SGSI basado en ISO 27000

Garantizar la seguridad de la información

www.abast.es

La información es uno de los principales activos de las organizaciones. En la actualidad, las empresas se enfrentan con riesgos e inseguridades procedentes de una amplia variedad de fuentes, tanto externas como internas, que pueden dañar de forma importante sus sistemas de información.

La serie ISO 27000 proporciona, a partir de un enfoque por procesos, un modelo para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la información (SGSI).

Beneficios

Una gestión eficaz de las seguridad de la información permite garantizar una serie de requerimientos de la información necesarios para alcanzar los objetivos del negocio:

- Confidencialidad, asegurando que sólo quienes están autorizados pueden acceder a la información.
- Integridad, asegurando que la información proporcionada a los procesos de negocio es exacta y completa.
- Disponibilidad, asegurando que la información está disponible en cualquier momento que sea requerida por los procesos de negocio.

Retorno de la Inversión en Seguridad (ROSI)

Los costes derivados del diseño e implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en ISO 27000 se ven ampliamente compensados gracias a:

- Reducción de riesgos. Minimizar o eliminar los riesgos para el negocio, resultantes de la materialización de las amenazas existentes sobre la seguridad de la información.
- Ahorro de costes. Racionalización de los recursos en base a la eliminación de inversiones innecesarias o ineficientes debidas a la infra o sobrestimación de los riesgos.
- Cumplimiento con la legislación vigente. Aseguramiento del cumplimiento del marco legal que protege a la empresa eliminando los riesgos y sanciones asociadas.
- Mejora de la competitividad en el mercado. Tener un buen nivel de seguridad de la información, mejora la confianza en el negocio entre clientes, proveedores y socios con los que se intercambia y/o comparte información.

¿Por qué ABAST?

ABAST cuenta con consultores y auditores certificados en la norma ISO 27001. Además, como se ha comentado, la norma establece la implementación de una serie de controles o contramedidas que minimicen el riesgo frente a un número cada vez mayor de amenazas (virus, spam, ataques, intrusiones, intercepción de datos, suplantación de identidades, etc). Por este motivo, es importante contar con un socio tecnológico como ABAST con la visión global y especialización adecuadas.

Nuestra metodología

- Inicio del proyecto y definición de alcance: La actividad importante de esta fase es la definición del alcance del SGSI donde se explicarán los detalles de los procesos, dependencia e interfaces incluidos y excluidos del SGSI.
- Análisis diferencial: Esta fase permite detectar áreas de carencia evidentes, conocer el nivel de madurez de los controles de seguridad de la organización ya existentes e identificar acciones de mejora sin esperar al análisis de riesgos.

- Análisis de riesgos: En esta fase se realizarán las actividades de identificación y valoración de activos, así como de análisis y gestión del riesgo seleccionando las contramedidas o controles necesarios para eliminar o mitigar el riesgo por debajo del umbral definido. Al finalizar esta fase se dispondrá de la Declaración de Aplicabilidad.
- Plan de tratamiento de riesgos: En esta fase se formulará un plan de tratamiento de riesgos que identifique las acciones, los recursos, las responsabilidades y las prioridades adecuadas para gestionar los riegos detectados.
- Planificación, documentación y certificación: En esta fase se planificará la ejecución de los proyectos resultantes de la fase anterior y se realizará la documentación pertinente basada en: políticas, procedimientos, tareas y evidencias o registros.

CYBALL. Servicios de seguridad global de Abast

ABAST ofrece una amplia oferta de servicios y soluciones para dar respuesta a sus necesidades en ciberseguridad y seguridad del negocio. Las estructuramos en 4 capas:

GOBIERNO: Alineación estratégica seguridad/negocio. Tratamiento del riesgo. Análisis coste/beneficio. Medición madurez de la seguridad.

GESTIÓN: Auditorías de Seguridad. Continuidad de negocio. Cumplimiento normativo/legal. Gestión de crisis y de incidencias. Formación y concienciación.

OPERACIONES (SOC/MDR): Monitorización de la Seguridad 24x7. Detección de Amenazas e incidentes. Prevención de brechas. Respuesta a los incidentes.

INFRAESTRUCTURA: Asesoramiento e implantación de infraestructura/soluciones de seguridad TI. Administración de la seguridad TI.

abast cyball 360°

Para más información:
seguridad@abast.es

abast
www.abast.es · info@abast.es

Tel. 933 666 900
Fax 933 666 910
Carrer Equador 39-45
08029 Barcelona

Tel. 914 061 601
Fax 914 061 604
Calle de la Basílica 19, 9° B
28020 Madrid

Tel. 97 170 68 82
Calle Fluviá 1, Bajos dcha.
Despacho 25 (Son Fuster)
07009 Palma de Mallorca