DOING THE RIGHT THING

SOTEC CONSULTING
AN ASTEK COMPANY

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	CAMBIOS
V1.0	Feb. 2015	Primera versión
V2.0	Feb. 2015	Revisión y aprobación
V3.0	Feb. 2015	Revisión y aprobación
V4.0	Feb.2016	Revisión y aprobación
V5.0	Marzo de 2016	Revisión y rectificación
V6.0	Mar. 2016	Revisión y rectificación
V7.0	Nov. 2017	Revise
V8.0	Mar. 2018	Punto 12.5.1
V9.0	Nov. 2018	Revise
V10.0	Dic. 2019	Revisión anual
V11.0	Dic. 2020	Revisión anual.
V12.0	Feb. 2021	Revisión NC.
V13.0	Agosto de 2022	Revisión y actualización
V14.0	Septiembre de 2023	Revise
V15.0	Oct. 2024	Actualización tras la adquisición por parte de ASTEK. Integración del nuevo formato.
V16.0	Dic. 2024	Formato ISO 27001:2022 Mejora del contenido tras la revisión de la gestión

REDACCIÓN Y VALIDACIÓN

ACCIÓN	NOMBRE	FUNCIÓN	FECHA	FIRMA
Editorial	François Février	Grupo CISO (Astek)	Nov. 2024	FF
Aprobación	María Jesús Ruiz	Jefe de SGSI (Sotec)	Nov. 2024	MJR
Aprobación	Andrea Vega	CSO (Sotec)	Nov. 2024	AV
Validación final	Luis Calero	Director general (Sotec)	Nov. 2024	LC

DISTRIBUCIÓN

COMPAÑÍA	NOMBRE	ACCIÓN	INFO
SOTEC CONSULTING	**TODOS LOS EMPLEADOS**		

1 Índice

2 PRESENTACIÓN DEL DOCUMENTO

2.1 Objeto

En todas las entidades que constituyen el grupo ASTEK se encuentra implantada una Política General de Seguridad de la Información (denominada PGSI).

La Política que contiene este documento y que se aplica al perímetro de Sotec, hereda este PGSI y tiene en cuenta y detalla las especificidades del ámbito

objetivo de aplicación, en particular el cumplimiento de la norma ISO 27001. Por lo dicho, la presente Política constituye el marco de referencia y coherencia en materia de seguridad de la información para todo el perímetro. Determina los principios de aplicación y las responsabilidades necesarias para alcanzar los objetivos de prevención, protección y respuesta en materia de seguridad fijados por la dirección de Sotec.

Este documento expone en primer lugar las cuestiones y los objetivos de seguridad, así como los requisitos fundamentales de seguridad que se aplican a Sotec.

En segundo lugar, se exponen las principales medidas de seguridad (clasificadas por temas según la norma ISO 27002) para hacer frente a estos retos.

Esta Política se actualiza cada año tras la Revisión de la Gestión.

2.2 Documentos de referencia

REFERENCIA	TÍTULO DEL DOCUMENTO	REFERENCIA
ISO 27001	Norma de seguridad del SGSI	ISO 27001:2013
PGSSI	Política general de seguridad de la SI (Grupo Astek)	SMI-000850-POL

3 Elementos estratégicos

3.1 Contexto y cuestiones

El sistema de información de Sotec está potencialmente sujeto a numerosas amenazas, tanto accidentales como malintencionadas. Por lo tanto, Sotec debe tener en cuenta estas amenazas e implementar una protección adecuada para sus sistemas de información contra las amenazas, ya sean de origen interno o externo, naturales, accidentales o deliberadas.

La aplicación de la política de seguridad de la información de Sotec es el resultado de la voluntad de la dirección de reforzar la relación de confianza entre la empresa y sus clientes. Esto se refleja en particular en el mantenimiento de un SGSI con certificación ISO 27001.

Las acciones emprendidas por Sotec para garantizar la seguridad de su SI se inscriben en este enfoque y tienen como objetivo llevar a cabo una reflexión global sobre la estrategia a adoptar y sus consecuencias organizativas y técnicas.

3.2 Gestión de riesgos y seguridad de la información

Con el objetivo de asegurar la continuidad del negocio y reducir al mínimo el riesgo de daño, la organización ha desarrollado una metodología de gestión

del riesgo que permite analizar de manera periódica el grado de exposición de nuestros activos más importantes, frente a aquellas amenazas que puedan valerse de ciertas vulnerabilidades y tengan como resultado impactos no deseados.
Cada año se lleva a cabo un análisis de riesgos para la seguridad. Su objetivo es :

- Identificar y evaluar los riesgos para la información esencial alojada y/o procesada por los distintos departamentos.
- Definir las medidas que deben mantenerse y las que deben aplicarse como parte de un plan de gestión de riesgos para reducir el alcance de los riesgos identificados.

3.3 Compromisos de gestión

En SOTEC, además del correcto desarrollo de los procesos de negocio, tenemos como objetivo alcanzar una posición de liderazgo en el ámbito de la **consultoría, desarrollo, implantación, integración y mantenimiento de proyectos de tecnología de la información, a través de las diferentes áreas de asistencia técnica, servicios gestionados, proyectos cerrados y formación; de acuerdo con la declaración de aplicabilidad (soa) versión 14.0.**

Para ello, SOTEC reconoce y asume la importancia de la seguridad de la información, que no es otra cosa que la protección de la información frente a diversas y múltiples amenazas con el fin de garantizar la continuidad del negocio, minimizar los riesgos empresariales y maximizar el retorno de las inversiones y oportunidades de negocio. De esta manera, se torna fundamental en la compañía identificar y proteger sus activos de información, evitando la destrucción no controlada, divulgación, modificación y la utilización no autorizada de toda información propiedad de la organización o de nuestras partes interesadas.

Así el estado de las cosas, esta política general sustenta y apoya el Sistema de Gestión de Seguridad de la Información, y debe ser comunicada y considerada por todos los miembros de la organización, y por nuestras partes interesadas más pertinentes. De esta manera, SOTEC se compromete también a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información.

Una protección fiable y eficaz permite a la organización percibir de forma más efectiva sus intereses y llevar a cabo de la mejor manera sus obligaciones en seguridad de la información. SOTEC considera que la inadecuada protección afecta al rendimiento general de la compañía y puede llegar a afectar negativamente a la imagen, reputación y confianza de los clientes.

Nuestros principios en materia de seguridad de la información son los siguientes:

1. SOTEC afronta la toma de riesgos y tolera aquellos, que previo análisis con base en la información disponible, son comprensibles, controlados y tratados cuando es necesario.
2. Todo el personal será informado y concienciado, para que asuman su responsabilidad en seguridad de la información, teniendo en cuenta el nivel de relevancia para el desempeño del trabajo.
3. Se dotará de la financiación suficiente para la correcta gestión operativa de los controles y procesos en materia de seguridad de la información.
4. Se implementarán métodos efectivos de detección de phishing, smishing…, o cualquier fraude cibernético y cualquier otro ataque que afecte a la información.
5. Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.
6. Aquellas situaciones que puedan dar lugar a incumplimientos normativos o contractuales no serán tolerados
7. La protección de los datos de carácter personal y la intimidad de las personas.
8. Garantizar la disponibilidad de la información que da soporte a los servicios.
9. La protección de los derechos de propiedad intelectual.
10. La asignación de responsabilidades de seguridad.
11. El registro de las incidencias de seguridad y la gestión de la continuidad del negocio.
12. La gestión de los cambios que pudieran darse en la empresa relativos a la seguridad

La Dirección de la Organización, mediante la elaboración e implantación del presente Sistema de Gestión de Seguridad de la Información adquiere los siguientes compromisos:

1. Desarrollar y dar servicios conformes con los requisitos legislativos aplicables.
2. Establecer y cumplr los requisitos contractuales con las partes interesadas.
3. Definir los requisitos de formación en seguridad y proporcionar la formación necesaria.
4. Prevenir y detectar virus y otro software malicioso, mediante el desarrollo de políticas específicas.
5. Gestionar la continuidad del negocio, desarrollando planes de continuidad.
6. Establecer las consecuencias de las violaciones de la política de seguridad.
7. Actuar en todo momento dentro de la más estricta ética profesional.

Como muestra de nuestro compromiso en esta materia, SOTEC mantiene su Sistema de Gestión de Seguridad de la Información en continua mejora, valor fundamental en nuestra compañía. Para ello, contamos desde 2015 con la certificación en ISO 27001.

La dirección cuenta con la implicación personal de todos y cada uno de los usuarios del sistema de información de la empresa para garantizar el éxito de esta política, de modo que tengamos una empresa segura, eficaz, sostenible y rentable.

4 Medidas de seguridad de la organización

4.1 Políticas de seguridad de la información

Esta Política de Seguridad sirve de referencia para la aplicación de la seguridad y para las auditorías internas. Describe las funciones y responsabilidades, así como la organización y las medidas relativas a la seguridad.

La presente Política se reexamina y reevalúa en particular en caso de cambios importantes en el SI y al menos una vez al año tras la actualización del análisis de riesgos. Es aprobado por el Comité de Gestión.

Se distribuye a todos los empleados de la empresa a través de la plataforma eManage, desde donde pueden acceder a ella en cualquier momento.

4.2 Organización de seguridad

Se ha creado un Comité de Seguridad para coordinar todos los asuntos relacionados con la seguridad de la información.

Está formado por al menos un representante de la Dirección, el Responsable del SGSI y el Responsable Técnico de Seguridad.

El Comité de Seguridad de la Información se reunirá de manera ordinaria al menos 1 vez al año, aunque podrá ser convocada de manera extraordinaria por cualquiera de sus miembros cuando se estime oportuno.

Entre las funciones del Comité se encuentra la de aprobar el análisis de riesgos como plan de tratamiento del riesgo y SOA, así como se aprobará el riesgo asumible o aceptable en cada caso.

Las funciones del Responsable del SGSI serán:

- Implantación, desarrollo y mantenimiento del SGSI.
- Mantenimiento de la documentación.
- Gestión de eventos de seguridad.
- Gestión de la no conformidad.
- Sensibilizacióna la organización
- Mediciónde l rendimiento del sistema de gestión de la seguridad de la información y cualquier necesidad de mejora.

- Monitorización de la efectividad de los controles implantados para garantizar la seguridad de la información..
- Promoción de planes de mejora

Contará con el apoyo de la Dirección, y con los recursos tecnológicos y de personal, que sean necesarios.

El responsable técnico de seguridad se encarga del mantenimiento y el funcionamiento de todas las soluciones técnicas destinadas a garantizar la seguridad de los activos.

4.3 Gestión de activos

Para aplicar y mantener una protección adecuada de los activos de la Empresa, es esencial identificarlos. Por ello, todos los activos de la Empresa son inventariados y actualizados cada año.

Se distribuyen guías de buenas prácticas a todos los empleados para garantizar el uso adecuado de los activos.

4.4 Clasificación y manipulación de la información

Existe un procedimiento de clasificación para definir la sensibilidad de la información.

El objetivo de la clasificación de los activos es permitir que todos los equipos implicados consideren la información en su justo valor y apliquen las medidas de seguridad adecuadas a las cuestiones en juego.

4.5 Gestión del acceso lógico

Para controlar y limitar el acceso a la información y a los recursos de procesamiento de la información, en la empresa se definen normas para controlar el acceso lógico.

Cada usuario dispone de derechos acordes con su perfil de actividad, que le dan acceso a una carpeta, una aplicación o un servicio.

Se definen roles de acceso para los distintos servicios y una política de contraseñas complejas.

4.6 Gestión de proveedores

Todas las relaciones con los proveedores se rigen por un contrato que contiene cláusulas de seguridad adaptadas a la finalidad del contrato y a los riesgos que conlleva.

Se mantiene un procedimiento de seguimiento y evaluación de los proveedores.

4.7 Gestión de incidentes de seguridad

Todos los incidentes de seguridad se recogen en un gestor de incidentes para facilitar su tratamiento.

Un flujo de trabajo de procesamiento permite asignar el incidente a la persona adecuada de la organización, para que pueda ser tratado de forma rápida y apropiada.

También nos permite aprovechar los comentarios y mejorar el funcionamiento del proceso.

4.8 Continuidad empresarial

Para garantizar la continuidad de la actividad en caso de crisis grave, se mantiene un plan general de emergencia y continuidad de la actividad.

Basado en la aplicación de planes de emergencia, pretende preservar la continuidad de las actividades proporcionando planes de acción para recuperarse lo antes posible de la acción perturbadora.

El plan incluye la continuidad de los sistemas de seguridad de los sistemas de información.

4.9 Aspectos jurídicos

La implantación de un sistema de información está sujeta a una serie de obligaciones legislativas y reglamentarias que confieren a esta actividad un elevado perfil jurídico.

De este modo, las principales leyes y reglamentos vigentes que deben ser conocidos y cumplidos por la empresa se consolidan en un registro interno.

Sotec utiliza los servicios de asesores jurídicos externos para controlar y cumplir con sus obligaciones.

4.10 Cumplimiento

Es importante asegurarse de que el sistema de información y su uso cumplen las políticas y normas de seguridad de la empresa.

Además de la auditoría externa del SGSI, cada año se lleva a cabo una auditoría interna, que puede ser realizada por un proveedor externo con experiencia.

5 Medidas de seguridad aplicables a las personas

5.1 Contratación

Se invita a los candidatos a autorizar el acceso a sus datos a través de las plataformas que utilizamos para publicar nuestras ofertas de empleo y, cuando envían su CV en nuestra página web, se les informa de que los datos se utilizarán para acceder al puesto solicitado.

Se analizan los currículums de los candidatos y se verifica que cumplan los requisitos solicitados para el puesto.

5.2 Sensibilización y formación

Para garantizar que los empleados son conscientes de sus responsabilidades en materia de seguridad de la información y que pueden desempeñar un papel activo en la protección de la SI, se ha puesto en marcha y se mantiene un programa de sensibilización. Adopta la forma siguiente:

- Comunicación mensual por correo electrónico sobre los riesgos de seguridad y las mejores prácticas a adoptar
- Campañas de phishing, para enseñar a los empleados a reconocer y evitar el fraude por correo electrónico.
- Carteles sobre la seguridad de la información pegados en las paredes de las oficinas para recordar la importancia de la prudencia

5.3 Responsabilidad de los trabajadores

Cada trabajador está sujeto a los derechos y deberes que se establecen en los siguientes documentos desde el momento en que se incorpora a la empresa:

- Código de conducta que cubre todos los aspectos de la seguridad de la información.
- Manual de acogida. Hace referencia a la prevención de riesgos profesionales y a la confidencialidad, así como a la política general de valores de SOTEC.

Existe un sistema disciplinario de faltas y sanciones.

5.4 Trabajo a distancia

Se aplica la normativa sobre teletrabajo y se pone a disposición de los empleados un Manual del trabajador.

6 Medidas de seguridad física

6.1 Seguridad física de los locales

El acceso a las oficinas está controlado por una alarma y el acceso al edificio por videovigilancia y un portero.

Un número limitado de responsables tiene las llaves de las instalaciones. La lista es inventariada y revisada regularmente.

Todos los visitantes (clientes, proveedores, etc.) estarán acompañados durante su visita por el personal de SOTEC que les haya invitado.

6.2 Seguridad de activos fuera de las instalaciones

El teletrabajo en SOTEC es excepcional pero tolerado. Por lo dicho, en supuestos tasados se permite al empleado solicitar teletrabajar y, por tanto, llevarse el equipo fuera de las instalaciones de la empresa.

Existen medidas de seguridad en los puestos de trabajo.

6.3 Seguridad de los equipos informáticos de las sucursales

Una sala técnica identificada se encuentra en las instalaciones y alberga el equipo de red.

El equipo es mantenido y operado por una empresa especializada.

6.4 Destrucción segura del material

Regularmente se contratan los servicios de una empresa externa de trituración para realizar una destrucción segura con un certificado de destrucción conforme a las normas y el medio ambiente de ordenadores, impresoras, documentación confidencial etc.

7 Medidas tecnológicas de seguridad

7.1 Seguridad en el puesto de trabajo

El puesto de trabajo es la principal herramienta utilizada diariamente por un empleado para procesar información. También es una herramienta que sirve de interfaz con Internet y otros sistemas, especialmente a través del correo electrónico.

Por lo tanto, se presta especial atención a la seguridad de este equipo

- Cada puesto de trabajo se asigna a un empleado por su nombre. El mantenimiento corre a cargo del proveedor de tecnología y el parque se renueva periódicamente.
- En cada estación de trabajo se activa un antivirus que se actualiza automáticamente.
- Si se ausenta durante un breve periodo de tiempo, los dispositivos se bloquean automáticamente tras unos minutos de inactividad.

7.2 Acceso seguro a los servicios

Cada usuario tiene acceso a los servicios de Google Workspace y a las distintas herramientas compartidas por la empresa en modo SAAS.

El acceso a estos servicios está asegurado de la siguiente manera:

- Todos los servicios relacionados con aplicaciones situadas en redes públicas están protegidos mediante certificados SSL.
- El acceso está controlado por los roles de la empresa sobre una base de derecho a saber estrictamente aplicada.
- Cada cuenta es nominativa y el acceso está asegurado por una contraseña compleja.

7.3 Seguridad de las infraestructuras de los sistemas de información

Con todos los servicios de aplicación externalizados, la infraestructura adopta la forma de una red local dedicada a la empresa.

Los elementos de infraestructura que hay que asegurar son los equipos de red de la sala técnica de nuestra oficina.

La gestión de los equipos y de la red se delega en un tercero en virtud de un contrato de explotación. Cualquier solicitud de cambios en la red se rastrea utilizando las herramientas operativas del proveedor de servicios.

7.4 Protección de la información

Todas las cuentas de correo electrónico tienen un nombre de usuario y una contraseña. Para los teléfonos móviles, el correo electrónico también tiene un nombre de usuario y una contraseña. Las comunicaciones siguen los protocolos de seguridad de los proveedores. Los correos electrónicos están encriptados SSL/TLS.

Al final de cada correo electrónico, se dedica un párrafo a la solicitud de confidencialidad del contenido del mismo.