|  |  |  |  |
| --- | --- | --- | --- |
| **Dominio (s)** | **Principio(s)** | **Norma(s)** | **Documentos CHU 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** | **Materias** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

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

**1. OBJETIVO**

Establecer los principios y lineamientos fundamentales sobre el resguardo, propiedad y divulgación de la información del Servicio, a nivel interno y especialmente a partes externas, por parte de los auditores internos o de cualquier persona que en forma permanente o esporádica desempeñe labores de auditoría interna dentro del Servicio.

**2. ALCANCE**

Esta política se aplica a la función de auditoría interna del Servicio y a cualquier persona que se desempeñe como auditor interno en labores permanentes o no, dentro del Servicio, direcciones, divisiones, unidades funcionales, etc. cuyos procesos sean objeto de trabajos de auditoría interna.

A esta política, estarán subordinadas todas las metodologías, procedimientos y prácticas que sean formalizadas para su implementación en la función de auditoría interna del Servicio.

**Para efectos de esta política, 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 (Central Harmonisation Unit - 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.

**3. RESPONSABILIDADES**

|  |  |
| --- | --- |
| **Cargo** | **Descripción** |
| **Jefe de Servicio** | * Aprobar la política de protección de información y supervisar su implementación. * Asegurar la asignación de recursos adecuados para el cumplimiento de la política. * Evaluar periódicamente los reportes de cumplimiento y adoptar medidas correctivas en caso de desviaciones. |
| **Jefe de Auditoría** | * Garantizar la aplicación de la política en todas las actividades de auditoría. * Validar y autorizar cualquier divulgación de información, asegurando el cumplimiento normativo. * Supervisar la implementación de controles de seguridad físicos y digitales. * Organizar y liderar capacitaciones anuales sobre la confidencialidad y seguridad de la información. * Reportar al Jefe de Servicio cualquier incidente relevante de manejo indebido de la información. |
| **Supervisor** | * Verificar que el equipo de auditores cumpla con los lineamientos de la política en cada auditoría. * Revisar periódicamente el cumplimiento de los controles de seguridad establecidos. * Participar en la identificación de mejoras en los procedimientos de protección de información. * Informar al Jefe de Auditoría sobre cualquier irregularidad detectada en la aplicación de la política. |
| **Auditor Interno** | * Cumplir con los principios de confidencialidad, integridad, objetividad y debido cuidado profesional en el manejo de la información. * Utilizar la información obtenida exclusivamente para fines profesionales y no compartirla sin autorización. * Aplicar los controles de seguridad establecidos, incluyendo la autenticación de dos factores y el cifrado de datos cuando corresponda. * Reportar cualquier incidente de acceso no autorizado o uso indebido de información al Supervisor de Auditoría. |

**4. DECLARACIONES DE LA POLÍTICA**

**4.1. PRINCIPIOS RECTORES**

La implementación de esta política se fundamenta en los siguientes principios:

* **Confidencialidad:** Garantizar que la información obtenida se utilice únicamente para fines profesionales y esté protegida adecuadamente.
* **Integridad:** Actuar con honestidad y profesionalismo, evitando el uso indebido de la información para beneficio personal o de terceros.
* **Objetividad:** Prevenir cualquier influencia indebida que pueda comprometer la imparcialidad en el manejo de información.
* **Debido Cuidado Profesional:** Aplicar controles adecuados para proteger la información sensible, incluyendo medidas físicas y digitales.
* **Cumplimiento Normativo:** Asegurar la adherencia a las leyes y regulaciones aplicables, incluyendo la Ley de Probidad y Transparencia Pública.
* **Supervisión y Monitoreo:** Implementar revisiones periódicas para evaluar el cumplimiento de la política y reportar incidentes significativos.

**4.2. LINEAMIENTOS FUNDAMENTALES**

**a. Uso de la Información**

* La información obtenida durante las auditorías debe utilizarse exclusivamente para fines profesionales.
* Se prohíbe el uso de información para beneficio personal o de terceros.
* Se debe cumplir con todas las leyes y regulaciones aplicables en materia de confidencialidad y protección de datos.

**b. Divulgación de Información**

* No se podrá divulgar información sin autorización expresa, salvo en casos de obligación legal o profesional.
* Toda solicitud de divulgación debe ser validada por el Jefe de Auditoría y registrada formalmente.

**c. Controles de Seguridad**

* Se implementarán controles físicos (acceso restringido a documentos y áreas seguras).
* Se adoptarán controles digitales como cifrado de datos, autenticación de dos factores y monitoreo de accesos.
* Se realizarán auditorías periódicas para verificar la efectividad de estos controles.

**d. Capacitación y Sensibilización**

* Se impartirán capacitaciones anuales sobre la importancia de la confidencialidad y seguridad de la información.
* Se incluirán simulaciones de riesgos y escenarios prácticos para reforzar la aplicación de esta política.

**e. Supervisión y Reporte de Incidentes**

* El Jefe de Auditoría será responsable de supervisar la aplicación de la política.
* Cualquier incidente de manejo indebido de información será gestionado conforme al protocolo interno y reportado al Jefe de Servicio y al Unidad Central de Armonización (CHU), en caso de ser significativo.

**f. Aprobación y Actualización**

Esta política es aprobada por el **Jefe de Servicio** y será revisada periódicamente, al menos una vez al año o cuando se presenten cambios significativos en la organización o en las normativas aplicables.

El **Jefe de Auditoría** será responsable de su revisión y actualización, garantizando su alineación continua con las **Normas Globales de Auditoría Interna** y los lineamientos establecidos por la **Unidad Central de Armonización (CHU).**

**5. REGISTRO**

Copia de la política aprobada y sus actualizaciones, se almacenarán digitalmente durante un período mínimo de XX años. El sistema de almacenamiento garantizará un acceso seguro y restringido, disponible únicamente para el Jefe de Auditoría, los supervisores y terceros autorizados cuando sea necesario.

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.

**6. LISTA DE DISTRIBUCIÓN**

La presente política será distribuida al Jefe de Servicio, publicada en la página web institucional y difundida en el Servicio y a terceras partes que deban estar en conocimiento, de acuerdo con lo establecido por el CAIGG, la Contraloría General de la República y las normas pertinentes.

**7. HISTORIAL DE REVISIONES**

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