

Manual para la Conducción de Autoevaluaciones de la Integridad en las Entidades Fiscalizadoras Superiores (*IntoSAINT*)

Versión 6 de octubre de 2014

NOTA

Este manual (versión 6 de octubre de 2014)¹ es una traducción al español, enriquecida por la Auditoría Superior de la Federación de México, y adaptada al contexto regional, con pleno apego a la metodología de *IntoSAINT* y debido conocimiento y autorización del Tribunal de Cuentas de los Países Bajos.



Algemene Rekenkamer

¹ En comparación con la versión anterior al presente Manual, en este documento se anexa traducción e información acerca de los diagramas sobre vulnerabilidades y resistencias a brechas de integridad (página 13), traducción e información sobre la clasificación de los factores que agravan la vulnerabilidad (páginas 31-32) así como ajustes de traducción en el anexo sobre los Sistemas de Controles de la Integridad (páginas 66 a 72).

ÍNDICE

Introducción a IntoSAINT.....	5
Relevancia para la OLACEFS.....	6
 PARTE 1: PRINCIPIOS DE LA METODOLOGÍA.....	8
Capítulo I. Concepto de <i>Integridad</i>	8
Capítulo II. Evaluación de riesgos y definiciones relevantes	11
Capítulo III. Principios básicos	14
Capítulo IV. Esbozo del método de evaluación	16
 PARTE 2: GUÍA DE INSTRUMENTACIÓN DEL TALLER.....	18
Capítulo V. Preparación	18
Capítulo VI. Definición del objeto y procesos	20
<u>a.</u> Introducción	20
<u>b.</u> Procesos Primarios	21
<u>c.</u> Procesos secundarios	21
<u>d.</u> Procesos de Gobernanza	22
Capítulo VII. Evaluación de las vulnerabilidades	23
<u>a.</u> Introducción	23
<u>b.</u> Vulnerabilidades y tentaciones	23
<u>c.</u> Evaluación de las vulnerabilidades inherentes.....	24
<u>d.</u> Factores que agravan la vulnerabilidad	29
<u>e.</u> Evaluación del perfil de vulnerabilidad	33

Capítulo VIII. Nivel de madurez del Sistema de Controles de la Integridad	34
<u>a.</u> Introducción	34
<u>b.</u> Grupos de Medidas	34
<u>c.</u> Descripción detallada de los grupos	35
<u>d.</u> Evaluación del nivel de madurez	60
<u>e.</u> Análisis de las fortalezas y debilidades del Sistema de Controles de la Integridad	61
 Capítulo IX. Análisis de Brechas.....	62
<u>a.</u> Descripción	62
<u>b.</u> Recomendaciones e Informe	64
 Anexo Sistema de Controles de la Integridad.....	66

Introducción a IntoSAINT

La Herramienta para la Autoevaluación de la Integridad en las Entidades Fiscalizadoras Superiores (*IntoSAINT*) consiste en un taller de autoevaluación con duración de dos días, que es impartido por dos moderadores capacitados previamente, a un grupo selecto de participantes (funcionarios de la entidad evaluada), quienes son seleccionados a partir de un filtro convenido con la alta dirección a fin de incluir personal multidisciplinario, de distintas áreas y niveles en la jerarquía institucional. Esto es clave porque se hace partícipe a todo el personal sobre la importancia de la integridad y se fomenta la propiedad colectiva de las medidas de integridad a lo largo y ancho de la institución en cuestión.

El instrumento es innovador puesto que permite que el propio personal, guiado por los facilitadores instruidos (preferiblemente de otra EFS para evitar sesgos) y a partir de su percepción, identifique las vulnerabilidades a la integridad en las EFS y evalúe el nivel de madurez (grado de eficacia) del sistema de controles de la integridad implementados, todo lo cual conlleva a la determinación de las brechas existentes, y a la definición de medidas para solventarlas. La premisa sobre la que se erige esta herramienta es que el propio personal (no consultores o auditores externos), en el cumplimiento de sus deberes, es quien experimenta los riesgos y quien se enfrenta a dilemas éticos, por lo que no existe mejor evaluador que ellos mismos para identificar el apoyo que se requiere, así como para tener una imagen realista de los retos encarados por la organización. Al mismo tiempo, ellos son quienes, al hablar con otros colegas sobre los riesgos a la integridad, concientizan sobre los riesgos y asuntos que impactan la integridad. Es decir, los propios empleados se convierten en defensores de la integridad al interior de su organización.

El proceso es asistido con matrices diseñadas por el Tribunal de Cuentas de los Países Bajos y adaptadas por la Auditoría Superior de la Federación de México, con estricto apego a la metodología. Las recomendaciones surgidas de esta herramienta pueden tener un alcance que requiera acciones de la propia administración, hasta medidas que impacten el marco de referencia legal, aspectos de remuneración, administración de riesgos, procedimientos de auditoría y administración específicos, entre otros procesos específicos.

Es tal la flexibilidad de *IntoSAINT* que puede practicarse a nivel general (toda la EFS, lo cual se recomienda al realizarse el primer ejercicio de autoevaluación), o bien a nivel Unidad, Dirección General, incluso a nivel departamental o áreas específicas.

Adicionalmente, cabe reiterar que *IntoSAINT* es una adaptación hecha por el Tribunal de Cuentas de los Países Bajos de la herramienta original, denominada *SAINT*. Ésta última fue desarrollada por el propio Tribunal de Cuentas de los Países Bajos, en colaboración con el Ministerio del Interior de dicho país y la Oficina de Integridad de la Ciudad de Ámsterdam, para que las organizaciones del sector público evalúen tanto su vulnerabilidad, como su resistencia a violaciones de la integridad. El objetivo ulterior es que las entidades públicas en general dispongan de un instrumento que les permita mejorar su gestión de la integridad institucional.

Esto explica por qué, a pesar de que *IntoSAINT* sea la versión adaptada para beneficio de los miembros de la INTOSAI y de toda la comunidad fiscalizadora mundial, la EFS de los Países Bajos ha sido insistente en su invitación para que las EFS e instancias de trabajo promotores (Comisión Técnica de Prácticas de Buena Gobernanza –CTPBG– en el caso de la OLACEFS), consideren la viabilidad de promover el empleo de *SAINT* entre las entidades públicas de los países de origen, aspecto que podría convenir a los miembros de la OLACEFS –en el ámbito de sus facultades– para continuar sus esfuerzos de fortalecimiento de una cultura de rendición de cuentas y de fiscalización en la región.

Relevancia para la OLACEFS

La Comisión Técnica de Prácticas de Buena Gobernanza (CTPBG) constituye la respuesta institucional que la OLACEFS ha generado para coadyuvar a la lucha regional contra la corrupción y en favor de la promoción de acciones que contribuyan a la buena gobernanza. En este sentido, la Herramienta para la Autoevaluación de la Integridad en las EFS (*IntoSAINT*) constituye un mecanismo apropiado para favorecer que, en el ámbito de ética pública, buena gobernanza y rendición de cuentas en el sector público, las EFS lideren con el ejemplo, como lo estipula la Norma Internacional de Entidades Fiscalizadoras Superiores (ISSAI) 20 de la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI).

En seguimiento a la presentación sobre los beneficios de esta herramienta, expuesta durante la XXII Asamblea General Ordinaria de la OLACEFS, llevada a cabo del 5 al 10 de noviembre de 2012 en Gramado, Brasil, esta iniciativa fue incorporada en el plano de la entonces Comisión Técnica Especial de Ética Pública, Probidad Administrativa y Transparencia (CEPAT). Actualmente, la CTPBG, en colaboración con el CCC, ha incorporado la implementación regional de esta iniciativa en su agenda de trabajo, desde el área temática *Estrategias Efectivas de Probidad Administrativa y Prevención de la Corrupción* de la comisión. De este modo, se impulsa el cumplimiento del **Plan Estratégico 2011-2015 de la OLACEFS**, en particular la estrategia 4 “Productos” de la Meta 1: “Organización Modelo”.

Como se observa, el concepto de integridad cobra relevancia en nuestra organización regional, pues en el quehacer diario de los miembros de la OLACEFS se debe asegurar el permanente cumplimiento de las normas y valores –destacando la integridad–, sobre las que se fundamentan las políticas institucionales, pues éstas son la base para el desarrollo de un clima organizacional abierto a las críticas, transparente, en el que existan espacios para discutir y solucionar conflictos, y en el que la administración lidere con el ejemplo.

La integridad no es un valor cuya responsabilidad sea absoluta de los funcionarios públicos, existe además corresponsabilidad de las organizaciones (particularmente de las EFS) pues éstas son las encargadas de implementar medidas no sólo correctivas, sino principalmente preventivas, a fin de asegurar que su personal no esté expuesto a tentaciones.

Precisamente éste último es uno de los argumentos que sostienen los esfuerzos actuales de la CTPBG por impulsar, desde las EFS, herramientas como *IntoSAINT* que permitan consolidar, en su ámbito de acción, una cultura de respeto hacia los valores éticos, en que debe sustentarse la gestión gubernamental, con la convicción de que tanto la institución como su personal deben anteponer el interés público al particular, asumiendo con ello sus responsabilidades y mandato otorgado.

Como se observa, el proyecto es ambicioso, pues las acciones implementadas y esfuerzos ya iniciados, en consideración del mandato otorgado a las EFS miembros de la OLACEFS, no se agota en la práctica de auditorías, ni tampoco en la emisión de informes y seguimiento correspondiente, sino conlleva un compromiso mayor al ser indispensable la atención a los nuevos desarrollos y a la adopción de las buenas prácticas internacionales, no sólo en materia de fiscalización, sino en un elemento medular: su consolidación como entidades que actúen con ética profesional, que privilegien acciones para incrementar la confianza de la sociedad, se mantengan comprometidas con la calidad de su trabajo, y sean siempre garante del interés público, pese y ante todo debido a los riesgos y vulnerabilidades existentes en el sector público en la región.

PARTE 1: PRINCIPIOS DE LA METODOLOGÍA

I. Concepto de *Integridad*

La integridad no es un concepto fácil de definir. Se utilizan muchas definiciones que se superponen. El término integridad se deriva del latín *in-tangere*, que significa intocable. Se refiere a una virtud, a la de incorruptibilidad y al estado de mantenerse intacto. La integridad está estrechamente relacionada con la ausencia de fraude y corrupción, pero también conlleva valores comunes. En ese sentido, es un concepto positivo y amplio que está relacionado a la ética y a la cultura. *IntoSAINT* usa esta amplia y positiva definición del término de integridad.

Existen cinco dimensiones en torno a las que puede concebirse el concepto de integridad:

1. *Responsabilidad de la Integridad*

Bajo esta concepción, los servidores públicos actúan con integridad cuando observan los valores y normas de la buena administración. La integridad abarca no sólo los requerimientos de incorruptibilidad, sino también valores como la honestidad, sinceridad, sociabilidad, neutralidad, consideración, fiabilidad, orientación al cliente, respeto y objetividad. Un servidor público debe tener cuidado de ejercer sus responsabilidades y usar sus facultades, información y recursos a su disposición, en beneficio del público o del interés general al cual sirve, y comportarse correctamente con sus colegas y el público.

Lo mismo aplica a una organización, que además debe hacer todo lo que esté a su alcance para asegurarse que su personal no sucumba a las tentaciones. Debería, por ejemplo, diseñar procesos de tal forma que los servidores públicos no estén expuestos a tentaciones; evitar hacer demandas irrazonables o imposibles (conflictivas); concientizar al personal –de manera regular y clara– sobre la importancia de la integridad; asegurar que los directivos actúen con el ejemplo, y crear una cultura abierta y transparente, en la cual las críticas sean aceptadas, los errores puedan ocurrir y las cuestiones difíciles puedan ser discutidas. En resumen, la organización debe implementar una política eficaz de integridad.

Por tanto, en esta primera dimensión, la integridad es un producto conjunto: tanto de la correcta administración (gobernanza de la EFS), como de las buenas prácticas de los empleados. Su evaluación se enfoca en los riesgos a la integridad que pueden socavar seriamente la confianza depositada en la organización y, en consecuencia, su imagen y permanencia.

2. *Precondición para la autoridad gubernamental y la confianza pública*

En la segunda dimensión de análisis, la integridad es una precondición para el desempeño eficaz y continuo del sector público. Un gobierno que carece de integridad pierde la confianza del público y, finalmente, también su autoridad. El público debe ser capaz de confiar en el gobierno porque es el único proveedor de muchos servicios básicos, tales como el otorgamiento de pasaportes, licencias y subsidios. Debido a este monopolio y a la dependencia pública, el gobierno debe ser intachable y posicionarse más allá de toda sospecha.

3. *Integridad: no sólo leyes y reglas, también responsabilidad moral*

Integridad significa más que simplemente observar leyes y reglas. La ley es apenas un límite inferior y un punto mínimo de partida moral. Las reglas y leyes no pueden cubrir todas las situaciones. La tensión es mayor cuando no existen reglas o éstas carecen de certeza, como sucede ante situaciones nuevas, complejas y cambiantes. Además, los servidores públicos pueden ser confrontados con un conjunto de valores contradictorios. Precisamente en tales situaciones, y cuando tengan poderes discrecionales, los servidores públicos deben ser capaces de formarse una opinión moralmente aceptable y actuar con responsabilidad de acuerdo con los valores y normas de buena gobernanza.

4. *Política de integridad: no sólo sanción sino sobre todo prevención*

La política de integridad exige una combinación de medidas sancionatorias y de prevención. Por un lado, una organización debe tomar medidas si su personal actúa inapropiadamente (sanción). Por el otro, debe hacer todo lo que pueda para eliminar las tentaciones que pudieran inducir a los servidores públicos a actuar inapropiadamente (prevención). Se debe dar prioridad a la prevención. Esto no sólo es más eficaz sino, en balance, la inversión es muchas veces menor que el costo de reparar el daño causado por conductas inapropiadas: “cada peso invertido en la prevención supera por mucho cada peso erogado para subsanar el daño o falla detectada”.

5. *Política de integridad: no ad hoc sino continua*

La quinta dimensión de análisis señala que la atención prestada a la integridad debe ser permanente. Si la Política de Integridad se relaja cuando las cosas van bien, el riesgo de incidentes incrementa. En otras palabras, la integridad y la Política de Integridad deben integrarse permanentemente a la organización y ser una parte fija de la gestión operativa y de calidad de la entidad. La integridad no puede ser tratada como un proyecto puesto que un proyecto termina y no es continuo. La integridad debe ser un componente estándar en la gestión y en el ciclo de políticas institucionales.

El concepto de integridad y las diferentes formas de enfocar este tema pueden ilustrarse en la siguiente tabla.

Criterio	Enfoque de Cumplimiento	Enfoque de Integridad
Enfoque	Negativo	Positivo
Fundamentación	Basado en reglas: normas impuestas (ley y regulaciones)	Basada en principios: normas y valores compartidos (valores)
Tipo de controles requerido	Controles duros	Controles suaves
Opinión	<i>La gente es mala</i>	<i>La gente es buena</i>
Énfasis	Prevención de las violaciones a la integridad.	Facilitación del buen comportamiento
Enfoque	Legal	Directivo
<i>Modus Operandi</i>	Sancionatorio / reactivo	Preventivo / proactivo

El consenso alcanzado es que el desarrollo y enriquecimiento de las Políticas de Integridad de las Entidades Fiscalizadoras Superiores requiere una combinación bien equilibrada de ambos enfoques para obtener buenos resultados.

La metodología de evaluación presentada en el presente manual ha adoptado el más amplio alcance del concepto de integridad, como se describe en esta sección. Este alcance es más adecuado para un instrumento que se diseñe para uso en el contexto de un enfoque preventivo.

- *La integridad y las EFS.*

Las EFS desempeñan un papel importante al fortalecer la rendición de cuentas y la transparencia, así como la integridad del gobierno y de las entidades públicas. Las EFS deben ser organizaciones modelo que lideren con el ejemplo.¹ Muchas EFS reconocen estos principios y lo reflejan en la formulación de sus misiones. Varias ISSAIs² usan el término *integridad* sin proporcionar una definición exacta, pero es razonable asumir que estas ISSAIs intentan adoptar el ámbito amplio del concepto como lo hace IntoSAINT.

¹ ISSAI X: El valor y beneficio de las EFS – haciendo una diferencia en la vida de los ciudadanos (versión para exposición).

² Por ejemplo, las ISSAIs 30 y 40.

II. Evaluación de riesgos y definiciones relevantes

El análisis de riesgos es un acto reflejo, algo natural en nuestra vida diaria. En cierto grado, estamos programados para analizar el riesgo inherente en cada situación. A menudo lo hacemos inconscientemente, de manera implícita o incluso intuitivamente. Sabemos por nuestra propia experiencia que estamos casi continuamente analizando y ponderando riesgos. El análisis de riesgos puede detenernos a hacer cosas o cambiar la forma en que las enfocamos. Nos pone en alerta para que podamos responder más rápidamente y, por ende, reduzcamos la probabilidad de una desgracia. Evaluamos la naturaleza y seriedad de un riesgo para que podamos tomar las medidas necesarias para impedir o mitigar consecuencias adversas.

Tal ejercicio es importante para nosotros personalmente, pero es vital para las organizaciones. Todas las organizaciones públicas son vulnerables y están expuestas en cierto grado a riesgos a la integridad. Por ello, todas las organizaciones deberían estar conscientes de sus vulnerabilidades y riesgos, para que puedan tomar medidas específicas. Es ilusorio e indeseable pensar que todos los riesgos pueden ser evitados o suprimidos. Eso requeriría de tantas reglas y procedimientos que la organización se volvería inoperante. El análisis de riesgos puede ayudar a decidir qué medidas ayudarán a reducir los principales riesgos de una organización a un nivel aceptable.

1. Definición de riesgos

En la literatura, un riesgo es descrito como la posibilidad o probabilidad de la ocurrencia de cierto incidente indeseable multiplicado por su impacto o el daño que causaría ($\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$). La formulación de un riesgo concreto incluye: evento indeseado (actor, acción, tiempo y lugar), el interés dañado y el daño causado.

Un evento indeseado es algo que puede suceder a toda institución, organización o persona, y causar daño a una situación / posición (deseada). Es causado por circunstancias específicas y/o una acción (no) deliberada.

El daño puede tomar diferentes formas y, por lo tanto, plantea diferentes tipos de riesgo. Por ejemplo, un riesgo político puede ser que una política deseable no sea aceptada por el Congreso, un riesgo de desempeño sería que una organización no alcanzara sus objetivos, y un riesgo financiero sería el que la organización pueda perder dinero. Estos riesgos pueden ser la consecuencia de cualquier circunstancia cambiante, una calamidad, actos de las personas o actos de las propias organizaciones. Las consecuencias se relacionan a las organizaciones, instituciones y/o personas.

2. Riesgos a la integridad

Un riesgo a la integridad es un posible evento indeseado que daña el sector público. El daño en el sector público puede ser definido en términos de pérdida económica, imparcialidad o baja calidad de los servicios y bienes públicos brindados al público en general, pérdida de ingresos tributarios, pérdida pública del respeto o confianza depositada en el gobierno, implicaciones políticas y administrativas, o deterioro del ambiente de trabajo. El común denominador es que el abuso de poder daña la imagen del sector público y socava la confianza pública y la legitimidad del gobierno.

3. Vulnerabilidades

Como se explicó anteriormente, los riesgos concretos se definen específicamente como eventos no deseados, formulados en términos del actor, acción, tiempo, lugar y los daños causados. Las vulnerabilidades se definen en un nivel más elevado de abstracción, indicando las áreas donde los riesgos son más probables de ocurrir. Es útil prestar atención a las vulnerabilidades, ya que proporciona una buena visión de los problemas potenciales y de las alternativas asequibles para abordarlos, sin tener que definir todos los riesgos posibles en detalle.

De la investigación, el conocimiento y la experiencia profesional, se sabe que algunas áreas y actividades en el sector público producen más riesgos a la integridad que otras. Estos son procesos o funciones inherentemente vulnerables. Los procesos en los que hay un contacto intenso con los "clientes" (usuarios, público en general, empresas) son más vulnerables a violaciones, porque hay más oportunidades y tentaciones. Lo mismo puede decirse de los procesos que involucran la gestión de los valiosos recursos públicos.

Además de las características de las actividades del sector público, determinadas circunstancias pueden incrementar la vulnerabilidad a las violaciones de integridad. Éstas se denominan "factores que agravan la vulnerabilidad"; no son los riesgos de integridad en sí mismos, pero pueden elevar considerablemente la vulnerabilidad debido a que:

- Incrementan la probabilidad de que ocurra un incidente;
- Elevan las consecuencias (impacto negativo) de un incidente (no sólo financieramente sino también con respecto a la credibilidad, ambiente de trabajo, relaciones y reputación, entre otros).

Ejemplos de estos factores que aumentan la vulnerabilidad son la complejidad o fragilidad del marco legal, las presiones externas, y la poca lealtad de los empleados.

En conjunto, las áreas inherentemente vulnerables y los factores que agravan la vulnerabilidad constituyen el llamado "Perfil General de Vulnerabilidad" para una organización, entidad, unidad o proceso.

4. Reducción de la vulnerabilidad y mitigación de riesgos

Las organizaciones pueden hacer frente a la vulnerabilidad de diferentes formas. Primero, todas ellas pueden tratar de eliminar o reducir las vulnerabilidades suprimiendo actividades vulnerables. A veces es posible llevar a cabo actividades de una manera diferente, eliminando actividades que son vulnerables a violaciones a la integridad. Esto implicaría que la organización sería capaz de ir al origen de la vulnerabilidad. En la práctica, sin embargo, esto raramente es factible. Las organizaciones públicas tienen obligaciones legales y no pueden evitar comprometerse en actividades sensibles.

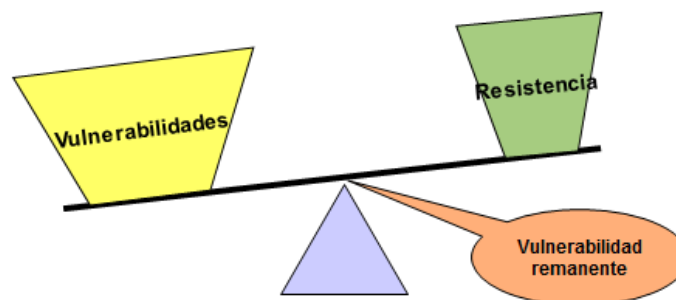
Usualmente, una forma más viable para hacer frente a las vulnerabilidades consiste en diseñar e implementar controles compensatorios (a la integridad). Dado que las vulnerabilidades son diversas en su naturaleza, es importante diseñar un conjunto de controles o incluso, preferiblemente, un Sistema de Controles de la Integridad (SCI) bien equilibrado. Dependiendo del 'nivel de madurez' (robustez) del SCI, la organización es más o menos resistente a las vulnerabilidades que enfrenta en su quehacer cotidiano.

Hasta este punto, se discute la forma en que las organizaciones pueden hacer frente a las vulnerabilidades. Para hacer frente no sólo a las vulnerabilidades, sino también a riesgos más específicos, es necesario analizar la exposición de la organización a estos riesgos específicos. Idealmente, un análisis completo incluiría:

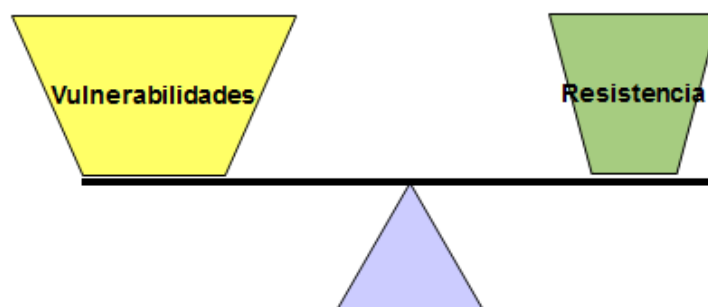
- un análisis de las vulnerabilidades de la organización (áreas vulnerables y factores que agravan la vulnerabilidad);
- un análisis de la resistencia de la organización a dichas vulnerabilidades, las cuales están determinadas por el nivel de madurez del Sistema de Controles de la Integridad (SCI) de la organización;
- un análisis de riesgos específicos de la organización, y
- un análisis de la mitigación de riesgos específicos mediante controles específicos.

Para ser capaz de descubrir los riesgos que no se han abordado apropiadamente, tendremos que ver qué riesgos “brutos” específicos no están cubiertos completamente por el efecto de las medidas compensatorias.

La relación entre vulnerabilidades y controles pueden ilustrarse en los siguientes diagramas. El primero de ellos muestra una relación donde la resistencia no está totalmente balanceada por las vulnerabilidades. Esto implica que existe una vulnerabilidad remanente, indicando que existe todavía espacio para mejoras.



El siguiente diagrama muestra otra situación posible pero que es poco probable de que ocurra en la vida real. Se ilustra la importancia de un enfoque bien balanceado, porque una implementación excesiva de controles de la integridad en contra de las vulnerabilidades debe también evitarse.



III. Principios básicos

La metodología descrita en este *Manual para la Conducción de Autoevaluaciones de la Integridad para las Entidades de Fiscalización Superior* está enfocada en la evaluación de:

- las vulnerabilidades y riesgos de integridad en una Entidad Fiscalizadora Superior (incluye el análisis de áreas vulnerables y factores que agravan la vulnerabilidad);
- la resistencia de la Entidad Fiscalizadora Superior a dichas vulnerabilidades, las cuales están determinadas por el nivel de madurez de su Sistema de Controles de la Integridad (SCI).

Para con ello realizar un análisis de brechas y emitir el informe con las recomendaciones correspondientes para desarrollar o fortalecer, según el caso, la Política de Integridad Institucional en las EFS, y velar por su cumplimiento.

Los principios básicos y las características de *IntoSAINT* se describen a continuación:

- *Orientado a la prevención*
Su metodología de evaluación se enfoca en la prevención. La herramienta no está diseñada para detectar violaciones a la integridad y, en consecuencia, sancionar (reprimir) conductas inaceptables. El método está diseñado para identificar las principales debilidades y riesgos a la integridad, y fortalecer la Política de Integridad Institucional de la EFS con el objetivo de prevenir violaciones futuras.
- *Enfoque: Autoevaluación*
IntoSAINT ha sido designada como una herramienta de autoevaluación. Es una herramienta de auto-diagnóstico presentada como un taller de dos días para 10 a 15 participantes. La autoevaluación significa que la propia organización pone a prueba su grado de resistencia a los riesgos a la integridad. La evaluación aprovecha el conocimiento, experiencia y opiniones del propio personal. Este enfoque se basa en la creencia de que el personal tiene la mejor perspectiva de las debilidades y riesgos institucionales, así como del nivel de madurez de las medidas (controles) de integridad de la EFS. Así, con esta herramienta se revelan las debilidades de la propia organización y el propio personal emite recomendaciones sobre cómo fortalecer la resistencia, bajo la premisa de que existe y se promueve un ambiente organizacional que favorece la pertenencia y compromiso institucional.
- *Moderador del taller*
El taller es encabezado por dos moderadores experimentados, debidamente capacitados para tal efecto. Su rol puede describirse de mejor manera como un supervisor de procesos. El moderador acompaña a los participantes a través de las diferentes etapas del taller, y los guía para identificar eficazmente las principales vulnerabilidades y riesgos, y para formular las recomendaciones de mayor impacto para fortalecer el Sistema de Controles de la Integridad de la EFS en cuestión, con el fin de eliminar o minimizar las vulnerabilidades y los riesgos.
- *Aprendizaje en términos de vulnerabilidad y riesgo*
El método de autoevaluación promueve el pensamiento en términos de vulnerabilidad y riesgo. Durante la autoevaluación, los participantes identifican las principales vulnerabilidades y riesgos, y posteriormente emiten recomendaciones sobre cómo minimizarlos. Pensar en términos de vulnerabilidad y riesgo es una habilidad específica que tiene que ser aprendida para formular una Política de Integridad Institucional equilibrada. Si un organismo auditor tiene relativamente

poca experiencia en esta área, la evaluación puede servir como una primera introducción. Las lecciones aprendidas pueden (y deben), por lo tanto, replicarse para mejorar el enfoque de la organización hacia la integridad.

- *Comprensión del Sistema de Controles de la Integridad*

El método de autoevaluación no sólo identifica las vulnerabilidades a la integridad sino que también se enfoca en la medición del grado de resistencia organizacional a las violaciones de la integridad. Teniendo a la mano un marco de referencia sobre las medidas de integridad idóneas, se evalúa si éstas han sido implementadas, si se observan y si han sido eficaces o no en la EFS en cuestión. Esto genera una buena comprensión de la madurez del Sistema de Controles de la Integridad y de la resistencia organizacional a violaciones a la integridad. Las medidas pueden dividirse en tres grandes categorías:

- (1) controles duros, compuestos de reglas, procedimientos y el diseño de sistemas administrativos y controles internos en el organismo auditor;
- (2) controles suaves, dirigidos a la gestión de la conducta, cultura y actitud del personal;
- (3) controles generales, que tienen un alcance y/o impacto más amplio, por ejemplo: la organización de la Política de Integridad.

- *Informe ejecutivo a la Alta Dirección / Plan de acción*

El producto final del taller de autoevaluación de la integridad (*IntoSAINT*) es un informe ejecutivo (acompañado de un plan de acción en el mejor de los casos). Este reporte explica a la Alta Dirección de la EFS evaluada las medidas que deben ser tomadas para fortalecer su grado de resistencia organizacional a las violaciones de integridad. El que el titular del organismo auditor y su Consejo de Dirección o altos mandos preste atención a los hallazgos y recomendaciones resultantes, contribuye a la consolidación de la Política de Integridad Institucional.

- *Concientización general de la integridad*

Además de proveer una comprensión concreta de las vulnerabilidades y debilidades vinculadas con la integridad, y de emitir recomendaciones para fortalecer la resistencia organizacional (el SCI), *IntoSAINT* puede contribuir a incrementar significativamente la conciencia del personal de la EFS sobre la integridad. Asumir un enfoque intenso y colectivo sobre el tema, como sucede con la autoevaluación, permite que la mente de los participantes se interese en las razones que sustentan la importancia de la integridad. Las discusiones colectivas de los participantes sobre la importancia y relevancia de la integridad antes, durante y después del taller son de gran valor. Los participantes transmiten sus hallazgos por toda la organización.

IV. Esbozo del método de evaluación

La metodología de autoevaluación de la herramienta *IntoSAINT* consiste en cinco pasos distintos:

1. Análisis e identificación del objeto y procesos clave

El primer paso es definir el *objeto* de la evaluación y analizar los *procesos* relevantes. El objeto puede ser toda la Entidad Fiscalizadora Superior (indispensable en el primer ejercicio) o bien una unidad, Auditoría Especial o departamento específico (recomendable sólo en etapas subsecuentes).

Para el objeto seleccionado, se tiene que preparar una lista de procesos primarios, secundarios y de gestión o control. La calidad de la lista determinará el curso siguiente de la evaluación. Además de estar completa, la lista debe indicar los procesos clave para que puedan ser reconocidos y comprendidos por los participantes del taller, sin ser demasiado detallada. La especificidad excesiva e indefinición de procesos llevan a la incertidumbre y deben ser evitadas.

2. Evaluación de las vulnerabilidades

En esta segunda fase, se estima la *vulnerabilidad*, por ejemplo: la exposición potencial a violaciones a la integridad de los procesos señalados en la etapa 1. Esta fase se divide a su vez en cuatro sub-etapas:

1. Vinculación de la lista de los procesos a una visión general de los procesos en el sector público que se sabe son vulnerables a violaciones a la integridad;
2. Consideración de la presencia o ausencia de factores que agravan la vulnerabilidad;
3. Generación de una visión general y un perfil de evaluación completo de la vulnerabilidad percibida, e
4. Indicación de los procesos más vulnerables.

3. Evaluación del nivel de madurez del Sistema de Controles de la Integridad

En esta etapa los participantes evalúan el nivel de madurez (robustez) de las medidas de integridad que, en conjunto, forman el *Sistema de Controles de la Integridad* (SCI) de la organización. El sistema se divide en 16 grupos, dividiéndose éstos en tres bloques (controles generales, duros y suaves). En el capítulo correspondiente se abordarán las siguientes sub-etapas con mayor detalle:

1. Breve introducción al Sistema de Controles de la Integridad, compuesto por medidas, grupos y categorías;
2. Breve introducción a los niveles de madurez;
3. Evaluación del nivel de madurez de todas las medidas, tras asignarles puntajes, y
4. Resumen y análisis de los puntajes para producir un promedio por grupo y bloque. Esto permite identificar qué grupos y bloques de controles de integridad son relativamente duros o débiles.

4. Análisis de Brechas

En esta etapa del taller se revela la conexión entre las vulnerabilidades (fase 2) y el nivel de madurez del Sistema de Controles de la Integridad (fase 3). El análisis debe claramente mostrar las vulnerabilidades restantes (no abordadas aún), después de haberse confrontado las vulnerabilidades con las medidas de control relevantes en el Sistema de Controles de la Integridad.

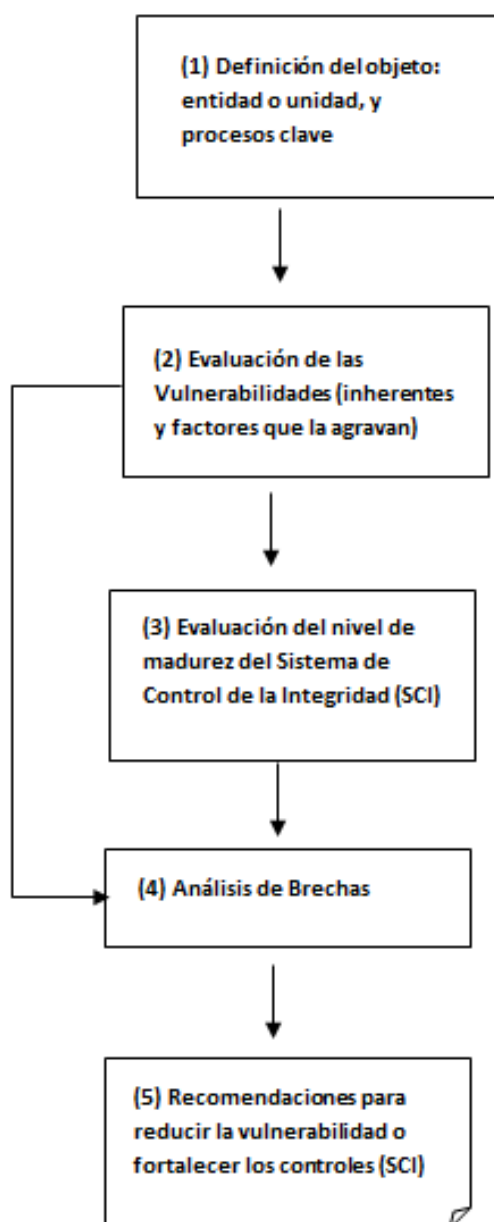
El análisis de brechas se puede extenderse al nivel de riesgos específicos por proceso vulnerable, para proporcionar recomendaciones más detalladas a la alta dirección.

5. Informe y recomendaciones a la Alta Dirección

Las etapas 1 a 4 antes descritas proporcionarían los insumos para generar el informe de la autoevaluación.

La pregunta central es qué medidas son las más apropiadas para robustecer los procesos más vulnerables. Los resultados de este ejercicio integran el insumo principal para generar el informe de la evaluación, así como las recomendaciones para fortalecer la resistencia del SCI contra los riesgos de integridad.

El siguiente diagrama presenta una visión esquemática de la metodología de la autoevaluación de *IntoSAINT*.



PARTE 2: GUÍA DE INSTRUMENTACIÓN DEL TALLER

V. Preparación

Esta sección proporciona una guía y explicaciones relevantes para los moderadores de un taller de autoevaluación (*IntoSAINT*). Se requiere de dos moderadores expertos, quienes conducirán el taller (uno sería insuficiente dadas las dinámicas y orientación prevista). Ellos son también los responsables de preparar cuidadosamente el taller de autoevaluación y de integrar posteriormente los resultados (hallazgos y recomendaciones de los participantes) en el reporte de la autoevaluación a ser presentado a la Alta Dirección.

Además de la guía incluida en esta sección del *Manual para la Conducción de Autoevaluaciones de la Integridad para las Entidades de Fiscalización Superior*, está disponible un *kit* de herramientas (traducidas también y adaptadas por la ASF), que incluye presentaciones y una hoja de cálculo para apoyar a los moderadores y a los participantes del taller en la implementación del método de autoevaluación.

- *Coordinación*

Antes de iniciar la autoevaluación, se requiere realizar ciertas acciones y contar con determinadas condiciones. Se debe garantizar (no asumir) que habrá alguien al interior de la Entidad Fiscalizadora Superior Local quien fungirá como coordinador, contacto durante la autoevaluación, y enlace con la Alta Dirección. Éste puede ser alguien de un área operativa o de personal de apoyo, pero deberá tener la capacidad, recursos y tiempo de comunicarse fácilmente con el moderador y con las áreas pertinentes en la EFS.

- *Apoyo de la Alta Dirección*

El primer paso es obtener el respaldo y apoyo del Titular de la EFS. A veces la Alta Dirección es la que toma la iniciativa respecto a la autoevaluación, pero también puede ser una iniciativa de un departamento de auditoría, de un área de apoyo o bien de una parte interesada externa. Es importante que la Alta Dirección reconozca que la integridad es una responsabilidad suya. El alcance de la autoevaluación debe estar claro y no debería realizarse una autoevaluación sin el conocimiento, apoyo y previo involucramiento de la Alta Dirección (se sugiere realizar una presentación introductoria).

- *Selección del objeto*

El segundo paso es decidir cuál será el objeto de la evaluación. Usualmente éste es la Entidad Fiscalizadora Superior como un todo, pero también puede ser una unidad específica. La responsabilidad de la Alta Dirección debe estar clara y, preferentemente, ésta debe involucrarse en la selección del objeto. Se sugiere que el primer ejercicio de autoevaluación en la EFS se haga a toda la institución, no a un área en particular.

Es importante hacer un inventario de los procesos relevantes antes de que inicie el taller. Al empezar éste, se mostrará a los participantes la lista propuesta y se les preguntará si deberían hacerse correcciones o adiciones.

La determinación de los procesos clave es responsabilidad de los participantes. Es de suma importancia la orientación de los moderadores, pues la calidad del listado determinará el curso de la autoevaluación. No existen procesos estándares a todas las EFS miembros de la ASOFIS; cada instancia podrá generar su propia lista, de conformidad con sus propias prioridades y necesidades.

Cabe señalar que ejercicios posteriores de autoevaluación no necesariamente tendrían que realizarse en torno al mismo listado, pues tampoco es indispensable disponer de los mismos participantes.

- *Selección de participantes*

El tercer paso es seleccionar un grupo de empleados, los cuales estén familiarizados con el quehacer de la EFS (o de la unidad) y de los procesos que deben ser evaluados. Por razones prácticas, el grupo no debería ser mayor a 15 personas. Es importante generar un ambiente de confianza que permita que los participantes se sientan libres de expresar sus opiniones y experiencias. Por lo tanto, es aconsejable evitar una combinación de subordinados y superiores en el mismo grupo. La participación en el taller debería ser de manera voluntaria.

- *Planeación*

El taller en sí mismo requiere de dos días, incluyendo una sesión introductoria. Es importante que el grupo pueda pasar estos días sin perturbaciones, por lo que una locación externa es ideal. Durante la sesión introductoria habrá tiempo para explicar el objetivo y la naturaleza de la autoevaluación, así como para discutir el concepto de integridad. Es importante que los participantes entiendan que el taller se enfoca en lo que ellos puedan decir acerca de los riesgos de integridad y de la resistencia contra violaciones a la integridad. La confidencialidad también debe destacarse.

- *Interacción*

Es importante tener discusiones libres durante el taller. La discusión enriquecerá los resultados. También contribuirá a aumentar la conciencia sobre la integridad y la herramienta *IntoSAINT*. Una forma de estimular la discusión es trabajar en parejas o en grupos pequeños durante los pasos del taller.

- *Informe*

Se pondrá a disposición un modelo (formato) de reporte, que puede usarse durante y después del taller, de tal forma que la preparación del reporte para la Alta Dirección no requiera de mucho trabajo adicional. La presentación de los resultados a la Alta Dirección debe abarcar las vulnerabilidades, el Sistema de Controles de la Integridad y el análisis de brechas. La atención debe centrarse en las mejoras y las recomendaciones: el plan de acción.

Para elevar el grado de concientización en toda la organización, la comunicación es vital. La intención de llevar a cabo una autoevaluación y los resultados del taller (incluido el plan de acción) deberían ser ampliamente comunicados dentro de la organización.

VI. Definición del objeto y procesos

a. Introducción

En esta parte del taller, las siguientes preguntas son esenciales:

1. ¿Se evaluará toda la Entidad Fiscalizadora Superior o sólo una parte de ella?
2. ¿Qué tareas son ejecutadas por el organismo auditor (o parte relevante del mismo)?
3. ¿Qué procesos organizacionales son vitales?

La evaluación se enfoca en los procesos clave de una organización o unidad de ésta. El objeto de la evaluación debe estar bien definido y claramente ligado a la responsabilidad de la Alta Dirección.

La identificación de procesos es una parte clave de la metodología de la evaluación. Este paso debe ser preparado antes de que inicie el taller. Muchas organizaciones tienen sólo un número limitado de procesos centrales. Para identificar estos procesos, tiene que considerarse la relevancia de la organización y el uso que haga ésta de los recursos. Los procesos centrales son a menudo relacionados a los deberes (mandato legal) de la organización. Las entrevistas con la Alta Dirección y con el personal ayudarán a identificar qué procesos son considerados importantes o incluso vitales para la organización. La lista de procesos debe estar completa, pero no ser demasiado detallada. La lista debe formularse de manera tal que todos puedan entender y reconocer la importancia de los procesos.

Los moderadores son responsables de guiar al grupo y a los participantes del taller, por la lista de procesos preparada, y de asegurarse de que la lista esté completa, es decir, incluya procesos primarios, secundarios y de gestión que contribuyen en conjunto a las tareas vitales de la organización o unidad organizacional. Se recomienda limitar el número de procesos a aproximadamente 10 a 15 procesos para evitar demasiado detalle. Al inicio del taller, los moderadores solicitarán que los participantes estén de acuerdo con la lista de procesos pre-seleccionados, haciendo algunas modificaciones en caso de ser necesario.

Las conclusiones de este paso deben incluirse en el informe para la Alta Dirección.

Los procesos pueden ser categorizados de la siguiente manera:

- *Procesos primarios,*
- *Procesos secundarios, y*
- *Procesos de gestión y control.*

La evaluación debe centrarse en los procesos vulnerables *primarios y secundarios*. Por su naturaleza, los procesos de gestión y control son menos vulnerables, pero en algunos casos éstos deben de ser considerados.

Cuando la evaluación se aplica a una *unidad organizacional* del organismo auditor (por ejemplo, un departamento en particular), será usualmente suficiente considerar solamente los procesos primarios y secundarios. La selección de procesos debería considerar sólo aquellos procesos (o sub-procesos) que realmente tengan lugar dentro de la unidad.

Cuando la evaluación se aplique al organismo auditor en su totalidad, los procesos de gestión y control son de interés y deberían de ser incluidos en la evaluación.

Las siguientes secciones proporcionan mayor información sobre los distintos tipos de procesos (primarios, secundarios, y de gestión y control), típicos para las Entidades Fiscalizadoras Superiores.

b. Procesos Primarios

Los procesos primarios son los procesos centrales de la organización. Un proceso primario puede definirse como “un método para convertir recursos (dinero, personal, información, etc.) en productos y servicios que logren las tareas y metas de la organización”. No hay una clasificación generalmente aceptada de procesos primarios. Éstos son altamente específicos al tipo de organización.

Teniendo en cuenta el conocimiento existente sobre la naturaleza de las Entidades Fiscalizadoras Superiores y los procesos dentro de éstas, puede considerarse válida la siguiente pre-selección de procesos primarios relevantes para la mayoría de las EFS:

- Monitoreo del ambiente de auditoría (por ejemplo: recopilación de información y comunicación con las partes interesadas);
- Procesos de auditoría (planeación, ejecución, provisión de reportes, emisión de dictámenes de auditoría, archivo, comunicación, control de calidad, seguimiento, etc.);
- Procesos de desarrollo (métodos de desarrollo, creación de capacidades, etc.);
- Actividades interinstitucionales (por ejemplo: conducción de auditorías conjuntas o en coordinación, mantenimiento de relaciones interinstitucionales y contribución a eventos de capacitación regional, nacional e internacional).

c. Procesos secundarios

Un proceso secundario puede definirse como “un proceso que directa o indirectamente facilita los procesos primarios”. Para referencia de las EFS miembros de la ASOFIS, hemos clasificado los procesos secundarios de la siguiente manera:

- Gestión de personal (recursos humanos),
- Gestión financiera,
- Gestión de información,
- Gestión de las instalaciones.

Estos procesos pueden dividirse en procesos subsidiarios, como se muestra a continuación (para fines ejemplificativos). Queremos destacar, sin embargo, que la propia EFS debe clasificar sus propios procesos subsidiarios:

1. Gestión de personal (recursos humanos):
 - a) reclutamiento y selección,
 - b) capacitación,
 - c) remuneración,
 - d) clima organizacional (condiciones de trabajo / salud y seguridad).
2. Gestión financiera:
 - a) presupuestación,
 - b) contabilidad,
 - c) gestión de fondos.
3. Gestión de la información:
 - a) desarrollo de sistemas de información,
 - b) mantenimiento de los sistemas de información,
 - c) acceso / continuidad de los sistemas de información,
 - d) colección de datos, entrada, almacenamiento y distribución.

4. Gestión de las instalaciones:
- a) administración del complejo de instalaciones,
 - b) abastecimiento de bienes y servicios,
 - c) equipamiento e instalaciones de tecnologías de información,
 - d) transporte.

d. Procesos de Gobernanza

Los procesos de gobernanza están íntimamente relacionados con los procesos de gestión y control.

Existen muchas definiciones sobre la gestión interna y el control.

La gestión interna puede definirse como “el proceso de dirigir una organización para alcanzar los objetivos de la política establecidos”. A un nivel organizacional, esto implica:

- 1) el diseño de la estructura organizacional;
- 2) el diseño e implementación del ciclo de planificación en los niveles estratégico, táctico y operativo;
- 3) comunicación con partes externas.

El control interno puede definirse como “el proceso de introducir e implementar un sistema de medidas y procedimientos para determinar si el desempeño de la organización es y se mantendrá en acuerdo con los planes y medidas correctivas acordadas para alcanzar los objetivos de la política”. A un nivel organizacional, esto implica:

1. análisis de riesgos y de gestión,
2. controles internos,
3. comunicación interna del efecto de los controles internos,
4. revisiones periódicas del progreso en respuesta a los informes a la Alta Dirección y medidas de seguimiento/cambios,
5. monitoreo de la correcta operación del sistema de control interno.

Para las EFS, los procesos de gobernanza importantes están relacionados con, por ejemplo:

- la estrategia: formulación de la misión y estrategia (a largo plazo), programación de auditorías y otras actividades, estrategia de comunicación, gestión de relaciones;
- la gestión organizacional: estructura organizacional, mandatos, supervisión, auditoría interna, y
- el Titular de la EFS y su Consejo Directivo: nombramiento y remuneración, relaciones de la Alta Dirección, etc.

VII. Evaluación de las vulnerabilidades

a. Introducción

Esta parte del taller se enfoca en el perfil de vulnerabilidad, para lo cual se deben responder las siguientes preguntas:

- ¿Cuáles son las vulnerabilidades inherentes?
- ¿Cuáles son los factores que agravan o incrementan la vulnerabilidad?
- ¿Cuál es el perfil de vulnerabilidad global?

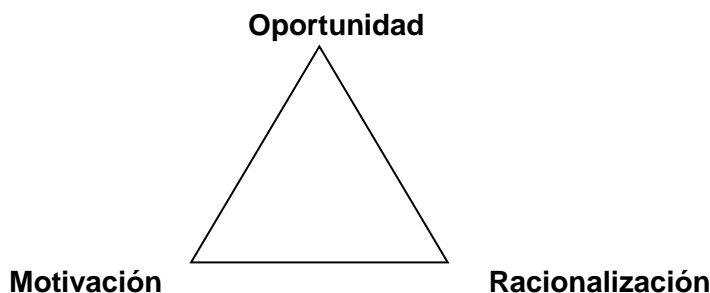
El perfil de vulnerabilidad se evalúa a través de un número de subetapas independientes. Primero, se consideran las vulnerabilidades inherentes de la organización y los factores que agravan la vulnerabilidad. Posteriormente, se evalúa el nivel de vulnerabilidad usando un modelo de puntuación. Aunque en general el nivel de vulnerabilidad es difícil de estimar y puede tener elementos subjetivos, esta metodología proporciona un enfoque relativamente simple y objetivo, categorizando el nivel de vulnerabilidad en bajo, medio y alto. Las vulnerabilidades inherentes y los factores que agravan la vulnerabilidad constituyen, en conjunto, el 'Perfil de Vulnerabilidad'. Los resultados de esta evaluación se incluyen en el informe a presentar a la Alta Dirección.

b. Vulnerabilidades y tentaciones

La mayoría de los servidores públicos que cometen una violación a la integridad no tenían la intención de hacerlo cuando entraron por primera vez al servicio público. Muchos sucumben a las tentaciones que ellos mismos enfrentan en la organización. Las tentaciones pueden ser tangibles (dinero, privilegios) o intangibles (estatus, reconocimiento, protección); también hay "tentaciones inversas", tales como amenazas y chantaje. A mayor tentación, es más probable que sucumbamos. Como sea posible, las tentaciones deberían de reducirse o eliminarse, y los servidores públicos deberían estar blindados ante la tentación.

Ceder a la tentación nunca debe ser tolerado. Los servidores públicos son personalmente responsables de sus acciones. Al concebir una violación como el "acto de sucumbir a la tentación", queda claro en qué dirección deben tomarse medidas preventivas. En gran medida, las violaciones pueden evitarse si se eliminan las tentaciones. Por lo tanto, un aspecto clave del análisis de riesgos es identificar las tentaciones. El análisis de riesgos no sólo revela cómo el personal puede dañar a la organización, sino además identifica las debilidades en la protección ofrecida por la organización.

En el contexto de la prevención del fraude, un concepto bien conocido es el llamado "triángulo del fraude".



La **oportunidad** se refiere a la posibilidad de cometer un fraude. Para que ocurra un fraude, debe existir esta posibilidad. Por lo tanto, quitar la oportunidad es una medida de prevención fuerte.

La **motivación** se relaciona a la tentación o presión percibida para cometer un fraude. Como se mencionó anteriormente, puede ser posible identificar las tentaciones y eliminarlas.

Finalmente, la **racionalización** es el argumento que ha elaborado un defraudador para justificar su comportamiento bajo las circunstancias dadas. Para una organización es posible tener influencia en este proceso de justificación. Por ejemplo, una racionalización puede ser que la cultura en la organización es una justificación para cometer fraude o corrupción. Si la organización ha invertido demasiado en iniciativas de concientización y en programas culturales, este argumento fallará y los defraudadores potenciales estarán más inclinados a ser leales a la organización.

Durante el taller, los participantes explorarán las oportunidades existentes dentro de su organización que pueden guiar a tentaciones (vulnerabilidades inherentes). Una parte importante de este análisis es la exploración de las condiciones para una posible motivación y justificación (racionalización), la cual puede disminuir el umbral de las violaciones a la integridad (factores que agravan la vulnerabilidad, tema que será abordado en la sección “d” de este capítulo).

c. Evaluación de las vulnerabilidades inherentes

Algunas funciones o procesos en el sector público son más vulnerables que otras a la comisión de violaciones a la integridad que otras. Éstos son procesos o funciones inherentemente vulnerables. Por ejemplo, el abastecimiento o el otorgamiento de subsidios son más vulnerables a violaciones a la integridad que las funciones de enseñanza o archivo documental.

Estos procesos vulnerables se resumen en la siguiente tabla:

	Áreas /actividades /acciones vulnerables	
<i>Relación de la entidad con su entorno</i>	Contratación	Abastecimiento / adquisiciones, licitaciones, pedidos, órdenes de compra, asignaciones, concesión de contratos
	Pago	Subsidios, beneficios, prestaciones, subvenciones / becas, patrocinios
	Concesión / Expedición	Permisos, licencias, documentos de identidad, autorizaciones, certificados
	Regulación	Requisitos / condiciones para obtener permisos, establecimiento de normas/criterios
	Auditoria / Inspección	Supervisión, vigilancia, control, inspección, auditoria
	Aplicación de la ley	Acusación o promoción de responsabilidades / juicio, imposición de sanciones / penas

	Áreas /actividades /acciones vulnerables	
<i>Gestión de la propiedad publica</i>	Información	Seguridad nacional, información confidencial, documentos, expedientes, derechos de autor
	Dinero	Tesorería, instrumentos financieros, gestión de cartera, dinero en efectivo/cuentas bancarias, primas, gastos, bonificaciones, prestaciones, etc.
	Bienes	Compra/venta, administración y consumo (acciones, equipos de cómputo)
	Bienes raíces	Compra/venta

Los procesos clave identificados en la entidad sujeta a evaluación, que tienen una o más de estas características son vulnerables a violaciones a la integridad. La columna de la izquierda contiene dos elementos característicos que deben de tomarse en cuenta al evaluar la vulnerabilidad.

- Los procesos en los cuales hay un contacto intensivo con “clientes” o relaciones externas prueban ser más vulnerables a incidentes porque hay más oportunidades y tentaciones. Los clientes pueden tener un considerable interés (financiero) en las actividades o servicios del gobierno. Esto implica que puede existir la tentación para sobornar a servidores públicos o manipular a los tomadores de decisiones del gobierno de una forma favorable para el cliente. Esto también crea tentaciones en los servidores públicos para aceptar o pedir favores.
- La administración de recursos públicos es también un área vulnerable. Una propiedad valiosa es vulnerable a robo o pérdida. Esto incluye no sólo dinero, muebles o bienes raíces, sino también la información como un bien público valioso.

Explicación por vulnerabilidad inherente

- a) Vulnerabilidades inherentes derivadas de la relación de la entidad con su entorno
- **Contratación**
Esto incluye principalmente la adquisición pública de bienes y servicios. Este tipo de actividad hace al gobierno vulnerable al fraude, corrupción, conflictos de interés y competencia desleal.
 - **Pagos**
El sector público paga por varias razones, por ejemplo subsidios, becas, beneficios (sociales) y prestaciones. Esto crea una vulnerabilidad debido a que los pagos pueden hacerse a beneficiarios que no tengan derecho a ellos. Hay riesgo de fraude, corrupción o conflictos de interés. No sólo los procedimientos para establecer la elegibilidad de pagos son vulnerables, sino también los propios procesos de pago.
 - **Concesión / expedición**
Por ley o regulación, el gobierno tiene el deber de otorgar o emitir licencias, permisos, pasaportes, credenciales de identidad, etc. Esto puede ser tan importante para ciertos

individuos o compañías que puede provocar una influencia indebida (soborno, por ejemplo) a servidores públicos, en el caso particular de que se prevea que la licencia o permiso pudiera no ser concedida. Esta vulnerabilidad se incrementa si los salarios de los servidores públicos son relativamente bajos en comparación con el valor de licencias y permisos.

- **Regulación**

Establecer normas y formular condiciones son actividades gubernamentales que pueden ser vulnerables al cabildeo e influencia indebida. Las compañías, por ejemplo, pueden beneficiarse demasiado cuando las normas les son favorables y desfavorables para los competidores. Al respecto, la vulnerabilidad de 'regulación' es comparable con la vinculada con la 'concesión / expedición'.

- **Auditoría / Inspección**

Las inspecciones y auditorías son usualmente llevadas a cabo por el gobierno para proteger los intereses vitales, por ejemplo: velar por la seguridad pública y por los intereses financieros. Los resultados de las inspecciones y auditorías pueden tener un impacto considerable en las partes involucradas. Los inspectores y los auditores son, por lo tanto, vulnerables a influencias indebidas. Pueden ser tentados a limitar el alcance de sus inspecciones y auditorías, o emitir un dictamen más favorable.

- **Aplicación de la ley**

El sector público tiene deberes y responsabilidades únicas para hacer cumplir las leyes y regulaciones. Esto incluye, por ejemplo: investigaciones, procesos de juicio / promoción de responsabilidades y sanciones. Obviamente, esto tiene un impacto considerable en las partes involucradas así que los servidores públicos que ejecutan estas tareas pueden estar bajo presión o estar sujetos a tentaciones. Estos procesos son vulnerables a la manipulación o conflictos de interés, pero también a la intimidación o influencia indebida. El hecho de que la aplicación de la ley implique el tratar con infractores y otros que no acaten la ley, incrementa la exposición a vulnerabilidades.

b) Vulnerabilidades inherentes derivadas de la gestión de propiedad pública

- **Información**

En la ejecución de sus deberes, el gobierno obtiene, procesa y suministra información, incluyendo aquella sensible acerca de, por ejemplo: amenazas de seguridad, defensa, impuestos y salud. En buena medida, esto implica información secreta o confidencial. La revelación sin autorización de tal información podría causar daño a los intereses del gobierno y al interés de aquellos a los que concierna. Por lo tanto, el mantenimiento de bases de datos y el procesamiento de información son actividades vulnerables. Los servidores públicos que tienen acceso a información sensible pueden ser corrompidos para proporcionar esta información a personas que no están autorizadas a acceder a ella. La información confidencial acerca de las compañías puede ser comercializada (con conocimiento de alguien con acceso a información privilegiada) en la bolsa de valores o bien, mal empleada para ganar una ventaja competitiva.

○ **Dinero**

Los procesos que implican el manejo o custodia de dinero poseen una alta vulnerabilidad al fraude. Esto aplica al dinero en efectivo, cuentas bancarias y algunos activos financieros de corto plazo, como las cuentas por cobrar. El dinero es generalmente más vulnerable que los bienes, pues puede ser gastado inmediatamente para cualquier propósito. Los bienes no siempre son fáciles de convertir en dinero. Esto requiere vender los bienes o la propiedad, lo cual significa usualmente que una tercera parte tiene que estar involucrada.

○ **Bienes muebles**

Debido a la escala de sus actividades, el gobierno consume y maneja volúmenes substanciales de bienes muebles y consumibles, por ejemplo: equipos de cómputo, inventario y vehículos. Los proveedores de bienes tienen un interés en adquirir contratos rentables con el gobierno, lo cual crea una vulnerabilidad (ver también “contratación”). La administración de bienes muebles y consumibles valiosos es también vulnerable a violaciones a la integridad, especialmente bienes que son fácilmente comercializables (por ejemplo, computadoras y teléfonos). Vender la propiedad del gobierno puede crear el riesgo de que la propiedad sea vendida a un precio muy bajo, debido a la manipulación por parte del comprador.

○ **Bienes raíces**

El gobierno posee y emplea tierras, edificaciones e infraestructura pública. En casi todos los casos, esto involucra intereses financieros considerables. Comprar, vender y administrar bienes raíces por lo general recae en manos de un pequeño grupo de servidores públicos especializados. Esto hace los procesos de bienes raíces vulnerables al fraude, a corrupción y a conflictos de interés.

Evaluación de las vulnerabilidades inherentes

Para evaluar el nivel de vulnerabilidad inherente, los participantes del taller deben cruzar la lista de procesos organizacionales vitales (abordados en el capítulo 6), con la lista de áreas inherentemente vulnerables, e identificar qué vulnerabilidades están presentes en su EFS. El grado de vulnerabilidad se indica empleando el método de puntuación siguiente.

Puntuación	Importancia para los procesos / actividades de la EFS
0	No Importante o casi irrelevante
1	Moderadamente relevante
2	Importante
3	Muy Importante

El nivel de vulnerabilidad inherente puede ser bajo, medio o alto, según los criterios siguientes:

Puntuación Media	Nivel
Promedio ≤ 0.8	Bajo
$0.8 < \text{Promedio} \leq 1.6$	Medio
Promedio > 1.6	Alto

El resultado debe incluirse en el informe a la Alta Dirección.

d. Factores que agravan la vulnerabilidad

Además de las características de una función o proceso vital para una entidad, ciertas circunstancias o factores pueden agravar o aumentar la vulnerabilidad a la comisión o presencia de violaciones a la integridad. Estos factores pueden agravar o incrementar las vulnerabilidades inherentes debido a que:

- incrementan la probabilidad de que ocurra un incidente, y
- agravan las consecuencias (impacto) de un incidente (no sólo financiero, sino también con respecto a la credibilidad, ambiente de trabajo, relaciones, imagen institucional, etc.)

En consideración de la metodología propuesta por *IntoSAINT*, los factores que agravan la vulnerabilidad se clasifican en cinco grupos, mostrados a continuación:

1. Complejidad del entorno,
2. Cambio / dinámica institucional,
3. Actitud de la Alta Dirección,
4. Personal y
5. Historial del problema / antecedentes.

Ejemplos de los factores o circunstancias que agravan la vulnerabilidad se observan, por grupo, en la siguiente tabla:

1. Complejidad
1.1 Innovación / sistemas (computacionales) avanzados
1.2 Legislación compleja
1.3 Estructuras (legales / fiscales) especiales
1.4 Burocracia (interna y externa)
1.5 Cabildeo político
1.6 Redes de relaciones
1.7 Combinación de intereses de los sectores público y privado (comercio / competencia)
1.8 Necesidad de contar con asesoría / pericia externa
1.9 Influencia / intervención política
2. Cambio / dinámica institucional
2.1 Organización joven
2.2 Legislación frecuentemente cambiante

2.3 Fuerte crecimiento o reducción de la organización
2.4 Privatización
2.5 Subcontratación
2.6 Crisis (reorganización, amenazas organizacionales con un fuerte impacto, supervivencia de la organización o trabajo en riesgo)
2.7 Presión externa (presión sobre el desempeño/resultados, gastos, tiempo; presión política; escasez / desequilibrio de los recursos en consideración de las tareas a cargo)
3. Alta Dirección
3.1 Dominante
3.2 Manipuladora
3.3 Formal / burocrática
3.4 Operación aislada
3.5 Remuneración fuertemente dependiente del desempeño/resultados
3.6 No comprometida con la rendición de cuentas
3.7 Ignora consejos / asesoría / señales
3.8 Respuesta defensiva ante críticas o quejas/demandas
4. Personal
<i>Ambiente de Trabajo / Lealtad</i>
4.1 Presión sobre el desempeño/resultados, ingresos dependen del rendimiento
4.2 Bajo estatus / falta de autoestima / bajos incentivos organizacionales / bajas perspectivas de crecimiento profesional
4.3 Condiciones de trabajo inadecuadas
4.4 Cargas de trabajo elevadas
4.5 Lealtad de grupo
4.6 Poder para obstaculizar
<i>Individual</i>
4.7 Tener otros intereses (empleo alternativo/secundario, etc.)

4.8 Deudas personales
4.9 Estilo de vida (extravagante o con gastos excesivos)
4.10 Secretos personales (vulnerabilidad ante chantajes)
4.11 Amenazas personales
4.12 Adicciones (alcohol, drogas)
5. Historial del problema / antecedentes
5.1 Quejas, denuncias
5.2 Chismes y rumores
5.3 Señales / denunciadores (<i>soplones</i> , informantes)
5.4 Incidentes previos (reincidencia)
5.5 Problemas administrativos (atrasos laborales, inconsistencias, tendencias anormales, etc.)

Muchos de los factores antes mencionados generan o dan pie a oportunidades, motivaciones o justificaciones (racionalización³) para violar la integridad. Cabe señalar que pueden existir otros factores que también agraven la vulnerabilidad; la metodología *IntoSAINT* bien podría no incluirlos, pero los reconoce como indicadores de una cultura de integridad (potencialmente) débil en una organización.

A continuación se proporciona una explicación para cada categoría.

Complejidad

Estructuras y sistemas complejos no son transparentes y representan una oportunidad para el fraude. A su vez, en ambientes complejos resulta más fácil ocultar acciones fraudulentas o suprimir signos que denoten brechas de integridad. Una legislación compleja se refiere a leyes que regulan (el trabajo de) la EFS en sí misma. La burocracia se refiere a procedimientos y reglamentos internos. El cabildeo, la influencia política o las intervenciones del sector privado deben ser evaluados considerando su posible influencia sobre los procedimientos y comportamientos internos.

Cambio / dinámica institucional

Los cambios en una organización o en su ambiente puede elevar la inestabilidad de la misma. Como en el caso de la complejidad, esto puede representar una oportunidad para cometer fraude. Cambios y ambientes dinámicos pueden llevar a la incertidumbre, insatisfacción y frustración entre los empleados, dando incentivos o una racionalización para el fraude u otras brechas de integridad. Una organización joven se refiere al tiempo de existencia de la propia organización, no a la edad promedio de su personal.

Alta Dirección

La actitud y comportamiento de la alta dirección puede agravar la vulnerabilidad debido a su influencia en la cultura organizacional. Además, puede dañar la resistencia de la organización frente a brechas de

³ En los términos concebidos para el análisis del Triángulo del Fraude.

integridad si los directivos no prestan la atención adecuada a controles necesarios o no aplican medidas de control a ellos mismos. Quien es visto como parte de la alta dirección depende del objeto de la autoevaluación: la EFS en su conjunto o unidades de la misma.

Personal

Diferentes circunstancias al interior de una organización impactan negativamente la lealtad del personal. Esto puede dar motivos para el fraude u otras brechas de integridad. A su vez, circunstancias individuales no relacionadas directamente con la organización (por ejemplo, estilos de vida personales o adicciones) pueden dar incentivos para brechas de integridad.

Historial del problema / antecedentes

Si una organización tiene un historial de un problema, sucede que problemas recurrentes tienden a ocurrir de nuevo relativamente. En muchos casos las brechas de integridad señalan debilidades estructurales existentes en una organización o en el sector donde ésta opera. A su vez, debilidades existentes en controles y en la cultura organizacional son difíciles de arreglar. En muchos casos, las organizaciones no aprenden de los incidentes del pasado.

Es importante destacar que la presencia de uno o más de estos factores no implica que existan violaciones a la integridad. Implica, únicamente, que la organización es más vulnerable y que hay un riesgo mayor para la comisión o presencia de violaciones a la integridad.

La relevancia de cada factor o circunstancia que agrava la vulnerabilidad se evalúa utilizando un modelo de puntuación similar al empleado para las vulnerabilidades inherentes. Los participantes en el taller de autoevaluación de integridad estiman el grado de relevancia que pueda tener cada factor, según su percepción, al otorgarle un puntaje de 0, 1, 2 o 3.

Puntuación	Relevancia del factor o circunstancia que agrava la vulnerabilidad
0	No importante o casi irrelevante (la situación no ocurre)
1	Moderadamente relevante (la situación ocurre esporádicamente)
2	Importante (la situación ocurre bastante)
3	Muy importante (la situación ocurre de forma exhaustiva)

Durante las discusiones grupales, los moderadores deben pedir ejemplos específicos que respalden los puntajes. Esto será de gran ayuda al formular las recomendaciones.

La evaluación grupal para ponderar, como un todo, los factores que agravan la vulnerabilidad organizacional, se obtendrá mediante el cálculo del promedio de puntos otorgados de forma individual, y una vez que este puntaje sea debatido en el grupo. Posteriormente, se calcula el puntaje promedio para cada una de las cinco clasificaciones. Por último, el resultado de este proceso se incluye en el informe a entregarse a la Alta Dirección.

La metodología de evaluación es igual que para las vulnerabilidades inherentes, por lo que igualmente el grado de exposición organizacional a factores o circunstancias que agraven la vulnerabilidad puede ser bajo, medio o alto, en consideración de los criterios siguientes:

Puntuación Media	Nivel
Promedio ≤ 0.8	Bajo
$0.8 < \text{Promedio} \leq 1.6$	Medio
Promedio > 1.6	Alto

e. Evaluación del perfil de vulnerabilidad

Los resultados de los pasos anteriores (la puntuación otorgada a las vulnerabilidades inherentes y la correspondiente a los factores o circunstancias que agravan la vulnerabilidad), se resumen en el así llamado “Perfil de Vulnerabilidad” de la organización o unidad/área sujeta a la autoevaluación de integridad.

En primer lugar, se calcula el nivel promedio de vulnerabilidad inherente; posteriormente, el nivel promedio de los grupos de factores que agravan la vulnerabilidad.

El nivel global de vulnerabilidad, es decir, el Perfil de Vulnerabilidad se basa en el “perfil” global de las vulnerabilidades inherentes y los factores que agravan la vulnerabilidad. La combinación de los niveles de las vulnerabilidades inherentes y de los factores que incrementan la vulnerabilidad, permiten conocer el nivel global de la vulnerabilidad.

El Perfil de Vulnerabilidad es determinado con base en la siguiente tabla:

Factores que agravan la vulnerabilidad	Bajo	Medio	Alto
Vulnerabilidades inherentes			
Bajo	Bajo	Bajo	Medio
Medio	Medio	Medio	Alto
Alto	Alto	Alto	Alto

El Perfil de Vulnerabilidad se incluye igualmente en el informe a presentarse a la Alta Dirección.

VIII. Nivel de madurez del Sistema de Controles de la Integridad

a. Introducción

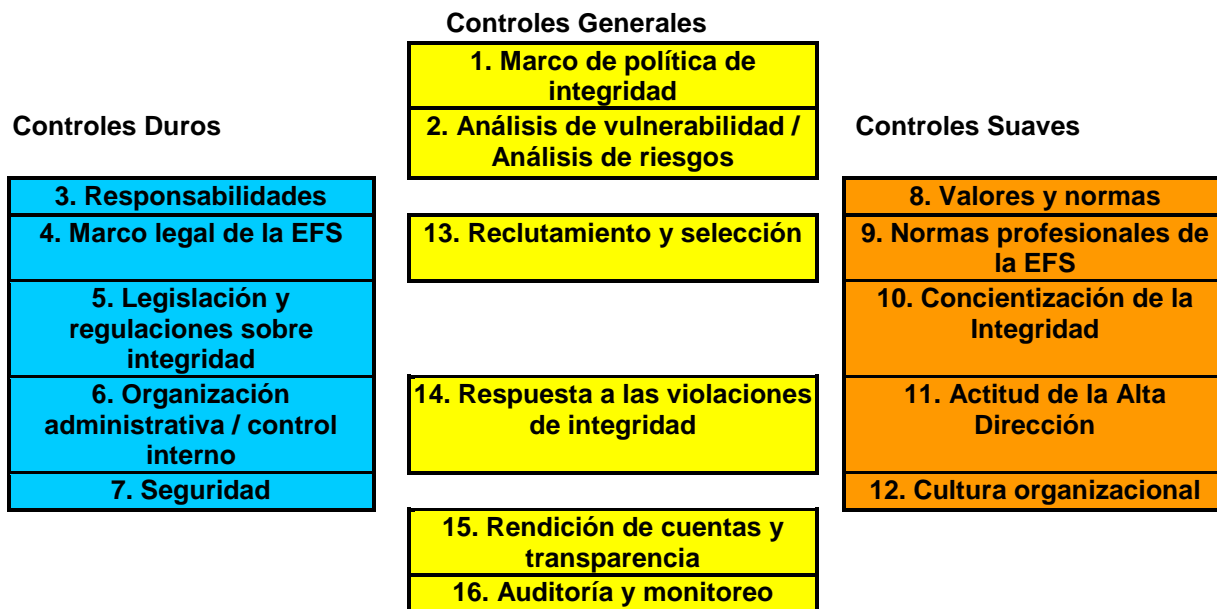
Un elemento clave de esta metodología es la evaluación del “nivel de madurez” del sistema de controles de la integridad (SCI). El SCI es el conjunto de medidas establecidas para promover, monitorear y mantener la integridad. De las muchas medidas conocidas de la literatura y de la práctica, se ha integrado un conjunto profundamente equilibrado para servir como referencia para este método de evaluación. Este conjunto de controles también toma en consideración las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAIs) por lo que integra componentes éticos.

La evaluación del nivel de madurez del sistema de controles de la integridad toma en cuenta la existencia, la operación y la eficacia de los controles. Esto hace posible analizar las fortalezas y las debilidades del sistema de controles de la integridad. De esta manera, se ofrece una visión de la resistencia que la organización ha desarrollado para hacer frente a las violaciones de la integridad.

b. Grupos de Medidas

El sistema de controles de la integridad de la organización se describe usando un amplio conjunto de medidas de integridad, dividido en tres bloques principales (controles generales, duros y suaves) y 16 grupos.

Los grupos se muestran en el siguiente modelo.



Los *controles duros*, como el término lo sugiere, se refieren principalmente a regulaciones, procedimientos y sistemas técnicos. Los *controles suaves* están diseñados para influir en el comportamiento, el ambiente de trabajo y la cultura dentro de la organización. Los grupos en la categoría de *controles generales* son de mayor alcance o tienen una mezcla de elementos duros y suaves.

A continuación se presenta la descripción de cada grupo. Esto incluye una breve descripción, preguntas clave y notas por cada grupo.

c. Descripción detallada de los grupos

1. Marco de política de integridad

1.1 Descripción

La gestión de la integridad debe de estar basada en la política, y la política de integridad (como cualquier otra política) debe de seguir los pasos del ciclo de políticas. El ciclo comienza con la formulación de una visión y metas, y termina cuando la política se evalúa y, consecuentemente, se revisa o actualiza de ser necesario. Para formular un marco de políticas para la integridad, la alta dirección primero deberá desarrollar una visión clara de la integridad y establecer una dirección clara para las medidas que deberán tomarse. El marco de políticas también debe garantizar que el diseño e implementación de las medidas de integridad sean y sigan siendo equilibradas y coherentes. Los elementos o etapas que conforman el marco de políticas se consideran a continuación.

1.2. Preguntas Clave

- ¿Las medidas de integridad están incorporadas en un marco de políticas sistemático?
- ¿Se han formulado objetivos concretos como parte del sistema de integridad?
- ¿Se ha considerado el tiempo requerido, además de los fondos necesarios para la implementación de medidas de integridad?
- ¿Se comunican las medidas de integridad?
- ¿La política de integridad está formalmente establecida dentro del plan general de políticas?

1.3 Notas

Marco de políticas

Las medidas de integridad deben estar integradas en un marco de políticas sistemático. Ya que la integridad es importante para la organización, la Alta Dirección debe desarrollar una visión coherente de la integridad y acordar principios. La visión y los principios se traducen en políticas y se establecen en un documento formal (plan de políticas de integridad). En cuanto a su alcance, la política debe de ser aplicable a través de toda la organización (integral). En la práctica, sin embargo, la política, algunas veces, se limita a la gestión del personal y a ciertos aspectos de la gestión de la integridad, tales como la seguridad; en otras palabras, en ocasiones la política de integridad no recibe la atención que merece. La influencia ejercida por el entorno de la organización también debe de ser reflejada en la política. La política deberá por lo tanto estar dirigida tanto interna como externamente.

Metas concretas

La integridad se vuelve un tema concreto de política cuando las metas se establecen. Para dirigir la política, las metas deben cumplir ciertos criterios, entre otros deben de ser:

- Específicas (concretas y enfocadas);
- Medibles (expresadas en términos verificables);
- Acordadas (aceptable para las partes interesadas);
- Realistas (factibles);
- Acotadas a un periodo (con plazos límite);
- Consistentes (las metas no deben de ser contradictorias).

Nombrar actividades y recursos

Las metas de la política sólo pueden lograrse si se toman acciones y si se implementan medidas. Los recursos (humanos, materiales, financieros) son necesarios para emprender acciones e implementar las medidas. También debe de quedar claro quién será el responsable del cumplimiento de las metas.

Comunicación de la Política

Para ser eficaz, la política debe de ser dada a conocer. Muchas de las herramientas y canales de comunicación se pueden utilizar para difundir la política y darla a conocer, por ejemplo, folletos, seminarios y la intranet.

Política formal de integridad

Para proporcionar una base adecuada para la gestión de la integridad, la política de integridad debe de estar formalmente establecida y ser aceptada.

2. Análisis de vulnerabilidades / análisis de riesgos

2.1 Descripción

Un análisis de vulnerabilidades implica un análisis sistemático de las acciones, procesos y posiciones que están expuestos a posibles violaciones de la integridad.

2.2 Preguntas clave

- ¿Se llevan a cabo con regularidad análisis de riesgos / de vulnerabilidad?
- ¿Se llevan a cabo análisis profundos respecto a las áreas y posiciones vulnerables?

2.3 Notas

Evaluación general de la vulnerabilidad / de riesgos

Todas las organizaciones en el sector público están expuestas a riesgos de integridad. Una evaluación general de los riesgos y vulnerabilidades es útil para identificar los riesgos de integridad de manera general. Para hacer frente a estas vulnerabilidades, la organización debe asegurarse de establecer una base de controles de integridad.

Evaluación a fondo de vulnerabilidades/riesgos

Algunos procesos y posiciones tienen un mayor riesgo de integridad porque ciertas áreas o circunstancias laborales incrementan su vulnerabilidad a violaciones de la integridad. Los factores que incrementan los riesgos deben de ser conocidos, de modo que se pueda decidir qué medidas de gestión de la integridad se deben de tomar para contrarrestar los riesgos mayores. Esto mejora la calidad del proceso desde la perspectiva de la integridad. El análisis de vulnerabilidades consiste en una evaluación de:

- Las operaciones, actividades y acciones vulnerables;
- Las circunstancias que agravan la vulnerabilidad de la organización a las violaciones de la integridad.

3. Responsabilidades

3.1 Descripción.

Para incorporar la gestión de la integridad en una organización, las responsabilidades de los distintos cargos y las de sus titulares deben ser claras. Si no lo son, será incierto quien está involucrado en la gestión de la integridad y quién es responsable de ello. Las responsabilidades deberán ser establecidas con las funciones regulares en la organización, pero también podría ser necesario crear posiciones específicas para gestionar la integridad, que tengan sus propias facultades y responsabilidades (consejeros, agentes de seguridad, coordinadores de integridad, etc.).

3.2 Preguntas clave

- ¿Existen responsabilidades (funcionales) asignadas para ocuparse del tema de integridad?
- ¿Existe algún esquema de consulta sistemática entre los funcionarios responsables de la integridad?
- ¿Existe algún consejero de la integridad?

- ¿Existe alguna coordinación periódica con organizaciones y otras partes interesadas externas?
- ¿Ha sido alguien (externo) nombrado para coordinar la política de integridad?

3.3 Notas

Responsabilidades sobre la integridad y la coordinación internas

Varios cargos están involucrados en la gestión de la integridad dentro de una organización, por ejemplo:

- Gerencia (alta dirección y mandos medios);
- asuntos financieros y económicos;
- departamento de personal;
- servicios generales;
- asuntos administrativos / legales;
- relaciones públicas;
- departamentos de auditoría, control e inspección.

Puestos especiales pueden ser establecidos dentro de una organización para tratar con los problemas de integridad (se trata de puestos dedicado al tema de integridad), por ejemplo:

- Oficial de seguridad;
- Oficial de cumplimiento;
- Coordinador de la integridad.

Tales puestos permiten que se preste una atención más sistemática a la integridad, que si este tema sólo fuera parte de las responsabilidades de otro puesto. La función y responsabilidades de cada puesto deben ser claras y deben estar coordinadas a través de una consulta estructurada con el fin de prevenir deficiencias y duplicaciones.

Consejeros de la integridad

Los consejeros de la integridad deben ser designados para que el personal de la organización pueda hablar con una persona de confianza, pedir asesoramiento sobre problemas de integridad e informar sobre violaciones de la integridad. Además de un consejero general de la integridad, podrían designarse consejeros especiales para tratar:

- Denunciantes (como parte de un esquema para denunciar malas conductas);
- Acoso sexual/discriminación.

Coordinación y responsabilidad sobre las relaciones externas de integridad

La integridad es importante no sólo dentro de la organización sino también respecto a sus relaciones con organizaciones externas. Debe de existir, por ejemplo:

- coordinación y consulta con otras organizaciones;
- análisis de las relaciones externas.

Alguien debe ser responsable de estas relaciones.

4. Marco legal de la EFS

4.1 Descripción

La integridad de las EFS y su independencia e imparcialidad son condiciones esenciales con el fin de cumplir los deberes de las EFS de forma eficaz y adecuada.

Por lo tanto, es lógico que en muchos países estas condiciones estén respaldadas en una ley o incluso en la Constitución. Se considera que las EFS desempeñan un papel vital en el sistema de integridad dentro de un país, siendo parte de los pesos y contrapesos en el sector público. Esto también requiere un marco jurídico sólido. Algunas de las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) proporcionan las directrices para un marco jurídico adecuado.

4.2 Preguntas Clave

- ¿La existencia e independencia de la EFS está incorporada en la Constitución (ISSAI 10; principio 1)?

¿Está establecido un marco jurídico para garantizar:

- la independencia del titular de la EFS y la de sus miembros (en el caso de instituciones colegiadas), incluyendo la seguridad la ocupación y la inmunidad legal en el desempeño normal de sus funciones (ISSAI 10, principio 2)?
- un mandato suficientemente amplio y con plena discreción, respecto al ejercicio de las funciones de la EFS (ISSAI 10, principio 3)?
- acceso irrestricto a la información (ISSAI 10, principio 4)?
- el derecho y obligación de informar sobre el trabajo de las EFS y la libertad de decidir el contenido y la periodicidad de los informes de auditoría para su publicación y difusión (ISSAI 10, principio 5/6)?
- autonomía financiera/gerencial/administrativa y la disponibilidad apropiada de recursos humanos, materiales y monetarios (ISSAI 10, principio 8)?

4.3 Notas

A pesar de que las preguntas clave en su mayoría se explican por sí mismas, es útil añadir algo de orientación adicional proporcionada por la ISSAI 11.

La ISSAI 11 establece las siguientes directrices para algunos de los principios mencionados en la ISSAI 10.

Principio 4 (Acceso irrestricto a la información): Las EFS deben disponer de las potestades adecuadas para obtener acceso oportuno, sin restricciones, directo y libre, a toda la documentación y la información necesarias para el apropiado cumplimiento de sus responsabilidades reglamentarias.

Principio 5 (El derecho y la obligación de informar sobre su trabajo): Las EFS no deben estar limitadas a informar sobre los resultados de su trabajo de auditoría. Deben estar obligadas por ley a informar por lo menos una vez al año sobre los resultados de su trabajo de auditoría.

Principio 8 (Autonomía financiera y gerencial/administrativa, al igual que disponibilidad de recursos humanos, materiales y económicos apropiados): Las EFS deben disponer de los recursos humanos, materiales y económicos necesarios y razonables; el Poder Ejecutivo no debe controlar ni supeditar el acceso a esos recursos. Las EFS administran su propio presupuesto y lo asignan de modo apropiado.

5. Legislación y regulaciones sobre la Integridad

5.1 Descripción

Ciertas reglas de integridad son aplicables específicamente a las organizaciones del sector público. Estos son controles duros que todos los miembros del personal deberán observar. En efecto, son normas mínimas. Las regulaciones precisas varían de una parte del sector público a otra, pero algunas de las normas y reglas más comunes se resumen a continuación.

5.2 Preguntas clave

¿Están las reglas establecidas (ya sea en la legislación o en los reglamentos) respecto a:

Conflicto de intereses

- posiciones externas / intereses financieros?
- la aceptación de regalos / invitaciones?
- la confidencialidad?

- prevención de “Acuerdos de Puerta Giratoria”⁴?
- identificación externa de los contratistas y / o solicitantes de licencias?
- el cabildeo?
- la influencia de los políticos sobre los servidores públicos?

Integridad dentro de las organizaciones

- La lucha/combate con la conducta indeseable?
- Las solicitudes de reembolso de gastos?
- Uso de e-mail, Internet y teléfono?
- Uso de la propiedad del empleador?

5.3 Notas

Las principales regulaciones se consideran brevemente a continuación. Los aspectos penales tales como la sanción de los servidores públicos implicados en sobornos y el mal uso de fondos, no son considerados. Esta legislación es aplicable, sin embargo, a las violaciones de la integridad.

Conflictos de interés

Posiciones externas/intereses

Si algún miembro del personal está implicado en el pago o no pago de actividades ajenas a la función pública, por ejemplo en la industria o el deporte, podría existir un conflicto de interés. Dependiendo de la naturaleza de las actividades, el personal podría estar obligado a reportarlo. Sin duda debe existir el deber de informar sobre las actividades si éstas están relacionadas con el trabajo del departamento en cuestión o si hay una conexión con el propio cargo del servidor público. Estas actividades, por lo tanto, deben de reportarse por si hay alguna relación entre las actividades externas y el puesto o las actividades del departamento, en la medida en que afecten el desempeño del funcionario. Si se reportan actividades externas, éstas también deben ser registradas. Para algunos puestos en el sector público, por ejemplo en el poder judicial, las regulaciones establecidas podrían requerir que los puestos externos sean públicos.

Intereses financieros y transacciones de valores

Un servidor público podría tener un interés financiero en una compañía que está asociada con su posición o bien podría desear comprar o vender valores en dicha compañía. Para prevenir conflictos de intereses indeseables, dichos intereses deben estar regulados dentro del sector público.

Regalos/invitaciones/beneficios

Una relación laboral podría abrir la oportunidad a un servidor público de obtener algo, tal como una botella de vino, una invitación a cenar o un boleto de admisión a un evento. El otorgante podría querer agradecer o influenciar al servidor público, mejorar la relación, o esperar algo a cambio. Aceptar un regalo podría por lo tanto ser un riesgo a la integridad. Los regalos no deberían ser aceptados sin haberlo meditado y, en algunas ocasiones, deberían rechazarse. Lo importante es que un servidor público no debe comprometer su independencia.

Confidencialidad/libertad de expresión

Muchos servidores públicos tienen acceso a información personal del público o a información que podría ser de interés a alguna parte externa. No hace falta decir que dicha información debe ser tratada con confidencialidad y no debe ser usada en beneficio propio. Sin embargo, los servidores públicos también tienen el derecho a la libertad de expresión, siempre que no perjudique su desempeño o el del

⁴ Por “arreglos de puerta giratoria” (*Revolving-door arrangement*, en inglés) debe entenderse aquellos casos en los que una persona que un día trabaja para el gobierno, bien puede trabajar el siguiente para la iniciativa privada u otras organizaciones que buscan algo del gobierno (ej: proveedores, consultores, firmas de auditoría, etc).

sector público. El derecho fundamental del servidor público de ejercer su libertad de expresión no es absoluto, está limitado por las garantías exigidas en relación a su desempeño y el de su departamento. Cualquier comentario que se haga debe ser juzgado en parte considerando la distancia existente entre él y la política a la que se hace referencia, la naturaleza de los comentarios y la manera en la cual expresa su opinión. Los comentarios pueden ser juzgados solamente después de que se hayan hecho.

Acuerdos de puerta giratoria

Por acuerdo de puerta giratoria debe entenderse aquel en el cual se contrató a un servidor público de determinado ministerio o instancia, inmediatamente o poco después que ha dejado su empleo para llevar a cabo el mismo trabajo, por ejemplo a través de una consultora externa. Dichos acuerdos rápidamente aumentan sospechas de favoritismo, competencia injusta o detentan un conflicto de interés. Por lo tanto, representan una amenaza a la integridad del sector público. Para prevenirlo, pueden introducirse regulaciones que exijan que un departamento contrate a un servidor público como consultor externo, sólo tras un determinado número de años de cese al servicio.

Detección de relaciones externas

Las autoridades públicas están obligadas por ley a rechazar las solicitudes de subvenciones o licencias, o bien a retirarlas si un hecho sancionable pudiera ser cometido o si se cree que el beneficiario cometerá una ofensa o delito. Bajo la ley, una autoridad pública puede decidir no adjudicar determinados contratos o cancelarlos si una compañía no satisface más los requisitos de fiabilidad.

Cabildeo

Las organizaciones del sector privado pueden tener intereses especiales para influenciar las opiniones o decisiones de políticos y/o servidores públicos. Para evitar la influencia indebida generada por los cabildeos, se pueden emitir regulaciones para promover la transparencia.

Influencia de los políticos sobre los servidores públicos

La integridad en el sector público requiere relaciones apropiadas entre los políticos y los servidores públicos. Pueden emitirse regulaciones para proteger a los servidores públicos contra la influencia indebida por parte de los políticos.

Integridad dentro de las organizaciones

Conducta indeseable

Los servidores públicos deben ser respetuosos y considerar seriamente las opiniones, puntos de vista y esfuerzos de otros. El respeto se muestra a través de las buenas relaciones de trabajo, el espíritu de equipo, la apertura y el enfoque en el cliente. El personal debe trabajar sin hacer una distinción por motivos de religión, fe, orientación política, raza, sexo u otras características personales. Los insultos, la discriminación, el acoso sexual y el *bullying* son formas de conducta indeseable y muestran una falta de respeto por los demás.

Solicitudes de reembolso de gastos

Si los servidores públicos incurren en gastos en el desempeño de sus funciones, pueden solicitar el reembolso a su empleador. Cada organización tiene sus propias reglas sobre las solicitudes de reembolso de gastos. Dado que las solicitudes de reembolso de gastos son muy susceptibles a la comisión de fraude, deben ser manejadas cuidadosamente. La cantidad reclamada y la razón por incurrir en el gasto deben ser detalladas. Comprobantes en forma de facturas, recibos y boletos de transporte deben ser presentados, y la solicitud de reembolso debe ser aprobada por un superior antes de que sea pagadera.

Uso del teléfono, internet y correo electrónico

Los miembros del equipo de trabajo pueden enviar y recibir correos electrónicos, y usar el internet durante las horas de trabajo usando los sistemas proveídos por el empleador para propósitos de trabajo. Puede permitirse el uso privado limitado de los sistemas siempre que éste no interrumpa el trabajo o no esté prohibido. Es técnicamente posible grabar (registrar) el uso de los sistemas de correo electrónico e internet del personal. Esto da una idea del uso individual y del departamento de los sistemas, y podría permitir la detección también de un uso indebido.

Uso de la propiedad del empleador

Durante las horas de trabajo, el personal inevitablemente hace uso de los bienes de la organización, tales como teléfonos, computadoras, impresoras, máquinas de fax, vehículos y fotocopadoras. Éstos deben ser tratados con cuidado y debe evitarse su daño. El tiempo es también un activo, y el personal debe usarlo de manera eficaz y eficiente. En general, los activos deben ser usados solamente para propósitos de trabajo y no privados. Si los bienes son también usados fuera del lugar de trabajo, por ejemplo en casa, aun así no deben ser usados para propósitos privados. Una excepción a esta regla es posible sólo si se hace un uso privado muy limitado de un bien. 'Reglas de la casa' adicionales pueden ser aplicables dentro de la organización.

6. Organización administrativa / control interno

6.1 Descripción

La organización administrativa y los controles internos son diseñados para controlar procesos y generar información confiable (completa, precisa y válida) sobre ellos. Aunque la organización administrativa no esté exclusiva y específicamente dirigida a la integridad, muchos de sus procedimientos y controles están conectados con la integridad. Por lo tanto, es importante que la organización administrativa y los controles internos estén óptimamente diseñados para los propósitos de integridad, con una visión de prevención (por ejemplo, eliminando la tentación), detección (por ejemplo, relevando las pérdidas de existencias) y sanción (por ejemplo, identificando a los responsables). Las notas siguientes consideran cómo la organización administrativa y los controles internos pueden promover la integridad.

6.2 Preguntas clave

- ¿Hay una especificación sobre las actividades y posiciones/cargos vulnerables?
- ¿Están establecidos procedimientos específicos para la realización de actividades vulnerables?
- ¿Todos tienen una descripción de su cargo?
- ¿Están los deberes/actividades segregados?
- ¿se aplica el 'principio de cuatro ojos'?
- ¿Hay regulaciones que rijan el mandato?
- ¿Está establecido un esquema de rotación de trabajo?

6.3 Notas

Especificación y procedimientos para las actividades y posiciones/cargos vulnerables

Las organizaciones deben especificar qué actividades y posiciones son consideradas como relativamente vulnerables y cuáles requieren más protección para prevenir violaciones de integridad. Deben diseñarse procedimientos dentro de la organización administrativa específicamente para las operaciones y actividades más vulnerables, tales como la recolección, la contratación, el pago, la ejecución y concesión de licencias. Las actividades que involucran información, dinero y bienes son particularmente vulnerables.

Descripciones de trabajo

Una descripción de trabajo es un documento que establece el contenido y esencia de un trabajo en particular. Explica lo que implica el trabajo y qué actividades acordadas forman parte o no del mismo. Si el personal no sabe precisamente qué se espera de ellos, serán más vulnerables. Deben saber lo que

tienen que hacer, cómo se espera que lo hagan y qué responsabilidades y poderes tienen. Las descripciones vagas e inciertas de trabajo le dan al personal una gran libertad de acción sin límites definidos.

Las descripciones claras y completas de trabajo dan claridad sobre las tareas y facultades. Las descripciones claras de los cargos son, por lo tanto, una precondition para la integridad. Las descripciones de trabajo también dan a la Alta Dirección de la organización una visión sobre las actividades vulnerables que son llevadas a cabo por una persona en particular. Los requisitos que deben cumplirse incluyen:

- Las descripciones de trabajo deben ser redactadas para todos los miembros del personal;
- A cada miembro del personal se le debe dar una copia de la descripción de su trabajo;
- Las descripciones de trabajo deben estar actualizadas y describir todas las actividades que tienen que llevarse a cabo;
- Las descripciones de trabajo deben claramente explicar los límites de las facultades y responsabilidades.

Segregación de funciones

La segregación de funciones significa que las actividades vulnerables se dividen en una serie de sub-actividades para prevenir que demasiados poderes y responsabilidades se concentren en una sola persona. Hay riesgos si las funciones ejecutadas en la realización de un proceso vulnerable no son segregadas. Las actividades que forman parte de dichos procesos son vulnerables si una misma persona siempre las lleva a cabo. La persona que analiza una solicitud de una licencia, por ejemplo, no debe verificar también si las condiciones de concesión de licencias están siendo observadas. Las funciones estarán convenientemente segregadas si:

- La organización entiende claramente qué actividades y funciones son vulnerables;
- las sub-actividades vulnerables son llevadas a cabo por diferentes personas;
- las actividades vulnerables que no se puedan dividir en sub-actividades y no puedan llevarse a cabo por varias personas, se llevarán a cabo por un equipo.

Principio de cuatro ojos

Esta medida evita que el personal en determinadas posiciones trabaje sin supervisión. En zonas o procedimientos de alto riesgo, por lo menos dos personas deben trabajar de manera conjunta. Esto se conoce como principio de "cuatro ojos" o "dos firmas". Los ejemplos incluyen la gestión clave para un seguro y la apertura de las propuestas.

Regulaciones que rigen el mandato

Las regulaciones de mandato establecen las facultades financieras y de otro tipo de una posición o cargo en particular. Pueden establecer límites, por ejemplo, en el supuesto de los compromisos financieros o de la ejecución de los pagos.

Rotación de Trabajo

Para evitar que en una organización se tenga demasiada proximidad en una relación laboral (por ejemplo, con un cliente o proveedor), deben establecerse esquemas de rotación de trabajo para el personal. Después de un cierto período de tiempo, el personal debe cambiar de responsabilidades y no tener más contacto con sus relaciones anteriores. Si es poco factible la rotación de trabajo, por ejemplo, debido a la pericia específica del personal, puede entonces cambiarse al proveedor o al cliente. El personal que realice el mismo trabajo durante un largo periodo de tiempo puede llegar a ser vulnerable. Existe el peligro de que las rutinas indeseables se arrastren y adopten, y que se entablen relaciones con, por ejemplo, clientes, proveedores y otras partes interesadas. El personal puede favorecer a un cliente en particular y tomar demasiado en cuenta sus intereses. Un sistema de rotación de trabajo

puede prevenir esto. Con una visión a la integridad, la rotación de trabajo es particularmente importante en relación con actividades muy vulnerables.

7. Seguridad

7.1 Descripción

La seguridad desempeña un papel importante en la protección de la integridad de una organización. La seguridad, como la política de integridad en general, debe ser cuidadosamente pensada para que la organización goce de la protección que se merece. Para fines de integridad, tanto la seguridad física (cerraduras, cajas fuertes, etc.) como la seguridad de la información (acceso a la computadora) son de gran importancia.

7.2 Preguntas clave

¿Se han implementado medidas en relación con:

- la seguridad física (cerraduras, ventanas, puertas, cajas fuertes, etc.)?
- la seguridad de la información (seguridad de las tecnologías de la información, política de escritorio limpio, clasificación de la información como confidencial/ secreta/ autorizaciones de acceso, sistemas de archivos)?

7.3 Notas

La seguridad física

La seguridad física se logra a través de cerraduras, ventanas, puertas, compartimientos, pases, cajas fuertes, etc., para evitar que personas no autorizadas entren en el edificio. Tales medidas incluyen pantallas irrompibles para el personal que trabaja en las ventanillas. En situaciones excepcionales, por ejemplo cuando el personal pueda ser amenazado, pueden ser necesarios guardias personales de seguridad. La seguridad física incluye también medidas para la protección segura de los objetos de valor, como dinero, bienes, equipos y documentos.

Seguridad de la información

La seguridad de la información comprende medidas de seguridad informática física y lógica. La seguridad física se refiere, por ejemplo, al acceso a las habitaciones en las que se utilizan las computadoras. La seguridad lógica del equipo forma parte del *software* del sistema e incluye:

- identificación (¿quién está tratando de acceder al sistema?)
- autenticidad (¿La persona que accede es quien dice ser?, establecida por medio de contraseñas o de identificación biométrica como huellas dactilares);
- autorización (que une la persona a los derechos en el sistema).

Estos elementos de seguridad lógica del equipo deben ser debidamente regulados para evitar violaciones de confidencialidad y privacidad, y también para limitar las posibilidades de comisión de un fraude.

Los elementos específicos de seguridad de la información en materia de integridad incluyen:

- La política de escritorio limpio: Los escritorios y cubículos para oficinas deben mantenerse limpios para que las personas no autorizadas no puedan obtener datos de los documentos abiertos.
- La clasificación de la información como confidencial o secreta: Los documentos y archivos deben ser clasificados por su grado de confidencialidad, de manera tal que deben establecerse procedimientos sobre la forma de manejar la información clasificada.
- Sistemas de archivo: Deben implementarse sistemas de archivo estrictamente controlados para asegurarse de que la información confidencial y clasificada no es accesible para personas no autorizadas.

8. Valores y normas

8.1 Descripción

El concepto de integridad está estrechamente asociado con los valores y normas. La integridad de un acto puede medirse por su compatibilidad con el sistema de valores y normas que prevalecen en la organización. Los valores deben ser significativos para la organización y las normas deben ser reconocidas universalmente. Los valores y normas deben incorporarse en la misión y estar establecidos en el código de conducta. Cuando un nuevo funcionario hace un juramento o promesa, debe ser informado y tomar conciencia de los valores y las normas aplicables dentro de la organización.

8.2 Preguntas clave

- ¿Es la integridad parte de la misión de la organización?
- ¿Están debidamente formulados los valores fundamentales (por ejemplo, imparcialidad, profesionalismo, etc.)?
- ¿Se ha introducido un código (de integridad) de la conducta?
- ¿Se hace juramento o promesa?
- ¿Hay una ceremonia especial para hacer un juramento o promesa?

8.3 Notas

Misión (relación con la integridad)

Cada organización debe ser capaz de definir sus propios objetivos y propósito específicos, es decir, su misión. Puesto que el propósito de una organización pública es invariablemente servir al interés público, la declaración de la misión no sólo debe considerar los objetivos y propósitos, sino también establecer los parámetros dentro de los cuales pueden ser logrados. La integridad es uno de los parámetros más importantes. La integridad debe ser parte de la misión para que no haya ninguna duda sobre su valor fundamental y su importancia central. La inclusión de la integridad en la misión se centra en la importancia que tiene la integridad y hace que sea más fácil de llevar a cabo la política de integridad.

Valores esenciales y código de conducta

Los códigos de conducta proporcionan una visión general y una descripción de los valores abstractos centrales de la organización, y las normas y reglas concretas basadas en ellos. Los códigos de conducta proveen al personal una orientación práctica y son un punto de referencia para las mejores prácticas en la función pública. Si el personal se enfrenta a un problema de integridad, el código debería ayudarles a ejercer su propio juicio y llegar a una decisión bien fundada. Todos los servidores públicos deben estar involucrados, directa o indirectamente, en el proceso de elaboración del código de conducta.

Juramento / promesa

Los servidores públicos tienen una posición especial en la sociedad y forman parte de una organización gubernamental cuyo propósito es servir al interés público. Los servidores públicos tienen facultades excepcionales y trabajan con fondos públicos. Las exigencias estrictas hacen referencia, por lo tanto, a la integridad que deben comportar las personas que trabajan en el sector público. Aunque todos deben respetar la ley y deben saber que el fraude y la corrupción, por ejemplo, son sancionables, los servidores públicos que hacen un juramento o una promesa se comprometen a respetar la Constitución y las demás leyes, así como a actuar "como corresponde a un buen servidor público". Son pues, conscientes de las responsabilidades inherentes a sus cargos y juran o prometen respetar los valores y las normas.

El valor y la relevancia de hacer un juramento/promesa es mayor cuando esta se realiza como parte de una ceremonia específica en el que se hace hincapié en la importancia de la integridad. Esto también permite a la Alta Dirección de la entidad demostrar que cree en la integridad como una precondition para la confianza en la organización.

9. Normas Profesionales de la EFS

9.1 Descripción

Debido a la naturaleza específica de las EFS y la importancia de la auditoría pública independiente, es muy importante que las EFS y su personal mantengan el más alto estándar de conducta ética. Esto no sólo requiere de un marco jurídico firme (véase el grupo 4 del Sistema de Controles de la Integridad), sino también la atención general dentro de la EFS de los valores y normas apropiadas. Estos valores y normas deben ser continuamente promovidos y reforzados con el fin de influir en el personal para que éste se comporte correctamente. Diversas ISSAI⁵ proporcionan orientación sobre los principios de ética profesional.

9.2 Preguntas clave

- ¿La EFS no está involucrada (ni se prevé que participe), de alguna forma, en la dirección y gestión de las organizaciones que audita (ISSAI 11, principio 3, Directrices)?
- Al trabajar con el Ejecutivo, ¿los auditores actúan solamente como observadores y no participan en el proceso de toma de decisiones (ISSAI 11, principio 3, Directrices)?
- ¿Garantizan las directrices emitidas por la EFS que su personal no desarrolle una relación demasiado estrecha con las entidades que auditan, por lo que parecen y siguen siendo objetivos (ISSAI 11, principio 3, Directrices)?
- ¿Se imparten cursos de capacitación al personal que den a conocer la importancia de la independencia dentro de la cultura de las EFS, que enfatizan la calidad requerida y los estándares de desempeño, y que aseguren que el trabajo es autónomo, objetivo y sin sesgo (ISSAI 11, el principio 3, buenas prácticas)?
- ¿Tiene la EFS un código de ética (profesional) y normas con significancia ética implementadas, que abarquen:
 - la confianza, confidencialidad y la credibilidad (ISSAI 30, capítulo 1)?
 - la integridad (ISSAI 30, capítulo 2)?
 - la independencia, la objetividad, la imparcialidad, la neutralidad (política), la prevención de conflictos de interés (ISSAI 30, capítulo 3; ISSAI 200/2. 1-2.32)?
 - el secreto profesional (ISSAI 30, capítulo 4)?
 - el debido cuidado y competencia (ISSAI 30, capítulo 5; ISSAI 200/2.1, 2.33-2.46)?
- ¿se ha involucrado a los empleados en la elaboración del código de ética y/o las normas con significancia ética?

9.3 Notas

Para explicar (los antecedentes de) las cuestiones clave antes mencionadas, se ha hecho referencia a las ISSAIs pertinentes.

ISSAI 30: Código de ética

Capítulo 1: Concepto, Antecedentes y Propósito del Código de Ética

2. Un Código de Ética constituye una exposición integral que abarca los valores y principios que guían la labor cotidiana de los auditores. La independencia, las facultades y las responsabilidades del auditor en el sector público plantean elevadas exigencias éticas a la EFS y al personal que emplean o contratan para la labor de auditoría. Un código de ética de los auditores pertenecientes al sector público debe tener en cuenta tanto las exigencias éticas de los funcionarios públicos en general, como las exigencias específicas de los auditores en particular, incluidas las obligaciones profesionales de estos.

4. Debido a las diferencias nacionales de cultura, idioma y sistemas jurídicos y sociales, es responsabilidad de cada EFS la elaboración de un Código de Ética propio que se ajuste de manera óptima a su propio entorno. Conviene que estos Códigos de Ética nacionales especifiquen con claridad los conceptos éticos. El Código de

⁵ ISSAI 11, 30 y 200.

Ética de la INTOSAI se propone servir de fundamento a los Códigos de Ética nacionales. Cada EFS tiene que garantizar que todos sus auditores estén familiarizados con los valores y principios que figuran en el Código de Ética nacional y actúen de acuerdo con ellos.

5. La conducta de los auditores debe ser irreproachable en todos los momentos y todas las circunstancias. Cualquier deficiencia en su conducta profesional o cualquier conducta inadecuada en su vida personal perjudica la imagen de integridad de los auditores, la EFS que ellos representan, la calidad y la validez de su labor de auditoría, lo que puede plantear dudas acerca de la fiabilidad y la competencia profesional de la propia EFS. La adopción y la aplicación de un código de ética para los auditores del sector público, promueve la confianza en los auditores y en su labor.

6. Tiene una importancia fundamental que la EFS suscite seguridad, confianza y credibilidad. El auditor lo logra mediante la adopción y la aplicación de las exigencias éticas de las nociones encarnadas en los siguientes conceptos clave: integridad, independencia y objetividad, confidencialidad y competencia profesional.

Seguridad, confianza y credibilidad

7. El Poder Legislativo y/o Ejecutivo, el público en general y las entidades fiscalizadas tienen derecho a esperar que la conducta y el enfoque de la EFS sean irreprochables, no susciten sospechas y sean dignos de respeto y confianza.

8. Los auditores deben conducirse de un modo que promueva la cooperación y las buenas relaciones entre los auditores y dentro de la profesión.

9. El Poder Legislativo y/o Ejecutivo, el público en general y las entidades fiscalizadas deberán tener una plena garantía de la justicia y la imparcialidad de toda la labor de la EFS. Por consiguiente, es esencial que exista un Código de Ética nacional o un documento semejante que rijan la prestación de servicios.

Capítulo 2: Integridad

12. La integridad constituye el valor central de un Código de Ética. Los auditores están obligados a cumplir normas elevadas de conducta (por ejemplo, honradez e imparcialidad) durante su trabajo y en sus relaciones con el personal de las entidades fiscalizadas. Para preservar la confianza de la sociedad, la conducta de los auditores debe ser irreproachable y estar por encima de toda sospecha.

13. La integridad puede medirse en función de lo que es correcto y justo. La integridad exige que los auditores se ajusten tanto a la forma como al espíritu de las normas de auditoría y de ética. La integridad también exige que los auditores se ajusten a los principios de objetividad e independencia, mantengan normas irreprochables de conducta profesional, tomen decisiones acorde con el interés público, y apliquen un criterio de honradez absoluta en la realización de su trabajo y el empleo de los recursos de la EFS.

Capítulo 3: Independencia, objetividad e imparcialidad

14. Para los auditores, es indispensable la independencia con respecto a la entidad fiscalizada y otros grupos de interés externos. Esto implica que los auditores actúen de un modo que aumente su independencia o que no la disminuya por ningún concepto.

15. Los auditores no sólo deben esforzarse por ser independientes de las entidades fiscalizadas y de otros grupos interesados, sino también deben ser objetivos al tratar las cuestiones y los temas sometidos a revisión.

16. Es esencial que los auditores no sólo sean independientes e imparciales de hecho, sino que también lo reflejen.

17. En todas las cuestiones relacionadas con la labor de auditoría, la independencia de los auditores no debe verse afectada por intereses personales o externos. Por ejemplo, la independencia podría verse afectada por presiones o influencias externas sobre los auditores; por prejuicios de los auditores acerca de las personas, las entidades fiscalizadas, los proyectos o los programas; por haber trabajado recientemente en la entidad fiscalizada, o por relaciones personales o financieras que provoquen conflictos de lealtad o de interés. Los auditores están obligados a no intervenir en ningún asunto en el cual tengan algún interés personal.

18. Se requiere objetividad e imparcialidad en toda la labor efectuada por los auditores, y en particular en sus informes, que deberán ser exactos y objetivos. Las conclusiones de los dictámenes e informes, por consiguiente, deben basarse exclusivamente en las pruebas obtenidas y unificadas de acuerdo con las normas de auditoría de la EFS.

19. Los auditores deberán utilizar la información aportada por la entidad fiscalizada y por terceros. Esta información deberá tenerse en cuenta de modo imparcial en los dictámenes expresados por los auditores. El auditor también deberá recopilar información acerca de los enfoques de la entidad fiscalizada y de terceros. Sin embargo, estos enfoques no deberán condicionar las conclusiones propias de los auditores.

Neutralidad política

20. Es importante mantener la neutralidad política -tanto la real como la percibida- de la EFS.

21. Es importante que, cuando los auditores se dediquen o estudien la posibilidad de dedicarse a actividades políticas, tengan en cuenta la forma en que tal dedicación podría afectar –o parecer que afecte- su capacidad de desempeñar con imparcialidad sus obligaciones profesionales. Si los auditores están autorizados a participar en actividades políticas, tienen que ser conscientes de que tales actividades pueden provocar conflictos profesionales.

Conflictos de interés

22. Cuando los auditores están autorizados a asesorar o a prestar servicios distintos de la auditoría a una entidad fiscalizada, hay que procurar que estos servicios no lleven a un conflicto de interés. En particular, los auditores deben garantizar que dichos servicios o asesoramiento no incluyan responsabilidades o facultades de gestión, que deben continuar desempeñando con claridad los directivos de la entidad fiscalizada.

23. Los auditores deberán proteger su independencia y evitar cualquier posible conflicto de interés rechazando regalos o gratificaciones que puedan interpretarse como intentos de influir sobre la independencia y la integridad del auditor.

24. Los auditores deben evitar toda clase de relaciones con los directivos y el personal de la entidad fiscalizada y otras personas que puedan influenciar, comprometer o amenazar la capacidad de los auditores para actuar y parecer que actúan con independencia.

25. Los auditores no deberán utilizar su cargo oficial con propósitos privados y deberán evitar relaciones que impliquen un riesgo de corrupción o que puedan suscitar dudas acerca de su objetividad e independencia.

26. Los auditores no deberán utilizar información recibida en el desempeño de sus obligaciones como medio para obtener beneficios personales para ellos o para otros. Tampoco deberán divulgar información que otorguen ventajas injustas o injustificadas a otras personas u organizaciones, ni deberán utilizar dicha información en perjuicio de terceros.

Capítulo 4: Secreto Profesional

27. La información obtenida por los auditores en el proceso de auditoría no deberá revelarse a terceros ni oralmente ni por escrito, salvo a los efectos de cumplir las responsabilidades legales o de otra clase que correspondan a la EFS, como parte de los procedimientos normales de ésta o de conformidad con las leyes pertinentes.

Capítulo 5: Competencia profesional

28. Los auditores tienen la obligación de actuar en todo momento de manera profesional y de aplicar elevados niveles profesionales en la realización de su trabajo con objeto de desempeñar sus responsabilidades de manera competente e imparcial.

ISSAI 40: Control de Calidad para la EFS.

La EFS debe establecer políticas y procedimientos diseñados a dar garantía razonable de que la EFS, incluyendo todo su personal y el personal contratado para realizar trabajos para la EFS, cumple con los requerimientos éticos relevantes.

La EFS debe enfatizar la importancia de cumplir los requisitos éticos en el trabajo.

Todo el personal de la EFS y todos los que realizan trabajos para la EFS deben demostrar un apropiado comportamiento ético.

- *El jefe de la EFS y su personal gerencial deben dar el ejemplo de un apropiado comportamiento ético.*
- *Los requerimientos éticos relevantes deben incluir los requerimientos estipulados en el marco legal y regulatorio que gobierna las operaciones de la EFS.*
- *Los requerimientos éticos para las EFS pueden incluir o estar basados en el código de ética de la INTOSAI (ISSAI 30) y en los requerimientos éticos de la Federación Internacional de Contadores (IFAC), apropiados a su mandato, circunstancias y las circunstancias de su personal profesional.*
- *Las EFS deben asegurarse que existen políticas y procedimientos que refuerzan los principios fundamentales de ética profesional como está definida en la ISSAI 30, por ejemplo:*
 - *integridad;*
 - *independencia, objetividad e imparcialidad;*
 - *secreto profesional; y*
 - *competencia.*
- *Las EFS deben asegurarse que todos los contratados a realizar trabajos para las EFS están sujetos a los apropiados acuerdos confidenciales.*
- *Las EFS deben considerar el uso de declaraciones escritas de su personal para confirmar el cumplimiento de los requerimientos éticos.*
- *Las EFS deben asegurarse que existen políticas y procedimientos para notificar oportunamente al jefe de la EFS de incumplimientos de los requerimientos éticos y permitir al jefe de la EFS tomar las acciones apropiadas para resolver estos asuntos.*
- *Las EFS deben asegurarse que existen políticas y procedimientos para mantener la independencia del jefe de la EFS, todo su personal y cualquier personal contratado para realizar trabajos para la EFS. (Para más información sobre independencia de las EFS, refiérase a la ISSAI 10 México Declaración de Independencia de la EFS y la ISSAI 11 Guía y buenas prácticas sobre la independencia de la EFS).*
- *La EFS debe asegurarse que existen políticas y procedimientos que refuerzan la importancia de rotar al personal clave en las auditorías, cuando sea apropiado, para reducir el riesgo de familiarizarse con la organización que está siendo auditada. Las EFS pueden también considerar otras medidas para reducir este riesgo.*

ISSAI 200: Normas Generales de Fiscalización Pública y Normas sobre los derechos y comportamiento de los auditores.

2. Normas con significancia ética

2.1 Las normas generales de fiscalización incluyen:

- (a) *Los auditores y la EFS deben ser independientes.*
- (b) *Las EFS deben evitar los conflictos de interés entre el fiscalizador y la entidad fiscalizada.*
- (c) *Los auditores y la EFS deben poseer la competencia profesional exigida.*
- (d) *Los auditores y la EFS deben emplear la debida diligencia y el máximo interés en el cumplimiento de las normas de auditoría de la INTOSAI. Esto abarca el empleo de la debida diligencia en la planeación y en la especificación, acumulación y evaluación de las pruebas, así como en el informe sobre resultados y en la elaboración de las conclusiones y recomendaciones.*

Independencia

2.3 *La necesidad de independencia y objetividad en la fiscalización es vital cualquiera que sea la forma de gobierno. Cierta grado de independencia, tanto del Poder Legislativo como del Ejecutivo, es esencial para la realización de la fiscalización y para la credibilidad de sus resultados.*

2.21 *La existencia de determinadas condiciones para ocupar el cargo de Titular de la EFS, como por ejemplo su nombramiento por un largo periodo de tiempo o hasta una edad concreta de jubilación puede contribuir a la independencia de la EFS respecto del Ejecutivo. A la inversa, la imposición de condiciones al respecto que inciten a la EFS a plegarse a los deseos del Ejecutivo tendría una repercusión erosiva en su independencia. Por esta razón es, en principio, deseable que las disposiciones relativas a la terminación del mandato o a la revocación del cargo sólo puedan aplicarse mediante un procedimiento especial semejante al que se utiliza para los miembros del Poder Judicial.*

2.27 La EFS no debe participar en la dirección ni en las actividades de las entidades fiscalizadas. Los auditores no deben ser miembros de los consejos de la Alta Dirección y si en el ámbito de sus funciones han de dar consejo, éste debe ser transmitido y aceptado claramente como asesoramiento o recomendación de auditoría.

2.28 El personal de la EFS que tenga estrechas relaciones de amistad, parentesco o de cualquier otro tipo con los directivos de una entidad fiscalizada que pudieran menoscabar su objetividad, no debe ser asignado a la fiscalización de la misma.

2.29 El personal de la EFS no debe ocuparse de instruir al personal de la entidad fiscalizada acerca de sus deberes. En los casos en que la EFS decida establecer una oficina en las instalaciones de la entidad fiscalizada con el fin de facilitar el examen continuo de sus operaciones, programas y actividades, el personal de la EFS no debe participar en proceso alguno de adopción de decisiones o de aprobación que se considere responsabilidad de la dirección de la entidad fiscalizada.

Conflictos de interés

2.31 Las EFS deben evitar los conflictos de interés entre el fiscalizador y la entidad fiscalizada.

2.32 La EFS cumple su función fiscalizando a las entidades cuentadantes e informando acerca de los resultados de la fiscalización. Para cumplir esta función, la EFS necesita conservar su independencia y objetividad. La aplicación de normas generales de auditoría adecuadas ayudará a la EFS a cumplir estos requisitos.

Competencia Profesional

2.35 El diálogo en el seno de la EFS fomenta la objetividad y la autoridad de sus opiniones y decisiones...

Diligencia debida

2.40 La EFS debe ser objetiva -y reflejarlo- en la fiscalización de los organismos y de empresas públicas. La EFS debe ser justa en sus evaluaciones y en su elaboración de informes de resultados de auditoría.

2.41 El ejercicio y aplicación de las diferentes especialidades técnicas debe ser de una calidad apropiada a la complejidad de cada fiscalización. Los auditores deben estar atentos a las deficiencias en el control, a las insuficiencias en la contabilidad, a las operaciones erróneas e irregulares, y a los resultados o situaciones que pueden ser indicativos de fraude, gastos inadecuados o ilícitos, operaciones no autorizadas, despilfarro, ineficiencia o falta de probidad.

2.46 Los datos relativos a las entidades fiscalizadas obtenidos por los auditores en el curso de sus tareas no deben ser utilizados para propósitos que queden fuera del alcance de la fiscalización y de la formación de una opinión, o de la elaboración de un informe conforme a las responsabilidades propias de un auditor. Es esencial que la EFS guarde reserva absoluta acerca del objeto de la fiscalización y de los datos obtenidos durante su realización. Sin embargo, la EFS debe estar facultada para dar cuenta a las autoridades competentes de las ilegalidades descubiertas.

10. Concientización de la integridad

10.1 Descripción

Además de las medidas para aumentar la resistencia de la organización a las violaciones a la integridad, se debe invertir en la recuperación moral de los miembros individuales del personal. La integridad, o la integridad de un acto, se preserva o deteriora a partir de la propia integridad de las personas involucradas. Para ello, se debe prestar atención a la formación y educación de los servidores públicos para que puedan responder adecuadamente ante situaciones de alto riesgo o cuando se enfrentan a dilemas en el trabajo.

10.2 Preguntas clave

- ¿Es la integridad un requisito explícito para todas las posiciones?
- ¿Se imparten cursos regulares de capacitación sobre el tema de integridad?
- ¿El personal en cargos vulnerables está informado de los riesgos particulares y medidas para contrarrestarlas?

- ¿El personal recibe asistencia especial y/o consejo para hacer frente a los riesgos de integridad?

10.3 Notas

La integridad como requisito explícito para todas las posiciones

Si una organización nombra la integridad como uno de los requisitos básicos para su personal, la competencia moral se deberá incluir sistemáticamente en el desarrollo o capacitación del personal.

Capacitación sobre integridad (entrenamiento sobre dilemas, juicio moral)

Debe invertirse en el fortalecimiento de la competencia moral del personal. La competencia moral es la voluntad y la capacidad para llevar a cabo tareas de forma adecuada y cuidadosamente, a la luz de todas las responsabilidades aplicables, incluso en situaciones nuevas, cambiantes y complejas para las cuales no existen directrices claras. Los cursos de capacitación enseñan a los servidores públicos a llegar a una conclusión moralmente correcta, la cual esté en concordancia con los valores de la organización y las normas.

Informar al personal de los riesgos y medidas de integridad

Adoptar las medidas adecuadas para reducir la exposición a las violaciones a la integridad no es suficiente. La organización también debe informar plenamente al personal, en situación de vulnerabilidad, de los riesgos y medidas de integridad implementadas. El personal debe ser consciente de los peligros potenciales y ser receptivo a las primeras señales de conducta inadecuada y responder a ellas convenientemente. Si es así, la organización puede hacer demandas estrictas al personal que lleva a cabo actividades vulnerables. Estos miembros del personal deberán ser examinados (véase también la sección sobre gestión de personal). El análisis correspondiente también deberá considerar las circunstancias personales y conducta del personal, por ejemplo, si tienen deudas o adicciones, etc.

Asistencia/consejo de integridad

El consejero de integridad (también) desempeña un papel de asesoramiento. Además de ser el funcionario de enlace, el consejero de integridad es una fuente para proveer orientación a los servidores públicos que enfrentan un problema de integridad.

11. Actitud de la Alta Dirección

11.1 Descripción

Las organizaciones y los estilos de dirección difieren entre sí en muchos aspectos. El estilo de gestión adoptada por una organización influirá en su integridad. La propia Alta Dirección debe dar un buen ejemplo y activamente llevar a cabo una política de integridad bien constituida. Si la Alta Dirección establece un mal ejemplo, el personal estará más inclinado a copiar su comportamiento y también será culpable de la falta de integridad. Si la Alta Dirección no implementa una política de integridad, o lo hace a medias, dará la impresión de que la integridad no tiene alta prioridad.

11.2 Preguntas clave

- ¿La Alta Dirección promueve activamente la importancia de la integridad?
- ¿La Alta Dirección busca activamente la implementación de una política de integridad y de medidas de integridad?
- ¿La Alta Dirección siempre responde adecuadamente a los problemas de integridad?
- ¿La Alta Dirección en sí misma cumple con las regulaciones de integridad y/o el código de conducta?

11.3 Notas

Fomento de la importancia de la integridad por parte de la Alta Dirección

No es suficiente que la Alta Dirección demuestre que ellos mismos actúan con integridad. Deben demostrar con palabras y hechos que la integridad es importante, que exige vigilancia y que a través de

la política de integridad, la organización ayuda al personal a ser buenos servidores públicos. Pueden hacerlo de palabra, enfatizando la importancia de la integridad, por ejemplo en la declaración de la misión de la organización, en los discursos, en los medios de comunicación internos y en los contactos informales. Pueden hacerlo, de hecho, mediante el desarrollo y adopción formal de una política de integridad, asignando al personal y proporcionando los recursos para ello, y asegurando su implementación.

Rectoría de la Alta Dirección

La Alta Dirección debe buscar activamente la puesta en práctica de una política y medidas de integridad. Al hacer esto, se debe lograr un equilibrio entre:

- Medidas preventivas y sancionatorias
- Cumplimiento y estímulo

Un sistema de integridad debe contener componentes tanto preventivos como sancionatorios. Los componentes preventivos están diseñados para prevenir las violaciones de integridad, mientras que los componentes sancionatorios están diseñados para detectar, investigar y sancionar violaciones. Si una violación de integridad queda impune, dará lugar a una pérdida de motivación entre el personal de la organización. Aunque ambos componentes son necesarios, la inversión debe centrarse en las medidas preventivas. El esfuerzo que implica prevenir incidentes es más sostenible, positivo, tiene un impacto más amplio y es menor (incluso en costo) que el esfuerzo requerido para investigar y reparar los daños, así como de restablecer la confianza después de un incidente.

Un sistema de integridad debe incluir elementos tanto de cumplimiento y estímulo. La estrategia de cumplimiento está basada en las reglas y, como tal, está dirigida a la imposición de regulaciones, directrices y los procedimientos antes señalados, así como al control y sanción de los comportamientos inaceptables. La estrategia de estímulo, por otro lado, está dirigida a fomentar la conciencia y la responsabilidad de la integridad entre el personal (competencia moral). Como regla general, un buen equilibrio se refiere al énfasis en el cumplimiento cuando este sea necesario, y al énfasis en el estímulo siempre que sea posible.

Tratando con problemas de integridad

La Alta Dirección debe abordar y solucionar los problemas de integridad con cuidado, pues el personal tomará nota de su respuesta y seguirá su ejemplo. La respuesta correcta de la Alta Dirección tendrá un impacto positivo en la conciencia que tenga el personal sobre la integridad. Véanse también las notas en la sección 10.3 sobre la respuesta a violaciones de integridad.

Papel ejemplar de la Alta Dirección

Un funcionario público debe actuar "como corresponde a un buen servidor público". En el primer caso, un servidor público es responsable de sus propios actos y omisiones. Si la organización y la Alta Dirección son buenos empleadores, van a animar y apoyar a su personal en esta área. La Alta Dirección, de arriba a abajo, debe establecer un buen ejemplo para el personal y ser ejemplo de integridad. Sus miembros deben ser conscientes de que su personal no sólo escucha lo que dicen, sino que sobre todo, observa lo que hacen.

12. Cultura organizacional

12.1 Descripción

La cultura organizacional da forma a la manera en que el personal de la organización se trata entre sí (internamente) y se comporta ante terceras partes (externos). La cultura es un área compleja y tiene una gran influencia en la integridad dentro de la organización. La cultura organizacional también incluye formas menos formales de conducta, tales como el ambiente de trabajo, el estilo de liderazgo, la

capacidad de discutir cuestiones y problemas privados, el compañerismo y la lealtad, y la apertura de la organización a la crítica y a la tolerancia de errores.

La atención que la Alta Dirección presta a la integridad, la importancia que concede a la misma y si existe una comunicación abierta al respecto; la apertura con las partes externas; la institucionalización de la integridad a través de consultas y entrevistas de desempeño, y la apertura mostrada cuando se tratan violaciones de integridad, son también aspectos importantes de la cultura organizacional. La clave de la promoción de la integridad a través de la cultura organizacional es la comunicación. La Alta Dirección debe fomentar la discusión de los problemas y dilemas, así como la prestación de asesoría.

12.2 Preguntas clave

- ¿Se presta regular atención a la importancia de la integridad?
- ¿Se pueden discutir las cuestiones de integridad de manera segura?
- ¿Hay suficientes oportunidades para expresar la crítica?
- ¿Está claramente explicada la importancia que tiene la integridad en la vinculación externa de la EFS?
- ¿Existe una comunicación abierta sobre las violaciones de integridad y la manera en que son tratadas?
- ¿Existe una cultura de hacerse responsables unos a otros de su propia conducta?
- ¿Se presta suficiente consideración a la satisfacción laboral?

12.3 Notas

Apertura interna y comunicación

Tener una política de integridad es fundamental, sin embargo, la comunicación de la misma no es menos importante. Para asegurarse de que se presta atención adecuada y permanente a la importancia de la integridad, deben aprovecharse todos los medios de comunicación disponibles. Si una organización no presta suficiente atención a la integridad o no resalta su importancia, se abre la puerta a los riesgos. Por un lado, podría conducir al personal a no darse cuenta de la gran importancia que la organización concede a la integridad. Por otra parte, podría dar lugar a la incertidumbre sobre el comportamiento que la organización espera del personal y lo que el personal debe hacer desde la perspectiva de integridad. Por lo tanto, es importante que la organización plantee regularmente la cuestión de la integridad. Al hacerlo, se mostrará que la integridad es importante y que se espera que el personal actúe con integridad. La integridad puede ser comunicada de diversas maneras y en distintos momentos:

- durante las entrevistas de desempeño y la evaluación/consulta del trabajo;
- mediante la producción y difusión de la información;
- a través de la organización mediante el apoyo a la Alta Dirección con paquetes de información y capacitación específica que favorezca la familiarización a la integridad de una manera natural y profesional;
- durante los cursos internos y de capacitación externa.

Capacidad para discutir problemas, dilemas y críticas con los superiores y colegas

La capacidad de discutir los problemas particulares y profesionales es una condición importante para la integridad. Si no se pueden discutir, el personal no será capaz de encontrar respuestas. Existe un riesgo de deterioro de la situación, que culmina en la pérdida de integridad. Lo mismo es cierto para los dilemas concretos que puedan surgir en el trabajo. Si no pueden ser discutidos, existe el riesgo de exceso de confianza en las opiniones personales y juicios del personal. La Alta Dirección en particular debe ser receptiva a los problemas, dilemas y críticas. Sin embargo, entre colegas también se debe ser capaz de tratar los problemas o inconsistencias en la conducta. Se genera una cultura de responsabilidad si los colegas no titubean en la discusión de temas difíciles, ni respecto a la sustancia y

límites de sus responsabilidades con los demás, ya sea que así se les haya instruido o no, con el fin de clarificar y poner a prueba las posiciones comunes morales y buscar marcos morales aplicables.

Apertura exterior y comunicación

La buena comunicación con terceros también contribuye a la integridad de la organización. Una organización con una cultura abierta indica lo que representa y de lo que es responsable. Dicha apertura es particularmente importante en los contactos con el público, proveedores, empresas e instituciones sociales. La publicación de los códigos de conducta en Internet o, mejor aún, la distribución activa de ellos o el involucramiento de partes externas en su elaboración contribuye a un buen entendimiento de las expectativas y obligaciones de cada una de las partes.

Apertura al tratar las violaciones de integridad

Un aspecto importante de la cultura de una organización es su respuesta consistente a violaciones de integridad. No realizar acción alguna o brindar respuesta a medias es una señal para el personal de que la organización no valora la integridad. En consecuencia, la falta de integridad de una persona anima la de otra. También existe el riesgo de que las infracciones menores crezcan y se conviertan en violaciones más serias si no se corrigen. Independientemente de la gravedad de la infracción, la Alta Dirección debe actuar consistente y conscientemente, y comunicar las respuestas al personal y a la organización para dejar en claro que dicha conducta no es tolerable.

Responsabilidad mutua

Un aspecto importante de una cultura abierta que promueve la integridad, es que los miembros del personal pueden hacerse mutuamente responsables de su comportamiento y así ayudar a mantener la integridad de la organización.

Satisfacción laboral

La falta de satisfacción laboral en el personal puede tener todo tipo de consecuencias negativas para la organización, tales como la baja productividad y el ausentismo elevado. También es una situación propensa a una conducta inaceptable. Por lo tanto, la Alta Dirección debe estar alerta a las señales de que el personal tiene poca o ninguna satisfacción en su trabajo. Las condiciones de trabajo tienen un gran impacto sobre la satisfacción laboral y, con ello, en la integridad del personal. El salario, la facilidad para tomar cursos de capacitación y la oportunidad de progresar dentro de la organización contribuyen a la satisfacción laboral. El personal mal pagado es susceptible al soborno. El personal que no puede desarrollarse profesionalmente se puede volver insatisfecho y amargado, y por lo tanto representa un riesgo de integridad. Por consiguiente, la organización debe reconocer la importancia de los esquemas de remuneración y los planes de capacitación y desarrollo profesional establecidos en la institución.

13. Reclutamiento y selección

13.1 Descripción

El personal es el capital social de la organización. Es por eso que la política de integridad debe centrarse en el personal. La gestión de recursos humanos y la política de personal proporcionan muchas oportunidades para que la organización considere la integridad del personal.

13.2 Preguntas clave

- ¿Existe un procedimiento establecido para tratar con todas las aplicaciones (de empleo)?
- ¿Se consulta a un comité asesor de selección (de personal)?
- ¿Se evalúan (antes de su contratación) las competencias profesionales e integridad moral necesarias para el cumplimiento de sus tareas, del personal y en particular de los auditores de la EFS (ISSAI 1: Declaración de Lima, Sección 14.1)?
- ¿Se corroboran los CV, diplomas, referencias, etc.?

- ¿Es el tema de integridad parte relevante del programa de inducción para los nuevos miembros del personal?
- En los casos que se requiere, ¿el personal firma una declaración de confidencialidad?
- ¿Se considera periódicamente la integridad a través de las evaluaciones/consultas de trabajo y entrevistas de desempeño?
- ¿Es la integridad una consideración específica en la contratación de personal temporal y externo?
- ¿Se ha considerado el tema de integridad cuando el personal deja la institución o durante las entrevistas de salida?

13.3 Notas

Reclutamiento, selección y procedimientos de contratación

La organización debe estar atenta a las "manzanas podridas", es decir, el personal deshonesto, durante el proceso de contratación de nuevo personal. La experiencia muestra que el comportamiento inapropiado de una persona induce a un comportamiento similar por otros. Este tipo de personas representa una amenaza seria a la integridad de la organización. Por tanto, es importante que la organización tenga una buena política de contratación. La selección de personal de nuevo ingreso deberá tener en cuenta no solamente las cualidades profesionales, como la formación académica y la experiencia laboral; debe además prestar atención a la confiabilidad de los nuevos miembros del personal. Esto en todo caso incluye:

- la introducción y el apego a un procedimiento de aplicación fijo para evitar decisiones arbitrarias y el favoritismo. La decisión de contratar a alguien debe ser tomada por más de una persona (por ejemplo, por un comité de selección);
- Los CV, diplomas y referencias deberán ser revisados con el fin de tener una impresión de los antecedentes del solicitante y de su desempeño (e integridad) en cargos anteriores.

Revisión

Las normas profesionales (ISSAI 1: Declaración de Lima, Sección 14.1) requieren que la Alta Dirección y el personal de las EFS sean evaluados respecto a sus competencias profesionales e integridad moral con el fin de garantizar que puedan cumplir plenamente sus funciones.

El personal debe ser examinado no sólo cuando éste se incorpora a la organización, sino también cuando se cambie de cargo o responsabilidad. La evaluación debe repetirse periódicamente y puede incluir:

- una revisión del expediente del solicitante;
- la presentación de un certificado de buena conducta;
- un control de seguridad (servicios de seguridad e inteligencia).

Consideración de la integridad durante la introducción/inducción

El personal de nuevo ingreso no conoce los reglamentos, procedimientos y comportamientos esperados por la organización a la que acaba de incorporarse, ni los canales que debe utilizar para plantear cuestiones de integridad. Se necesita algún tiempo para que un nuevo miembro del personal se familiarice y adquiera los conocimientos básicos para el desarrollo de sus actividades. En un principio, tanto él como la organización serán vulnerables. Los nuevos miembros del personal deben, por lo tanto, ser informados acerca de la importancia de la integridad cuando se integren a la organización. Aquí es donde cobra relevancia una buena política de introducción/inducción, con especial consideración en la integridad. Una buena política de introducción/inducción incluye:

- hacer juramento o protesta oficial en relación con la integridad;
- explicar y proporcionar el código de conducta;
- presentar al consejero de integridad.

Declaración de confidencialidad

El personal de nuevo ingreso debe ser informado de las cuestiones de integridad en su trabajo. Hacerlos firmar una declaración de confidencialidad es un medio especial para atraer su atención a estos temas.

Consideración de la integridad en la consulta/evaluación de trabajo y entrevistas de desempeño

El tema de la integridad debe ser planteado en diversos momentos. Dado que la política de integridad debe ser una parte fija de la política de personal, la integridad debe también ser considerada durante la consulta o evaluaciones de trabajo, así como durante las entrevistas de desempeño.

Contratación de personal temporal o externo

A menudo, se contrata personal externo para solventar temporalmente los desafíos de capacidad institucional o para proporcionar los conocimientos técnicos específicos que la organización pudiera no tener. Se debe prestar un cuidado especial a dicho personal, dado que podrán no estar conscientes de las reglas específicas y procedimientos (estructura) o valores (cultura) que prevalecen en la organización. La EFS debe estar preparada para esto y formular una política específica ante la contratación requerida de personal externo.

Consideración de la integridad cuando el personal deja la organización

Los empleados pueden dejar la organización por varias razones. Pueden jubilarse, puede concluir un contrato temporal, puede ser que se tenga una alternativa laboral distinta o que no se está satisfecho con la organización. Cualquiera que sea la razón, las entrevistas de salida siempre deben realizarse cuando un miembro del personal se marcha de la institución. El empleador debe saber por qué la gente deja la organización. Es factible que la gente esté insatisfecha con la cultura, la remuneración salarial, el estilo de la Alta Dirección o las perspectivas de desarrollo profesional. Las entrevistas de salida representan un insumo importante porque a partir de sus hallazgos se puede facilitar la identificación los factores que pueden propiciar una conducta inaceptable. Cuando los empleados abandonan la organización se sienten más libres para hablar de tales asuntos y expresan sus opiniones con más facilidad. También podrían señalar en dónde es que la organización puede emprender mejoras.

Como parte de la política de salida:

- las entrevistas de salida deben realizarse cada vez que un miembro del personal se va;
- durante la entrevista de salida, el empleador debe preguntar en dónde se pueden hacer mejoras;
- la cuestión de la integridad debe ser planteada durante la entrevista de salida;
- se debe hacer un informe de todas las entrevistas de salida;
- las entrevistas de salida deben ser registradas y coordinadas por el departamento de recursos humanos, y
- deben elaborarse análisis anuales sobre las razones por las que se deja a la institución y los puntos de mejora.

14. Respuesta a violaciones de integridad

14.1 Descripción

Independientemente de las medidas preventivas implementadas para favorecer que no ocurran violaciones a la integridad, la organización debe estar plenamente preparada para reaccionar ante una violación de integridad o ante la sospecha de alguna en particular. Una respuesta eficaz a una violación (ya sea real o presunta) también ayudará a prevenir futuras violaciones; confirma los valores y normas y anima al personal a resistir ante tentaciones. La sospecha de una violación conduce rápidamente a la inestabilidad y tensión dentro de la organización. Se requiere pues una adecuada preparación para evitar una mayor escalada y ayudar a restablecer la calma. Las medidas esenciales incluyen:

- notificación y procedimientos de denuncia para identificar violaciones reales o potenciales de manera oportuna;

- procedimientos de investigación sistemática;
- sanciones (castigos) establecidos en un marco claro;
- registros de violaciones reales o potenciales y de sanciones implementadas.

14.2 Preguntas clave

- ¿Está establecido un procedimiento de notificación para que los empleados reporten sospechas de violaciones (procedimiento de denunciantes)?
- ¿Los empleados pueden acceder con facilidad a la Alta Dirección o a los mandos medios superiores para reportar sospechas de violaciones?
- ¿Se involucra a un consejero de integridad en el proceso de notificación de violaciones?
- ¿Existe un procedimiento para manejar señales y quejas procedentes de fuentes externas?
- ¿Existe un protocolo para investigar las violaciones de integridad?
- ¿Se registran de manera central las violaciones de integridad?
- ¿La organización siempre responde a las violaciones de integridad?
- ¿Las sospechas de delitos son reportadas al ministerio público o a la policía?
- ¿Los incidentes son evaluados y discutidos con el personal involucrado?

14.3 Notas

Procedimiento de notificación y participación de la Alta Dirección y de los consejeros de integridad

Antes de que se pueda responder a una violación de integridad, la Alta Dirección de la organización debe saber sobre ella. Los procedimientos, por lo tanto, deben estar bien establecidos para reportar conductas inadecuadas, y para proteger a los servidores públicos que informan a la Alta Dirección. Tales procedimientos se conocen comúnmente como sistemas de denunciantes. Por lo general, se caracteriza al tipo de conducta inapropiada que debe ser reportada, como se señala a continuación:

- delitos serios;
- violaciones graves de los reglamentos o normas;
- el engaño a las autoridades judiciales;
- amenazas graves a la salud pública, a la seguridad o al entorno;
- supresión deliberada de la información sobre dichas conductas.

Una condición previa para la presentación de informes o denuncias sobre sospechas de violaciones, es que la Alta Dirección sea accesible a los empleados.

Las notificaciones deben basarse en "sospechas razonables" y no deben ser hechas con el propósito de obtener beneficios personales o para criticar las decisiones políticas. El procedimiento de notificación deberá complementar el diseño de la función del consejero en la organización. De manera complementaria al procedimiento de notificación, un procedimiento de quejas ayuda a recibir señales externas acerca de posibles conductas inapropiadas (por ejemplo, del público en general).

Manipulación de señales y quejas de fuentes externas

La organización no sólo debe contar con procedimientos establecidos para los denunciantes internos, sino también para el manejo de señales y quejas de fuentes externas.

Protocolo de investigación

Debe establecerse un protocolo o procedimiento para investigar las denuncias de posibles conductas inapropiadas. Se debe establecer, por ejemplo, cómo la investigación se llevará a cabo y quién será el responsable de ella.

Registro de conductas inapropiadas

Los registros deben contener, entre otras cosas, la notificación de violaciones reales o potenciales, información sobre el seguimiento de las notificaciones y las sanciones aplicadas. Los registros forman la base de la información suministrada a la Alta Dirección.

Sanciones (respuesta a violaciones)

La sanción (castigo) de violaciones de integridad debe estar basada en una política de sanciones que establezca los criterios que se utilizan para decidir cómo una violación de integridad será castigada. Las políticas de sanciones muestran al personal qué tan seriamente la Alta Dirección asume la integridad. En este sentido, debe mantenerse un registro de las sanciones impuestas en el pasado y las razones para hacerlo.

Presentación de informes al Ministerio Público o la policía

Si se piensa que se ha cometido un delito, podría informarse al Ministerio Público o a la policía. En algunos casos, podría incluso ser obligatorio reportar tales incidentes. También podrían imponerse medidas disciplinarias como amonestaciones, suspensiones, trasferencias o despidos (deshonrosos).

Evaluación de incidentes

Aprender de los incidentes es importante para evaluar las violaciones de integridad después de que éstas hayan sido investigadas. Tal vez la violación no es un incidente aislado y denota más bien un patrón más amplio de incumplimiento de integridad. La evaluación de estos incidentes es útil para identificar si existen debilidades (sistemáticas) en los controles, lo que posiblemente hace factible la violación. Finalmente, las violaciones de integridad y sus consecuencias pueden tener un impacto significativo en el personal que trabaja en el medio donde la violación tuvo lugar, por ejemplo, colegas directos del infractor. Esto debe tenerse en cuenta para implementar las medidas para elevar la moral y no afectar la calidad del trabajo fiscalizador en cuestión.

15. Transparencia y Rendición de Cuentas

15.1 Descripción

La integridad de la organización es de gran importancia para las partes interesadas, tanto las internas como las externas. La Alta Dirección debe, por tanto, tomar en cuenta a ambos en el diseño y operación del sistema de controles de integridad y cualquier cambio que en él se suscite. La rendición de cuentas también hace que la Alta Dirección se sienta más responsable por la integridad de la organización.

La ISSAI 20 dedica especial atención a la transparencia y la rendición de cuentas como un elemento de buena gobernanza para las EFS. Esto está explícitamente reflejado en cuestiones clave de este grupo del Sistema de Controles de Integridad.

15.2 Preguntas clave

General

- ¿La Alta Dirección recibe informes que den cuenta del estado de la política de integridad implementada?
- ¿Los representantes del personal reciben informes que den cuenta del estado de la política de integridad implementada?
- ¿Las autoridades elegidas democráticamente (Congreso, Consejo Municipal, etc.) reciben informes que den cuenta del estado de la política de integridad implementada?
- ¿Los informes están sistemáticamente estructurados y contienen indicadores claros?

Específico para las EFS

- ¿Se publican el mandato, papel, responsabilidades, organización, misión, estrategias, manuales de auditoría, procedimientos y criterios de auditoría de la EFS (ISSAI 20, capítulo 2/3)?

- ¿Los hallazgos y conclusiones de auditoría de la EFS se sujetan a procedimientos contradictorios (consulta/comparecencia con la entidad auditada) (ISSAI 20, capítulo 3)?
- ¿Las cuentas públicas de la EFS se sujetan a auditoría externa o revisión del Congreso (ISSAI 20, capítulo 4)?
- ¿La EFS está abierta a medidas para prevenir la corrupción y garantizar la transparencia y la legalidad en sus propias operaciones (por ejemplo, las sanciones disciplinarias) (ISSAI 20, capítulo 5)?
- ¿Se publica información de los auditores, tales como sus facultades y obligaciones (ISSAI 20, capítulo 5)?
- En los casos en que se recurre a la subcontratación, pericia y servicios de auditoría externos, sean adquiridos de otras entidades públicas o privadas, ¿la responsabilidad de su desempeño recae en la EFS y se les sujeta a reglas precisas (ISSAI 20, capítulo 5)?
- ¿Se publica el código de ética de la EFS (ISSAI 20, capítulo 5)?
- ¿La EFS emite informes públicos sobre los resultados de auditoría, así como respecto a su gestión y desempeño, y se comunica abiertamente con los medios de comunicación u otras partes interesadas (ISSAI 20, capítulo 6)?

15.3 Notas

Rendición de cuentas interna (Alta Dirección y representantes del personal)

Debe someterse a la Alta Dirección y a los representantes del personal, de manera periódica, los informes de integridad. La cuenta rendida a la Alta Dirección podría formar parte de la planeación de la organización y el ciclo de control/gestión. De ser el caso, el informe a los representantes del personal podría proporcionarse como parte del Reporte Social Anual, o el documento similar aplicable.

Rendición de cuentas externa (autoridades elegidas democráticamente)

La organización debe también informar externamente sobre su integridad, por ejemplo, como parte de un reporte anual, a las autoridades elegidas democráticamente (ejemplo, congreso o consejo municipal). Al hacerlo, reconoce ante las partes interesadas externas la importancia que asigna a la integridad.

También se debe rendir un informe a los supervisores de la organización, así como a las autoridades elegidas democráticamente. Los supervisores pueden entonces crearse una imagen del Sistema de Controles de Integridad que supervisan y determinar si hay alguna debilidad.

Dentro del sector público hay un deber general de rendir cuentas al público. El público, involuntariamente, contribuye a los fondos públicos sin el cual el sector público no podría ser capaz de funcionar. Las naturaleza exclusiva de las tareas públicas (tales como el tomar medidas coercitivas) también significa que al público se le deben dar garantías de que la integridad está salvaguardada en la medida de lo posible. Por medio de una cuenta externa, por ejemplo un informe anual, o a través de otra vía pública tal como el Internet, el público interesado puede tener una visión del diseño y operación de la gestión de la integridad.

Estructura sistemática de provisión de informes e indicadores claros

El valor de los informes para rendir cuentas de las políticas de integridad incrementa cuando se emplea una estructura sistemática, así como cuando se incluyen indicadores claros en los informes.

Normas Profesionales de las EFS

Debido a la naturaleza típica de las EFS, se aplican altos estándares en torno a la transparencia y la rendición de cuentas. Esto se refleja en la norma mencionada anteriormente, ISSAI 20: "Principios de Transparencia y Rendición de Cuentas".

16. Auditoría y monitoreo

16.1 Descripción

Las auditorías a la integridad son medidas *ad hoc* implementadas por la Alta Dirección para obtener una idea de la calidad del Sistema de Controles de Integridad de la organización. Dichas auditorías pueden ser realizadas por un departamento interno de control o auditoría, o bien por un auditor externo. Adquieren mayor valor si la Alta Dirección es consciente de los hallazgos y recomendaciones de auditoría, y responde consistentemente a ellos.

16.2 Preguntas clave

- ¿un auditor interno audita periódicamente el Sistema de Integridad?
- ¿un auditor o supervisor externo audita periódicamente el Sistema de Integridad?
- ¿la Alta Dirección monitorea o evalúa periódicamente el Sistema de Integridad?

16.3 Notas

Evaluación interna (departamento de control/auditoría interna)

El departamento de control o auditoría interna, o bien el área afín, debe llevar a cabo auditorías a la integridad, así como proporcionar informes de sus hallazgos a la Alta Dirección de la organización. Antes de que la auditoría inicie, debe decidirse su alcance y profundidad. Esto provee una oportunidad para conocer las necesidades de la Alta Dirección, en la medida de lo posible; sin embargo, podría ponerse en tela de juicio la independencia de esta auditoría.

Evaluación externa (auditor/supervisor externo)

El auditor/supervisor externo revisa e informa sobre la gestión de la integridad en la organización. En el caso de la auditoría externa, el auditor o supervisor determinará el alcance y profundidad (con referencia a la regulación aplicable). Este tipo de revisión contribuye a respaldar la independencia de la auditoría. Para que la revisión de realizada por un auditor externo tenga un impacto positivo debe, sin embargo, generar resultados que puedan ser empleados por la Alta Dirección.

Monitoreo y evaluación de la política

La política de integridad debe ser expresada en objetivos y actividades concretas. Para evitar que los objetivos y actividades sean pasados por alto, deben formar parte del ciclo de planificación y control establecido para vigilar los procesos de la organización. Dentro de esta estructura, los informes de gestión notificarán a los altos directivos sobre la ejecución de las actividades acordadas y sus resultados. Se deben hacer revisiones periódicas de los logros de la política de integridad. ¿Se implementaron realmente las actividades y medidas acordadas?, ¿La política arrojó el resultado deseado? Si el resultado no es del todo satisfactorio, la política debe ser revisada.

d. Evaluación del nivel de madurez

La evaluación del nivel de madurez del Sistema de Controles de la Integridad proporciona una idea general de la resistencia que la organización ha desarrollado en torno a posibles violaciones a la integridad.

En una situación ideal, el nivel de madurez se basa en:

- la presencia de medidas;
- la calidad y conveniencia de las medidas y de su diseño;
- la comunicación de las medidas y la concientización que al respecto se genere en el personal;
- la aceptación de las medidas;
- la incorporación de las medidas en el ciclo de planeación y control;
- la calidad de la implementación de las medidas, y su obligatoriedad;
- el suministro de información y la rendición de cuentas para la implementación y efecto de las medidas;
- la evaluación y, en caso necesario, la revisión de las medidas.

Podría ser muy complejo incluir todos estos elementos por separado en el método de evaluación. Por lo tanto, se ha diseñado un método relativamente sencillo para calificar el nivel de madurez:

Nivel	Criterio
0	- La medida no existe, al menos hasta donde tengo conocimiento
1	- La medida existe - Sin embargo, la medida no es implementada / no se observa
2	- La medida existe - La medida se implementa / observa - Sin embargo, la medida no es eficaz
3	- La medida existe - La medida se implementa / observa - La medida es eficaz

El puntaje indica el nivel de madurez ya alcanzado. En principio, el nivel de madurez requerido es de alto nivel. En ciertas organizaciones, sin embargo, algunas medidas serán menos relevantes o no aplicables. Esto quedará más claro cuando se evalúe el nivel de madurez y se discutan los resultados con los participantes.

La evaluación del nivel de madurez considera todas las medidas relevantes y sus efectos. Como se ha enfatizado, esta evaluación bien puede hacerse a toda una organización o bien respecto a las medidas implementadas por un departamento o división organizacional específica.

Evaluación del nivel de madurez del Sistema de Controles de la Integridad

Para evaluar el nivel de madurez del Sistema de Controles de la Integridad, puede ser conveniente la discusión de los grupos de medidas se discuta grupalmente (grupos pequeños de tres a cuatro integrantes), pero manteniendo la calificación de manera individual.

La evaluación del nivel de madurez del Sistema de Controles de la Integridad se realiza en 3 pasos:

1. Se evalúa el nivel de madurez de cada medida promediando los puntajes individuales y haciendo una discusión grupal;
2. Se define el nivel de madurez de cada grupo de medidas computando el promedio de las calificaciones otorgadas a cada una de las medidas en el grupo;
3. Se define el nivel de madurez de todo el Sistema de Controles de la Integridad, registrando el promedio de los grupos.

e. Análisis de las fortalezas y debilidades del Sistema de Controles de la Integridad

A partir de la evaluación completa del Sistema de Controles de la Integridad, es ahora posible resumir los resultados sobre los principales grupos. Esto permitirá un análisis de las fortalezas y debilidades relativas del Sistema, mediante el registro de los puntajes promedio del nivel de madurez de cada grupo y, posteriormente, el cálculo de la calificación promedio total (ver tabla mostrada a continuación). Las calificaciones se registran en el informe a la Alta Dirección.

Núm	Grupos de Controles	Promedio	Nivel
	Controles Generales		
1	Marco de política de integridad		
2	Análisis de vulnerabilidad / análisis de riesgos		
13	Reclutamiento y selección		
14	Respuesta a las violaciones de la integridad		
15	Rendición de cuentas y transparencia		
16	Auditoria y monitoreo		
	Controles Duros		
3	Responsabilidades		
4	Marco legal de la EFS		
5	Legislación y regulaciones sobre integridad		
6	Organización administrativa / control interno		
7	Seguridad		
	Controles suaves		
8	Valores y normas		
9	Normas profesionales de la EFS		
10	Concientización de la integridad		
11	Actitud de la Alta Dirección		
12	Cultura organizacional		
	Promedio general de todos los grupos		

El promedio total determina el nivel de madurez del Sistema de Controles de Integridad, en su totalidad. Ver tabla mostrada a continuación.

Puntaje del nivel de madurez del Sistema de Controles de la Integridad	Nivel
$0 \leq x \leq 1$	1 Bajo
$1 < x \leq 2$	2 Medio
$2 < x \leq 3$	3 Alto

El nivel de madurez es el insumo base para realizar el análisis de brechas que se estudia en el siguiente capítulo.

IX. Análisis de brechas

a. Descripción

Después de completar la evaluación tanto de las vulnerabilidades (incluyendo la de los factores que agravan la vulnerabilidad) como del nivel de madurez del Sistema de Controles de la Integridad, es posible analizar si este Sistema es eficaz, es decir, si sus medidas contrarrestan eficazmente el nivel de vulnerabilidad de la organización y de sus procesos. Si ambos elementos no están en equilibrio, hay una brecha, lo que usualmente implica que el Sistema de Controles de la Integridad requiere ser fortalecido.⁶

Este análisis de brechas puede realizarse en dos niveles o perspectivas agregadas:

- Nivel 1: en el nivel relativo a toda la organización, el Sistema de Controles de la Integridad como un todo debería estar en equilibrio respecto al nivel de vulnerabilidad de la organización/EFS;
- Nivel 2: en un nivel más detallado, el de riesgos específicos, el nivel de madurez o grado de robustez de los controles o medidas implementadas para mitigar las vulnerabilidades debería ser suficiente.

El taller *IntoSAINT* está diseñado para abarcar por lo menos un análisis de brechas en el primer nivel: en un nivel agregado o global. El segundo nivel (un análisis de brechas pormenorizado) es opcional, se recomienda pero sólo si las restricciones de tiempo e interés de los participantes lo permiten.

Las organizaciones pueden hacer frente a las vulnerabilidades de diferentes formas. Primero, pueden intentar eliminar o reducir las vulnerabilidades evitando las actividades vulnerables. En ocasiones, es posible llevar a cabo actividades de una manera diferente, eliminando así la ejecución de actividades que son vulnerables a violaciones de integridad. Esto implica que la organización podría ser capaz de abordar el origen de la vulnerabilidad. En la práctica, sin embargo, esto podría no ser factible (o lo sería con cierta dificultad). Las organizaciones públicas tienen obligaciones legales y no pueden evitar su involucramiento en actividades sensibles.

Usualmente, una manera más viable para hacer frente a la vulnerabilidad es diseñar e implementar controles o medidas (de integridad) compensatorias. Dependiendo del “nivel de madurez” del Sistema de Controles de la Integridad, la organización puede ser más o menos resistente a las vulnerabilidades que enfrenta.

Nivel 1 – Análisis de Brechas General

Primero, se necesita determinar si el nivel de madurez del Sistema de Controles de la Integridad de la EFS está en equilibrio o contrarresta eficazmente el perfil de vulnerabilidad de la entidad. Para saberlo, se compara el puntaje total del perfil general de vulnerabilidad con la puntuación total del nivel de madurez del SCI. El (des)equilibrio resultante se expresa en un nivel agregado, lo que significa que el análisis de brechas a este nivel no pretende evaluar si hay un vínculo exacto entre una vulnerabilidad específica y una medida o control determinado. Como se mostró anteriormente, el Sistema de Controles de la Integridad (SCI) también incluye (grupos de) controles o medidas generales que no están

⁶ Es más viable fortalecer las propias medidas implementadas que abatir las vulnerabilidades, pues éstas últimas son inherentes o se agravan por la influencia de factores muchas veces externos o ajenos a la influencia de la EFS.

diseñadas específicamente para abordar o contrarrestar un riesgo o vulnerabilidad en específico, sino para tener un impacto mucho más amplio en la robustez o resistencia contra violaciones a la integridad. Ejemplos son la formulación de una política de integridad y un curso de capacitación para concientizar sobre la integridad. De esta manera, el análisis de brechas en este nivel permite establecer si la resistencia global de la entidad es consistente con su nivel total de vulnerabilidad.

Los participantes del taller discutirán las vulnerabilidades más relevantes identificadas durante la evaluación, así como las debilidades más destacadas que se identifiquen en el Sistema de Controles de la Integridad. Los participantes también discutirán posibles vínculos entre ambos elementos. El objetivo de la discusión es llegar a conclusiones y principalmente recomendaciones que se presentarán a la Alta Dirección sobre cómo reducir las vulnerabilidades y/o mejorar el Sistema de Controles de la Integridad.

Si el objetivo de la autoevaluación es obtener una visión global del nivel de vulnerabilidad y/o una idea general del estado que guarda el Sistema de Controles de la Integridad, el análisis de brechas podrá concluir hasta esta fase. Sin embargo, si la Entidad de Fiscalización Superior sujeta a la autoevaluación quiere tener una clara impresión sobre los riesgos específicos y los mecanismos más convenientes para mitigarlos, se requiere un análisis de brechas más detallado (de nivel 2).

Nivel 2 – Análisis de Riesgos Detallado

El análisis en el nivel 2 comienza con la selección de los procesos más vulnerables.

Después de completar el perfil de la vulnerabilidad, los participantes en el taller compararán los procesos más importantes de la organización con las vulnerabilidades inherentes y, en caso de aplicar, también con los factores que agravan la vulnerabilidad. Partiendo de este análisis, los participantes identificarán así los procesos más vulnerables de la organización sujeta a la autoevaluación. Para mantener el enfoque adecuado, resulta muy útil limitar la selección de tres y hasta cinco procesos. La decisión grupal puede asumirse tras una votación, seguida por una discusión plenaria para llegar al consenso requerido.

El siguiente paso es la formulación de los riesgos específicos más importantes. Para ello, es necesario considerar los ‘acontecimientos indeseables’ o adversos que podrían presentarse como resultado de los procesos más vulnerables ya seleccionados. La pregunta clave que debe hacerse es ¿qué podría ir mal en estos procesos de manera tal que podría favorecerse o constatarse la presencia de violaciones a la integridad?

El nivel de riesgo inicial (bajo, medio, alto) para cada uno de los eventos identificados es la probabilidad de que dicho incidente pueda ocurrir. Se trata de un riesgo ‘bruto’, para el que la organización podría aun no haber considerado o previsto medidas o controles para mitigar posibles violaciones de integridad. Sólo tras haberse identificado o previsto medidas o controles para mitigar brechas de integridad, puede estimarse el así llamado riesgo ‘neto’.

Desde luego, es teóricamente posible pensar en un gran número de posibles ‘eventos’. Sin embargo, es necesario acotar el análisis a los riesgos más relevantes o que por su naturaleza detentarían mayor impacto organizacional, pues de otra forma se favorecería el desperdicio de esfuerzos, pues para la mayoría de estos eventos su probabilidad, y por tanto su riesgo, será baja. También es necesario tomar en cuenta que la sola identificación de muchos ‘problemas’ menores podría paralizar a la Alta Dirección e impactar negativamente en su compromiso a la acción. Es mejor concentrarse en un número limitado

de riesgos, los más urgentes. Por lo tanto, es recomendable concentrarse en un número limitado (tres a cinco) de los eventos posibles que podrían tener un alto impacto.

A fin de poder estimar el nivel de riesgo ‘neto’, se debe considerar la existencia (o implementación) o bien la ausencia (o ineficacia) de las medidas o controles para mitigar las brechas de integridad. La mayoría de las organizaciones implementan controles específicos con el objetivo de reducir los riesgos de integridad. Con el fin de obtener una estimación razonable del nivel de riesgo remanente, el efecto de estas medidas o controles debe de ser evaluado frente a los riesgos iniciales. Si los controles específicos ya están incluidos en el Sistema de Controles de la Integridad, entonces los puntajes o resultados registrados para su nivel de madurez se pueden utilizar para evaluar qué riesgos remanentes aún existen y deben solventarse.

Las conclusiones de esta evaluación, junto con las recomendaciones específicas para hacer frente a los riesgos remanentes, se deberán de incluir en el informe que se entrega a la Alta Dirección.

b. Recomendaciones e Informe

Un análisis de brechas minucioso y bien llevado a cabo conduce a y fundamenta adecuadamente las recomendaciones sobre la forma en que la Alta Dirección puede reducir el nivel general de riesgo mediante el establecimiento de prioridades y la aplicación de nuevas medidas, o bien el mejoramiento/fortalecimiento de las ya existentes.

El informe de la autoevaluación debe centrarse en el análisis de brechas, ya que este análisis muestra el nivel de la vulnerabilidad remanente, es decir la aún no abordada por la organización, lo cual debe ser la base para las formulación de las recomendaciones.

En esta parte del taller, se deben contestar las siguientes preguntas:

- ¿Qué se debe mejorar?
- ¿Qué debe hacer la Alta Dirección?

Existen dos tipos de posibles recomendaciones con base en la evaluación:

- Recomendaciones destinadas a reducir las vulnerabilidades y mitigar el impacto de los factores que agravan la vulnerabilidad, y
- Recomendaciones destinadas a mejorar los controles de integridad.

Para integrar las recomendaciones, los participantes trabajarán en subgrupos y emitirán las recomendaciones tanto para reducir la vulnerabilidad como para fortalecer los controles escribiéndolas en *post-its*. Durante las sesiones plenarias, los moderadores ayudarán a los participantes a combinar y agrupar las recomendaciones en temas relevantes y a calificarlas de acuerdo a la prioridad e importancia. Es importante agregar una línea del tiempo indicando qué tan pronto debería dar inicio la implementación de las recomendaciones.

Al final de la sesión, los moderadores recapitularán las recomendaciones y manejarán de nueva cuenta las prioridades, consultando a los participantes para asegurarse de que esta recapitulación refleje la opinión del grupo.

Con base en ello, los moderadores, en cooperación con el coordinador del taller, prepararán la versión preliminar del informe y la presentación a la alta dirección.

Por último, el informe de la autoevaluación, incluyendo las recomendaciones, debe ser presentado a la Alta Dirección, ya que ésta es la principal responsable del mantenimiento y eficacia del Sistema de Controles de la Integridad. De preferencia, una delegación de los participantes debe asistir a la reunión en donde los resultados del taller se presenten a la alta dirección, pues el taller refleja su evaluación y los participantes podrían responder preguntas y proporcionar comentarios.

Para favorecer la concientización sobre el tema de integridad y apoyar el enfoque de integridad en general y de las medidas específicas que se adopten, es recomendable comunicar los resultados del taller a toda la organización.

Anexo: Sistema de Controles de la Integridad

Grupo	Medida	
1		Marco de Política de Integridad
	1.1	Medidas de integridad incorporadas en un marco sistemático de políticas
	1.2	Objetivos concretos formulados como parte del Sistema de Integridad
	1.3	Tiempo y fondos presupuestados/previstos para la implementación de medidas de integridad
	1.4	Comunicación/divulgación de las medidas de integridad
	1.5	Política de integridad formalmente plasmada/incluida en un plan general de políticas
2		Análisis de la vulnerabilidad / Análisis de riesgos
	2.1	Realización regular de análisis de la vulnerabilidad general / análisis de riesgos
	2.2	Ejecución de análisis detallados para áreas y posiciones/responsabilidades vulnerables
3		Responsabilidades
	3.1	Designación de posiciones/cargos funcionales responsables de la integridad
	3.2	Realización de consultas sistemáticas entre servidores públicos responsables de la integridad
	3.3	Consejero de la Integridad
	3.4	Coordinación periódica con otras organizaciones y partes interesadas externas
	3.5	Designación de un coordinador (externo) para la política de integridad
4		Marco legal de la EFS
	4.1	Inclusión en la Constitución de la existencia e independencia de la EFS (ISSAI 10, principio 1)
		Existencia de un marco legal que garantiza:
	4.2	- la independencia del titular (y miembros, en el caso de instituciones colegiadas) de la EFS, incluyendo seguridad en el cargo y la inmunidad legal en el desempeño/descargo normal de sus funciones (ISSAI 10, principio 2)
	4.3	- un mandato suficientemente amplio y discreción plena en el ejercicio/ejecución de las funciones de la EFS (ISSAI 10, principio 3)

Grupo	Medida	
	4.4	- acceso irrestricto a la información (ISSAI 10, principio 4)
	4.5	- el derecho y obligación de informar sobre el trabajo de la EFS, y la libertad de decidir el contenido y la oportunidad/periodicidad de los informes de auditoría, así como de su publicación y divulgación (ISSAI 10, Principio 5/6)
	4.6	- la autonomía financiera y administrativa/de gestión, así como la disponibilidad apropiada de recursos humanos, materiales y monetarios (ISSAI 10, principio 8)
5		Legislación y regulaciones en materia de integridad.
		Existen reglas establecidas con respecto a:
		<i>a) Conflictos de interés</i>
	5.1	... cargos o puestos externos / intereses financieros
	5.2	... la aceptación de regalos / invitaciones / beneficios
	5.3	... confidencialidad
	5.4	... prevención de “arreglos de puerta giratoria” ⁷
	5.5	... evaluación/supervisión externa de los contratistas y/o solicitantes de licencias
	5.6	... cabildeo
	5.7	... influencia de políticos sobre los servidores públicos
		<i>b) Integridad dentro de las organizaciones</i>
	5.8	... combate/tratamiento/frente a conductas indeseables
	5.9	... solicitud de reembolso de gastos
	5.10	... uso de email, internet y de la línea telefónica
	5.11	... uso de la propiedad / bienes de los empleadores
6		Organización administrativa y control interno
	6.1	Especificación de actividades y posiciones/cargos vulnerables

⁷ Por “arreglos de puerta giratoria” (*Revolving-door arrangement*, en inglés) debe entenderse aquellos casos en los que una persona que un día trabaja para el gobierno, bien puede trabajar el siguiente para la iniciativa privada u otras organizaciones que buscan algo del gobierno (ej: proveedores, consultores, firmas de auditoría, etc).

Grupo	Medida	
	6.2	Existencia de procedimientos específicos para realizar actividades vulnerables
	6.3	Descripciones de puesto para todo el personal/todas las responsabilidades funcionales
	6.4	Segregación de funciones/tareas
	6.5	Aplicación del “Principio de cuatro ojos” ⁸
	6.6	Regulaciones sobre el mandato
	6.7	Esquema de rotación del trabajo (ISSAI 40, sección 6b, elemento 2)
7		Seguridad. Se han implementado medidas con relación con
	7.1	... seguridad física (cerraduras, ventanas, puertas, cajas de seguridad, etc.)
	7.2	... seguridad de la información (seguridad para las tecnologías de la información, política de escritorio limpio, ⁹ clasificación de la información como confidencial/secreta, autorizaciones de acceso, sistemas de archivo)
8		Valores y normas
	8.1	La integridad es parte de la misión de la organización
	8.2	Se han formulado los valores fundamentales (ej. imparcialidad, profesionalismo, etc.)
	8.3	Código de conducta (de integridad)
	8.4	Juramento o promesa
	8.5	Ceremonia especial para hacer un juramento o presentar la promesa
9		Normas Profesionales de la EFS
	9.1	La EFS no está involucrada (o parece no estarlo) de alguna manera en la dirección/gestión de las organizaciones que audita (ISSAI 11, principio 3, Pautas Básicas)

⁸ El “Principio de cuatro ojos”, también llamado de “dos firmas”, se refiere al trabajo realizado por, al menos, dos personas para asegurar la revisión/validación de las tareas llevadas a cabo, particularmente en casos de actividades vulnerables.

⁹ La “política de escritorio limpio” implica mantener el lugar de trabajo de manera ordenada y asegurar la debida clasificación de los documentos. Su enfoque es preservar la confidencialidad de la información ante terceras partes.

Grupo	Medida	
	9.2	Al trabajar con el ejecutivo, los auditores actúan únicamente como observadores y no participan en el proceso de toma de decisiones (ISSAI 11, principio 3, Pautas Básicas)
	9.3	Existencia de lineamientos emitidos por la EFS para asegurar que su personal no desarrolle una relación demasiado cercana con las entidades que audita, para que así sigan siendo objetivas y además lo parezcan (ISSAI 11, principio 3, Pautas Básicas)
	9.4	Existencia de cursos de capacitación ofrecidos al personal, para introducir/inducir sobre la importancia de la independencia en la cultura de la EFS, y para enfatizar la calidad requerida y las normas de desempeño, asegurando que el trabajo sea autónomo, objetivo y sin sesgos (ISSAI 11, principio 3, Buenas Prácticas)
	9.5	La EFS ha establecido un código de ética (profesional) y normas con significancia ética que abarcan los siguientes temas: <ul style="list-style-type: none"> - confianza, confidencialidad y credibilidad (ISSAI 30, capítulo 1); - integridad (ISSAI 30, capítulo 2); - independencia, objetividad, imparcialidad, neutralidad (política), anulación/prevención de conflictos de interés (ISSAI 30, capítulo 3; ISSAI 200/2.1-2.32); - secreto profesional (ISSAI 30, capítulo 4); - debido cuidado y competencia (ISSAI 30, capítulo 5; ISSAI 200/2.1, 2.33-2.46)
	9.6	Se hace partícipe a los empleados en la formulación del código de ética y/o las normas con significancia ética
10		Concientización de la integridad
	10.1	La integridad es un requerimiento explícito para todos los puestos/posiciones
	10.2	Realización regular de cursos de capacitación en materia de integridad o que incluyan este tópico en su temario
	10.3	Notificación al personal en posiciones/cargos vulnerables sobre los riesgos particulares y medidas para abatirlos
	10.4	Asesoría especial y/o existencia de un consejo que apoye al personal para enfrentar/resolver los riesgos de integridad
11		Actitud de la Alta Dirección

Grupo	Medida	
	11.1	La alta dirección promueve activamente la importancia de la integridad
	11.2	La alta dirección busca activamente la implementación de una política de integridad y de medidas de integridad
	11.3	La alta dirección siempre responde apropiadamente a las cuestiones/desafíos/problemas de integridad
	11.4	La propia alta dirección cumple con las regulaciones de integridad y/o código de conducta, dando ejemplo de un apropiado comportamiento ético (ISSAI 40, sección 6b, elemento 2)
12		Cultura organizacional
	12.1	Se presta atención regular a la importancia de la integridad
	12.2	Las cuestiones o desafíos en torno a asuntos de integridad se pueden discutir de forma segura
	12.3	Hay suficiente oportunidad de expresar las críticas
	12.4	La importancia de la integridad está claramente explicada a las partes interesadas externas
	12.5	Existe una comunicación abierta sobre violaciones a la integridad y respecto a la forma en que se abordan/resuelven
	12.6	Existencia de una cultura en la que se hace responsable a todos los empleados por sus propios actos/conducta
	12.7	Se presta consideración suficiente a la satisfacción laboral
13		Reclutamiento y selección
	13.1	Existen procedimientos ya establecidos para atender todas las solicitudes de empleo
	13.2	Existencia de un comité asesor de selección (de nuevas contrataciones)
	13.3	Se realiza comprobación de CV, diplomas, referencias, etc.
	13.4	Se evalúa (análisis previo a la contratación) al personal auditor y demás personal de la EFS respecto a las capacidades profesionales e integridad moral necesarias para el cumplimiento de sus tareas (ISSAI 1: Declaración de Lima; sección 14.1)
	13.5	La integridad es parte del programa de inducción ofrecido a personal de nuevo ingreso
	13.6	El personal firma una declaración de confidencialidad

Grupo	Medida	
	13.7	Se considera periódicamente la integridad durante reuniones de consulta/evaluación laboral y en entrevistas sobre el desempeño del personal
	13.8	La integridad es una consideración específica en la contratación de personal temporal y externo (ISSAI 40, sección 6b, elemento 2)
	13.9	La integridad es considerada cuando un empleado deja la EFS o durante las entrevistas de salida
14		Respuesta a las violaciones de integridad
	14.1	Existencia de un procedimiento/mecanismo de denuncia para que los empleados reporten (presuntas) violaciones (“procedimiento de denunciante”)
	14.2	La alta dirección es accesible para que los empleados reporten (presuntas) violaciones
	14.3	El Consejero de la Integridad está involucrado en el proceso/mecanismo de denuncia de (presuntas) violaciones
	14.4	Existencia de un procedimiento para el manejo de las señales y quejas/denuncias de fuentes/partes interesadas externas
	14.5	Existencia de un protocolo para investigar (presuntas) violaciones a la integridad
	14.6	Existencia de un registro central de violaciones de integridad
	14.7	La organización siempre responde a las violaciones de integridad
	14.8	Las sospechas respecto a la comisión de delitos son siempre notificadas a la fiscalía/procuraduría/ministerio público o a la policía
	14.9	En caso de incidentes, estos son evaluados y discutidos con el personal involucrado
15		Transparencia y Rendición de cuentas
		<i>Medidas Generales</i>
	15.1	La alta dirección recibe informes que dan cuenta de la política de integridad llevada a cabo/implementada
	15.2	Los representantes del personal reciben informes dan cuenta de la política de integridad llevada a cabo/implementada

Grupo	Medida	
	15.3	Las autoridades elegidas democráticamente (Parlamento/Congreso, Consejo Municipal, etc.) reciben informes que dan cuenta de la política de integridad llevada a cabo/implementada
	15.4	Los informes están sistemáticamente estructurados y contienen indicadores claros
		<i>Medidas Específicas para una EFS</i>
	15.5	El mandato de la EFS, así como su función, responsabilidades, organización, misión, estrategias, manuales de auditoría, procedimientos y criterios, son públicos (ISSAI 20, capítulo 2/3)
	15.6	Los hallazgos de auditoría y las conclusiones de la EFS están sujetas a los procedimientos contradictorios o de confronta (consultas con la entidad auditada) (ISSAI 20, capítulo 3)
	15.7	Las cuentas/estados financieros de la EFS son públicas y están sujetos a auditoría externa o revisión parlamentaria/del Congreso (ISSAI 20, capítulo 4)
	15.8	La EFS tiene apertura para la adopción de medidas para prevenir la corrupción y garantizar la claridad y legalidad en sus propias operaciones (por ejemplo, sanciones disciplinarias) (ISSAI 20, capítulo 5)
	15.9	Es público el status, competencias y obligaciones de los auditores (funcionarios públicos u otros) (ISSAI 20, capítulo 5)
	15.10	La subcontratación de actividades de auditoría o servicios periciales con entidades externas, públicas o privadas se realizan bajo la responsabilidad de la EFS y están sujetas a reglas precisas (ISSAI 20, capítulo 5)
	15.11	Los códigos de ética se emiten y ponen a disposición del público (ISSAI 20, capítulo 5)
	15.12	La EFS emite informes públicos sobre los hallazgos de la auditoría, su gestión y desempeño, y se comunica abiertamente con los medios de comunicación u otras partes interesadas (ISSAI 20, capítulo 6)
16		Auditoría y monitoreo
	16.1	El sistema de integridad es periódicamente auditado por un auditor interno.
	16.2	El sistema de integridad es revisado periódicamente por un auditor y/o supervisor externo
	16.3	El sistema de integridad es periódicamente monitoreado o evaluado por la alta dirección