1. INTRODUCCIÓN

SOMOSOCIALMEDIA, S.L. nace en 2010 en Málaga para dar respuesta a la necesidad de los clientes de ZIENideas de adaptarse a las nuevas tecnologías. Inicialmente centrada en diseño web y redes sociales, la organización ha evolucionado hacia una oferta de soluciones digitales 360, incorporando desarrollo a medida, consultoría tecnológica, automatización y servicios de ciberseguridad.

La Dirección entiende que el sistema de información que da soporte a la prestación de sus actividades es un activo fundamental. Dicho sistema soporta, en particular, la monitorización, detección, análisis y respuesta ante incidentes, vulnerabilidades y eventos de ciberseguridad, así como la ejecución de procesos automatizados.

La organización mantiene un compromiso firme con la protección de sus activos de información, la continuidad del negocio, la gestión de riesgos y el fortalecimiento de una cultura sólida de seguridad. Este compromiso se apoya en el equipo de personas de SOMOS.plus, en recursos humanos y técnicos adecuados, instalaciones seguras, experiencia probada en la gestión de soluciones de externalización y herramientas técnicas y de control.

La presente Política establece el marco de actuación necesario para proteger la información frente a amenazas internas o externas, deliberadas o accidentales, asegurando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Asimismo, regula las responsabilidades, principios y obligaciones aplicables a la seguridad de la información, incluyendo el cumplimiento normativo, la gestión de incidentes, la protección de datos personales, la relación con terceros y la mejora continua.

SOMOS.plus implanta, opera y mantiene un marco de seguridad integral alineado con UNE-ISO/IEC 27001:2023, el Esquema Nacional de Seguridad conforme al Real Decreto 311/2022, la Directiva NIS2 y demás normativa aplicable, con el objetivo de garantizar la resiliencia y continuidad de los servicios.

Los principios clave de esta Política son:

- **Enfoque basado en riesgos:** gestión sistemática y proactiva de amenazas y vulnerabilidades, aplicando defensa en profundidad y medidas de mitigación proporcionadas.
- **Cumplimiento normativo:** observancia de los requisitos legales, reglamentarios, contractuales y normativos aplicables a la seguridad de la información.
- **Mejora continua:** revisión, auditoría, actualización y mejora permanente del Sistema de Gestión de Seguridad de la Información y de los controles implantados.
- **Seguridad en la cadena de suministro:** exigencia a terceros y proveedores críticos de estándares de seguridad equivalentes a los de la organización.
- **Concienciación y reporte:** formación del personal y establecimiento de mecanismos de notificación obligatoria de incidentes, vulnerabilidades o anomalías de seguridad.

La Dirección valora especialmente la disponibilidad, confidencialidad e integridad de la información propia y de sus clientes como criterios esenciales para la estimación de riesgos y la toma de decisiones.

2. ALCANCE

Esta Política aplica a los sistemas de información, procesos, activos y servicios de SOMOS.plus incluidos en el ámbito de aplicación de ISO 27001, del Esquema Nacional de Seguridad y de la Directiva NIS2, asegurando la protección de activos críticos y la resiliencia operativa.

El alcance específico comprende el sistema de información que da soporte a los servicios de monitorización, detección, análisis y respuesta ante incidentes, vulnerabilidades y eventos de ciberseguridad en infraestructuras tecnológicas de clientes, sustentado en la plataforma Irishawk, así como a la ejecución de procesos automatizados, conforme con la declaración de aplicabilidad vigente.

La Política abarca:

- **Sistemas de información y procesos relacionados:** todos los sistemas que soportan los servicios anteriores, garantizando confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad.

- **Actividades de soporte:** gestión de incidentes, mantenimiento, actualización, protección de activos tecnológicos y supervisión de proveedores críticos.
- **Activos y procesos críticos:** identificación, clasificación, evaluación y tratamiento de riesgos conforme a las categorías de seguridad aplicables.
- **Cumplimiento legal, reglamentario y contractual:** aplicación de la legislación española y europea, así como de los compromisos con clientes y partes interesadas.
- **Declaración de aplicabilidad:** establecimiento y mantenimiento de una declaración de aplicabilidad alineada con ENS e ISO 27001, definiendo las medidas aplicables a los sistemas cubiertos.
- **Personas y partes interesadas:** extensión de los principios de seguridad al personal, proveedores, terceros y partes interesadas que accedan a sistemas o información de la organización.

3. MISIÓN

La misión de SOMOS.plus es identificar vulnerabilidades mediante herramientas especializadas y contribuir a su mitigación para reforzar la seguridad de los sistemas de información de las empresas. Para cumplir esta misión, la organización se compromete a:

- **Garantizar la seguridad de la información:** adoptar un enfoque integral basado en ISO 27001, ENS y NIS2 para proteger la información de clientes y datos internos frente a amenazas y vulnerabilidades.
- **Asegurar la gestión y protección de activos críticos:** aplicar medidas adecuadas para preservar confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- **Fomentar la mejora continua:** revisar y adaptar los procesos de seguridad ante nuevas amenazas, cambios regulatorios y necesidades del negocio.
- **Concienciar y capacitar al personal:** desarrollar programas de formación y sensibilización para consolidar una cultura de ciberseguridad.
- **Cumplir los requisitos legales, regulatorios y contractuales:** garantizar que todas las actividades y servicios se ejecutan conforme a las obligaciones aplicables.
- **Proteger la continuidad del negocio:** mantener planes de continuidad y recuperación ante desastres que aseguren la resiliencia de los servicios esenciales.

SOMOS.plus se orienta a ofrecer soluciones seguras e innovadoras a sus clientes, optimizando sus procesos y protegiéndolos frente a los riesgos inherentes al tratamiento de la información.

4. MARCO NORMATIVO

SOMOS.plus se compromete a cumplir la normativa aplicable a su actividad, incluyendo legislación general y específica en materia de seguridad de la información, ciberseguridad, comunicaciones electrónicas, propiedad intelectual y protección de datos.

4.1. Normativa nacional

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, en lo que resulte aplicable.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.
- Guías CCN-STIC, especialmente la serie 800, como referencia técnica para la implementación del ENS y buenas prácticas de seguridad.

- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a comunicaciones electrónicas, cuando sea aplicable.
- Real Decreto Legislativo 1/1996, de 12 de abril, sobre propiedad intelectual, incluyendo la protección de software y derechos digitales.
- Real Decreto 424/2005, de 15 de abril, en lo que conserve relevancia para la prestación de servicios de comunicaciones electrónicas y protección de usuarios.

4.2. Normativa europea

- Directiva (UE) 2022/2555 (NIS2), relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión.
- Reglamento (UE) 2016/679 (RGPD), relativo a la protección de datos personales.
- Reglamento (UE) 910/2014 (eIDAS), sobre identificación electrónica y servicios de confianza.
- Reglamento (UE) 2019/881, Reglamento de Ciberseguridad de la Unión Europea.
- Reglamento (UE) 2024/2690, en relación con requisitos técnicos y metodológicos para la gestión de riesgos de ciberseguridad y la consideración de incidentes significativos en el marco de NIS2.

5. ROLES: FUNCIONES Y RESPONSABILIDADES

La organización define los roles y responsabilidades del Sistema de Gestión de Seguridad de la Información conforme a ISO/IEC 27001. Estos roles aseguran la dirección, operación, mantenimiento y mejora continua del SGSI, así como la aplicación efectiva de los controles de seguridad sobre los sistemas, procesos y servicios incluidos en el alcance.

Las responsabilidades se asignan atendiendo al principio de segregación de funciones, la competencia del personal y la necesidad de mantener evidencias objetivas del funcionamiento del sistema de gestión.

5.1. Dirección

La Dirección asume la responsabilidad última sobre la seguridad de la información y sobre la eficacia del Sistema de Gestión de Seguridad de la Información.

- Aprobar la Política de Seguridad de la Información, el alcance del SGSI, los objetivos de seguridad y los criterios generales de aceptación y tratamiento del riesgo.
- Garantizar que el SGSI está alineado con la estrategia de la organización, los requisitos contractuales, los requisitos legales y reglamentarios aplicables y las necesidades de las partes interesadas.
- Asignar responsabilidades, autoridad y recursos suficientes para implantar, operar, mantener y mejorar el SGSI.
- Promover la cultura de seguridad de la información, la concienciación del personal y el cumplimiento de las políticas y procedimientos internos.
- Revisar periódicamente el desempeño del SGSI mediante la revisión por la Dirección, evaluando indicadores, resultados de auditorías, estado de acciones correctivas, riesgos, oportunidades y necesidades de mejora.
- Aprobar las acciones necesarias ante riesgos significativos, incumplimientos relevantes, incidentes graves o cambios que puedan afectar a la seguridad de la información.

5.2. Responsable de Seguridad

El Responsable de Seguridad coordina la aplicación operativa de la seguridad de la información y vela por que los controles definidos sean adecuados, eficaces y coherentes con los riesgos identificados.

- Impulsar la identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información, en coordinación con el Responsable del SGSI y con los responsables técnicos o de proceso que correspondan.
- Definir, revisar y supervisar los requisitos de seguridad aplicables a la información, servicios, procesos, proveedores y sistemas incluidos en el alcance.
- Proponer controles de seguridad y medidas de tratamiento del riesgo, verificando su implantación y eficacia junto con los responsables técnicos.

- Coordinar la gestión de incidentes de seguridad, incluyendo su registro, análisis, respuesta, escalado, comunicación interna y seguimiento de acciones correctivas.
- Supervisar la gestión de vulnerabilidades, la priorización de acciones de mitigación, la aplicación de parches y la revisión de configuraciones de seguridad.
- Participar en la evaluación de proveedores y terceras partes cuando su actividad pueda afectar a la confidencialidad, integridad o disponibilidad de la información.
- Informar a la Dirección y al Responsable del SGSI sobre el estado de la seguridad, los riesgos relevantes, los incidentes significativos y las necesidades de mejora.

5.3. Responsable del Sistema de Gestión de Seguridad de la Información

El Responsable del Sistema de Gestión de Seguridad de la Información es responsable de mantener el SGSI conforme a ISO/IEC 27001, asegurando que sus procesos, documentación, evidencias y mecanismos de mejora permanecen actualizados y controlados.

- Mantener el alcance del SGSI, la política, los objetivos de seguridad, la metodología de gestión de riesgos, la Declaración de Aplicabilidad y la información documentada requerida por ISO/IEC 27001.
- Coordinar la planificación, implantación, seguimiento y mejora de los procesos del SGSI, asegurando su integración con los procesos de negocio de la organización.
- Planificar y coordinar auditorías internas, revisiones de cumplimiento, revisiones por la Dirección y actividades de seguimiento del desempeño del SGSI.
- Gestionar no conformidades, acciones correctivas y oportunidades de mejora, verificando su cierre eficaz y la conservación de evidencias.
- Asegurar el control de la información documentada del SGSI, incluyendo versiones, aprobaciones, distribución, conservación y disponibilidad.
- Coordinar la definición y seguimiento de indicadores del SGSI, programas de concienciación, formación y comunicación interna en materia de seguridad de la información.
- Mantener la trazabilidad entre riesgos, controles, objetivos, evidencias y decisiones de mejora del SGSI.

5.4. Administrador de Sistemas

El Administrador de Sistemas es responsable de la operación técnica de los sistemas de información y de la implantación práctica de los controles tecnológicos definidos por el SGSI y por el Responsable de Seguridad.

- Administrar, operar y mantener los sistemas, plataformas, redes, aplicaciones y servicios tecnológicos incluidos en el alcance, conforme a las políticas y procedimientos aprobados.
- Implantar y mantener controles técnicos de seguridad, incluyendo gestión de identidades y accesos, configuración segura, copias de seguridad, registro de eventos, monitorización, protección frente a malware y actualización de sistemas.
- Ejecutar los procesos de gestión de cambios, parches, vulnerabilidades y configuraciones, conservando evidencias de las actuaciones realizadas.
- Mantener inventarios actualizados de activos tecnológicos, software, versiones, servicios, cuentas privilegiadas y elementos críticos para la continuidad de la operación.
- Aplicar el principio de mínimo privilegio, segregación de funciones y trazabilidad en la administración de sistemas.
- Colaborar en la investigación y resolución de incidentes de seguridad, aportando registros, evidencias técnicas, análisis de impacto y medidas de contención o recuperación.
- Informar al Responsable de Seguridad y al Responsable del SGSI de desviaciones, vulnerabilidades, incidentes, cambios significativos o limitaciones técnicas que puedan afectar a la seguridad de la información.

Cuando una misma persona asuma más de un rol, la organización deberá justificarlo, documentar los controles compensatorios necesarios y preservar, en la medida de lo posible, la independencia en la revisión, aprobación y verificación de las actividades críticas del SGSI.

6. GESTIÓN DE VULNERABILIDADES

6.1. Identificación y evaluación

SOMOS.plus establecerá un proceso continuo de detección, análisis y gestión de vulnerabilidades en sus sistemas de información. Se emplearán herramientas de análisis de vulnerabilidades y pruebas de penetración basadas en estándares reconocidos. Los resultados serán documentados y revisados periódicamente.

Se realizarán revisiones trimestrales y análisis específicos cuando existan cambios críticos en la infraestructura o incidentes relevantes. El Responsable de Seguridad supervisará estos procesos y verificará su alineación con ISO 27001, ENS y NIS2.

6.2. Corrección y mitigación

Las vulnerabilidades detectadas serán evaluadas y clasificadas según su criticidad e impacto. Salvo justificación documentada, se aplicarán los siguientes plazos de corrección:

- Críticas: corrección en un máximo de 30 días.
- Altas: corrección en un máximo de 60 días.
- Medias o bajas: corrección en un máximo de 90 días.

Estos plazos podrán ajustarse en función de la evolución de las amenazas y el contexto de seguridad. Cuando una vulnerabilidad crítica o de alto riesgo no pueda corregirse en plazo, se aplicarán medidas de mitigación inmediatas, como segmentación de redes, restricciones de acceso o refuerzo de monitorización.

6.3. Supervisión y mejora continua

El proceso de gestión de vulnerabilidades será revisado anualmente con participación del Comité de Seguridad para identificar mejoras. La revisión incluirá métricas de vulnerabilidades corregidas en plazo, cumplimiento y efectividad de plazos, tendencias de amenazas, lecciones aprendidas y actualización de estrategias.

Todas las vulnerabilidades detectadas y las acciones adoptadas se registrarán en el Registro de Incidentes y Riesgos, asegurando trazabilidad y supervisión efectiva.

6.4. Notificación de vulnerabilidades

Todo el personal deberá reportar de inmediato cualquier vulnerabilidad o anomalía detectada en los sistemas. Las vulnerabilidades críticas deberán notificarse internamente en un máximo de 24 horas y las de alto riesgo en un máximo de 48 horas.

Cuando una vulnerabilidad crítica pueda comprometer la seguridad de la organización o generar un incidente significativo, SOMOS.plus notificará a las autoridades competentes, CCN-CERT o INCIBE, conforme a ENS y NIS2. La evaluación del impacto y la decisión de notificación corresponderán al Responsable de Seguridad, en coordinación con el Comité de Seguridad de la Información.

7. DATOS DE CARÁCTER PERSONAL

SOMOS.plus trata datos de carácter personal y mantiene un registro de actividades de tratamiento accesible únicamente a personas autorizadas. Dicho registro recoge los tratamientos realizados, los datos afectados y los responsables de su gestión.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa vigente para garantizar confidencialidad, integridad y disponibilidad de los datos personales, conforme al RGPD, la LOPDGDD y las medidas establecidas en el ENS.

SOMOS.plus cuenta con un Responsable de Protección de Datos (RPD/DPO), cuya función es garantizar el cumplimiento de la normativa en materia de protección de datos personales, actuar como punto de contacto

con la Agencia Española de Protección de Datos y asesorar a la organización en la aplicación de medidas para un tratamiento seguro de los datos personales.

8. OBLIGACIONES DEL PERSONAL

Todos los trabajadores de SOMOS.plus tienen la obligación de conocer, comprender y cumplir esta Política de Seguridad de la Información. El Comité de Seguridad garantizará que las responsabilidades en materia de seguridad lleguen al personal de forma clara y accesible.

La organización establecerá un programa de concienciación continua en seguridad de la información, dirigido a todo el personal y con especial atención a nuevas incorporaciones.

El personal con funciones de uso, operación o administración de sistemas TIC dentro del alcance del ENS deberá recibir formación específica en seguridad antes de asumir responsabilidades. Esta formación será obligatoria en la asignación inicial y cuando existan cambios de puesto o nuevas funciones que impliquen manejo de sistemas críticos o información sensible.

9. TERCERAS PARTES

Las terceras partes que accedan a sistemas de SOMOS.plus o gestionen información de la organización deberán cumplir requisitos de seguridad equivalentes a los establecidos por la organización, el ENS y NIS2.

En particular, deberán:

- Firmar acuerdos de confidencialidad y protección de la información, garantizando el cumplimiento de la normativa aplicable.
- Aplicar medidas de seguridad alineadas con ISO 27001, ENS y NIS2, incluyendo controles técnicos, organizativos y de gestión de riesgos adecuados.
- Someterse a auditorías o revisiones periódicas cuando resulte aplicable, para verificar su alineación con las medidas de seguridad exigidas.

Se consideran proveedores críticos aquellos que desempeñan funciones esenciales para la organización, soportan sistemas clave, gestionan información sensible o intervienen en procesos críticos para la continuidad del negocio. Estos proveedores estarán sujetos a requisitos adicionales de seguridad y podrán ser objeto de supervisión por parte del Responsable de Seguridad.

Cuando SOMOS.plus utilice servicios de terceros o ceda información a terceros, estos deberán adherirse a esta Política o acreditar procedimientos propios que garanticen un nivel de seguridad equivalente o superior. Si una tercera parte no pudiera satisfacer alguno de los requisitos establecidos, el Responsable de Seguridad elaborará un informe con los riesgos asociados y las medidas compensatorias necesarias.

10. REVISIÓN, DIFUSIÓN Y APROBACIÓN

Esta Política será revisada al menos una vez al año, o siempre que se produzcan cambios normativos, tecnológicos, organizativos o estratégicos que impacten en la seguridad de la información. La revisión será realizada por la Dirección en coordinación con el Responsable de Seguridad y el Comité de Seguridad de la Información.

Se documentarán todas las modificaciones realizadas, justificando los cambios en base a auditorías, incidentes de seguridad, actualizaciones normativas o evaluaciones de riesgos. La Declaración de Aplicabilidad del ENS e ISO 27001 se revisará en cada actualización significativa para asegurar coherencia con los controles aplicados y trazabilidad.

La versión actualizada de la Política será comunicada a todo el personal de la organización y estará disponible para su consulta por las partes interesadas bajo solicitud.

Revisión	Fecha	Razón modificación
00	07/01/2025	Documento inicial MS-01.
01	21/05/2026	Revusión y alineación con el ENS

La Dirección se asegura de que la Política de Seguridad de la Información es entendida, implantada y mantenida al día en todos los niveles de la organización.

Dirección

En Málaga, a 21 de mayo de 2026