|  |  |  |  |
| --- | --- | --- | --- |
| **Dominio (s)** | **Principio(s)** | **Norma(s)** | **Documentos CAIGG relacionados** |
| Dominio II: Ética y profesionalidad | Principio 5 Mantener la confidencialidad | 5.1 Uso de información | …… |
| 5.2 Protección de la información | …… |
| Dominio IV:  Gestión de la Función  de Auditoría Interna | Principio 9 Planificar estratégicamente | Norma 9.3 Metodologías | …… |

**ÍNDICE**

|  |  |
| --- | --- |
| **Materias** | **Página** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Responsable** | **Nombre** | **Fecha** | **Firma** |
| **Realizado por:** |  |  |  |
| **Revisado por:** |  |  |  |
| **Aprobado por:** |  |  |  |

**1. OBJETIVO**

Establecer un proceso sistemático y disciplinado para garantizar un uso ético, seguro y adecuado de la información obtenida durante los servicios de auditoría interna, protegiendo su confidencialidad e integridad. Asimismo, busca prevenir el acceso, uso o divulgación no autorizada de información sensible, asegurando que su utilización se limite exclusivamente a fines profesionales y dentro de los límites establecidos.

**2. ALCANCE**

Este procedimiento abarca el uso ético, seguro y adecuado de la información a lo largo de todo el ciclo de las actividades de auditoría, tanto por parte del Jefe de Auditoría y a todos los integrantes de la función de auditoría interna, como del personal que brinde servicios de auditoría interna —de manera permanente u ocasional— en las dependencias del Servicio.

**3. DEFINICIONES**

* **Consentimiento y Autorización:** Requisito de obtener la aprobación correspondiente para compartir o divulgar información, excepto en casos de obligación legal o profesional que lo permitan o exijan.
* **Información Confidencial:** Datos sensibles obtenidos durante los trabajos de auditoría interna, cuyo acceso y divulgación deben limitarse exclusivamente a los fines profesionales autorizados.
* **Protección de la Información:** Conjunto de medidas para salvaguardar la información, incluyendo su almacenamiento, acceso y eliminación, con el fin de evitar su uso indebido o divulgación no autorizada.
* **Sector Público:** Según las NOGAI, el Estado y todas las agencias, empresas y otras entidades bajo control estatal o con presupuesto público que gestionan programas, bienes y servicios al público.
* **Seguridad de la Información:** Prácticas y herramientas utilizadas para garantizar que la información digital y física esté protegida frente a accesos no autorizados, alteraciones, pérdidas o divulgaciones.
* **Unidad Central de Armonización (Central Harmonisation Unit - CHU):** El Consejo de Auditoría Interna General de Gobierno (CAIGG) o el Servicio de Auditoría Interna de Gobierno (SAIG) son reconocidos como la Unidad Central de Armonización (CHU) a nivel gubernamental. Este organismo es responsable de establecer el marco normativo general, definir estándares y desarrollar instrumentos para la gestión de la auditoría interna en el sector público. Asimismo, tiene la función de evaluar la calidad de las disposiciones normativas y metodológicas aplicadas en la auditoría interna, garantizando su efectividad y alineación con las mejores prácticas internacionales.

Además, la CHU puede asumir la responsabilidad de dirigir, coordinar, supervisar y evaluar el desempeño de las unidades de auditoría interna de los servicios públicos que dependen o están vinculados al Poder Ejecutivo, asegurando su eficiencia y cumplimiento normativo.

* **Uso Ético de la Información:** Principio que regula que los auditores internos utilicen la información únicamente para los fines definidos en sus responsabilidades profesionales, prohibiendo el lucro personal o uso indebido.

**4. RESPONSABILIDADES**

|  |  |
| --- | --- |
| **Cargo** | **Descripción** |
| **Jefe de Auditoría** | * Entrega y supervisa la firma del compromiso de confidencialidad. * Planifica capacitaciones anuales sobre protección de la información. * Gestiona incidentes de confidencialidad, documentando medidas correctivas. * Evalúa y mejora continuamente los controles aplicados en la auditoría interna. |
| **Supervisor** | * Monitorea el cumplimiento de las medidas de seguridad y confidencialidad. * Revisa y documenta irregularidades detectadas en el manejo de la información. * Asegura la correcta clasificación y protección de la información en cada auditoría. |
| **Auditor Interno** | * Firman el compromiso de confidencialidad y cumplen con sus disposiciones. * Aplican medidas de seguridad en la recopilación y almacenamiento de datos. * Reportan incidentes de acceso no autorizado o mal manejo de información. * Asisten a capacitaciones y aplican buenas prácticas de protección de datos. |

**5. DESCRIPCIÓN PROCEDIMIENTO USO Y PROTECCIÓN DE LA INFORMACIÓN**

* 1. **Entrega y Conocimiento del Procedimiento**
* Al ingresar a la función de auditoría interna, el Jefe de Auditoría y cada auditor interno recibirán una copia del procedimiento de confidencialidad y protección de la información, junto con las políticas relacionadas.
* Deberán firmar el **Formulario Entrega de Procedimiento de Confidencialidad y Protección de la Información** para evidenciar la recepción y comprensión del contenido.
  1. **Declaración de Compromiso de Confidencialidad**
* Todos los auditores internos y personal externo que tenga acceso a información sensible deberán completar el **Formulario de Compromiso de Confidencialidad y Uso de Información.**
* Esta declaración será actualizada de manera anual o siempre que surja un cambio en las funciones del personal.
  1. **Manejo y Protección de la Información Sensible**
* Durante los trabajos de auditoría, se deberá clasificar la información recopilada según su nivel de sensibilidad y documentarla en el **Formulario de Clasificación de Información Confidencial**.
* Los auditores deberán emplear medidas como: contraseñas, sistemas de encriptación y controles de acceso según los lineamientos establecidos para garantizar la seguridad de la información.
  1. **Reporte de Incidentes Relacionados con la Información**
* En caso de pérdida, mal manejo o acceso no autorizado a información confidencial, el auditor deberá completar el **Formulario de Reporte de Incidente de Confidencialidad** y notificar de inmediato al Jefe de Auditoría.
* El Jefe de Auditoría gestionará la investigación y documentará las medidas correctivas aplicadas.
  1. **Supervisión y Verificación de Cumplimiento**
* El Supervisor revisará de manera periódica el cumplimiento de las medidas de confidencialidad y los controles aplicados, utilizando el **Formulario de Supervisión de Cumplimiento de Confidencialidad**.
* Este formulario debe incluir observaciones, irregularidades detectadas y acciones correctivas realizadas.
  1. **Capacitación y Actualización**
* El Jefe de Auditoría planificará capacitaciones anuales sobre confidencialidad, seguridad de la información y manejo de datos sensibles.
* La asistencia a las capacitaciones será registrada en el **Formulario de Registro de Capacitación en Confidencialidad**.
  1. **Evaluación y Mejora Continua**
* Al final de cada periodo anual, se completará el **Formulario de Evaluación de Cumplimiento de Confidencialidad**, donde se analizarán los resultados de los trabajos de auditoría interna, retroalimentación de incidentes y áreas de mejora.
* Este análisis será usado para actualizar y fortalecer el procedimiento y los controles aplicados.

**5.8. Aprobación y Actualización**

Este procedimiento es aprobado por el Jefe de Auditoría y por el Jefe de Servicio (cuando así se ha definido en el Servicio) y será revisado de manera periódica, al menos una vez al año, o cuando se produzcan cambios significativos en la organización o en las políticas y/o normativas aplicables.

El Jefe de Auditoría será responsable de su revisión y actualización, asegurando su continua alineación con las Normas Globales de Auditoría Interna y los lineamientos sobre la materia definidos por el Consejo de Auditoría Interna General de Gobierno (CAIGG) o por el Servicio de Auditoría Interna de Gobierno (SAIG).

**6. INDICADORES CLAVE DE DESEMPEÑO (MEDIDAS DE DESEMPEÑO)**

Para medir el progreso y el cumplimiento de los objetivos de desempeño, en alineación con las Normas Globales de Auditoría Interna, especialmente la Norma 12.2: Medición del Desempeño, y las mejores prácticas, se deben utilizar indicadores clave de desempeño, previamente aprobados por el Jefe de Servicio.

En su desarrollo, estos indicadores deben considerar los aportes y expectativas del Jefe de Servicio, con el propósito de evaluar, monitorear e informar sobre el avance y cumplimiento de la materia regulada en este procedimiento.

El período durante el cual se recopilarán y analizarán los datos de los indicadores clave de desempeño será de xx (mensual, trimestral, semestral o anual, según las metas de la función de auditoría interna y los ciclos de evaluación establecidos en la planificación estratégica). Los resultados deberán ser informados al Jefe de Servicio dentro de un plazo de xx (mensual, trimestral, semestral o anual).

Para el registro y reporte de los indicadores clave de desempeño se debe utilizar el **Formulario Cumplimiento Indicadores Desempeño.**

Los indicadores clave de desempeño a considerar son los siguientes (la lista no es taxativa):

| **Áreas Claves de Resultados** | **Categorías de Desempeño** | **Objetivos de Desempeño** | **Medidas de Desempeño** | **Fórmula de Medición** | **Metas de Desempeño** | **Frecuencia de Medición** |
| --- | --- | --- | --- | --- | --- | --- |
| **Eficiencia financiera y operativa** | Gestión del cumplimiento de procedimientos internos | Asegurar que las políticas de confidencialidad sean implementadas de manera eficiente y oportuna | Porcentaje de declaraciones de compromiso de confidencialidad firmadas a tiempo | (N° de declaraciones firmadas dentro del plazo / Total de declaraciones requeridas) × 100 | ≥ 95% | Anual |
| Cumplimiento con procedimientos internos en tiempos definidos | Garantizar que los incidentes de confidencialidad sean atendidos y resueltos en los plazos establecidos | Porcentaje de incidentes de confidencialidad gestionados dentro del tiempo definido | (N° de incidentes gestionados a tiempo / Total de incidentes reportados) × 100 | ≥ 90% | Trimestral |
| **Expectativas de los grupos de interés** | Protección de la información y cumplimiento de normativas | Asegurar que la confidencialidad de la información sea respetada en las auditorías internas | Tasa de cumplimiento en la protección de información confidencial | (N° de auditorías cumplidas sin incidentes / Total de auditorías realizadas) × 100 | ≥ 95% | Semestral |
| Control y monitoreo de riesgos relacionados con la confidencialidad | Minimizar los incidentes de mal manejo de información en auditoría interna | Número de incidentes relacionados con mal manejo de información confidencial | Conteo de incidentes detectados en el periodo | ≤ 2 incidentes al año | Anual |
| **Necesidades de recursos humanos** | Formación en normativas de confidencialidad y manejo de información | Asegurar que el equipo de auditoría y personal externo cuenten con la capacitación adecuada sobre protección de información | Porcentaje de personal capacitado en confidencialidad y protección de información | (N° de asistentes a capacitaciones / Total de personal requerido) × 100 | 100% | Anual |
| **Eficiencia financiera y operativa** | Gestión oportuna de riesgos en confidencialidad | Reducir el tiempo promedio de respuesta y resolución de incidentes de confidencialidad | Tiempo promedio de resolución de incidentes de confidencialidad | (Suma de días para resolver cada incidente / Total de incidentes gestionados) | ≤ 10 días | Trimestral |

**7. CONSIDERACIONES DE TELETRABAJO**

En el caso de encontrase realizando el trabajo por vía virtual o teletrabajo, los formularios y actas deberán realizarse igualmente, pero su conformidad se otorgará por los medios telemáticos de que se disponga. En caso de no contar con firma electrónica, la conformidad se otorgará mediante un correo electrónico de aprobación y/o forma electrónica simple.

**8. REGISTRO**

Los registros derivados de la implementación del procedimiento de formulación del Plan de Desarrollo de Competencias incluirán los formularios utilizados en cada fase, el inventario de competencias, las listas de asistencia a capacitaciones y los reportes de seguimiento y evaluación. Estos documentos serán almacenados en un sistema digital centralizado con acceso restringido. Se conservarán por un período de XX años, tras lo cual serán remitidos al archivo general del Servicio, asegurando el cumplimiento de las normativas vigentes en materia de conservación y seguridad de la información.

En esta materia, es fundamental considerar la legislación y normativa, tanto general como específica, que regula la conservación, transferencia y eliminación de documentos en el Estado.

**9. LISTA DE DISTRIBUCIÓN**

Los registros y formularios asociados al procedimiento serán distribuidos de la siguiente manera:

* **Jefe de Servicio:** Reportes anuales de evaluación de cumplimiento y registros de incidentes críticos.
* **Jefe de Auditoría:** Acceso completo a todos los documentos del procedimiento y gestión de incidentes.
* **Supervisores:** Formularios de supervisión y verificación del cumplimiento de confidencialidad.
* **Auditores Internos:** Formularios de entrega y compromiso, registros de capacitación y documentación específica según su rol.
* **Unidad de Recursos Humanos:** Registros de capacitaciones y compromisos de confidencialidad del personal.
* **Archivo General del Servicio:** Documentación transferida tras el periodo de almacenamiento digital establecido.

**10. HISTORIAL DE REVISIONES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Antecedente** | **Edición** | **Fecha** | **Aprobación final** | **Descripción del cambio** |
| Emisión |  |  |  |  |
| Primera revisión |  |  |  |  |
| Segunda revisión |  |  |  |  |
| Tercera revisión |  |  |  |  |
| Cuarta revisión |  |  |  |  |

**11. ANEXOS**

|  |  |
| --- | --- |
| **Anexo N°** | **Nombre** |
| 1 | Formulario Entrega de Procedimiento de Confidencialidad y Protección de la Información |
| 2 | Formulario de Compromiso de Confidencialidad y Uso de Información |
| 3 | Formulario de Clasificación de Información Confidencial |
| 4 | Formulario de Reporte de Incidente de Confidencialidad |
| 5 | Formulario de Supervisión de Cumplimiento de Confidencialidad. |
| 6 | Formulario de Registro de Capacitación en Confidencialidad. |
| 7 | Formulario de Evaluación de Cumplimiento de Confidencialidad |
| 8 | Formulario Cumplimiento Indicadores Desempeño. |