

ISO 27001:2013 NMX-I-27001-NYCE-2015

Evaluamos y certificamos la conformidad del **sistema de gestión de seguridad de la información**, implementado en su organización conforme a lo establecido en la norma de referencia **ISO 27001:2013**.



BENEFICIOS DE LA CERTIFICACIÓN

- Identificación de los riesgos y controles de seguridad de la información en el sitio para gestionarlos o eliminarlos.
- Flexibilidad para adaptar controles de seguridad de la información a todas las áreas de la organización.
- Confiabilidad en la protección de los datos del cliente.
- Fomenta el cumplimiento de las leyes y normativas que sean de aplicación.
- Proceso de evaluaciones periódicas, ayuda a supervisar continuamente el rendimiento y la mejora del **sistema de gestión de seguridad de la información**.

REQUISITOS PARA INICIAR EL PROCESO DE CERTIFICACIÓN

- **Determinación del alcance de la certificación:**

Para definir el alcance de su sistema le sugerimos que considere si desea implementarlo en toda la organización o tan solo en parte.

- **Tener implementado un sistema de gestión de seguridad de la información:**

El tiempo para la implementación de su sistema generalmente depende de las medidas de seguridad que se establezcan dentro de la Organización y del tiempo que tardan en implementarse las mismas.



PROCESO DE CERTIFICACIÓN

- Solicitar de manera formal la certificación del sistema de gestión de seguridad de la información.
- Para la realización del proceso inicial de certificación, se realizan las etapas 1 y 2.

AUDITORÍA ETAPA 1

Consiste en verificar si el **sistema de gestión de seguridad de la información**, contempla todos los elementos señalados por la norma de referencia, así como la viabilidad para realizar la auditoría de etapa 2. Para su realización, es necesario la documentación de soporte requerida, incluyendo:

- Políticas, procedimientos e implementación técnica.
- Implementación de medidas de seguridad de la información.
- Los requisitos legales y reglamentarios aplicables en materia de seguridad de la información.
- Evaluación y tratamiento de riesgos.
- El desarrollo de la revisión por la dirección y la auditoría interna.

AUDITORÍA ETAPA 2

Consiste en la visita de un equipo auditor en las instalaciones de la organización; para evaluar la conformidad e implementación del **sistema de gestión de seguridad de la información** con la norma de referencia. El equipo auditor decide si, con base a los resultados, se recomienda que el expediente del cliente pase a dictamen de un comité de certificación.

Sí, la dictaminación resulta favorable, se otorga la certificación correspondiente.

