# Política de

# Seguridad de la Información

Actualización Julio 2023

## PREÁMBULO

En ServiceTonic, entendemos que la seguridad de la información es un pilar fundamental para la confianza de nuestros clientes, la continuidad del negocio y la protección de los activos digitales. Como empresa dedicada al desarrollo y comercialización de software para la gestión de servicios, activos y proyectos, gestionamos información sensible y datos críticos, por lo que asumimos el compromiso inquebrantable de protegerlos frente a amenazas, vulnerabilidades y accesos no autorizados.

Nuestra Política de Seguridad de la Información refleja nuestro compromiso con la integridad, confidencialidad y disponibilidad de los datos, asegurando el cumplimiento de normativas legales y estándares internacionales. Todos los miembros de la empresa, desde la dirección hasta cada colaborador, tienen un rol activo en la implementación y mejora continua de nuestras medidas de seguridad.

A través de esta política, fomentamos una cultura de seguridad en la organización, promoviendo buenas prácticas, formación continua y el uso responsable de la tecnología. Con ello, garantizamos la resiliencia de nuestros sistemas y servicios, fortaleciendo la confianza de nuestros clientes y socios.

Esta política se aplica a todos los procesos, sistemas, empleados y terceros que interactúan con la información de ServiceTonic, y es revisada y actualizada periódicamente para adaptarse a las nuevas necesidades y desafíos del entorno digital.

# 1.- Política General de la Seguridad de la Información

La Política de Seguridad de ServiceTonic refleja los **principios y objetivos** en materia de seguridad de la información, cuyos resultados permiten a nuestra empresa alcanzar su propósito de ofrecer un Sistema de gestión de seguridad de la información qué de soporte a la infraestructura, a los procesos internos de la compañía y a los Servicios relacionados con las **aplicaciones comerciales de ServiceTonic.**

Mediante la elaboración, comunicación y mantenimiento de esta política, la Dirección de Service-Tonic muestra su **compromiso** de proteger la confidencialidad de la información con la que opera en la prestación de sus servicios, garantizar su integridad en todos los procesos de tratamiento que lleve a cabo, así como la disponibilidad de los sistemas de información implicados en estos tratamientos.

Para ello, la Dirección ha **definido e implantado un Sistema de Gestión de la Seguridad de la Información** que permite a la compañía garantizar que los sistemas de información y la información que se crea, recopila, almacena y procesa **se compromete con los siguientes principios**:

- La seguridad en la Gestión de los Recursos Humanos, antes, durante y al finalizar el empleo.
- La gestión adecuada de los activos que implique la clasificación de la información y la manipulación de los soportes, y el establecimiento de un robusto control de acceso lógico a sus sistemas y aplicaciones, gestionando los permisos y los privilegios de los usuarios.
- La protección de las instalaciones y del entorno físico, mediante el diseño de áreas de trabajo seguras y la seguridad de los equipos.
- La garantía de la seguridad en las operaciones mediante la protección contra el software malicioso, la realización de copias de seguridad, el establecimiento de registros y su supervisión así como el control del software en explotación.
- La gestión de las vulnerabilidades técnicas y la elección de técnicas adecuadas para la auditoría de los Sistemas.
- La seguridad de las comunicaciones, protegiendo las redes y el intercambio de información.
- El aseguramiento de la seguridad en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.
- La realización de un desarrollo seguro de software, separando los entornos de desarrollo y producción, y realizando las pruebas funcionales de aceptación adecuadas
- El control de las relaciones con los proveedores, exigiendo de forma contractual el cumplimiento de las medidas de seguridad pertinentes y unos niveles aceptables en sus servicios.
- La eficacia en la gestión de los incidentes de seguridad, estableciendo los canales adecuados para su notificación, respuesta y aprendizaje oportuno.
- La realización de un plan de continuidad de negocio que proteja la disponibilidad de los servicios durante una crisis o desastre.
- La Identificación y cumplimiento de la normativa aplicable poniendo especial interés en la propiedad intelectual y en la protección de los datos de carácter personal.

- La revisión periódica y mejora continua de nuestro sistema de gestión de la seguridad de la información para garantizar el cumplimiento y eficacia de estos requisitos.

Todo el personal de la organización tiene el deber de acatar esta política, para lo cual la Dirección dispone los medios necesarios y recursos suficientes para su cumplimiento, y asume la responsabilidad de comunicar y mantenerla accesible a todas las partes interesadas.

A los efectos de un mejor cumplimiento en materia de Seguridad de la Información, la empresa ha establecido diferentes políticas con el objetivo de establecer unos principios y unas guías en aspectos específicos y relevantes en materia de Seguridad de la Información.