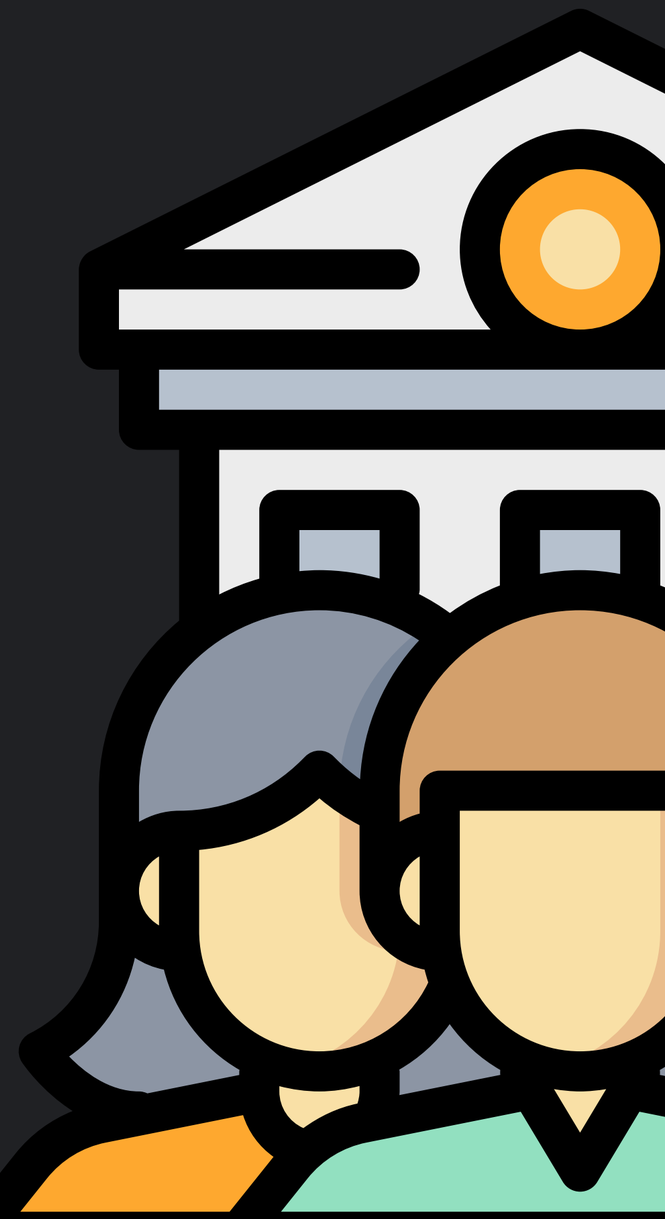
ISO 27001

IT Governance

04/03/2022

Martínez Coronel
Brayan Yosafat



Itinerario 1/2

- ¿Qué es?
- ¿Para qué sirve?
- Propósito
- Principios
- Beneficios
- Herramientas
- Relación con frameworks

Itinerario 2/2

- Relación con el modelo Calder Moir
- Enfoque de TI
- Costo
- Público a certificar
- Vigencia de la certificación
- Organismo que lo avala

Qué es

Se trata de una norma internacional que permite el aseguramiento, la confidencialidad y la integridad de los datos y la información. Así como la de los sistemas que la procesan.

La última versión es la ISO 27001:2013 para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Para qué sirve

Permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigar esos riesgos, y en el mejor de los casos, eliminarlos.

Propósito

Pretende minimizar los riesgos, asegurando que se identifiquen y valoren los procesos del negocio y/o servicios de TI, activos y sus riesgos, considerando el impacto para la organización, mediante controles y procedimientos eficaces y coherentes con mejoras contínuas.

Principios

Algunos de los principios que sigue son:

- Liderazgo: Todos en la empresa deben comprometerse para establecer la norma en la empresa, especialmente la alta dirección.
- Planificación y Evaluación: Una vez implementadas, se debe dar un seguimiento y se debe de mejorar contínuamente.
- Operación y Soporte: Se debe contar con los recursos para que se implemente realmente en los procesos de la empresa.

Beneficios

Está diseñada para ser implementada en cualquier tipo de empresa, sin importar su tamaño o tipo, además de ser una de las más usadas en todo el mundo. Por lo que generará confianza en cuanto se tenga la certificación de alguna de las entidades que pueden avalar la misma.

Herramientas

Utiliza políticas en general. Sin embargo, siendo más precisos, tiene 10 artefactos (documentos):

- Documento de la Política
- Alcance del SGSI
- Análisis de Riesgos
- Resultados (de Riesgo)
- Controles seleccionado
- Declaración de aplicabilidad
- Revisión del SGSI
- Plan de auditorías

Frameworks relacionados

La norma ISO 27001 está basada en el marco de trabajo británico conocido como BS 77699-2, se considera una ampliación del mismo. Además de que, suele complementarse con la ISO 27002.

Segmentos en Calder Moir

Definitivamente esta certificación abarca en todas partes del hexágono, desde las claras hasta las oscuras, ya que, se pide el compromiso de todas las partes para cumplir la norma. Y los 6 segmentos los abarca porque lleva a la empresa desde el análisis, la planeación, la ejecución, la evaluación y la mejora durante todo el tiempo que se implementa, e incluso se tiene la certificación.

Enfoque de TI

Definitivamente integra todas las áreas. Pero, claro, principalmente las que sean de Recursos y Medición de desempeño, ya que son las que obtienen los resultados de cómo se está aplicando el proceso. Sin embargo, debemos considerar que esta es una certificación bastante integral y desde el comienzo se pretende involucrar toda la empresa y sus trabajadores.

Costo

Es bastante variable, ya que depende de:

- El tamaño de la organización
- El alcance definido de la implementación
- La madurez del sistema de seguridad
- El nivel de criticidad de la información
- La rápidez con la que se pretende certificarse
- Los recursos internos que se puedan dedicar al proceso
- La legislación en la que esté la empresa

Público a certificar

Solo se certifica a la empresa en conjunto, sin embargo, se capacita a todo el personal.

Vigencia

Después de que el auditor avale que se implementó, se da un certificado de 3 años, en ese tiempo se puede perder en las auditorias.

Certificador

Existen diversas organizaciones que tienen la capacidad de certificar, y sus procesos de auditoría varían un poco. Pero todas están avaladas ante la Organización Internacional de Normalización (ISO)

¡Muchísimas gracias!