Organiza

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Foro GRC
Privacidad · IA · Ciberseguridad

Insight Foro GRC

Gobierno de la IA : Cómo implementar el modelo de gobernanza. Cómo hacerlo realidad en la organización

Mesa dialogo: Autenticación Multifactor (MFA) como medida estratégica de seguridad

Taller práctico para Socios: Cuando la IA falla, cómo gestionar un incidente siguiendo el RIA

Partners Estratégicos

Telefónica

GOVERTIS
Part of Telefónica Tech

CANAL AEC

"Gobierno de la IA: cómo implementar el modelo de gobernanza. Cómo hacerlo realidad en la organización"

Laura Vico Gabarda

Consultora senior GRC, Govertis part of Telefónica Tech

https://es.linkedin.com/in/laura-vico

Organiza: AEC Asociación Española para la Calidad

Partners Estratégicos: Govertis, Telefónica

Contexto actual

La inteligencia artificial **ya está en la organización**

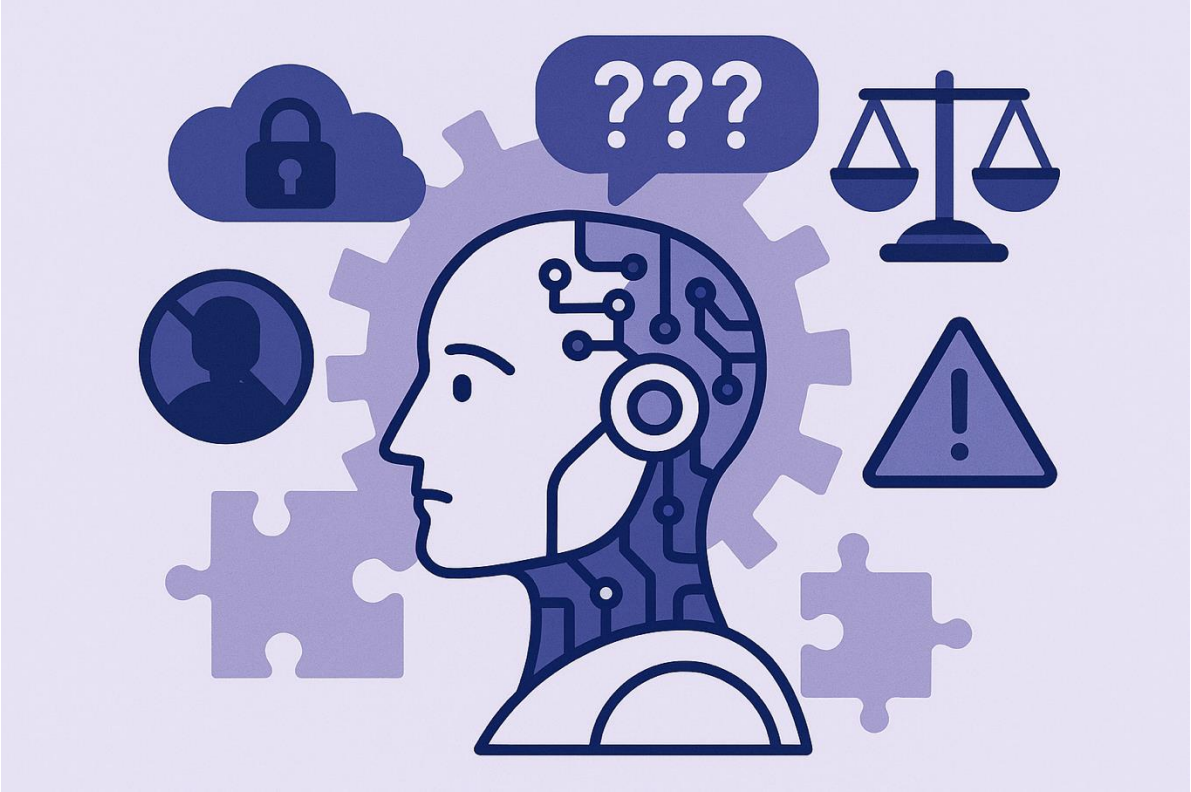
Uso creciente la de IA
El personal “se trae la IA de casa”
Riesgos asociados a la **pérdida de control sobre la información**, posibles fugas de datos.

Riesgo de **uso no controlado**.
La organización todavía no ha definido su regulación interna (p.ej. Política de IA).

Riesgos asociados a **incumplimiento de obligaciones legales** (Reglamento de Inteligencia Artificial, Reglamento General de Protección de Datos, etc)

Problemas frecuentes

- Casos de uso de la IA dispersos
- Responsabilidades difusas
- Controles reactivos, no preventivos
- Transferencias internacionales no controladas
- Shadow IA
- …



Régimen jurídico

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (**Reglamento de Inteligencia Artificial**).

Proyecto de Ley Orgánica para el buen uso y la gobernanza de la IA

Legislaciones autonómicas: por ejemplo, la *LEY 2/2025, de 2 de abril, para el desarrollo e impulso de la inteligencia artificial en Galicia.*

Calendario de aplicación tras AI Omnibus

Actualizado con acuerdo provisional de simplificación · mayo 2026

Calendario de aplicación

Vigente / consolidado

Propuesta / acuerdo provisional

Nota: pendiente de adopción formal por Parlamento y Consejo.

1. Prácticas prohibidas

Mantener el bloque actual, pero añadir **la nueva prohibición de sistemas de IA para nudificación no consentida y creación de material de abuso sexual infantil.**

Estado: en vigor + ampliación prevista dic. 2026

2. Alfabetización en IA

Sin cambio material. Reforzar que ya aplica desde febrero de 2025 y que debe evidenciarse con formación, comunicaciones, registros y contenidos adaptados por perfil.

Estado: en vigor

3. Alto riesgo, GPAI y simplificación

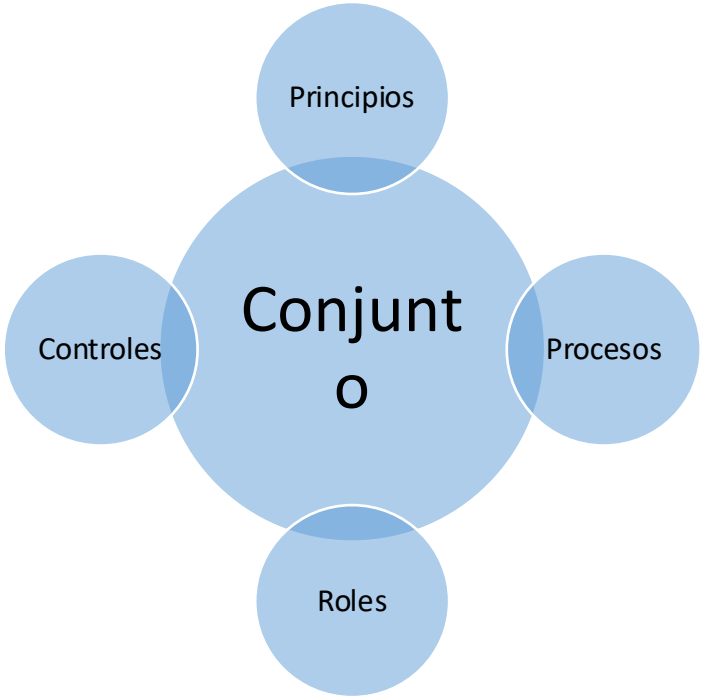
Sustituir el foco exclusivo en GPAI por una lectura de impacto: alto riesgo aplazado, enforcement GPAI más centralizado y menos solapamientos sectoriales.

Estado: fechas críticas 2027/2028

Fuente: Parlamento Europeo, comunicado de prensa “AI Act: deal on simplification measures, ban on nudifier apps”, 07/05/2026. Diseño orientativo: validar tras publicación del texto definitivo.

¿Y ahora, qué hacemos?

¿Qué es el gobierno de la IA?



Ética ✓

Segura ✓

Cumple normativa ✓

Alineada al negocio ✓

ISO 42001 SGIA

- La ISO/IEC 42001 es una norma internacional que establece los requisitos para implantar, mantener y mejorar un sistema de gestión de la inteligencia artificial (SGIA) dentro de una organización.

- Es un estándar de gestión que ayuda a las organizaciones a desarrollar, usar y gobernar sistemas de IA de forma responsable, ética y segura, abordando riesgos como sesgos, falta de transparencia o impactos negativos.

- Enfoque de **sistema de gestión** (similar a ISO 27001 o ISO 9001)
- Aplicable a cualquier organización (empresa, administración pública, etc.)
- Cubre todo el ciclo de vida de la IA (diseño, desarrollo, despliegue y uso)
- Integra aspectos clave:
  - ✓ Gobernanza de IA
  - ✓ Gestión de riesgos
  - ✓ Ética y transparencia
  - ✓ Seguridad y privacidad
  - ✓ Responsabilidad y supervisión humana

RIA ¿Qué cumplir? ISO 42001 ¿Cómo hacerlo?

Cuerpo de la Norma + ANEXO A. CONTROLES

PLAN

- 4. Contexto de la organización
  - 4.1 Comprensión de la organización y su contexto
  - 4.2 Comprensión necesidades y expectativas de las partes interesadas
  - 4.3 Determinación del alcance del SGIA
  - 4.4 SGIA
- 5. Liderazgo
  - 5.1 Liderazgo y compromiso
  - 5.2 Política de IA
  - 5.1 Roles, responsabilidades y autoridades
- 6. Planificación
  - 6.1 Acciones para abordar riesgos y oportunidades
  - 6.2 Objetivos de la IA y planificación para alcanzarlos
  - 6.3 Planificación de cambios
- 7. Apoyo
  - 7.1 Recursos
  - 7.2 Competencia
  - 7.3 Concienciación
  - 7.4 Comunicación
  - 7.5 Información documentada

DO

- 8. Operación
  - 8.1 Planificación y control operativo
  - 8.2 Evaluación de riesgos de la IA
  - 8.3 Tratamiento de riesgos de la IA
  - 8.4 Evaluación del impacto del sistema de IA

CHECK

- 9. Evaluación del desempeño
  - 9.1 Seguimiento, medición, análisis y evaluación
  - 9.2 Auditoría interna
  - 9.3 Revisión por la dirección

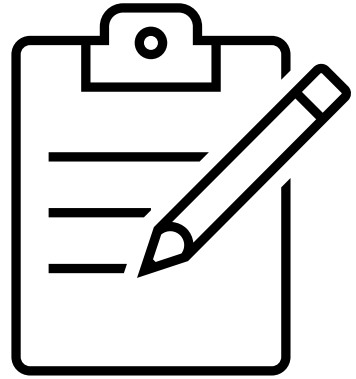
ACT

- 10. Mejora
  - 10.1 Mejora continua
  - 10.2 No conformidades y acciones correctivas

Política de IA

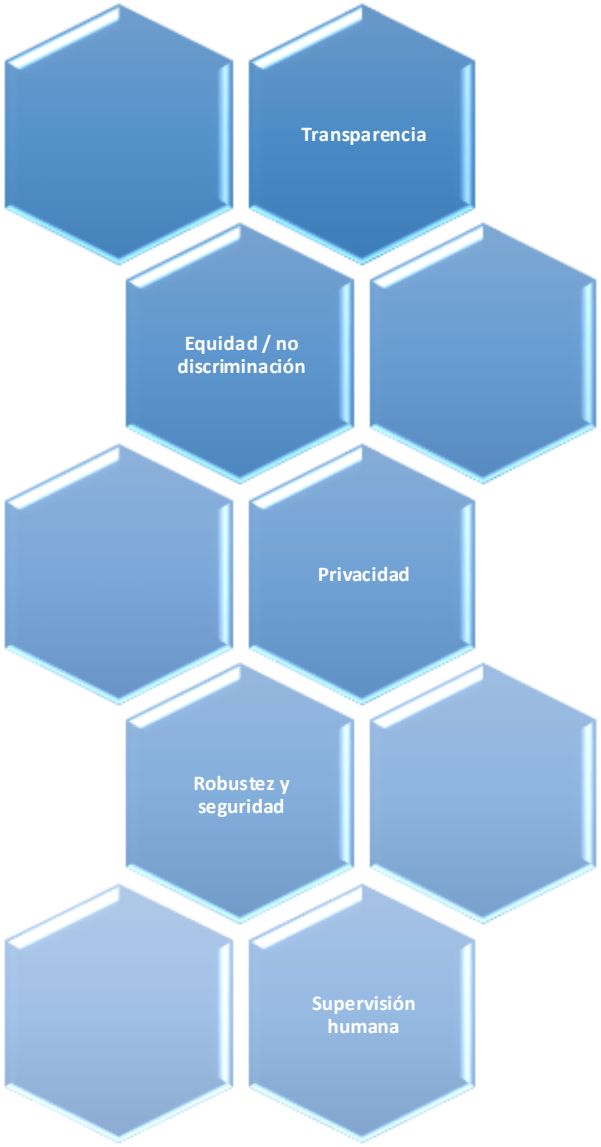
- Es un documento formal aprobado por la alta dirección que establece los **principios, objetivos y compromisos** de la organización respecto al **uso y la gestión de sistemas de IA**.

- Algunos elementos clave:
  - Propósito y alcance
  - Principios de uso responsable
  - Compromiso con la gestión de riesgos
  - Cumplimiento normativo
  - Roles y responsabilidades
  - Mejora continua



Principios de la IA responsable

Deben traducirse en **normativas y procedimientos.**



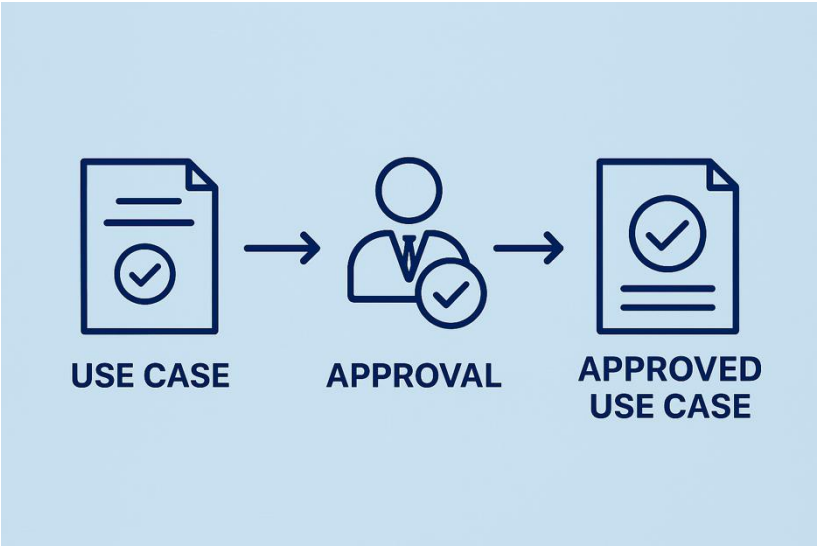
Organización y roles

- Diferenciar el rol que tiene la propia organización frente a cada uso de la IA de los roles que se identifican dentro de la propia organización.
- Proveedor vs Responsable del despliegue.
- Definir ¿quién hace qué?
- Evitar solapamientos y vacíos
- Ejemplos: Comité de IA, AI Officer, CISO, DPO, Negocio (owners de casos de uso)

Modelo operativo

¿Cómo funciona en la práctica?

- Flujo de aprobación de casos de uso
- Evaluación de riesgos
- Decisión: aprobar/condicionar/rechazar
- Seguimiento continuo
- Es aconsejable integrarlo en procesos existentes



Inventario de IA

- Identificación de todos los casos de uso de IA
- Clasificación (tipo, finalidad, impacto)
- Registro centralizado
- Sin inventario → no hay gobierno

Clasificación según los riesgos

ILUSTRACIÓN 4: CLASIFICACIÓN DE SISTEMAS DE IA SEGÚN EL RIESGO

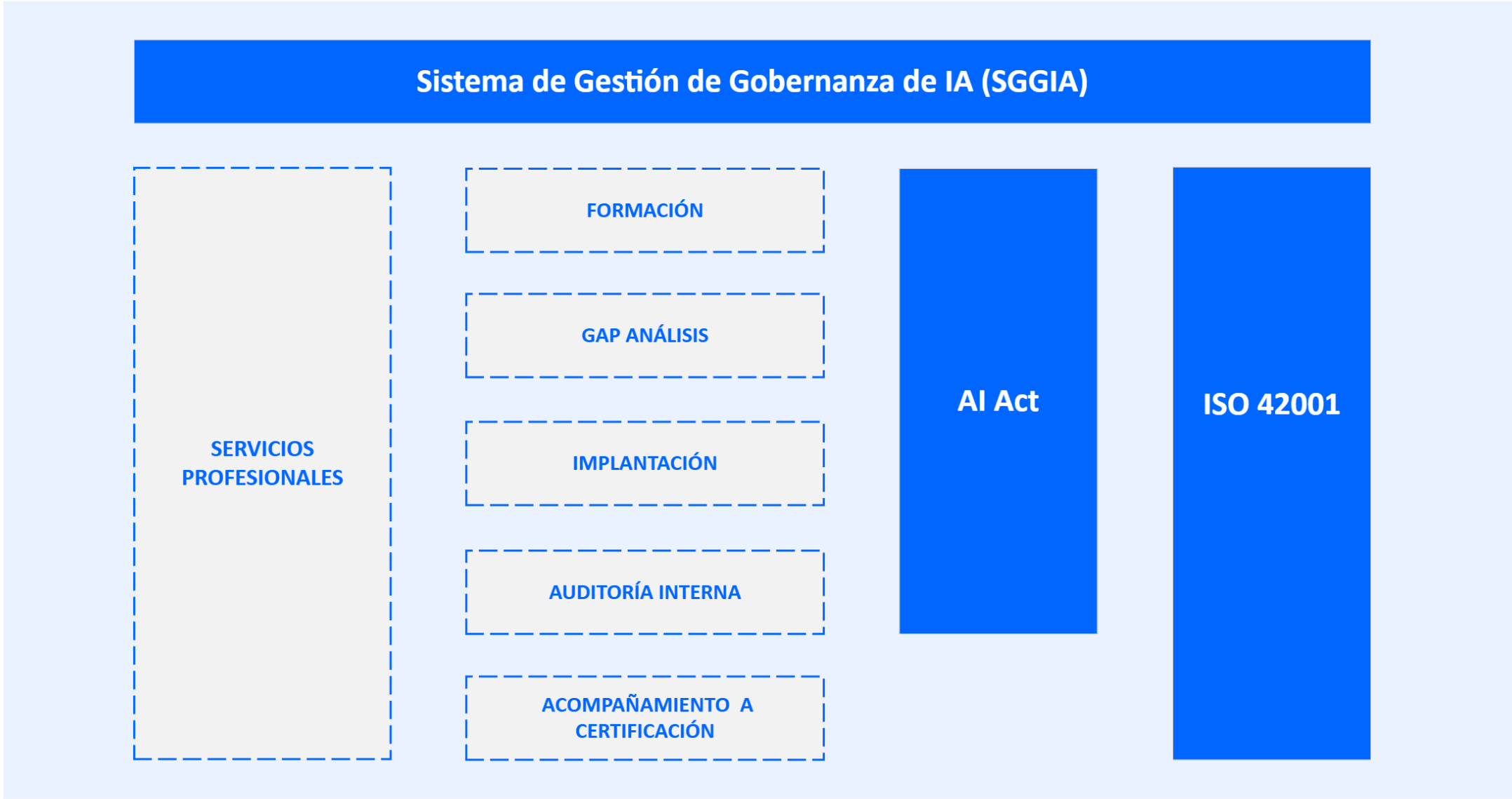
Fuente: Guía introductoria al reglamento de IA (AESIA)

- **Sistemas prohibidos.** Por ejemplo: Un sistema de IA que se aprovecha de las vulnerabilidades de las personas mayores para defraudarles o influir en sus decisiones, lo que puede empeorar su salud mental y causarles graves daños psicológicos.
- **Sistemas de alto riesgo.** Por ejemplo: Sistema de IA que analiza en tiempo real las actividades del alumnado durante un examen con el objetivo de saber si están copiando.
- **Sistemas con obligaciones de transparencia.** Por ejemplo: chatbots.
- **Resto de sistemas de IA:** Por ejemplo: aplicación de la IA a los videojuegos.
- **Sistemas NO considerados de IA:** determinados algoritmos más clásicos, como los basados en reglas o heurísticas, no son considerados sistemas de IA en el marco del Reglamento, y por tanto no les aplica.

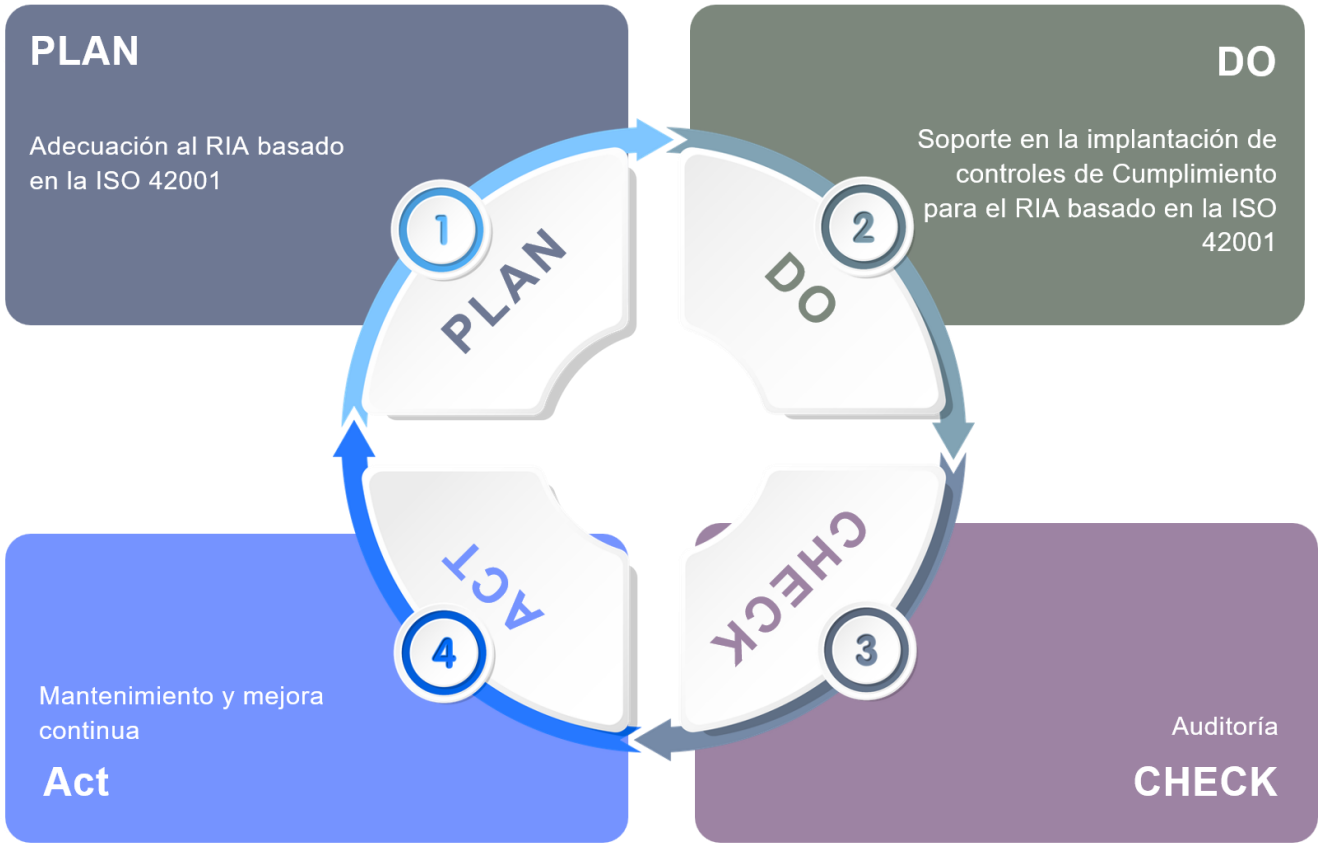
Alfabetización

Considerando 20 RIA

"Con el fin de obtener los mayores beneficios de los sistemas de IA, protegiendo al mismo tiempo los derechos fundamentales, la salud y la seguridad, y de posibilitar el control democrático, ***la alfabetización en materia de IA*** *debe dotar a los proveedores, responsables del despliegue y personas afectadas de los* ***conceptos necesarios para tomar decisiones con conocimiento de causa en relación con los sistemas de IA.*** *Esos conceptos pueden variar en función del contexto pertinente e incluir el entendimiento de la correcta aplicación de los elementos técnicos durante la fase de desarrollo del sistema de IA, las medidas que deben aplicarse durante su uso, las formas adecuadas de interpretar los resultados de salida del sistema de IA y, en el caso de 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. En el contexto de la aplicación del presente Reglamento, la alfabetización en materia de IA debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución"*



Roadmap de implantación



Beneficios

Visibilidad y control sobre el uso actual y futuro de la Inteligencia Artificial en la organización.

Mayor trazabilidad, supervisión y capacidad de auditoría sobre sistemas y decisiones basadas en IA.

Alineamiento con el Reglamento Europeo de IA (RIA) y otros marcos regulatorios aplicables.

Integración del gobierno de IA con modelos ya existentes de seguridad, privacidad, compliance y gestión de riesgos.

Reducción de riesgos regulatorios, operativos, éticos y reputacionales asociados al uso de IA.

Mejora del control y evaluación de proveedores y terceros involucrados en soluciones de IA.

Definición de procesos claros para evaluar, adoptar y supervisar nuevos proyectos de IA.

Refuerzo de la confianza de organizaciones, empleados, dirección y organismos supervisores.

Preparación de la organización para evolucionar hacia un **modelo certificable** basado en ISO/IEC 42001.

Gobierno de la IA: cómo implementar el modelo de gobernanza.

Cómo hacerlo realidad en la organización.

Raúl Avedillo

Gerente Digital Compliance & DPO, Telefónica, S.A.

https://www.linkedin.com/in/raveloz

Organiza: AEC Asociación Española para la Calidad

Partners Estratégicos: GOVERTIS, Telefónica, Part of Telefónica Tech

Cómo hacerlo realidad en la organización.

¿Y ahora, qué hacemos?

¿Y ahora, qué hacemos?

CLIENTES

RED Y TECNOLOGÍA

EMPLEADOS

OPTIMIZACIÓN DE PROCESOS

APLICACIÓN EN TODAS LAS ÁREAS DE LA COMPAÑÍA

Telefónica

Organiza:

AEC

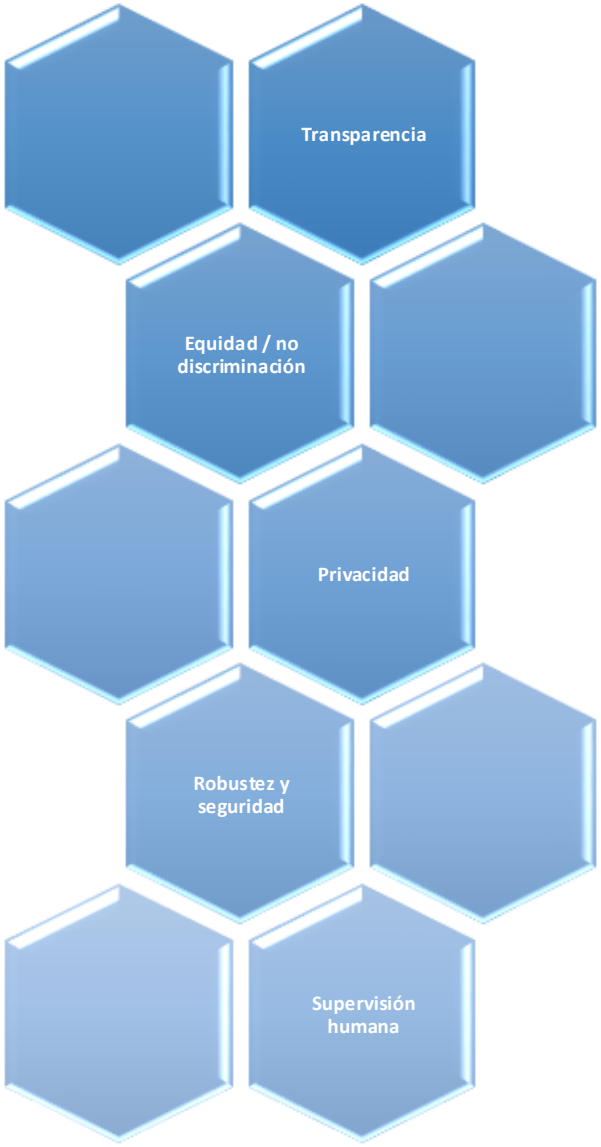
Partners Estratégicos:

GOVERTIS

Telefónica

Principios de la IA responsable

Deben traducirse en **normativas y procedimientos.**



Principios de la IA responsable

Telefónica

Principios de IA de Telefónica

Aprobado por el Comité Ejecutivo

TELEFÓNICA, S.A.

Octubre 2018

El **big data** y la **inteligencia artificial (IA)** nos permiten transformar los negocios, la vida de las personas y la sociedad. Con estos avances queremos **mejorar como Compañia** al mismo tiempo que hacemos del mundo un lugar mejor para todos. Para ello, nos comprometemos a diseñar, desarrollar y usar una IA.

Justa

Nos aseguramos de que las aplicaciones **no conducen a resultados con sesgos e impactos discriminatorios e injustos.**

Garantizamos que **no hay elementos discriminatorios** cuando la IA aprende y los algoritmos deciden o recomiendan.

Transparente y explicable

Damos a conocer a los usuarios **los datos que usamos y su próposito.**

Tomamos las medidas suficientes para garantizar la comprensión de sus decisiones o recomendaciones.

Requerimos a nuestros proveedores que tengan o adopten nuestros principios de IA o similares suyos.

Con las personas como prioridad

Nos aseguramos de que la **IA respeta siempre los Derechos Humanos.**

Estamos **comprometidos con los Objetivos de Desarrollo Sostenible de la ONU.**

Contribuimos a **evitar usos inadecuados** de la tecnología.

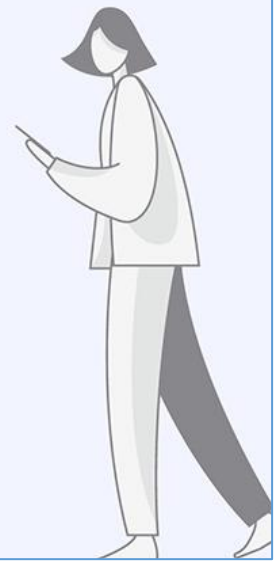
Con privacidad y seguridad desde el diseño

Al construir sistemas de Inteligencia Artificial **cuidamos especialmente la seguridad de la información.**

Respetamos el derecho a la privacidad de las personas y sus datos.

Con socios y terceras partes

Confirmamos la veracidad de la lógica y los datos utilizados por los proveedores.



Organiza: QAEC Asociación Española para la Calidad

Partners Estratégicos: GOVERTIS, Telefónica

Principios de la IA responsable

ACTUALIZACIÓN EN 2024

Telefónica

Principios de inteligencia artificial de Telefónica

Centrada en las personas

Queremos que la IA contribuya a hacer nuestro mundo más humano, velando porque la IA respete y promueva los Derechos Humanos.

Nos comprometemos a trabajar para preservar la integridad personal, proteger a los grupos vulnerables y evitar los posibles impactos negativos de la IA.

Creemos que la supervisión humana es crucial para preservar la dignidad humana, la autonomía y la libertad de decisión.

Transparente y explicable

Tratamos de entender la lógica detrás de los resultados de los modelos para incrementar la confianza del usuario y nos esforzamos por mantener un equilibrio justo entre rendimiento y explicabilidad.

Nos aseguramos de que las personas sean conscientes de que están interactuando con la IA.

Justa e inclusiva

Promovemos la precisión de los resultados de nuestros sistemas de IA para tomar decisiones justas y confiables.

Queremos garantizar que nuestra IA sea representativa y accesible, inclusiva y equitativa.

Trabajamos para que las aplicaciones no produzcan sesgos e impactos discriminatorios.

Respetuosa de la privacidad y seguridad

Nos comprometemos a respetar el derecho a la protección de datos y a la privacidad. Además, utilizamos un enfoque de privacidad desde el diseño.

Siguiendo nuestro enfoque de seguridad desde el diseño, trabajamos para asegurar sistemas de IA sólidos y robustos. También creemos que la trazabilidad es esencial para garantizar la ciberseguridad de nuestros sistemas de IA.

Comprometida con el medio ambiente

Promovemos la IA como herramienta diferencial para preservar el medio ambiente, impulsar la sostenibilidad, fomentar la economía circular y paliar la crisis climática.

Trabajamos para evaluar y minimizar el impacto medioambiental, para reducir su huella de carbono y optimizar la eficiencia energética de los sistemas IA.

Con responsabilidad y rendición de cuentas en toda la cadena de valor

Creemos firmemente que la responsabilidad y rendición de cuentas son insustituibles por la IA.

Trabajamos para asegurar la trazabilidad de las decisiones a lo largo de toda la cadena de valor, también cuando trabajamos con socios o terceros.

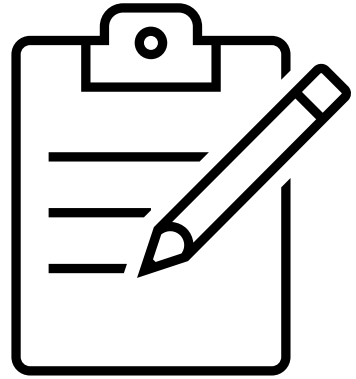
Disponemos de un modelo de gobierno de IA que define roles y responsabilidades, y que permite identificar y mitigar los riesgos, así como asegurar la auditabilidad de los sistemas.

https://www.telefonica.com/es/wp-content/uploads/sites/4/2024/07/principios-inteligencia-artificial.pdf

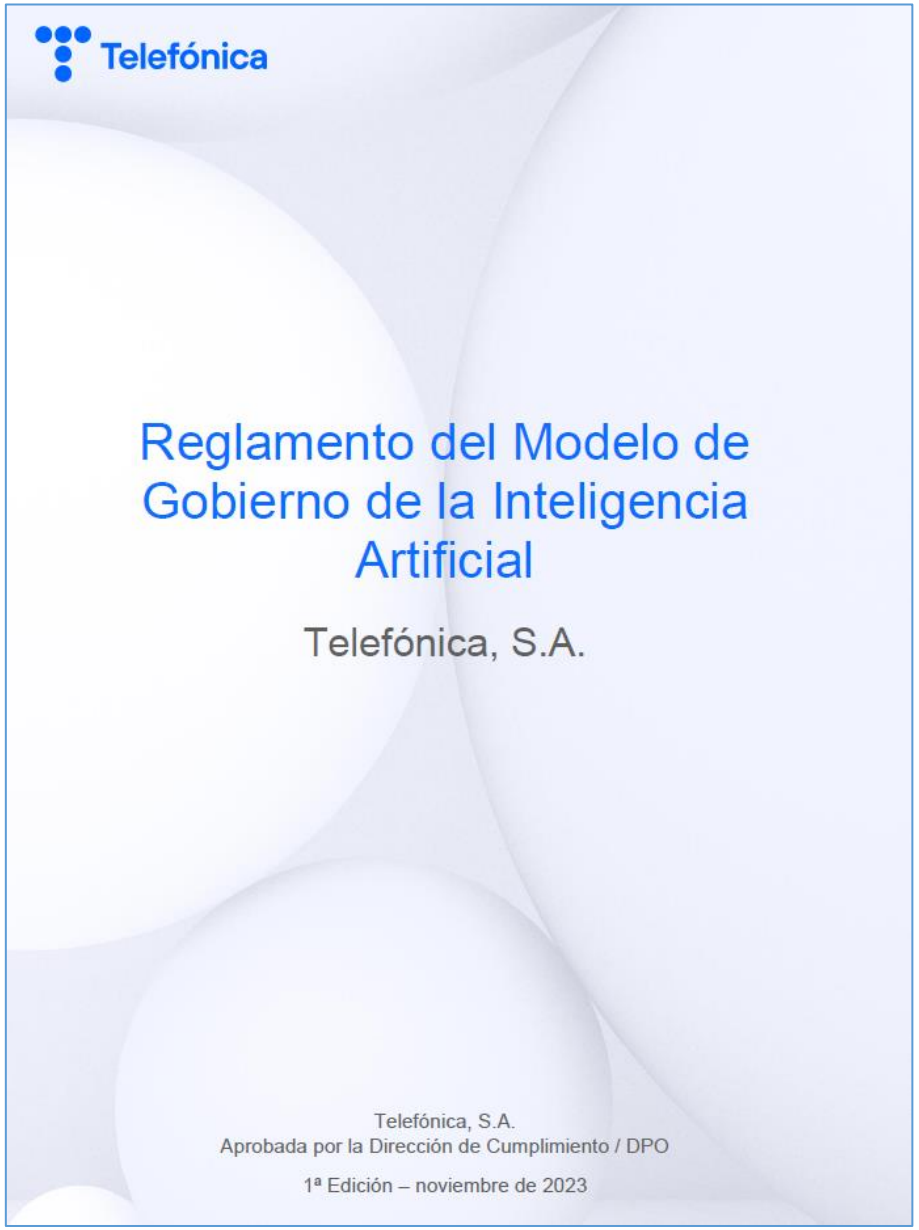
Política de IA

- Es un documento formal aprobado por la alta dirección que establece los **principios, objetivos y compromisos** de la organización respecto al **uso y la gestión de sistemas de IA**.

- Algunos elementos clave:
  - Propósito y alcance
  - Principios de uso responsable
  - Compromiso con la gestión de riesgos
  - Cumplimiento normativo
  - Roles y responsabilidades
  - Mejora continua



Política de IA



Modelo de gobierno

Nuestro modelo de gobierno de IA responsable nos permite aprovechar todo el potencial de la IA al tiempo que protegemos a las personas y minimizamos los posibles riesgos.

Nuestros principios de IA y modelo de gobierno aplican a todos nuestros productos y servicios desde el diseño y se extiende a nuestros proveedores y socios comerciales. Además, nos va a permitir cumplir con las leyes de IA aplicables en cada uno de los países en los que operamos.

Nuestro **modelo de gobierno de la IA** fue aprobado en 2023, y define procesos y determina roles asociados a responsabilidades concretas, que nos permiten aprovechar todo el potencial de la IA al tiempo que protegemos a las personas y minimizamos los posibles riesgos durante todo el ciclo de vida de los sistemas de inteligencia artificial en todas las actividades en las que el Grupo Telefónica participe: **diseño, desarrollo, adquisición, comercialización y utilización**.

Organización y roles

- Diferenciar el rol que tiene la propia organización frente a cada uso de la IA de los roles que se identifican dentro de la propia organización.
- Proveedor vs Responsable del despliegue.
- Definir ¿quién hace qué?
- Evitar solapamientos y vacíos
- Ejemplos: Comité de IA, AI Officer, CISO, DPO, Negocio (owners de casos de uso)

Organización y roles

ÁREAS DE SOPORTE

SOSTENIBILIDAD

SEGURIDAD

PRIVACIDAD

ASESORÍA JURÍDICA

GLOBAL

COORDINACIÓN DE IA GLOBAL

COMPLIANCE GLOBAL

LOCAL

RAI CHAMPIONS LOCALES

COORDINADORES DE IA LOCALES

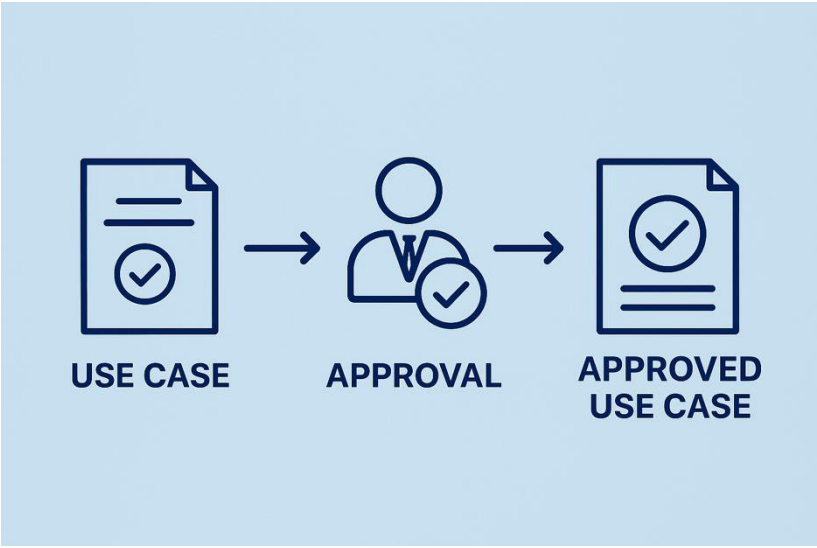
COMPLIANCE LOCAL

RESPONSABLES DE PRODUCTO

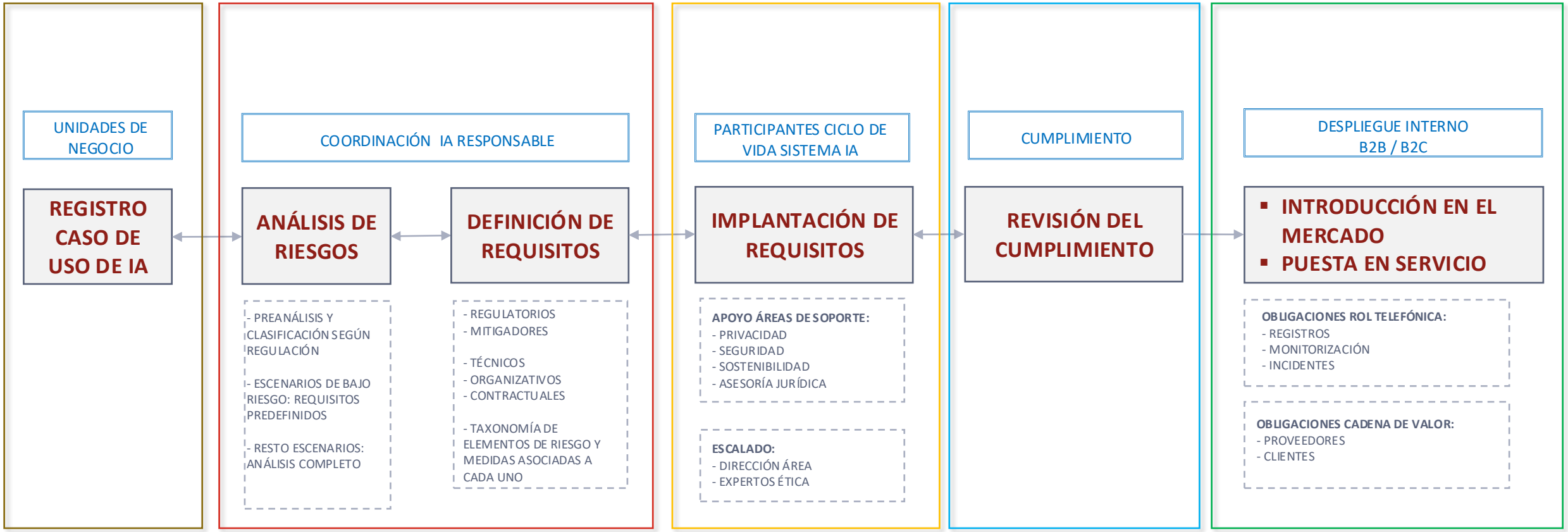
Modelo operativo

¿Cómo funciona en la práctica?

- Flujo de aprobación de casos de uso
- Evaluación de riesgos
- Decisión: aprobar/condicionar/rechazar
- Seguimiento continuo
- Es aconsejable integrarlo en procesos existentes



Proceso: Desarrollo, adquisición, comercialización y utilización de IA



Inventario de IA

- Identificación de todos los casos de uso de IA
- Clasificación (tipo, finalidad, impacto)
- Registro centralizado
- Sin inventario → no hay gobierno

Aplicación Gobernanza IA (GIA)

Telefónica

1	2	3	4
UNIDADES DE NEGOCIO	COORDINACIÓN IA RESPONSABLE	UNIDADES DE NEGOCIO	CUMPLIMIENTO
REGISTRO	**ANÁLISIS DE RIESGOS**	**IMPLEMENTACIÓN DE REQUISITOS**	**RESULTADOS**
CLASIFICACIÓN CATEGORÍA DE RIESGO SEGÚN AI ACT		NORMATIVOS	APROBADO
REQUISITOS NORMATIVOS	REQUISITOS DERIVADOS DEL ANÁLISIS DE RIESGOS	DERIVADOS DEL ANÁLISIS DE RIESGOS	DESCARTADO
			ESCALADO

Clasificación según los riesgos

ILUSTRACIÓN 4: CLASIFICACIÓN DE SISTEMAS DE IA SEGÚN EL RIESGO

Fuente: Guía introductoria al reglamento de IA (AESIA)

- **Sistemas prohibidos.** Por ejemplo: Un sistema de IA que se aprovecha de las vulnerabilidades de las personas mayores para defraudarles o influir en sus decisiones, lo que puede empeorar su salud mental y causarles graves daños psicológicos.
- **Sistemas de alto riesgo.** Por ejemplo: Sistema de IA que analiza en tiempo real las actividades del alumnado durante un examen con el objetivo de saber si están copiando.
- **Sistemas con obligaciones de transparencia.** Por ejemplo: chatbots.
- **Resto de sistemas de IA:** Por ejemplo: aplicación de la IA a los videojuegos.
- **Sistemas NO considerados de IA:** determinados algoritmos más clásicos, como los basados en reglas o heurísticas, no son considerados sistemas de IA en el marco del Reglamento, y por tanto no les aplica.

Aplicativo Gobernanza IA (GIA): Pre-análisis de riesgos

Para los sistemas que por normativa no sean de alto riesgo, se ha habilitado un “fast track” del análisis de riesgos, para que únicamente se le asocien los mínimos requisitos que tenga que cumplir a este tipo de sistemas de riesgo limitado. Estos requisitos se asocian de forma automática a los sistemas con las siguientes condiciones:

	REQUISITOS APLICABLES
A TODOS:	**Ciberseguridad** Incorporar la ciberseguridad en el diseño, las pruebas, la implementación y la operación del sistema de IA. Proporcionaremos actualizaciones de seguridad al sistema de IA
Si se utilizan datos personales:	**Privacidad** Integrar la privacidad en el diseño, las pruebas, la implementación y el funcionamiento del sistema IA. Si los datos incluyen información confidencial o de identificación personal, incluidos datos biométricos, se identificarán las precauciones adicionales que se tomarán
Si utilizan IA Generativa:	**Propiedad intelectual** Asegurar que el sistema de IA no infringe los derechos de terceros, como por ejemplo los derechos de autor en los contenidos que alimentan l sistema o los contenidos que genera el sistema

SIEMPRE TENEMOS QUE TENER EN CUENTA LA APLICACIÓN DE **NUESTRO CÓDIGO DE CONDUCTA: LOS PRINCIPIOS DE IA**

Aplicativo Gobernanza IA (GIA): Análisis de riesgos

Telefónica

ANÁLISIS DE RIESGOS

IMPACTO	PROBABILIDAD
Salud física y mental	Justa e inclusiva
Seguridad de las personas	Transparente y explicable
Derechos humanos	Centrada en las personas
Ciberseguridad	Cadena de valor
Privacidad	Gobernanza
Propiedad intelectual	
Medioambiente	
Implicaciones éticas	

→ REQUISITOS DERIVADOS DEL ANÁLISIS DE RIESGOS

Alfabetización

Considerando 20 RIA

"Con el fin de obtener los mayores beneficios de los sistemas de IA, protegiendo al mismo tiempo los derechos fundamentales, la salud y la seguridad, y de posibilitar el control democrático, ***la alfabetización en materia de IA*** *debe dotar a los proveedores, responsables del despliegue y personas afectadas de los* ***conceptos necesarios para tomar decisiones con conocimiento de causa en relación con los sistemas de IA.*** *Esos conceptos pueden variar en función del contexto pertinente e incluir el entendimiento de la correcta aplicación de los elementos técnicos durante la fase de desarrollo del sistema de IA, las medidas que deben aplicarse durante su uso, las formas adecuadas de interpretar los resultados de salida del sistema de IA y, en el caso de 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. En el contexto de la aplicación del presente Reglamento, la alfabetización en materia de IA debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución"*

Alfabetización

- Nuestros principios de IA
- Modelo gobierno de IA
- Evaluación de riesgos de la IA de P&S
- Plan de cultura de IA Responsable

Muchas gracias

Organiza:

Partners Estratégicos:

Telefónica Tech

GOVERTIS
Part of Telefónica Tech

Mesa de dialogo sobre medidas estratégicas de seguridad

Autenticación Multifactor (MFA)
Sistema Integral de Ciberseguridad y
Gestión de Identidades y Control de Accesos (IAM)

Intervienen:

José Antonio Sánchez, Senior Consultant Advisor en Govertis

Jesús Amorín, Jefe de Ciberseguridad en RTVE

QAEC
Club del CISO

Foro GRC Gobierno, Riesgo y Cumplimiento
Ciberseguridad - Privacidad - IA

La **seguridad digital** ya no es un tema exclusivo de los departamentos de IT. Afecta a ciudadanos, empresas públicas y privadas, pymes y administraciones.

Esta mesa de diálogo se estructura en tres bloques temáticos progresivos, con la siguiente lógica:

- la **Autenticación Multifactor (MFA)** como **capa de autenticación**,
- el **Sistema Integral de Ciberseguridad**, como **marco estratégico** que lo envuelve, y
- la **Gestión de Identidades y control de acceso (IAM),** que es la **capa de gobierno** que orquesta todo.

Para situar el contexto:

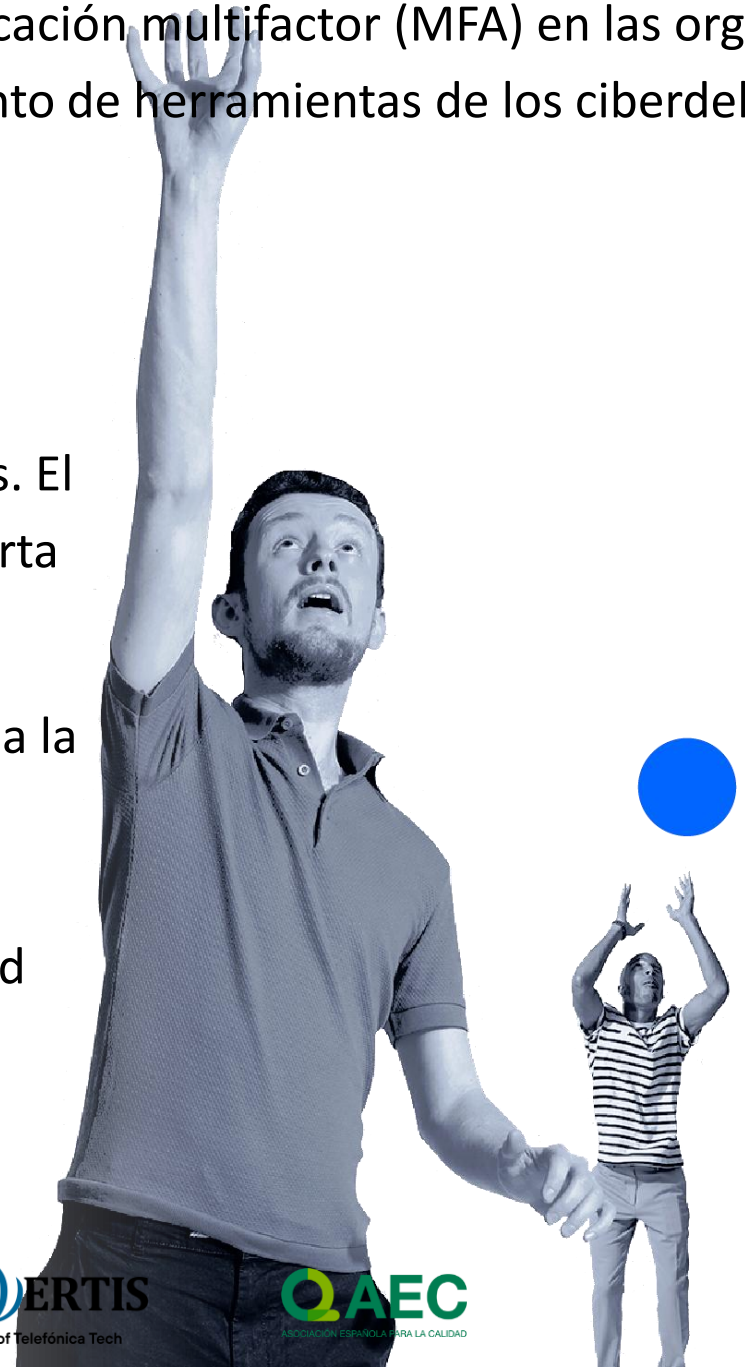
- la **Directiva NIS2**,
- el **Esquema Nacional de Seguridad ENS**,
- el **Reglamento General de Protección de Datos (RGPD)**,
- el **Reglamento DORA**,
- el **Reglamento de Inteligencia Artificial (RIA)**, y
- la **Directiva CER**,

entre otras normativas, están redefiniendo las obligaciones de seguridad para un número creciente de organizaciones públicas y privadas, lo que convierte estas materias en urgentes, no solo relevantes.

No se debe posponer la implementación de la autenticación multifactor (MFA) en las organizaciones, ya que las credenciales son una parte fundamental del conjunto de herramientas de los ciberdelincuentes.

Según datos recientes del **CCN-CERT**, los incidentes de seguridad en la administración pública española han aumentado significativamente en los últimos tres años. El **factor de autenticación deficiente** sigue siendo la puerta de entrada más común en ataques dirigidos.

Según el **Informe Verizon DBIR 2026**, en la exposición a la nube de terceros, solo el 23 % de las organizaciones corrigieron por completo la autenticación multifactor (MFA), siendo en ocasiones inexistente o con seguridad inadecuada en sus cuentas en la nube.



DBIR (Data Breach Investigations Report)

Telefónica Tech

GOVERTIS Part of Telefónica Tech

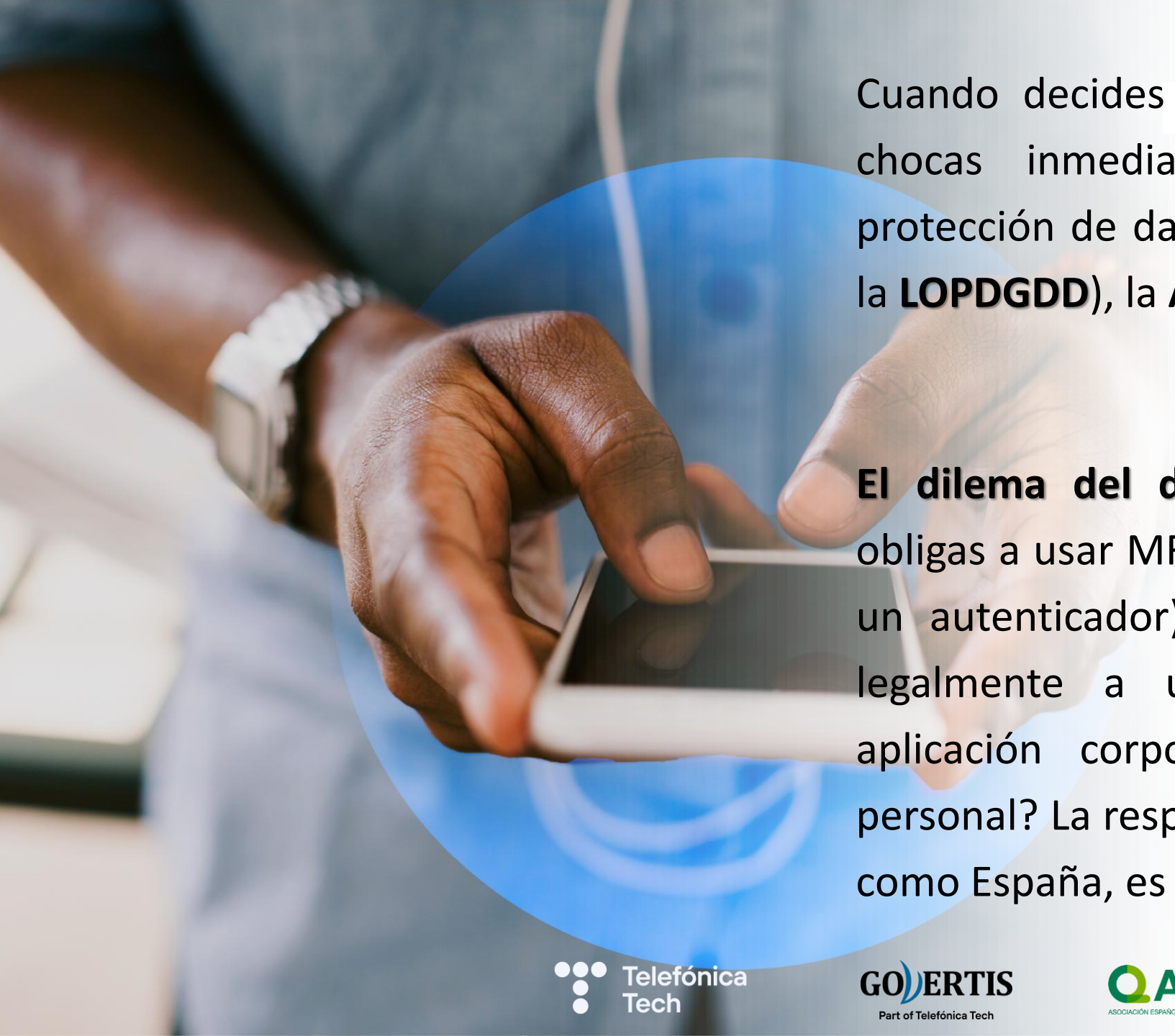
AEC Asociación Española para la Calidad

BLOQUE 1
Autenticación Multifactor

Comenzando con el primer bloque, existen numerosos métodos de autenticación que aprovechan el multifactor para reforzar la seguridad de los accesos en base a algo que **SABES**, que **TIENES**, que **ERES**, la **UBICACIÓN** o los **RIESGOS** (contexto y comportamiento), utilizando:

- Aplicaciones de autenticación en dispositivos móviles
- Notificaciones emergentes
- Correo electrónico
- Huella dactilar o reconocimiento facial (**biometría**)
- Tokens hardware
- Uso de SMS

El poder optar por un MFA robusto ya está disponible, pero cuenta con un obstáculo para su implementación, y no es técnico, sino jurídico, organizativo y de recursos.



Cuando decides implementar un MFA robusto, chocas inmediatamente con normativas de protección de datos (como el **RGPD** en Europa o la **LOPDGDD**), la **AEPD** y con el **derecho laboral**.

El dilema del dispositivo personal (BYOD): Si obligas a usar MFA basado en aplicaciones (como un autenticador) o biometría, ¿puedes obligar legalmente a un empleado a instalar una aplicación corporativa en su teléfono móvil personal? La respuesta jurídica en muchos países, como España, es no.

Protección de datos biométricos: Si optas por usar la huella dactilar o el reconocimiento facial del usuario como factor, la legislación considera estos datos como "**categorías especiales**". Aunque el procesamiento se haga localmente en el dispositivo, los departamentos legales suelen exigir análisis de impacto de privacidad muy estrictos antes de dar el visto bueno.

El obstáculo Organizativo (Resistencia y Usabilidad) Obligar a un operario de fábrica que lleva guantes a quitarse el equipo para poner una huella, o a un médico en urgencias a sacar el teléfono cada vez que cambia de ordenador, rompe el ritmo de trabajo. Si la seguridad impide que la gente haga su labor, los empleados buscarán la forma de saltarse la norma.

Coste real

Creer que el MFA es gratis o barato porque "**viene incluido**" en la licencia de Microsoft 365 o Google Workspace es un error de cálculo enorme. El **coste real** no es la licencia, **es la operación**. Si jurídicamente no puedes obligar a usar el móvil personal, la empresa tiene que comprar miles de llaves físicas de seguridad (hardware tokens) o teléfonos corporativos.

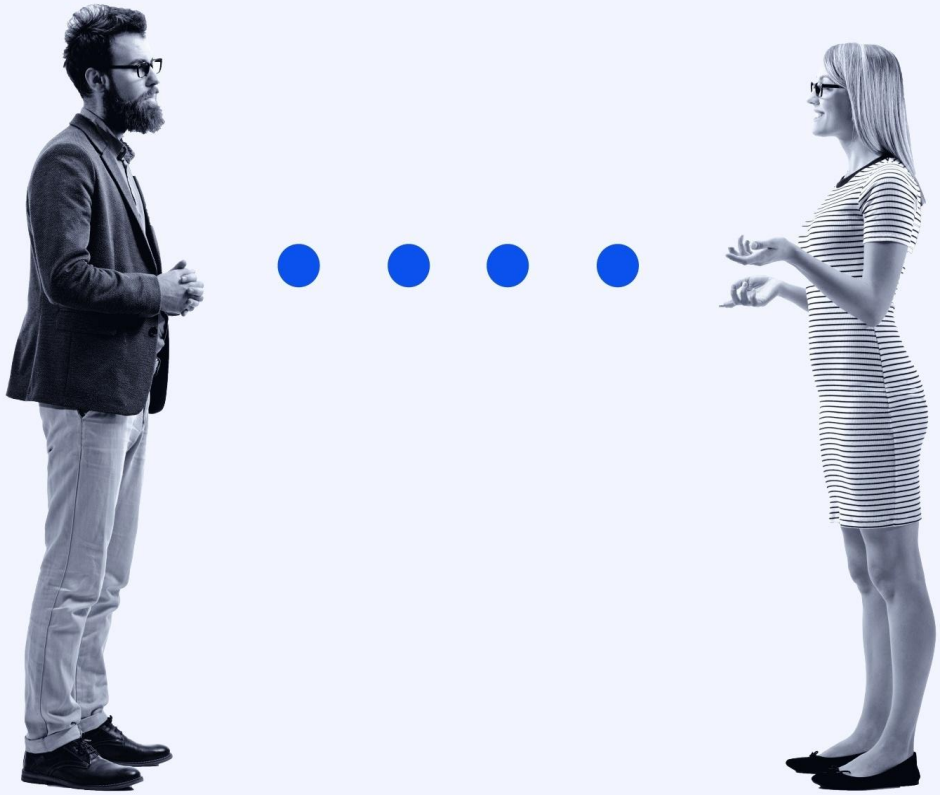
MFA como cumplimiento de mínimos o MFA como herramienta real de reducción de riesgo

Es una distinción crucial y da en el clavo del gran dilema de los departamentos de seguridad y TI. La diferencia radica en la **mentalidad de la organización**: ver la ciberseguridad como una muesca, un check en una lista de tareas legales, proporciona una falsa sensación de seguridad, frente a verla como un escudo dinámico contra amenazas reales, con un enfoque basado en riesgo.

En el sector público y en las pymes, el **argumento** más frecuente **contra el uso de la Autenticación Multifactor (MFA)** es la **resistencia interna del usuario**, el fenómeno de la fatiga de MFA por saturación en la frecuencia de las solicitudes, las incidencias, limitaciones y fallos en los dispositivos y con las aplicaciones, errores biométricos de reconocimiento, y sobre todo la falta de formación y concienciación del usuario.

Esa resistencia es el pan de cada día, especialmente en el sector público (con plantillas a menudo envejecidas y procesos muy burocratizados) y en las PYMEs (donde el personal tiene múltiples sombreros y poco tiempo). Los argumentos —fatiga de alertas, fallos técnicos, falta de formación— son **quejas legítimas** de usabilidad, no simple terquedad. Si respondemos a los usuarios con el típico discurso técnico de "**es obligatorio por seguridad**", la **resistencia se duplicará.**

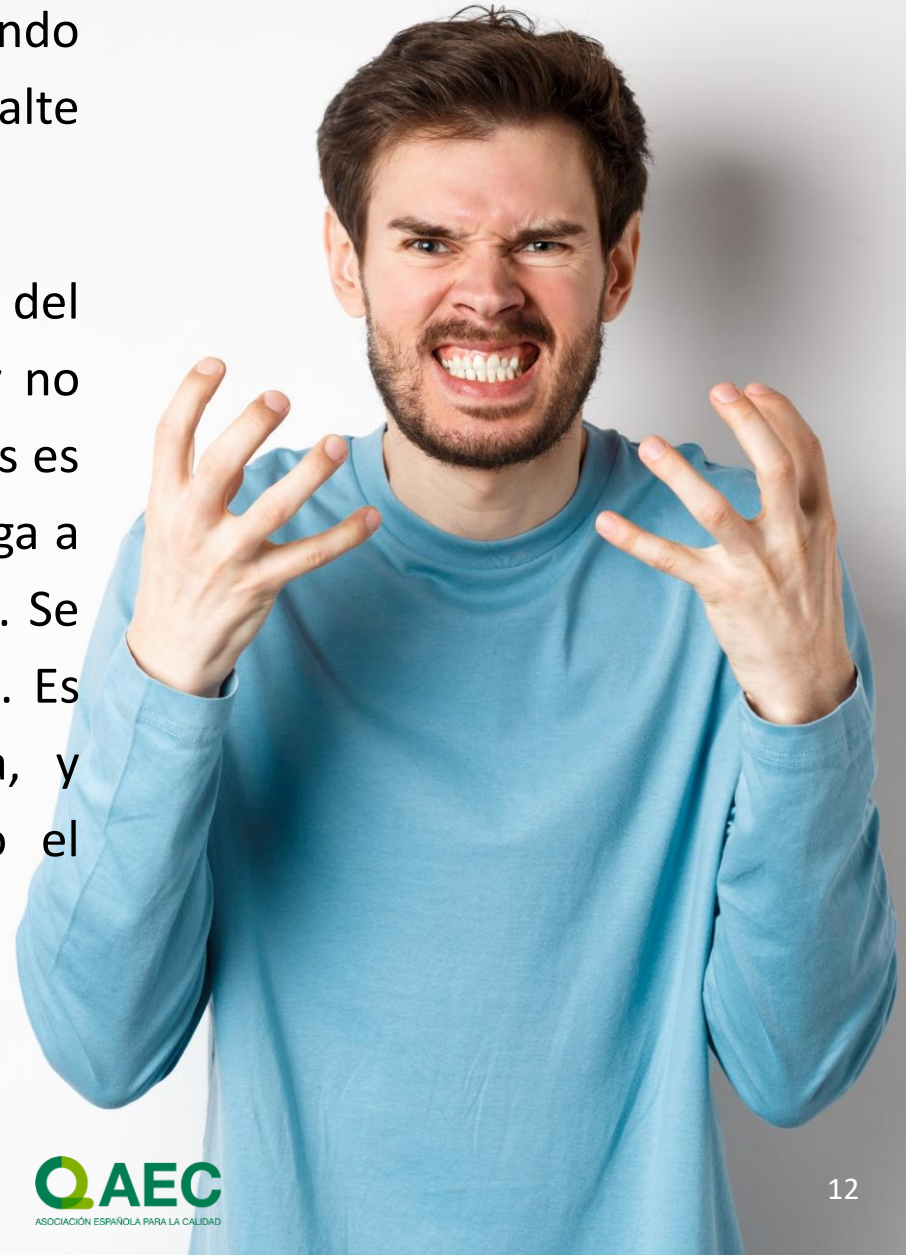
Resistencia Interna



Argumentos del usuario

"No puedo trabajar si cada 20 minutos el ordenador me está pidiendo un código en el móvil", la solución pasa por que el **MFA** solo salte **cuando cambie el contexto**.

"El lector de huellas no me lee el dedo", "No quiero instalar apps del trabajo en mi móvil personal" o "Me he quedado sin batería y no puedo trabajar". La solución idónea para el sector público y PYMEs es **desplegar llaves físicas**. Si la biometría falla o el empleado se niega a usar su móvil, se le entrega un **token físico** que va **en su llavero**. Se conecta por USB o se acerca al teclado por aproximación (NFC). Es instantáneo, no falla por problemas de cobertura o batería, y jurídicamente disuelve cualquier conflicto con el sindicato o el departamento legal sobre el uso de dispositivos personales.



NFC (Near Field Communication)

Telefónica Tech

GOVERTIS Part of Telefónica Tech

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

CUMPLIMIENTO NORMATIVO

La MFA contribuye directamente al cumplimiento de marcos regulatorios y estándares de seguridad.

Normativas y estándares relacionados

RGPD Reglamento General de Protección de Datos.

ENS Esquema Nacional de Seguridad Mecanismos de autenticación.

RIA Reglamento de Inteligencia Artificial.

DORA Reglamento de Resiliencia Operativa

ISO/IEC 27001: Controles de acceso y gestión de identidades.

NIST SP 800-53 r5: Controles de seguridad y privacidad para sistemas de información y organizaciones

NIST SP 800-63: Directrices de identidad digital, recomendación explícita de MFA.

Respecto a la **Protección de los Datos Personales y la Privacidad**, la **AEPD** no exige el MFA de forma explícita como obligación legal autónoma, pero su postura práctica lo convierte en casi ineludible.

El artículo 32 del RGPD obliga a **implementar medidas técnicas y organizativas apropiadas** al riesgo. La propia AEPD, en su informe de brechas de junio de 2025, señala que el uso de VPN con autenticación multifactor es crucial para asegurar el acceso remoto a sistemas corporativos, y que añade una capa adicional de seguridad que dificulta el acceso a los datos, aunque se comprometa una contraseña. En la práctica, si ocurre una brecha y no había MFA, la AEPD puede concluir que no se tomaron las medidas adecuadas.

Por otra parte, el **ENS** establece para el **mecanismo de autenticación** el refuerzo R8 para todos los niveles y categorías cuando el **acceso** se realiza **desde zonas no controladas**, lo que en la práctica equivale a exigir MFA para el teletrabajo y el acceso remoto en la Administración.

Como vemos, el MFA es **casi obligatorio por vía del RGPD y el ENS**, pero **implementarlo mal** —usando el teléfono personal del trabajador sin base legal, sin informar, sin alternativa corporativa— genera sanciones por sí mismo.

El **RIA** obliga a que los sistemas de IA de alto riesgo incorporen ciberseguridad como requisito de diseño. Los sistemas de alto riesgo deben garantizar precisión, robustez y ciberseguridad según el artículo 15. El **uso de factores biométricos dentro de MFA en el entorno IA es lícito**, pero exige medidas adicionales de seguridad, minimización y control del tratamiento de datos biométricos, al ser considerados altamente sensibles.

Si analizamos la normativa vigente (tanto en España como a nivel europeo), el **panorama legal respecto al MFA** sufre de un problema clásico del derecho tecnológico: **las leyes dicen qué** tienes que conseguir, **pero casi nunca detallan cómo** debes hacerlo. La normativa es ambigua, fragmentada y avanza a distintas velocidades según el sector, lo que genera una enorme **inseguridad jurídica**.

BLOQUE 2
Sistema Integral de Ciberseguridad

Telefónica Tech

GOBERTIS
Part of Telefónica Tech

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Conectando con lo tratado en el punto anterior, si el **MFA** es la llave, el **SOC** y el **SIEM** son la alarma y la Cámara de seguridad.

El **SOC (Security Operations Center)** es el Centro de Operaciones de Seguridad. No es un software, sino **un equipo humano** de expertos (analistas, ingenieros y cazadores de amenazas) y un espacio (físico o virtual) encargado de supervisar y defender la infraestructura tecnológica de una empresa las 24 horas del día, los 7 días de la semana.

Su función: Monitorear, detectar, analizar y responder a los incidentes de seguridad en tiempo real. Los analistas del SOC toman decisiones críticas, investigan alertas sospechosas y contienen los ataques antes de que causen daños graves.

El **SIEM (Security Information and Event Management)** es la Gestión de Información y Eventos de Seguridad. Es una **plataforma de software centralizada** que recolecta, normaliza y analiza masivamente los registros (logs) de actividad de todos los dispositivos de la red (servidores, firewalls, antivirus, bases de datos, etc.).

Su función: Centralizar la información y buscar patrones sospechosos mediante la correlación de eventos. Su verdadero poder radica en conectar puntos inconexos. Por ejemplo, si un usuario falla 5 veces su contraseña en un servidor de Madrid y, un segundo después inicia sesión con éxito desde una IP en Barcelona, el SIEM identifica esto como una anomalía y genera una alerta.

La **relación entre el SOC y el SIEM es simbiótica**: el SOC es el cerebro y el SIEM son los ojos y oídos. Un SOC sin un SIEM estaría ciego ante la inmensidad de datos de la empresa, y un SIEM sin un SOC sería solo un software costoso acumulando alertas que nadie atiende. Dentro de un **Sistema Integral de Ciberseguridad**, funcionan como una línea de producción perfectamente engrasada.

Para que un **Sistema Integral de Ciberseguridad** sea maduro y realmente eficiente, necesita la aportación de la potencia analítica de la tecnología (SIEM) combinada con el conocimiento, criterio, experiencia y capacidad de reacción del talento humano (SOC).

Actividades principales de un Servicio Integral de Ciberseguridad

- el análisis de ciber-riesgos en servicios críticos.
- el seguimiento de vulnerabilidades y medidas correctoras.
- la gestión de incidentes y la coordinación de respuesta con las áreas afectadas.
- el análisis de ciber seguridad en desarrollos, cambios y proyectos.
- la gestión de vulnerabilidades.
- soporte al cumplimiento de las normativas y regulaciones.
- el análisis de riesgos y Controles de seguridad en los servicios críticos.
- test de intrusión y gestión de vulnerabilidades
- la monitorización a través de un SIEM (como IBM Qradar) proporcionado por un SOC.

Telefónica Tech

GOUERTIS Part of Telefónica Tech

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Incidentes de Ciberseguridad en tiempo real

Que **la mayoría de los incidentes de seguridad no se detecten en tiempo real** es una de las realidades más frustrantes (y peligrosas) de la ciberseguridad. Existe una brecha enorme entre el momento en que un atacante entra a un sistema y el momento en que la organización se da cuenta, que a menudo son semanas o meses.

Hoy en día, los cibercriminales rara vez entran haciendo ruido o usando malware obvio que haga saltar las alarmas de un antivirus. En su lugar, **roban credenciales legítimas** y utilizan las propias **herramientas del sistema operativo** (como PowerShell en Windows o SSH en Linux) para moverse por la red.

Los ataques modernos están diseñados específicamente para **pasar desapercibidos**, ejecutados directamente en la memoria RAM o mediante **exfiltración lenta** de pocos kilobytes, pero durante mucho tiempo.

Plan de Respuesta a Incidentes

En el panorama actual de ciberseguridad disponer de un **Plan de Respuesta a Incidentes** es una pieza tan crítica como tener un seguro de incendios o una salida de emergencia en un edificio físico. De hecho, hay una máxima muy conocida en el sector: "**No se trata de si te van a atacar, sino de cuándo**". Cuando el ataque ocurre, el factor que define si la empresa sobrevive o quiebra no es la tecnología que tenía para evitarlo, sino la velocidad y eficacia con la que responde.

Sin un plan, se toman **decisiones viscerales e improvisadas**. Alguien podría apagar un servidor a la fuerza (destruyendo evidencia volátil en la memoria RAM que ayudaría a saber cómo entraron). Con un plan hay una **lista de pasos fríos y calculados**. El equipo **sabe exactamente a quién llamar**, **qué desconectar primero** y **qué mantener encendido** para la investigación.

Zero Trust

Zero Trust se ha convertido en un término de marketing, pero **Zero Trust** no es un producto que compras, es una estrategia arquitectónica que **asume que el enemigo ya está dentro** de la red. Su lema práctico es:

"**Nunca confiar, siempre verificar**".

En la práctica, Zero Trust significa dejar de dar prioridad a proteger "el perímetro" de la empresa y empezar a **proteger** cada **usuario**, cada **dispositivo** y cada **dato** de forma individual, sin importar dónde estén.

BLOQUE 3
Gestión de Identidades y Control de Accesos (IAM)

Cerramos este dialogo con este último bloque, los **Sistemas de Gestión de Identidades y Control de Accesos**.

Hemos hablado de **MFA**, de los **Sistemas Integrales de Ciberseguridad**, de arquitectura de seguridad **Zero Trust** y ahora del **IAM** como si fueran dominios distintos, pero la realidad es que no son elementos aislados, todos juntos conforman un mismo engranaje.

Para que funcione, se necesita una coreografía muy precisa entre **tres perfiles** con **mentalidades**, **objetivos** y, a veces, **presupuestos** completamente **diferentes**.

- El **CISO,** dueño del riesgo de seguridad y decide la estrategia y la arquitectura.
- El **Responsable de IT,** dueño de la disponibilidad y la operación (que los sistemas funcionen, la red sea rápida y los usuarios no se quejen).
- El **DPD** es el garante del cumplimiento legal (RGPD), un perfil jurídico/consultivo.

El mayor error es que el **CISO e IT** vean al **DPD** como "el abogado que siempre dice que no", o que **IT** vea al **CISO** como "el paranoico que lo quiere bloquear todo". Las organizaciones que mejor funcionan son aquellas donde el **CISO** utiliza los **argumentos legales** del **DPD** para conseguir presupuesto de la dirección, e **IT** utiliza la **estrategia** del **CISO** para modernizar una infraestructura que de otro modo se quedaría obsoleta.

Pero si solo contásemos con un único técnico de IT en un ayuntamiento pequeño —que seguro está desbordado arreglando desde la impresora del alcalde hasta los servidores del padrón—, el único consejo sería '**No intentes proteger todo el ayuntamiento a la vez**; aplica MFA robusto y Acceso Condicional exclusivamente a las cuentas de Administrador y al personal que teletrabaja.

Sistema de Gestión de Identidades y Control de Accesos (IAM)

Disponer de un **Sistema de Gestión de Identidades y Control de Accesos (IAM)** es recomendable porque la identidad se ha convertido en el nuevo perímetro de seguridad de las organizaciones.

En un mundo donde los empleados trabajan desde sus casas, los servidores están en la nube y los datos se comparten con colaboradores externos, el viejo "**cortafuegos**" de la oficina ya no sirve como garantía de seguridad total. La única forma de saber si quien intenta ver una base de datos es realmente quien dice ser es **controlando su identidad**.

Beneficios que aporta un Sistema de Gestión de Identidades y Control de Accesos (IAM)

Seguridad y Mitigación de Riesgo al centralizar los accesos, el IAM permite aplicar de forma masiva políticas como la Autenticación Multifactor (MFA) o el Acceso Condicional, automatiza las bajas de usuarios, revocando todos los accesos de golpe y aplica el **Principio de Mínimo Privilegio**.

Eficiencia y productividad, con el uso del Single Sign-On (SSO) permite a los empleados iniciar sesión una sola vez con una contraseña única y segura para acceder a todas sus aplicaciones.

Cumplimiento Legal gracias a la trazabilidad total ante una auditoría o un incidente de seguridad, un control estricto y auditable de quién accede a los datos de carácter personal o crítico, exigido por las normativas.

Justificación inversión en un Sistema de Gestión de Identidades y Control de Accesos (IAM)

Argumento del **Riesgo Financiero y Reputacional**. Un ciberataque grave que secuestre nuestros datos no solo implica una multa potencial por normativas como el RGPD o NIS2. Significa paralizar las operaciones de la organización durante días o semanas. El coste de tener a la empresa parada un solo día supera con creces la inversión anual en una plataforma de IAM.

Argumento de la **Eficiencia Operativa** (Ahorro de costes ocultos) Con una solución de IAM, cuando un empleado entra a la organización, sus accesos se crean en minutos de forma automatizada; y lo más importante, cuando se marcha, sus accesos se revocan al instante y por completo, eliminando el peligro de las "**cuentas zombis**".

Telefónica Tech

GOVERTIS Part of Telefónica Tech

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Argumento del **Crecimiento del Negocio** (Habilitador, no freno) El IAM actúa como un **facilitador de negocio**: permite abrir de forma segura nuestros sistemas a nuevos modelos de trabajo y socios comerciales, garantizando que el acceso se da bajo la premisa de "**mínimo privilegio**".

Cerramos este diálogo con tres ideas:

Primera: el MFA no es una opción, es el mínimo exigible.

Segunda: la Ciberseguridad Integral se construye, y requiere tanto inversión técnica (SOC / SIEM), como cultura organizativa y procesos bien definidos.

Tercera: el Sistema de Gestión de Identidades y Control de Accesos (IAM) es la capa de gobierno que une todo. Quien controla la identidad, controla el acceso.

GRACIAS POR SU ATENCIÓN

Telefónica Tech

GOVERTIS
Part of Telefónica Tech

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD