Kepar Group

Contenido

1. Política de Seguridad del SGSI

Kepar Electrónica S.L. considera la seguridad de la información un aspecto fundamental para conseguir la confianza de sus clientes.

La adecuada gestión de la seguridad de la Información es por tanto uno de los objetivos que la Dirección que la Organización contempla para la prestación de sus servicios tecnológicos a clientes, para ello la Dirección establece y mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) documentado y actualizado, a partir de la elaboración de un análisis de riesgos de seguridad de la información y basado en la norma ISO 27001:2022.

Asegurar los correctos niveles de confidencialidad de la información, así como la integridad de los datos y por supuesto la disponibilidad y continuidad del servicio son objetivos estratégicos de dicho sistema. Para alcanzar dichos objetivos, la Dirección proporciona los recursos adecuados para el mantenimiento y mejora del SGSI, participa activamente en el establecimiento y seguimiento de objetivos estratégicos de seguridad, así como en la revisión del SGSI, y lleva a cabo las acciones formativas necesarias en materia de seguridad.

En todas sus actividades la Organización mantiene firme el cumplimiento con legislación vigente y especialmente la relativa a la protección de datos personales (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) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y a la prestación de servicios de la sociedad de la información (Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.), así como el cumplimiento de los compromisos contractuales adquiridos con sus clientes y terceras partes. Para más detalle, contemplar el documento "**PS002-04 Política de cumplimiento normativo"**.

La Dirección de la Organización mantiene un compromiso permanente respecto a la mejora continua del SGSI así como de su eficacia.

1.1 Objetivos de la Organización

La presente Política pretende establecer las directrices necesarias en cuanto a Seguridad de la Información, las cuales son consideradas por la Dirección de la Organización como un requisito imprescindible para la consecución de los objetivos estratégicos y operativos.

La decisión de la Dirección de Kepar Electrónica S.L. de establecer, implantar, monitorizar, revisar, mantener y mejorar un SGSI en la organización, responde a unos planteamientos estratégicos nacidos desde la toma de conciencia de la Dirección de la necesidad de gestionar adecuadamente la información que sirve para alimentar sus procesos operativos, asegurar la continuidad de la organización y la fiabilidad de sus clientes internos y externos.

1.2 Principios de Seguridad de la Información

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001:2022, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, apliquen a la Organización.

La Organización establece los siguientes principios básicos:

- **Alcance estratégico**: La seguridad de la información cuenta con el compromiso y apoyo de la Dirección de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.
- **Seguridad como proceso integral**: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información. Además, se prestará atención a la concienciación de las personas para evitar que la ignorancia, la falta de organización y de coordinación, constituyan fuentes de riesgo.
- **Gestión de seguridad basada en los riesgos**: Se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC, siento parte esencial del proceso de seguridad de la información el análisis y gestión de riesgos. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.

- **Proporcionalidad**: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua**: La vigilancia continua detectará actividades anómalas a las que dará respuesta. Los controles y medidas de seguridad implantados se reevaluarán y actualizarán periódicamente al objeto de adecuar su eficacia a la constante evolución de los riesgos, de los sistemas de protección y del entorno tecnológico. La seguridad de la información será atendida, revisada y auditada por personal cualificado.
- **Prevención, detección, respuesta y conservación**: Se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad. De igual manera, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.
- **Diferenciación de responsabilidades**: La responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad de seguridad, así como de la responsabilidad de la información y la responsabilidad del servicio. Los roles y responsabilidades de cada una de estas funciones deberán quedar debidamente acotadas y reflejadas documentalmente.
- **Seguridad por defecto**: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

1.3 Requisitos Mínimos de Seguridad

Esta Política de Seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

- **Organización e implantación de un Sistema de Gestión de seguridad**: la seguridad de los sistemas de información compromete a todos los miembros de Kepar Electrónica S.L. Así mismo, la estructura organizativa establecida en Kepar Electrónica S.L., cumplirá el principio de Diferenciación de Responsabilidades.
- **Análisis y gestión de los riesgos**: el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.
- **Gestión del personal**: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus

responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

- **Profesionalidad**: la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables. Se exigirá, de manera objetiva y no discriminatoria, que los prestadores de servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
- **Autorización y control de los accesos**: se limitará el acceso a los activos de información por parte de usuarios, procesos, dispositivos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- **Protección de las instalaciones**: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- **Adquisición de productos de seguridad y contratación de servicios de seguridad**: en la adquisición de productos de seguridad será exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, según la categoría del sistema y el criterio del responsable de seguridad. Para la contratación de servicios de seguridad se estará obligado a lo dispuesto en el principio de profesionalidad.
- **Mínimo privilegio:** lo sistemas de información se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño.
- **Integridad y actualización del sistema**: la inclusión de elementos físicos o lógicos requerirán autorización formal previa a su instalación en el sistema. También para cualquier modificación de la configuración de hardware y software.
- **Protección de la información almacenada y en tránsito**: se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles, dispositivos portátiles, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. También forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por Kepar Electrónica S.L.. Así como la información en soporte no electrónico que haya sido causa o consecuencia de ellos.

- **Prevención ante otros sistemas de información interconectados**: se protegerá el perímetro del sistema de información. También se analizará los riesgos derivados de la interconexión de sistemas y se controlará el punto de unión.
- **Registro de actividad y detección de código dañino**: Se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.
- **Incidentes de seguridad**: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad. Esta gestión de los incidentes se empleará para la mejora continua de la seguridad del sistema.
- **Continuidad de la actividad**: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
- **Mejora continua del Sistema de Gestión de seguridad**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

1.4 Directrices de la Política de Seguridad

La Dirección de la Organización considera que la consecución de los objetivos y el respeto a los principios se encuentra sujeta al cumplimiento de diversos requerimientos encaminados a garantizar la Seguridad de la Información dentro de la Organización. De esta manera, se considera que la Seguridad de la Información debe ser una prioridad para la organización y para ello, la presente Política establece las siguientes directrices:

- La información de la que la Organización es propietaria y/o depositaria debe ser únicamente accesible para las personas debidamente autorizadas, pertenezcan o no a la Organización.
- La presente Política de Seguridad, así como el resto de Cuerpo Normativo del SGSI (procedimientos, guías, etc.) deberá ser accesible para todos los miembros de la Organización dentro del alcance del SGSI, así como el personal ajeno al mismo que se relaciona con éste a través de alguno de sus procesos.
- La Organización debe cumplir con todos aquellos requerimientos legales, regulatorios y estatuarios que le sean de aplicación, así como los requerimientos contractuales.
- La confidencialidad de la información debe garantizarse en todo momento.
- La integridad de la información debe asegurarse a través de todos los procesos que la gestionan, procesan y almacenan dicha información.

- La disponibilidad de la información debe garantizarse mediante las adecuadas medidas de respaldo y continuidad del negocio.
- Todo el personal dentro del alcance del SGSI de la Organización, deberá disponer de la adecuada formación y concienciación en materia de Seguridad de la Información.
- Todo incidente o debilidad que pueda comprometer o haya comprometido la confidencialidad, integridad y/o disponibilidad de la información deberá ser registrado y analizado para aplicar las correspondientes medidas correctivas y/o preventivas. Así mismo se comunicarán a las partes interesadas en los plazos correspondientes.
- Todo miembro de la Organización que esté dentro del alcance del SGSI es responsable de implementar, mantener y mejorar la presente Política, así como de velar por el cumplimiento de la misma.
- Todo miembro de la Organización dentro del alcance del SGSI es responsable de garantizar la adecuada implementación, mantenimiento y mejora del SGSI, así como su conformidad con el estándar ISO/IEC 27001:2022.

2. Revisión de la Política de Seguridad del SGSI

Esta Política de Seguridad será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la misma.

La Política de Seguridad será propuesta y revisada por el Comité de Seguridad y aprobada y difundida por Kepar Electrónica S.L. para que la conozcan todas las partes afectadas.

En caso de conflictos o diferentes interpretaciones se recurrirá al Comité de Seguridad para resolución de estos, previo informe propuesta del Departamento de Seguridad.

3. Marco Normativo

A los efectos previstos en esta Política de Seguridad, el marco normativo de referencia es el que estipula la legislación vigente en materia de seguridad.

Debido al carácter personal y reservado de la información manejada y a los servicios puestos a disposición de los usuarios, Kepar Electrónica S.L. desarrolla sus actividades de acuerdo a la normativa vigente en dichas materias, de entre las que actualmente cabe destacar por su especial relevancia:

- 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.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- 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 (Reglamento eIDAS).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

Responsabilidades

Dirección

- ❑ Establecer y mantener un SGSI documentado y actualizado
- ❑ Proporcionar los recursos adecuados para el mantenimiento y mejora del SGSI.
- ❑ Participar activamente en el seguimiento de objetivos estratégicos de seguridad.
- ❑ Revisión de la Política de Seguridad del SGSI.

Referencias

- ❑ Norma ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos.

Historial de revisiones

Revisión	Fecha	Motivo
1	16/09/2024	Inicial