POL-CORP-SEC-001 - Política de Seguridad de la Información de Anjana Data

Anjana Data · Security & Compliance

Código	POL-CORP-SEC-001	**Versión**	2.1 (13/02/2026)
Estado	VIGENTE	**Clasificación**	PÚBLICO
Equipo	Security	**Próxima revisión**	2027-06-01
Cumplimiento	ENS RD 311/2022 (org.1, org.2, org.3, org.4) · ISO/IEC 27001:2022 (5.1, 5.2) · CCN-STIC-805 · Reglamento UE 2024/1689 (AI Act)		
Aprobado por	CSI - S-ACTA-CSI-2026-01 (13/02/2026), Acuerdo 4		

1. Objeto

Anjana Data es una empresa tecnológica española especializada en el desarrollo y comercialización de Anjana Data Platform (Gobierno del Dato & Analytics). Esta política establece los principios y directrices de obligado cumplimiento para la protección de la información y los servicios de Anjana Data. Su objetivo es garantizar la **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (CIDA+T)** de los sistemas de información y los servicios prestados, conforme al Esquema Nacional de Seguridad (ENS RD 311/2022) y la norma ISO/IEC 27001:2022.

La seguridad de la información es una responsabilidad de toda la organización, liderada por la Dirección y gestionada operativamente por el equipo de Security & Compliance.

2. Alcance

Parametro	Descripción
En alcance	Todos los sistemas de información que soportan el desarrollo, gestión y prestación (IaaS/PaaS/SaaS), mantenimiento y mejora de Anjana Data Platform. Incluye infraestructura cloud (AWS), entornos SaaS de clientes, sistemas corporativos internos y herramientas de desarrollo.
Fuera de alcance	Sistemas de información propios de clientes; entornos personales no corporativos de empleados fuera del perimetro de seguridad.

Parametro	Descripción
Aplicabilidad	Todo el personal de Anjana Data (empleados, becarios), contratistas y terceros con acceso a sistemas o información bajo alcance. Esta política aplica con independencia del tipo de contrato o vinculo con Anjana Data.

3. Marco normativo y referencias

Referencia	Descripción
ENS RD 311/2022	Controles org.1 (Política de seguridad), org.2 (Normativa de seguridad), org.3 (Procedimientos de seguridad), org.4 (Procesos de autorización)
ISO/IEC 27001:2022	5.1 (Liderazgo y compromiso), 5.2 (Política de seguridad de la información)
RGPD (Reglamento UE 2016/679)	Protección de datos personales
LOPDGDD (Ley Organica 3/2018)	Garantias de los derechos digitales
Reglamento UE 2024/1689 (AI Act)	Uso de herramientas de inteligencia artificial en procesos internos de desarrollo. Anjana actua como deployer de herramientas de IA de riesgo minimo/limitado, siempre bajo supervisión humana como instancia final de validación.
CCN-STIC-805	Guía de política de seguridad de la información
CCN-STIC-808 (op.mon.3)	Vigilancia activa de amenazas e inteligencia de seguridad. Complementa los requisitos de monitorizacion continua para la detección proactiva de amenazas.
NOR-CORP-DOC-001	Marco documental corporativo Anjana Data (Confluence genint)
Documentación técnica complementaria	NOR-SEC-CLOUD-001, NOR-SEC-NET-001, NOR-SEC-DEV-001, POE-SEC-ACC-001 (Confluence SEC)

4. Roles y responsabilidades

Rol	Persona o unidad	Responsabilidad
Responsable de Seguridad	Ana Melcón Sanjuán ana.melcon@anjanadata.com	Propietaria de esta política. Aprobación formal, revisión periódica y supervisión de cumplimiento.
Responsable de la Información	Mario de Francisco Ruiz	Establece los requisitos de seguridad de la información. Aprobación del nivel de riesgo aceptable.
Responsable del Servicio	Antonio Jose Gomez Diaz	Determina los requisitos de seguridad de los servicios. Define RTO/RPO.
Responsable del Sistema	Antonio Jose Gomez Diaz	Opera y mantiene los sistemas de información. Implementa las medidas técnicas de seguridad. Reporta incidentes.
Delegado de Protección de Datos (DPD)	Mario de Francisco Ruiz	Supervisión del cumplimiento RGPD/ LOPDGDD. Punto de contacto con la AEPD.
Comité de Seguridad de la Información (CSI)	Dirección + Responsable de Seguridad + roles designados	Aprobación de la Política. Supervisión estrategica. Reunión cuatrimestral minimo.
Todo el personal	—	Conocimiento y cumplimiento de esta política en el ejercicio de sus funciones. Reporte de incidentes o sospechas.

5. Directrices de la política

5.1 Principios rectores

> **Principio 1 - CIDA+T:** Los activos de información de Anjana Data están protegidos frente a accesos no autorizados (Confidencialidad), modificaciones no autorizadas (Integridad), interrupcion del servicio (Disponibilidad), suplantacion de identidad (Autenticidad) y borrado de trazas (Trazabilidad).

> **Principio 2 - Seguridad integral y proporcionalidad:** La seguridad se concibe como un proceso integral que abarca elementos técnicos, humanos y organizativos. Las medidas implementadas son proporcionales al nivel de riesgo y a la criticidad de los activos protegidos.

> **Principio 3 - Gestión basada en riesgo:** La toma de decisiones de seguridad se basa en análisis de riesgos formales, periodicos y documentados. Las medidas de seguridad se calibran para reducir los riesgos a niveles aceptables por la Dirección.

> **Principio 4 - Prevención, detección, respuesta y recuperacion:** Anjana Data adopta un enfoque proactivo y reactivo: previene con controles técnicos y formativos; detecta mediante monitorizacion continua; responde con procedimientos documentados; y recupera los servicios conforme a los planes de continuidad.

> **Principio 5 - Función diferenciada:** La seguridad se gestiona desde roles claramente separados: Responsable de la Información (que proteger), Responsable del Servicio (requisitos del servicio), Responsable del Sistema (operación técnica) y Responsable de Seguridad (supervisión y control).

> **Principio 6 - Concienciacion y formación:** Todo el personal recibe formación periódica en seguridad. La cultura de seguridad es un activo de la organización y se fomenta continuamente.

> **Principio 7 - Mejora continua:** La efectividad de los controles se revisa al menos anualmente. Los incidentes, auditorias y cambios del entorno se utilizan como fuente de mejora.

> **Principio 8 - Seguridad en el ciclo de vida:** Los requisitos de seguridad se incorporan desde el diseño inicial de los sistemas y servicios (security by design & by default), y se mantienen durante todo su ciclo de vida.

5.2 Requisitos obligatorios

Análisis y gestión de riesgos

- Realizar análisis de riesgos formal al menos anualmente, con metodología documentada, inventario de activos y planes de tratamiento.
- Todo cambio significativo en sistemas, arquitectura o procesos requiere evaluación de impacto en seguridad previa.
- El nivel de riesgo residual aceptable es aprobado por el Comité de Seguridad de la Información (CSI).
- Los planes de tratamiento de riesgos se revisan y actualizan trimestralmente.

Control de accesos e identidades

- Aplicar el principio de minimo privilegio: los accesos se otorgan en función de la necesidad operativa demostrada.
- Todo acceso a sistemas requiere autenticación; los accesos privilegiados o remotos requieren autenticación multifactor (MFA).
- Los derechos de acceso se revisan al menos trimestralmente.

- Los accesos de empleados dados de baja se revocan en un plazo maximo de 24 horas. Procedimiento: POE-SEC-ACC-001.

Gestión de incidentes de seguridad

- Cualquier incidente real o sospecha de incidente debe comunicarse al equipo de Security de forma inmediata.
- Los incidentes con impacto en datos personales se notifican a la AEPD dentro de las 72 horas desde su conocimiento (RGPD Art. 33).
- Los incidentes significativos con impacto en la continuidad del servicio se notifican a INCIBE-CERT en un plazo maximo de 72 horas (ENS op.exp.9 / NIS2). Procedimiento: POE-SEC-INC-001.
- Se mantiene un registro de todos los incidentes para análisis forense y mejora continua.

Continuidad del servicio

- Anjana Data mantiene un Análisis de Impacto al Negocio (BIA) actualizado, con RTO y RPO definidos.
- Los planes de contingencia se prueban al menos anualmente. Copias de seguridad: POE-IT-BKP-001. Plan de Continuidad: POE-CORP-CONT-001.

Gestión de proveedores y terceras partes

- Los proveedores con acceso a sistemas o información de Anjana Data deben conocer y aceptar está Política.
- Los contratos con terceros incluyen clausulas de seguridad, confidencialidad y auditoria.
- Procedimiento: POE-CORP-PRV-001 Procedimiento de Gestión de Proveedores v2.0.

Formación y concienciacion

- Todo el personal recibe formación en seguridad de la información al menos una vez al año.
- El programa cubre como minimo: phishing, gestión de contraseñas, clasificación de la información e incidentes.
- Procedimiento: POE-SEC-FORM-001.

Monitorizacion, auditoria y vigilancia (op.mon.3)

- Los sistemas de información bajo alcance disponen de registro de actividad (logs) con retención minima de 12 meses.
- Se realiza una auditoria interna de seguridad al menos anualmente.
- Anjana Data mantiene vigilancia activa de amenazas conforme a op.mon.3 (CCN-STIC-808): monitorizacion continua de indicadores de compromiso, alertas de inteligencia de amenazas y revisión periódica de la postura de seguridad.
- Anjana Data somete sus sistemas al proceso de certificación ENS conforme al calendario definido.

Protección de la información

- La información se clasifica en cuatro niveles: PUBLICO / INTERNO / CONFIDENCIAL / RESERVADO (ver NOR-CORP-DOC-001 §5).
- Las comunicaciones con información clasificada como CONFIDENCIAL o superior se cifran en transito y en reposo.
- Los datos personales se tratan conforme al RGPD y la LOPDGDD.

Desarrollo seguro y gestión del cambio

- Los cambios en sistemas de producción siguen el procedimiento de gestión del cambio documentado. Procedimiento: POE-CORP-CHG-001.
- Los requisitos de seguridad se incorporan desde las fases iniciales del desarrollo (security by design).
- El código producido sigue las buenas prácticas de NOR-SEC-DEV-001.

Uso de herramientas de inteligencia artificial

- Anjana Data utiliza herramientas de IA generativa como apoyo a procesos internos de desarrollo de software. Su uso queda limitado a procesos internos: no se emplean en interacciones directas con clientes ni en decisiones autonomas sobre personas.
- Todo output generado por herramientas de IA es revisado y validado por un profesional de Anjana Data antes de incorporarse a cualquier entregable o proceso finalizado (supervisión humana como instancia final).
- En el marco del Reglamento UE 2024/1689 (AI Act), Anjana actua como deployer de herramientas de riesgo minimo/limitado. A medida que la plataforma incorpore capacidades de gobernanza de IA, esta política se actualizara para reflejar las Obligaciones correspondientes.

> **Prácticas expresamente prohibidas (no exhaustivo):** compartir credenciales de acceso; instalar software no autorizado; acceder a información fuera del ámbito de las funciones del usuario; realizar escaneos de red sin autorización expresa; establecer conexiones remotas desde equipos personales a sistemas corporativos sin VPN corporativa autorizada; usar herramientas de IA para interactuar con clientes o terceros sin autorización expresa del Responsable de Seguridad.

6. Cumplimiento y excepciones

Excepciones

Cualquier excepción a esta política debe ser:

- Solicitada formalmente al Responsable de Seguridad con justificacion técnica o de negocio documentada.
- Aprobada por escrito antes de su Aplicación.
- Documentada con plazo de vigencia maximo (no superior a 12 meses) y medidas compensatorias.

- Revisada periódicamente. Las excepciones no renovadas expiran automaticamente.

Incumplimiento

El incumplimiento de esta política podrá conllevar:

- Revisión disciplinaria conforme al reglamento interno de Anjana Data.
- Escalado al equipo Legal en caso de incumplimiento de Obligaciones legales o contractuales.
- Suspension temporal de accesos hasta la regularizacion.

> **Auditoria:** El cumplimiento de esta política será verificado periódicamente por el equipo de Security & Compliance y, en el marco de la certificación ENS, por auditores externos acreditados.

7. Revisión

Esta política se revisa al menos anualmente, y siempre ante cambios significativos en la organización, sistemas, normativa aplicable o resultados de auditoria. La fecha de próxima revisión se indica en la cabecera. La revisión es responsabilidad del Responsable de Seguridad, con aprobación del Comité de Seguridad de la Información (CSI).

8. Historial de cambios

Versión	Fecha	Autor	Cambios	Aprobador
1.0	19/12/2023	Anjana CS - Responsable del Sistema	Creación del documento.	Comité de Seguridad de la Información (CSI)
2.0	23/10/2024	Security & Compliance	Actualización al marco NOR-CORP-DOC-001 v1.6; recodificación a POL-CORP-SEC-001; reestructuración de secciones; actualización de referencias a documentación vigente; adición campo Clasificación (INTERNO); eliminación de secciones obsoletas de V1.0.	Antonio Gómez / Ana Melcón Sanjuán

Versión	Fecha	Autor	Cambios	Aprobador
2.1	13/02/2026	Antonio Gomez	Adición Reglamento UE 2024/1689 (AI Act) en §3 y §5: uso de herramientas IA internas bajo supervisión humana, rol deployer riesgo minimo/limitado. Adición CCN-STIC-808 (op.mon.3) en §3 y §5: vigilancia activa de amenazas. Adición referencia NIS2/op.exp.9 en §5 gestión incidentes (notificación INCIBE-CERT 72h). Actualización roles §4 con personas designadas.	Antonio Jose Gomez Diaz

Aprobación

> **Aprobado por el Comité de Seguridad de la Información (CSI)**
>
> Acta de referencia: S-ACTA-CSI-2026-01 (13/02/2026).
> Autor y proponente: Responsable de Seguridad (Ana Melcón Sanjuán). Revisado por el Responsable del Sistema (Antonio José Gómez Díaz).
>
> Las políticas no requieren firma individual. La aprobación queda acreditada mediante el acta del CSI referenciada.