

Título: Gobernanza Digital: Seguridad de la Información y uso responsable de la Inteligencia Artificial.

Categoría: La práctica se inscribe en la **Categoría 1, Gobernanza y liderazgo**, subcategoría: **Modelos de gestión de órganos de gobierno que mejoran la calidad de las decisiones.**

Introducción:

La práctica nace para mantener y garantizar la buena reputación y, por tanto, la sostenibilidad de la Asociación.

El origen de esta práctica se debe a varios motivos:

1. El desarrollo tecnológico tan acelerado que se ha producido en la Asociación
2. El auge de la IA
3. El elevado número de normativas relacionadas con la ciberseguridad y la IA publicadas.

Todo ello nos llevó a replantearnos, cómo tenemos que abordar la gobernanza digital: la seguridad de la información de la Asociación y el uso ético y responsable de la IA, evitando malas praxis, manteniendo los niveles de excelencia en la gestión y dando cumplimiento a la legislación.

Esta práctica nace de la voluntad de la asociación de ser coherente con su visión y mantener los altos estándares de gobernanza que definen su identidad como entidad. En definitiva, una decisión de gobierno donde se asume la **gobernanza digital** como una dimensión propia de responsabilidad, incorporando nuevos mecanismos de control, supervisión y rendición de cuentas que **mejora la calidad de las decisiones estratégicas**.

Objetivos:

1. **Ampliar el alcance de la Gobernanza de la Asociación**, a la ciberseguridad y uso responsable de la IA.
2. Fomentar una **cultura organizacional centrada en la ciberseguridad y uso responsable de la IA**.
3. Garantizar la **sostenibilidad** de la Asociación.
4. **Proteger** de manera proactiva contra ataques dirigidos hacia datos.
5. Mejorar la **resistencia y la capacidad de respuesta** ante amenazas.
6. **Concienciar, formar y capacitar** a las partes implicada en todos los niveles de la importancia de la Ciberseguridad.
7. Garantizar los **derechos digitales de las personas con discapacidad intelectual y del desarrollo** como sujetos de derechos en el ecosistema digital.
8. **Dotar a la Junta Directiva y órganos de gobierno** de información fiable, indicadores de seguimiento y sistemas de control **que mejoren la calidad y la trazabilidad de sus decisiones estratégicas en el ámbito digital**.

2.- Desarrollo de la práctica

La Asociación tiene implantado un sistema de gestión integrado según el [Modelo EFQM](#), las [normas ISO 9001 y 14001](#), el [Reglamento EMAS](#), [modelo de Plena Inclusión](#), [modelo de conciliación de Empresa Familiar responsable \(EFR\)](#), [dona con confianza](#) y [sistema de gestión del Compliance](#).

En los últimos años, la Asociación ha vivido un proceso de desarrollo tecnológico muy acelerado: el uso del Teams, sharePoint en móviles personales, el uso de móviles, portátiles, tablets corporativos con información sensible se había extendido entre el equipo de profesionales, la automatización de procesos, los sistemas digitales de registro, comunicación y coordinación, el teletrabajo han multiplicado los puntos por donde fluye información de las personas con discapacidad y del desarrollo, sus familias y profesionales, así como el uso de la inteligencia artificial (IA) han entrado en el día a día de la gestión y la prestación de apoyos.

Todo ello, refleja el **compromiso de la Asociación APROSU con la innovación y la mejora continua**, pero se convierte en un punto de inflexión para preguntarnos **¿estamos gobernando esta nueva realidad con los mismos estándares de rigor y excelencia con los que gobernamos el resto de la gestión de la entidad, es decir, datos económicos, inmuebles, etc?**.

La visión de la Asociación es ser un referente en los servicios y apoyos a las personas con discapacidad y del desarrollo. Pero ser referente no admite medias tintas o se es coherente en todas las dimensiones de gestión y, eso implica adaptarse a los cambios del ecosistema, o se deja de ser un referente y, la gobernanza de la información, unido al auge de la IA estaba quedando rezagada respecto al ritmo de la gobernanza en otras áreas de la Asociación.

Lo que nos llevó a seleccionar una empresa que nos apoyara en la implementación del Sistema de Seguridad de la Información, según el Esquema Nacional de Seguridad.

La información que gestiona la Asociación- datos médicos, historias de apoyo, situaciones familiares, evaluaciones personales, datos de profesionales, **es su activo más valioso y el soporte para dar cumplimiento a su propósito** y donde **la confianza de sus grupos de interés es la propuesta de valor que la Asociación construye.**

Para el desarrollo se siguieron **los siguientes pasos:**

1. **Diagnóstico: Análisis de riesgos, mecanismo de control, documentos y procedimientos para la gestión de la seguridad de la información.**
2. **Constitución y definición de funciones del Comité de seguridad de Información.**
3. **Elaboración y aprobación de documentos.**
4. **Adquisición, instalación y puesta en marcha de programas, equipos para el cumplimiento del modelo de gestión del sistema de seguridad de la información.**
5. **Concienciación, formación y difusión del Sistema a todas las partes implicadas.**
6. **Revisión y sistema de evaluación.**

1. Diagnóstico: Análisis de riesgos, de mecanismo de control, documentos y procedimientos para la gestión de la seguridad de la información.

Se realizó la identificación del equipo de profesionales implicados, calendario y jornadas de trabajo. Se identificaron los riesgos de seguridad de información (entorno tecnológico, activos críticos, ...) y los riesgos de las IA en uso, según:

- a. Criterios: Confidencialidad, disponibilidad, Integridad, autenticidad, trazabilidad, probabilidad.
- b. Nivel: Crítico, alto, medio y bajo

Se proponen plan de actuación con los controles, medidas adicionales, responsable y, plazos.

2. Constitución y definición de funciones del Comité de seguridad de Información.

Se constituye el Comité de seguridad con fecha 01/10/2025 y se define las funciones y responsabilidades del: Responsable de la información, responsable del servicio, de seguridad y del sistema.

Se actualiza el organigrama incorporando el nuevo Comité, así como los perfiles profesionales de Comité y añadiendo como responsabilidades en todos los perfiles de puestos de la Asociación el cumplimiento de seguridad de la información y el uso responsable de la IA.

3. Elaboración y aprobación de documentos del Sistema de gobernanza digital.

Se analizan los documentos que disponíamos, y se definieron los nuevos documentos necesarios para la implementación del sistema, así como actualización de otros.

Se clasifica la información (pública, interna y confidencial), se categorizan los puestos de trabajo, se evalúan los proveedores críticos del sistema.

Se actualizan:

- El Mapa de procesos.
- Política de uso de recursos técnicos e informáticos.
- Código Ético

Se elaboran:

- El PS.10 Seguridad de la Información.
- Política de Seguridad de Información
- Manual de Seguridad de información
- Decálogo 20 formas en las que la IA te ayuda en tu día a día
- Declaración de aplicabilidad
- Procedimiento de Seguridad de la información
- Política de Robo o Pérdida de dispositivos móviles
- Proceso de autorización
- Protocolo de inundación de sala de Servidor
- Procedimiento metodológico de análisis de riesgos
- Arquitectura de seguridad.
- Gestión de incidencias de seguridad, gestión de cambios, bastionado, control de accesos, mantenimiento y actualizaciones de seguridad,) etc.

Se actualiza el inventario de activo de seguridad de información y de IA en uso. Los documentos son aprobados por Junta Directiva o Comité de seguridad, según proceda.

4. Adquisición, instalación y puesta en marcha de programas, equipos y modelo de gestión del sistema de seguridad de la información.

Esta fase supone una gran carga de trabajo más técnica relacionada con las empresas de mantenimiento de informática, redes, sistema, página web, firmas electrónicas y, otros proveedores de programas y sistemas, que son los encargados de poner las salvaguardas necesarias para garantizar la seguridad y un mayor control, trazabilidad y seguridad de la información en equipos informáticos en sedes, tablets, móviles, software, programas, telefonía, web, servidores, firmas electrónicas de Órganos de gobierno y profesionales, doble factor de autenticidad, etc.

Se contrató plataforma de gestión de certificado de firmas digitales, sistema que aglutina en una única plataforma en nube la gestión de certificados digitales, nueva centralita avanzada con Microsoft Authenticator, actualización de Windows, software de gestión de impresión, adquisición de nuevos equipos, control de humedad, temperatura e inundaciones para sala servidor, copias de seguridad externas, etc....

Esta fase implicó un elevado coste económico por los innumerables sistemas y equipos que hubo que adquirir.

Para la implementación del sistema se hizo necesario la implicación de todas las partes implicadas, para ello se crea en el Share Point, el **proceso de Seguridad de Información**, con los canales correspondientes: Comité de seguridad de información, comunicación de incidencias de seguridad, con un cuestionario para que los profesionales cuando identifiquen una incidencia la comuniquen, gestión de las incidencias, gestión de solicitudes y aprobaciones y protección de datos.

5. Concienciación, formación y difusión del Sistema a las partes implicadas.

Para que el sistema funcione, y dado que la información es el activo que compartimos todas las personas que formamos parte de la Asociación, se hace necesario concienciar, formar y capacitar a todas las partes implicadas. Para ello, se ha realizado acciones de concienciación y formación tanto para profesionales como personas con discapacidad intelectual. Se hace necesario crear **la cultura de seguridad de la información**.

Para ello, se realizan las siguientes acciones:

1. **Concienciación:** a través de reuniones de Gerencia con todas las personas trabajadoras para poner en conocimiento todos los cambios y novedades que van a afectar en el día a día de nuestro trabajo. Se utiliza reuniones, comunicados y [fondos de pantalla](#)
2. **Formación:** Se elabora el módulo formativo de Seguridad de la Información (Políticas, Normas y procedimiento de seguridad, etc.) que se realiza de manera presencial y online para todas las personas trabajadoras, con evaluación de contenido. Se envían Píldoras formativas de seguridad de información.
Se realiza formación presencial del [Uso responsable y seguro de la IA](#) a todas las personas trabajadoras.
Se adapta [Módulo formativo](#) para las personas con discapacidad intelectual: [La IA en nuestra vida](#).
El equipo de prensa y comunicación es el encargado de impartir la formación al resto de personas con discapacidad que hacen uso de móviles, tables u otros dispositivos.
3. **Firma de documentación:** Se hace necesario la recogida de firmas de políticas, procedimientos, ..., a todas las personas a las que afecta la seguridad de la información y el uso de la IA.

4. Revisión y sistema de evaluación.

La revisión se realiza junto con la revisión del sistema de gestión de la Asociación, esto es, en mayo y octubre, así como tantas veces sea necesaria para adoptarnos a los cambios del ecosistema (legislación riesgos, nuevas IA, etc....). Anualmente se realizará el análisis de riesgos. Además, se realizará auditoría interna y externa del Esquema Nacional de Seguridad. En 2026, se realizó con fecha 18 de junio la auditoría interna, pendiente de la auditoría externa para los días 10, 29 y 30 de julio.

El proceso cuenta con indicadores que se avalúan mensual, trimestral, semestral y anualmente.

RECURSOS:

Recursos Humanos: Junta Directiva, gerencia, dirección de innovación, técnico en desarrollo e innovación, técnico de proyectos, responsable de protección de datos, dirección de finanzas y dirección técnica, técnico en accesibilidad, área de personas y talento, profesionales y personas con discapacidad intelectual y del desarrollo.

Recursos humanos externos: Profesionales de las empresas asesoramiento del Sistema, de empresas externas (mantenimiento equipos informativos, sistemas, redes, telefonía, ...) y certificadora Bureau Veritas.

Recursos Técnicos: Plataforma de Formación On line, Notebook LM, Ivsign, Signaturit, etc.

Recursos económicos:

Gastos: 45.960,24 €

Ingresos:

- **Subvención del Kit Consulting para el asesoramiento para la transformación digital:** 18.000 €
- **Aportación Asociación:** 27.960,24 €

Principal contratiempo: la dificultad propia en la implantación del modelo, por varios motivos:

1. El elevado coste económico de su implantación
2. El no manejar la parte técnica propia de profesionales informáticos, de redes y sistemas, etc.
3. No disponer de otras entidades del sector o de otras Asociaciones que hayan implantado el sistema para hacer benchmarking.
4. La falta de tiempo, debido al alto volumen de trabajo de las entidades.

Principales lecciones aprendidas: una vez comienza de proceso de análisis identificas:

1. **El poder de la Información:** es el principal activo. La Asociación gestiona información de una extraordinaria sensibilidad, lo que a su vez hace que sea el **valor más frágil y decisivo** que tiene, donde una mala praxis puede afectar a la confianza de sus grupos de interés.
2. Una vez se evalúan los posibles **puntos de información expuesta a la falta de seguridad**, tomas conciencia de la vulnerabilidad a la que está expuesta la Asociación, pudiendo provocar un daño reputacional que puede afectar a la reputación y/o a la Sostenibilidad.
3. **El uso de la IA** y la cantidad de información relacionada lleva a los profesionales a implementarla, sin contar con la Asociación, exponiendo a la Asociación a una situación de vulnerabilidad que pudiera desencadenar en un daño reputacional.
4. Lo que comenzó como un proceso de mejora de la seguridad de información, identificamos que, por la propia actividad, estamos **obligados al cumplimiento del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad**.

3.- Método empleado para la puesta en marcha

El punto de partida fue una **convicción estratégica**: la seguridad de la información no es una cuestión técnica, sino una decisión de **gobernanza estratégica**. Desde ese enfoque, la Asociación activó un proceso de inteligencia organizacional que comenzó haciéndose tres preguntas clave: ¿qué sabe la entidad de sí misma en el plano digital?, ¿quién decide sobre ello?, y ¿quién responde cuando algo falla? Ese ejercicio de lucidez fue el verdadero detonante de la implantación.

Se adoptó una metodología de **“gobernanza desde el riesgo”**: antes de diseñar soluciones, se analizó el ecosistema digital de la Asociación —equipos, accesos, flujos de información, herramientas de IA en uso— para identificar con precisión los vectores de vulnerabilidad. El análisis de riesgos no fue un trámite documental, sino el dispositivo central de toma de decisiones que orientó cada inversión, cada procedimiento y cada responsabilidad asignada. Sobre esa base se construyó la arquitectura del sistema: el Comité de Seguridad de la Información como órgano de gobierno permanente; la Declaración de Aplicabilidad como mapa de controles activos; y los indicadores de proceso como mecanismo de aprendizaje continuo integrado en los ciclos de revisión de la Asociación.

La dimensión humana del método fue tan determinante como la técnica. La concienciación y formación no se plantearon como una obligación de cumplimiento, sino como la palanca para **construir una cultura de seguridad** que cambia conductas, no solo firma documentos. Por eso se diseñaron itinerarios diferenciados: módulo presencial y módulos online evaluable para profesionales, píldoras periódicas de actualización y, en un ejercicio innovador, contenidos adaptados para que las personas con discapacidad intelectual comprendieran el impacto de la información y de la IA en su vida cotidiana y tomaran decisiones informadas sobre sus propios datos.

4.- Principales resultados obtenidos.

Los **resultados obtenidos se agrupan en cuatro ámbitos de impacto**:

A. Gobernanza organizacional y toma de decisiones

- Consolidación de un **modelo de gobernanza** que integra la ciberseguridad y la IA como dimensión propia del buen gobierno de la entidad.
- Mejora de la **calidad y trazabilidad de las decisiones** de la Junta Directiva, y equipo de direcciones gracias a información fiable, indicadores de seguimiento y una estructura de responsabilidades clara en el ámbito digital.
- Sistema de **gestión de buen gobierno robusto**, con órgano propio (Comité de Seguridad de la Información) y ciclo de revisión.
- Planes de actuación específicos para **mitigar los riesgos potenciales** identificados en ciberseguridad y uso de la IA.
- **Eficacia operativa**: mayor trazabilidad de la información, procesos de autorización más ágiles y reducción de incidencias no gestionadas.

B. Seguridad, cumplimiento normativo y protección legal

- **Reducción del riesgo de brechas de datos y ciberataques** mediante controles técnicos y organizativos documentados y auditados externamente.
- **Protección de los datos sensibles** de personas beneficiarias, familias, profesionales, asociados y órganos de gobierno.
- **Garantía de continuidad** del servicio ante incidentes en sistemas críticos.
- **Alineación plena con la legislación** vigente: RGPD, Reglamento del Esquema Nacional de Seguridad (ENS) y Reglamento Europeo de Inteligencia Artificial.
- **Prevención de sanciones económicas significativas** y atenuación o exención de responsabilidad penal ante posibles incumplimientos.

C. Cultura interna, formación y capacitación

- **Formación** de las personas trabajadoras en seguridad de la información, y uso responsable de IA con evaluación de contenido y registro de superación.
- Construcción de una **cultura de responsabilidad proactiva**: la seguridad de la información pasa de obligación técnica a valor compartido por toda la organización.
- **Formación adaptada e inclusiva** para personas con discapacidad intelectual sobre el impacto de la IA en su vida y sus derechos digitales.
- **Efecto disuasorio** generalizado ante la percepción de controles claros y responsabilidades asumidas por todas las partes.

D. Reputación, confianza y sostenibilidad

- **Prevención activa del riesgo reputacional**: la Asociación actúa antes del incidente, no como respuesta a él.
- **Aumento de la confianza de todos los grupos de interés**: personas, familias, profesionales, asociados, financiadores y administraciones, al saber que sus datos están protegidos con los más altos estándares.
- **Mayor credibilidad y diferenciación positiva** ante financiadores y administraciones: APROSU es la primera entidad del sector social certificada en el ENS en Canarias y sin referentes similares en Plena inclusión.
- **Mejora de la imagen de marca** como entidad pionera y referente en gobernanza digital en el tercer sector.
- **Garantía de sostenibilidad a largo plazo**, protegiendo el activo más valioso de la Asociación —la información— y la confianza que sus grupos de interés depositan en ella.

5.- Justificación del cumplimiento de los criterios de valoración expuestos en el documento “Bases de Participación”

a. Necesidad. Como ya se explicó, la práctica surge del desarrollo tecnológico muy acelerado, el auge del uso de la IA en el día a día de nuestro trabajo, multiplicando los puntos por donde fluye información de las personas con discapacidad, sus familias y profesionales, poniendo en riesgo la seguridad de la información y el buen uso de la IA. La necesidad fue identificada y liderada desde la propia Gerencia, que la asumió como una cuestión de buen gobierno, no como una exigencia externa, convirtiendo esta decisión en el punto de partida de un nuevo modelo de gestión de sus órganos de gobierno en el ámbito digital.

b. Contribución a la sostenibilidad. Gobernar bien el activo principal de la asociación y construir activamente la confianza de sus grupos de interés son dos de las palancas más directas de sostenibilidad. Esta práctica actúa sobre ambas simultáneamente: reduce riesgos legales y reputacionales, fortalece vínculos con personas, familias, profesionales y financiadores, y amplía la capacidad de gobierno.

c. Carácter innovador. Enmarcar la gobernanza de la información y la IA desde la lógica del activo estratégico y la confianza como valor añadido, además del cumplimiento normativo es una aproximación singular en el sector. En la web del registro del ENS no hay entidad del sector certificada en Canarias. La práctica se inscribe en la Categoría 1, Gobernanza y liderazgo, subcategoría “Modelos de gestión de órganos de gobierno que mejoran la calidad de las decisiones”, siendo hasta la fecha la única práctica documentada en Plena inclusión que aborda la gobernanza digital como modelo integral de gobierno corporativo.

d. Basada en evidencias. La práctica se sustenta en evidencias reales, tales como los documentos trabajados, esto es, análisis de riesgos, políticas, procedimientos, normativas elaboradas y aprobadas por Junta Directiva y Comité de seguridad de información, actas del Comité, Charlas, formación, material del módulo formativo, material formativo adaptado: La IA en nuestra vida, subvención del Kit Consulting, auditoría interna y externa, informe de auditorías, etc.

e. Garantías de continuidad. La implantación del Sistema de Gobernanza de seguridad se ha implantado para dar continuidad y así permitir la sostenibilidad de la Asociación. Este sistema tiene como objetivo garantizar la continuidad del

negocio previniendo cualquier ciberataque que ponga en peligro la seguridad de la información o las multas elevadas por la falta de seguridad de la información.

f. Participación de personas con discapacidad y familias. Las personas con discapacidad intelectual no fueron objeto de la práctica: fueron agentes de ella. Participaron en el análisis real de los usos tecnológicos que ya estaban haciendo en su día a día, sus conexiones con la wifi de los centros, aportando información de primera mano que ningún diagnóstico externo podría haber obtenido. Recibieron formación específica y adaptada sobre seguridad de la información e inteligencia artificial, y posteriormente actuaron como formadores de sus propios compañeros/as: La IA en nuestra vida, trasladando los contenidos desde su propia experiencia. Además, Su contribución no fue simbólica: fue la que hizo que el sistema de gobernanza digital de APROSU tuviera sentido también para las personas a quienes apoya.

g. Carácter sistemático. El proceso tiene fases definidas, indicadores de proceso y resultado diferenciados por grupos de interés, estructura de responsabilidad clara y revisión periódica consolidada e integrado en el sistema de gestión de la Asociación. La memoria anual y evaluaciones externas actúan como mecanismo de cierre del ciclo de rendición de cuentas. Los indicadores de seguimiento del sistema incluyen: tasa de cumplimiento de la formación (objetivo: 100% de la plantilla); % de personas con discapacidad formadas (100% de los que hacen uso de móviles y dispositivos), número de incidencias de seguridad reportadas por profesionales y tiempo medio de resolución; porcentaje de controles del ENS implementados sobre el total declarado en la Declaración de Aplicabilidad; Importe en € de implantación del sistema, importe en € de pagos para uso de IA, nº de no conformidades en auditorías internas y externas, etc. Estos indicadores son evaluados mensual, trimestral, semestral y anualmente por el Comité de Seguridad y presentados ante el equipo de direcciones y a la Junta Directiva, que los utiliza como base para la toma de decisiones estratégicas.

h. Transferibilidad. El modelo es transferible en su totalidad o por partes, adaptándose a las necesidades de cada entidad. Los elementos replicables incluyen: la metodología de diagnóstico inicial basada en análisis de riesgos; la estructura del Comité de Seguridad de la Información y sus normas de funcionamiento; el sistema de indicadores, los materiales formativos, incluidos los adaptados para personas con discapacidad intelectual.

j. Revisión periódica. La revisión periódica está garantizada porque se ha integrado en el sistema de gestión y adaptado a la revisión del modelo de la Asociación, esto es, mayo y octubre, así como anualmente con la evaluación de resultados. Ya se han producido actualizaciones concretas, lo que demuestra que el sistema aprende y se adapta.

k. Novedad. Esta práctica no ha sido presentada en ningún congreso, jornada o evento similar de Plena inclusión con anterioridad.

6.- Conclusiones

¿En qué medida la práctica ha tenido impacto en sostenibilidad de la entidad y le ha permitido avanzar?

Gobernar bien en el siglo XXI significa gobernar también lo digital. La Asociación APROSU ha dado ese paso: ha incorporado la ciberseguridad y la IA a su modelo de buen gobierno con la misma exigencia con la que gestiona sus finanzas, sus personas o sus servicios.

El **impacto** no es solo normativo, aunque el cumplimiento del Esquema Nacional de Seguridad es ya un hecho, sino **estratégico**: la entidad ha ganado **capacidad para tomar decisiones sobre su ecosistema tecnológico con criterio, datos y responsabilidad distribuida**.

Lo más transformador no ha sido instalar herramientas ni redactar políticas: ha sido el cambio en la **cultura interna**. Cuando una organización del tercer sector es capaz de formar al 100% de sus profesionales en seguridad de la información, y en uso de IA, adaptar esos contenidos para que las personas con discapacidad intelectual comprendan sus derechos digitales, y poder rendir cuentas sobre el estado del sistema, ha producido algo más profundo que cumplimiento: ha producido **consciencia institucional**. Eso es lo que distingue una buena práctica de un trámite.

En términos de **sostenibilidad**, el retorno es múltiple y acumulativo: reduce la exposición a sanciones cuantiosas, protege el activo más frágil y decisivo, la información de las personas, diferencia a la Asociación ante administraciones y financiadores, y genera un efecto de confianza que ninguna campaña de imagen puede sustituir. APROSU entra así en un pequeño grupo de entidades del tercer sector y/o empresas en España que han decidido no esperar a sufrir un incidente para actuar. Esa anticipación, convertida en sistema, es precisamente la definición más honesta de sostenibilidad.