Fundada en 1998, **TAYA** (**Tesorería, Análisis y Aplicaciones**) es una empresa española dedicada al desarrollo de aplicaciones informáticas financieras especializadas en la gestión de la Tesorería y del Endeudamiento para empresas y entidades de administración pública. Nuestras herramientas y desarrollos permiten a los equipos financieros centrarse en actividades de gestión, evitando así tareas rutinarias y repetitivas.

TAYA asume su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de la misma, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

- ✓ Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- ✓ Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones
- ✓ Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- ✓ Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, así como la protección de los datos personales y los sistemas de información contra accesos indebidos y modificaciones no autorizadas.

Para poder lograr estos objetivos es necesario:

- ✓ **Mejorar continuamente** nuestro sistema de seguridad de la información
- ✓ Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribamos además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos. El marco legal y regulatorio en el que desarrollamos nuestras actividades es:
    - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
    - 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.
- 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) No 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 y por la que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- Norma de referencia ISO/IEC 27001:2022 para la definición del sistema de gestión de la seguridad de la información.
- El SGSI de TAyA se mantendrá cumpliendo y respetando la Ley de Propiedad Intelectual en lo que se refiere al uso del software, obteniendo las licencias correspondientes y llevando un registro y control de estas para el empleo adecuado de éstas en el desarrollo de las actividades

✓ Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.

✓ Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.

✓ Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.

✓ Evaluar y garantizar la **competencia técnica del personal**, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos,

proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.

- ✓ Garantizar el **correcto estado de las instalaciones y el equipamiento** adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- ✓ Garantizar un **análisis** de manera continua de todos los **procesos relevantes**, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- ✓ Estructurar nuestro sistema de gestión de forma que sea fácil comprender. Nuestro sistema de gestión tiene la siguiente estructura:

La documentación del sistema estará disponible en nuestros sistemas de información, en un repositorio al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

La Dirección de TAYA tiene como responsabilidad la de liderar y comprometerse con respecto al SGSI/ENS.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política de Seguridad de la Información.

La Política de Seguridad se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

Considerando las directrices desarrolladas en la Política de Seguridad de la Información ENS, se desarrollarán un conjunto de procedimientos operativos que permitan garantizar la

implantación de dichas directrices, y la consecución de los objetivos de la organización en materia de seguridad de la información.

b) Análisis y gestión de los riesgos.

Todos los sistemas sujetos a esta Política de Seguridad deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos, incluyéndose los derivados de la normativa de protección de datos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando cambien elementos relevantes del sistema
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

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

c) Gestión de personal.

La Dirección se asegurará que el personal dispone de la formación necesaria teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones.

Para lograr los objetivos de seguridad de la información todo el personal debe estar involucrado en el tratamiento y saber de qué forma se puede contribuir a su consecución.

Estas medidas se encuentran desarrolladas en el procedimiento de seguridad relativa a los recursos humanos.

d) Profesionalidad.

La Dirección deberá garantizar que el personal dispone del conocimiento y habilidades necesarias para el adecuado desempeño de sus funciones. Además, deberá proporcionar la formación necesaria cuando se detecten carencias en el cumplimiento de las actividades.

e) Autorización y control de los accesos.

Los sistemas de información deberán disponer de un mecanismo de control de accesos que limite su acceso a los usuarios y dispositivos que estén debidamente autorizados, restringiendo el acceso a las funciones que le son permitidas.

Las medidas de seguridad aplicadas se encuentran descritas en el procedimiento de control de acceso.

f) Protección de las instalaciones.

La organización deberá disponer de un conjunto de controles de acceso físico a las instalaciones, que permita limitar el acceso únicamente a las personas autorizadas a las zonas de almacenamiento y/o procesamiento de información confidencial.

Las medidas de protección se encuentran descritas en el procedimiento relativo a la seguridad física y del entorno.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

La adquisición de productos y servicios deberá considerar y garantizar el cumplimiento con los requisitos de seguridad establecidos por la Dirección, tal y como se detalla en el procedimiento relativo a adquisición, desarrollo y mantenimiento.

h) Mínimo privilegio.

Los sistemas deberán configurarse según las políticas y procedimientos de seguridad definidos. El procedimiento de seguridad de las operaciones desarrolla las medidas de seguridad que se deben aplicar a los sistemas de información en el que se considera siempre el principio de mínimo privilegio

i) Integridad y actualización del sistema.

Se deberán aplicar medidas que permitan conocer el estado de seguridad de los sistemas, y que permitan identificar y gestionar los riesgos de seguridad de los mismos. Estas medidas se encuentran desarrolladas en el procedimiento de seguridad de las operaciones.

j) Protección de la información almacenada y en tránsito.

Se deberán aplicar medidas de seguridad que permitan garantizar un adecuado nivel de protección de la información almacenada y en tránsito. Estas medidas se encuentran detalladas en el procedimiento de gestión de activos.

k) Prevención ante otros sistemas de información interconectados.

Se deberán analizar y gestionar los riesgos derivados de las conexiones de los sistemas de información con redes públicas, y aplicar las medidas necesarias de protección según el nivel de seguridad requerido por el sistema.

l) Registro de la actividad y detección de código dañino.

Los sistemas de información deberán contar con registros de actividad de los usuarios que permitan custodiar la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas. Además, se deberá disponer de sistemas que permitan la detección de código dañino.

m) Incidentes de seguridad.

Los sistemas de información deberán contar con un sistema de detección y reacción frente a código dañino. Además, existirá un registro de incidentes de seguridad que permitirá realizar un seguimiento de la resolución de los mismos y aplicar mejoras a través de las lecciones aprendidas.

n) Continuidad de la actividad.

Se deberán establecer, en la medida de lo posible y según el nivel de riesgo asociado, los mecanismos necesarios para garantizar la recuperación de la información y la continuidad de las operaciones.

o) Mejora continua del proceso de seguridad.

La Dirección deberá llevar a cabo una revisión periódica del sistema para asegurarse de su conveniencia, adecuación y eficacia continua. Ante la ocurrencia de cualquier desviación respecto a los resultados esperados, se deberá iniciar el proceso de tratamiento de la misma mediante los procesos establecidos.

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsable de la información	- Tomar las decisiones relativas a la información tratada
Responsable de los servicios	- Coordinar la implantación del sistema - Mejorar el sistema de forma continua - Categorizar los servicios
Responsable de la seguridad	- Determinar la idoneidad de las medidas técnicas - Proporcionar la mejor tecnología para el servicio
Responsable del sistema	- Coordinar la implantación del sistema - Mejorar el sistema de forma continua
POC (Punto o Persona de Contacto)	- Actúa como responsable de seguridad del servicio prestado o solución provista
Dirección	- Proporcionar los recursos necesarios para el sistema - Liderar el sistema

Esta definición se completa en los perfiles de puesto y en los documentos del sistema.

El procedimiento para su designación y renovación será la ratificación en el comité de seguridad. El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité. Los miembros del comité de seguridad de la información son:

- Responsable de la información.

- Responsable de los servicios.
- Responsable de la seguridad.
- Responsable del sistema.
- Dirección Empresa (socios-administradores)

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa.

En TAyA está contemplado el uso de herramientas de IA, que se regirá por los siguientes principios básicos:

1. Transparencia y responsabilidad: Las decisiones y procesos impulsados por IA deben ser comprensibles y rastreables, informando siempre al usuario sobre la utilización de la IA en el procesamiento de datos personales. La organización es responsable del uso de la IA y debe garantizar que los sistemas implementados actúen conforme a los principios éticos y legales.
2. Justicia y no discriminación: Los sistemas de IA no deben generar discriminaciones indebidas. Los modelos de IA deben ser diseñados y entrenados para evitar sesgos que puedan perjudicar a ciertos grupos o individuos.
3. Seguridad: Las herramientas de IA deben ser implementadas con controles de seguridad adecuados, previniendo el acceso no autorizado, la manipulación de datos y cualquier otro tipo de vulnerabilidad.
4. Protección de la privacidad y datos personales: En cumplimiento con las regulaciones de protección de datos, las herramientas de IA deben ser diseñadas para proteger la privacidad por diseño y por defecto. Los datos personales deben ser minimizados, anonimizados o seudonimizados siempre que sea posible.
5. Supervisión humana: Aunque las herramientas de IA pueden automatizar ciertos procesos, las decisiones críticas, especialmente aquellas que impacten en los derechos de las personas, deberán contar con la intervención y revisión humana.

Terceras partes

Cuando TAYA preste servicios a otras entidades o maneje información de otras, se les hará partícipes de este Manifiesto de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando TAYA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de este Manifiesto de Seguridad de la Información y de la Normativa de Seguridad complementaria que ataña a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos realizado al tercero.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las guías que las desarrollan.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que TAYA pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en este Manifiesto o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto del Manifiesto no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe que precise los riesgos en los que se incurren y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

Gestión de incidentes de seguridad

TAYA dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios. Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados

Coordinación Resolución de Conflictos

La Coordinación se lleva a cabo en el seno del Comité de Seguridad.

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección General.

Está política se complementa con el resto de políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

Madrid, a 19 de septiembre de 2025