UNE Normalización Española

Norma Española
UNE-EN ISO/IEC 27000
Febrero 2019

UNE Normalización Española

Norma Española
UNE-ISO/IEC 27001
Mayo 2023

Seguridad de la información, ciberseguridad y protección de la privacidad

Sistemas de gestión de la seguridad de la información

Requisitos

SERVICIOS DE CONSULTORÍA EN SEGURIDAD DE LA INFORMACIÓN.

Adecuación a los requisitos en ciberseguridad, implantando técnicas de seguridad para establecer objetivos de control y controles de referencia de la tecnología de la información.

91 109 05 11
info@controlaltsup.com
C/ Puerto de la Cruz Verde, 26. 28045 - Madrid

BASE NORMATIVA Y CONCEPTUAL.

La adopción de un sistema de gestión de seguridad de la información (SGSI) es una decisión estratégica cuyo establecimiento e implementación está condicionado por sus necesidades y objetivos, sus requisitos de seguridad, los procesos organizativos utilizados y su tamaño y estructura. Lo previsible es que todos estos factores condicionantes cambien con el tiempo.

El SGSI preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos, conforme a las exigencias de la norma UNE -ISO/IEC 27001:2023.

Es importante que el SGSI forme parte y esté integrado con los procesos de la organización y con la estructura de gestión global, y que la seguridad de la información se considere durante el diseño de procesos, de los sistemas de información y de los controles. Es de esperar que la implementación del SGSI se ajuste a las necesidades de la organización.

RESPONSABILIDAD EN LAS ORGANIZACIONES.

Las organizaciones son responsables de satisfacer los requisitos para la seguridad de la información. En el mundo empresarial, hay una tendencia generalizada a considerar como activos de la empresa únicamente los bienes tangibles: mobiliario, maquinaria, servidores, etc. Sin embargo, existen bienes intangibles como el inventario de clientes, las tarifas, el conocimiento comercial, la propiedad intelectual o la reputación. Todos estos elementos forman parte de la información de la organización y constituyen uno de los activos más importantes de nuestra organización.

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos en cuanto a la seguridad de la información.

Garantizar la ciberseguridad de los sistemas de información se ha convertido en uno de los principales objetivos de cualquier organización. La ciberseguridad y los actuales riesgos y amenazas tecnológicas, como los virus (*malware*), los ataques de intrusión y ataques persistentes (*APTs*), los fraudes informáticos, los secuestros de información (*Ransomware*), la falta de protección o cualquier otro riesgo no controlado, pueden ocasionar pérdidas importantes y repercutir directamente en la calidad del servicio.

Gracias al uso de la tecnología, el tratamiento de grandes volúmenes de datos se ha vuelto muy sencillo, ya que, por ejemplo, en una memoria externa se podría almacenar sin autorización alguna, una gran cantidad de información confidencial e incluso, a través de correo electrónico se podría enviar información confidencial de la organización, con fines distintos a los permitidos, siendo contrario a las buenas prácticas.

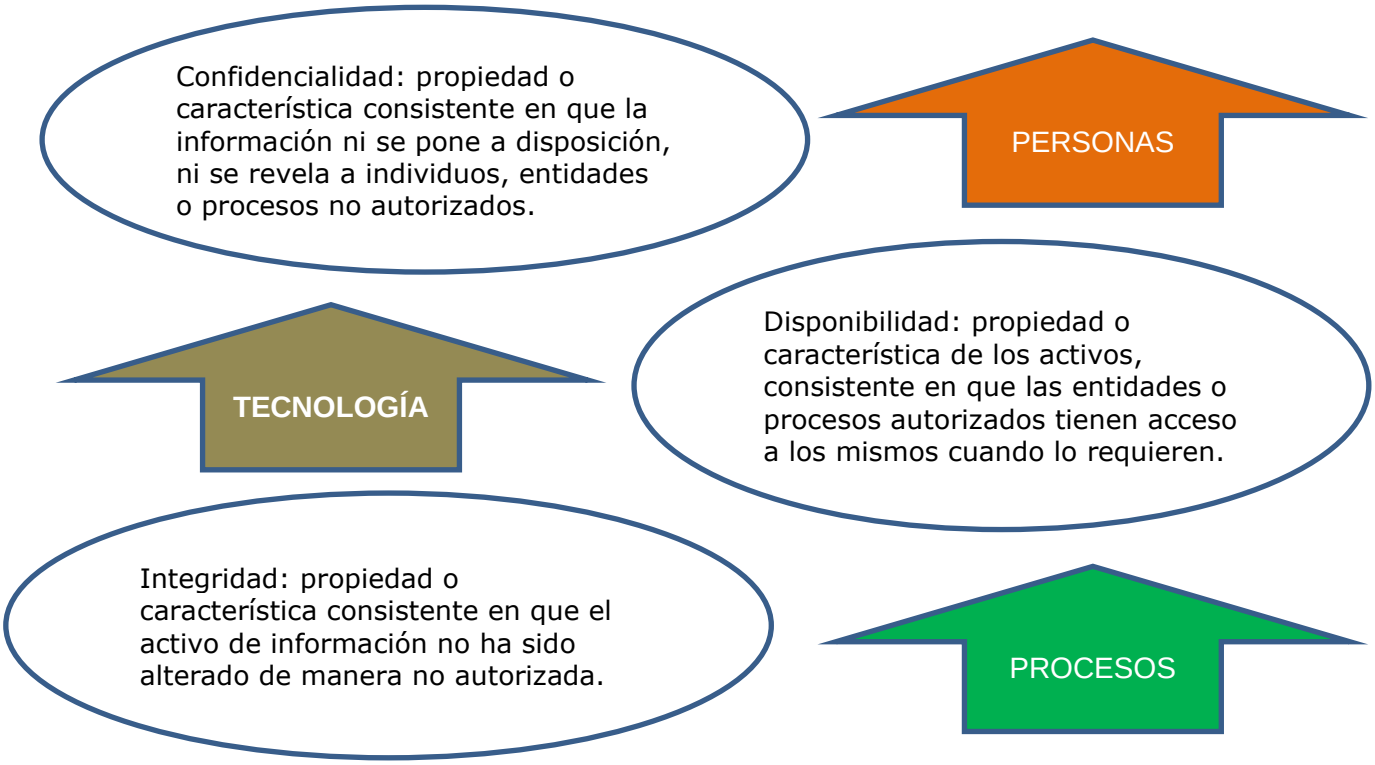
El diseño y la implantación de un SGSI según la Norma ISO 27001 da confianza a clientes y proveedores, preservando la confidencialidad, integridad y disponibilidad de la información, siendo el medio más eficaz para la minimización de riesgos de seguridad de la información, al asegurar que se identifican y valoran los procesos de negocio y/o servicios de TI, los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes en línea con la estrategia de negocio.

Aunque la tecnología es un elemento indispensable de cualquier organización, debe utilizarse de forma adecuada para evitar riesgos en la gestión de la información. Por tanto, es de extrema importancia que se adopten las decisiones y medidas necesarias antes de que se produzca un incidente de seguridad de la información.

El SGSI también tiene como propósito el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de la organización y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas a la seguridad de la información.

DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN.

La seguridad de la información se articula sobre tres dimensiones, que son los pilares sobre los que aplicar las medidas de protección de la información:



ELEMENTOS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

La norma internacional UNE -ISO/IEC 27001:2023, especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua del SGSI en el contexto de la organización, incluyendo los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de la información que se deberán analizar para su disposición y tratamiento a la medida de las necesidades de la organización.

Dichos requisitos, son genéricos y aplicables a cualquier organización, independientemente de su tipo, tamaño, naturaleza y sector. Sin embargo, para poderse certificar por una Entidad de Certificación, el SGSI conforme a UNE -ISO/IEC 27001:2023, deben incluirse elementos como:

4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
7. Soporte.
8. Operación.
9. Evaluación del desempeño.
10. Mejora.

VENTAJAS DEL ASESORAMIENTO EXPERTO SOBRE EL SGSI.

La evaluación de los objetivos de control y controles que se corresponden directamente con los que figuran en la Norma ISO/IEC 27002:2023, capítulos 5 a 18, deben ser empleados en el contexto que se debe definir para efectuar un proceso de tratamiento de los riesgos de la seguridad de la información

Para ello contar con un asesoramiento experto es fundamental. El SGSI promovido por CONTROL ALT SUP, tiene las siguientes ventajas:

a) Conocimiento sobre cuál de las dimensiones de seguridad es más importante proteger en cada sistema de información.

b) Establecimiento de los activos de información de la organización en relación a las dimensiones de la seguridad.

c) Apreciación de los riesgos en función de las amenazas y consecuencias en cada activo de la información.

d) Disposición de información para determinar la dirección a seguir en la implantación y selección de medidas técnicas y organizativas.

e) Claridad en la selección de objetivos, medidas y salvaguardas.

f) Verificación de los controles determinados para asegurar que no se pasa por alto ninguno necesario.

g) Elaboración de la Declaración de Aplicabilidad, que contenga la justificación de las inclusiones, estén implementadas o no, y la justificación de las exclusiones de los controles.

h) Ayuda externa para establecer la gestión de la información documentada, incluyendo la relativa a las no conformidades.

i) Asesorar en el seguimiento, medición, análisis y evaluación.

j) Llevar a cabo la auditoría interna e informar sobre la revisión por la dirección.

Se debe tener en cuenta que hay decisiones complejas que interfieren entre determinados elementos del SGSI. Por ejemplo, la adopción de un determinado control para mejorar la seguridad en una dimensión, puede afectar de forma negativa o positiva a otra de las dimensiones.

O también, que sea necesario implantar un control de acceso para proteger un activo en cuanto a su confidencialidad, que puede producir un retardo en el acceso a la información afectando a su disponibilidad, lo cual no sería lo más adecuado.

Asimismo, asesorar e informar a la organización sobre cómo puede mejorar de manera continua, manteniendo la idoneidad, adecuación y eficacia del SGSI y, más concretamente, en relación a la consecución y mantenimiento de la Certificación en base a ISO 27001, en fundamental para que el Cliente se centre en los aspectos clave y su reprocesamiento.

Para saber más:

https://garanteprivacy.es/

https://controlaltsup.com/

91 109 05 11
info@controlaltsup.com
C/ Puerto de la Cruz Verde, 26. 28045 - Madrid