CONTRALORÍA GENERAL DE LA REPÚBLICA DE CUBA

AUTOEVALUACIÓN DE INTEGRIDAD

14, 15 y 16 de noviembre de 2016

Informe de la Evaluación
Versión final

Moderadores de la *Auditoría Superior de la Federación de México*

Mtra. Melissa Janeth Narro Saucedo, Jefa de Departamento en la Dirección de Relaciones Institucionales, Encargada de Asuntos INTOSAI y Moderadora Certificada de IntoSAINT.

Lic. Francisco Tomás Parral Pineda, Supervisor en la Dirección de Relaciones Institucionales, Coordinador para la Implementación del Modelo de Integridad en las EFS de la OLACEFS y Moderador Certificado de IntoSAINT.

Equipo coordinador del Taller en la *Contraloría General de la República de Cuba*:

Mtra. Nelva Ibarra Mirón, Contralora Jefa de la Oficina de la Contralora General.

Mtra. Sonia María Beretervide Dopico, Especialista A Ramal Superior de la Oficina de la Contralora General.

Mtra. María Clara Castro Acosta, Contralora Jefa de la Dirección de Atención al Sistema Nacional de Auditoría (SNA) y Planificación.

Este informe es confidencial.

La información contenida en el presente informe es exclusivamente para uso de la Contraloría General de la República de Cuba.

Contenido

Resumen Ejecutivo

Una Autoevaluación de la Integridad como IntoSAINT tiene el objetivo de permitir a las Entidades Fiscalizadoras Superiores (EFS) evaluar el grado de vulnerabilidad institucional y la resistencia de su sistema de controles internos contra posibles violaciones de integridad, aportándole un producto compuesto: este informe dirigido a la Alta Dirección, así como la capacitación y concientización brindadas al personal seleccionado en temas de integridad. El valor del conocimiento obtenido por los 15 participantes del Taller de Autoevaluación de la Integridad correspondiente a la Contraloría General de la República de Cuba (CGR) es imprescindible, y se espera que ellos contribuyan como agentes de cambio y promotores del proceso de fortalecimiento y concientización sobre el tema de integridad.

El taller de autoevaluación se desarrolló con apego estricto a la metodología IntoSAINT. Los resultados del mismo mostraron que existe un Marco de Control Interno sólido y que, además, es eficaz, lo cual impactó positivamente en los diversos indicadores de esta herramienta que evalúan los riesgos y el nivel de madurez de controles de la integridad. Con base en un análisis meticuloso, los participantes, orientados por el equipo de moderadores, han identificado áreas de oportunidad y emitido, en consecuencia, recomendaciones a ser tomadas en cuenta por la Alta Dirección, para fortalecer las diversas medidas de controles de la integridad en la Contraloría General de la República de Cuba, así como para garantizar su sostenibilidad en el largo plazo mediante su incorporación en un marco de políticas sistémico.

Nota aclaratoria

Los hallazgos y las recomendaciones que se describen en el presente informe son el resultado de la aplicación estricta de la metodología IntoSAINT. Si bien la herramienta evalúa la implementación y eficacia de medidas específicas de integridad aplicadas por la EFS, cabe mencionar que existen elementos que no necesariamente son aplicables a la Contraloría General de la República. Esto se debe a que el marco de control interno intrínseco al sistema político-gubernamental de Cuba incluye medidas con una denominación y operación diferentes, pero que cumplen con la función de fomentar la integridad institucional y, por ende, la buena gobernanza. Por lo tanto, se sugiere que la CGR evalúe, en la medida de lo posible, la aplicabilidad de las recomendaciones derivadas de la autoevaluación, tomando en cuenta aquellas que se complementen con las medidas ya existentes.

No se propone una priorización ni una programación cronológica de las recomendaciones a implementarse, así como tampoco un modelo organizacional para su cabal puesta en marcha, puesto que esto va más allá del alcance de la metodología IntoSAINT, y por considerarse todo ello una decisión que debe recaer en la Alta Dirección, en consideración del mandato, recursos, capacidades y estrategia institucional.

Los grandes rubros en los que recaen las recomendaciones derivadas del Taller IntoSAINT son los siguientes:

1. **Política de Integridad Institucional.** En la integración de esta Política se propone articular los diferentes elementos existentes en la CGR en la materia, así como desarrollar medidas complementarias y actividades para su evaluación.

2. **Concientización y creación de capacidades.** Con el propósito de fortalecer las acciones de concientización de la integridad, incluir en los planes institucionales de capacitación tópicos relacionadas con la integridad.

3. **Rendición de cuentas.** Con la finalidad de informar sobre los asuntos relacionados con la integridad, su relevancia, mecanismos, logros, entre otros.

Es de esperarse que la inversión que realice la CGR para la instrumentación de estas recomendaciones tenga impactos positivos y eficaces para el fortalecimiento y consolidación de la integridad institucional. Asimismo, se espera que la Alta Dirección de la institución dé seguimiento a los resultados del taller de autoevaluación, que implemente procesos de evaluación sobre la eficacia de las acciones emprendidas y que, en lo sucesivo, promueva la realización periódica de talleres IntoSAINT. Al respecto, futuras evaluaciones podrían ser igualmente aplicadas a toda la institución o a áreas específicas, según lo determine la Alta Dirección.

Introducción

Este informe refleja los resultados de la autoevaluación de la integridad en la Contraloría General de la República de Cuba. La autoevaluación se llevó a cabo aplicando la metodología SAINT[1], adaptada a las Entidades Fiscalizadoras Superiores (EFS) miembros de la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI, por sus siglas en inglés), de conformidad con lo dispuesto por el Tribunal de Cuentas de los Países Bajos, creador de la herramienta. Esta metodología es aplicable a todos los miembros de la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS).

El enfoque de la autoevaluación fue global, teniendo alcance a toda la organización, toda vez que se realizó con la participación de representantes de las diversas áreas que componen a la CGR.

Los conceptos básicos de la metodología SAINT pueden resumirse como sigue:

- La integridad implica no solamente la observancia de las reglas y leyes, sino además conlleva una responsabilidad moral.
- La integridad es un aspecto de la calidad de una organización y, por lo tanto, es una responsabilidad de la Alta Dirección.
- La integridad es una condición esencial para la confianza en el sector público.
- La prevención y la concientización sobre las vulnerabilidades existentes son acciones más eficaces para proteger la integridad de una organización. Las organizaciones pueden reducir su vulnerabilidad al contar con un sistema de controles de integridad maduro y bien implementado.
- Un sistema de integridad maduro consta de controles generales, duros y suaves.
- Como conocedores de los procesos, los empleados con frecuencia están en una posición privilegiada para identificar las vulnerabilidades, para detectar debilidades en el sistema de controles de integridad e identificar las maneras de fortalecer la resistencia de la EFS a violaciones a la integridad.
- La participación de los empleados en la evaluación de la integridad contribuye a elevar el grado de concientización respecto al tema de integridad.

La autoevaluación se realizó los días 14, 15 y 16 de noviembre de 2016, por un grupo cuidadosamente seleccionado de empleados, provenientes de posiciones estratégicas en la organización. La lista de los participantes se incluye en el **Anexo 1**. Durante el taller, los participantes ejecutaron las diversas etapas previstas en la metodología de la evaluación.

Este informe dirigido a la Alta Dirección describe los resultados de las fases consecutivas de la metodología, a saber:

a. descripción de los procesos organizacionales seleccionados;
b. identificación del perfil de vulnerabilidad;
c. madurez del sistema de controles de la integridad existente;

[1] Siglas en inglés del concepto *Self Assessment on Integrity,* evaluación del grado de vulnerabilidad institucional y nivel de madurez del sistema de los controles de la integridad implementados, aplicable a entidades del sector público.

d. análisis de brechas existentes entre el perfil de vulnerabilidad y las medidas de control de integridad que ha implementado la organización.

Con base en estas descripciones, se formularon recomendaciones para fortalecer el sistema de controles de integridad.

Queremos agradecer la cooperación que hemos recibido por parte de la Contraloría General de la República de Cuba para llevar a cabo el taller IntoSAINT, en especial los esfuerzos de los participantes del taller y del Equipo coordinador.

1 Descripción de los procesos organizacionales

Antes de dar inicio al taller, la Contraloría General de la República de Cuba, en cooperación con los moderadores, hizo una preselección de los procesos clave. Al inicio del taller, se discutió y complementó esta preselección, tras lo cual los participantes acordaron enfocar la autoevaluación en los siguientes procesos.

Los procesos vitales de la organización incluidos en la autoevaluación fueron:

PROCESOS DE DIRECCIÓN GENERAL (DE CONTROL O DE GOBERNANZA)

1-01 Planeación y Organización

1-01-001 Sistema de Control Interno

1-01-001-0001 Revisión del Sistema de Control Interno
1-01-001-0002 Gestión de riesgos

1-01-002 Planeación, elaboración de los planes de trabajo

1-01-002-0001 Elaboración de los objetivos de trabajo
1-01-002-0002 Elaboración del plan de trabajo anual y mensual
1-01-002-0003 Evaluación y calificación de los objetivos de trabajo
1-01-002-0004 Elaboración de los procedimientos de trabajo

1-01-003 Plan y Presupuesto

1-01-003-0001 Elaboración del plan
1-01-003-0002 Desagregación del plan
1-01-003-0003 Control del plan
1-01-003-0004 Elaboración del anteproyecto de presupuesto
1-01-003-0005 Notificación del presupuesto
1-01-003-0006 Ejecución y control del presupuesto
1-01-003-0007 Liquidación del presupuesto

1-01-004 Plan de Acciones de Control

1-01-004-0001 Elaboración de consulta y aprobación de las directivas
1-01-004-0002 Elaboración, conciliación y aprobación del plan de acciones de control
1-01-004-0003 Modificaciones del plan anual de acciones de control
1-01-004-0004 Resumen del cumplimiento del plan y las directivas

1-01-005 Asesoramiento Jurídica

1-01-005-0002 Proyectos legislativos

1-01-008 Proyectos Metodológicos

1-01-008-0001 Planificación de proyectos metodológicos
1-01-008-0002 Ejecución de proyectos metodológicos
1-01-008-0003 Evaluación de proyectos metodológicos

1-02 Gestión del Capital Humano

1-02-001 Trabajo con el personal

1-02-001-0001 Competencias laborales
1-02-001-0002 Selección e integración
1-02-001-0007 Evaluación del desempeño

1-02-003 Capacitación

1-02-003-0001 Gestión de capacitación y desarrollo
1-02-003-0002 Atención metodológica a los centros de capacitación
1-02-003-0003 Programa de formación emergente

1-03 Gestión de Investigación e Información

1-03-003 Captación, procesamiento e información de los resultados del cumplimiento del plan anual de acciones de auditorías, supervisión y control

1-05 Gestión de las Tecnologías de la Información y las Comunicaciones

1-05-001 *Gestión de la seguridad informática*

1-05-001-0001 Actualizar el Plan de Seguridad Informática

PROCESOS PRIMARIOS

2-01 Acciones de Auditoría, Supervisión y Control

2-01-001 Auditoría

2-01-001-0001 Planeación
2-01-001-0002 Ejecución
2-01-001-0003 Informe
2-01-001-0004 Seguimiento
2-01-001-0005 Supervisión

2-01-003 Comprobación Especial

2-01-004 Control Integral Estatal

2-02 Respuesta a las Inconformidades

2-02-001 Recurso de apelación de auditoría, supervisión y control

2-02-001-0001 Presentación, recepción e inscripción de las inconformidades en el sistema automatizado
2-02-001-0002 Revisión para determinar si procede o no la admisión de la inconformidad
2-02-001-0003 Revisión y emisión del dictamen
2-02-001-0004 Actualización del resultado final en el sistema automatizado

2-03 Atención al Sistema Nacional de Auditoría

2-03-001 Visita de Supervisión y Control

2-03-001-0001 Planeación
2-03-001-0002 Ejecución
2-03-001-0003 Informe
2-03-001-0004 Seguimiento

2-04 Atención a la población

2-04-001 Gestión de los planteamientos (denuncias, quejas y peticiones)

2-04-001-0001 Estudio y exploración
2-04-001-0002 Propuesta de tramitación
2-04-001-0003 Seguimiento
2-04-001-0004 Cierre de la tramitación

PROCESOS SECUNDARIOS

3-01 Administración General

3-01-008 Servicios de transportación con terceros

3-01-008-0001Control de los servicios de transportación con terceros

3-02 Gestión Económica y Contable

3-02-002 *Gestión Contable*

3-02-002-0001 Actividad contable de la sede de la CGR
3-02-002-0002 Actividad contable de las Contralorías Provinciales

Esta lista de procesos sirvió como referencia para la conducción de las demás etapas del taller IntoSAINT.

2 Vulnerabilidades

2.1 Vulnerabilidades inherentes

Todas las organizaciones son, hasta cierto punto, vulnerables a violaciones de integridad. Sin embargo, ciertas actividades y funciones en el sector público son especialmente vulnerables. Éstas se conocen como vulnerabilidades inherentes y suelen estar relacionadas con las tareas específicas de una organización. Durante el taller, los procesos y funciones de la Contraloría General de la República de Cuba se compararon con una lista de vulnerabilidades inherentes, como se indica en la tabla siguiente.

Como se indica a continuación, los 15 participantes asignaron una calificación a cada vulnerabilidad inherente en consideración de la relevancia que guarda cada una de ellas para la realización de los procesos organizacionales definidos para esta institución. Las calificaciones otorgadas por los participantes oscilan de 0 a 3, según el siguiente criterio:

Puntaje	Relevancia
0	No importante
1	Relevante
2	Importante
3	Muy importante

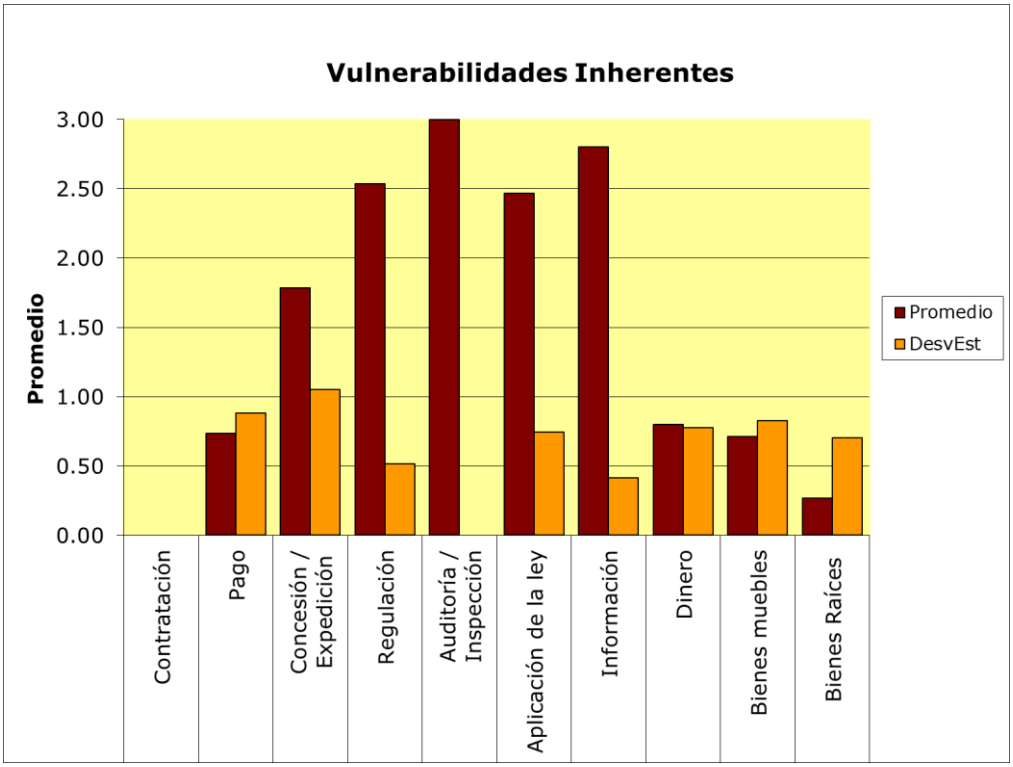
	Áreas /actividades/acciones Vulnerables		**Puntaje promedio**	**Nivel**
Relación de la entidad con su ambiente	Contratación	Abastecimiento / adquisiciones, procesos de licitación, pedidos, asignaciones, concesión de contratos.	**0.00**	**Bajo**
	Pagos	Otorgamiento de subsidios, beneficios, prestaciones, subvenciones / becas, patrocinios.	**0.73**	**Bajo**
	Concesión / expedición	Otorgamiento de permisos, licencias, documentos de identidad, autorizaciones, certificados.	**1.79**	**Alto**
	Regulación	Definición de requisitos / condiciones de los permisos, establecimiento de normas / criterios / lineamientos.	**2.53**	**Alto**
	Inspección / auditoría	Supervisión, vigilancia, control, inspección, auditoría, revisión.	**3.00**	**Alto**
	Aplicación de la ley	Denuncia / enjuiciamiento, justicia, aplicación/promoción de sanciones/castigos.	**2.47**	**Alto**

Gestión de la propiedad pública	Información	Seguridad nacional, información confidencial, documentos de trabajo, expedientes, derechos de autor.	**2.80**	**Alto**
	Dinero	Tesorería, instrumentos financieros, gestión de cartera, dinero en efectivo / cuentas bancarias, primas, gastos, bonificaciones, prestaciones, etc.	**0.80**	**Medio**
	Bienes muebles	Compra / venta / arrendamiento, consumo, gestión, mantenimiento de bienes muebles.	**0.71**	**Bajo**
	Bienes raíces	Compra / venta / arrendamiento, mantenimiento, gestión de bienes raíces.	**0.27**	**Bajo**
		Promedio	**1.51**	**Medio**

En las dos últimas columnas de la derecha, la tabla indica el promedio de los puntajes asignados por los participantes en el taller y el nivel de vulnerabilidad inherente.

El nivel de vulnerabilidad puede ser bajo, medio o alto, con base en los siguientes criterios:

Puntuación promedio	**Nivel**
promedio < 0.8	Bajo
0.8 ≤ promedio ≤ 1.6	Medio
promedio > 1.6	Alto



Las puntuaciones de las vulnerabilidades inherentes a la CGR están representadas en el siguiente diagrama.

En rojo se destaca el puntaje promedio asignado por los participantes; en naranja, la desviación estándar aplicable a cada vulnerabilidad inherente, que refleja el grado de divergencia en las calificaciones otorgadas por los participantes.

El puntaje promedio otorgado por los participantes para la vulnerabilidad inherente de la CGR de Cuba fue de **1.51**. De esta forma, según los parámetros antes señalados, la vulnerabilidad inherente promedio identificada durante el taller se encuentra en un nivel **medio**.

De la tabla y del diagrama correspondiente, se puede concluir que las áreas vulnerables aplicables a la labor de la CGR son:

- **Auditoría e inspección**
- **Manejo de información**
- **Regulación**
- **Aplicación de la ley**
- **Concesión / expedición**

En consideración del mandato de una Entidad Fiscalizadora Superior, es de entenderse que las áreas de **auditoría e inspección**, manejo de **información** y **aplicación de la ley** hayan reflejado un nivel alto de vulnerabilidad inherente.

Para el caso particular de la CGR de Cuba, cabe resaltar que los rubros **regulación** y **concesión / expedición** presentaron, a su vez, puntajes altos. En el caso de la "regulación", el puntaje alto se debió a la facultad de la institución para emitir normas que son vinculantes tanto de manera interna como externa. Para el caso externo, éstas aplican a órganos, organismos, entidades nacionales, empresas y otros actores en Cuba. Un ejemplo claro es el Marco de Control Interno emitido por la CGR.

Por otro lado, acerca del rubro "concesión / expedición", el puntaje se debe a la atribución que tiene la institución para llevar a cabo el registro de los contralores y auditores en Cuba, requisito indispensable para que éstos puedan ejercer su profesión como tales.

2.2 Factores que agravan la vulnerabilidad

Además de las actividades inherentemente vulnerables, algunas circunstancias o factores pueden elevar la vulnerabilidad a violaciones de integridad. Estos factores pueden aumentar la vulnerabilidad debido a que:

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

La mayoría de las circunstancias o factores que agravan la vulnerabilidad dan pie a oportunidades, motivaciones y/o racionalizaciones para la comisión de violaciones a la integridad. Existen otras circunstancias que se les conoce como indicadores de una (potencialmente) débil cultura de integridad dentro de una organización.

Cabe destacar que la presencia de una o más de estas circunstancias no implica que se violente la integridad; implica, simplemente, que la organización es más vulnerable y que hay un mayor riesgo para que se den violaciones de integridad.

Dentro del marco de referencia de este método de evaluación, los factores que agravan la vulnerabilidad en las EFS se dividen en cinco grupos:

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

Durante el taller, los participantes evaluaron y discutieron la lista completa de los factores que agravan la vulnerabilidad. Posteriormente, asignaron una calificación a cada factor, en consideración de la incidencia real de cada uno de ellos en la CGR de Cuba. Las calificaciones otorgadas por los participantes oscilaron de 0 a 3, según el siguiente criterio:

Puntuación	Relevancia
0	No importante
1	Relevante
2	Importante
3	Muy importante

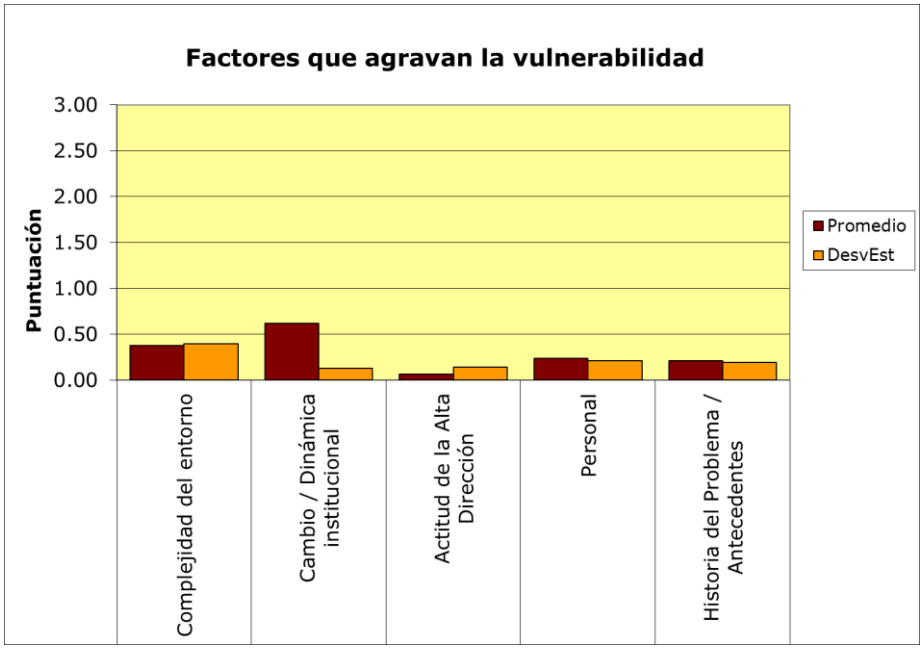
La lista completa de factores que agravan la vulnerabilidad y el puntaje promedio otorgado a cada uno de ellos se pueden consultar en el **Anexo 2**. A continuación se presenta una tabla que consolida la puntuación promedio y por grupo de los factores, según fue asignada por los participantes del taller, así como el nivel resultante de los factores que agravan la vulnerabilidad institucional.

Grupos de factores que agravan la vulnerabilidad	**Puntaje promedio (0-3)**	**Nivel**
1. Complejidad del entorno	**0.38**	**Bajo**
2. Cambio / Dinámica institucional	**0.62**	**Bajo**
3. Actitud de la Alta Dirección	**0.07**	**Bajo**
4. Personal	**0.24**	**Bajo**
5. Historia del problema / antecedentes	**0.21**	**Bajo**
Puntuación promedio general	**0.30**	**Bajo**

Al igual que en el caso de las vulnerabilidades inherentes, el nivel de los factores que agravan la vulnerabilidad puede ser bajo, medio o alto, con base en los siguientes criterios:

Puntuación promedio	Nivel
promedio < 0.8	Bajo
0.8 ≤ promedio ≤ 1.6	Medio
promedio > 1.6	Alto

Las puntuaciones promedio de los grupos de factores que agravan la vulnerabilidad pueden representarse con un diagrama, como se observa a continuación:



En rojo se destaca el puntaje promedio asignado por los participantes; en naranja, la desviación estándar aplicable a cada grupo de factores que agravan la vulnerabilidad, que refleja el grado de divergencia en las calificaciones otorgadas por los participantes.

De la tabla se concluye que el impacto actual que pudiera tener el conjunto de factores que agravan la vulnerabilidad, al obtener un puntaje promedio de 0.30, es **bajo**.

A continuación se presentan las conclusiones basadas en los resultados obtenidos a partir de los puntajes asignados por los participantes.

- **Complejidad del entorno**

Los participantes del taller consideran que no existen elementos relacionados con la complejidad del entorno que impacten a la CGR en términos negativos. Se hizo mención sobre la implementación de **nuevos sistemas de información** en la institución, lo cual puede representar un desafío, sin embargo la CGR se ha adaptado y capacitado en el uso de estas nuevas tecnologías. Asimismo, se trató el tema de la **legislación** aplicable a los entes auditados, la que podría tornarse **compleja**, lo que obliga a los contralores y auditores de la institución a mantenerse actualizados. Asimismo, consideran que, por el sistema político de Cuba, hay un **cabildeo político** nulo, y que no existen **conflictos de intereses públicos y privados** dadas

las regulaciones en la materia. Tampoco se perciben **redes de relaciones**, **burocracia**, ni **influencia o intervención política** que atente contra la eficacia de la labor de control de la CGR.

- **Cambio / dinámica institucional**

Los resultados muestran que los recientes cambios de mandato y estructura (**organización joven**) que se han llevado a cabo en la Contraloría General de la República han obligado a la institución a tomar las medidas necesarias para reducir el impacto de riesgos potenciales. Esta reestructuración conllevó una serie de **cambios legislativos** a los que la CGR tuvo que estar atenta, alineando sus actividades al nuevo marco legal. Los participantes consideraron que la **privatización**, **subcontratación** y **crecimiento/reducción de la organización** no se da en el caso de la CGR. Tampoco se percibe un ambiente de **crisis** y **presión externa**.

- **Actitud de la Alta Dirección**

Los participantes consideran que la Alta Dirección se compone por: la Contralora General de la República y los Vicecontralores Generales, a quienes se les percibe con visión, liderazgo, profesionalismo y sentido humano. Asimismo, los participantes reconocieron que la Alta Dirección está **comprometida con la rendición de cuentas**, que atiende **consejos** y que se muestra **flexible ante críticas**, **quejas/demandas**, lo que ha permeado positivamente en el clima organizacional y en la manera en que el personal se conduce dentro y fuera de la institución. Además, se hizo hincapié en la **facilidad para llegar** a la Contralora General y poder compartir ideas, en su actitud receptiva, así como en el sentido humano de su conducir diario.

- **Personal**

De acuerdo con los resultados, no se perciben amenazas en el ambiente de trabajo ni en los asuntos de carácter individual del personal. No existen grupos herméticos en la institución que **obstaculicen el trabajo de otras áreas**, lo cual también favorece el clima organizacional. Se percibe un ambiente de altos principios éticos y de conducta, los cuales, al ser asumidos por el personal, se crea una atmósfera de profesionalismo. Si bien existen **altas cargas de trabajo**, la CGR asume la responsabilidad y forma equipos que desahoguen las labores encomendadas. En los asuntos individuales, los participantes sostienen que en general el personal no suele tener **deudas personales** ni **estilos de vida extravagantes** o con **gastos excesivos**, ni **secretos ni amenazas personales** que los pueda hacer vulnerables ante chantajes. A pesar de que en Cuba existen índices de tabaquismo, esto no tiene un impacto en el quehacer institucional, dadas las medidas de salubridad implementadas en la materia.

- **Historial del problema / antecedentes**

Los participantes consideran que los controles implementados en la CGR se encuentran bien monitoreados, lo que evita **problemas administrativos**. Asimismo, sostienen que ante **quejas** y **denuncias** sobre posibles actos contrarios a la integridad se crea una comisión especial investigadora al respecto, la cual sigue un protocolo para esclarecer los hechos (visitas domiciliarias, entrevistas a conocidos, entre otros). Al atender los casos y denuncias de manera oportuna, se fortalece la gobernanza institucional. Además, las medidas de control aplicadas en el proceso de **reclutamiento y selección** funcionan como filtro para llamar y retener a personal calificado en materia de integridad y con compromiso institucional.

2.3 Perfil de Vulnerabilidad

El nivel global de vulnerabilidad, o también llamado perfil de vulnerabilidad, se basa en la fotografía actual que integra tanto a las vulnerabilidades inherentes como a los factores que agravan la vulnerabilidad. Los niveles combinados de vulnerabilidades inherentes y de factores que agravan la vulnerabilidad dan como resultado el nivel global de vulnerabilidad.

De conformidad con la evaluación realizada por los participantes en el taller, el nivel de vulnerabilidad inherente de la CGR es **medio**.

El nivel de los factores que agravan la vulnerabilidad es **bajo**.

En conjunto, estos resultados se traducen en un perfil de vulnerabilidad **MEDIO**, como se muestra en la siguiente tabla.

Perfil de Vulnerabilidad

Factores que agravan la vulnerabilidad / **Vulnerabilidades Inherentes**	**Bajo**	Medio	Alto
Bajo	Bajo	Bajo	Medio
Medio	**Medio**	Medio	Alto
Alto	Alto	Alto	Alto

Este perfil de vulnerabilidad es tomado en cuenta al realizarse su comparación con el nivel de madurez del sistema de controles de integridad y tiene un papel importante en el análisis de brechas.

3 Nivel de madurez del Sistema de Controles de la Integridad

Un elemento clave de esta metodología es la evaluación del "nivel de madurez" del sistema de controles de integridad. El sistema de controles de integridad es el conjunto de medidas implementadas para promover, monitorear y mantener la integridad. De las muchas medidas conocidas a partir de la literatura y la práctica, se ha integrado un conjunto bien balanceado de éstas para servir como referencia para este método de evaluación. Este conjunto de controles también considera las Normas Internacionales de Entidades Fiscalizadoras Superiores (ISSAI, por sus siglas en inglés), por lo que los componentes éticos están contemplados.

El sistema de controles de la integridad de la organización se puede describir usando un amplio conjunto de medidas de integridad dividido en tres clasificaciones principales (los controles generales, duros y suaves), que a su vez se categorizan en 16 grupos.

Los grupos se muestran en el siguiente modelo.

Controles Generales

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

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

La evaluación del nivel de madurez del sistema de controles de integridad toma en cuenta la existencia, la implementación, la operación y la eficacia de los controles. Las puntuaciones sobre las medidas individuales van de 0 cuando una medida es inexistente, a 3 cuando la medida existe, se observa y es eficaz, como se indica en la tabla siguiente.

Puntaje	**Criterio de evaluación**
0 – Bajo	- La medida no existe, al menos hasta donde los participantes tienen conocimiento
1 – Bajo	- La medida existe - La medida no se implementa / no se observa
2 – Medio	- La medida existe - La medida se implementa / se observa - La medida no funciona / no es eficaz
3 - Alto	- La medida existe - La medida se implementa / se observa - La medida funciona / es eficaz

En principio, el nivel más alto (nivel de madurez 3) es el ideal. Las puntuaciones de las medidas individuales nos permiten conocer los resultados por grupo y, al final, también el nivel global de madurez correspondiente al sistema de controles de integridad como un todo. El sistema de controles de integridad y las puntuaciones de madurez de cada medida de control se pueden consultar en el **Anexo 3**.

El resultado de la evaluación del sistema de controles de integridad se muestra a continuación por grupo de medidas.

No.	**Grupos de control**	**Promedio**	**Nivel**
	Controles Generales	**2.58**	**Alto**
1	Marco de política de integridad	1.95	Medio
2	Análisis de vulnerabilidad / análisis de riesgos	3.00	Alto
13	Reclutamiento y selección	2.91	Alto
14	Respuestas a las violaciones de integridad	2.80	Alto
15	Transparencia y rendición de cuentas	2.80	Alto
16	Auditoría y monitoreo	1.99	Medio

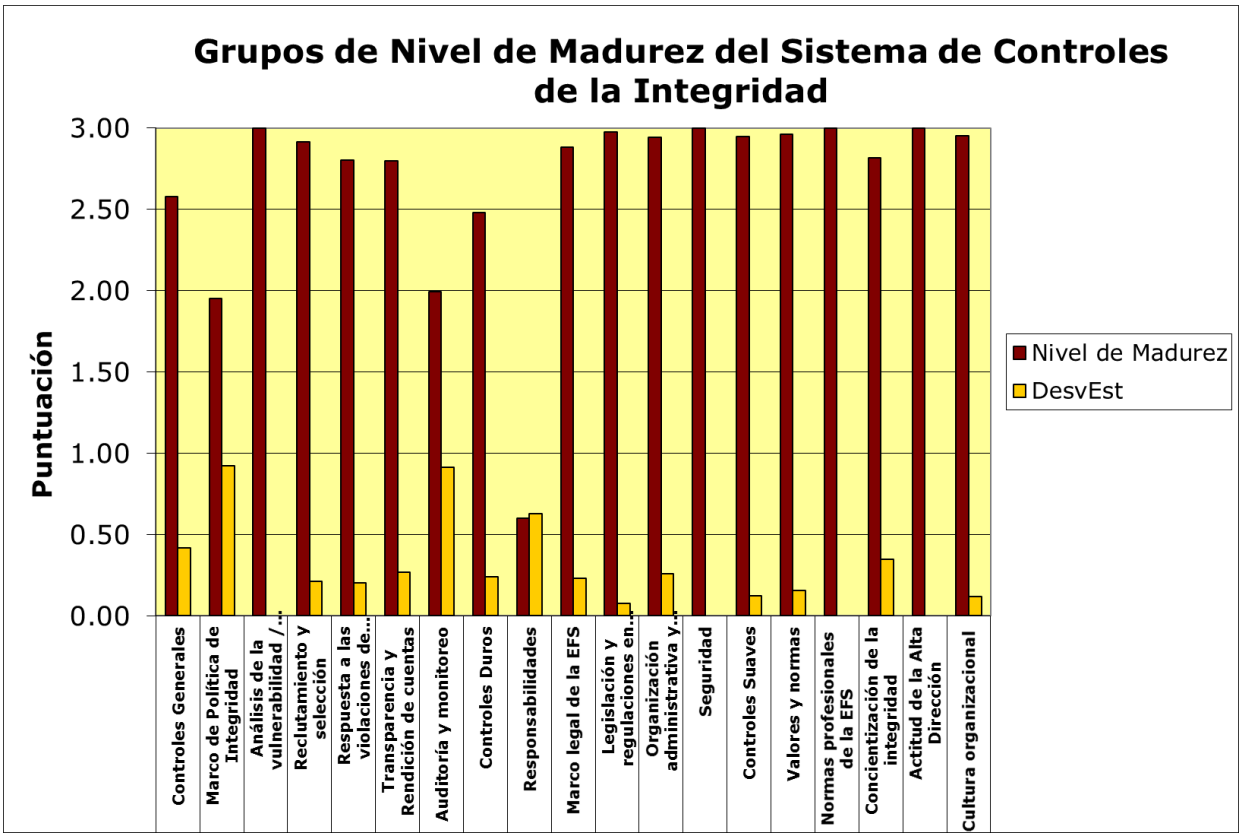
No.	Grupos de control	Promedio	Nivel
	Controles duros	**2.48**	**Alto**
3	Responsabilidades	0.60	Bajo
4	Marco legal de la EFS	2.88	Alto
5	Legislación y regulaciones en materia de integridad	2.97	Alto
6	Organización administrativa y control interno	2.94	Alto
7	Seguridad	3.00	Alto
	Controles suaves	**2.95**	**Alto**
8	Valores y normas	2.96	Alto
9	Normas profesionales de la EFS	3.00	Alto
10	Concientización de la integridad	2.82	Alto
11	Actitud de la Alta Dirección	3.00	Alto
12	Cultura organizacional	2.95	Alto
	Puntaje promedio general de todos los grupos	**2.66**	**Alto**

La puntuación promedio general obtenida determina, de manera global, el nivel de madurez del sistema de controles de integridad. Refiérase a la tabla siguiente:

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

En el caso de la CGR de Cuba, la puntuación promedio fue de **2.66**. Por lo cual, de acuerdo con la metodología de IntoSAINT, el nivel de madurez del sistema de controles de la integridad implementado es **ALTO**.

El siguiente diagrama muestra el nivel de madurez de los grupos de controles de integridad implementados en la CGR de Cuba, según lo evaluado por los participantes del Taller.



Las **principales fortalezas** del sistema de controles de integridad se pueden encontrar en los siguientes rubros:

- Análisis de vulnerabilidad / análisis de riesgos
- Marco legal de la EFS
- Legislación y regulaciones en materia de integridad
- Organización administrativa y control interno
- Seguridad
- Valores y normas
- Normas profesionales de la EFS
- Concientización de la integridad
- Actitud de la Alta Dirección
- Cultura organizacional
- Reclutamiento y selección
- Respuesta a violaciones de integridad

Las principales **áreas de oportunidad** se encuentran en los siguientes rubros:

- Responsabilidades específicas en materia de integridad
- Marco de Política de Integridad
- Auditoría y monitoreo de la integridad

Para el caso de la CGR de Cuba, se observa que la administración ha implementado un sólido Marco de Control Interno, que incluye una norma específica sobre integridad y valores éticos, y que además es eficaz, lo que ha favorecido que la institución reduzca el impacto de

posibles riesgos de integridad y se encuentre mejor preparada ante posibles hechos que puedan vulnerar la gobernanza organizacional.

Los puntajes detallados de los niveles de madurez fueron empleados por los participantes en el taller para discutir las posibles mejoras del sistema de controles de integridad. Los participantes consideraron también qué controles estaban ya en un nivel satisfactorio, es decir, aquellos controles sin necesidad de ser mejorados, ya sea porque no se aplicaban a la situación dentro de la CGR de Cuba o bien porque podrían causar un exceso de burocracia, en relación con su contribución al sistema de controles de integridad. Los resultados finales de este ejercicio se reflejan en las recomendaciones.

4 Análisis de brechas

Después de completarse la evaluación del perfil de vulnerabilidad institucional y del nivel de madurez del sistema de controles de integridad, es posible contrastarlos y analizar si se encuentran en equilibrio. Si no lo están, hay una brecha, lo cual usualmente indica que el sistema de controles de integridad necesita reforzarse.

Las organizaciones pueden hacer frente a las vulnerabilidades de diferentes maneras. En primer lugar, se puede tratar de eliminar o reducir las vulnerabilidades, evitando las actividades vulnerables. A veces es posible llevar a cabo las actividades de una manera diferente, eliminando las actividades que son vulnerables a las violaciones de integridad. Esto significa que la organización es capaz de direccionar el origen de la vulnerabilidad. Sin embargo, en la práctica esto puede ser difícil. Los organismos públicos tienen obligaciones legales y no pueden evitar involucrarse en actividades inherentemente vulnerables o que puedan agravarse por otros factores ajenos al mandato institucional.

Por lo general, una forma más viable para hacer frente a la vulnerabilidad consiste en diseñar y poner en práctica controles (de integridad) compensatorios. Dependiendo del “nivel de madurez” del sistema de controles de integridad, la organización es más o menos resistente a las vulnerabilidades a las que se enfrenta.

Durante el taller, los participantes realizaron una evaluación sobre el nivel general de vulnerabilidad y la madurez de su sistema de controles de integridad. Para el caso de la Contraloría General de la República de Cuba, el taller permitió visualizar que el sistema de controles de integridad (nivel alto) presenta **mayor fuerza** *vis-à-vis* el perfil de vulnerabilidades (nivel medio) en la entidad. Si bien este resultado es favorable en la actualidad, es fundamental que los esfuerzos de la organización sean continuos, persistentes y que estén en constante evaluación y monitoreo, a fin de garantizar la gobernanza de la institución en el largo plazo.

5 Recomendaciones

Con base en la evaluación de las vulnerabilidades y del nivel de madurez del sistema de controles de integridad, los participantes del taller formularon una serie de recomendaciones a la Alta Dirección. Estas recomendaciones se presentan a continuación:

A. Política de Integridad Institucional

1. Documentar una Política de Integridad Institucional que articule todas las normas y mecanismos en la materia que hoy se implementan (ej. Código de Ética para los auditores del Sistema Nacional de Auditoría, Código de Conducta, principios éticos, lineamientos para la prevención de conflictos de intereses, Declaración de compromiso ético de los trabajadores de la CGR, Guía de Autocontrol General, comités de investigación de presuntos actos contrarios a la integridad, etc.) y que, además, considere nuevos componentes, según sea pertinente. Se sugiere que esta Política se incluya en el Marco Institucional de Políticas y en el Plan Anual de Actividades de la CGR.

2. Implementar una evaluación periódica sobre la eficacia de todos los elementos y acciones que compongan la Política de Integridad, a efecto de garantizar el alcance de sus objetivos, así como su sostenibilidad y mejora continua.

B. Concientización y creación de capacidades

3. Fortalecer acciones de concientización sobre la relevancia, avances y el papel de la CGR en materia de integridad (ej. materiales audiovisuales, publicaciones, entre otros).

4. Incluir en los planes institucionales de capacitación temáticas relacionadas con la integridad, así como con los diversos elementos que compongan la Política de Integridad Institucional.

5. Adaptar, según el contexto y las circunstancias, el Modelo de Integridad de la INTOSAI y replicarlo en las diferentes áreas de la CGR.

C. Rendición de cuentas

6. Incorporar en los balances e informes de rendición de cuentas de la CGR un apartado especial sobre los asuntos relacionados con la integridad (relevancia, indicadores, logros institucionales en la materia, recomendaciones, etc).

Consideramos que la implementación de estas 6 recomendaciones contribuirá a mejorar, aún más, el sistema de controles de integridad de la Contraloría General de la República de Cuba.

Anexo 1 Lista de participantes

No.	Nombre y apellidos	Cargo	Años de experiencia en la entidad
1.	José Luis Nicolau Cruz	Contralor Asesor de la Contralora General	15 años Lic. Sociología
2.	Ana Silvia Valladares Arenas	Contralora Jefa de Dirección de Tecnología de la Información y las Comunicaciones.	5 años y 9 meses Lic. Cibernética Matemática
3.	Fernando Alpízar Caballero	Auditor Supervisor de la Dirección Jurídica	6 años Lic. Derecho
4.	Sonia María Beretervide Dopico	Especialista A Ramal Superior de la Oficina de la Contralora General	4 años y 5 meses Lic. Filosofía
5.	Félix Emilio Miyar Abreu	Especialista A Ramal Superior de la Oficina de la Contralora General	12 años Lic. Ciencias Sociales
6.	Mevis Clarivel Linares Rodríguez	Auditora Supervisora de la Dirección de Metodología e Inconformidades	10 años y 10 meses Lic. Economía
7.	Ana Gloria Gómez Cruz	Subjefa de la Dirección de Atención a la Población	10 años Lic. Educación
8.	Yoel Gómez Ramírez	Subjefe de la Dirección Integral de Control Organismos Globales y Sistema Bancario	11 años Lic. Filosofía e Historia
9.	Aymeé González Hermida	Auditora Supervisora de la Dirección Integral de Control Servicios Sociales Presupuestados	24 años Lic. Contabilidad y Finanzas
10.	Demetrio Morales Gómez	Sub jefe de Dirección Integral de Control al Sector Agroalimentario	9 años Lic. Ciencias Sociales
11.	Marcos Antonio Hernández Hernández	Jefe de Grupo de la Dirección Integral de Control Turismo, Comercio y los Servicios	13 años Lic. Ciencias Sociales
12.	Orestes Felipe Hondal Egues	Jefe de la Dirección de Contabilidad	4 años Contador Público
13.	Luis Porro López	Especialista A Ramal Superior de la Dirección de Recursos Humanos	2 años y 6 meses Ingeniero Mecánico
14.	Isabel Ovich Mendoza	Contralora Jefe de la Dirección de Capacitación e Investigaciones	11 años Lic. Ciencias Humanísticas
15.	Iraida Marbán González	Especialista Jurídica A Auditora de la Dirección Jurídica	6 años Lic. Derecho

Equipo coordinador del Taller en la *Contraloría General de la República de Cuba*:

- **Mtra. Nelva Ibarra Mirón,** Contralora Jefa de la Oficina de la Contralora General.
- **Mtra. Sonia María Beretervide Dopico**, Especialista A Ramal Superior de la Oficina de la Contralora General.
- **Mtra. María Clara Castro Acosta,** Contralora Jefa de la Dirección de Atención al Sistema Nacional de Auditoría (SNA) y Planificación.

Anexo 2 Factores que agravan la vulnerabilidad

	Factores que agravan la vulnerabilidad	Promedio	Puntaje
	1 Complejidad del entorno		
1.1	Innovación/sistemas (computacionales) avanzados	0.87	Medio
1.2	Legislación compleja	0.93	Medio
1.3	Estructuras legales/fiscales (especiales)	0.40	Bajo
1.4	Burocracia	0.53	Bajo
1.5	Cabildeo político	0.00	Bajo
1.6	Redes de relaciones	0.13	Bajo
1.7	Combinación de intereses de los sectores público y privado (comercio / competencia)	0.07	Bajo
1.8	Necesidad de contar con asesoría / pericia externa	0.40	Bajo
1.9	Influencia / intervención política	0.07	Bajo
	Puntuación Promedio Grupo 1	**0.38**	**Bajo**
	2 Cambio / dinámica institucional		
2.1	Organización joven	1.87	Alto
2.2	Legislación frecuentemente cambiante	1.93	Alto
2.3	Fuerte crecimiento o reducción de la organización	0.40	Bajo
2.4	Privatización	0.00	Bajo
2.5	Subcontratación	0.00	Bajo
2.6	Crisis (reorganización, amenazas organizacionales con un fuerte impacto, supervivencia de la organización o trabajo en riesgo)	0.00	Bajo
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)	0.13	Bajo
	Puntuación Promedio Grupo 2	**0.62**	**Bajo**
	3 Actitud de la Alta Dirección		
3.1	Dominante	0.07	Bajo
3.2	Manipuladora	0.00	Bajo
3.3	Formal / burocrática	0.13	Bajo
3.4	Operación aislada	0.00	Bajo
3.5	Remuneración fuertemente dependiente del desempeño/resultados	0.00	Bajo
3.6	No comprometida con la rendición de cuentas	0.07	Bajo
3.7	Ignora consejos / asesoría / señales	0.07	Bajo
3.8	Respuesta defensiva ante críticas o quejas/demandas	0.20	Bajo
	Puntuación Promedio Grupo 3	**0.07**	**Bajo**
	4 Personal		
*	***Ambiente de trabajo / lealtad***		
4.1	Presión sobre el desempeño/resultados, ingresos dependen del rendimiento	0.27	Bajo
4.2	Bajo estatus / falta de autoestima / bajos incentivos organizacionales / bajas perspectivas de crecimiento profesional	0.27	Bajo
4.3	Condiciones de trabajo inadecuadas	0.40	Bajo
4.4	Cargas de trabajo elevadas	1.27	Medio
4.5	Lealtad de grupo	0.20	Bajo
4.6	Poder para obstaculizar	0.07	Bajo
*	***Individual***		

4.7	Tener otros intereses (empleo alternativo/secundario, etc.)	0.27	Bajo
4.8	Deudas personales	0.00	Bajo
4.9	Estilo de vida (extravagante o con gastos excesivos)	0.00	Bajo
4.10	Secretos personales (vulnerabilidad ante chantajes)	0.07	Bajo
4.11	Amenazas personales	0.07	Bajo
4.20	Adicciones (alcohol, drogas)	0.00	Bajo
	Puntuación Promedio Grupo 4	**0.24**	**Bajo**
	5 Historia del Problema / Antecedentes		
5.1	Quejas, denuncias	0.47	Bajo
5.2	Chismes y rumores	0.20	Bajo
5.3	Señales / denunciantes (*soplones,* informantes)	0.00	Bajo
5.4	Incidentes previos (reincidencia)	0.00	Bajo
5.5	Problemas administrativos (atrasos laborales, inconsistencias, tendencias anormales, etc.)	0.40	Bajo
	Puntuación Promedio Grupo 5	**0.21**	**Bajo**
	Promedio de Todos los Grupos	**0.30**	**Bajo**

Anexo 3 Sistema de Controles de Integridad

Grupo	Medida		Promedio
1		**Marco de Política de Integridad**	
	1.1	Medidas de integridad incorporadas en un marco sistemático de políticas	1.29
	1.2	Objetivos concretos formulados como parte del Sistema de Integridad	2.00
	1.3	Tiempo y fondos presupuestados/previstos para la implementación de medidas de integridad	3.00
	1.4	Comunicación/divulgación de las medidas de integridad	2.40
	1.5	Política de integridad formalmente plasmada/incluida en un plan general de políticas	1.07
		Puntuación Promedio del Grupo	**1.95**
2		**Análisis de la vulnerabilidad / Análisis de riesgos**	
	2.1	Realización regular de análisis de la vulnerabilidad general / análisis de riesgos	3.00
	2.2	Ejecución de análisis detallados para áreas y posiciones/responsabilidades vulnerables	3.00
		Puntuación Promedio del Grupo	**3.00**
3		**Responsabilidades**	
	3.1	Designación de posiciones/cargos funcionales responsables de la integridad	0.43
	3.2	Realización de consultas sistemáticas entre servidores públicos responsables de la integridad	0.57
	3.3	Consejero de la Integridad	0.21
	3.4	Coordinación periódica con otras organizaciones y partes interesadas externas	1.79
	3.5	Designación de un coordinador (externo) para la política de integridad	0.00
		Puntuación Promedio del Grupo	**0.60**
4		**Marco legal de la EFS**	
	4.1	Inclusión en la Constitución de la existencia e independencia de la EFS (ISSAI 10, principio 1)	2.36
		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)	3.00
	4.3	- un mandato suficientemente amplio y discreción plena en el ejercicio/ejecución de las funciones de la EFS (ISSAI 10, principio 3)	3.00
	4.4	- acceso irrestricto a la información (ISSAI 10, principio 4)	3.00
	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)	3.00
	4.6	- la autonomía financiera y administrativa/de gestión, así como la disponibilidad apropiada de recursos humanos, materiales y monetarios (ISSAI 10, principio 8)	2.93
		Puntuación Promedio del Grupo	**2.88**
5		**Legislación y regulaciones en materia de integridad**	
		Existen reglas respecto a:	
		Conflictos de interés	
	5.1	… (reglas sobre) cargos o puestos externos / intereses financieros	3.00
	5.2	… (reglas sobre) la aceptación de regalos / invitaciones / beneficios	3.00

Grupo	Medida		Promedio
	5.3	… (reglas sobre) confidencialidad	3.00
	5.4	… (reglas sobre) prevención de “arreglos de puerta giratoria”**	3.00
	5.5	… (reglas sobre) evaluación/supervisión externa de los contratistas y/o solicitantes de licencias	3.00
	5.6	… (reglas sobre) cabildeo	3.00
	5.7	… (reglas sobre) influencia de políticos sobre los servidores públicos	3.00
		Integridad dentro de las organizaciones	
	5.8	… (reglas sobre) combate/tratamiento/frente a conductas indeseables	3.00
	5.9	… (reglas sobre) solicitud de reembolso de gastos	2.79
	5.10	… (reglas sobre) uso de email, internet y de la línea telefónica	2.93
	5.11	… (reglas sobre) uso de la propiedad / bienes de los empleadores	3.00
		Puntuación Promedio del Grupo	**2.97**
6		**Organización administrativa y control interno**	
	6.1	Especificación de actividades y posiciones/cargos vulnerables	3.00
	6.2	Existencia de procedimientos específicos para realizar actividades vulnerables	3.00
	6.3	Descripciones de puesto para todo el personal/todas las responsabilidades funcionales	3.00
	6.4	Segregación de funciones/tareas	3.00
	6.5	Aplicación del “Principio de cuatro ojos”***	3.00
	6.6	Regulaciones sobre el mandato	2.80
	6.7	Esquema de rotación del trabajo	2.80
		Puntuación Promedio del Grupo	**2.94**
7		**Seguridad**	
		Se han implementado medidas en relación con	
	7.1	… seguridad física (cerraduras, ventanas, puertas, cajas de seguridad, etc.)	3.00
	7.2	… seguridad de la información (seguridad para las tecnologías de la información, política de escritorio limpio****, clasificación de la información como confidencial/secreta, autorizaciones de acceso, sistemas de archivo)	3.00
		Puntuación Promedio del Grupo	**3.00**
8		**Valores y normas**	
	8.1	La integridad es parte de la misión de la organización	2.80
	8.2	Se han formulado los valores fundamentales (ej. imparcialidad, profesionalismo, etc.)	3.00
	8.3	Código de conducta (de integridad)	3.00
	8.4	Juramento o promesa	3.00
	8.5	Ceremonia especial para hacer un juramento o presentar la promesa	3.00
		Puntuación Promedio del Grupo	**2.96**
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)	3.00
	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)	3.00

Grupo	Medida		Promedio
	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)	3.00
	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)	3.00
	9.5	La EFS ha establecido un código de ética (profesional) y normas con significancia ética que abarcan los siguientes temas:	3.00
		- 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	3.00
		Puntuación Promedio del Grupo	**3.00**
10		**Concientización de la integridad**	
	10.1	La integridad es un requerimiento explicito para todos los puestos/posiciones	3.00
	10.2	Realización regular de cursos de capacitación en materia de integridad o que incluyan este tópico en su temario	2.93
	10.3	Notificación al personal en posiciones/cargos vulnerables sobre los riesgos particulares y medidas para abatirlos	2.80
	10.4	Asesoría especial y/o existencia de un consejo que apoye al personal para enfrentar/resolver los riesgos de integridad	2.53
		Puntuación Promedio del Grupo	**2.82**
11		**Actitud de la Alta Dirección**	
	11.1	La alta dirección promueve activamente la importancia de la integridad	3.00
	11.2	La alta dirección busca activamente la implementación de una política de integridad y de medidas de integridad	3.00
	11.3	La alta dirección siempre responde apropiadamente a las cuestiones/desafíos/problemas de integridad	3.00
	11.4	La propia alta dirección cumple con las regulaciones de integridad y/o código de conducta	3.00
		Puntuación Promedio del Grupo	**3.00**
12		**Cultura Organizacional**	
	12.1	Se presta atención regular a la importancia de la integridad	3.00
	12.2	Las cuestiones o desafíos en torno a asuntos de integridad se pueden discutir de forma segura	3.00
	12.3	Hay suficiente oportunidad de expresar las críticas	2.93
	12.4	La importancia de la integridad está claramente explicada a las partes interesadas externas	2.93

Grupo	Medida		Promedio
	12.5	Existe una comunicación abierta sobre violaciones a la integridad y respecto a la forma en que se abordan/resuelven	3.00
	12.6	Existencia de una cultura en la que se hace responsable a todos los empleados por sus propios actos/conducta	3.00
	12.7	Se presta consideración suficiente a la satisfacción laboral	2.79
		Puntuación Promedio del Grupo	**2.95**
13		**Reclutamiento y selección**	
	13.1	Existen procedimientos ya establecidos para atender todas las solicitudes de empleo	3.00
	13.2	Existencia de un comité asesor de selección (de nuevas contrataciones)	3.00
	13.3	Se realiza comprobación de CV, diplomas, referencias, etc.	3.00
	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)	3.00
	13.5	La integridad es parte del programa de inducción ofrecido a personal de nuevo ingreso	3.00
	13.6	El personal firma una declaración de confidencialidad	2.79
	13.7	Se considera periódicamente la integridad durante reuniones de consulta/evaluación laboral y en entrevistas sobre el desempeño del personal	3.00
	13.8	La integridad es una consideración específica en la contratación de personal temporal y externo	2.79
	13.9	La integridad es considerada cuando un empleado deja la EFS o durante las entrevistas de salida	2.64
		Puntuación Promedio del Grupo	**2.91**
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”)	3.00
	14.2	La alta dirección es accesible para que los empleados reporten (presuntas) violaciones	3.00
	14.3	El Consejero de la Integridad está involucrado en el proceso/mecanismo de denuncia de (presuntas) violaciones	1.56
	14.4	Existencia de un procedimiento para el manejo de las señales y quejas/denuncias de fuentes/partes interesadas externas	3.00
	14.5	Existencia de un protocolo para investigar (presuntas) violaciones a la integridad	2.93
	14.6	Existencia de un registro central de violaciones de integridad	2.71
	14.7	La organización siempre responde a las violaciones de integridad	3.00
	14.8	Las sospechas respecto a la comisión de delitos son siempre notificadas a la fiscalía/procuraduría/ministerio público o a la policía	3.00
	14.9	En caso de incidentes, estos son evaluados y discutidos con el personal involucrado	3.00
		Puntuación Promedio del Grupo	**2.80**
15		**Transparencia y Rendición de cuentas**	
		General	
	15.1	La alta dirección recibe informes que dan cuenta de la política de integridad llevada a cabo/implementada	3.00

Grupo	Medida		Promedio
	15.2	Los representantes del personal reciben informes dan cuenta de la política de integridad llevada a cabo/implementada	3.00
	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	2.54
	15.4	Los informes están sistemáticamente estructurados y contienen indicadores claros	2.57
		Medidas Específicas para una EFS	
	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)	3.00
	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)	3.00
	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)	2.67
	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)	3.00
	15.9	Es público el status, competencias y obligaciones de los auditores (funcionarios públicos u otros) (ISSAI 20, capítulo 5)	3.00
	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)	2.40
	15.11	Los códigos de ética se emiten y ponen a disposición del público (ISSAI 20, capítulo 5)	3.00
	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)	2.40
		Puntuación Promedio del Grupo	**2.80**
16		**Auditoría y monitoreo**	
	16.1	El sistema de integridad es periódicamente auditado por un auditor interno.	2.08
	16.2	El sistema de integridad es revisado periódicamente por un auditor y/o supervisor externo	1.10
	16.3	El sistema de integridad es periódicamente monitoreado o evaluado por la alta dirección	2.80
		Puntuación Promedio del Grupo	**1.99**
		Puntuación Total = Puntuación promedio de todos los grupos	**2.66**

**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).
***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.
****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.