Denominación	**Manual de Buenas Prácticas en el despliegue y uso de la Inteligencia Artificial**
Información documentada	Instrucción de Seguridad y Privacidad de la información
Referencia	ISP-0601

Rev.	Autor	Fecha	Control de modificaciones
0.0	RSEG RSIS AS	10 nov 2025	Versión inicial

*El presente documento tendrá efectos desde la fecha de su firma electrónica.

** El presente documento contiene información calificada como de uso público, por cuanto podrá ser distribuida a través de los siguientes medios:

- ☑ Tablón de anuncios virtual/Intranet de la organización
- ☑ Dirección de correo corporativa (indicar): (Distribucion) Consorcio Zona Franca Cadiz
- ☑ Otro (indicar): Sitios web, Portal de transparencia o cualquier otro medio de difusión

ÍNDICE

1. MARCO DE APLICABILIDAD

1.1 Objeto y alcance

El presente manual establece un contexto ético y operativo de promoción de las nuevas tecnologías proyectado sobre el despliegue y uso de sistemas de Inteligencia Artificial (IA) en el Consorcio de la Zona Franca de Cádiz (CZFC).

Su principal propósito consiste en asegurar que la IA se utilice como una herramienta segura, fiable y centrada en el ser humano, que contribuya a la mejora de los servicios prestados por la entidad, garantizando siempre el respeto a los derechos fundamentales y la normativa vigente en materia de protección de datos personales y seguridad de la información.

1.2 Marco normativo específico

Sin perjuicio de la aplicabilidad de otras normas generales y de aquellas que recaen sobre las entidades estatales de derecho público y la actividad del CZFC, serán de aplicación específica el Reglamento (UE) 2016/679 Reglamento General de Protección de Datos (RGPD) y el Reglamento (UE) 2024/1689 por el que se establecen las normas armonizadoras en materia de Inteligencia Artificial (RIA), así como cualquier otra norma nacional o comunitaria que regule el despliegue y uso de sistemas de Inteligencia Artificial.

Asimismo, el despliegue y uso de estos sistemas deberá integrar en todo caso los principios, reglas y criterios de aplicabilidad establecidos en el RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

1.3 Clasificación

Los sistemas de inteligencia artificial objeto de despliegue y utilización en el seno de la entidad se encuentran clasificados como **NO DE ALTO RIESGO** (riesgo limitado), asumiendo el CZFC el rol de **Responsable del despliegue**, en los términos de dicho reglamento (RIA), en virtud del cual el CZFC deberá aplicar las medidas técnicas y organizativas adecuadas para garantizar un uso conforme a estas instrucciones y mitigar los riesgos que puedan derivarse del despliegue y uso de estos sistemas.

Los usos previstos para la IA generativa dentro del CZFC (como el desarrollo de chatbots, la sintetización de documentos legales y normativos, la generación de borradores de actas y la asistencia en investigación de mercado) cumplen las condiciones para no ser considerados de Alto Riesgo, ya que no influyen sustancialmente en el resultado de la toma de decisiones.
En concreto, estos usos se consideran:

- Sistemas destinados a realizar una tarea preparatoria para una evaluación o análisis.
- Sistemas destinados a realizar una tarea de procedimiento limitada.
- Sistemas destinados a mejorar el resultado de una actividad humana previamente realizada.

Debido a ello, la calificación de No Alto Riesgo se mantiene en tanto el CZFC utilice estas herramientas solo como apoyo auxiliar e informativo y no las integre en procesos automatizados que tomen decisiones finales que produzcan efectos jurídicos o afecten significativamente los derechos fundamentales de las personas.
Los usos prohibidos del Anexo I del RIA son de Riesgo Inaceptable y, por tanto, están terminantemente vetados, independientemente de la clasificación.

2 DEFINICIONES

A los efectos de este manual, y en los términos establecidos en el RIA, se entenderá por:

1. **Sistema IA**: Sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

2. **Proveedor**: persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente.

3. **Responsable de despliegue**: persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.

4. **Puesta en servicio**: el suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista.

5. **Datos de entrenamiento**: los datos usados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables.

6. **Datos de entrada (prompt)**: los datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce un resultado de salida.

7. **Datos biométricos**: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos.

8. **Identificación biométrica**: el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos.

9. **Verificación biométrica**: : la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente.

10. **Categorías especiales de datos personales o datos personales sensibles**: las categorías de datos personales a que se refieren el artículo 9, apartado 1, del Reglamento (UE) 2016/679, el artículo 10 de la Directiva (UE) 2016/680 y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725.

11. **Anonimización**: el tratamiento que permite transformar datos personales para que estos no puedan ser vinculados a una persona identificable. Se logra eliminando o modificando identificadores directos como nombres y direcciones, o transformando otros datos (generalización) para que no puedan ser usados para reidentificar a un individuo.

12. **Seudonimización**: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

13. **Sistema de reconocimiento de emociones**: un sistema de IA destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos.

14. **Sistema de categorización biométrica**: un sistema de IA destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas.

15. **Sistema de identificación biométrica remota**: un sistema de IA destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia.

16. **Sistema de identificación biométrica remota en tiempo real**: un sistema de identificación biométrica remota, en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa; engloba no solo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas.

17. **Elaboración de perfiles**: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

18. **Alfabetización en materia de IA**: las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y demás personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar.

19. **Ultrasuplantación**: un contenido de imagen, audio o vídeo generado o manipulado por una IA que se asemeja a personas, objetos, lugares, entidades o sucesos reales y que puede inducir a una persona a pensar erróneamente que son auténticos o verídicos.

20. **Modelo de IA de uso general**: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas, independientemente de la manera en que el modelo se introduzca en el mercado, y que puede integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado.

21. **Sistema de IA de uso general**: un sistema de IA basado en un modelo de IA de uso general y que puede servir para diversos fines, tanto para su uso directo como para su integración en otros sistemas de IA.

22. **Riesgo sistémico**: un riesgo específico de las capacidades de gran impacto de los modelos de IA de uso general, que tienen unas repercusiones considerables en el mercado de la Unión debido a su alcance o a los efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a gran escala a lo largo de toda la cadena de valor.

23. **Asuntos de interés público**: cualquier información, comunicación oficial o contenido divulgativo publicado por el CZFC destinado al conocimiento o consulta general de los ciudadanos, empresas o administraciones públicas, cuya inexactitud, error o falta de transparencia pudiera afectar a la toma de decisiones, a los derechos, al cumplimiento de obligaciones o a la percepción de la entidad.

3. PRINCIPIOS RECTORES DEL USO DE LA IA EN CZFC

Principio	Descripción
I. Supervisión Humana	La IA es un apoyo; la **responsabilidad final** de cualquier decisión recae en el personal del CZFC.
II. Transparencia y Trazabilidad	El funcionamiento, las limitaciones y las fuentes de datos del sistema de IA deben ser **comprensibles y rastreables** (*auditables*).
III. Equidad y No Discriminación	Los sistemas de IA deben ser diseñados y probados para **evitar sesgos** que puedan conducir a resultados discriminatorios.
IV. Seguridad y Robustez	Los sistemas de IA deben ser técnicamente resistentes a errores, fallos y ataques (***ciberseguridad***), conforme al Esquema Nacional de Seguridad (**ENS**).
V. Sostenibilidad	Se priorizará el uso **eficiente y ambientalmente responsable** de los recursos necesarios para la IA.

3.1 Supervisión humana

La IA es un apoyo, y debe concebirse como una herramienta de apoyo auxiliar.
Responsabilidad final: La responsabilidad final de cualquier decisión que se tome recae siempre en el personal del CZFC.
La IA **complementa la experiencia y el juicio humano. En ningún caso los reemplaza**. Los usuarios deben tener la capacidad de anular o modificar las decisiones del sistema.

3.2 Transparencia y Trazabilidad

Comprensibilidad: El funcionamiento del sistema de IA debe ser **comprensible**.

Rastreabilidad (Auditable): Las limitaciones y las fuentes de datos del sistema de IA deben ser **rastreables** (auditables).

Para la trazabilidad, se deben mantener **registros de actividad (logs)** del uso del sistema.

3.3 Equidad y No discriminación

Diseño y prueba: Los sistemas de IA deben ser probados con el objetivo de **evitar sesgos**.
Resultados justos: Se busca prevenir sesgos que puedan conducir a **resultados discriminatorios** o injustos.

3.4 Seguridad y Robustez

Resistencia técnica: Los sistemas de IA deben ser técnicamente resistentes a errores, fallos y ataques (ciberseguridad).
Cumplimiento: Esta resistencia debe ser conforme al Esquema Nacional de Seguridad (ENS).

3.5 Sostenibilidad

Uso eficiente: Se debe priorizar el **uso eficiente** de los recursos necesarios para la IA.
Responsabilidad ambiental: Se priorizará también el uso **ambientalmente responsable** de dichos recursos.

4. PROCEDIMIENTO PARA EL DESPLIEGUE DE NUEVOS SISTEMAS DE INTELIGENCIA ARTIFICIAL

Con carácter previo a la adquisición y puesta en servicio de cualquier sistema de IA, el CZFC establece el siguiente procedimiento, distribuido en tres fases:
IMPORTANTE: los usuarios **no deberán desplegar ni utilizar un sistema IA que no haya sido previamente autorizado por la entidad**. Asimismo, los usuarios no deberán loguearse en las aplicaciones de IA mediante cuentas personales.

4.1 FASE I: Evaluación Preliminar

1. **Autorización**: De conformidad con el procedimiento ***PSP-02 Autorizaciones y gestión de cambios***, el departamento proponente deberá motivar la necesidad del uso del sistema, detallando los tipos de datos que utilizará y los procesos de negocio que automatizará o asistirá.
   La autorización corresponde al Responsable del Servicio, función integrada de forma colegiada en el Comité de Seguridad de la Información (CSEG) del CZFC.

2. **Clasificación del riesgo**: El Responsable de Seguridad y Privacidad de la información, de conformidad con lo dispuesto en el RIA, clasifica el sistema siguiendo las categorías de riesgos legalmente establecidas:
   a. Riesgo inaceptable
   b. Alto Riesgo
   c. Riesgo Limitado

En la edición inicial de este manual, la clasificación de los sistemas IA en el CZFC es de riesgo limitado o no de alto riesgo.

3. **Evaluación de Impacto relativa a la Protección de Datos (EIPD)**

En la medida en que el sistema trate datos personales, será necesaria la realización de una evaluación de necesidad de EIPD conforme al RGPD para mitigar los riesgos que recaen sobre la privacidad. En caso de que no fuera necesaria una EIPD, en esta fase será obligatorio en cualquier caso un Análisis de Riesgos. En todo caso deberá ser informado el Delegado de Protección de Datos (DPD) de la entidad.

4.2 FASE II: Requisitos de conformidad (exclusivo de sistemas de Alto Riesgo)

En caso de que a lo largo de la implantación y consolidación del uso de sistemas IA en el seno de la organización deviniera en la adquisición, despliegue y uso de sistemas calificados como de Alto Riesgo conforme al RIA, con carácter previo, el CZFC exigirá y verificará los siguientes puntos:

Requisito	Acción en el CZFC
Calidad y Gobernanza de Datos	Auditoría de Sesgos: Los *datasets* de entrenamiento deben ser representativos, completos y sometidos a pruebas para detectar y corregir sesgos que puedan generar resultados injustos o discriminatorios.
Documentación Técnica	Mantener un expediente técnico completo que incluya la documentación del ciclo de vida del sistema, objetivos, datos de entrenamiento, rendimiento y el proceso de evaluación de riesgos.
Supervisión Humana	Definir claramente los puntos de intervención del personal. Los usuarios deben tener la capacidad técnica y la autoridad para anular, modificar o detener una decisión del sistema.
Ciberseguridad y Robustez	Implementar medidas de seguridad para garantizar la integridad y disponibilidad del sistema, protegiéndolo de ataques que busquen modificar su comportamiento (ataques de *envenenamiento de datos* o *adversarial attacks*).
Transparencia y Explicabilidad	El sistema debe ser capaz de explicar sus resultados en términos comprensibles para el usuario y el afectado (el ciudadano o empresa).
Registro	El sistema debe ser registrado en la base de datos de la UE/AESIA antes de su puesta en servicio.

El despliegue consolidado de sistemas calificados como de Alto Riesgo implicará la revisión total del presente manual.

Asimismo, la utilización puntual u ocasional de sistemas de Alto Riesgo requerirá en todo caso autorización previa del Comité de Seguridad de la información, previo análisis de riesgos y EIPD.

4.3 FASE III: Despliegue y Monitoreo

Aprobación Formal: El Comité de Seguridad de la Información aprueba formalmente el despliegue tras verificar el cumplimiento de los requisitos.

Monitoreo Continuo: El rendimiento y la precisión del sistema deben ser supervisados continuamente para garantizar que no degrade su calidad.
Asimismo, el Responsable de Seguridad y Privacidad podrá realizar auditorías a los sistemas IA autorizados, a efectos de verificar el cumplimiento del Esquema Nacional de Seguridad, el RGPD, la LOPDGDD y las políticas internas de seguridad y privacidad de la información aprobadas en el seno de la organización.

5 ANÁLISIS DE IMPACTO Y GESTIÓN DE RIESGOS

Aunque los sistemas no están clasificados como de alto riesgo, el CZFC debe gestionar los riesgos operativos y de conformidad identificados en los análisis de riesgos periódicos. Estos análisis serán realizados, como mínimo, con carácter anual o cuando modificaciones de naturaleza tecnológica, legislativa, organizativa u operativa así lo aconsejen.

5.1 Gestión y Análisis de Riesgos

El sistema de gestión de riesgos debe ser un proceso iterativo continuo planificado y ejecutado durante todo el ciclo de vida del sistema de IA, el cual requiere revisiones y actualizaciones sistemáticas periódicas. Este proceso debe incluir la determinación y el análisis de los riesgos conocidos y previsibles que el sistema pueda plantear, la estimación y evaluación de riesgos por uso indebido razonablemente previsible, y la adopción de medidas de gestión de riesgos adecuadas y específicas.
El Responsable de Seguridad y Privacidad realizará estos análisis mediante la metodología que mejor se adapte a los sistemas IA, sin perjuicio de su inclusión como activos cuyos riesgos serán analizados a través de la metodología MAGERIT para la gestión de riesgos de seguridad de la información.

5.2 Riesgos Críticos identificados en torno a la IA de uso general

Se han identificado riesgos específicos, con un impacto calificado como alto, que deben ser mitigados:

Fugas de Datos/Exposición de Información Sensible	Riesgo de compromiso de la confidencialidad, integridad y disponibilidad de la información si se introducen datos sensibles o clasificados en los modelos de IA, especialmente si el proveedor los retiene para entrenamiento.
Incumplimiento Normativo (RGPD/LOPDGDD/RIA	El procesamiento de datos personales sin una base legal adecuada, sin informar a los interesados o sin aplicar los principios de minimización y limitación de la finalidad, puede generar sanciones y daño reputacional.
Dependencia Excesiva y Falta de Juicio Humano	La facilidad de uso puede llevar a la complacencia, minimizando la verificación y el juicio crítico del usuario, lo que resulta en ceguera algorítmica y toma de decisiones incorrectas.
Falta de Transparencia y Explicabilidad	La dificultad para entender cómo el modelo llega a conclusiones complica auditorías e impide justificar decisiones.
Apariencia de infalibilidad: "alucinaciones de la IA"	La presentación y el desarrollo del contenido de los resultados obtenidos ofrecen una falsa seguridad que puede llevar a obviar errores o información ficticia o falsa.
Riesgo de *Prompt Injection*	Vulnerabilidad de ciberseguridad que se da cuando un usuario malintencionado introduce datos o instrucciones manipuladoras (*prompts*) para **anular las reglas de seguridad** internas del modelo o **exfiltrar información confidencial o sensible** (ej., datos internos de sesiones anteriores o detalles de su entrenamiento).

5.3 Evaluación de Impacto referida a la Protección de Datos (EIPD)

El CZFC deberá realizar una EIPD conforme al artículo 35 del Reglamento (UE) 2016/679 en los siguientes supuestos:

1. **Cuando se implante la utilización de Sistemas de Alto Riesgo**: La EIPD es obligatoria cuando se trate de la adquisición, despliegue y uso de sistemas calificados como de Alto Riesgo conforme al Reglamento de Inteligencia Artificial (RIA). El despliegue de sistemas de IA de alto riesgo que son utilizados por organismos de Derecho público (como el CZFC) requiere llevar a cabo una evaluación de impacto relativa a los derechos fundamentales.

2. **Cuando se utilice el sistema IA para el tratamiento de Datos Personales a Gran Escala o Categorías Especiales**: Aunque un sistema de IA no esté clasificado como de alto riesgo, si se utiliza para alguna actividad que conlleve el tratamiento de datos personales a gran escala o categorías especiales, el CZFC debe realizar una Evaluación de Impacto en la Protección de Datos (EIPD) conforme al artículo 35 del Reglamento General de Protección de Datos (RGPD). Las categorías especiales de datos incluyen, por ejemplo, los datos biométricos utilizados para inferir emociones.

3. **Tratamiento de Datos Personales en General**: En la medida en que un sistema de IA trate datos personales, la necesidad de realizar una Evaluación de Impacto en la Protección de Datos (EIPD) se rige por el Reglamento General de Protección de Datos (RGPD, Art. 35). Esta evaluación será obligatoria cuando el tratamiento de datos genere un alto riesgo para los derechos y libertades de las personas físicas. Dicho riesgo se activa, en particular:
   - si se realiza una evaluación sistemática y exhaustiva de aspectos personales (incluida la elaboración de perfiles);
   - tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato;
   - el uso de datos biométricos con el propósito de identificar de manera única a una persona física;

- tratamientos de categorías especiales de datos;
- tratamientos que impliquen el uso de datos a gran escala.

Actualmente, dado que los sistemas de IA utilizados por el CZFC se clasifican como de No Alto Riesgo según el RIA, y su uso se limita a funciones de apoyo auxiliar e informativo (ej., tareas preparatorias que no dan lugar a efectos jurídicos), la EIPD no es obligatoria automáticamente. No obstante, toda nueva implementación de IA que implique tratamiento de datos personales deberá someterse a un análisis previo del Responsable de Privacidad para determinar si se cumplen las condiciones del RGPD que exigen la EIPD, independientemente de su clasificación en el RIA.

Sin perjuicio de lo anterior y con independencia de su calificación o no como sistema de Alto Riesgo, será necesario realizar una EIPD cuando, con objeto de aplicar medidas de seguridad que incorporen la monitorización continua del tráfico web, análisis de URLs completas, descargas y aplicación de modelos predictivos mediante IA y otras medidas de monitorización tales como:

- Evaluación o puntuación del comportamiento digital del usuario;
- Observación sistemática de la actividad de navegación y uso del correo electrónico corporativo;
- Uso de tecnologías innovadoras, como algoritmos de IA y aprendizaje automático;
- Posibilidad de decisiones automatizadas, como bloqueos de accesos o descargas.

6 OBLIGACIONES DEL CZFC COMO RESPONSABLE DE DESPLIEGUE

6.1 Alfabetización en materia de IA

El CZFC adoptará medidas para garantizar que su personal y demás personas encargadas de la utilización de estos sistemas tengan un nivel suficiente de capacidad, conocimiento y comprensión en materia de IA, teniendo en cuenta el contexto de uso previsto. Se implementarán medidas como:

1. Comprensión de la Aplicación Técnica: El entendimiento de la correcta aplicación de los elementos técnicos durante la fase de desarrollo del sistema de IA.
2. Medidas de Uso y Ejecución: El conocimiento de las medidas que deben aplicarse durante el uso del sistema y los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución.

3. Interpretación de Resultados: Las formas adecuadas de interpretar los resultados de salida del sistema de IA.
4. Repercusiones en Personas Afectadas: Para las personas afectadas, los conocimientos necesarios para comprender el modo en que las decisiones adoptadas con la ayuda de la IA tendrán repercusiones para ellas.
5. Personal Operativo: Para el personal encargado del funcionamiento y la supervisión de los sistemas de IA, contar con un nivel suficiente de alfabetización teniendo en cuenta su conocimiento técnico, experiencia, educación y formación.

6.2 Transparencia en la Interacción

En caso de que los sistemas de IA estén destinados a interactuar directamente con personas físicas, estas deben ser informadas de que están interactuando con un sistema de IA. Para ello, se usarán etiquetas del tipo "*Le informamos que está interactuando con un sistema de Inteligencia Artificial (IA)*."

6.3 Transparencia en Contenidos Sintéticos

En caso de utilización de un sistema de IA para generar o manipular texto que se publique con el fin de informar a terceros sobre asuntos de interés público, el CZFC debe divulgar que el texto ha sido generado o manipulado de manera artificial (salvo que el contenido haya sido sometido a revisión humana o control editorial).
Para ello se usarán etiquetas del tipo "*Contenido sintético elaborado por IA*".

6.4 Transparencia en Biometría/Emociones

En caso de que el CZFC despliegue un sistema de reconocimiento de emociones o un sistema de categorización biométrica, debe informar de su funcionamiento a las personas físicas expuestas a él y tratar sus datos personales conforme a las leyes de protección de datos (RGPD).
En estos casos de uso de sistema de alto riesgo, será necesario, con carácter previo a su despliegue, la autorización del Comité de Seguridad de la información, un análisis de riesgos de seguridad de la información y una EIPD, además de la revisión total del presente manual.

6.5 Gobernanza de Datos y Minimización

Como parte de una buena gestión de riesgos y para cumplir con el RGPD, los usuarios deben abstenerse de introducir información personal o sensible que no sea estrictamente necesaria, y, en caso de que lo sea, seudonimizar o anonimizar los datos sensibles no necesarios antes de introducirlos en las plataformas.

6.6 Alineación con las Políticas Internas de Seguridad

El CZFC deberá garantizar que el despliegue y uso de la IA generativa en el seno de la entidad está alineado con la política de seguridad de la información y con sus directrices de desarrollo.
Deberá asimismo definir procesos de revisión y aprobación para funciones críticas, e implementar controles de acceso y autenticación robustos, como la autenticación multifactor (MFA).

6.7 Supervisión Humana y Verificación

El CZFC deberá garantizar que la IA sea vista como una herramienta que complementa la experiencia humana. El personal debe verificar la exactitud y fiabilidad de los resultados generados por la IA para evitar "alucinaciones" o información incorrecta.
En ningún caso, el despliegue y uso de la IA generativa tendrá naturaleza sustitutiva de las personas que trabajan o interactúan con el CZFC.

7 USO ACEPTABLE Y GOBERNANZA DE DATOS

Las buenas prácticas se centrarán en la supervisión humana, la minimización de riesgos y el cumplimiento normativo (ver Anexo II).
El uso de modelos de IA de propósito general (*chatbots*, generadores de texto/código) por parte del personal está sujeto a las restricciones esenciales de uso establecidas en el apartado siguiente.

7.1 Reglas esenciales de uso

1. **Prohibición Absoluta de utilización de Datos Sensibles:** Nunca se debe introducir información calificada como confidencial, de secreto profesional o datos personales identificativos en herramientas de IA Generativa de propósito general no controladas por el CZFC.

2. **Verificación Humana Obligatoria:** Cualquier contenido generado por una IA se considera un borrador preliminar. El usuario es totalmente responsable de la exactitud, licitud, originalidad y adecuación institucional del resultado final.

3. **Transparencia:** Si una IA Generativa interactúa directamente con ciudadanos o empresas (ej. *chatbot* en la web), esta debe identificarse claramente como un agente artificial.

4. **Propiedad Intelectual y *Compliance*:** El personal debe ser consciente de que los resultados de la IA generativa podrían generar contenido con derechos de autor. Se debe revisar y reescribir el material para evitar infracciones y asegurar que la fuente de información es lícita.

5. **Revisión de Contratos de Proveedores:** El Responsable de Seguridad y Privacidad debe asegurarse de que las versiones corporativas de las herramientas de IA generativa contratadas incluyen cláusulas que impidan al proveedor utilizar los datos introducidos por el CZFC para reentrenamiento de sus modelos.

7.2 Juicio Crítico (Supervisión Humana)

1. **No Dependencia Exclusiva:** La IA debe ser tratada como una herramienta que complementa la experiencia y el juicio humano, no que los reemplaza.

2. **Verificación de Resultados:** Los usuarios deben **verificar la exactitud y fiabilidad** de los resultados generados por la IA (riesgo de "alucinaciones").

3. **Intervención Humana:** Es crucial diseñar procesos que permitan a los operadores humanos **intervenir, descartar o revertir** las predicciones o decisiones de la IA.

4. **Capacitación de Usuarios:** El personal y demás personas encargadas del funcionamiento y la utilización de los sistemas deben tener un nivel suficiente de **alfabetización en materia de IA**.

Esto incluye formación sobre cómo identificar y reportar posibles "alucinaciones" y prácticas de creación de *prompts* seguros para evitar inyecciones. La formación debe cubrir la **detección y reporte de intentos de inyección de comandos maliciosos**

5. **Políticas de Uso:** Se debe establecer una instrucción de seguridad clara de uso de IA generativa, detallando **qué tipo de información puede o no puede introducirse**.

6. **Matriz de Uso Aceptable de Herramientas de IAG autorizadas**

Esta tabla clasifica el uso permitido de herramientas de IA Generativa basándose en el tipo de información manejada, con foco en las herramientas populares del mercado (se aplica a cualquier herramienta similar que el CZFC haya previamente autorizado.

Información	Tarea	Riesgo	Uso Aceptable
Pública General	Resumen de normativa B.O.E., búsqueda de tendencias sectoriales, traducción de textos genéricos de la web.	Mínimo	Permitido. El resultado debe ser verificado por el usuario.
Interna Oficial	Borradores de correos internos no sensibles, esquemas de presentaciones no estratégicas, generación de código para tareas rutinarias no críticas.	Limitado	Permitido con cautela. Se debe asegurar que el proveedor garantice la no utilización de los datos introducidos para reentrenamiento.
Datos Personales Anonimizados	Análisis de sentimientos sobre comentarios anónimos en redes sociales; resumen de encuestas internas sin identificadores.	Medio-Alto	Requiere aprobación del Comité de Seguridad. Solo para análisis masivos, no para datos individuales. Requiere valoración de recalificación del sistema.

Información	Tarea	Riesgo	Uso Aceptable
Confidencial Difusión limitada Estratégica Datos personales no anonimizados	Planes Estratégicos, Datos fiscales de empresas, Información comercial sensible, Datos de proyectos sujetos a secreto, Informes sobre personas físicas	Inacepta-ble	Estrictamente Prohibido. Se considera una brecha de seguridad si se introduce en una plataforma externa no controlada.

7.3 Gobernanza de Datos y Privacidad

1. **Minimización de Datos:** Se debe evitar introducir información corporativa, personal o confidencial de alto valor directamente en las plataformas de IA. Los datos deben ser seudonimizados o anonimizados antes de introducirlos siempre que sea posible.

2. **Cumplimiento de RGPD:** El tratamiento de datos personales en relación con la IA debe cumplir con el Derecho de la Unión en materia de protección de datos personales. Se debe asegurar que existe un **Contrato de Encargado de Tratamiento** con el proveedor de IA que cumpla con el RGPD y que se evalúen los términos de servicio para optar por configuraciones que deshabiliten el uso de datos de entrada para entrenamiento del modelo, si es posible.

3. **Controles de Acceso:** Implementar la **autenticación multifactor (MFA)** para las cuentas que accedan a las plataformas de IA y revisar y limitar los permisos de usuario según el principio de mínimo privilegio.

4. **Registro y Trazabilidad:** Mantener **registros de actividad** (logs) del uso del sistema para facilitar la trazabilidad, auditoría y corrección de errores. Los archivos de registro se deben

conservar por un período adecuado a la finalidad, que será de al menos seis meses, a menos que el Derecho de la Unión o nacional disponga otra cosa.

5. **Gobernanza de Seguridad:** Se deben implementar políticas internas de seguridad que incluyan el uso aceptable de activos de información, protección de datos y gestión de contraseñas robustas. La información en desuso debe eliminarse mediante un procedimiento de borrado seguro.

7.4 Prácticas de IA prohibidas

De conformidad con el Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial), queda prohibida la utilización de los siguientes sistemas o prácticas de Inteligencia Artificial (IA) dentro de las actividades del CZFC, ya que contravienen los valores de la Unión y los derechos fundamentales consagrados:

1. **Manipulación Subliminal y Conductual Perjudicial:** Queda prohibida la introducción, puesta en servicio o utilización de sistemas de IA que se sirvan de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o colectivo. Esta alteración debe mermar apreciablemente la capacidad de la persona para tomar una decisión informada, haciendo que tome una decisión que de otro modo no habría tomado, y provocar, o ser razonablemente probable que provoque, perjuicios considerables (físicos, psíquicos, sociales o económicos) a esa persona o a otra.

2. **Explotación de Vulnerabilidades:** Se prohíbe el uso de sistemas de IA que exploten las vulnerabilidades de personas físicas o colectivos específicos (derivadas de su edad, discapacidad o una situación social o económica específica) con la finalidad o el efecto de alterar sustancialmente su comportamiento de un modo que cause, o sea razonablemente probable que cause, perjuicios considerables.

3. **Puntuación Ciudadana (Social Scoring)**: Se prohíbe la utilización de sistemas de IA para evaluar o clasificar a personas físicas o colectivos basándose en su comportamiento social o características personales, de forma que la puntuación resultante provoque:

◦ Trato perjudicial o desfavorable en contextos sociales no relacionados con donde se generaron los datos originalmente.

◦ Trato perjudicial o desfavorable injustificado o desproporcionado respecto a la gravedad del comportamiento social.

4. **Evaluación Predictiva de Riesgos Penales Basada Exclusivamente en Perfiles**: Se prohíbe la utilización de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que cometan un delito basándose únicamente en la elaboración del perfil o en la evaluación de los rasgos y características de su personalidad. Esta prohibición no se aplica a sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se base en hechos objetivos y verificables directamente relacionados con la actividad delictiva.

5. **Bases de Datos de Reconocimiento Facial no Selectivas**: Se prohíbe el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión.

6. **Reconocimiento de Emociones en el Trabajo:** Se prohíbe el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos. Quedan exceptuados los sistemas destinados a ser instalados o introducidos en el mercado por motivos médicos o de seguridad.

7. **Clasificación Biométrica de Atributos Sensibles:** Se prohíbe el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual.
(Ver Anexo I).

8 POLÍTICA DE TRANSPARENCIA

El CZFC, como responsable del despliegue, y sus proveedores de IA de uso general tienen una serie de obligaciones en torno a la transparencia.

8.1 Interacción con Personas Físicas

Los sistemas de IA destinados a interactuar directamente con personas físicas (como chatbots avanzados para la web corporativa) deben diseñarse para que la persona esté informada de que está interactuando con un sistema de IA.

8.2 Contenido Generado o Manipulado Artificialmente

Si el sistema de IA (incluyendo los de uso general) genera contenido sintético (audio, imagen, vídeo o texto), el proveedor debe garantizar que los resultados de salida estén **marcados en un formato legible por máquina y que sea posible detectar** que han sido generados o manipulados de manera artificial.

El responsable del despliegue (CZFC) tiene la obligación de divulgar que el texto se ha generado o manipulado artificialmente si este se publica con el fin de **informar al público sobre asuntos de interés público**. Esta obligación no se aplica si el contenido ha sido sometido a un proceso de revisión humana o control editorial y una persona física o jurídica ejerce la responsabilidad editorial.

Escenario	Obligación de Transparencia (RIA)	Medida Organizativa Sugerida
Borradores/ Análisis Internos	**No requerida.** Es de uso interno o de apoyo a la edición estándar.	**Documentar internamente** el uso de la IA para el borrador y realizar una **revisión humana completa** posterior para asegurar la exactitud.
Comunicaciones Públicas (Institucional, Comercial)	**Requerida.** Si el texto se publica para informar al público sobre asuntos de interés público y **no ha sido objeto de revisión humana o control editorial**.	**Establecer un proceso de control editorial obligatorio:** Todo contenido destinado al público debe ser revisado y aprobado por una persona física responsable de la edición, asumiendo la responsabilidad editorial. Dicho control editorial deberá ser documentado y trazable. ó

		Etiquetar el documento como “Contenido sintético elaborado por IA”.
Contenido Multimedia (Ultrasuplantación)	**Requerida.** Si la IA genera imágenes/vídeos que se asemejan a personas/eventos reales ("ultrasuplantación").	**Etiquetado claro y distinguible** de todo contenido multimedia sintético de uso público. “Contenido sintético elaborado por IA”.

9 CAPACITACIÓN, CONCIENCIACIÓN Y CULTURA DE LA INTELIGENCIA ARTIFICIAL

El CZFC elaborará anualmente planes de formación y programas de concienciación en materia de despliegue y uso de Inteligencia Artificial.

1. **Formación Obligatoria:** Todo el personal que interactúe o utilice sistemas de IA de forma regular debe completar alguna acción formativa o acudir a sesiones formativas, dentro de los programas de formación y concienciación de la entidad.
2. **Notificación de Incidentes:** Cualquier comportamiento inesperado, resultado sesgado o fallo de seguridad en un sistema de IA debe ser notificado de inmediato al Responsable de Seguridad y Privacidad.
3. **Fomento del Debate Ético:** Se promoverán foros internos para discutir los retos éticos y de servicio que plantea la IA, buscando siempre una adaptación ágil y responsable.

9.1 Temática y contenido clave

Los planes de formación de la entidad deberán tener en consideración los siguientes módulos adaptados a los distintos roles del personal del CZFC, a fin de garantizar el conocimiento técnico, la experiencia y la formación adecuados.

Módulo 1: **Fundamentos y Obligaciones del Usuario (Todo el Personal)**

Este módulo se centra en la alfabetización básica en IA y las reglas esenciales de uso para los sistemas de No Alto Riesgo.

Tema	Contenido Clave
I. Alfabetización en IA y Principios Éticos	Definición de IA de uso general (GPAI) y su finalidad prevista. Comprensión de las oportunidades y los riesgos que plantea la IA. Los cinco principios rectores del CZFC: Supervisión Humana, Transparencia, Equidad, Seguridad y Sostenibilidad.
II. Supervisión Humana y Juicio Crítico	Explicar que la IA es una herramienta que **complementa la experiencia humana** y no la sustituye. Obligación de **Verificación Humana Obligatoria** (*Human-in-the-Loop*) de todo resultado generado por IA. Cómo la IA puede generar "**alucinaciones**" o información incorrecta/sesgada y cómo reportarlas.
III. Reglas de Gobernanza de Datos (Uso Aceptable)	**Prohibición Absoluta** de introducir información clasificada como **confidencial, de secreto profesional o datos personales identificativos** en herramientas de IA Generativa no controladas por el CZFC. Instrucción de seguridad clara sobre qué tipo de información NO debe introducirse. La necesidad de **seudonimizar o anonimizar** los datos antes de introducirlos, si es posible.
IV. Riesgos de Seguridad Específicos	Formación en prácticas de **creación de prompts seguros** para mitigar los **ataques de Inyección de Prompts**.
V. Cumplimiento de Transparencia	Uso de etiquetas claras para informar a las personas físicas de que están interactuando con un sistema de IA (ej. *chatbot*). Obligación de **divulgar** que el texto se ha generado artificialmente si se publica para **informar al público sobre asuntos de interés público**.

Módulo 2: Formación Especializada para Personal Técnico (TI y Seguridad)

Este módulo profundiza en la gestión del riesgo técnico y la ciberseguridad.

Tema	Contenido Clave
I. Seguridad y Arquitectura	Configuración de seguridad y privacidad en las plataformas (tipo Gemini o NotebookLM). Implementación de **controles de acceso y autenticación robustos** como la autenticación multifactor (MFA).
II. Trazabilidad y Auditoría	Requisitos para mantener **registros de actividad (*logs*)** del uso del sistema para facilitar la trazabilidad y la corrección de errores. Monitoreo de *logs* y auditorías de uso. Deben incluir la capacidad de relacionar el **dato de entrada (prompt)** y el **resultado de salida** con el **usuario, la fecha y el sistema de IA** utilizado, para poder realizar auditorías completas en caso de incidentes.
III. Gestión de Incidentes	Actualización del plan de respuesta a incidentes de ciberseguridad. Respuesta a **incidentes graves** relacionados con IA (ej., fuga de datos a través de IA).

Módulo 3: Formación para Directivos y Comité de Seguridad

Este módulo se centra en la responsabilidad proactiva (*accountability*) y la gobernanza estratégica.

Tema	Contenido Clave
I. Marco Legal y Riesgo de Conformidad	Revisión de los **riesgos y beneficios estratégicos** de la IA. Comprensión de la **responsabilidad legal y ética** ante el incumplimiento normativo (Ley de IA de la UE). Identificación del riesgo de cruzar el umbral de **Alto Riesgo** y las obligaciones adicionales que implicaría.

II. Gobernanza y Supervisión	La importancia de la **gobernanza y la supervisión**. Definición de procesos de **revisión y aprobación** para funciones críticas. Obligación de realizar una **Evaluación de Impacto en los Derechos Fundamentales (EIPD)** si el uso del sistema se encuadra en los supuestos de alto riesgo.
III. Sesgos y Equidad	La necesidad de implementar mecanismos para **monitorear y mitigar activamente los sesgos algorítmicos** si los sistemas se utilizan para tareas sensibles (ej. clasificación,

9.2 Programa de concienciación y cultura ética de la IA

El CZFC se compromete en la elaboración e implantación de un programa que permita garantizar el desarrollo continuo de capacidades y la cultura ética de la IA.

Actividad	Frecuencia	Propósito y Base Normativa
1. Fomento del Debate Ético y de Servicio	Promoción periódica de foros internos.	Discutir los **retos éticos y de servicio** que plantea la IA, incluyendo la **diversidad, no discriminación y equidad**.
2. Notificación Inmediata de Incidentes/Riesgos	Inmediata.	Establecer un mecanismo claro para que cualquier comportamiento inesperado, resultado sesgado, o fallo de seguridad se **notifique de inmediato al Responsable de Seguridad y Privacidad**. Esto también incluye la obligación de notificar si se tienen motivos para considerar que el uso del sistema puede dar lugar a un riesgo, y **suspender el uso**.

3. Campañas de Concientización Periódicas	Trimestral o al introducir nueva funcionalidad de IA.	Crear una **cultura de ciberseguridad**, asegurando que el personal es consciente de las **limitaciones** reales del sistema de IA para evitar falsas expectativas. Recordatorio continuo sobre la **prohibición absoluta de introducir datos sensibles**.
4. Incentivo a la Responsabilidad	Continua.	Fomentar la **responsabilidad individual** en el uso de herramientas de IA. Incentivar la **notificación de usos inadecuados o riesgos percibidos**

10 REVISIÓN Y MONITOREO CONTINUO

Dado que el entorno regulatorio y tecnológico de la Inteligencia Artificial es dinámico, el CZFC, en calidad de responsable del despliegue, garantiza el monitoreo continuo para asegurar que el uso auxiliar de los sistemas IA no se transforme inadvertidamente en un uso de Alto Riesgo.
Para ello, el Comité de Seguridad de la Información del CZFC, a través del Responsable de Seguridad y Privacidad, revisará el presente manual con una periodicidad mínima anual o cuando, debido a modificaciones tecnológicas, normativas, operativas o de nivel de alguno de los sistemas, resulte obligatorio o conveniente realizar dicha revisión.

Las revisiones serán parciales cuando la necesidad revisora se proyecte sobre una parte no estructural del manual. En caso de que la necesidad de revisión sea estructural o afecte a la clasificación de los sistemas como de Alto Riesgo, la revisión será total.

10.1. Revisión y Actualización Periódica del Manual

El Manual de Buenas Prácticas en el despliegue y uso de la Inteligencia Artificial (ISP-0601) es un documento vivo sujeto a revisión para mantener la vigencia del marco ético y normativo:

1. **Periodicidad Mínima:** Los análisis de riesgos que sustentan este manual se realizarán, **como mínimo, con carácter anual**. La revisión y actualización de este Manual estará vinculada directamente a dichos análisis.

2. **Activadores de Revisión:** La revisión y potencial actualización del Manual se llevará a cabo **sin demora indebida** cuando se den:

- **Modificaciones Sustanciales:** Se produzcan **modificaciones de naturaleza tecnológica, legislativa, organizativa u operativa** que así lo aconsejen.
- **Uso de Alto Riesgo:** El CZFC evalúe la adquisición, despliegue y uso de sistemas IA de **Alto Riesgo** (como los sistemas de reconocimiento de emociones o categorización biométrica), lo que implicará la **revisión total del presente manual** antes de la puesta en servicio.
- **Cambio en la Clasificación de Riesgo:** El Responsable de Seguridad y Privacidad de la información determine que un sistema, que inicialmente era de No Alto Riesgo, ha cruzado el umbral para ser considerado de **Alto Riesgo**.

10.2. Monitoreo Continuo del Despliegue de Sistemas de IA

El CZFC debe garantizar un proceso **iterativo continuo** de seguimiento del uso de los sistemas de IA durante todo su ciclo de vida. Este monitoreo incluye:

1. **Monitoreo del Rendimiento:** El rendimiento y la precisión del sistema deben ser **supervisados continuamente** para garantizar que no degrade su calidad. El monitoreo tiene como objetivo detectar y resolver **anomalías, problemas de funcionamiento y comportamientos inesperados**.

2. **Trazabilidad y Conservación de Registros (Logs):** Se deben **mantener registros de actividad (*logs*)** del uso del sistema para facilitar la **trazabilidad, auditoría y corrección de errores**. Dichos archivos de registro deben conservarse durante un período de tiempo adecuado para la finalidad prevista, de **al menos seis meses**.

3. **Vigilancia de Riesgos Operacionales:** El Responsable de Seguridad y Privacidad debe realizar auditorías a los sistemas de IA autorizados a efectos de verificar el cumplimiento del Esquema Nacional de Seguridad (ENS), el RGPD, la LOPDGDD y las políticas internas.

4. **Detección de Riesgos de Conformidad:** Se debe vigilar el funcionamiento del sistema de IA para determinar si su uso continuado, incluso como apoyo auxiliar e informativo, está dando lugar a que el sistema **presente un riesgo** en el sentido del Artículo 79, apartado 1, del Reglamento.

10.3. Gestión de Incidentes y Modificaciones

1. **Notificación de Incidentes y Riesgos:** Si se manifestaran motivos para considerar que el uso de un sistema de IA (No Alto Riesgo) puede dar lugar a un riesgo, es necesario **informar sin demora indebida al proveedor o distribuidor y a la autoridad de vigilancia del mercado pertinente, y suspender el uso** de ese sistema. Cualquier comportamiento inesperado, resultado sesgado o fallo de seguridad debe ser **notificado inmediatamente** por parte del usuario al Responsable de Seguridad y Privacidad.

2. **Modificaciones Sustanciales:** Un **cambio sustancial** en un sistema de IA tras su puesta en servicio (es decir, un cambio no previsto o proyectado que afecte el cumplimiento del Reglamento o su finalidad prevista) requerirá que el sistema se someta a un **nuevo procedimiento de evaluación**. El proveedor inicial deberá cooperar con el CZFC, como nuevo proveedor, facilitando la **información necesaria, el acceso técnico u otra asistencia razonablemente prevista** para el cumplimiento de las obligaciones.

Los usuarios que detecten o sospechen de un incidente de seguridad, deberán atenerse al proceso de notificación y gestión del Anexo III del presente manual (ver Anexo III).

ANEXO I. TABLA DE USOS ACEPTABLES Y PROHIBIDOS DE SISTEMAS NO DE ALTO RIESGO DE IA GENERATIVA

La siguiente tabla resume el **Uso Aceptable** (basado en las utilidades de los sistemas de No Alto Riesgo) y el **Uso Prohibido** (basado en el Artículo 5 del RIA).

Los usuarios **solamente podrán utilizar los sistemas (aplicaciones) IA previamente autorizados por la entidad**. En caso de necesidad de incorporar el despliegue de un sistema distinto, este deberá ser previamente autorizado.

Uso Aceptable (Sistemas de NO ALTO RIESGO)	Uso Prohibido (Prácticas Inaceptables)
I. SOPORTE DE GESTIÓN Y DOCUMENTACIÓN	**I. MANIPULACIÓN Y CLASIFICACIÓN DISCRIMINATORIA**
Análisis y Síntesis de Documentos: Utilización de sistemas de IA autorizados para sintetizar documentos legales y normativos (como leyes de aduanas, urbanismo, contratos públicos, ENS) con el fin de generar resúmenes, extraer puntos clave o responder preguntas específicas sobre su contenido.	**Manipulación Conductual Perjudicial:** Emplear técnicas subliminales o deliberadamente engañosas/manipuladoras para alterar sustancialmente el comportamiento de una persona o colectivo, haciendo que tome una decisión que, de otro modo, no habría tomado, y que cause perjuicios considerables (físicos, psíquicos, sociales o económicos).
Generación de Borradores: Creación de borradores de documentos estándar (aduaneros, certificados, formularios) y generación de borradores de actas o resúmenes de reuniones a partir de notas o transcripciones.	**Explotación de Vulnerabilidades:** Explotar vulnerabilidades específicas (derivadas de la edad, discapacidad o situación social/económica) con el objetivo o efecto de alterar sustancialmente el comportamiento y causar perjuicios considerables.
Investigación de Mercado: Analizar grandes volúmenes de datos para identificar tendencias y generar informes sobre oportunidades de negocio, siempre y cuando estos datos no sean personales o sensibles.	**Puntuación Ciudadana (*Social Scoring*):** Evaluar o clasificar a personas físicas basándose en el comportamiento social o características personales que resulten en trato perjudicial o desfavorable injustificado o desproporcionado.

Uso Aceptable (Sistemas de NO ALTO RIESGO)	Uso Prohibido (Prácticas Inaceptables)
Traducción y Edición: Uso de sistemas de IA para facilitar la traducción de contenidos web y comunicaciones o para realizar tareas de apoyo a la edición estándar que no alteren sustancialmente la semántica de los datos de entrada.	**Clasificación Biométrica Sensible:** Clasificar individualmente a personas basándose en datos biométricos para deducir o inferir su **raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual**.
II. COMUNICACIÓN Y ATENCIÓN AL PÚBLICO	**II. USO INTRUSIVO Y VIGILANCIA MASIVA**
Chatbots Informativos: Despliegue de chatbots avanzados en la web corporativa para ofrecer respuestas instantáneas a preguntas frecuentes sobre servicios del CZFC (oferta pública, gestión aduanera, proyectos). (Condicionado a la obligación de informar al usuario de que está interactuando con una IA).	**Reconocimiento de Emociones en Contextos de Desequilibrio de Poder:** Inferir emociones de una persona física en los **lugares de trabajo**.
Generación de Contenido Público (con Divulgación): Generación de noticias, comunicados o descripciones de inmuebles para publicación, con la obligación de **divulgar claramente** que el texto se ha generado o manipulado artificialmente (salvo que se haya sometido a revisión humana o control editorial).	**Bases de Datos de Reconocimiento Facial Ilegal:** Crear o ampliar bases de datos de reconocimiento facial mediante la extracción **no selectiva** de imágenes faciales de internet o de circuitos cerrados de televisión (CCTV).
III. CONDICIONES ESPECÍFICAS OBLIGATORIAS	**III. PREDICCIÓN BASADA EN PERFILES**
Transparencia en la Interacción: Informar a las personas físicas de que están interactuando con un sistema de IA (ej. chatbot).	**Evaluación Predictiva de Riesgos de infracciones penales o administrativas:** Realizar evaluaciones de riesgo para predecir la comisión de un delito o incumplimiento administrativo basándose **únicamente** en la elaboración del perfil o en la

Uso Aceptable (Sistemas de NO ALTO RIESGO)	Uso Prohibido (Prácticas Inaceptables)
	evaluación de los rasgos y características de la personalidad del individuo. Evaluación predictiva de **capacidades y rendimiento** laboral de personas físicas.
Supervisión Humana: Todo resultado o decisión asistida por IA debe ser objeto de **revisión humana y juicio crítico** antes de su uso o publicación, para mitigar riesgos de "alucinaciones" (información falsa) o sesgos.	**Sistemas de IA de Alto Riesgo sin Conformidad:** Utilizar sistemas de IA en contextos de Alto Riesgo (ej. contratación, toma de decisiones que afecten a la promoción laboral, o evaluación de solicitudes de servicios esenciales) sin cumplir con los requisitos obligatorios del Capítulo III (gestión de riesgos, documentación técnica, supervisión humana reforzada).

ANEXO II. TABLA DE BUENAS PRÁCTICAS PARA USUARIOS DE IA GENERATIVA EN EL CZFC

Con carácter previo al despliegue y uso de un sistema de seguridad, el Comité de Seguridad de la información del CZFC deberá proceder a su aprobación, correspondiendo al Responsable del Sistema y/o al Responsable de Seguridad de la información evaluar dicho sistema de conformidad con el RIA y el ENS. Los usuarios deberán abstenerse de utilizar sistemas IA que no hayan sido previamente aprobados.
A continuación, se presenta una tabla con las medidas y precauciones específicas que los usuarios del CZFC deben adoptar en el uso de los sistemas de IA generativa aprobados por la entidad:

I. Supervisión Humana y Calidad de la Información	
Juicio Crítico	La IA debe ser vista como una herramienta que **complementa la experiencia y el juicio humano**, no que los reemplaza.
Verificación Obligatoria	El usuario debe **verificar la exactitud y fiabilidad de los resultados** generados por la IA antes de su uso.
Intervención Humana	Implementar procesos que permitan a los operadores humanos **intervenir, descartar o revertir** las predicciones o decisiones de la IA.
Detección de Errores	Establecer umbrales de calidad para la información inferida e identificar y reportar posibles "**alucinaciones**" (información plausible pero incorrecta) o comportamientos inesperados de la IA.
Revisión de Contenido Crítico	Establecer un **proceso de revisión humana** para cualquier contenido o decisión generada por la IA antes de que sea pública o afecte a los ciudadanos.
II. Gestión de Datos y Privacidad	

Minimización de Datos	**Evitar introducir información personal, corporativa o confidencial de alto valor** directamente en las plataformas de IA generativa.
Anonimización/Seudonimización	**Seudonimizar o anonimizar los datos** antes de introducirlos en las plataformas cuando sea posible, para cumplir con el principio de minimización.
Calidad de Datos de Entrada	Asegurar que cualquier dato de entrada proporcionado sea **relevante y representativo** para la tarea.
III. Transparencia y Conformidad Legal	
Transparencia en la Interacción	Informar a las personas físicas de manera **clara y distinguible** que están interactuando con un sistema de IA (ej., un *chatbot*), a más tardar con la primera interacción.
Etiquetado de Contenido Público	**Divulgar claramente** que el texto se ha generado o manipulado artificialmente si se publica con el fin de **informar al público sobre asuntos de interés público**.
Trazabilidad y Auditoría	Mantener **registros de actividad (logs)** del uso del sistema para facilitar la trazabilidad, auditoría y corrección de errores.
Revisión de Sesgos	Si los sistemas se utilizan para tareas sensibles (ej., clasificación, decisión), implementar mecanismos para **monitorear y mitigar activamente los sesgos algorítmicos**.
IV. Seguridad Operativa y Capacitación	

Gobernanza de Uso	Establecer una **instrucción de seguridad clara** de uso de IA generativa, detallando qué tipo de información puede o no puede introducirse en los modelos.
Alfabetización en IA	Garantizar que el personal tenga un **nivel suficiente de alfabetización en materia de IA** para un despliegue informado, que incluye formación sobre el uso seguro y ético.
Creación de Prompts Seguros	Recibir formación sobre **prácticas de creación de prompts seguros** para mitigar el riesgo de ataques de inyección de comandos.
Controles de Acceso	Implementar **autenticación multifactor (MFA)** para todas las cuentas y limitar los permisos de usuario al principio de **mínimo privilegio**.
Notificación de Riesgos	Cuando el usuario tenga motivos para considerar que el uso del sistema puede dar lugar a un riesgo, debe informar **sin demora indebida** al proveedor o distribuidor y a la autoridad de vigilancia del mercado pertinente, y **suspender el uso**

ANEXO III. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INCIDENTES

I. Detección y Acción Inmediata (Usuario/Personal)

Evento	Tarea Clave (Acción Inmediata)	Resultado
Detección de Incidente/Riesgo	Identificación de: **Comportamiento inesperado, resultado sesgado, fallo de seguridad, o riesgo de conformidad**	Detección de una anomalía.
Evaluación del Riesgo	¿Existen motivos para considerar que el uso del sistema puede dar lugar a un riesgo?	Determinación de la existencia de un riesgo.
Suspensión de Uso	**Sí, hay riesgo:** Suspender **sin demora indebida** el uso de ese sistema de IA. **No hay riesgo inmediato:** Continuar con el siguiente paso.	Mitigación del daño potencial.
Notificación Interna Obligatoria	Notificar **de inmediato** (en el plazo más breve posible) el incidente al **Responsable del Sistema** y al **Responsable de Seguridad y Privacidad** del CZFC. La notificación deberá realizarse de forma que deje constancia de la misma; preferiblemente a través de correo electrónico corporativo.	Registro del incidente y activación del protocolo de respuesta.

II. Respuesta y Escalada (Responsable del Sistema y Responsable de Seguridad y Privacidad)

Tarea Clave	Criterio de Decisión	Escalada/Acción
Análisis y Clasificación del Incidente	El Responsable evalúa: 1. Gravedad del impacto (Seguridad/Privacidad/Conformidad). 2. Causa raíz (fallo del modelo, inyección de *prompt*, o mal uso).	Documentación del incidente en el **Registro de Actividad (Logs)**
Riesgo por No Alto Riesgo	¿Es un sistema de **No Alto Riesgo** que está generando un riesgo en el sentido del Artículo 79.1 del Reglamento de IA?	**Sí:** Informar sin demora indebida al **Proveedor** o **Distribuidor** y a la **Autoridad de Vigilancia del Mercado pertinente**.
Modificación Sustancial	¿El incidente revela un **cambio sustancial** en el sistema de IA tras su puesta en servicio?	**Sí:** El sistema se somete a un **nuevo procedimiento de evaluación**, que podría requerir la revisión de la clasificación de riesgo.
Acciones de Mitigación	Implementación de las medidas técnicas y organizativas adecuadas (ej., borrado seguro de datos, actualización de configuraciones, suspensión de cuentas, o re-entrenamiento del modelo).	Cierre del incidente tras verificación y aprobación por el **Responsable de Seguridad de la Información**.

III. Revisión y Aprendizaje (Comité de Seguridad de la Información)

Tarea Clave	Frecuencia	Propósito
Revisión de Incidentes	Periódica o tras incidentes graves.	Actualizar el plan de respuesta a incidentes de ciberseguridad.
Actualización del Manual	Sin demora indebida si un sistema ha cruzado el umbral de Alto Riesgo, o si se producen modificaciones operativas.	Asegurar la vigencia del marco ético y normativo.

ANEXO IV. LISTADO DE SISTEMAS DE ALTO RIESGO (Art. 6 y Anexo III RIA)

Los sistemas de IA se clasifican como de **Alto Riesgo** bajo el RIA en dos grandes bloques:

1. Sistemas de IA como Componentes de Seguridad (Art. 6.1)

Son aquellos sistemas de IA destinados a ser utilizados como **componentes de seguridad** de un producto o el propio producto, siempre que dicho producto esté regulado por alguno de los **actos legislativos de armonización de la Unión Europea** (ej., seguridad de juguetes, equipos a presión, ascensor, y aviación civil).

2. Sistemas de IA en Ámbitos Específicos (Anexo III RIA)

Se consideran de alto riesgo todos los sistemas de IA utilizados en alguno de los siguientes **ocho ámbitos** específicos, debido a su potencial para afectar negativamente a los derechos fundamentales y la seguridad:

I. Identificación Biométrica y Categorización de Personas Físicas

- Sistemas de **identificación biométrica a distancia** (excepto la verificación biométrica uno a uno).
- Sistemas de **categorización biométrica** basados en atributos o características sensibles o protegidas (como la raza, convicciones o vida sexual).
- Sistemas de **reconocimiento de emociones**.

II. Infraestructuras Críticas

- Sistemas de IA destinados a ser utilizados como **componentes de seguridad** en la gestión y explotación de infraestructuras críticas, como la gestión y explotación de infraestructuras digitales críticas, el tráfico rodado, o el suministro de agua, gas, calefacción o electricidad.

III. Educación y Formación Profesional

- Sistemas de IA destinados a la **admisión** de personas en centros de educación o formación.
- Sistemas utilizados para **evaluar el aprendizaje** o el nivel de educación que recibirá una persona.
- Sistemas para la **detección de comportamientos prohibidos** en los exámenes.

IV. Empleo, Gestión de Trabajadores y Acceso al Autoempleo

- Sistemas utilizados para decidir la **contratación** o el proceso de selección, o para **filtrar y evaluar candidatos**.
- Sistemas que deciden las **condiciones de trabajo**, la asignación de tareas, la **evaluación del rendimiento**, ascensos o despidos.

V. Acceso a Servicios Esenciales

- Sistemas de IA utilizados para **evaluar la solvencia crediticia** o establecer puntuaciones de crédito.
- Sistemas utilizados para **evaluar riesgos y fijar precios** en seguros de vida y salud.
- Sistemas para la **priorización de servicios** de envío o despacho de llamadas de emergencia.

VI. Garantías de Cumplimiento del Derecho (Aplicación de la Ley)

- Sistemas de IA utilizados para **evaluar pruebas** en procesos penales o administrativos.
- Sistemas que evalúan el **riesgo de ser víctima** o de cometer un delito.
- Sistemas de **elaboración de perfiles** de personas en el marco de la aplicación de la ley.

VII. Migración, Asilo y Gestión del Control Fronterizo

- Sistemas de IA destinados a ayudar a las autoridades para **evaluar riesgos para la seguridad o la salud** en la gestión fronteriza.
- Sistemas utilizados para **examinar solicitudes** de asilo, visados y residencia.

VIII. Administración de Justicia y Procesos Democráticos

- Sistemas de IA destinados a **ayudar a un órgano judicial** a investigar o a interpretar hechos o la Ley.
- Sistemas destinados a **influir en el resultado de una elección** o referéndum, o en el comportamiento electoral de los votantes (salvo que sea para organizar la logística de campañas).

ANEXO V. EJEMPLO DE SUPUESTOS DE USO DE IA (MINI CASOS)

1. Gobernanza de Datos y Prohibición de Datos Sensibles

Escenario	Uso del Sistema IA	Clasificación y Requisito Aplicable	Decisión y Fundamento
Caso 1.1: Borrador de Contrato Confidencial	Un técnico desea que el Sist.IA revise y simplifique el texto de un **borrador de contrato** de adjudicación en curso con una empresa. El borrador contiene **datos fiscales y cláusulas de confidencialidad** que no son públicas.	**Regla Esencial de Uso**: Prohibición de utilización de Datos Sensibles.	**USO PROHIBIDO**. Se considera una **fuga de datos/exposición de información sensible**. Solo se permitiría usar una **versión Corporativa (Enterprise)** y si el texto sensible no necesario se ha **anonimizado/seudonimizado previamente**. (versión pública del documento);
Caso 1.2: Resumen de Normativa Pública	Un empleado introduce el texto de un artículo completo de la **Ley de Aduanas (BOE)** en una herramienta de IA Generativa de uso general (versión gratuita) para generar un resumen y responder a 3 preguntas frecuentes.	**Información Pública General** Uso Aceptable de Sistemas No de Alto Riesgo.	**USO PERMITIDO**. El resultado debe ser **verificado por el usuario** (Supervisión Humana) antes de cualquier uso oficial, ya que existe riesgo de **"alucinaciones"**.

2. Transparencia y Supervisión Humana (Human-in-the-Loop)

Escenario	Uso del Sistema IA	Clasificación y Requisito Aplicable	Decisión y Fundamento
Caso 2.1: Comunicación Pública	El Gabinete de Comunicación utiliza Copilot (versión corporativa) para generar el **borrador de un comunicado de prensa** sobre los resultados económicos anuales del CZFC. El texto se publicará en la web institucional.	**Obligación de Transparencia** en Contenidos Sintéticos y en Asuntos de Interés Público	USO PERMITIDO PERO CONDICIONADO. El contenido debe ser sometido a un **proceso de revisión humana y control editorial obligatorio** por una persona física, que asumirá la responsabilidad. Si no se revisa o se publica directamente, debe llevar la etiqueta: **"Contenido sintético elaborado por IA"**.
Caso 2.2: Respuesta a Consulta Ciudadana	Un chatbot impulsado por IA responde a la pregunta de un ciudadano sobre el procedimiento para el arrendamiento o adquisición de una parcela en la Zona Franca.	**Transparencia en la Interacción** con Personas Físicas	USO PERMITIDO PERO CONDICIONADO. El sistema debe **identificarse claramente** como un agente artificial usando una etiqueta del tipo: **"Le informamos que está interactuando con un sistema de Inteligencia Artificial (IA)."**

3. Clasificación de Riesgos y Prácticas Prohibidas

Escenario	Uso del Sistema IA	Clasificación y Requisito Aplicable	Decisión y Fundamento
Caso 3.1: Evaluación de Solicitudes de Empleo	El departamento de RR.HH. desea utilizar un sistema de IA para **filtrar currículums** y puntuar a los candidatos para un puesto, basándose en la experiencia y formación.	**Sistema de Alto Riesgo** (Anexo III, IV. Empleo).	**USO DE ALTO RIESGO**. La aplicación de este sistema requiere un **procedimiento de autorización y verificación riguroso**: **EIPD obligatoria**, **Análisis de Riesgos**, y cumplimiento de los requisitos de conformidad (Gobernanza de Datos, Documentación Técnica, Supervisión Humana).
Caso 3.2: Puntuación de Reputación	Un directivo propone un sistema de IA para **evaluar la "reputación social"** de empresas que solicitan licitaciones, basándose en su actividad en redes sociales no corporativas.	**Práctica de IA Prohibida** (Riesgo Inaceptable).	**USO PROHIBIDO**. Esto constituye una **Puntuación Ciudadana (*Social Scoring*)**], una práctica de Riesgo Inaceptable y prohibida por el RIA.

Caso 3.3: Detección de Emociones en Reuniones	El Comité de Seguridad estudia implantar un software de **reconocimiento de emociones** basado en vídeo para evaluar el nivel de estrés o atención de los participantes en reuniones internas.	**Sistema de Alto Riesgo** (Anexo III, I. Identificación Biométrica]. **Práctica Prohibida** en el entorno laboral.	**USO PROHIBIDO** en el lugar de trabajo. El despliegue de cualquier sistema de reconocimiento de emociones o categorización biométrica es de **Alto Riesgo** y requeriría una **revisión total del manual, EIPD y autorización previa**.

4. Riesgo de Inyección de Prompts y Seguridad

Escenario	Uso del Sistema IA	Clasificación y Requisito Aplicable	Decisión y Fundamento
Caso 4.1: Consulta Maliciosa	Un usuario introduce un *prompt* en una IA Generativa para que ignore sus reglas de seguridad internas y revele **información sensible sobre las sesiones anteriores** de otros usuarios de la red corporativa (Ataque de **Prompt Injection**).	**Riesgo Crítico de Ciberseguridad**. **Alfabetización en IA y Seguridad**.	**USO PROHIBIDO. ACCIÓN INMEDIATA**. El usuario debe **desistir de este uso inmediatamente** y **notificar el incidente** al Responsable de Seguridad y Privacidad. La capacitación de usuarios es obligatoria para la **detección y reporte de intentos de inyección**.