GUÍA PARA LA AUDITORÍA DEL USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL EN LA SUPERINTENDENCIA DE COMPETENCIA ECONÓMICA (SCE)

V1.

2025

Índice

Introducción **4**
1. Principios rectores de la auditoría **4**
2. Proceso de auditoría **5**
2.1. Fase I: Planificación **5**
2.1.1 Objetivos de la Planificación 5
2.1.2 Alcance de la Auditoría: 5
2.1.3 Metodología de la Auditoría: 6
2.1.4 Actividades 6
2.1.5 Entregables de la Fase I 7
2.1.6 Responsables de la Fase I 7
2.1.7 Cuadro resumen – Fase I: Planificación de la Auditoría de IA 8
2.2. Fase II: Levantamiento e Inventario **8**
2.2.1 Objetivo del Levantamiento e Inventario 9
2.2.2 Alcance del Levantamiento e Inventario 9
2.2.3 Actividades del Levantamiento e Inventario 9
2.2.4 Entregables de la Fase II 10
2.2.5 Responsables de la Fase II 11
2.2.6 Cuadro resumen – Fase II: Levantamiento e Inventario de Herramientas de IA 11
2.3. Fase III: Revisión documental y normativa **12**
2.3.1 Objetivo de la revisión documental y normativa 12
2.3.2 Alcance de la Revisión documental y normativa 12
2.3.3 Actividades de la Revisión documental y normativa 13
2.3.4 Entregables de la Fase III 13
2.3.5 Responsables de la Fase III 13
2.3.6 Cuadro resumen – Fase III: Revisión Documental y Normativa 14
2.4. Fase IV - Evaluación técnica y de procesos **14**
2.4.1 Objetivo de la Fase Evaluación técnica y de procesos 15
2.4.2 Alcance de la Evaluación técnica y de procesos 15
2.4.3 Actividades de la evaluación técnica y de procesos 15
2.4.4 Entregables de la Fase IV 16
2.4.5 Responsables de la Fase IV 16
2.4.6 Cuadro resumen – Fase IV: Evaluación Técnica y de Procesos 16
2.5. Fase V: Evaluación de riesgos e impactos **17**
2.5.1 Objetivo de la Evaluación de riesgos e impactos 17

2.5.2 Metodología de Evaluación de riesgos e impacto 18
2.5.3 Actividades de Evaluación de riesgos e impacto 18
2.5.4 Entregables de la Fase V 19
2.5.5 Responsables de la Fase V 19
2.5.6 Cuadro resumen – Fase V: Evaluación de Riesgos e Impactos 19
2.6. Fase VI: Elaboración del informe de auditoría 20
2.6.1 Objetivo del informe 20
2.6.2 Estructura mínima del informe 21
2.6.3 Entregables de la Fase VI 22
2.6.4 Responsables de la Fase VI 23
2.6.5 Cuadro resumen – Fase VI: Elaboración del Informe de Auditoría de IA 23
2.7. Fase VII - Plan de acción y seguimiento 24
2.7.1 Objetivo del Plan de acción y seguimiento 24
2.7.2 Elaboración del Plan de Acción Correctiva y Preventiva 24
2.7.3 Responsables de la Fase VII 25
2.7.4 Seguimiento periódico 25
2.7.5 Herramientas de control 26
2.7.6 Entregables de la Fase VII 26
2.7.7 Cuadro resumen – Fase VII: Plan de Acción y Seguimiento 26
3. Indicadores de auditoría 28
3.1. Cumplimiento normativo 29
3.2. Protección de datos 29
3.3. Ética 29
3.4. Seguridad de la información 29
4. Seguimiento y mejora continua 30
4.1 Verificación de cierre de hallazgos 30
4.2 Informes periódicos 30
4.3 Lecciones aprendidas 30
4.4 Actualización normativa 31
4.5 Capacitación continua 31
Base Legal 31
Glosario 32
Nivel de Aprobación V1 33

Control de versiones del documento

Título del documento:	GUÍA PARA LA AUDITORÍA DEL USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL EN LA SUPERINTENDENCIA DE COMPETENCIA ECONÓMICA (SCE)		
Propietario:	SCE		
Distribución:	Electrónica		
Versión:	1.0	**Fecha de aprobación:**	14-10-2025
Uso de IA generativa	SI		

Introducción

El uso de herramientas de Inteligencia Artificial (IA) representa una oportunidad estratégica para mejorar la eficiencia, la transparencia y la capacidad analítica de la Superintendencia de Competencia Económica (SCE). Sin embargo, también introduce riesgos éticos, legales, técnicos y organizacionales que deben gestionarse con rigor.

Consciente de estas implicaciones, la SCE establece esta Guía para la Auditoría del Uso de IA, destinada a ser aplicada mediante la coordinación con las áreas pertinentes por medio del Comité de Ética de la Inteligencia Artificial (IA) como órgano responsable de la supervisión interna. Su propósito es garantizar que todas las aplicaciones de IA dentro de la institución respeten el marco normativo nacional (especialmente la Ley Orgánica de Protección de Datos Personales – LOPDP y su Reglamento), los principios del Código de Ética de la SCE, el Esquema Gubernamental de Seguridad de la Información (EGSI) y los lineamientos de ética pública.

La guía desarrolla un proceso de auditoría detallado, indicadores de seguimiento y un sistema de mejora continua que permitirán mantener administrados los riesgos y generar confianza tanto interna como hacia la ciudadanía.

1. Principios rectores de la auditoría

La auditoría del uso de IA se fundamenta en un conjunto de principios que orientan su alcance y metodología:

- **Legalidad**: toda herramienta de IA debe sustentarse en un marco jurídico válido. No se podrá implementar una solución de IA si el tratamiento de datos carece de base legal o si vulnera derechos constitucionales.

- **Ética institucional**: la SCE, como órgano de control, debe utilizar la IA con imparcialidad, responsabilidad y respeto a los valores, evitando cualquier riesgo de sesgo o manipulación indebida.
- **Protección de datos personales**: la auditoría debe confirmar que cada sistema de IA cumple con los principios de licitud, finalidad, proporcionalidad, minimización y confidencialidad, garantizando que los titulares puedan ejercer sus derechos.
- **Supervisión humana**: ninguna decisión automatizada puede adoptarse sin revisión y validación de los servidores de la SCE**.**
- **Transparencia y explicabilidad**: la auditoría exigirá que se cuente con documentación que permita explicar cómo se toman las decisiones.
- **Rendición de cuentas**: toda acción vinculada al uso de IA debe poder ser atribuida a responsables específicos, con capacidad para responder ante la autoridad y la ciudadanía.

2. Proceso de auditoría

El proceso de auditoría contempla una serie de fases que deben aplicarse de manera sistemática a todos los sistemas de IA en uso o en evaluación por la SCE.

2.1. Fase I: Planificación

La auditoría inicia con la elaboración del Plan Anual de Auditoría de IA, documento que define los objetivos, el alcance, la metodología, los recursos y el cronograma del proceso.

Esta fase es liderada por el Comité de Ética de IA, en coordinación con el Oficial de Seguridad de la Información (OSI) y el Delegado de Protección de Datos (DPD), con la participación de las unidades dueñas de procesos.

2.1.1 Objetivos de la Planificación

El Comité de Ética de IA debe definir con precisión los siguientes objetivos:

- Verificar el cumplimiento de la LOPDP, su Reglamento, la LOTDA, el EGSI y demás normativa aplicable.
- Evaluar riesgos éticos del uso de IA: sesgos, discriminación y falta de explicabilidad.
- Medir la seguridad de la información y los datos conforme al EGSI.
- Determinar el nivel de supervisión humana y trazabilidad en los procesos automatizados.
- Identificar oportunidades de mejora en políticas, procesos y controles**.**

2.1.2 Alcance de la Auditoría:

- **Identificar las herramientas y sistemas de IA que serán objeto de evaluación**, priorizando aquellos con mayor impacto en los procesos institucionales o en la gestión de datos personales.
- **Delimitar las unidades y áreas organizacionales incluidas en el alcance de la auditoría**, en función de su rol en el uso, desarrollo o supervisión de herramientas de IA.
- **Precisar el enfoque de revisión**, estableciendo si la auditoría abarcará el uso operativo actual, los procesos de adquisición y desarrollo de soluciones de IA, o ambos ámbitos de manera integral.

2.1.3 Metodología de la Auditoría:

- **Definir el enfoque metodológico de la auditoría**, determinando si se aplicará una revisión documental, técnica, ética y/o de procesos, según la naturaleza de los sistemas de IA evaluados.
- **Establecer los criterios de auditoría**, considerando el cumplimiento del marco legal vigente, los principios de ética pública, los estándares de ciberseguridad y las buenas prácticas internacionales en gobernanza de IA.
- **Seleccionar los métodos de recolección de evidencia**, tales como entrevistas, encuestas, pruebas técnicas, revisión documental, análisis de registros (logs) y otros mecanismos que aseguren la objetividad y trazabilidad de los hallazgos, entre otros que se consideren necesarios.

2.1.4 Actividades

- **Levantamiento de insumos iniciales**: recopilar normativa vigente, políticas internas, inventario de sistemas de IA, informes de auditorías previas y matrices de riesgos existentes.
- **Definición de objetivos y prioridades**: establecer si la auditoría será de carácter general o focalizado (por ejemplo, en sistemas de alto impacto en derechos ciudadanos).
- **Determinación de recursos**: definir el equipo auditor (miembros del Comité de Ética de la IA, OSI, DPD y personal técnico), así como presupuesto de ser el caso y tiempos requeridos.
- **Diseño del cronograma de auditoría**: programar las fases (revisión documental, pruebas técnicas, entrevistas, elaboración de informe, entre otros), indicando fechas de inicio y fin.
- **Definición de criterios y umbrales de evaluación**: establecer qué se considerará como cumplimiento, incumplimiento o cumplimiento parcial; fijar indicadores claves.
- **Aprobación del plan:** el Comité de Ética de IA aprobará el Plan Anual de Auditoría de IA.

2.1.5 Entregables de la Fase I

Entradas:

- Normativa aplicable (LOPDP, su Reglamento, EGSI y Código de Ética).
- Inventario preliminar de herramientas y sistemas de IA.
- Informes de auditorías anteriores, si los hubiere.
- Matriz institucional de riesgos relacionados con el uso de IA.

Salidas:

- Objetivos, alcance y metodología de la auditoría definidos.
- Cronograma y recursos asignados.
- Criterios e indicadores de evaluación establecidos.

Entregables principales:

Plan Anual de Auditoría de IA, que debe incluir:

- Objetivos y justificación.
- Alcance institucional y tecnológico.
- Criterios y marcos de referencia.
- Recursos humanos, técnicos y financieros requeridos.
- Cronograma detallado.
- Indicadores de cumplimiento.
- Roles y responsabilidades asignados.

2.1.6 Responsables de la Fase I

- **Comité de Ética de la IA:** liderará el diseño, coordinación y aprobación del Plan Anual de Auditoría.
- **Oficial de Seguridad de la Información (OSI):** aportará lineamientos técnicos y criterios de ciberseguridad.
- **Delegado de Protección de Datos (DPD):** garantizará la conformidad con la normativa de protección de datos personales.
- **Unidades dueñas de procesos:** reportarán los sistemas de IA en uso y proporcionan la información requerida para la auditoría.
- **Intendencia Nacional Administrativo-Financiera:** autorizará los recursos financieros necesarios de ser el caso.

2.1.7 Cuadro resumen – Fase I: Planificación de la Auditoría de IA

Nro.	Actividad	Responsables Principales	Duración Estimada	Productos / Resultados Esperados
1	**Levantamiento de insumos iniciales:** recopilación de normativa, políticas internas, inventario de sistemas de IA, auditorías previas y matrices de riesgos.	Comité de Ética de IA, OSI, DPD	5 días hábiles	Matriz consolidada de insumos y riesgos iniciales.
2	**Definición de objetivos, alcance y prioridades** de la auditoría (general o focalizada).	Comité de Ética de IA	3 días hábiles	Documento de definición de objetivos y alcance.
3	**Determinación de recursos humanos, técnicos y financieros.**	Comité de Ética de IA, OSI, INAF	4 días hábiles	Lista del equipo auditor y recursos aprobados.
4	**Diseño del cronograma de auditoría**, estableciendo fases, actividades, responsables y fechas.	Comité de Ética de IA, OSI	3 días hábiles	Cronograma aprobado por el Comité.
5	**Definición de criterios, umbrales e indicadores de evaluación.**	Comité de Ética de IA, DPD, OSI	4 días hábiles	Matriz de criterios e indicadores de cumplimiento.
6	**Elaboración del Plan Anual de Auditoría de IA.**	Comité de Ética de IA	3 días hábiles	Borrador del Plan de Auditoría.
7	**Revisión y aprobación del Plan Anual de Auditoría.**	Comité de Ética de IA	2 días hábiles	Plan Anual de Auditoría de IA aprobado y oficializado.

Tabla 1: Cuadro Resumen de la Fase I

Nota: Duración total estimada de la Fase I: 24 días hábiles (aproximadamente 5 semanas)

2.2. Fase II: Levantamiento e Inventario

Es esencial que la auditoría identifique todas las herramientas de Inteligencia Artificial (IA) utilizadas en la institución. Para ello, se debe realizar un censo integral que incluya desde generadores de *prompts* hasta modelos predictivos o generativos. El inventario deberá registrar al menos los datos tratados, la base legal, el nivel de criticidad, los controles de seguridad y los responsables internos de cada herramienta.

El levantamiento e inventario constituye una fase crítica del proceso de auditoría, ya que proporciona una visión integral y actualizada del uso de IA en la (SCE). Sin este mapeo inicial, no sería posible evaluar de forma precisa los riesgos asociados, el grado de cumplimiento normativo ni la efectividad de los controles técnicos y organizacionales.

2.2.1 Objetivo del Levantamiento e Inventario

El propósito es construir un Inventario Oficial de Herramientas de IA que sirva como registro único y obligatorio. Este inventario será la fuente de referencia para todas las auditorías, evaluaciones de impacto y procesos de control ético, legal y técnico.

2.2.2 Alcance del Levantamiento e Inventario

El censo debe abarcar el uso de Inteligencia Artificial (IA) dentro de la institución, tanto en entornos. Esto incluye:

- **Herramientas adquiridas** mediante contratación o suscripción.
- **Desarrollos internos**, como prototipos o modelos entrenados por la SCE.
- **Sistemas integrados** en plataformas o aplicaciones institucionales existentes.
- **Proyectos piloto y pruebas de concepto** en ejecución o finalizados.
- **Mecanismos de detección mediante Data Loss Prevention (DLP)**, para identificar el uso no autorizado de servicios de IA externos (*shadow AI*) a través del monitoreo técnico.

2.2.3 Actividades del Levantamiento e Inventario

Diseño del cuestionario institucional: el Comité de Ética de IA, dispondrá a la Intendencia Nacional de Tecnología de la Información y Comunicaciones, el Delegado de Protección de Datos (DPD) y el Oficial de Seguridad de la Información (OSI), elaborará un cuestionario estandarizado que deberá ser completado por todas las unidades institucionales.

El cuestionario recopilará información clave sobre cada herramienta de IA, incluyendo:

- Nombre y versión de la herramienta.
- Finalidad de uso.
- Categorías de datos tratados (personales, sensibles o anonimizados).
- Base legal que respalda el tratamiento de los datos.
- Nivel de criticidad (alto, medio o bajo).
- Controles de seguridad implementados.
- Existencia de supervisión humana en decisiones automatizadas.
- Unidad responsable y funcionario encargado.

Recolección de información en las unidades: cada dirección o unidad funcional reportará los usos de IA bajo su responsabilidad. La no declaración de herramientas será considerada una falta de cumplimiento.

Descubrimiento técnico y validación: la INTIC, en coordinación con el Oficial de Seguridad de la Información (OSI), realizará verificaciones técnicas para identificar el uso de herramientas de IA no reportadas oficialmente.

Estas acciones incluirán, entre otras:

- **Revisión de registros y trazas de red,** para detectar accesos a servicios de IA externos no incluidos en el inventario institucional.
- **Análisis del software instalado,** en los equipos institucionales para identificar aplicaciones o complementos de IA.
- **Validación de logs,** en sistemas y aplicaciones críticas a fin de confirmar posibles interacciones con servicios de IA no declarados.

Consolidación de información: el Comité de Ética de la IA instruirá al órgano administrativo correspondiente la integración y estandarización de los datos en una base centralizada, contrastando los reportes remitidos por las unidades con los hallazgos técnicos obtenidos por la INTIC.

Clasificación y priorización: cada herramienta se clasificará según su criticidad:

- **Alta**: herramientas que procesan datos personales o sensibles, o que influyen directamente en decisiones sobre ciudadanos u operadores económicos.
- **Media**: herramientas de apoyo analítico o administrativo sin impacto directo en derechos ciudadanos o de operadores económicos.
- **Baja**: aplicaciones auxiliares sin acceso a datos sensibles ni incidencia en decisiones institucionales.

2.2.4 Entregables de la Fase II

El resultado de esta fase es el Inventario Oficial de Herramientas de IA, el cual deberá actualizarse semestralmente y contener, al menos:

- Identificación de la herramienta: nombre, versión y proveedor.
- Finalidad y ámbito de uso.
- Unidad responsable y funcionario custodio.
- Tipo de datos tratados y existencia de datos personales o sensibles.
- Base legal del tratamiento.
- Nivel de criticidad asignado.
- Controles de seguridad implementados (cifrado, autenticación, acceso, anonimización).
- Supervisión humana en decisiones automatizadas.
- Documentación de respaldo: políticas, evaluaciones de impacto, manuales y registros.

2.2.5 Responsables de la Fase II

- **Comité de Ética de IA:** liderará la elaboración del cuestionario, coordinará la consolidación y validación de la información, y aprobará el Inventario Oficial de Herramientas de IA como documento institucional obligatorio.
- **Oficial de Seguridad de la Información (OSI):** ejecutará el descubrimiento técnico y verifica la aplicación de las medidas de seguridad correspondientes.
- **Delegado de Protección de Datos (DPD):** evaluará la base legal del tratamiento y garantiza la conformidad con la normativa de protección de datos personales.
- **Unidades dueñas de procesos:** reportarán las herramientas utilizadas y designadas a los responsables internos para su gestión y actualización.

2.2.6 Cuadro resumen – Fase II: Levantamiento e Inventario de Herramientas de IA

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
1	**Diseño del cuestionario institucional** para identificar herramientas de IA, sus datos, base legal, controles y responsables.	Comité de Ética de IA, INTIC, DPD, OSI	5 días hábiles	Cuestionario estandarizado aprobado por el Comité.
2	**Distribución y aplicación del cuestionario** a todas las unidades institucionales.	Comité de Ética de IA, Unidades dueñas de procesos	5 días hábiles	Formularios remitidos con la información de cada herramienta de IA.
3	**Recolección y consolidación inicial de información** proveniente de las unidades.	Unidades dueñas de procesos, INTIC	4 días hábiles	Base preliminar de herramientas reportadas.
4	**Descubrimiento técnico y validación** para detectar uso no declarado (shadow AI). Incluye revisión de red, software y logs.	INTIC, OSI	6 días hábiles	Informe técnico de detección de herramientas no reportadas.
5	**Integración y estandarización de la información** en una base centralizada.	Comité de Ética de IA, INTIC	3 días hábiles	Inventario consolidado con datos validados.
6	**Clasificación y priorización** de herramientas según su criticidad (alta, media o baja).	Comité de Ética de IA, DPD, OSI	3 días hábiles	Matriz de criticidad aprobada.
7	**Aprobación del Inventario Oficial de Herramientas de IA** como documento institucional.	Comité de Ética de IA	2 días hábiles	Inventario Oficial aprobado y publicado.

Tabla 2: Cuadro Resumen de la Fase II

Nota: Duración total estimada: 28 días hábiles (≈ 6 semanas)

2.3. Fase III: Revisión documental y normativa

Una vez concluido el levantamiento e inventario, el Comité de Ética de la IA procederá a revisar la documentación asociada al uso de Inteligencia Artificial (IA) en la Superintendencia de Competencia Económica (SCE). El objetivo es verificar que todos los documentos estén actualizados y alineados con la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento, el Esquema Gubernamental de Seguridad de la Información (EGSI), la Ley Orgánica de Transformación Digital y Audiovisual (LOTDA) y el Código de Ética Institucional**.**

Esta fase garantizará que el uso de la IA en la SCE se encuentre debidamente regulado, documentado y conforme al marco legal y ético vigente**.** Constituye un paso esencial para asegurar que cada herramienta de IA cuente con respaldo normativo y técnico suficiente**,** minimizando los riesgos de incumplimiento, arbitrariedad o falta de transparencia.

2.3.1 Objetivo de la revisión documental y normativa

Verificar que toda la documentación relacionada con las herramientas de IA cumpla con los siguientes criterios:

- **Completitud:** que incluya políticas, manuales, registros, evaluaciones y demás documentos requeridos.
- **Actualización:** que refleje la normativa y las prácticas vigentes, evitando versiones desactualizadas u obsoletas.
- **Conformidad normativa:** que esté alineada con el marco legal e institucional aplicable, incluyendo:
    - Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento.
    - Esquema Gubernamental de Seguridad de la Información (EGSI).
    - Código de Ética de la SCE.
    - Políticas y lineamientos internos de la institución.

2.3.2 Alcance de la Revisión documental y normativa

La revisión documental debe abarcar el ciclo de vida de las herramientas de IA, incluyendo:

- **Políticas y lineamientos internos:** uso de IA, seguridad de la información, protección de datos personales y ética institucional.
- **Evaluaciones de impacto:** análisis de riesgos en privacidad, seguridad y ética.
- **Registros de tratamiento:** conforme a la LOPDP, con detalle de responsables, finalidades y tipos de datos tratados.
- **Documentación técnica y manuales:** operación, trazabilidad de decisiones y supervisión humana.

- **Evidencias y auditorías previas:** informes, actas y resultados de pruebas de cumplimiento o seguridad.

2.3.3 Actividades de la Revisión documental y normativa

- **Requerimiento de información:** el Comité de Ética de la IA solicitará que cada unidad entregue la documentación asociada a las herramientas bajo su responsabilidad.
- **Verificación de completitud:** se comprobará la existencia de la documentación mínima obligatoria (política de privacidad, registro de tratamiento y manual de uso).
- **Revisión de vigencia:** se validará que los documentos estén actualizados y alineados con la normativa vigente; aquellos con más de dos años sin revisión deberán actualizarse.
- **Contraste normativo:**

    - El DPD verifica la conformidad con la LOPDP y su Reglamento.
    - El OSI evalúa la alineación con el EGSI.
    - El Comité de Ética de la IA revisa la coherencia con el Código de Ética Institucional.
      Identificación de brechas: se detectan inconsistencias, omisiones o falta de alineación con los marcos normativos.
    - Registro y seguimiento: se elabora una matriz de brechas documentales, con responsables, nivel de riesgo y plazos para su corrección.

2.3.4 Entregables de la Fase III

El producto de esta fase es el **Informe de Revisión Documental y Normativa**, que debe incluir:

- Listado de documentos revisados por cada herramienta de IA.
- Evaluación de completitud y vigencia (completo, parcial, ausente / actualizado o desactualizado).
- Nivel de alineación con la LOPDP, su Reglamento, el EGSI y el Código de Ética.
- Brechas identificadas, clasificadas por nivel de riesgo (alto, medio o bajo).
- Recomendaciones para la actualización o elaboración de la documentación faltante.

2.3.5 Responsables de la Fase III

- **Comité de Ética de la IA:** lidera la fase, coordina los requerimientos de información, consolida los hallazgos y valida los resultados finales.
- **Delegado de Protección de Datos (DPD):** verifica el cumplimiento de la **LOPDP** y revisa las **evaluaciones de impacto** relacionadas con el tratamiento de datos personales.

- **Oficial de Seguridad de la Información (OSI):** analiza la alineación con el **EGSI** y evalúa la efectividad de los **controles de ciberseguridad** implementados.
- **Unidades dueñas de procesos:** entregan la documentación solicitada, atienden las observaciones y ejecutan las acciones correctivas correspondientes.

2.3.6 Cuadro resumen – Fase III: Revisión Documental y Normativa

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
1	**Requerimiento de información** a las unidades sobre documentación de las herramientas de IA.	Comité de Ética de IA	3 días hábiles	Solicitudes enviadas y cronograma de recepción definido.
2	**Recepción y verificación de completitud** de la documentación mínima (política de privacidad, registro de tratamiento, manual de uso).	Comité de Ética de IA, Unidades dueñas de procesos	5 días hábiles	Lista de documentos recibidos y matriz de completitud.
3	**Revisión de vigencia** de documentos y validación de actualizaciones normativas.	Comité de Ética de IA, DPD, OSI	4 días hábiles	Registro de documentos actualizados u obsoletos.
4	**Contraste normativo:** – DPD verifica LOPDP – OSI evalúa EGSI – Comité de Ética revisa coherencia con el Código de Ética.	Comité de Ética de IA, DPD, OSI	6 días hábiles	Informe de conformidad normativa y ética.
5	**Identificación de brechas documentales** (inconsistencias, omisiones, desactualizaciones).	Comité de Ética de IA	3 días hábiles	Matriz de brechas y clasificación de riesgos (alto, medio, bajo).
6	**Registro y seguimiento de brechas**, con designación de responsables y plazos de corrección.	Comité de Ética de IA, Unidades dueñas de procesos	4 días hábiles	Plan de acción correctiva documentado.
7	**Elaboración y aprobación del Informe de Revisión Documental y Normativa.**	Comité de Ética de IA	3 días hábiles	Informe final aprobado con recomendaciones.

Tabla 3: Cuadro Resumen de la Fase III

Nota: Duración total estimada: 28 días hábiles (≈ 6 semanas)

2.4. Fase IV - Evaluación técnica y de procesos

La auditoría evaluará el funcionamiento práctico de los sistemas de IA, verificando las medidas de seguridad (accesos, monitoreo e incidentes), la supervisión humana en procesos críticos y la aplicación de técnicas de anonimización o seudonimización de datos**.** Asimismo, revisa la calidad de los datos de entrada y la trazabilidad de los resultados**.**

El propósito es asegurar que la implementación de la IA cumpla con los principios de seguridad, transparencia, confiabilidad y ética**,** de modo que la tecnología actúe como un instrumento de apoyo institucional y no como un factor de riesgo**.**

2.4.1 Objetivo de la Fase Evaluación técnica y de procesos

Evaluar de forma integral los aspectos técnicos de las herramientas de IA y sus procesos asociados, verificando que:

- Se cumplan los estándares de seguridad de la información, conforme al EGSI.
- Existan mecanismos de supervisión humana en las decisiones críticas.
- El tratamiento de datos respete los principios de licitud, minimización y proporcionalidad establecidos en la LOPDP y su Reglamento.
- Los modelos generen resultados trazables, explicables y verificables.
- Los procesos internos estén documentados, controlados y orientados a la mejora continua.

2.4.2 Alcance de la Evaluación técnica y de procesos

Esta fase abarca la revisión de los principales componentes técnicos y operativos vinculados al uso de IA, incluyendo:

- **Infraestructura tecnológica:** hardware, software, entornos en la nube y mecanismos de ciberseguridad.
- **Gestión de accesos:** roles, autenticación y segregación de funciones.
- **Protección de datos:** aplicación de técnicas de anonimización, seudonimización y cifrado.
- **Supervisión humana:** validación o corrección de decisiones automatizadas por personal autorizado.
- **Calidad de datos:** pertinencia, exactitud y actualización de los datos de entrenamiento y operación.
- **Procesos internos:** manuales de uso, gestión de incidentes, control de cambios y mantenimiento.

2.4.3 Actividades de la evaluación técnica y de procesos

- **Pruebas de seguridad informática:** validación de controles de acceso (roles, autenticación multifactor), revisión de registros y *logs*, ejecución de pruebas de *ethical hacking* y verificación de políticas de actualización y parches de seguridad.
- **Supervisión humana:** identificación de decisiones críticas, confirmación de instancias de validación humana y revisión de protocolos de intervención ante resultados anómalos.
- **Anonimización y seudonimización:** evaluación de técnicas aplicadas para proteger datos personales o sensibles, verificación de su irreversibilidad y cumplimiento de la LOPDP y su Reglamento.

- **Calidad de datos:** revisión de fuentes, detección de sesgos, validación de integridad y actualización de datos, garantizando el principio de minimización.
- **Trazabilidad y explicabilidad:** análisis de bitácoras y registros que documentan la generación de decisiones, evaluación de la capacidad explicativa y validación periódica de modelos.
- **Procesos de gestión:** verificación de manuales de operación, protocolos de respuesta ante incidentes y aplicación de procedimientos formales de gestión de cambios en algoritmos, modelos o proveedores.

2.4.4 Entregables de la Fase IV

El resultado de esta fase es el Informe de Evaluación Técnica y de Procesos, que debe incluir:

- Estado de las medidas de seguridad (cumple, parcialmente cumple o no cumple).
- Nivel y efectividad de la supervisión humana.
- Resultados de la validación de anonimización y seudonimización.
- Calidad de los datos (alta, media o baja) y riesgos identificados.
- Grado de trazabilidad y explicabilidad de los sistemas evaluados.
- Procesos documentados y nivel de cumplimiento.
- Recomendaciones de mejora, con responsables y plazos definidos.

2.4.5 Responsables de la Fase IV

- **Comité de Ética de la IA:** coordinará la fase, consolidará los hallazgos técnicos y los evalúa desde una perspectiva ética y de gobernanza.
- **Oficial de Seguridad de la Información (OSI):** ejecutará las pruebas de seguridad, analiza los registros (*logs*) y valida el cumplimiento del EGSI y los controles de ciberseguridad.
- **Delegado de Protección de Datos (DPD):** verificará el cumplimiento de la LOPDP y la correcta aplicación de las medidas de anonimización y seudonimización**.**
- **Unidades dueñas de procesos:** facilitarán el acceso a los sistemas, reportarán incidentes y presentan las evidencias de operación requeridas.
- **Equipo técnico de TI:** realizarán las pruebas técnicas, brindarán soporte operativo y documentarán los resultados.

2.4.6 Cuadro resumen – Fase IV: Evaluación Técnica y de Procesos

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
1	**Pruebas de seguridad informática:** revisión de controles de acceso, autenticación multifactor, logs, parches de seguridad y pruebas de ethical hacking.	OSI, Equipo Técnico de TI	6 días hábiles	Informe técnico de ciberseguridad con hallazgos y nivel de cumplimiento del EGSI.

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
2	**Verificación de supervisión humana:** identificación de decisiones críticas, validación de instancias humanas y revisión de protocolos de intervención.	Comité de Ética de IA, Unidades dueñas de procesos	4 días hábiles	Registro de decisiones críticas y evidencia de validación humana.
3	**Evaluación de anonimización y seudonimización:** análisis de técnicas aplicadas, irreversibilidad y conformidad con la LOPDP y su Reglamento.	DPD, OSI	4 días hábiles	Informe de cumplimiento de protección de datos personales.
4	**Revisión de calidad de datos:** validación de fuentes, detección de sesgos, integridad, actualización y principio de minimización.	Comité de Ética de IA, Equipo Técnico de TI	4 días hábiles	Matriz de calidad de datos (alta, media o baja) y riesgos asociados.
5	**Evaluación de trazabilidad y explicabilidad:** análisis de bitácoras, trazas de decisiones y capacidad de los modelos para ser interpretables.	Comité de Ética de IA, Equipo Técnico de TI	4 días hábiles	Registro de trazabilidad y evidencias de explicabilidad de los sistemas.
6	**Revisión de procesos de gestión:** verificación de manuales, gestión de incidentes, control de cambios y mantenimiento de modelos o algoritmos.	Comité de Ética de IA, Unidades dueñas de procesos, OSI	4 días hábiles	Informe de cumplimiento de procesos internos y gestión operativa.
7	**Consolidación y emisión del Informe de Evaluación Técnica y de Procesos:** integración de resultados, hallazgos y recomendaciones.	Comité de Ética de IA	2 días hábiles	Informe final aprobado con hallazgos técnicos, brechas y plan de mejora.

Tabla 4: Cuadro Resumen de la Fase IV

Nota: Duración total estimada: 28 días hábiles (≈ 6 semanas)

2.5. Fase V: Evaluación de riesgos e impactos

Todo uso de Inteligencia Artificial (IA) implica riesgos que deben ser gestionados. Por ello, la auditoría aplicará, según corresponda, la Evaluación de Impacto en Protección de Datos y los análisis de riesgos éticos, técnicos y operativos, considerando el cumplimiento del **EGSI**, la **LOPDP** y la **LOTDA**.

Esta fase es esencial para anticipar, clasificar y mitigar los riesgos asociados al uso de la IA en la Superintendencia de Competencia Económica (SCE)**,** garantizando que su implementación sea responsable, ética y segura, y que las decisiones institucionales se adopten con base en evidencia y sostenibilidad.

2.5.1 Objetivo de la Evaluación de riesgos e impactos

El objetivo principal es identificar, medir y priorizar los riesgos asociados al uso de IA, con el fin de:

- Proteger los derechos de las personas, especialmente la privacidad y la no discriminación.
- Reducir vulnerabilidades técnicas y de ciberseguridad.
- Prevenir sesgos y falta de transparencia en decisiones automatizadas.
- Garantizar la continuidad operativa de los servicios institucionales.
- Asegurar la conformidad normativa y ética de todas las actividades de IA.

2.5.2 Metodología de Evaluación de riesgos e impacto

La auditoría aplicará una combinación de metodologías**,** según la naturaleza del sistema evaluado:

- **Evaluación de Impacto en Protección de Datos:** se aplicará cuando la IA procesa datos personales o sensibles. Considera la finalidad del tratamiento**,** los flujos de datos**,** los riesgos de privacidad, y las medidas de mitigación técnicas y organizativas.
- **Análisis de riesgos éticos:** examinará riesgos relacionados con los principios éticos como la falta de explicabilidad, la pérdida de control humano o el uso indebido de la IA fuera de su propósito original.
- **Análisis de riesgos técnicos y operativos:** evaluará vulnerabilidades de infraestructura y procesos**,** como ciberataques**,** fallos de disponibilidad**,** dependencia tecnológica y obsolescencia de modelos.

2.5.3 Actividades de Evaluación de riesgos e impacto

- **Identificación de riesgos:** recopilar información del Inventario de IA, realizar entrevistas con responsables y técnicos, y revisar incidentes o fallos previos.
- **Clasificación de riesgos:**
    - **Altos:** afectan derechos fundamentales, generan sanciones o comprometen servicios esenciales.
    - **Medios:** impactan la reputación institucional o la operación interna.
    - **Bajos:** de impacto limitado y fácil mitigación.

- **Valoración de impacto y probabilidad:** cada riesgo se evalúa según su probabilidad (alta, media, baja) y su impacto (grave, moderado, menor), estableciendo el nivel de riesgo correspondiente.

Ejemplo de matriz:

Riesgo	Probabilidad	Impacto	Nivel de riesgo
Sesgo en decisiones de IA	Alta	Grave	Crítico
Dependencia de proveedor único	Media	Grave	Alto
Ciberataque al sistema de IA	Alta	Grave	Crítico
Obsolescencia tecnológica	Media	Moderado	Medio

Riesgo	Probabilidad	Impacto	Nivel de riesgo
Fallo en supervisión humana	Baja	Grave	Alto

Tabla 5: Tabla clasificación de riesgos

- **Medidas de mitigación:** incluir acciones correctivas inmediatas, preventivas (como pruebas de sesgo) y planes de contingencia ante incidentes críticos.
- **Documentación:** registrar todos los riesgos y medidas asociadas en una Matriz de Riesgos de IA, que formará parte del Informe Final de Auditoría.

2.5.4 Entregables de la Fase V

El resultado de esta fase es el Informe de Evaluación de Riesgos e Impactos, que debe contener:

- **Listado de riesgos identificados.**
- **Clasificación** según probabilidad e impacto.
- **Nivel de riesgo** (crítico, alto, medio o bajo).
- **Medidas de mitigación** propuestas.
- **Matriz de riesgos consolidada.**
- **Recomendaciones** para su monitoreo y reevaluación periódica.

2.5.5 Responsables de la Fase V

- **Comité de Ética de la IA:** liderará la fase de evaluación y determina los niveles de riesgo ético e institucional**.**
- **Delegado de Protección de Datos (DPD):** ejecutará la Evaluación de Impacto en Protección de Datos y analiza los riesgos vinculados a la privacidad y al tratamiento de información personal**.**
- **Oficial de Seguridad de la Información (OSI):** identificará y evalúa los riesgos técnicos y de ciberseguridad asociados al uso de IA.
- **Unidades dueñas de procesos:** proporcionarán la información sobre el uso operativo de las herramientas de IA y colaboran en la definición de medidas de mitigación**.**

2.5.6 Cuadro resumen – Fase V: Evaluación de Riesgos e Impactos

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
1	**Identificación de riesgos:** recopilación de información del Inventario de IA, entrevistas a responsables y revisión de incidentes o fallos previos.	Comité de Ética de IA, DPD, OSI	5 días hábiles	Listado preliminar de riesgos asociados a herramientas y procesos de IA.
2	**Clasificación de riesgos:** categorización de riesgos en niveles alto, medio o bajo según su impacto en	Comité de Ética de IA, OSI	4 días hábiles	Matriz de clasificación de riesgos con criterios y categorías definidas.

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
	derechos, reputación o servicios esenciales.			
3	**Valoración de impacto y probabilidad:** análisis de probabilidad (alta, media, baja) e impacto (grave, moderado, menor) para definir el nivel de riesgo.	Comité de Ética de IA, DPD, OSI	5 días hábiles	Evaluación priorizada de riesgos según criticidad.
4	**Evaluación específica de riesgos:** aplicación de metodologías complementarias: – Evaluación de Impacto en Protección de Datos (EIPD).– Análisis de riesgos éticos.– Análisis de riesgos técnicos y operativos.	DPD, Comité de Ética de IA, OSI	6 días hábiles	Informes parciales de riesgos éticos, técnicos y de privacidad.
5	**Definición de medidas de mitigación:** formulación de acciones correctivas, preventivas y de contingencia.	Comité de Ética de IA, OSI, DPD, Unidades dueñas de procesos	4 días hábiles	Plan de mitigación documentado con responsables, tiempos y acciones priorizadas.
6	**Documentación y consolidación de resultados:** registro en la **Matriz de Riesgos de IA** y elaboración del **Informe de Evaluación de Riesgos e Impactos.**	Comité de Ética de IA	4 días hábiles	Informe final con matriz consolidada de riesgos y recomendaciones.

Tabla 6: Cuadro Resumen de la Fase V

Nota: Duración total estimada: 28 días hábiles (≈ 6 semanas)

2.6. Fase VI: Elaboración del informe de auditoría

El Comité de Ética de la IA consolidará los resultados en el Informe de Auditoría de IA, que resumirá el grado de cumplimiento normativo, los riesgos identificados, las medidas implementadas y las recomendaciones de mejora**.** Los hallazgos se clasifican como cumplimiento total, parcial o incumplimiento, y se jerarquizan según su nivel de riesgo (alto, medio o bajo).

Esta fase marca la culminación del proceso de auditoría, transformando los hallazgos en un documento formal, verificable y orientado a la toma de decisiones. El informe constituye no solo un registro de cumplimiento, sino también una herramienta de mejora continua y rendición de cuentas institucional**.**

2.6.1 Objetivo del informe

- **Infraestructura:** evaluación de la situación de la infraestructura tecnológica existente.
- **Continuidad operativa:** verificación de SLA y planes de contingencia.

- **Síntesis de hallazgos:** presentación estructurada de todos los resultados de la auditoría.
- **Cumplimiento normativo:** valoración clara del grado de conformidad con la normativa vigente.
- **Gestión de riesgos:** exposición de riesgos actuales y potenciales.
- **Recomendaciones:** propuesta de medidas correctivas y preventivas, con responsables y plazos.
- **Priorización:** jerarquización de observaciones según su nivel de criticidad para orientar la gestión institucional.

2.6.2 Estructura mínima del informe

- **Portada e identificación**
  - Nombre de la auditoría y período evaluado.
  - Equipo auditor (Comité de Ética de la IA, OSI, DPD y unidades participantes).
  - Fecha y versión del documento.

- **Resumen ejecutivo**
  - Principales hallazgos y conclusiones.
  - Nivel global de cumplimiento (alto, medio o bajo).
  - Recomendaciones estratégicas prioritarias.

- **Introducción y marco normativo**
  - Objetivos, alcance y metodología aplicada.
  - Normativa de referencia (LOPDP, LOTDA, Reglamento, EGSI, Código de Ética y políticas internas).

- **Descripción de sistemas auditados**
  - Listado de herramientas de IA incluidas en el alcance.
  - Finalidad, ámbito de aplicación y unidad responsable.

- **Hallazgos de auditoría**
  - Cumplimiento normativo (total, parcial o incumplimiento).
  - Riesgos técnicos, éticos y legales identificados.
  - Evidencias revisadas y medidas correctivas implementadas.

- **Clasificación y priorización de hallazgos**
  - **Por cumplimiento:** total, parcial o incumplimiento.
  - **Por riesgo:** alto, medio o bajo.

- Matriz de hallazgos con responsables y plazos.

Ejemplo:

Sistema de IA	Hallazgo	Cumplimiento	Riesgo	Responsable	Plazo
Prompts	Falta de Evaluación de Impacto en Protección de Datos	Incumplimiento	Alto	DPD	60 días
Motor predictivo de denuncias	Manual técnico desactualizado	Parcial	Medio	Unidad Técnica	90 días

Tabla 7: Tabla clasificación y priorización de hallazgos

- **Recomendaciones de mejora**
  - Medidas correctivas y preventivas priorizadas según riesgo.
  - Incorporación de buenas prácticas.

- **Plan de acción correctiva y preventiva**
  - Acciones asignadas a responsables con plazos e indicadores de seguimiento.

- **Conclusiones y cierre**
  - Nivel de madurez en el uso de IA en la SCE.
  - Recomendaciones estratégicas para el fortalecimiento institucional.

2.6.3 Entregables de la Fase VI

El principal producto de esta fase es el **Informe de Auditoría de IA**, emitido en versión oficial, que debe ser:

- **Claro y objetivo:** libre de ambigüedades y juicios subjetivos.
- **Evidenciado:** sustentado en documentación, pruebas y entrevistas.
- **Priorizado:** con hallazgos jerarquizados que orienten la toma de decisiones.
- **Accionable:** con medidas concretas y responsables definidos.

El informe se distribuye a:

- La **máxima autoridad de la SCE**.
- Las **unidades responsables de los hallazgos**.
- El **Comité de Seguridad de la Información**, para su incorporación en la gestión institucional de riesgos.

2.6.4 Responsables de la Fase VI

- **Comité de Ética de la IA**: lidera la redacción, consolidación y validación del informe final de auditoría.
- **Delegado de Protección de Datos (DPD):** revisa y valida los hallazgos vinculados al tratamiento y protección de datos personales.
- **Oficial de Seguridad de la Información (OSI):** verifica los hallazgos técnicos y de ciberseguridad, asegurando su conformidad con el EGSI.
- **Unidades auditadas:** proporcionan evidencias de cumplimiento y observaciones de descargo durante el proceso de revisión.
- **Máxima autoridad de la SCE:** recibe, evalúa y aprueba el informe final de auditoría, disponiendo las acciones correspondientes.

2.6.5 Cuadro resumen – Fase VI: Elaboración del Informe de Auditoría de IA

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
1	**Consolidación de resultados:** recopilación y análisis de hallazgos, medidas y riesgos identificados en fases anteriores.	Comité de Ética de IA	4 días hábiles	Compendio consolidado de hallazgos técnicos, éticos y normativos.
2	**Redacción del informe preliminar:** elaboración del documento con resumen ejecutivo, marco normativo, descripción de sistemas, hallazgos y clasificación.	Comité de Ética de IA, OSI, DPD	5 días hábiles	Borrador del Informe de Auditoría de IA estructurado conforme al formato institucional.
3	**Clasificación y priorización de hallazgos:** asignación de niveles de cumplimiento (total, parcial, incumplimiento) y niveles de riesgo (alto, medio, bajo).	Comité de Ética de IA, OSI, DPD	3 días hábiles	Matriz de hallazgos clasificada con responsables, riesgos y plazos definidos.
4	**Revisión técnica y normativa:** validación del informe por parte del DPD (protección de datos) y OSI (ciberseguridad).	DPD, OSI	3 días hábiles	Informe revisado y ajustado conforme al EGSI y la LOPDP.
5	**Incorporación de observaciones:** inclusión de comentarios y descargos presentados por las unidades auditadas.	Comité de Ética de IA, Unidades auditadas	3 días hábiles	Versión ajustada con observaciones verificadas y atendidas.
6	**Formulación de recomendaciones y plan de acción:** desarrollo de medidas correctivas y preventivas con responsables y plazos de ejecución.	Comité de Ética de IA, OSI, DPD	3 días hábiles	Plan de acción correctiva y preventiva incluido en el informe.
7	**Aprobación y emisión del Informe Final de Auditoría:** validación por la máxima autoridad de la SCE y disposición de acciones institucionales.	Comité de Ética de IA, Máxima autoridad de la SCE	3 días hábiles	Informe Final de Auditoría aprobado, firmado y distribuido oficialmente.

Tabla 8: Cuadro Resumen de la Fase VI

Nota: Duración total estimada: 24 días hábiles (≈ 5 semanas)

2.7. Fase VII - Plan de acción y seguimiento

El informe debe ir acompañado de un Plan de Acción Correctivo y Preventivo, donde se asignan responsables y plazos para la implementación de mejoras. Posteriormente, el Comité de Ética de la IA realiza verificaciones periódicas (30, 90 y 180 días según la criticidad del hallazgo) para asegurar el cierre efectivo de las observaciones.

La fase de Plan de Acción y Seguimiento garantiza que la auditoría no se limite a un ejercicio diagnóstico, sino que se traduzca en mejoras concretas y sostenibles para el uso de Inteligencia Artificial (IA) en la Superintendencia de Competencia Económica (SCE). Esta etapa establece los pasos para implementar medidas correctivas y preventivas, asignar responsabilidades claras y verificar periódicamente el cumplimiento de las recomendaciones.

2.7.1 Objetivo del Plan de acción y seguimiento

- Corregir las deficiencias identificadas durante la auditoría.
- Prevenir la recurrencia de riesgos técnicos, éticos, legales y organizacionales.
- Asegurar que los hallazgos no se conviertan en problemas estructurales.
- Consolidar una cultura de mejora continua en la gestión de IA de la SCE.

2.7.2 Elaboración del Plan de Acción Correctiva y Preventiva

El Plan de Acción Correctiva y Preventiva es un documento que acompaña al informe de auditoría y que debe contener:

- **Descripción del hallazgo:** resumen claro del incumplimiento o brecha detectada.
- **Clasificación del riesgo:** alto, medio o bajo, según la metodología de la auditoría.
- **Causa raíz:** explicación de por qué ocurrió el hallazgo (ej. ausencia de controles, falta de capacitación, obsolescencia tecnológica).
- **Acción correctiva:** medidas inmediatas para resolver el problema actual.
- **Acción preventiva:** medidas estructurales para evitar la repetición.
- **Responsable asignado:** unidad o funcionario encargado de ejecutar la acción.

- **Plazo de cumplimiento:** tiempo máximo establecido para implementar la medida.
- **Indicador de verificación:** métrica que permitirá comprobar objetivamente el cierre del hallazgo.

Ejemplo de matriz "*Plan de Acción Correctiva y Preventiva*":

Nro.	Hallazgo	Riesgo	Acción Correctiva	Acción Preventiva	Responsable	Plazo	Indicador
1	Falta de Evaluación de Impacto en	Alto	Elaborar Evaluación de Impacto en	Establecer procedimiento obligatorio de Evaluación de	DPD	60 días	Evaluación de Impacto en Protección

	Protección de Datos		Protección de Datos	Impacto en Protección de Datos para nuevos proyectos			de Datos validada por Comité de Ética de la IA
2	Manual técnico desactualizado	Medio	Actualizar manual	Crear calendario semestral de revisión de manuales	Unidad Técnica	90 días	Manual actualizado publicado

Tabla 9: Cuadro Plan de Acción Preventiva y Correctiva

2.7.3 Responsables de la Fase VII

- **Comité de Ética de la IA:** coordina la elaboración del Plan de Acción Correctiva y Preventiva, aprueba las medidas propuestas y supervisa el cumplimiento.
- **Delegado de Protección de Datos (DPD):** responsable de acciones relacionadas con la privacidad y el cumplimiento de la LOPDP.
- **Oficial de Seguridad de la Información (OSI):** encargado de implementar acciones vinculadas con seguridad técnica y EGSI.
- **Unidades dueñas de procesos:** responsables de ejecutar las acciones correctivas y preventivas en sus sistemas de IA.
- **Máxima autoridad de la SCE:** valida el Plan de Acción Correctiva y Preventiva y exige rendición de cuentas en caso de incumplimiento.

2.7.4 Seguimiento periódico

El Comité de Ética de la IA debe establecer un cronograma de verificaciones periódicas, cuyo intervalo dependerá del nivel de criticidad del hallazgo:

- **Hallazgos críticos (alto riesgo):**
    - Primera verificación a los **30 días**.
    - Seguimiento adicional a los **90 días**.
    - Cierre obligatorio antes de los **120 días**.
- **Hallazgos de riesgo medio:**
    - Primera verificación a los **90 días**.
    - Cierre en un máximo de **150 días**.
- **Hallazgos de bajo riesgo:**
    - Verificación dentro de los **180 días** o en la siguiente auditoría semestral.

El seguimiento debe incluir revisión documental, entrevistas y pruebas prácticas para confirmar que las medidas adoptadas funcionan efectivamente y no solo en teoría.

2.7.5 Herramientas de control

Para gestionar el plan y su seguimiento se utilizarán:

- **Matriz Plan de Acción Correctiva y Preventiva**: documento maestro que centraliza todas las acciones correctivas y preventivas.
- **Bitácora de seguimiento**: registro de verificaciones realizadas, evidencia recibida y observaciones de avance.

2.7.6 Entregables de la Fase VII

Los principales productos de esta fase son:

- **Plan de Acción Correctiva y Preventiva**, aprobado por el Comité de Ética de la IA y validado por la máxima autoridad.
- **Informes de seguimiento** a los 30, 90 y 180 días (según criticidad), que indiquen avances y pendientes.
- **Informe de cierre de auditoría**, en el que se confirmen las medidas implementadas, se documenten las lecciones aprendidas y se actualicen las políticas internas en consecuencia.

2.7.7 Cuadro resumen – Fase VII: Plan de Acción y Seguimiento

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
1	**Elaboración del Plan de Acción Correctiva y Preventiva:** compilación de hallazgos, causas raíz y definición de medidas correctivas y preventivas.	Comité de Ética de IA, DPD, OSI, Unidades dueñas de procesos	5 días hábiles	Plan de Acción Correctiva y Preventiva elaborado y estructurado.
2	**Revisión y aprobación del Plan de Acción:** validación por el Comité de Ética de la IA y aprobación por la máxima autoridad de la SCE.	Comité de Ética de IA, Máxima autoridad de la SCE	3 días hábiles	Plan de Acción aprobado y oficializado.
3	**Asignación de responsables y plazos:** designación formal de responsables institucionales para cada acción y definición de tiempos de cumplimiento.	Comité de Ética de IA, Unidades dueñas de procesos	3 días hábiles	Matriz de responsabilidades y plazos institucionales aprobada.
4	**Implementación de acciones correctivas y preventivas:** ejecución de medidas inmediatas y estructurales según el riesgo del hallazgo.	Unidades dueñas de procesos, OSI, DPD	30 a 180 días (según criticidad)	Acciones implementadas y evidencias registradas en la matriz.
5	**Seguimiento periódico:** verificaciones a los 30, 90 y 180 días, según el nivel de riesgo (alto,	Comité de Ética de IA, OSI, DPD	En intervalos definidos	Informes de seguimiento con

Nro.	Actividad	Responsables Principales	Duración Estimada	Resultados / Productos Esperados
	medio o bajo). Incluye revisión documental y validación técnica.		(30/90/180 días)	avances, observaciones y pendientes.
6	**Control y registro:** actualización continua de la **Matriz del Plan de Acción** y la **Bitácora de Seguimiento**, con evidencias y observaciones de cumplimiento.	Comité de Ética de IA	Durante todo el período de seguimiento	Registros actualizados y trazables del cumplimiento de acciones.
7	**Elaboración del Informe de Cierre de Auditoría:** consolidación de resultados, verificación del cierre de observaciones y documentación de lecciones aprendidas.	Comité de Ética de IA, OSI, DPD	5 días hábiles	Informe de Cierre aprobado con evaluación final de cumplimiento.

Tabla 10: Cuadro Resumen de la Fase VII

Nota: Duración total estimada: Variable (de 45 a 180 días según criticidad del hallazgo)

Resumen de responsables y tiempos estimados

Resumen general – Fases, tiempos y responsables de la Auditoría de IA

Fase	Nombre de la Fase	Actividades Principales	Responsables Clave	Duración Estimada	Entregables / Resultados Principales
I	**Planificación**	- Elaboración del Plan Anual de Auditoría de IA.- Definición de objetivos, alcance, metodología y recursos.- Diseño del cronograma y criterios de evaluación.	Comité de Ética de IA, OSI, DPD, Unidades dueñas de procesos.	24 días hábiles (≈ 5 semanas)	**Plan Anual de Auditoría de IA** con objetivos, alcance, metodología, recursos y cronograma aprobados.
II	**Levantamiento e Inventario**	- Censo de herramientas de IA.- Recolección de información de unidades.- Validación técnica (INTIC–OSI) y consolidación de datos.- Clasificación por criticidad.	Comité de Ética de IA, INTIC, DPD, OSI, Unidades dueñas de procesos.	28 días hábiles (≈ 6 semanas)	**Inventario Oficial de Herramientas de IA**, validado y priorizado por nivel de criticidad.
III	**Revisión Documental y Normativa**	- Requerimiento y revisión de documentación de IA.- Verificación de completitud, vigencia y conformidad legal.- Identificación de brechas y elaboración	Comité de Ética de IA, DPD, OSI, Unidades dueñas de procesos.	28 días hábiles (≈ 6 semanas)	**Informe de Revisión Documental y Normativa**, con brechas, riesgos y recomendaciones.

Fase	Nombre de la Fase	Actividades Principales	Responsables Clave	Duración Estimada	Entregables / Resultados Principales
		de matriz de seguimiento.			
IV	**Evaluación Técnica y de Procesos**	- Pruebas de seguridad informática.- Evaluación de anonimización, trazabilidad y supervisión humana.- Revisión de calidad de datos y procesos operativos.	Comité de Ética de IA, OSI, DPD, Equipo Técnico de TI, Unidades dueñas de procesos.	28 días hábiles (≈ 6 semanas)	**Informe de Evaluación Técnica y de Procesos**, con hallazgos, riesgos y medidas de mejora.
V	**Evaluación de Riesgos e Impactos**	- Identificación, clasificación y valoración de riesgos.- Evaluación de impacto en protección de datos.- Formulación de medidas de mitigación y consolidación de la matriz de riesgos.	Comité de Ética de IA, DPD, OSI, Unidades dueñas de procesos.	28 días hábiles (≈ 6 semanas)	**Informe de Evaluación de Riesgos e Impactos**, con matriz consolidada y plan de mitigación.
VI	**Elaboración del Informe de Auditoría**	- Consolidación y redacción del informe.- Clasificación y priorización de hallazgos.- Validación técnica y normativa.- Aprobación y emisión del informe final.	Comité de Ética de IA, DPD, OSI, Unidades auditadas, Máxima autoridad de la SCE.	24 días hábiles (≈ 5 semanas)	**Informe Final de Auditoría de IA**, con resultados, riesgos y plan de acción aprobado.
VII	**Plan de Acción y Seguimiento**	- Elaboración y aprobación del Plan Correctivo y Preventivo.- Asignación de responsables y plazos.- Seguimiento a 30, 90 y 180 días según criticidad.- Elaboración del Informe de Cierre.	Comité de Ética de IA, DPD, OSI, Unidades dueñas de procesos, Máxima autoridad de la SCE.	45 a 180 días (según nivel de riesgo)	**Plan de Acción Correctiva y Preventiva**, **Informes de Seguimiento** y **Informe de Cierre de Auditoría**.

Tabla 11: Cuadro Resumen de las Fases de la Auditoría

Duración total estimada del ciclo completo: De 205 a 340 días hábiles (aprox. 9 a 15 meses, según el nivel de riesgo de los hallazgos).

3. Indicadores de auditoría

Los indicadores de auditoría permitirán al Comité de Ética de la IA medir, de forma clara y objetiva, si la Superintendencia de Competencia Económica (SCE) utiliza la Inteligencia Artificial (IA) conforme a los principios de legalidad, ética y seguridad.

3.1. Cumplimiento normativo

Indicador	Método de medición	Meta	Ejemplo
¿Todas las herramientas de IA están registradas en el inventario oficial?	Verificar si cada sistema (predictivo, generativo, etc.) consta en la lista oficial.	100% de los sistemas registrados.	Si la SCE usa 5 herramientas de IA, las 5 deben estar en el inventario.

Tabla 12: Indicadores cumplimiento normativo

3.2. Protección de datos

Indicador	Método de medición	Meta	Ejemplo
¿Las bases de datos usadas en IA están protegidas?	Verificar si los datos fueron anonimizados o seudonimizados antes de su uso.	≥ 95% de las bases de datos protegidas.	De 10 bases usadas, al menos 9 deben estar anonimizadas.
¿Se registraron incidentes de seguridad de datos?	Contar los casos de filtraciones, accesos indebidos o uso no autorizado.	Tendencia hacia cero incidentes.	—

Tabla 13: Indicadores protección de datos

3.3. Ética

Indicador	Método de medición	Meta
¿Se detectaron sesgos en los resultados de IA?	Revisar si los resultados afectaron de forma desigual a grupos (p. ej. género, tamaño de empresa).	0 casos en producción.
¿Las decisiones críticas fueron revisadas por un humano?	Confirmar si toda decisión sensible (p. ej. sanción o exclusión) fue validada por un funcionario.	100% de decisiones revisadas.

Tabla 14: Indicadores Ética

3.4. Seguridad de la información

Indicador	Método de medición	Meta
¿Se realizaron pruebas de seguridad en las herramientas de IA durante el último año?	Verificar la existencia de informes o actas de pruebas de seguridad.	100% de herramientas probadas.
¿Se efectuó al menos una auditoría técnica en los sistemas de IA críticos?	Revisar informes de revisión técnica emitidos durante el año.	Al menos una auditoría por cada sistema crítico.

Tabla 15: Indicadores Seguridad de la Información

4. Seguimiento y mejora continua

La auditoría del uso de IA en la Superintendencia de Competencia Económica (SCE) es un proceso permanente y evolutivo, orientado a la mejora continua. Los hallazgos no son un fin en sí mismos, sino oportunidades para fortalecer la ética, la seguridad y la eficiencia institucional, asegurando que la SCE se mantenga alineada con los avances tecnológicos y normativos.

4.1 Verificación de cierre de hallazgos

- **Descripción:** Todo hallazgo identificado debe corregirse dentro de los plazos establecidos en el Plan de Acción Correctiva y Preventiva.
- **Proceso:**
    - Las unidades responsables presentan evidencias documentales que demuestren la corrección (manuales, informes, registros de pruebas).
    - El Comité de Ética de la IA valida el cierre y la efectividad de las acciones.
    - En caso de incumplimiento, se notifica a la Máxima Autoridad y puede activarse una auditoría extraordinaria.
- **Resultado esperado:** Todos los hallazgos cerrados y documentados, con trazabilidad verificable.

4.2 Informes periódicos

- **Descripción:** El Comité de Ética de la IA informa semestralmente a la Máxima Autoridad sobre el avance de la auditoría y las acciones de mejora.
- **Contenido del informe:**
    - Estado del Plan de Acción Correctiva y Preventiva.
    - Cumplimiento de los indicadores de auditoría.
    - Áreas de mejora y recomendaciones estratégicas.
- **Resultado esperado:** La autoridad dispone de información actualizada para decisiones oportunas en políticas, recursos y contratación.

4.3 Lecciones aprendidas

- **Descripción:** Cada auditoría debe generar un espacio de **retroalimentación institucional**.
- **Proceso:**
    - Reuniones con equipos auditados.
    - Registro de buenas prácticas y errores recurrentes.
    - Incorporación de lecciones en capacitaciones y auditorías futuras.
- **Resultado esperado:** Repositorio institucional de lecciones aprendidas para fortalecer la gestión de IA.

4.4 Actualización normativa

- **Descripción:** Los hallazgos importantes deben convertirse en acciones concretas que mejoren la forma en que la institución trabaja y se organiza.
- **Acciones:**
    - Actualización de políticas de privacidad y seguridad.
    - Inclusión de cláusulas específicas en contratos con proveedores de IA (explicabilidad, auditorías, pruebas de sesgo).
    - Adaptación de protocolos a nuevas normas nacionales o internacionales.
- **Resultado esperado:** Marco normativo y contractual actualizado y alineado con las mejores prácticas.

4.5 Capacitación continua

- **Descripción:** La mejora del uso de IA dependerán de las competencias del talento humano.
- **Acciones:**
    - Implementar un programa anual de formación en ética, protección de datos, ciberseguridad y gobernanza tecnológica.
    - Realizar talleres prácticos basados en casos detectados durante auditorías.
    - Actualizar contenidos según tendencias tecnológicas y regulatorias.
- **Resultado esperado:** Consolidar una cultura institucional de uso responsable de la IA**,** basada en conocimiento y ética pública.

Base Legal

Ley Orgánica de Protección de Datos Personales
Ley Orgánica para la Transformación Digital y Audiovisual
Reglamento para la seudonimización, anonimización, bloqueo y eliminación de datos personales
Normativas sobre Gobierno Digital
Código de Ética de la Superintendencia de Competencia Económica
Guía de uso de herramientas de Inteligencia Artificial “IA” en la Superintendencia de Competencia Económica -SCE-
Esquema Gubernamental de Seguridad de la Información

Glosario

IA (Inteligencia Artificial): Conjunto de técnicas y sistemas que permiten a las máquinas realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, la toma de decisiones o el reconocimiento de patrones.

LOTDA: Ley Orgánica de Transformación Digital y Audiovisual.

EGSI: Esquema de Gestión de la Seguridad de la Información.

LOPDP: Ley Orgánica de Protección de Datos Personales.

INTIC: Intendencia Nacional de Tecnologías de la Información y Comunicaciones

Auditoría de IA: Proceso de revisión sistemática de los sistemas de inteligencia artificial, para verificar su cumplimiento normativo, ético y de seguridad.

Comité de Ética de la IA: Órgano interno encargado de supervisar y evaluar el uso responsable y ético de la inteligencia artificial en la institución.

DPD (Delegado de Protección de Datos): Funcionario responsable de velar por el cumplimiento de la Ley Orgánica de Protección de Datos Personales y garantizar los derechos de los titulares de datos.

OSI (Oficial de Seguridad de la Información): Responsable de coordinar las acciones de seguridad informática y proteger los activos de información de la institución.

Anonimización: Proceso por el cual los datos personales se transforman de manera irreversible, impidiendo que se identifique a una persona.

Seudonimización: Proceso mediante el cual los datos personales se sustituyen por identificadores ficticios, permitiendo cierto nivel de análisis sin identificar directamente a los titulares.

EGSI (Esquema Gubernamental de Seguridad de la Información): Conjunto de controles y buenas prácticas obligatorias para proteger la seguridad de la información en entidades públicas.

Sesgo algorítmico: Distorsión en los resultados de un sistema de IA que genera un trato desigual o injusto hacia determinados grupos de personas.

Human-in-the-Loop (HITL): Enfoque en el cual las decisiones críticas tomadas por un sistema de IA deben ser revisadas o validadas por una persona antes de su aplicación.

Nivel de Aprobación V1

Elaborado y Revisado por:	Alberto David Segovia Araujo **Intendente General Técnico**	Firmado electrónicamente por: ALBERTO DAVID SEGOVIA ARAUJO Validar únicamente con FirmaEC
	Mónica Uyana García **Intendente Nacional de Tecnología de la Información y Comunicaciones**	Firmado electrónicamente por: MONICA ALEXANDRA UYANA GARCIA Validar únicamente con FirmaEC
	Alejandro Cerón Gruezo **Intendente Nacional Administrativo Financiero**	Firmado electrónicamente por: ANGEL ALEJANDRO CERON GRUEZO Validar únicamente con FirmaEC
	Carlos Muñoz Montesdeoca **Director Nacional de Control Procesal** **Oficial de Seguridad de la Información**	Firmado electrónicamente por: CARLOS EDUARDO MUÑOZ MONTESDEOCA Validar únicamente con FirmaEC
	Gabriela Cristina Loaiza Suarez **Secretario General (s)** **Delegado de Protección de Datos Personales**	Firmado electrónicamente por: GABRIELA CRISTINA LOAIZA SUAREZ Validar únicamente con FirmaEC