como una declaración anual de cumplimiento de estos, conforme al mecanismo que determine el OIC.

El Comité de Ética deberá formalizar un mecanismo de capacitación y de evaluación del conocimiento, comprensión y cumplimiento del Código de Ética y del Código de Conducta del INE. Conocerá las evaluaciones del conocimiento y comprensión de lo establecido en ambos códigos y determinará las áreas de oportunidad y las acciones para mejorar continuamente su índice de cumplimiento.

### 1.4 Programa, política o lineamiento de Promoción de la Integridad y Prevención de la Corrupción.

La DEA, con el acompañamiento del OIC, deberá articular un programa permanente de promoción de la integridad y prevención de la corrupción, que considere como mínimo lo siguiente:

I. La capacitación continua de las y los servidores públicos en materia de control interno, administración de riesgos e integridad y
II. La difusión de las presentes disposiciones, así como de los Códigos de Ética y de Conducta entre el personal del Instituto, estos últimos en coordinación con el OIC.

Al respecto, el Comité de Ética propondrá estrategias para la difusión, promoción seguimiento y fortalecimiento de los principios, valores, reglas de integridad y conductas de dichos códigos.

La DEA deberá desarrollar y dar a conocer el programa de promoción de la integridad y prevención de la corrupción entre las y los Titulares de las UR, mismos que deberán dar las facilidades necesarias para garantizar su cumplimiento.

El establecimiento, difusión y operación de una línea de ética o mecanismo de denuncia de hechos contrarios a la ética, normas de conducta e integridad que puedan presentarse en el INSTITUTO estará a cargo del Comité de Ética, de conformidad con los Lineamientos que regulan el Comité de Ética del Instituto, el Manual de desahogo de Consultas y Denuncias ante el Comité de Ética del Instituto Nacional Electoral y demás normatividad aplicable.

1.5 Cumplimiento, Supervisión y Actualización Continua del Programa de Promoción de la Integridad y Prevención de la Corrupción.

La DEA, con el apoyo del Comité de Ética, deberá asegurar una supervisión continua sobre la aplicación oportuna, efectiva y apropiada del programa de promoción de la integridad, medir si es suficiente y eficaz y con base en los resultados de las evaluaciones internas y externas a que esté sujeto, proponer e instrumentar las mejoras necesarias para corregir sus deficiencias.

**Principio 2. Ejercer la responsabilidad de vigilancia**. – La Presidencia del CG, la JGE, la SE, el CPI, la DEA y la Administración en el ámbito de sus atribuciones, deberán demostrar imparcialidad y objetividad al desarrollar la supervisión en la implementación y el fortalecimiento del SCII.

2.1 Vigilancia General del Control Interno.

La Presidencia del CG, la JGE, la SE, el CPI, la DEA y la Administración en el ámbito de sus atribuciones deberán vigilar, de manera general, el diseño,

implementación y operación del control interno realizado por la Administración, así como promover la mejora de los procesos de prevención, denuncia y detección de faltas administrativas y hechos de corrupción. Las responsabilidades, entre otras, son las siguientes:

- **Ambiente de Control**. Establecer y promover la integridad, los valores éticos y las normas de conducta, así como la estructura de vigilancia, desarrollar expectativas de competencia profesional y mantener la rendición de cuentas.
- **Administración de Riesgos.** Vigilar los resultados de la evaluación de los riesgos que pudieran amenazar el logro de las metas y objetivos institucionales, incluyendo el impacto potencial de los cambios normativos y de organización que sean significativos, la corrupción y la omisión en el establecimiento de controles responsabilidad de las y los servidores públicos.
- **Actividades de Control.** Vigilar a la Administración en el desarrollo y ejecución de las actividades de control.
- **Información y Comunicación.** Analizar y discutir la información relativa al avance en el cumplimiento de metas y objetivos institucionales.
- **Supervisión.** Examinar la naturaleza y alcance de las actividades de supervisión de la Administración, así como analizar los resultados de las evaluaciones realizadas por ésta y las acciones correctivas implementadas para remediar las deficiencias identificadas.

**Principio 3. Establecer la estructura, responsabilidad y autoridad. -** La SE y la Administración, con el apoyo de la DEA, establecerá la estructura, líneas de reporte, los niveles de autoridad y de responsabilidades para el logro de los objetivos institucionales y metas asociadas:

3.1 Estructura Organizacional.

La Administración en el ámbito de sus atribuciones y con base en lo establecido

en el Estatuto del Servicio Profesional Electoral y del Personal de la Rama Administrativa, en el Reglamento Interno del Instituto Nacional Electoral y en la normatividad aplicable deberá verificar:

- Que el Manual de Organización General sea acorde a la estructura organizacional vigente autorizada, a la estructura de políticas institucionales y a las atribuciones y responsabilidades establecidas en las leyes, reglamentos y demás ordenamientos aplicables.
- Que los manuales de organización general, específicos y de procesos y procedimientos, así como sus modificaciones, están actualizados, autorizados y publicados.
- Que los perfiles y descripciones de puestos están definidos, alineados, actualizados y autorizados.

### 3.2 Asignación de Responsabilidad y Delegación de Autoridad.

Para alcanzar los Objetivos Estratégicos Institucionales, la Presidencia del CG y la SE en el ámbito de sus competencias deberá asignar responsabilidad y delegar autoridad para el cumplimiento de las presentes disposiciones, a los puestos clave a lo largo del INSTITUTO.

La Administración en el ámbito de sus atribuciones y de acuerdo la normatividad aplicable, deberá definir en los manuales de organización general y específicos, así como de procesos y procedimientos, los niveles de autoridad y responsabilidad, la segregación y delegación de funciones, evitando que dos o más de éstas se concentren en una misma persona.

### 3.3 Documentación y Formalización del Control Interno.

La Administración en el ámbito de sus atribuciones deberá desarrollar y actualizar la documentación y formalización de cada uno de los controles implementados en el marco de las presentes Disposiciones.

**Principio 4. Demostrar compromiso con la competencia profesional.-** La Administración en el ámbito de sus atribuciones será la responsable de

seguir los procedimientos establecidos en la normatividad vigente para contratar, capacitar, buscar la permanencia y pertinencia de los profesionales competentes en cada puesto y área de trabajo.

4.1 Expectativas de Competencia Profesional.

La Administración en el ámbito de sus atribuciones deberá establecer expectativas de competencia profesional sobre los puestos clave y los demás cargos institucionales para ayudar al INSTITUTO a lograr sus objetivos.

La Administración en el ámbito de sus atribuciones deberá contemplar los estándares de conducta, las responsabilidades asignadas y la autoridad delegada al establecer expectativas de competencia profesional para los puestos directivos, de gestión y de operación.

4.2 Atracción, Desarrollo y Retención de Profesionales.

La Administración en el ámbito de sus atribuciones deberá captar, capacitar de forma continua y retener profesionales competentes para lograr los objetivos institucionales y metas. Por lo tanto, deberá seleccionar y contratar de forma eficaz; establecer programas de capacitación continua para lograr la profesionalización del capital humano y establecer programas de evaluación del desempeño, motivación y gestión participativa en la toma de decisiones.

**Principio 5. Establecer la estructura para el reforzamiento de la rendición de cuentas. -** La Administración en el ámbito de sus atribuciones, en coordinación con la DEA, deberá evaluar el desempeño del control interno en la institución.

5.1 Establecimiento de la Estructura para Responsabilizar al Personal por sus Obligaciones de Control Interno.

La Administración en el ámbito de sus atribuciones deberá establecer y mantener una estructura que permita, de manera clara y sencilla, responsabilizar al personal por sus funciones y por sus obligaciones específicas

en materia de control interno, lo cual forma parte de la obligación de rendición de cuentas institucional.

II. Norma General Segunda. - Administración de Riesgos.

Es el proceso dinámico desarrollado para identificar, analizar, evaluar, responder, supervisar y comunicar los riesgos, incluidos los de corrupción, inherentes o asociados a los procesos (sustantivos y de soporte) por los cuales se logran los objetivos institucionales y sus metas, mediante el análisis de los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias y acciones que permitan mitigarlos y asegurar el logro de los objetivos estratégicos institucionales de una manera razonable.

Para la aplicación de esta norma, la JGE, el CPI y la Administración en el ámbito de sus atribuciones y bajo la coordinación de la DEA, deberán vigilar la implementación y operación en conjunto y de manera sistémica de las acciones que erradiquen o mitiguen áreas de riesgo de los siguientes principios y elementos de control.

**Principio 6. Definir Objetivos Institucionales y Metas. -** El INSTITUTO deberá definir claramente sus objetivos a través de un plan estratégico que, de manera coherente y ordenada, se asocie a su mandato legal.

6.1 Planeación Institucional.

La Administración con el apoyo de la DEA, la Coordinación de Planeación y del CPI en el ámbito de sus atribuciones, deberá efectuar la planeación institucional a través de procesos sistemáticos, con mecanismos de control para el seguimiento y evaluación, que proporcionen periódicamente información relevante y confiable para la toma oportuna de decisiones, con especial atención en la planeación, programación, presupuestación y ejercicio del gasto con un enfoque de máxima publicidad.

6.2 Definición de Objetivos.

El INSTITUTO deberá definir en la planeación institucional y de forma precisa, los objetivos institucionales, a los cuales se deberá implementar el proceso de administración de riesgos. La misión, visión, objetivos y proyectos estratégicos institucionales y la definición de metas deberán estar alineados a la planeación institucional y ser difundidos para el conocimiento de las y los funcionarios.

**Principio 7. Identificar, analizar y responder a los riesgos.** - La Administración en el ámbito de sus atribuciones en coordinación con la DEA, deberá identificar los riesgos en sus procesos (sustantivos y de soporte), analizar su relevancia y diseñar acciones suficientes para responder a éstos y asegurar de manera razonable el logro de los Objetivos Institucionales, todo ello en cumplimiento de las presentes Disposiciones.

Los riesgos deberán ser comunicados al personal de la institución, mediante las líneas de reporte que la DEA establezca para tal fin.

7.1 Identificación de Riesgos.

La Administración con el apoyo de la DEA y en el ámbito de sus atribuciones, deberá identificar los riesgos en los procesos que se definan para analizarlos, diseñar respuestas y atenderlos de acuerdo con los requerimientos y expectativas de la planeación estratégica, y a las disposiciones jurídicas y normativas aplicables.

Para identificar los riesgos, la Administración en el ámbito de sus atribuciones deberá considerar los tipos de eventos que pudieran impactar o hayan impactado de forma negativa la consecución de los Objetivos Estratégicos Institucionales y sus metas; siendo estos, tanto riesgos inherentes como residuales.

La Administración en el ámbito de sus atribuciones deberá considerar todas las interacciones significativas dentro del INSTITUTO y con actores externos, así como los cambios y otros factores tanto internos como externos, que le den un

contexto integral para identificar los riesgos.

7.2 Análisis de Riesgos.

La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá analizar los posibles riesgos que pudieran materializarse para estimar su relevancia, lo cual proveerá la base para implementar las acciones preventivas correspondientes. La relevancia de un riesgo se deberá estimar considerando la magnitud del impacto, la probabilidad de ocurrencia y la naturaleza del riesgo.

Los riesgos pueden ser analizados sobre bases individuales o agrupadas dentro de categorías de riesgos asociados, los cuales son analizados de manera colectiva. La Administración en el ámbito de sus atribuciones deberá considerar la correlación entre los distintos riesgos o grupos de riesgos al estimar su relevancia.

7.3 Respuesta a los Riesgos.

La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá diseñar respuestas a los posibles riesgos de tal modo que éstos se encuentren debidamente controlados para asegurar razonablemente el cumplimiento de los Objetivos Institucionales y de sus metas.

Con base en la clasificación del riesgo y sus factores, en el análisis de acuerdo con el tipo de riesgo, incluidos los de corrupción, en el nivel de exposición de los procesos, la Administración en el ámbito de sus atribuciones y bajo la coordinación de la DEA, determina la respuesta al riesgo debiendo integrar, bajo el enfoque de procesos, su Matriz y Mapa de Riesgos, así como de resultar necesario su PTAR, el cual proveerá una seguridad razonable de que la institución alcance sus objetivos, y de ser el caso, fortalecerá los elementos de control que establece el artículo 9 de las presentes disposiciones, a través de un PTCI.

La Administración en el ámbito de sus atribuciones deberá efectuar

evaluaciones periódicas de riesgos, con el fin de asegurar la efectividad de las acciones de control propuestas para mitigarlos.

**Principio 8. Considerar el Riesgo de Corrupción.** - La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá considerar la posibilidad de ocurrencia de actos de corrupción, abuso, desperdicio y otras irregularidades relacionadas con la eficaz salvaguarda de los recursos públicos a través de la identificación, análisis y establecimiento de estrategias de respuesta a los riesgos asociados, principalmente a los procesos financieros, presupuestales, de contratación, de información y documentación, así como de trámites que establecen ciudadanos y empresas con el Instituto, y servicios internos y externos.

8.1 Tipos de Corrupción.

La Administración con el apoyo de la DEA y en el ámbito de sus atribuciones, deberá considerar los tipos de corrupción señalados en la Ley General de Responsabilidades Administrativas[1] y en el Código Penal Federal vigentes[2], que pueden ocurrir en los procesos (sustantivos y de soporte) del INSTITUTO. Entre los tipos de corrupción más comunes, que la citada ley de responsabilidades regula, se encuentran:

- Cohecho.
- Peculado.
- Desvío de recursos públicos.
- Utilización indebida de información.
- Abuso de funciones.
- Actuación bajo Conflicto de Interés.
- Contratación indebida.
- Enriquecimiento oculto u ocultamiento de Conflicto de Interés.
- Tráfico de influencias.

[1] http://www.diputados.gob.mx/LeyesBiblio/pdf/LGRA_130420.pdf
[2] http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_Penal_Federal.pdf

- Encubrimiento.
- Desacato.

8.2 Factores de Riesgo de Corrupción.

La Administración con el apoyo de la DEA y en el ámbito de sus atribuciones, deberá considerar los factores de riesgos de corrupción, abuso, desperdicio y otras irregularidades. Estos factores no implican necesariamente la existencia de un acto corrupto, pero están usualmente presentes cuando éstos ocurren.

La Administración en el ámbito de sus atribuciones al considerar el abuso, desperdicio y otras irregularidades como factores de riesgos de corrupción, deberá tomar en cuenta que cuando uno o más de estos estén presentes, podría indicar un posible riesgo de corrupción y que puede incrementarse la posibilidad cuando los tres factores estén presentes. También se deberá utilizar la información provista por partes internas y externas para identificar los riesgos de corrupción.

8.3 Respuesta a los Riesgos de Corrupción.

La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá analizar y responder a los riesgos de corrupción a fin de que sean efectivamente mitigados. Estos riesgos deberán ser analizados por su relevancia, tanto individual como en su conjunto, conforme lo establecido en las presentes Disposiciones.

La Administración en el ámbito de sus atribuciones deberá responder a los riesgos de corrupción, mediante el mismo proceso de respuesta general y acciones específicas para gestionar todos los riesgos institucionales analizados. A partir de ello, para el caso que nos ocupa, se definirán controles anticorrupción.

**Principio 9. Identificar, analizar y responder al cambio. -** La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá identificar, analizar y responder a los cambios internos y

externos que puedan impactar en el control interno, ya que pueden generar que los controles se vuelvan ineficaces o insuficientes para alcanzar los Objetivos Institucionales y el cumplimiento de las metas, así también podrían provocar la creación de nuevos riesgos.

Los cambios internos y externos podrían afectar a los procesos, procedimientos y actividades institucionales, a la función de supervisión, a la estructura organizacional, al personal y al uso de las tecnologías de la información y la comunicación. Los cambios tanto internos como externos que incrementen la probabilidad de impactar al ambiente de control interno deberán ser comunicados a las y los funcionarios involucrados en la gestión y toma de decisiones de la institución mediante las líneas de reporte y autoridad establecidas.

### 9.1 Identificación del Cambio.

En la administración de riesgos la Administración, bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá identificar cambios que puedan impactar significativamente al control interno. La identificación, análisis y respuesta al cambio es parte del proceso regular de la administración de riesgos.

La Administración en el ámbito de sus atribuciones deberá prevenir y planear acciones ante cambios significativos en las condiciones internas (modificaciones a los procesos, procedimientos o actividades institucionales, a la función de supervisión, a la estructura organizacional, al personal y a las tecnologías de la información y comunicación), así como en las condiciones externas (cambios en los entornos gubernamentales, económicos, tecnológicos, legales, regulatorios y físicos).

### 9.2 Análisis y Respuesta al Cambio.

La Administración, bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá analizar y responder a los cambios identificados y a los

riesgos asociados con éstos, con el propósito de mantener un control interno adecuado.

Las condiciones cambiantes usualmente generan nuevos riesgos o cambios a los riesgos existentes, los cuales deberán ser evaluados para identificar, analizar y responder a cualquiera de éstos.

III. Norma General Tercera. - Actividades de Control.

Son las políticas, procedimientos, normatividad interna u otros mecanismos de control, prioritariamente de los procesos, así como en el entorno tecnológico que da soporte a la operación.

**Principio 10. Diseñar actividades de control**. - La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá diseñar, actualizar y garantizar la suficiencia e idoneidad de las actividades de control establecidas para lograr los Objetivos Institucionales definidos en la planeación institucional y el cumplimiento de las Metas. En este sentido, la Administración es responsable de que existan controles apropiados para hacer frente a los riesgos que se encuentran presentes en los procesos institucionales, incluyendo los riesgos de corrupción.

10.1 Respuesta a los Riesgos de los Objetivos Institucionales y Metas.

La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá diseñar actividades de control (políticas, procedimientos, técnicas, sistemas y mecanismos) en respuesta a los riesgos asociados con los Objetivos Institucionales y el cumplimiento de las metas, a fin de alcanzar un control interno eficaz.

10.2 Actividades de Control.

Las actividades de control pueden ser preventivas, detectivas o correctivas. La primera se dirige de manera anticipada, a fin de evitar que la institución falle en lograr un objetivo o para prevenir que un riesgo se materialice; la segunda

se establece en el momento que se detecta una falla en los controles o en el momento que se identifique el incremento de la probabilidad de que un riesgo no previsto se origine y la tercera corrige una falla después de que esta se presentó.

La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá evaluar el propósito de las actividades de control, así como el efecto que una deficiencia tiene en el logro de los Objetivos Institucionales y el cumplimiento de metas.

Las actividades de control deberán implementarse ya sea de forma automatizada o manual, considerando que las automatizadas tienden a ser más confiables, ya que son menos susceptibles a errores humanos y suelen ser más eficientes.

Los Comités Institucionales permanentes y temporales deberán funcionar en los términos de sus respectivas reglas de operación, lineamientos y la normatividad que en cada caso resulte aplicable.

El INSTITUTO deberá establecer y operar los instrumentos y mecanismos, para medir y/o analizar los avances, resultados y variaciones en el cumplimiento de objetivos y metas, a través del Sistema de Indicadores y Metas Institucionales.

La DEA deberá clasificar la información del Sistema Integral de Seguimiento de Auditorías (SISA) para identificar las recurrencias en las observaciones emitidas en los resultados de las auditorías realizadas por las diversas instancias de fiscalización, a efecto de comunicarlas a la Administración en el ámbito de sus atribuciones, con la finalidad de que identifiquen su causa raíz y se abata su recurrencia.

La DEA, con apoyo de la Coordinación de Planeación y el CPI, en el ámbito de sus atribuciones, deberá establecer un mecanismo de planeación, programación y presupuestación de cada ejercicio fiscal para la integración del anteproyecto de presupuesto del año siguiente.

10.3 Actividades de Control en varios niveles.

La Administración bajo la coordinación de la DEA y en el ámbito de sus atribuciones, deberá diseñar actividades de control para:

- Cada nivel de la estructura organizacional, según corresponda.
- Las distintas actividades de autocontrol que se realizan en el ámbito de competencia, entre otras, registros, autorizaciones, verificaciones, conciliaciones, bitácoras de control, revisiones, resguardo de archivos, alertas y bloqueo de sistemas y distribución de funciones.

La administración, operación y gestión de recursos humanos, materiales, financieros y tecnológicos, deberán estar registradas y soportadas con la documentación organizada y resguardada para su consulta, y en cumplimiento a las leyes que le apliquen.

La Administración en el ámbito de sus atribuciones deberá establecer los espacios y medios necesarios para asegurar y salvaguardar los bienes, incluido el acceso restringido al efectivo, títulos de valor u otros equivalentes, inventarios, mobiliario y equipo u otros que pueden ser vulnerables al riesgo de pérdida, al uso no autorizado, actos de corrupción, errores, malversación de recursos o cambios no autorizados.

La administración concentrará la información de contrataciones públicas tanto de órganos centrales como de órganos desconcentrados mediante un mecanismo de control que permita acceder a información relevante, oportuna y confiable en tiempo real sobre la situación que guarda cada procedimiento de contratación. Los órganos desconcentrados deberán reportar esa información que para tal efecto se requiera conforme al mecanismo y las modalidades que la DEA determine, con el auxilio de las áreas competentes del Instituto.

10.4 Segregación de Funciones.

La Administración con el apoyo de la DEA y en el ámbito de sus atribuciones, deberá considerar la delimitación de funciones para garantizar que un/a funcionario/a no sea juez y parte en la ejecución de un procedimiento determinado, a partir del diseño de actividades de control para que las funciones incompatibles sean segregadas y, cuando dicha segregación no sea práctica, se deberán diseñar actividades de control alternativas para enfrentar los posibles riesgos asociados.

**Principio 11. Seleccionar y desarrollar actividades de control basadas en las TIC´s.-** La Administración con apoyo de la UTSI en el ámbito de sus atribuciones, deberá desarrollar actividades de control que contribuyan a dar respuesta y reducir los riesgos identificados, apoyadas de las tecnologías de la información y comunicaciones para el logro de objetivos y proyectos estratégicos institucionales y el cumplimiento de sus respectivas metas.

Para la implementación de los mecanismos necesarios en materia de TIC´s, la Administración en el ámbito de sus atribuciones, deberá considerar la normatividad aplicable, el Manual del Sistema de Gestión de Tecnologías de la Información y Comunicaciones (SIGETIC) y lo que determine la UTSI.

11.1 Diseño de la Infraestructura de las TIC's.

La Administración en el ámbito de sus atribuciones, con apoyo de la UTSI deberá diseñar las actividades de control sobre la infraestructura de las TIC's para soportar la integridad, exactitud y validez del procesamiento de la información mediante el uso de TIC's.

11.2 Diseño de la Seguridad de la Información.

Para el diseño de la seguridad de la información se deberá seguir el procedimiento establecido en el SIGETIC referente a la administración de la seguridad de la información.

La gestión de la seguridad deberá incluir los procesos de información y las actividades de control relacionadas con los permisos de acceso a las TIC's, incluyendo quién tiene la capacidad de ejecutar transacciones. La gestión de la seguridad deberá incluir los permisos de acceso a través de varios niveles de datos, el sistema operativo (software del sistema), la red de comunicación, aplicaciones y segmentos físicos, entre otros. La Administración con apoyo de la UTSI en el ámbito de sus atribuciones, deberá diseñar las actividades de control sobre permisos para proteger a la institución del acceso inapropiado y el uso no autorizado del sistema.

La Administración con apoyo de la UTSI en el ámbito de sus atribuciones, deberá evaluar las amenazas de seguridad a las TIC's tanto de fuentes internas como externas.

La Administración en el ámbito de sus atribuciones y con el apoyo de la UTSI deberá diseñar actividades de control para limitar el acceso de las y los usuarios a las TIC's a través de controles como la asignación de claves de acceso y dispositivos de seguridad para autorización de usuarios.

La Administración en el ámbito de sus atribuciones, con el apoyo de la UTSI deberán determinar qué sistemas se requieren para establecer un plan de contingencias y de recuperación de desastres que dé continuidad a la operación de las TIC y de la Institución, centrándose en los procesos vinculados a la consecución de Objetivos Institucionales y el cumplimiento de metas.

La Administración en el ámbito de sus atribuciones y con el apoyo de la UTSI deberán establecer los procedimientos de respaldo y recuperación de información, datos, imágenes, voz y video, en servidores y centros de información, y programas de trabajo de los operadores de dichos centros.

11.3 Diseño de la Adquisición, Desarrollo y Mantenimiento de las TIC's.

La Administración en el ámbito de sus atribuciones con el apoyo de la UTSI deberá seguir los procedimientos establecidos en el SIGETIC para la

adquisición, desarrollo y mantenimiento de TIC´s.

La contratación de servicios tercerizados para el desarrollo de las TIC's es una alternativa de solución, por lo que la Administración con el apoyo de la UTSI en el ámbito de sus atribuciones, deberá evaluar los riesgos que su utilización podrían representar para la integridad, exactitud y validez de la información institucional.

La Administración en el ámbito de sus atribuciones con el apoyo de la UTSI deberán desarrollar los sistemas de información del INSTITUTO de manera tal que se cumplan los Objetivos Institucionales y Metas y se responda a los riesgos asociados a las TIC´s.

11.4 Operación del Comité de Tecnologías de la Información y Comunicación

La UTSI deberá liderar el Comité de Tecnologías de la Información y Comunicaciones con base en sus atribuciones y medir objetivamente la actuación de este.

**Principio 12. Implementar Actividades de Control. -** La Administración en el ámbito de sus atribuciones deberá establecer políticas y procedimientos que regulen su operación, los cuales deberán estar documentados y formalmente establecidos.

12.1 Documentación y Formalización de Responsabilidades a través de Políticas.

La Administración con el apoyo de la DEA en el ámbito de sus atribuciones, deberá documentar a través de políticas, manuales, lineamientos y otros documentos de naturaleza similar las responsabilidades de control interno en el INSTITUTO.

La Administración bajo la coordinación de la DEA en el ámbito de sus atribuciones, deberá comunicar al personal las políticas y procedimientos para que éste pueda implementar las actividades de control respecto de las

responsabilidades que tiene asignadas.

12.2 Revisiones Periódicas a las Actividades de Control.

La DEA deberá realizar periódicamente la evaluación y en su caso, la actualización, autorización y difusión, de las políticas, procedimientos y demás normativa de control interno conducente, que establezcan actividades de control para los procesos vinculados con la consecución de los Objetivos Institucionales y el cumplimiento de metas, así como para la mitigación de sus riesgos.

IV. Norma General Cuarta. - Información y Comunicación.

La información y comunicación son relevantes para el logro de los Objetivos Institucionales y el cumplimiento de metas. Al respecto, la Administración en el ámbito de sus atribuciones deberá establecer mecanismos que aseguren que la información relevante cuenta con los elementos de calidad suficientes y que los canales de comunicación tanto al interior como al exterior sean efectivos. Los sistemas de información y de comunicación deberán diseñarse e instrumentarse bajo los criterios que establezcan las UR competentes.

La Administración en el ámbito de sus atribuciones requiere tener acceso a la información relevante y a los mecanismos de comunicación confiables, con relación a los eventos internos y externos que pueden afectar al cumplimiento de los objetivos institucionales y las metas del INSTITUTO.

**Principio 13. Usar Información relevante y de calidad.** - Se deberán implementar los medios necesarios para que las áreas generen y utilicen información relevante y de calidad, que contribuyan al logro de las metas y los objetivos institucionales y den soporte al SCII.

La DEA deberá proveer de información periódica y relevante al CPI y la Administración de los avances en la atención de los acuerdos y compromisos que se determinen para el SCII, del estado que guarda el SCII y de las acciones de mejora y de control comprometidas en los PTCI y PTAR para su

fortalecimiento, a fin de impulsar su cumplimiento oportuno y obtener los resultados esperados.

La Administración en el ámbito de sus atribuciones y con el apoyo de la UTSI deberán diseñar sistemas de información apoyados en TIC que, en condiciones de integridad, veracidad, actualización, oportunidad, accesibilidad y seguridad, resuelven necesidades de información relevante a sus usuarios, para facilitar la toma de decisiones adecuada, su comunicación interna y externa, la transparencia y la rendición de cuentas.

**Principio 14. Comunicar Internamente. -** Se deberán establecer mecanismos de comunicación interna adecuados y de conformidad con las disposiciones aplicables, para difundir la información relevante y de calidad que den soporte al SCII.

14.1 Comunicación en toda la Institución.

La DEA y la Administración en el ámbito de sus atribuciones deberán comunicar información de calidad en toda la institución utilizando las líneas de reporte y autoridad establecidas.

El CG, la JGE, la SE y los comités y comisiones permanentes y temporales deberán recibir información de calidad que fluya ascendentemente, por las líneas de reporte, proveniente de la Administración en el ámbito de sus atribuciones. La información relacionada con el control interno deberá incluir asuntos importantes acerca de la adhesión, cambios o asuntos emergentes en materia de control interno, administración de riesgos e integridad.

Deberán existir y operar mecanismos para el registro, análisis y atención oportuna de quejas y denuncias en materia electoral, administrativa y ética, las dos últimas relacionadas con servidores públicos del Instituto. Las denuncias en materia de ética serán recibidas, desahogadas y resueltas por el Comité de Ética, de acuerdo con los Lineamientos que regulan el Comité de Ética del Instituto, el Manual de desahogo de Consultas y Denuncias ante el

Comité de Ética del Instituto Nacional Electoral y las demás normas aplicables.

La Dirección del Secretariado deberá llevar el registro de acuerdos y compromisos en materia de control interno, correspondientes a los acuerdos aprobados en las Sesiones de la JGE, así como de su seguimiento, a fin de que se cumplan en tiempo y forma.

**Principio 15.- Comunicar Externamente.** - Se deberán establecer mecanismos de comunicación externa apropiados y de conformidad con las disposiciones aplicables, para difundir la información relevante que dé soporte al SCII, a otras instituciones del estado mexicano, así como a las y los ciudadanos.

15.1 Comunicación con Partes Externas.

La Administración en el ámbito de sus atribuciones deberá comunicar información adecuada a entidades externas específicamente a instituciones públicas. De ese modo, las partes externas pueden contribuir a la consecución de los objetivos institucionales y cumplimiento de las metas institucionales y a enfrentar sus riesgos asociados.

El INSTITUTO deberá recibir información externa a través de las líneas de reporte establecidas y autorizadas.

V. Norma General Quinta. - Supervisión y Mejora Continua.

El SCII se supervisa y mejora periódicamente bajo la coordinación de la DEA mediante la autoevaluación y evaluaciones de control interno implementadas en los procesos (sustantivos y de soporte) y el cumplimiento en tiempo y forma de las acciones de mejora y de control comprometidas en los PTCI y PTAR.

**Principio 16. Realizar actividades de supervisión.-** La Administración en el ámbito de sus atribuciones y bajo la coordinación de la DEA, implementará actividades para la adecuada supervisión del control interno en los procesos

(sustantivos y de soporte) y la evaluación de sus resultados, por lo que deberá efectuar autoevaluaciones y considerar las auditorías y evaluaciones de las diferentes instancias fiscalizadoras y verificadoras, sobre el diseño y eficacia operativa del control interno, documentando sus resultados para identificar las deficiencias y cambios que son necesarios aplicar al control interno.

16.1 Supervisión del Control Interno.

La Administración en el ámbito de sus atribuciones deberá supervisar el control interno en los procesos (sustantivos y de soporte) a través de autoevaluaciones coordinadas por la DEA y evaluaciones externas.

El OIC y otras instancias de fiscalización conforme a sus atribuciones, si así lo determinaran conveniente, podrán realizar evaluaciones externas del SCII.

La Administración en el ámbito de sus atribuciones, bajo la coordinación de la DEA, puede incorporar evaluaciones externas para supervisar el diseño y la eficacia operativa del control interno en un momento determinado, o de una función o proceso específico.

La Administración con el apoyo de la DEA en el ámbito de sus atribuciones, conservará la responsabilidad de supervisar, si el control interno en los procesos (sustantivos y de soporte) es eficaz y apropiado, aun cuando los procesos sean asignados a servicios tercerizados.

16.2 Evaluación de Resultados.

La Administración, en coordinación con la DEA, en el ámbito de sus atribuciones deberán documentar los resultados de las autoevaluaciones en materia de control interno conforme las presentes disposiciones y de las evaluaciones externas para identificar debilidades de control y/o problemas de control interno, con la finalidad de incorporar acciones de control en el PTCI, las cuales previa ejecución de la metodología de administración de riesgos, pueden ser tomadas en cuenta para la generación del PTAR.

La Administración, en coordinación con la DEA, en el ámbito de sus atribuciones deberán identificar los cambios que han ocurrido en el control interno, derivados de modificaciones en el INSTITUTO y en su entorno; a su vez, el entorno también puede contribuir con la Administración en el ámbito de sus atribuciones a identificar problemas en el control interno como son las quejas o denuncias de la ciudadanía y el público en general, o de los cuerpos revisores o reguladores externos.

**Principio 17. Evaluar los problemas y corregir las deficiencias**. - La DEA en el ámbito de su competencia, deberá evaluar y comunicar las deficiencias de control interno en forma oportuna a las partes responsables de tomar acciones correctivas, preventivas o detectivas, así como a otras áreas involucradas.

17.1 Informe sobre Problemas.

El personal deberá identificar problemas de control interno en el desempeño de sus responsabilidades. Asimismo, deberá comunicarlas internamente al personal en la función clave responsable del control interno y, cuando sea necesario, a otro de un nivel superior a dicho responsable.

17.2 Evaluación de Problemas.

La Administración en el ámbito de sus atribuciones deberá evaluar y documentar los problemas y deficiencias detectadas en materia de control interno, ya sea en el PTCI o en el PTAR, en coordinación con la DEA, con la finalidad de determinar las acciones apropiadas para hacerles frente oportunamente.

Adicionalmente, puede asignar responsabilidades y delegar autoridad para corregir las deficiencias de control interno.

17.3 Acciones Preventivas, Detectivas y Correctivas

La Administración en el ámbito de sus atribuciones deberá formalizar ante la DEA, el establecimiento de un PTCI y un PTAR, según sea el caso, las acciones

a realizar para prevenir, detectar o corregir las deficiencias de control interno con la finalidad de establecer tiempos y responsables de llevarlas a acabo.

### De las etapas del SCII

**Artículo 10.** La implementación y fortalecimiento del SCII, para apoyar el logro de los objetivos de operación, de información y de cumplimiento, se deberá realizar conforme a lo previsto en los capítulos III, IV y V de las presentes disposiciones, que consideran lo siguiente:

A. Evaluación y fortalecimiento del SCII;
B. Administración de riesgos, y
C. Seguimiento

## Capítulo III. Evaluación y fortalecimiento del SCII

### Del objetivo

**Artículo 11.** La evaluación y fortalecimiento del control interno se encuentran relacionados con lo previsto en los artículos 7 y 8 de las presentes disposiciones y tienen como objetivos:

I. Determinar el estado que guarda el SCII, con base en la autoevaluación y evaluaciones de los avances en la implementación de los elementos de control interno vinculados a sus respectivos componentes o normas generales, y

II. Establecer e implementar las acciones de mejora para su fortalecimiento, a fin de que, en coexistencia con las etapas previstas en los capítulos IV y V de estas disposiciones, contribuya a que el INSTITUTO cuente con un SCII sólido que proporcione una seguridad razonable en el logro de los objetivos establecidos en la planeación institucional y permita prevenir los actos contrarios a la integridad o de corrupción.

## Sección I. De la autoevaluación y la evaluación anual del SCII

### De la autoevaluación anual

**Artículo 12.** El estado que guarda el SCII, con respecto a los procesos que se determine conforme al artículo 7, se deberá autoevaluar anualmente a más tardar el 30 de noviembre, mediante la aplicación de cuestionarios que consideran los componentes o normas generales, principios y elementos de control interno previstos en el artículo 9 de las presentes disposiciones; para la definición del contenido del cuestionario de autoevaluación anual se podrá solicitar la opinión del OIC con el propósito de fortalecerlo.

Para tal efecto, la DEA determinará el uso de alguna herramienta informática disponible en el INSTITUTO para su aplicación vía remota, así como el mecanismo de difusión y el periodo de aplicación de dicho cuestionario, de acuerdo con lo dispuesto en el presente artículo.

Derivado de la aplicación anual de los cuestionarios de autoevaluación de control interno se obtendrá el diagnóstico institucional, el cual será insumo para que las UR en coordinación con la DEA elaboren el PTCI, o en su caso cuando sea procedente, el PTAR, considerando también los hallazgos identificados en el levantamiento, modelado y reevaluación de procesos, para establecer las acciones de control o de mejora a implementar, que se consideren necesarias.

**Artículo 13.** Adicionalmente a los resultados de la autoevaluación, se deberán considerar las evaluaciones, observaciones y recomendaciones, tanto del CPI, como las correspondientes a órganos fiscalizadores y especialistas externos (OIC, ASF, auditores, etc.).

### De las evidencias de la autoevaluación

**Artículo 14.** El resultado de la aplicación de los cuestionarios deberá

conservarse en archivos electrónicos en el RICI, para consulta de todo el personal del INSTITUTO.

## Sección II. Del PTCI y PTAR, y del Informe Anual del Estado que Guarda el SCII.

### De la integración y aprobación del PTCI y PTAR, y del Informe Anual

**Artículo 15.** La DEA deberá presentar al CPI para su conocimiento, los documentos siguientes:

I. Los informes trimestrales y anual del estado que guarda el SCII, considerando cuando menos:

En el caso de los informes trimestrales:

a. Resumen de los avances de las acciones de control establecidas en los PTCI o la estrategia para administrar el riego de los PTAR;

b. Resumen de los resultados de aquellas acciones de control de los PTCI y estrategias de los PTAR que ya fueron concluidas y

c. Las demás actividades realizadas por la DEA para el fortalecimiento del SCII

En el caso del informe anual:

a. Actividades generales realizadas por la DEA para el fortalecimiento del SCII;

b. Resultados relevantes derivados de la aplicación de los cuestionarios de autoevaluación, así como, en su caso, las correspondientes a órganos fiscalizadores y especialistas externos;

c. Resumen de los PTCI y PTAR que se encuentran en ejecución y concluidos;

d. Resumen de los PTCI y PTAR nuevos que hayan elaborado las UR;

e. Resultados relevantes alcanzados en el fortalecimiento del SCII, que procedan del año inmediato anterior, una vez implementadas las acciones de control o estrategias para la administración de riesgos y,

f. Los PTCI y PTAR elaborados por las y los Titulares de las UR de los procesos, de acuerdo a lo establecido en el inciso c), de la fracción I del artículo 18, de este ordenamiento, los cuales estarán a disposición de los miembros del CPI en el RICI o en los medios electrónicos que la DEA establezca para tales efectos.

## Del seguimiento al PTCI y PTAR

**Artículo 16.** El seguimiento a la implementación de las acciones de control comprometidas en el PTCI y PTAR, se deberá realizase por las UR a través del RICI de manera trimestral, a más tardar 10 días hábiles posteriores al término del trimestre de que se trate, considerando lo siguiente:

I. Acciones de control comprometidas, concluidas y en proceso, con sus porcentajes de avance;

II. En su caso, descripción de las principales problemáticas que obstaculizan el cumplimiento de las acciones de control comprometidas, así como las propuestas de solución;

III. Evidencias que soporten los avances de las acciones de control comprometidas, las cuales deberán ser integradas en el RICI, y

IV. El personal responsable del proceso, del cual se reporta el avance, deberá registrar la información de las fracciones I a III anteriores, en el RICI.

Una vez validada dicha actualización en el RICI, la DEA lo incluirá en los Informes Trimestrales y Anual del estado que guarda el SCII, que deberá presentar al CPI a más tardar 20 días hábiles contados a partir de la conclusión

del trimestre de que se trate; y en el caso del Informe Anual también deberá ser presentado a la JGE.

Además, pondrá dichos informes a disposición del OIC en el RICI, para llevar a cabo el acompañamiento en el proceso de control interno, conforme a su competencia.

### De las evidencias de la ejecución del PTCI y PTAR

**Artículo 17.** La evidencia documental y/o electrónica que acredite la implementación, de las acciones de control de los PTCI y PTAR, los avances reportados sobre su cumplimiento, deberá ser conservada y resguardada en el RICI por la DEA.

## Sección III. De las y los Participantes y Funciones

**Artículo 18.** Las y los participantes, así como sus responsabilidades en la evaluación y fortalecimiento del SCII son:

I. Titulares de las UR de los procesos con la participación del personal del INSTITUTO y las y los prestadores de servicios, a través de su Enlace de Control Interno o la persona que designe para tal efecto:

   a. Implementar el SCII, mediante el cumplimiento de los elementos de control interno correspondientes, vinculados a los componentes o normas generales de control interno y a los principios asociados, conforme a lo dispuesto en el artículo 9 de las presentes Disposiciones;

   b. Supervisar y autoevaluar anualmente el funcionamiento del SCII, mediante el cumplimiento a la Norma general Quinta "Supervisión y Mejora Continua" prevista en el artículo 9, fracción V, en concordancia con lo dispuesto en los artículos 10, 11, 12, 13 y 14 de estas Disposiciones.

   c. Proponer a la DEA los PTCI y PTAR de los procesos, los cuales

deberán contemplar cuando menos:

d. Las acciones de control derivadas, según corresponda, de los resultados del cuestionario de autoevaluación y del levantamiento, documentación y análisis de los procesos y la base de datos de riesgos materializados.

e. Las fechas de inicio y término;

f. La o el responsable de la implementación de las acciones de control;

g. Los medios de verificación o evidencia documental de las acciones o estrategias realizadas;

h. Firmas de la o el responsable de la implementación, del responsable de los riesgos del proceso y la o el Titular de la UR.

i. El objetivo de implementar la acción de control;

j. Los resultados esperados de la implementación de la acción de control;

k. Indicar si requiere de financiamiento a través de un proyecto específico; y

l. La propuesta de avance por trimestre calendario, hasta que se concluya la acción de control.

m. Reportar en el RICI los avances trimestrales en la implementación de las acciones de control comprometidas, mediante el cumplimiento a la Norma General Quinta "Supervisión y Mejora Continua" prevista en el artículo 9, fracción V, en concordancia con lo dispuesto en los artículos 15, 16 y 17 de estas Disposiciones.

n. Nombrar a un Enlace de Control Interno, con nivel jerárquico de Director/a u homólogo/a, quien será el contacto con la DEA; excepcionalmente se podrá nombrar un enlace con nivel de

Subdirector/a u homólogo/a.

II. Personal del INSTITUTO y las y los prestadores de servicios:

a. Informar al superior jerárquico sobre las deficiencias relevantes, riesgos asociados y sus actualizaciones, identificadas en los procesos sustantivos y de soporte en los que participan y/o son responsables;

b. Evaluar el SCII verificando el cumplimiento de los componentes o normas generales, sus principios y elementos de control, así como proponer las acciones de control;

c. Implementar las acciones de mejora, señaladas en el inciso anterior, en las fechas y bajo los formatos y/o mecanismos establecidos, como parte del proceso de mejora continua.

III. Enlace de Control Interno de la UR:

a. Ser el canal de comunicación e interacción entre la DEA (UR coordinadora del Control Interno), y las UR para el control interno;

b. Aplicar los criterios establecidos en las presentes Disposiciones o los que establezca la DEA para priorizar los procesos (sustantivos o de soporte) en los que participa la UR;

c. Proponer al o la Titular de la UR los procesos prioritarios en donde será aplicado el SCII;

d. Enviar a la DEA la lista de procesos seleccionados para ser incorporados al SCII autorizada por el o la Titular de la UR y los nombres y puestos de las y los responsables de cada proceso;

e. Instrumentar las acciones con el apoyo de la DEA, con la finalidad de que las y los Responsables de los Riesgos del Proceso realicen la autoevaluación de sus procesos conforme con las presentes Disposiciones y con base en el calendario establecido.

f. Asesorar a los Responsables de los Riesgos del Proceso sobre el uso de los formatos y/o mecanismos establecidos por la DEA para la integración del PTCI y PTAR, y de los reportes de avance trimestral;

g. Acompañar a las y los Analistas de Riesgos en el diseño de la propuesta de acciones de control que serán incorporadas al PTCI y PTAR para atender la inexistencia, insuficiencia o deficiencia de control identificadas en la implementación de los componentes o normas generales, sus principios y elementos de control interno;

h. Promover la propuesta del PTCI y PTAR hasta su revisión por la o el Titular de la UR;

i. Solicitar a la o el Titular de la UR, a las y los Responsables de los Riesgos de los Procesos y Responsables de las Acciones de Control, la firma electrónica de la versión final del PTCI y PTAR;

j. Solicitar a las y los Responsables de los Riesgos de los Procesos, el reporte de avance trimestral del cumplimiento del PTCI y PTAR, y que sea presentado a la DEA para revisión, a través del RICI y

k. Solicitar a la o el Titular de la UR, a las y los Responsables de los Riesgos de los Procesos, y a las y los Responsables de las Acciones de Control preferentemente la firma electrónica del reporte de avance trimestral del PTCI y PTAR.

IV. DEA:

a. Aprobar preferentemente mediante firma electrónica los cuestionarios a aplicar, sus criterios de medición y el calendario de actividades para llevar a cabo la autoevaluación anual del SCII;

b. Coordinar la implementación y fortalecimiento del SCII;

c. Verificar que las propuestas de las acciones de control que se incorporarán al PTCI y PTAR de las y los Analistas de Riesgos de los Procesos y las y los Titulares de las UR, para su aprobación,

están integradas conforme al artículo 18, fracción I, incisos c), d), e), f), g), h), i), j) y k) de las presentes Disposiciones;

d. Dar seguimiento y revisar de manera trimestral el reporte de avance de los PTCI y PTAR propuestos por las y los Titulares de las UR de los procesos;

e. Elaborar los Informes Trimestrales del PTCI y PTAR, y el Informe Anual del estado que guarda el SCII.

f. Presentar a la JGE para su conocimiento el Informe Anual del estado que guarda el SCII;

g. Elaborar el PTCI Institucional en el RICI, con la información de los PTCI y sus avances, de los procesos analizados.

h. Presentar al CPI los documentos previstos en los incisos, e), y g) de esta fracción IV;

i. Informar al OIC que los documentos previstos en los incisos e) y g) de esta fracción IV se encuentran disponibles para su consulta en el RICI; y

j. Determinar los procesos vinculados a los objetivos establecidos en la planeación institucional, en los que se realizará la evaluación del SCII, conforme a lo dispuesto en el artículo 7 de las presentes disposiciones.

k. Solicitar a la o el Titular de la UR, a las y los responsables de los Riesgos de los Procesos, y a las y los Responsables de las Acciones de Control la firma electrónica del Reporte de Avance Trimestral del PTCI y PTAR.

V. Comité de Planeación Institucional

a. Conocer los resultados de las distintas evaluaciones del SCII; y
b. Conocer los documentos señalados en los incisos e) y g), de la fracción IV de este artículo 18.

VI. Junta General Ejecutiva:

a. Conocer el Informe Anual del Estado que Guarda el SCII señalado en el inciso f) y el PTCI Institucional, indicado en el inciso g), de la fracción IV de este artículo 18.

VII. OIC

a. En el ámbito de sus atribuciones podrá realizar evaluaciones externas al SCII.

b. Tendrá a su disposición en el RICI la siguiente documentación, para llevar a cabo el acompañamiento en el proceso de control interno, conforme a su competencia:

1. PTCI y PTAR;
2. Reportes de avance trimestral del PTCI y PTAR;
3. Informes Trimestrales del Estado que Guarda el SCII;
4. Informe Anual del Estado que Guarda el SCII.

c. Acompañar a la DEA en la revisión de las actualizaciones de las presentes disposiciones.

d. Acompañar a la DEA en la revisión del contenido del cuestionario de autoevaluación anual que deberá aplicarse.

# Capítulo IV. Administración de Riesgos

## Del objetivo

**Artículo 19.** La administración de riesgos apoya a lo previsto en las Normas Generales Segunda y Tercera "Administración de Riesgos" y "Actividades de Control", establecidas en el artículo 9, fracciones II y III, respectivamente, en concordancia con lo dispuesto en los artículos 7 y 8, de las presentes disposiciones, tiene como objetivo:

Implementar un proceso sistemático de administración de riesgos, mediante el cual se identifiquen, evalúen, jerarquicen, controlen, reporten y se les dé seguimiento, para que en coexistencia con lo previsto en los capítulos III y V

de estas Disposiciones, contribuya a contarse con un SCII sólido.

## Sección I. De la Administración de Riesgos

## De la Metodología de Administración de Riesgos

**Artículo 20.** La metodología de administración de riesgos se debe alinear con lo establecido en los artículos 7, 8 y 9, fracciones II y III, de las presentes disposiciones, y debe considerar al menos lo siguiente:

I. Las fases del proceso;

II. Matriz de administración de riesgos;

III. Mapa de riesgos institucionales;

IV. Estructura del PTAR y PTCI, y

V. Estructura de los Informes Trimestral y Anual del Estado que Guarda el SCII.

**Artículo 21.** Las fases de la metodología de administración de riesgos son:

I. Identificación de Riesgos:

El INSTITUTO identifica los eventos potenciales o riesgos operativos y de corrupción, con base en las metas y objetivos estratégicos institucionales a través de los procesos sustantivos y de soporte definidos para el logro de los objetivos operacionales, de información, de cumplimiento y salvaguarda, que de materializarse afectarían negativamente la capacidad, la operación y/o el patrimonio institucional.

Los eventos con impactos negativos que representen riesgos exigirán la evaluación y respuesta de las y los Titulares de las UR y las y los Responsables de los Riesgos del Proceso. Los eventos con impactos positivos que representen áreas de oportunidad deberán ser tomados en cuenta por las y los responsables para reconducir hacia la estrategia y el proceso de fijación de objetivos. Cuando

se identifiquen los eventos, las y los Responsables de los Riesgos del Proceso deberán contemplar una serie de factores internos y externos que puedan dar lugar a riesgos y oportunidades en el ámbito institucional.

La descripción de los riesgos deberá de considerar la siguiente estructura: sustantivo, verbo en participio y adjetivo o adverbio o complemento circunstancial negativo. Los riesgos deberán ser descritos como una situación negativa que puede ocurrir y afectar el cumplimiento de metas y objetivos institucionales.

La vinculación entre los riesgos identificados debe estar relacionada con su impacto en el objetivo, la tolerancia asociada y la unidad de medición. La metodología que el INSTITUTO ha definido para la identificación de eventos comprende una combinación de técnicas y herramientas de apoyo, basándose en eventos pasados y futuros que afectaron o podrán afectar el logro de los objetivos estratégicos institucionales. Estas técnicas se emplean para la identificación de riesgos y oportunidades. Las herramientas que podrán utilizarse para identificar eventos son, entre otras:

*Figura 4. Algunas técnicas para identificar eventos*


II. Clasificación de riesgos:

Las y los responsables o dueñas(os) de los procesos como encargadas(os) de la eficiencia y efectividad de las actividades de administración de riesgo clasifican los riesgos identificados en seis tipos, como sigue:

| ***Cuadro 1. Clasificación de riesgos*** | |
|---|---|
| Tipo de riesgo | Descripción |
| Estratégico | Se asocia a los asuntos relacionados con la misión y el cumplimiento de los objetivos estratégicos. |

| | |
|---|---|
| Financiero | Se relaciona con los recursos económicos de la institución, principalmente de la eficiencia y transparencia en el manejo de los recursos. |
| Operativo | Este rubro considera los riegos relacionados con fallas en los procesos, en los sistemas o en la estructura de la institución. |
| Legal | Afecta la capacidad de la institución para dar cumplimiento a la legislación, normas, reglamentos, prácticas internas y obligaciones contractuales. |
| Tecnológico | Se relaciona con la capacidad de la institución para que las herramientas tecnológicas soporten el logro de los objetivos estratégicos. |
| Integridad/Corrupción | Está relacionado con la posibilidad de que un servidor público actúe de modo voluntario para obtener un beneficio propio en detrimento de la ciudadanía. |

Los riesgos estratégicos, financieros, operativos, legales y tecnológicos, a su vez se subclasifican en siete categorías de acuerdo al factor que los origina, como se muestra a continuación:

| ***Cuadro 2. Tipos de Riesgo*** | |
|---|---|
| Sub clasificación | Descripción |
| Humano | Se relacionan con las personas (internas o externas), que participan directa o indirectamente en los programas, procesos/subprocesos, actividades o tareas |
| Financiero Presupuestal | Se refieren a los recursos financieros y presupuestales necesarios para el logro de metas y objetivos. |
| Técnico-Administrativo | Se vinculan con la estructura orgánica funcional, políticas, sistemas no informáticos, procedimientos, comunicación e información, que intervienen en la consecución de las metas y objetivos. |
| TIC's | Se relacionan con los sistemas de información y comunicación automatizados. |
| Material | Se refieren a la infraestructura y recursos materiales necesarios para el logro de las metas y objetivos. |
| Normativo | Se vinculan con las leyes, reglamentos, normas y disposiciones que rigen la |

| | |
|---|---|
| | actuación de la organización en la consecución de las metas y objetivos. |
| Entorno | Se refieren a las condiciones externas a la organización, que pueden incidir en el logro de las metas y objetivos. |

De acuerdo con lo que establece la Ley General de Responsabilidades Administrativas, los riesgos de integridad / corrupción, a su vez se subclasifican en doce categorías, de acuerdo al factor que los origina, como se muestra a continuación:

***Cuadro 3. Subclasificación de riesgos de Integridad / Corrupción***

| Categoría | Descripción |
|---|---|
| Peculado | Personal del INSTITUTO o prestador de servicios que autorice, solicite o realice actos para el uso o apropiación para sí o para alguna persona, de recursos públicos, sean materiales, humanos o financieros, sin fundamento jurídico o en contraposición a las normas aplicables. |
| Desvío de Recursos Públicos | Personal del INSTITUTO o prestador de servicios que autorice, solicite o realice actos para la asignación o desvío de recursos públicos, sean materiales, humanos o financieros, sin fundamento jurídico o en contraposición a las normas aplicables. |
| Utilización indebida de información | Personal del INSTITUTO o prestador de servicios que adquiera para sí o para otra persona, bienes inmuebles, muebles y valores que pudieren incrementar su valor o, en general, que mejoren sus condiciones, así como obtener cualquier ventaja o beneficio privado, como resultado de información privilegiada de la cual haya tenido conocimiento. |
| Uso ilícito de atribuciones y facultades | Aprovechamiento del cargo o comisión del personal del INSTITUTO o prestador de servicios para inducir a que un tercero efectúe, retrase u omita realizar algún acto de su competencia, que le reporte cualquier beneficio, provecho o ventaja indebida para sí o para un tercero. |
| Conflicto de interés | Personal del INSTITUTO o prestador de servicios que intervenga por motivo de su empleo, cargo o comisión en cualquier forma, en la atención, tramitación o resolución de asuntos en los que tenga conflicto de interés o impedimento legal. |
| Contratación indebida | Personal del INSTITUTO o prestador de servicios que autorice cualquier tipo de contratación, así como la selección, nombramiento o designación, de quien se encuentre impedido por disposición legal o inhabilitado por resolución de autoridad competente para ocupar un empleo, cargo o comisión en el INSTITUTO, o inhabilitado para realizar contrataciones con los entes públicos. |
| Enriquecimiento oculto u Ocultamiento de Conflicto de Interés | Personal del INSTITUTO o prestador de servicios que falte a la veracidad en la presentación de las declaraciones de situación patrimonial o de intereses, que tenga como fin ocultar, respectivamente, el incremento en su patrimonio o el uso y disfrute de bienes o servicios que no sea explicable o justificable, o un conflicto de interés. |
| Tráfico de influencias | Personal del INSTITUTO o prestador de servicios que utilice la posición que su empleo, cargo o comisión le confiere para inducir a que otro servidor público efectúe, retrase u omita realizar algún acto de su competencia, para generar cualquier beneficio, provecho o ventaja para sí o para alguna persona. |

| Categoría | Descripción |
|---|---|
| Informes financieros fraudulentos | Consistentes en errores intencionales u omisiones de cantidades o revelaciones en los estados financieros para engañar a los usuarios de dichos documentos. |
| Apropiación indebida de activos | Entendida como el robo de activos del INSTITUTO. Esto podría incluir el robo de la propiedad, la malversación de los ingresos o pagos fraudulentos. |
| Obtención de beneficios adicionales a las otorgadas | Pretensión del personal del INSTITUTO o prestador de servicios de obtener beneficios adicionales a las contraprestaciones comprobables que el INSTITUTO le otorga por el desempeño de su función.<br>Intimidación o extorsión: Intimidación del personal del INSTITUTO o prestador de servicios o extorsión para presionar a otro a realizar actividades ilegales o ilícitas. |
| Colusión de servidores/as públicos/as | Colusión con personal del INSTITUTO, prestador de servicios o terceros para obtener ventajas o ganancias ilícitas. |

Para la identificación de los riesgos de corrupción, las y los Titulares de las Unidades Responsables y las y los Responsables de los Riesgos de los Procesos, deberán considerar los procesos financieros, presupuestales, de contratación, de información y documentación, investigación y sanción, así como de ser el caso los trámites y servicios internos y externos.

Para el caso de los riesgos de corrupción, las causas se establecerán a partir de la identificación de las debilidades (factores internos) y las amenazas (factores externos) que pueden influir en los procesos y subprocesos, que generan una mayor vulnerabilidad frente a los riesgos de corrupción.

Procesos susceptibles a un posible conflicto de interés:

- **Adquisiciones:** Todos aquellos servicios cuya prestación genera una obligación de pago para las dependencias o entidades.
- **Obra pública:** Las relaciones con la creación, mantenimiento y destrucción de construcciones.
- **Recursos Financieros:** El uso del dinero disponible para ser gastado en forma de efectivo, valores líquidos y líneas de crédito.
- **Recursos Humanos:** El reclutamiento, capacitación y pago de salario del personal.
- **Recursos Materiales:** La administración y distribución de bienes, insumos y servicios, así como el manejo de almacenes a nivel general.
- **Tecnologías de Información:** Los dispositivos tecnológicos que permiten producir, almacenar y transmitir datos entre sistemas de información que cuentan con protocolos comunes.

- **Transparencia:** Las acciones enfocadas en permitir y garantizar el acceso a la información pública.
- **Auditoría:** Las actividades independientes, objetivas y sistemáticas que tienen el propósito de evaluar la actuación y el resultado de las entidades.
- **Control Interno:** Las acciones encaminadas a proporcionar un grado de seguridad razonable en la consecución de los objetivos y metas de la Institución.

Los riesgos de corrupción serán normalmente de impacto grave, ya que la materialización de este tipo de riesgos es inaceptable e intolerable, en tanto lesionan la imagen, confianza, credibilidad y transparencia en el INE, afectando los recursos públicos y el cumplimiento de los objetivos.

### III. Factores de los riesgos

Durante la ejecución de las distintas herramientas será necesario contar con un enfoque a identificar aquellos factores de riesgo, el riesgo posible de presentarse y el efecto que tendría en el INSTITUTO.

Algunos ejemplos de estos factores son falta o falla en el diseño de la normativa; deficiencia en el diseño del programa o política pública; insuficiencia de recursos financieros; falta de planeación; falta de capacidades de gestión; falta de capacitación técnica; falta de automatización o integración de procesos; uso indebido de información privilegiada; brechas de integridad y falta de transparencia.


*Figura 5. Identificación de eventos*

El seguimiento de la información relevante de acontecimientos pasados con impacto negativo permite cuantificar las pérdidas asociadas y su impacto, a fin de predecir futuros sucesos o riesgos con alta probabilidad de ocurrencia, con base en la experiencia.

Al igual que los riesgos, los factores se clasifican en:

| ***Cuadro 4. Clasificación de los Factores de Riesgo*** | |
|---|---|
| Subclasificación | Descripción |
| Humano | Se relacionan con las personas (internas o externas), que participan directa o indirectamente en los programas, procesos/subprocesos, actividades o tareas |
| Financiero Presupuestal | Se refieren a los recursos financieros y presupuestales necesarios para el logro de metas y objetivos. |
| Técnico-Administrativo | Se vinculan con la estructura orgánica funcional, políticas, sistemas no informáticos, procedimientos, comunicación e información, que intervienen en la consecución de las metas y objetivos. |
| TIC's | Se relacionan con los sistemas de información y comunicación automatizados. |
| Material | Se refieren a la infraestructura y recursos materiales necesarios para el logro de las metas y objetivos. |
| Normativo | Se vinculan con las leyes, reglamentos, normas y disposiciones que rigen la actuación de la organización en la consecución de las metas y objetivos. |
| Entorno | Se refieren a las condiciones externas a la organización, que pueden incidir en el logro de las metas y objetivos. |

Es importante considerar el origen de los factores que pueden favorecer que se materialice un riesgo, ya que, si se trata de factores internos, en la mayoría de los casos es posible atenuarlos, mientras que si se trata de factores externos, difícilmente se tiene injerencia en ellos.


*Figura 6. Tipos de factores*

Ⅳ. Evaluación de riesgos:

Los riesgos se evalúan desde una doble perspectiva, probabilidad de ocurrencia en función al número de veces que pudiera ocurrir un evento dentro de un periodo de tiempo determinado o durante el ciclo de un proceso, e impacto que considera el efecto sobre las capacidades del Instituto, afectando el cumplimiento de los objetivos estratégicos institucionales.

Al estimar la probabilidad e impacto de posibles eventos, ya sea sobre la base del efecto inherente o residual, se deberá aplicar una medición ordinal que describa los riesgos en orden de importancia a lo largo de escalas contenidas en esta metodología.

La evaluación de la probabilidad de materialización del riesgo se clasifica de acuerdo al siguiente cuadro:

| Cuadro 5. Evaluación de probabilidad | | |
|---|---|---|
| Escala de Valor | Probabilidad de Ocurrencia | Descripción |
| 5 | Recurrente | Probabilidad de ocurrencia **muy alta**.<br>Se tiene la seguridad de que el riesgo se materialice, tiende a estar entre 90% y 100% |
| 4 | Muy probable | Probabilidad de ocurrencia **alta**.<br>Está entre 75% a 89% la seguridad de que se materialice el riesgo. |
| 3 | Probable | Probabilidad de ocurrencia **media**.<br>Está entre 51% a 74% la seguridad de que se materialice el riesgo |
| 2 | Inusual | Probabilidad de ocurrencia **baja**.<br>Esta entre 25% a 50% la seguridad de que se materialice el riesgo. |
| 1 | Remota | Probabilidad de ocurrencia **muy baja**.<br>Está entre 1% a 24% la seguridad de que se materialice el riesgo. |

La evaluación del impacto se realiza considerando la afectación del riesgo al objetivo estratégico institucional, con base en los criterios establecidos para los tipos de objetivo COSO-ERM correspondientes a los procesos y subprocesos, sustantivos y de soporte en lo que se pudiera materializar, de acuerdo con al siguiente cuadro:

| Cuadro 6. Evaluación del Impacto | | |
|---|---|---|
| Escala de Valor | Impacto | Descripción |
| 5 | Catastrófico | ▪ Impide el cumplimiento de la misión, visión y objetivos estratégicos institucionales.<br>▪ Imposibilita la toma de decisiones debido a que la emisión de información no es clara, confiable, exacta y oportuna.<br>▪ Incumplimiento en los objetivos constitucionales y legales del INSTITUTO.<br>▪ Implica pérdida patrimonial.<br>▪ Afecta la continuidad de las operaciones, sin la posibilidad de operar por más de un mes.<br>▪ Interrupción total de los sistemas de información.<br>▪ Deterioro de la imagen institucional o daño reputacional ante la ciudadanía de manera internacional. |

| Escala de Valor | Impacto | Descripción |
|---|---|---|
| 4 | Grave | ▪ Impacta sustancialmente el cumplimiento de los objetivos estratégicos.<br>▪ Interrupción prolongada del proceso, con posibilidad operar en menos de un mes.<br>▪ Desconfianza en la emisión de información.<br>▪ Puede implicar pérdida patrimonial.<br>▪ Daños reputacionales del INSTITUTO ante la ciudadanía.<br>▪ Interrupción intermitente de los sistemas de información.<br>▪ Se incurre en posibles responsabilidades administrativas y daños patrimoniales y/o penales. |
| 3 | Importante | ▪ Impacta el cumplimiento de los objetivos del proceso.<br>▪ Interrupción corta del proceso, con la posibilidad de renovar su operación en menos de dos días.<br>▪ Errores advertidos externamente (por un ente fiscalizador o verificador).<br>▪ Incurren en incumplimientos normativos que pueden ser atendidos en el corto plazo.<br>▪ Daño reputacional al interior del Instituto del área encargada de administrar, ejecutar y dar seguimiento al proceso. |
| 2 | Débil | ▪ Causa un daño en el patrimonio o imagen institucional, que se puede corregir en el corto tiempo y no afecta el cumplimiento del objetivo del proceso o de los objetivos estratégicos.<br>▪ Desviación en la normatividad aplicable que puede implicar un impacto poco relevante.<br>▪ Errores advertidos internamente.<br>▪ Interrupción del proceso que no afecta considerablemente la operación del mismo.<br>▪ Daños en la operación que pueden ser corregidos de manera inmediata. |
| 1 | Marginal | ▪ Riesgo que puede ocasionar pequeños o nulos efectos en la operación del proceso o en el INSTITUTO.<br>▪ Dificultad en la ejecución del proceso de forma adecuada. |

V. Criterios de Riesgos

Los criterios determinados para los impactos negativos de los eventos deberán ser examinados por las UR, individualmente y por categoría en los procesos del INSTITUTO y evaluados con un doble enfoque: riesgo inherente y riesgo residual.


*Figura 7. Inherente y Residual*

El riesgo residual refleja el riesgo remanente una vez que se han implementado de manera eficaz las acciones planificadas por cada responsable para mitigar el riesgo inherente. Estas acciones o planes de mitigación pueden incluir las estrategias de diversificación, establecimiento de controles que fijen límites, autorizaciones y otros protocolos, el personal de supervisión para revisar medidas de rendimiento e implantar acciones al respecto o a la automatización de criterios para estandarizar y acelerar la toma de decisiones recurrentes y aprobación de transacciones. Además, tiene el objetivo de reducir la probabilidad de ocurrencia y el impacto.

Con el propósito de orientar a las y los Responsables de los Riesgos del Proceso en la aplicación de la administración de riesgos, como anexo a este MNCI, se incluye la Guía de Apoyo para el cumplimiento de las Normas Generales de Control Interno, con el propósito de facilitar la identificación de riesgos y establecimiento de actividades de control.

**Artículo 22.** Matriz de riesgos.

Con la información obtenida de la aplicación del cuestionario de autoevaluación y del levantamiento, modelado y análisis de los procesos, los Responsables de los Riesgos de los Procesos elaborarán la matriz de riesgos, en donde se concentrará dicha información para la toma de decisiones, la cual contendrá por lo menos:

I. Nombre del proceso;
II. Descripción de los riesgos identificados;
III. Clasificación de los riesgos;
IV. Descripción de los factores de riesgo identificados;
V. Clasificación de los factores de riesgo;
VI. Evaluación de los riesgos;
VII. Controles identificados;
VIII. Clasificación de los controles; y
IX. Evaluación de los controles.

Dicha matriz se construirá en el RICI o en el mecanismo que se establezca para ello, en donde será revisada por la DEA, y en su caso hará las recomendaciones necesarias.

**Artículo 23.** Mapa de riesgos.

Cada Responsable de los Riesgos del Proceso evaluará los riesgos identificados de acuerdo a las métricas señaladas para obtener la exposición al riesgo y con base en ella se generará el mapa de riesgos correspondiente, que deberá ser firmado electrónicamente por él mismo y la o el Titular de la UR, de acuerdo a lo siguiente:

| *Cuadro 7. Mapa de riesgos* | |
|---|---|
| Cuadrante | Descripción |
| I | Riesgos de Atención Inmediata |
| II | Riesgos de Atención Periódica |
| III | Riesgos Controlados |
| IV | Riesgos de Seguimiento |

El nivel de exposición al riesgo evaluado deberá ubicarse en un mapa de riesgos como a continuación se muestra.

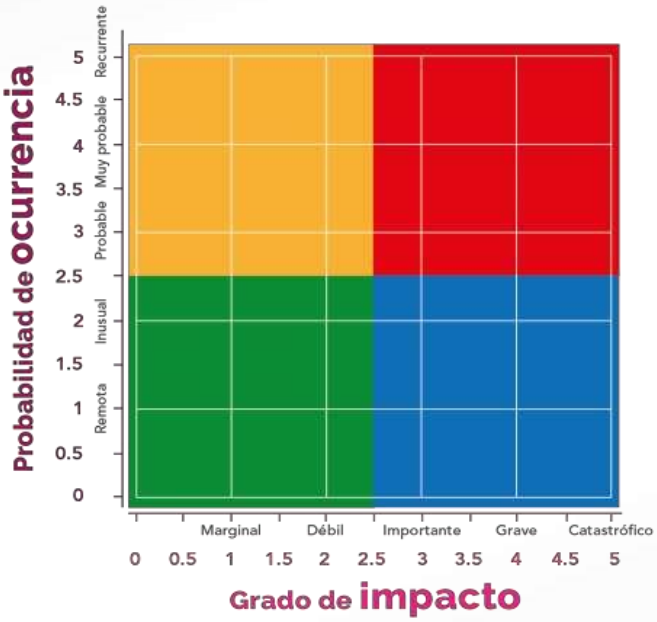



*Figura 9. Mapa de riesgos*

Una vez realizada la evaluación de riesgos y con base en los aspectos de probabilidad de ocurrencia e impacto, el Instituto debe priorizar los riesgos ya evaluados, para determinar cuáles requieren de un tratamiento inmediato. Así mismo el Instituto debe establecer su nivel de tolerancia a riesgos.

La priorización de riesgos es el proceso donde las y los Titulares de las UR y las y los Responsables de los Riesgos del Proceso determinan las prioridades para la Administración de Riesgos mediante la comparación de la exposición de los riesgos obtenida como resultado de la evaluación de riesgos con los criterios aceptados a continuación:

***Cuadro 8. Priorización de riesgos***

| Exposición al Riesgo | Criterio de priorización |
|---|---|
| Alto | Requiere un plan de mitigación o control inmediato |
| Medio | Dar seguimiento para evitar impacto mayor |
| Bajo | Requiere poco monitoreo |
| Muy bajo | Operación normal, por lo general no es necesario atenderlo |

**Artículo 24.** Programa de Trabajo de Control Interno (PTCI) y de Administración de Riesgos (PTAR)

Una vez evaluados los riesgos -incluidos los de corrupción- y priorizados, las URs identifican cuáles son las acciones y controles que actualmente se ejecutan a través de sus actividades cotidianas dentro de sus procesos y, en su caso, subprocesos, para determinar cómo responder a sus riesgos.

| *Cuadro 9. Respuestas al riesgo* | |
|---|---|
| **Evitar**<br>Se refiere a eliminar el factor o factores que pueden provocar la materialización del riesgo, considerando que si una parte del proceso/subproceso tiene alto riesgo, el segmento completo recibe cambios sustanciales por mejora, rediseño o eliminación, resultado de controles suficientes y acciones emprendidas. | **Reducir**<br>Implica establecer acciones dirigidas a disminuir la probabilidad de ocurrencia (acciones de prevención) y el impacto (acciones de contingencia), tales como la optimización de los procedimientos y la implementación o mejora de controles. |
| **Transferir**<br>Consiste en trasladar el riesgo a un externo a través de la contratación de servicios tercerizados, el cual deberá tener la experiencia y especialización necesaria para asumir el riesgo, así como sus impactos o pérdidas derivadas de su materialización. Esta estrategia cuenta con tres métodos:<br>1. Protección o cobertura: La acción que se realiza para reducir la exposición a una pérdida.<br>2. Aseguramiento: Significa pagar una prima (el precio del seguro) para que, en caso de tener pérdidas, éstas sean asumidas por la aseguradora.<br>3. Diversificación: Implica mantener cantidades similares de muchos activos riesgosos en lugar de concentrar toda la inversión en uno sólo, en consecuencia, la diversificación reduce la exposición al riesgo de un activo individual. | **Asumir**<br>Se aplica cuando el riesgo se encuentra en el Cuadrante III, Riesgos Controlados de baja probabilidad de ocurrencia y grado de impacto y puede aceptarse sin necesidad de tomar otras medidas de control diferentes a las que se poseen, o cuando no se tiene opción para abatirlo y sólo pueden establecerse acciones de contingencia. |
| **Compartir**<br>Se refiere a distribuir parcialmente el riesgo y las posibles consecuencias, a efecto de segmentarlo y canalizarlo a diferentes UR, las cuales se responsabilizarán de la parte del riesgo que les corresponda en su ámbito de competencia. | |

Algunos criterios para considerar la respuesta a los riesgos son:

**Evitar**

1. Eliminar el factor o factores que provoquen la materialización del riesgo.
2. Cambiar sustancialmente los procesos o subprocesos con alto riesgo, a fin de mejorarlos, rediseñarlos o eliminarlos.

**Reducir**

1. Disminuir la probabilidad de ocurrencia a través del establecimiento de acciones preventivas.
2. Disminuir el impacto a través del establecimiento de acciones de contingencia o correctivas.

**Transferir**

1. Trasladar el riesgo a un tercero, a través de la contratación de servicios especializados, vastos en experiencia para asumir el riesgo, su impacto o pérdidas derivadas de su materialización, mediante protecciones o coberturas, aseguramiento y diversificaciones.

**Compartir**

1. Distribuir parcialmente el riesgo y sus posibles consecuencias.
2. Segmentar y canalizar a diferentes unidades de acuerdo a su competencia, la responsabilidad de la parte del riesgo que le corresponde.

**Asumir o aceptar**

1. Existen controles suficientes que apoyan a mitigar el riesgo identificado.
2. El costo o beneficio de implantación de las acciones es más alto que el impacto que puede generar el riesgo.

Las estrategias de respuesta pueden ser de evitar, reducir, transferir, compartir y aceptar el riesgo. Al considerar su respuesta, la o el Responsable de los riesgos del Proceso debe evaluar su efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios de la implementación.

Además de ello, habrá de determinar si las acciones de control a implementar impactan solamente a la operación de un proceso específico -por lo que se habrá de diseñar un PTAR-, o bien impactan transversalmente al Instituto o a un conjunto de procesos, en cuyo caso habrá de establecerse un PTCI; en este último escenario será necesario definir también el o los componentes o normas generales que serán fortalecidas con dichas acciones de control.

Después de haber seleccionado la respuesta al riesgo, las y los Titulares de las UR y las y los Responsables de los Riesgos del Proceso identifican las actividades de control, que se incorporarán al Programa de Trabajo de Control Interno (PTCI) o de Administración de Riesgos (PTAR), necesarias para ayudar a asegurar que las respuestas a los riesgos se lleven a cabo adecuada y oportunamente, de acuerdo a lo referido en el párrafo precedente. El INSTITUTO considera 3 tipos de controles:


*Figura 10. Tipos de control*

Si bien las actividades de control se establecen para asegurar que se lleven a cabo de manera adecuada las respuestas a los riesgos en el caso de ciertos objetivos las propias actividades de control podrán constituir una respuesta al riesgo.

### Del calendario de actividades del Proceso de Administración de Riesgos

**Artículo 25.** El calendario de actividades para llevar a cabo el proceso de administración de riesgos con base en la metodología deberá aprobarse por la JGE. El calendario, al igual que estas disposiciones y la metodología de administración de riesgos, se pondrán en el RICI a disposición de las y los Titulares de las UR, los Responsables de los Riesgos del Proceso, así como de sus Enlaces de Control Interno para facilitar su consulta y seguimiento.

## Capítulo V. Del Seguimiento

### Del objetivo

**Artículo 26.** El seguimiento, deberá ser conforme lo previsto en la Norma general Quinta "Supervisión y Mejora Continua", establecida en el artículo 10, fracción V, en concordancia con los artículos 3, fracción III, 8, 16, 18, fracción V inciso h) y 24 y demás relativos, de las presentes disposiciones.

**Artículo 27.** El CPI conocerá y dará seguimiento a la implementación del Control Interno a través de los informes trimestrales y anuales que presente la DEA y respecto a los resultados de los mecanismos de evaluación que se apliquen en forma interna o externa, con el fin de proponer acciones para fortalecer el Control Interno institucional.

# Artículos transitorios

Artículo transitorio primero. Debido a que, a la fecha de autorización de las presentes Disposiciones ya se concluyó la estructura del Repositorio Institucional de Control Interno, pero aún se encuentran en proceso de automatización algunos de los procedimientos de Gestión de Control Interno que serán alojados en dicho repositorio, los documentos e información generada del proceso de control interno se manejarán de manera física y/o en medios electrónicos, hasta que se concluya con dicha implementación.

Artículo transitorio segundo. El programa permanente de integridad se articulará una vez que el Comité de Ética valide de acuerdo con sus Lineamientos los contenidos de dicho programa.

# Lista de Cuadros



# Lista de Figuras