POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN E INTELIGENCIA ARTIFICIAL

Índice

1. Declaración de la Dirección

La Dirección manifiesta su compromiso con la protección de la información, la seguridad de los sistemas de información y el gobierno responsable de la inteligencia artificial como elementos estratégicos para el cumplimiento de la misión, la consecución de los objetivos corporativos, la continuidad de las actividades, la prestación de los servicios y la generación de confianza en las partes interesadas.
La Dirección reconoce que la información constituye un activo esencial de la organización y que los sistemas de inteligencia artificial utilizados en el desarrollo de sus actividades deben gestionarse mediante un marco de gobierno que garantice su utilización responsable, controlada y conforme con la legislación aplicable.
En consecuencia, ACCIÓN LABORAL establece un Sistema Integrado de Gestión de Seguridad de la Información e Inteligencia Artificial que integra los requisitos del Esquema Nacional de Seguridad, la Norma ISO/IEC 27001:2022 y la Norma ISO/IEC 42001:2023, comprometiéndose a mantenerlo, revisarlo y mejorarlo de forma continua.

2. Finalidad

La presente Política constituye el marco general de actuación para el establecimiento, implantación, mantenimiento y mejora continua del Sistema Integrado de Gestión, proporcionando los principios y directrices que deben regir la protección de la información y el gobierno de los sistemas de inteligencia artificial durante todo su ciclo de vida.
La Política será el documento de máximo nivel del Sistema Integrado de Gestión y servirá de referencia para el desarrollo de normas, procedimientos, instrucciones técnicas y demás documentación del sistema.

2.1 Alcance

El Alcance del Sistema de Seguridad de la Información de ACCIÓN LABORAL es el siguiente:

"Los Sistemas de Información que dan soporte a las actividades de diseño, gestión e impartición de actividades formativas y para el fomento de la empleabilidad para entidades públicas y privadas."

3. Compromisos de la Dirección

La Dirección asume el compromiso de:
a) Liderar y apoyar activamente el Sistema Integrado de Gestión de Seguridad de la Información e Inteligencia Artificial.
b) Integrar la seguridad de la información y el gobierno de la inteligencia artificial en la estrategia, los procesos y la toma de decisiones de la organización.
c) Establecer objetivos medibles, coherentes con esta Política y alineados con la estrategia corporativa.
d) Proporcionar los recursos humanos, técnicos, tecnológicos, económicos y organizativos necesarios para el funcionamiento eficaz del Sistema Integrado de Gestión.
e) Garantizar la asignación de funciones, responsabilidades y autoridades para la gestión de la seguridad de la información y de la inteligencia artificial.
f) Promover una cultura organizativa basada en la seguridad, la gestión responsable de la inteligencia artificial, la ética profesional y la mejora continua.
g) Impulsar la formación, sensibilización y competencia del personal en materia de seguridad de la información y gobierno de la inteligencia artificial.

h) Asegurar la integración de la gestión de riesgos en los procesos de negocio.
i) Revisar periódicamente la eficacia del Sistema Integrado mediante la Revisión por la Dirección.
j) Garantizar la mejora continua del desempeño del Sistema Integrado.

4. Principios de actuación

La organización desarrollará sus actividades conforme a los siguientes principios generales.

4.1 Protección de la información

La organización protegerá la información durante todo su ciclo de vida mediante la implantación de medidas organizativas, físicas y técnicas apropiadas que permitan preservar los siguientes principios:
La política de seguridad de la información de **ACCIÓN LABORAL** se desarrolla de acuerdo con los siguientes principios:

- **Principio de confidencialidad**: se deberá garantizar que la información sea accesible únicamente para aquellas personas expresamente autorizadas para ello.
- **Principio de integridad**: se deberá asegurar que la información con la que se trabaja sea completa y precisa, y se incidirá en la exactitud tanto de su contenido como de los procesos involucrados.
- **Principio de disponibilidad**: se garantizará la prestación continua de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada.
- **Principio de gestión del riesgo:** Se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre las medidas de seguridad y la naturaleza de la información.
- **Principio de mejora continua**: se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados para aumentar la capacidad de adaptación a la constante evolución del entorno.
- **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.
- **Principio de cumplimiento normativo**: todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquella relacionada con la intimidad y la protección de datos de carácter personal y con la seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.
- **Principio de prevención**: Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben: autorizar los sistemas antes de entrar en operación; evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria; solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

- **Principio de detección**: Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.
- **Principio de respuesta**: Los departamentos deben: establecer mecanismos para responder eficazmente a los incidentes de seguridad; designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos; establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- **Principio de recuperación**: Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

La protección será proporcional al valor de la información, a los riesgos existentes y a los requisitos legales, contractuales y organizativos aplicables.

4.2 Seguridad como proceso integral

La seguridad será considerada un proceso permanente integrado en todas las actividades de la organización, aplicándose desde el diseño, desarrollo, adquisición, explotación, mantenimiento y retirada de los sistemas de información y de los sistemas de inteligencia artificial.
La seguridad no se entenderá como un conjunto de actuaciones aisladas, sino como un elemento inherente a la gestión corporativa.

4.3 Gestión basada en riesgos

Las decisiones relativas a la seguridad de la información y a la inteligencia artificial estarán basadas en la identificación, análisis, evaluación y tratamiento de los riesgos.
La organización mantendrá procesos sistemáticos de gestión de riesgos que permitan determinar las medidas necesarias para mantener dichos riesgos dentro de los niveles aceptados por la Dirección.
La evaluación de riesgos será revisada periódicamente y siempre que se produzcan cambios relevantes en el contexto de la organización, en los servicios, en los sistemas de información o en los sistemas de inteligencia artificial.

4.4 Cumplimiento normativo

La organización desarrollará sus actividades asegurando el cumplimiento de la legislación aplicable, de los requisitos reglamentarios, contractuales y organizativos, así como de las obligaciones derivadas del Esquema Nacional de Seguridad y de las normas internacionales adoptadas por el Sistema Integrado.

4.5 Gobierno de la inteligencia artificial

La organización gestionará los sistemas de inteligencia artificial mediante un marco de gobierno que permita asegurar que su utilización se desarrolla conforme a los objetivos de la organización, los requisitos legales y los principios establecidos en esta Política.
Los sistemas de inteligencia artificial serán objeto de supervisión durante todo su ciclo de vida, considerando, entre otros aspectos:

- los riesgos asociados a su utilización;
- su finalidad prevista;
- el contexto de uso;
- las responsabilidades asociadas a su gestión;
- la necesidad de seguimiento y revisión periódica.

4.6 Supervisión humana

La organización garantizará que los procesos de negocio que incorporen sistemas de inteligencia artificial dispongan de mecanismos de supervisión adecuados cuando resulten necesarios de acuerdo con la naturaleza del sistema, el contexto de utilización y los riesgos identificados.
La utilización de sistemas de inteligencia artificial no eximirá de las responsabilidades asignadas a los responsables de los procesos ni sustituirá las funciones de gobierno establecidas por la organización.

4.7 Transparencia organizativa

La organización promoverá que la utilización de sistemas de inteligencia artificial se gestione de forma documentada y controlada, manteniendo la información necesaria para facilitar su gestión, supervisión, auditoría y revisión.

4.8 Gestión del ciclo de vida

La seguridad y el gobierno de la inteligencia artificial serán considerados durante todas las fases del ciclo de vida de los sistemas, incluyendo su planificación, diseño, adquisición, desarrollo, implantación, explotación, mantenimiento, modificación y retirada.

4.9 Gestión de proveedores

Los productos y servicios suministrados por terceros que puedan afectar a la seguridad de la información o incorporar capacidades de inteligencia artificial serán evaluados conforme a los procedimientos establecidos por la organización, considerando los riesgos derivados de su utilización y las obligaciones contractuales correspondientes.

4.10 Mejora continua

La organización mantendrá un proceso permanente de seguimiento, medición, evaluación y mejora del Sistema Integrado de Gestión con objeto de incrementar su eficacia, adecuación y capacidad de adaptación a la evolución tecnológica, organizativa y normativa.

5. Objetivos generales

La presente Política proporciona el marco para el establecimiento de objetivos del Sistema Integrado orientados, entre otros, a:

- proteger la información y los activos asociados;
- garantizar la continuidad de las actividades y de los servicios;
- gestionar los riesgos de seguridad de la información y de inteligencia artificial;
- fortalecer la resiliencia de la organización frente a amenazas e incidentes;
- asegurar el uso controlado y gobernado de la inteligencia artificial;
- mejorar continuamente la eficacia del Sistema Integrado;
- incrementar el nivel de confianza de clientes, administraciones públicas, proveedores y demás partes interesadas.

Los objetivos específicos serán establecidos, revisados y evaluados periódicamente por la Dirección.

6. Comunicación y cumplimiento

La presente Política será comunicada a todo el personal, permanecerá disponible para las partes interesadas cuando resulte procedente y será revisada periódicamente para garantizar su adecuación al contexto de la organización y a la evolución de los requisitos legales, reglamentarios y normativos.

Todo el personal, así como aquellas personas y organizaciones que actúen en nombre de la organización cuando resulte aplicable, deberán conocer y cumplir las disposiciones contenidas en esta Política y en la documentación que la desarrolla.

La Dirección será responsable de su aprobación y el Comité de Seguridad de la Información e Inteligencia Artificial supervisará su implantación, mantenimiento, revisión y mejora continua.

7. Marco normativo

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Real Decreto ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones.
- Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

8. Vigilancia continua y reevaluación periódica

ACCIÓN LABORAL llevará a cabo una vigilancia continua que permita la detección de actividades o comportamientos anómalos y su oportuna respuesta.
La evaluación permanente del estado de la seguridad de los activos permite a ACCIÓN LABORAL medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.
ACCIÓN LABORAL reevaluará y actualizará periódicamente las medidas de seguridad, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

9. Roles y Responsabilidades

ACCIÓN LABORAL tendrá en cuenta la diferenciación de responsabilidades en su sistema de información siempre que sea posible. El detalle de las atribuciones de cada responsable, los mecanismos de coordinación y la resolución de conflictos se detallarán a lo largo de la presente política de seguridad.

9.1 Organización de la seguridad.

La implantación de la Política de Seguridad en **ACCIÓN LABORAL** requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información
b) Responsables del Servicio
c) Responsables de la Información
d) Responsable de Seguridad de la Información
e) Responsable de Sistemas

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

9.2 Comité de seguridad de la información e IA.

La seguridad de la Información es una responsabilidad organizativa que es compartida con la Dirección. En consecuencia, la Dirección de **ACCIÓN LABORAL** promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vida definida y el palpable apoyo a las iniciativas de seguridad.
Dicho Comité está compuesto por las figuras anteriormente mencionadas.
Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
  - Principales incidencias en la Seguridad de la Información
  - Elaboración y actualización de planes de continuidad
  - Cumplimiento y difusión de las Políticas de Seguridad

Mediante acta se designan las siguientes responsabilidades:

- **Responsable del Servicio**
- **Responsable de la Información**
- **Responsable de Seguridad**
- **Responsable del Sistema**

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.
El Responsable de Seguridad de la Información será nombrado por la Dirección a propuesta del Comité de Seguridad.

10. Revisión de la política de seguridad de la información.

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

11. Datos de carácter personal.

ACCIÓN LABORAL trata datos de carácter personal.

Todos los sistemas de información de **ACCIÓN LABORAL** se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado 5. Marco Normativo, de la presente Política de Seguridad de la Información.

12. Gestión de riesgos

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

13. Calificación de la información

Para calificar la información **ACCIÓN LABORAL** atenderá a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.

Tanto el responsable de cada información manejada por el sistema como los criterios de calificación de la información, que determinarán el nivel de seguridad requerido, se establecen en el procedimiento **Calificación y Etiquetado de la Información**

14. Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de **ACCIÓN LABORAL** son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de **ACCIÓN LABORAL** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de **ACCIÓN LABORAL** recibirán formación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **ACCIÓN LABORAL,** en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

15. Incumplimiento

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

16. Documentación relacionada

Asignación de Roles y Responsabilidades para la Seguridad de la Información.

- Acta del Comité de Seguridad con los nombramientos asociados a cada uno de los Roles relativos a Seguridad de la Información.
- Instrucciones Técnicas CCN-STIC-Serie 800, emitidas por el CCN.
- RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

22 de junio de 2026

La Dirección