

SISTEMA DE GESTIÓN
DE SEGURIDAD DE
LA INFORMACIÓN
ISO 27001:2022



SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En el mundo actual, en donde las tecnologías de la información tienen un rol clave para que las organizaciones presten sus servicios de forma virtual, operen de forma remota y cada vez más automatizada, y donde la información es cada vez más un factor clave para el éxito, es necesario establecer mecanismos de “Seguridad de la Información”, con el objetivo de mantener de manera fiable, la protección de los sistemas y la información, para evitar alteraciones malintencionadas o por error y que su acceso se permita exclusivamente a personas autorizadas en la forma debida, es decir, asegurar la seguridad de la información en cuanto a la confidencialidad, integridad y disponibilidad de la información y los datos.

ISO 27001:2022, establece las pautas generales para un Sistema de Gestión de la Seguridad de la Información (SGSI). Incluye como identificar los riesgos de seguridad de la información y como planificar, implementar, operar, mantener y actualizar una serie de estrategias y acciones, para minimizar la probabilidad y el impacto que pueda tener algún incidente malintencionado o por error, que ponga en riesgo la información.

¿PARA QUÉ?

Las organizaciones y sus colaboradores actualmente realizan sus operaciones mediante el móvil, el internet o mediante sistemas digitales de alta velocidad, con los cuales se conectan desde los hogares, escuelas, trabajo, un café internet o en el sitio remoto de trabajo, y así exponen a la información de la organización a una serie de amenazas cada vez más novedosas, que ponen en riesgo la continuidad del negocio, o se exponen a demandas externas por manejo inadecuado de esta información, muchas veces propiedad de terceros.

Para ello y mediante ese estándar de Buenas Prácticas de Seguridad de la Información ISO 27001:2013, se establecen acciones y mecanismos de control, que nos permitan operar con mayor tranquilidad, y sobre todo garantizar a los clientes, a los colaboradores, o a las partes interesadas, que su información se encuentre segura. Además, se maneja de forma confidencial, es decir, está disponible solo para aquel personal autorizado en dónde su integridad se mantiene confiable.

BENEFICIOS

- ❖ Reduce el riesgo de que se produzcan pérdidas de información en las organizaciones.
 - ❖ Prevención y revisión continua de los riesgos y controles de seguridad de la información.
 - ❖ Define metodologías estándares para gestionar la seguridad de la información. Identifica y atiende riesgos de seguridad para clientes, colaboradores, proveedores y partes interesadas, considerando el manejo seguro de la información.
 - ❖ Brinda mecanismos para restablecer la continuidad del servicio en el menor tiempo posible, en el caso de materializarse amenazas, tales como ataques cibernéticos.
 - ❖ Brinda garantía y confianza frente a clientes, socios estratégicos y proveedores. Garantiza cumpliendo la legislación vigente en materia de información personal y propiedad intelectual.
-

¿QUÉ ORGANIZACIONES REQUIEREN LA CERTIFICACIÓN DE LOS SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2022?

- ❖ Proveedores de cadenas de servicios, multinacionales. Proveedores del estado.
 - ❖ Proveedores del sector de banca.
 - ❖ Proveedores en general de banco de datos, software, aplicaciones, integradores y servicios de comunicación.
 - ❖ Usuarios de información en la nube.
 - ❖ Proveedores de productos o servicios de consumo masivo o crítico.
 - ❖ Banca u organizaciones de carácter financiero.
-

LOS SISTEMAS DE SEGURIDAD
DE LA INFORMACIÓN
DESEMPEÑAN UN PAPEL
CRÍTICO EN LA TOTALIDAD DE
LAS EMPRESAS.

CONTACTO@GCBGLOBAL.COM



GLOBAL CERTIFICATION
BUREAU