civitphone

2026

SGSI01-Política de Seguridad de la Información

PROPIEDADES DEL DOCUMENTO

Fecha de creación:	Julio de 2026	Nombre del fichero:	SGSI01-PS_CIVITPHONE
Destinatario documento:	CIVITPHONE	Número de páginas:	17
Clasificación documento:	*PÚBLICA*		
Nombre del documento:	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		
Versión actual:	1.0		
Resumen:	Política que establece el marco general de gestión de la seguridad de la información en CIVITPHONE, S.L., definiendo los principios, objetivos, roles y responsabilidades para proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y los servicios digitales de la organización.		

CONTROL DE REVISIONES		
APELLIDOS, NOMBRE	FECHA	FIRMA
Elaborado por: Raúl Gisbert Rodas	01/07/2026	
Revisado por: Jordi Gisbert Rodas	01/07/2026	
Aprobado por: Dirección	01/07/2026	
Otros:		

HISTORIAL DE REVISIONES			
VERSIÓN	FECHA	AUTOR	DETALLES
1.0	Julio 2026		Primera versión formal

Índice

Contenido

1. Aprobación y entrada en vigor

Texto aprobado el día **01 de JULIO de 2026** por el **Comité de Seguridad de la Información de CIVITPHONE, S.L.**

La presente Política de Seguridad de la Información (en adelante, "la Política") será efectiva desde la fecha de aprobación y permanecerá vigente hasta su sustitución por una nueva versión aprobada formalmente.

Cualquier modificación deberá ser validada y aprobada por el Comité de Seguridad de la Información.

2. Introducción

CIVITPHONE, S.L. (en adelante CIVITPHONE) depende de sus sistemas de información, inteligencia artificial y plataformas digitales para desarrollar su actividad y alcanzar sus objetivos estratégicos.

Estos sistemas son activos esenciales que deben gestionarse con diligencia y bajo un marco de seguridad que garantice su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, protegiéndolos frente a daños accidentales o deliberados que puedan comprometer la información o los servicios prestados.

La evolución tecnológica y las nuevas formas de amenaza exigen una estrategia dinámica, capaz de adaptarse al entorno y garantizar la continuidad operativa de los servicios.

Para ello, CIVITPHONE adopta las medidas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), estableciendo los mecanismos necesarios para su adecuación progresiva conforme a los principios, requisitos y medidas recogidos en dicho marco normativo.

La categorización del sistema y la determinación de las medidas aplicables se realizarán en fases posteriores del proceso de adecuación, conforme a lo establecido en el Anexo I del Real Decreto 311/2022.

La seguridad de la información se integra en todo el ciclo de vida de los sistemas desde su diseño y desarrollo hasta su operación y retirada, incorporando controles preventivos, técnicos y organizativos en cada etapa.

Los requisitos de seguridad y las necesidades de financiación se incluyen en la planificación y en todos los procesos de adquisición, licitación o contratación relacionados con sistemas TIC o servicios basados en inteligencia artificial.

El objetivo final de la seguridad de la información en CIVITPHONE es garantizar la calidad, fiabilidad y continuidad de sus servicios digitales, aplicando un enfoque proactivo que permita prevenir, detectar, responder y recuperar eficazmente ante cualquier incidente, conforme a los principios del artículo 7 del ENS.

2.1. Prevención

Con el fin de evitar incidentes que afecten a la información o a los servicios, CIVITPHONE implementará las medidas de seguridad establecidas por el ENS y aquellas adicionales que resulten necesarias según los resultados del análisis de riesgos.

Estas medidas, junto con las responsabilidades asociadas a cada rol, estarán claramente definidas y documentadas dentro del sistema de gestión de seguridad.

Para garantizar el cumplimiento efectivo de la Política, CIVITPHONE:

- Autorizará formalmente los sistemas antes de su puesta en producción.
- Evaluará de forma continua la seguridad, incluyendo los cambios de configuración realizados en los entornos TIC.
- Promoverá la revisión y auditoría independiente, para asegurar la objetividad de las evaluaciones.
- Fomentará la concienciación y formación del personal en materia de ciberseguridad y buenas prácticas.

2.2. Detección

CIVITPHONE dispondrá de mecanismos técnicos y operativos destinados a detectar desviaciones o anomalías en la prestación de los servicios y en la integridad de los sistemas de información.

Estas medidas permitirán identificar comportamientos no habituales, analizar su impacto y notificar los hallazgos a los responsables de seguridad.

De acuerdo con el artículo 9 del ENS, CIVITPHONE llevará a cabo reevaluaciones periódicas y mantendrá un sistema de monitorización continua para la detección temprana de incidentes o vulnerabilidades relevantes.

2.3. Respuesta

En caso de incidente, CIVITPHONE activará los procedimientos de respuesta definidos, que incluirán:

- Mecanismos de actuación inmediata para mitigar los efectos del incidente.
- Designación de un punto de contacto operativo para la coordinación de la respuesta.
- Protocolos de comunicación interna y externa, incluyendo el intercambio de información con los Equipos de Respuesta ante Emergencias (CERT/CCN-CERT) y otros organismos competentes.
- Acciones de contención, análisis y restauración del servicio, garantizando la documentación de las actuaciones y la incorporación de las lecciones aprendidas al proceso de mejora continua.

2.4. Recuperación

Para garantizar la disponibilidad de los servicios, CIVITPHONE establecerá los medios y procedimientos necesarios que aseguren la recuperación oportuna de los servicios críticos ante cualquier incidente o contingencia.

3. Misión de CIVITPHONE

La misión de CIVITPHONE, S.L. es proporcionar asistencia telefónica con IA, accesible para todos.

La seguridad de la información constituye un requisito esencial para garantizar la confianza, la calidad y la continuidad de dichos servicios.

Por ello, CIVITPHONE establece un marco de seguridad integral que protege los activos de información, los sistemas tecnológicos, los algoritmos de inteligencia artificial y los datos tratados, asegurando su correcta gestión durante todo el ciclo de vida de los sistemas.

4. Principios Básicos

1. **Compromiso directivo**: la dirección asume la seguridad de la información como elemento estratégico de negocio.
2. **Responsabilidad definida:** cada rol del ENS (responsable de Seguridad, del Sistema, de la Información y del Servicio) tendrá funciones formalmente asignadas.

3. **Seguridad integral y por diseño:** la seguridad será considerada desde el diseño y durante todo el ciclo de vida de los sistemas.
4. **Gestión del riesgo:** todas las decisiones se basarán en la identificación, análisis y tratamiento de los riesgos.
5. **Proporcionalidad:** las medidas se aplicarán en función de la categoría del sistema y los riesgos asociados.
6. **Mejora continua:** revisión y actualización constante del marco de seguridad.
7. **Seguridad por defecto**: los servicios se configurarán con el máximo nivel de protección desde su puesta en marcha.
8. **Cumplimiento normativo:** CIVITPHONE se compromete a cumplir el ENS, el RGPD, la LOPDGDD, el Reglamento de IA y el resto de normativa aplicable en materia de seguridad y protección de datos.

5. Objetivos de seguridad de la información

CIVITPHONE establece los siguientes objetivos estratégicos:

- Proteger la información frente a accesos, usos o divulgaciones no autorizadas.
- Garantizar la disponibilidad continua de los servicios de IA y las plataformas de las plataformas de asistencia telefónica
- Asegurar la integridad y trazabilidad de los modelos y datos utilizados.
- Cumplir con el ENS, el RGPD, la LOPDGDD y demás normativa aplicable.
- Promover la cultura de ciberseguridad y responsabilidad compartida entre el personal y los proveedores.
- Mejorar de forma continua la eficacia del Sistema de Gestión de Seguridad de la Información.
- Garantizar que los sistemas de inteligencia artificial de CIVITPHONE se diseñan, desarrollan y operan conforme a principios de seguridad, gestión del riesgo y cumplimiento normativo, alineados con el Reglamento (UE) 2024/1689 y las normas de referencia en gestión de riesgos e IA (ISO/IEC 23894 e ISO/IEC 42001).

6. Alcance

Esta Política se aplica a todos los **sistemas de información, activos, servicios y procesos** de CIVITPHONE, S.L. que gestionen información o soporten funciones necesarias para el desarrollo de su actividad y la prestación de sus servicios digitales.

Afecta a **todo el personal con acceso autorizado a los sistemas de información**, con independencia de la naturaleza de su relación contractual o profesional con

CIVITPHONE, incluyendo empleados, colaboradores, contratistas y proveedores externos que intervengan en el tratamiento, mantenimiento o gestión de la información.

Todos ellos tienen la **obligación de conocer, respetar y cumplir** lo establecido en esta Política y en la normativa de seguridad derivada.

Es responsabilidad del **Comité de Seguridad** de la Información disponer los medios necesarios para asegurar que esta Política sea **difundida, comprendida y aplicada** por todas las partes afectadas.

7. Marco normativo

El marco normativo en que se desarrollan las actividades de CIVITPHONE, S.L., y en particular la prestación de sus servicios digitales y electrónicos está integrado por las siguientes normas y marcos de referencia:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- 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 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y su desarrollo mediante el Real Decreto 43/2021, de 26 de enero.
- Directiva (UE) 2022/2555, del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS 2).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, en lo que resulte aplicable a la colaboración y prestación de servicios digitales a administraciones públicas.
- Reglamento (UE) 2024/1689, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.

- Reglamento (UE) 2022/2065, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales.
- Reglamento (UE) 2022/1925, de 14 de septiembre de 2022, sobre mercados digitales.
- Guías CCN-STIC del Centro Criptológico Nacional, especialmente:
    - Serie 800 (marco organizativo del ENS).
    - Serie 900 (medidas de seguridad).
    - CCN-STIC-801 (responsabilidades y funciones en el ENS).
- Norma ISO/IEC 27001:2022, sobre sistemas de gestión de la seguridad de la información.
- Norma ISO/IEC 22301:2019, sobre sistemas de gestión de la continuidad del negocio.
- Norma ISO/IEC 23894:2023, sobre gestión de riesgos en inteligencia artificial.
- Norma ISO/IEC 42001:2023, sobre sistemas de gestión de inteligencia artificial.
- Normativa interna ENS-CIVITPHONE, compuesta por los procedimientos, instrucciones técnicas y registros aprobados por el Comité de Seguridad de la Información.

- Las normas y marcos de referencia de carácter voluntario (ISO/IEC 27001, 22301, 23894, 42001) se utilizarán como guía para la mejora continua del Sistema de Gestión de Seguridad de la Información y de la gestión de riesgos en inteligencia artificial.

Este marco servirá como base de cumplimiento y alineación normativa para CIVITPHONE, y será revisado periódicamente para garantizar su actualización conforme a las disposiciones legales, reglamentarias y técnicas que resulten de aplicación.

8. Organización de la seguridad de la información

8.1. Criterios organizativos

La organización de la seguridad de la información en CIVITPHONE, S.L. se estructura conforme a los principios y directrices del Esquema Nacional de Seguridad (ENS) y a las pautas definidas en la Guía CCN-STIC-801 “Responsabilidades y funciones en el ENS”.

Con el fin de garantizar una gestión eficaz y coherente de la seguridad, CIVITPHONE establece una estructura organizativa específica, compuesta por los roles y órganos necesarios para coordinar, supervisar y mejorar de forma continua la seguridad de la información.

Se designarán los siguientes roles en materia de seguridad de la información:

- Responsable del Servicio
- Responsable de la Información
- Responsable del Sistema
- Responsable de Seguridad
- Delegado/a de Protección de Datos (DPD)

Asimismo, se constituirá un Comité de Seguridad de la Información, como órgano colegiado de carácter consultivo y estratégico, encargado de coordinar las actuaciones en materia de seguridad y de impulsar la mejora continua del sistema.

8.2. Roles y responsabilidades

Responsable de la Información y del Servicio

- Determinar los requisitos de seguridad aplicables a la información y a los servicios.
- Aceptar los niveles de riesgo residual y comunicar las variaciones relevantes al Comité de Seguridad.
- Garantizar la correcta gestión de la información bajo su ámbito de responsabilidad.

Responsable de Seguridad

- Velar por el cumplimiento de esta Política y del marco ENS.
- Promover la formación y concienciación del personal.
- Coordinar los análisis de riesgos, la declaración de aplicabilidad y los planes de mejora de la seguridad.
- Gestionar auditorías internas y externas, y la relación con los organismos competentes.

Responsable de la Información

- Determinar los requisitos de seguridad aplicables a la información.
- Aprobar la clasificación de la información y sus niveles de protección.
- Aceptar el riesgo residual asociado a la información de su ámbito.

Responsable del Servicio

- Determinar los requisitos de seguridad aplicables al servicio.
- Aceptar los niveles de riesgo residual que afectan a la prestación del servicio.
- Garantizar la continuidad y calidad del servicio dentro de los niveles acordados.

Responsable del Sistema

- Asegurar la operación segura de los sistemas de información durante todo su ciclo de vida.
- Aplicar los controles técnicos de seguridad y mantener actualizados los sistemas y configuraciones.
- Coordinar la gestión de accesos, la monitorización de eventos y la detección de vulnerabilidades.
- Colaborar en la investigación y resolución de incidentes.
- Delegado/a de Protección de Datos (DPD)
- Supervisar el cumplimiento de la normativa vigente en materia de protección de datos personales.
- Asesorar sobre evaluaciones de impacto y principios de privacidad desde el diseño y por defecto.
- Cooperar con la Agencia Española de Protección de Datos y actuar como punto de contacto con ella.

Comité de Seguridad de la Información

- Coordinar la aplicación de esta Política y del conjunto normativo ENS-CIVITPHONE.
- Revisar y aprobar las propuestas en materia de seguridad de la información.
- Realizar el seguimiento de riesgos, incidentes y planes de mejora.
- Impulsar la formación y sensibilización del personal.
- Promover las auditorías periódicas de cumplimiento ENS y RGPD.

8.3. Procedimientos de designación

Los **nombramientos de los roles definidos y la constitución formal del Comité de Seguridad de la Información** se realizarán mediante **acta de constitución o resolución interna** aprobada por la Dirección de CIVITPHONE.

Dicha acta recogerá la composición, las funciones detalladas, la periodicidad de las reuniones y los criterios de revisión, evitando que esta Política deba modificarse ante cambios organizativos.

Una misma persona podrá asumir más de un rol, siempre que se garantice la independencia y el cumplimiento de las obligaciones asociadas.

9. Protección de datos personales

CIVITPHONE, S.L. únicamente tratará datos personales adecuados, pertinentes y limitados a las finalidades propias de sus servicios, garantizando en todo momento el cumplimiento del Reglamento (UE) 2016/679 (RGPD) y de la Ley Orgánica 3/2018 (LOPDGDD).

Se adoptarán las medidas técnicas y organizativas apropiadas para proteger los datos personales frente a su destrucción, pérdida, alteración o acceso no autorizado, asegurando su confidencialidad, integridad, disponibilidad y resiliencia.

Asimismo, CIVITPHONE integrará los principios de privacidad desde el diseño y por defecto en el desarrollo de sus productos y servicios, especialmente en aquellos que incorporen tecnologías de inteligencia artificial o tratamiento automatizado de información.

La organización contará con un delegado de Protección de Datos (DPD) que supervisará el cumplimiento de la normativa aplicable, asesorará a la Dirección y actuará como punto de contacto con la Agencia Española de Protección de Datos (AEPD).

La Política de Privacidad de CIVITPHONE complementará a la presente Política de Seguridad de la Información y estará publicada en la sede electrónica y en los canales oficiales de la organización.

10. Obligaciones del personal

Todo el personal de CIVITPHONE, S.L., así como los colaboradores, contratistas y proveedores que tengan acceso a la información o a los sistemas de la organización, deberán conocer, respetar y cumplir las normas establecidas en la presente Política de Seguridad de la Información y en la normativa derivada de la misma.

Para ello, CIVITPHONE garantiza que todas las personas con acceso a la información y a los sistemas:

- Recibirán formación y concienciación en materia de seguridad de la información y protección de datos personales, al menos una vez al año o cuando se produzcan cambios relevantes.
- Serán informadas de sus responsabilidades y obligaciones antes de asumir funciones que impliquen el acceso a información o recursos tecnológicos.
- Deberán utilizar los recursos TIC de forma responsable y conforme a los principios de confidencialidad, integridad, disponibilidad y trazabilidad.
- Están obligadas a comunicar de inmediato cualquier incidente, anomalía o vulnerabilidad detectada que pueda afectar a la seguridad o a la continuidad del servicio.
- Deberán cumplir los acuerdos de confidencialidad y uso responsable de los sistemas y activos de información.
- Evitarán la instalación, modificación o uso de software y herramientas no autorizadas.
- Conservarán y custodiarán adecuadamente las credenciales de acceso y los dispositivos asignados para el desempeño de sus funciones.
- El incumplimiento de las obligaciones descritas podrá dar lugar a las acciones disciplinarias o contractuales correspondientes, según lo establecido en la normativa laboral y los acuerdos internos de CIVITPHONE.

La Dirección y el Comité de Seguridad de la Información garantizarán que el personal dispone de los medios, formación y apoyo necesarios para cumplir con estas obligaciones, fomentando una cultura de seguridad y responsabilidad compartida en toda la organización.

Estas obligaciones serán de aplicación tanto en las instalaciones de CIVITPHONE como en los entornos de teletrabajo y acceso remoto, utilizando únicamente canales y dispositivos autorizados.”

11. Gestión de riesgos

Todos los sistemas estarán sujetos a un proceso formal de análisis y gestión de riesgos, conforme a las Guías CCN-STIC-803 y 804 y a los Anexos I y II del RD 311/2022.

El análisis se actualizará:

- Anualmente.
- Cuando se produzcan cambios relevantes en servicios o infraestructuras.
- Tras incidentes graves o vulnerabilidades críticas.

El responsable de Seguridad coordinará los análisis y propondrá las medidas de mitigación.

El Comité de Seguridad aprobará los planes de tratamiento de riesgos y las medidas compensatorias necesarias.

12. Gestión y notificación de incidentes

CIVITPHONE mantendrá un p**rocedimiento de gestión de incidentes** que incluirá mecanismos de detección, análisis, registro, respuesta y recuperación.

Los incidentes con impacto significativo se notificarán al **CCN-CERT** conforme al artículo 36 del RD 311/2022.

Se designará un punto de contacto oficial para la comunicación de incidentes y se mantendrán registros auditables de todas las actuaciones realizadas.

Cuando un incidente suponga una violación de la seguridad de los datos personales, CIVITPHONE seguirá los procedimientos de notificación establecidos en el RGPD y la LOPDGDD, incluyendo, en su caso, la comunicación a la Agencia Española de Protección de Datos y a los interesados afectados, dentro de los plazos legalmente establecidos.

13. Desarrollo normativo

La presente Política de Seguridad de la Información se desarrollará mediante un conjunto de normas, procedimientos e instrucciones técnicas que detallarán las medidas organizativas, operativas y tecnológicas necesarias para garantizar su aplicación efectiva dentro de CIVITPHONE, S.L.

Este marco normativo interno formará el Sistema de Gestión de la Seguridad de la Información (SGSI-ENS) y estará estructurado en tres niveles de desarrollo, de acuerdo con su ámbito y grado de detalle:

- **Nivel 1:** Política de Seguridad de la Información y Normativa general de seguridad.

- **Nivel 2:** Procedimientos y normas internas derivadas, aprobadas por el Comité de Seguridad de la Información (por ejemplo, gestión documental, control de accesos, arquitectura de seguridad, etc.).
- **Nivel 3**: Instrucciones técnicas, registros y guías operativas que especifican tareas concretas, controles de seguridad y mecanismos de verificación.

El Comité de Seguridad de la Información será el órgano responsable de la revisión, actualización y mantenimiento de este marco normativo, al menos una vez al año o cuando se produzcan cambios relevantes en los servicios, sistemas o requisitos legales aplicables.

Asimismo, la presente Política complementa y se coordina con la Política de Privacidad de CIVITPHONE, en materia de protección de datos personales, y con el resto de las políticas corporativas de la organización que contribuyan a mantener un entorno digital seguro y confiable.

14. Relaciones con terceros

Cuando CIVITPHONE **utilice servicios de terceros, colabore con otras entidades o ceda información a proveedores o socios tecnológicos**, dichos terceros quedarán sujetos a las obligaciones y compromisos de seguridad establecidos en esta Política y en la normativa interna.

En particular, CIVITPHONE:

- Exigirá a sus proveedores el **cumplimiento de medidas de seguridad equivalentes** a las adoptadas internamente, especialmente en materia de confidencialidad, protección de datos y gestión de incidentes.
- Incluirá en los **contratos y acuerdos de prestación de servicios** cláusulas específicas sobre seguridad de la información, confidencialidad y notificación de incidentes.
- Supervisará periódicamente el nivel de cumplimiento de los proveedores críticos mediante revisiones, auditorías o solicitudes de evidencias de conformidad.
- Coordinará la **gestión conjunta de incidentes de seguridad,** garantizando la comunicación y resolución eficaz entre las partes implicadas.
- Promoverá **la concienciación y formación básica en seguridad** para el personal externo o subcontratado que tenga acceso a los sistemas o datos de CIVITPHONE.

En los casos en que algún aspecto de esta Política no pueda ser cumplido por una tercera parte, el responsable de Seguridad elaborará un informe de riesgo residual, que deberá ser aprobado por el Comité de Seguridad de la Información antes de la contratación o continuidad del servicio.

Cuando un tercero trate datos personales por cuenta de CIVITPHONE, se formalizarán los correspondientes contratos de encargo de tratamiento conforme al artículo 28 del RGPD, definiendo de forma clara las instrucciones de tratamiento, las medidas de seguridad exigidas y el régimen de subcontratación.

15. Mejora continua

La gestión de la seguridad de la información en CIVITPHONE, S.L. se concibe como un proceso continuo de mejora y adaptación a los cambios tecnológicos, normativos y organizativos.

Para garantizar su eficacia y alineación permanente con el Esquema Nacional de Seguridad (ENS), CIVITPHONE llevará a cabo de forma periódica las siguientes acciones:

- Revisión y actualización de la presente Política de Seguridad de la Información y de la normativa derivada, para asegurar su vigencia y adecuación a la evolución de los servicios, riesgos y tecnologías empleadas.
- Evaluación periódica de riesgos, incluyendo la revisión de la categorización de los sistemas, los controles implantados y las medidas compensatorias, con el fin de mantener los riesgos en niveles aceptables.
- Ejecución de auditorías internas y externas, de acuerdo con la periodicidad establecida en el ENS, para verificar el cumplimiento de las medidas y detectar oportunidades de mejora.
- Análisis de incidentes de seguridad y lecciones aprendidas, aplicando los resultados para fortalecer las medidas de protección y respuesta.
- Revisión de los servicios, infraestructuras y proveedores, asegurando la coherencia con los principios y objetivos de seguridad definidos por la organización.
- Promoción de la formación, sensibilización y cultura de seguridad, fomentando la participación del personal en la mejora del sistema.

El Comité de Seguridad de la Información supervisará las actividades de mejora y propondrá a la Dirección las actualizaciones necesarias para mantener un nivel de seguridad adecuado, proporcional y sostenible en el tiempo.