POLÍTICA GENERAL DE CALIDAD Y DE SEGURIDAD DE LA INFORMACIÓN

Propósito

La alta dirección manifiesta su compromiso de establecer, implementar y mantener la política general de calidad y de seguridad de la información, para realizar las actividades y el buen funcionamiento de OG CONSULTORES.

La Gerencia General entiende que, dada la naturaleza de las actividades que OG CONSULTORES desarrolla, la calidad de dichas actividades es un valor esencial para garantizar la credibilidad de la organización y la confianza que han depositado en ella los clientes, proveedores, la administración, la sociedad en general.

El uso de las tecnologías de la información hace necesario que la organización tenga el propósito de proteger los activos de información de las amenazas, internas o externas, deliberadas o accidentales de OG CONSULTORES y de los clientes.

Objetivos

La implantación de esta política es importante para mantener y demostrar nuestra integridad en la conducta de los negocios con las partes interesadas.

Los compromisos acerca de calidad se concretan en los siguientes aspectos:

- Siendo apropiada y de orientación al contexto de la organización establecidos en el plan estratégico de OG CONSULTORES, para el adecuado establecimiento de los objetivos de calidad y por consiguiente el logro de los objetivos estratégicos.
- Cumplir con los requisitos regulatorios, legislativos y compromisos OG.
- Abordar y gestionar los riesgos y las oportunidades de calidad y seguridad de la información.
- La mejora continua del sistema de gestión de la calidad y seguridad de la información.

Los compromisos acerca de la seguridad engloban:

- Que la información sea protegida contra el acceso no autorizado.
- Que la confidencialidad de la información sea mantenida.
- Que la información no sea revelada a personas no autorizadas a través de acciones deliberadas o descuidadas.
- Mantener la integridad de la información a través de la protección de modificaciones no autorizadas.
- Mantener la disponibilidad de la información para usuarios autorizados cuando lo requieran.
- Que el plan de continuidad de negocio sea generado, mantenido y probado.
- Que todos los colaboradores sean capacitados en seguridad de la información.
- Todos los incumplimientos con la seguridad de la información, las vulnerabilidades sospechosas serán informadas e investigadas.