

Deloitte.

Information •
Security
Community

Gobierno, riesgo y cumplimiento





GOBIERNO

Proceso por el cual políticas y objetivos son establecidas, mantenidas y efectivamente comunicadas a toda la organización.



RIESGOS

Proceso que asegura que las decisiones importantes del negocio permanezcan acorde al nivel de riesgo y a la tolerancia de riesgo aceptable según los objetivos estratégicos de la organización.



CUMPLIMIENTO

Proceso de adherencia a las políticas y sus controles asociados, derivados de directivas internas, procedimientos, requerimientos, leyes externas, regulaciones, estándares y/o acuerdos contractuales.

Herramienta GRC

Una herramienta GRC mantiene **la relación entre** procesos de negocio, regulaciones, normas, riesgos, controles e incidentes **para gestionar el cumplimiento de objetivos**



Sistema de Gestión de Seguridad de Información (SGSI)

- Sistema de administración **de una organización que coordina** y atiende la **Gestión de Riesgos** de Seguridad de Información (**Confidencialidad, Integridad, y Disponibilidad**) mediante un ciclo de mejora continua.
- Un SGSI **proporciona un modelo** para establecer, implementar, operar, monitorear, revisar, mantener y mejorar **la protección de los activos de información** para lograr **los objetivos del negocio** administrando **los riesgos en niveles aceptables**.
- El estándar utilizado para crear y mantener un SGSI es **ISO 27001:2013**.

Modelo de mejora continua de un SGSI

- Objetivos, alcance y políticas
- Proceso de Administración de Riesgos SI (CIA, amenazas, y vulnerabilidades)
- Procesos de Auditoría, Acciones Correctivas, Incidentes, Vulnerabilidades



- Implementación de Mejoras
- Implementación de AC*
- Comunicar resultados al CSGSI**

- Capacitación
- Cumplimiento Técnico de SI
- Tratamiento de Riesgos: mitigar con controles o aceptar riesgos
- Auditoría
- Definición de indicadores
- Arquitectura Técnica de Seguridad

- Monitoreo
- Medición de Efectividad
- Riesgo residual
- Auditoría interna
- Revisión por el CSGSI**

Necesidades de SGSI

- Definir un alcance (objetivos, procesos, servicios, activos, geográfico)
 - Modelo de gestión de riesgos
 - Diseñar e implementar controles versus riesgos
 - Revisión y cumplimiento de controles de ISO 27001:2005
 - Gestión de la declaración de aplicabilidad (SoA)
 - Gestión de políticas y normas de SI
 - Gestión de plan de tratamiento de riesgos
 - Gestión de incidentes SI
 - Gestión de vulnerabilidades
 - Gestión de control de acceso
 - Auditorías Interna y Externa
 - Monitoreo continuo de eficiencia y eficacia de controles
 - Indicadores del SGSI alineado con Negocio
- Gobierno**
- Riesgos**
- Cumplimiento**

Sinergias GRC

SGSI

Un SGSI puede **establecer o reutilizar** elementos de GRC:

- **Repositorio único para la gestión empresarial** de riesgos y controles
- **Identificación centralizada** de dueños de negocio y de riesgos empresariales; y también de Custodios de activos y controles
- **Modelo único de riesgos empresarial** (evitar re-trabajos, silos, metodologías aisladas)
- Usar el Modelo de **Control Interno y Administración** de la empresa (**organización, responsables y funciones**)

Sinergias GRC

SGSI

- **Integración para la gestión de hallazgos y Acciones Correctivas de Auditoría y Control**
 - Un hallazgo – Un riesgo – Una acción – Un responsable – Un plan
- Es un **subconjunto o vista** del modelo de **Gobierno y Control Interno** con un **enfoque a Seguridad de información y un alcance preestablecido**
- **Es un caso de uso útil** que utiliza y mide componentes de Control Interno, como:
 - Regulaciones aplicables
 - Procesos de negocio
 - Inventario de Activos de Información
 - Monitoreo continuo de controles
 - Roles y responsabilidades de activos y controles
 - Continuidad de Negocio



Deloitte se refiere a Deloitte Touche Tohmatsu Limited, sociedad privada de responsabilidad limitada en el Reino Unido, y a su red de firmas miembro, cada una de ellas como una entidad legal única e independiente. Conozca en www.deloitte.com/mx/conozcanos la descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Deloitte presta servicios profesionales de auditoría, impuestos, consultoría y asesoría financiera, a clientes públicos y privados de diversas industrias. Con una red global de firmas miembro en más de 150 países, Deloitte brinda capacidades de clase mundial y servicio de alta calidad a sus clientes, aportando la experiencia necesaria para hacer frente a los retos más complejos de los negocios. Cuenta con más de 200,000 profesionales, todos comprometidos a ser el modelo de excelencia.

Tal y como se usa en este documento, “Deloitte” significa Galaz, Yamazaki, Ruiz Urquiza, S.C., la cual tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría, consultoría fiscal, asesoría financiera y otros servicios profesionales en México, bajo el nombre de “Deloitte”.

Esta publicación sólo contiene información general y ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro, ni ninguna de sus respectivas afiliadas (en conjunto la “Red Deloitte”), presta asesoría o servicios por medio de esta publicación. Antes de tomar cualquier decisión o medida que pueda afectar sus finanzas o negocio, debe consultar a un asesor profesional calificado. Ninguna entidad de la Red Deloitte, será responsable de pérdidas que pudiera sufrir cualquier persona o entidad que consulte esta publicación.