LOOMIS Spain

POLÍTICA DE

SEGURIDAD DE LA INFORMACIÓN

CONTROL DE VERSIONES

FECHA	VERSIÓN	AUTOR	DESCRIPCIÓN DEL CAMBIO
20/09/2018	1.0	LOOMIS	VERSIÓN INICIAL
30/04/2021	1.1	LOOMIS	REVISIÓN CUMPLIMIENTO NORMA ISO 27001
19/06/2021	1.2	LOOMIS	CAMBIO DIRECTOR GENERAL POR CONSEJERO DELEGADO
20/06/2021	1.3	LOOMIS	CAMBIO EN LA PORTADA, SUSTITUCIÓN LOOMIS ESPAÑA POR LOOMIS SPAIN
18/02/2022	1.4	LOOMIS	1.1. ÁMBITO DE APLICACIÓN
23/09/2022	1.5	LOOMIS	2.5. MEJORA CONTINUA DEL SGSI 2.6. ÁREAS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 2.7. APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 1.1. ÁMBITO DE APLICACIÓN REVISIÓN 2. TÉRMINOS Y DEFINICIONES ACTUALIZACIÓN 2.4. RESPONSABILIDADES ACTUALIZACIÓN
13/12/2023	1.6	LOOMIS	2.6. ÁREAS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ACTUALIZACIÓN DE POLÍTICAS
24/07/2024	1.7	LOOMIS	2.6. ÁREAS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ACTUALIZACIÓN DE POLÍTICAS
02/01/2025	1.8	LOOMIS	2.9. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI ACTUALIZACIÓN DEL NOMBRE DEL CONSEJERO DELEGADO (CEO) DEBIDO A NUEVA DESIGNACIÓN
15/12/2025	1.9	CISO	REVISIÓN ANUAL

DISTRIBUCIÓN

NOMBRE	PUESTO
TODOS LOS EMPLEADOS	TODOS

CONTENIDOS

1. INTRODUCCIÓN

Este documento define la política de seguridad de la información de LOOMIS Spain.

Como empresa moderna y con visión de futuro, la dirección general de LOOMIS Spain reconoce la necesidad de garantizar que su negocio funcione sin problemas y sin interrupciones en beneficio de sus clientes, accionistas y otras partes interesadas.

Con el fin de proporcionar dicho nivel de funcionamiento continuo, LOOMIS Spain ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) en línea con la Norma Internacional de Seguridad de la Información, ISO/IEC 27001. Esta norma define los requisitos para un SGSI basado en las mejores prácticas reconocidas internacionalmente.

El funcionamiento del SGSI tiene muchos beneficios para la empresa, entre ellos

- Protección de los flujos de ingresos y de la rentabilidad de la empresa
- Garantizar el suministro de bienes y servicios a los clientes
- Mantenimiento y mejora del valor para los accionistas
- Cumplimiento de los requisitos legales y reglamentarios

LOOMIS Spain ha decidido mantener la certificación completa de la norma ISO/IEC 27001 para que la adopción efectiva de las mejores prácticas de seguridad de la información pueda ser validada por una tercera parte independiente.

Esta política se aplica a todos los sistemas, personas y procesos que constituyen los sistemas de información de la organización, incluidos los miembros del comité de dirección, directores, empleados, proveedores y otros terceros que tienen acceso a los sistemas de LOOMIS Spain.

2. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.1. OBJETIVOS Y MEDICIÓN

Los objetivos generales de la seguridad de la información es la protección de la información para garantizar:

- **Confidencialidad**: asegurar que la información sea accesible sólo a las personas autorizadas para acceder a ella.
- **Integridad**: asegurar que la información sea exacta y completa y que no se modifique sin autorización.
- **Disponibilidad**: asegurar que la información sea accesible a los usuarios autorizados cuando sea necesario.

Los objetivos de seguridad de la información se documentarán durante un período de tiempo acordado, junto con los detalles de cómo se lograrán. Estos objetivos serán evaluados y controlados como parte de las revisiones de la gestión para garantizar que siguen siendo válidos. Si se requieren modificaciones, éstas se gestionarán mediante el proceso de gestión de cambios.

Se utilizará un ciclo regular para la fijación de objetivos en materia de seguridad de la información, que coincidirá con el ciclo de planificación presupuestaria. Esto garantizará que se obtenga la financiación adecuada para las actividades de mejora identificadas. Estos objetivos se basarán en una clara comprensión de las necesidades de la empresa, informada por el proceso de revisión de la gestión durante el cual se pueden obtener las opiniones de las partes interesadas pertinentes.

De acuerdo con la norma ISO/IEC 27001, los controles de referencia detallados en el Anexo A de la norma serán adoptados, en su caso, por LOOMIS Spain. Estos controles se revisarán periódicamente a la luz de los resultados de las evaluaciones de riesgos y en consonancia con los planes de tratamiento de los riesgos para la seguridad de la información.

2.2. REQUISITOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Se acordará y mantendrá una definición clara de los requisitos para la seguridad de la información dentro de LOOMIS Spain con el negocio interno para que toda la actividad del SGSI se centre en el cumplimiento de esos requisitos. Los requisitos legales, reglamentarios y contractuales también se documentarán y se introducirán en el proceso de planificación. Los requisitos específicos sobre la seguridad de los sistemas o servicios nuevos o modificados se capturarán como parte de la etapa de diseño de cada proyecto.

Un principio fundamental del sistema de gestión de la seguridad de la información de LOOMIS Spain es que los controles aplicados se basen en las necesidades de la empresa, lo que se comunicará periódicamente a todo el personal mediante reuniones de equipo y documentos informativos.

2.3. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

El proceso de escoger los controles de seguridad está definido en la metodología de evaluación y tratamiento de riesgos (Metodología de Evaluación de Tratamiento de Riesgos).

Los controles seleccionados y su estado de implementación se detallan en la Declaración de aplicabilidad.

2.4. RESPONSABILIDADES

Las responsabilidades para el SGSI son las siguientes:

- El Consejero Delegado es el responsable de garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y de garantizar que todos los recursos necesarios estén disponibles.
- El Director de Operaciones e IT es el responsable de la coordinación operativa del SGSI, como también de informar de su desempeño.
- El Consejero Delegado debe revisar el SGSI al menos una vez por año o cada vez que se produzcan cambios relevantes para la organización, ya sean de tipo operativo, legal, regulatorio o contractual y siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento. El objetivo de las verificaciones por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGSI y debe elaborar actas de dichas reuniones.
- El Director de Operaciones e IT implementará programas de capacitación y concienciación adecuados a los empleados sobre seguridad de la información y buenas prácticas en relación con el desempeño de sus funciones, así como, facilitará el acceso y conocimiento de las actualizaciones regulares tanto de la presente Política como al resto del Cuerpo Normativo y Documental del SGSI (procedimientos, guías…).
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades de seguridad que puedan comprometer o hayan comprometido la confidencialidad, integridad y/o disponibilidad de la información deben ser comunicados al Director de Operaciones e IT, debiendo ser registrados y analizados con la finalidad de aplicar las correspondientes medidas correctivas y/o preventivas.
- El Director de Operaciones e IT definirá qué información relacionada con la seguridad de la información será comunicada a qué parte interesada (tanto interna como externa), por quién y cuándo.

- El Director de Operaciones e IT es el responsable de adoptar e implementar el Plan de capacitación y concienciación, que corresponde a todas las personas que cumplen una función en la gestión de la seguridad de la información.

2.5. MEJORA CONTINUA DEL SGSI

La política de LOOMIS Spain con respecto a la mejora continua es:

- Mejorar continuamente la eficacia del SGSI.
- Mejorar los procesos actuales para alinearlos con las buenas prácticas definidas en la norma ISO/IEC 27001 y normas relacionadas.
- Conseguir la certificación ISO/IEC 27001 y mantenerla de forma continua.
- Aumentar el nivel de proactividad (y la percepción de proactividad de las partes interesadas) en relación con la seguridad de la información.
- Hacer que los procesos y controles de seguridad de la información sean más medibles para proporcionar una base sólida para la toma de decisiones informadas.
- Revisar anualmente las métricas pertinentes para evaluar si es conveniente modificarlas, basándose en los datos históricos recopilados.
- Obtener ideas de mejora mediante reuniones periódicas y otras formas de comunicación con las partes interesadas.
- Revisar las ideas de mejora en las reuniones periódicas de gestión para priorizar y evaluar los plazos y beneficios.

Las ideas de mejora pueden obtenerse de cualquier fuente, incluidos los empleados, los clientes, los proveedores, el personal de TI, las evaluaciones de riesgo y los informes de servicio. Una vez identificadas, se registrarán y evaluarán en el marco de las revisiones de gestión.

2.6. ÁREAS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

LOOMIS Spain define la política en una amplia variedad de áreas relacionadas con la seguridad de la información que se describen en detalle en un conjunto completo de documentación de políticas que acompaña a esta política general de seguridad de la información.

Cada una de estas políticas es definida y acordada por una o más personas con competencia en el área correspondiente y, una vez aprobada formalmente, se comunica al personal de la organización adecuado, tanto dentro como fuera de la organización.

El siguiente cuadro muestra las políticas individuales dentro del conjunto de documentación y resume el contenido de cada política y el público objetivo de las partes interesadas.

POLÍTICA	ÁMBITO	PÚBLICO DESTINATARIO
Política de acceso a Internet	Uso empresarial de Internet, uso personal de Internet, gestión de cuentas de Internet, seguridad y supervisión y usos prohibidos del servicio de Internet.	Todos los empleados
Política de computación en nube	Diligencia debida, alta, configuración, gestión y baja de servicios de computación en nube.	Empleados implicados en la adquisición y gestión de servicios en la nube
Política de dispositivos móviles	Cuidado y seguridad de dispositivos móviles como ordenadores portátiles, tabletas y teléfonos inteligentes, ya sean proporcionados por la organización para uso empresarial.	Usuarios de dispositivos móviles proporcionados por la empresa
Política BYOD	Consideraciones sobre el programa «Traiga su propio dispositivo» (BYOD) cuando el personal desee utilizar sus propios dispositivos móviles para acceder a la información corporativa.	Usuarios de dispositivos personales para uso profesional restringido
Política de trabajo remoto	Consideraciones relativas a la seguridad de la información en el establecimiento y la gestión de un lugar de teletrabajo, por ejemplo, seguridad física, seguros y equipos.	Directivos y empleados implicados en la creación y el mantenimiento de un lugar de teletrabajo
Política de control de acceso	Registro y baja de usuarios, concesión de derechos de acceso, acceso externo, revisiones de acceso, política de contraseñas, responsabilidades de los usuarios y control de acceso a sistemas y aplicaciones.	Empleados implicados en la configuración y gestión del control de acceso
Política de control de acceso dinámico	Aplicabilidad y uso de controles de acceso dinámicos disponibles en entornos específicos.	Propietarios de activos y equipo TIC
Política criptográfica	Evaluación de riesgos, selección de técnicas, despliegue, pruebas y revisión de la criptografía, y gestión de claves.	Empleados implicados en la configuración y gestión del uso de tecnología y técnicas criptográficas
Política de seguridad física	Zonas seguras, seguridad del papel y los equipos y gestión del ciclo de vida de los equipos.	Todos los empleados
Política antimalware	Cortafuegos, antivirus, filtrado de spam, instalación y escaneado de software, gestión de vulnerabilidades, formación para la concienciación de los usuarios, supervisión y alertas de amenazas, revisiones técnicas y gestión de incidentes de malware.	Empleados responsables de la protección de la infraestructura de la organización frente al malware
Política de copias de seguridad	Ciclos de copias de seguridad, copias de seguridad en la nube, almacenamiento externo, documentación, pruebas de recuperación y protección de soportes de almacenamiento.	Empleados responsables de diseñar y aplicar regímenes de copias de seguridad
Política de registro y vigilancia	Configuración para la recopilación, protección y revisión de eventos	Empleados responsables de proteger la infraestructura de la organización frente a ataques
Política de software	Adquisición de software, registro de software, instalación y eliminación, desarrollo interno de software y uso de software en la nube.	Todos los empleados
Política de gestión técnica de vulnerabilidades	Definición de vulnerabilidades, fuentes de información, parches y actualizaciones, evaluación de vulnerabilidades, endurecimiento, formación de concienciación y divulgación de vulnerabilidades.	Empleados responsables de proteger la infraestructura de la organización contra programas maliciosos
Política de seguridad de redes	Diseño de la seguridad de la red, incluida la segregación de la red, la seguridad del perímetro, las redes inalámbricas y el acceso remoto; gestión de la seguridad de la red, incluidas funciones y responsabilidades, registro y supervisión y cambios.	Empleados responsables de diseñar, implantar y gestionar redes

POLÍTICA	ÁMBITO	PÚBLICO DESTINATARIO
Política de mensajería electrónica	Envío y recepción de mensajes electrónicos, supervisión de los servicios de mensajería electrónica y uso del correo electrónico.	Usuarios de servicios de mensajería electrónica
Política de colaboración en línea	Utilización de herramientas de colaboración para la comunicación, el intercambio y la videoconferencia.	Usuarios de herramientas de colaboración en línea
Política de desarrollo seguro	Especificación de requisitos empresariales, diseño, desarrollo y comprobación de sistemas y desarrollo de software subcontratado.	Empleados responsables de diseñar, gestionar y escribir código para desarrollos de software a medida
Política de seguridad de la información para las relaciones con los proveedores	Diligencia debida, acuerdos con proveedores, supervisión y revisión de servicios, cambios, litigios y finalización de contratos.	Empleados encargados de establecer y gestionar las relaciones con los proveedores
Política de gestión de la disponibilidad	Requisitos y diseño de la disponibilidad, supervisión y elaboración de informes, no disponibilidad, comprobación de los planes de disponibilidad y gestión de los cambios.	Empleados responsables de diseñar sistemas y gestionar la prestación de servicios.
Política de cumplimiento de la propiedad intelectual y los derechos de autor	Protección de la propiedad intelectual, legislación, sanciones y cumplimiento de licencias de software.	Todos los empleados
Política de protección y conservación de documentos	Periodo de conservación para tipos de registro específicos, uso de criptografía, selección de soportes, recuperación, destrucción y revisión de registros.	Empleados responsables de la creación y gestión de registros
Política de privacidad	Legislación aplicable en materia de protección de datos, definiciones y requisitos.	Empleados responsables de diseñar y gestionar sistemas que utilicen datos personales
Política de escritorio y pantalla limpios	Seguridad de la información mostrada en pantallas, impresa y conservada en soportes extraíbles.	Todos los empleados
Política de medios sociales	Directrices sobre el uso de las redes sociales cuando se represente a la organización y se discutan asuntos relevantes para la misma.	Todos los empleados
Política de seguridad de RRHH	Contratación, contratos de trabajo, cumplimiento de las políticas, proceso disciplinario, despido.	Todos los empleados
Política de uso aceptable	Compromiso de los empleados con las políticas de seguridad de la información de la organización.	Todos los empleados
Política de gestión de activos	Este documento establece las normas sobre cómo deben gestionarse los activos desde el punto de vista de la seguridad de la información.	Todos los empleados
Política de CCTV	El uso de CCTV en la seguridad física, incluidas las cuestiones y consideraciones relativas a la ubicación y la protección de datos.	Empleados responsables de CCTV
Política de gestión de la configuración	La configuración segura de hardware, software, servicios y redes.	Empleados responsables de diseñar sistemas y gestionar la prestación de servicios
Política de eliminación de información	La eliminación de la información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento, cuando ya no sea necesaria.	Empleados responsables del diseño y la gestión de sistemas que utilizan datos personales

POLÍTICA	ÁMBITO	PÚBLICO DESTINATARIO
Política de anonimización de datos	El uso de técnicas de enmascaramiento de datos, como la anonimización y la seudonimización, para proteger la información personal identificable (IPI).	Empleados responsables del diseño y la gestión de sistemas que utilizan datos personales
Política de prevención de fuga de datos	La configuración de las herramientas informáticas pertinentes para detectar y evitar la fuga de datos.	Empleados responsables del diseño de sistemas y de la gestión de la prestación de servicios
Política de supervisión	La supervisión del entorno de las TIC para detectar actividades anómalas.	Empleados responsables de diseñar sistemas y gestionar la prestación de servicios
Política de filtrado web	La restricción del acceso a sitios de Internet que se consideren inapropiados.	Empleados responsables de diseñar sistemas y gestionar la prestación de servicios
Política de codificación segura	Los principios que se utilizarán al desarrollar código seguro.	Empleados responsables de diseñar, gestionar y escribir código para desarrollos de software a medida
Política de inteligencia sobre amenazas	Recopilación y utilización de información sobre amenazas a nivel estratégico, táctico y operativo.	Empleados responsables de proteger la infraestructura de la organización frente a ataques
Política de seguridad de la información	El planteamiento de cuestiones sobre seguridad de la información dentro de la organización.	Todos los empleados y otras partes interesadas

2.7. APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las declaraciones de política realizadas en este documento y en el conjunto de políticas de apoyo enumeradas en el apartado anterior han sido revisadas y aprobadas por la dirección de LOOMIS Spain y deben ser cumplidas. El incumplimiento de estas políticas por parte de un empleado puede dar lugar a la adopción de medidas disciplinarias de acuerdo con el Proceso Disciplinario de Empleados de la organización.

Las preguntas relativas a cualquier política de LOOMIS Spain deben dirigirse en primer lugar al superior jerárquico del empleado.

2.8. COMUNICACIÓN DE LA POLÍTICA

El Consejero Delegado debe asegurarse de que todos los miembros de LOOMIS Spain, como también los terceros externos correspondientes, estén familiarizados con esta Política.

2.9. APOYO PARA LA IMPLEMENTACIÓN DEL SGSI

A través del presente, el Consejero Delegado declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

05287140S RAFAEL MOYANO (R: A79493219)

Firmado digitalmente por 05287140S RAFAEL MOYANO (R: A79493219)
Fecha: 2025.12.10 12:19:50 +01'00'

Rafael Moyano

Consejero Delegado

_____