TUTORIAS
Tu Certificación a un Click

INTRODUCCION ISO/EIC 27001 – SEGURIDAD DE LA INFORMACION

CONTENIDO

TUTORIAS
Tu Certificación a un Click

01 Sociedad de la información

La Sociedad de la Información
Como influye en la sociedad
Características
Tipos de información

02 Riesgo

Que es el riesgo?
Como medir el riesgo?
Como afecta el riesgo a una organización?

03 ISO 27001

ISO27001 – Qué es?
ISO 27001 – Importancia en una organización

04 ISO 27001 - SGSI

Definición del SGSI
Bases del SGSI – Uso
Beneficios del SGSI

05 ISO 27001 – SGSI Estructura

Componentes del SGSI

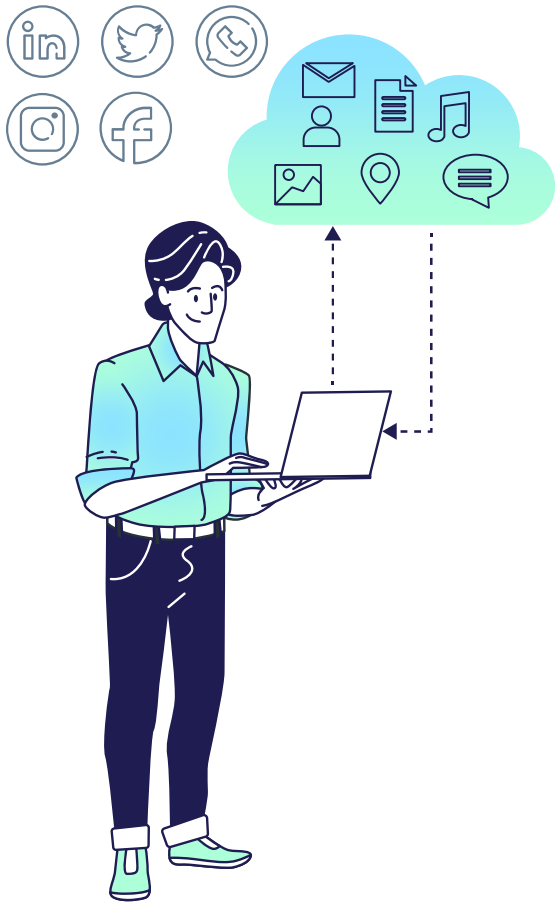
Sociedad de la Información

- Hace referencia a que la información de cualquier naturaleza, su generación, su distribución y su uso se han convertido en el eje fundamental de todo lo que hacen los seres humanos.
- Se la asocia con la evolución de la organización industrial a otra postindustrial o de la información
- Se la relaciona también con la idea de conocimiento : Sociedad de la Información y Conocimiento
- Implica beneficios sociales, culturales, económicos.

Características

La sociedad de la información se caracteriza :

- Impulsar la globalización mediante uso de las TIC
- Fomentar el conocimiento, el aprendizaje
- Mantener el flujo de información dentro de una generación, organización
- Permite una mayor influencia de la sociedad en decisiones
- Fomentar la interconexión remota, para fines laborales, estudiantiles, etc.
- Optimización de procesos industriales que convergen hacia la transformación digital.

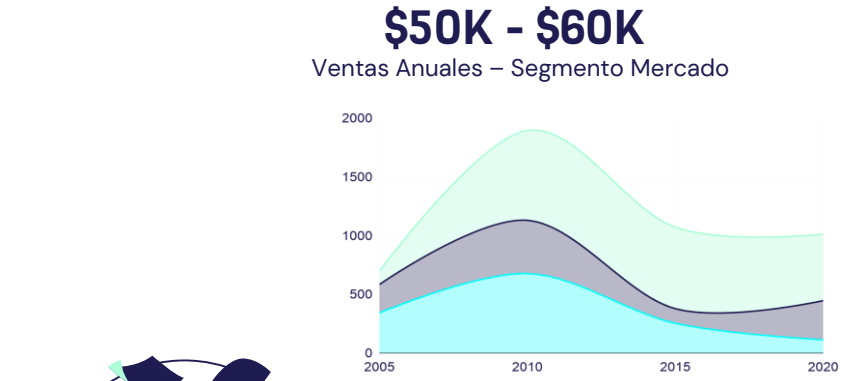


Tipos de Información

- Información privada / clasificada Direccionada a usuarios específicos
- Información pública: de conocimiento y acceso a todo el público en general
- Información personal – redes sociales, fotos, ubicaciones, publicaciones.
- Información de empresas (interna / externa)

Interna: Conocida por un determinado grupo de personas (proyecto / desarrollo de una marca/ formulas)

Externa: Aquella que nos permite poder gestionar temas en específico, para valorar la competencia (estudios de mercado / benchmarking)



02. Riesgo

Se define como riesgo a la combinación de eventos que pueden o no producirse y sus probables consecuencias.

Es también una definición para el riesgo aquello que causa INCERTIDUMBRE para un escenario conocido o desconocido.

INCERTIDUMBRE: Es la falta de conocimiento acerca de un evento que reduce la confianza en las conclusiones extraídas de datos (calidad, costos, comunicaciones)

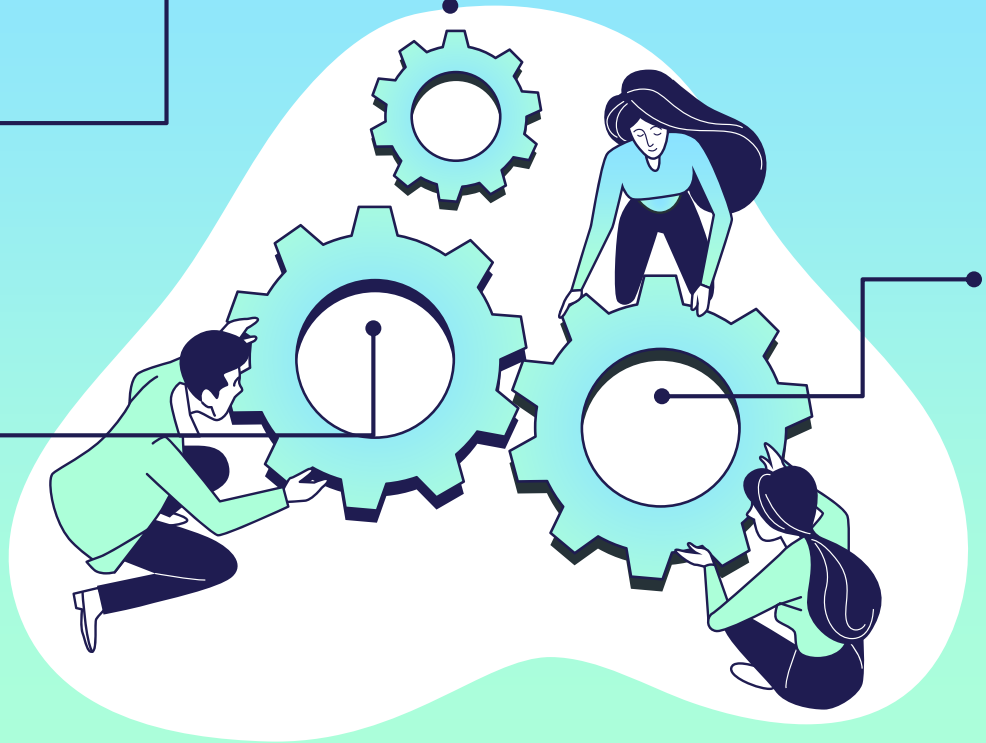
Riesgos - Tics

- Riesgo de Integridad: asociado con la autorización, acceso, procesamiento aplicaciones, información de una organización
- Riesgo de Relación : uso oportuno de la información creada por una aplicación (toma de decisiones)
- Riesgo de Acceso : Riesgos enfocados al inapropiado acceso a sistemas, datos, información de la organización (sistemas de bases de datos)
- Riesgos de infraestructura (relacionado directamente a la infraestructura informática de una organización)
- Riesgos de Seguridad General

Riesgo : Factores de Riesgo

Probabilidad de Ocurrencia

Frecuencia Anticipada del evento



Rango posible de salidas (Impacto)

Medición del Riesgo

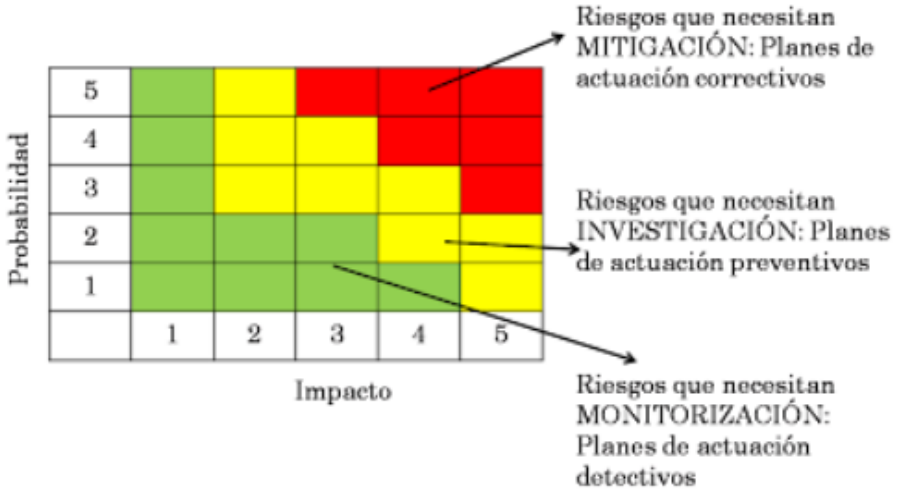
Con el fin de poder darle una categoría tanto cualitativa como cuantitativa a los riesgos, se deberán aplicar varios artefactos.

Se determina como probabilidad como a la frecuencia de un acontecimiento, de la misma manera el impacto es el efecto a la materialización de una consecuencia (planeada o aleatoria)

Probabilidad : Que tan probable es que ocurra el daño de un servidor central?
Impacto : que efecto, que causaría el daño del servidor central en mi organización?

Riesgo: Matriz de Probabilidad e Impacto

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

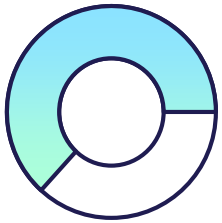


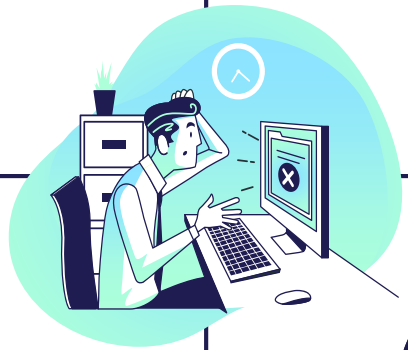
Impacto de riesgo - Organización

60%

50%

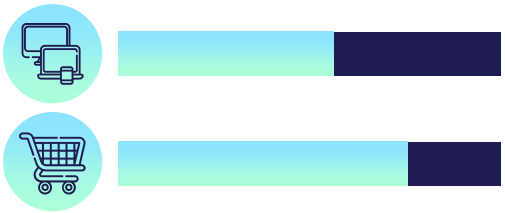
Deserción Clientela



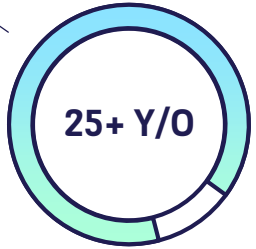


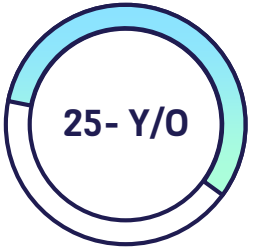
$50K - $60K

Perdidas Tangibles (Multas Económicas)

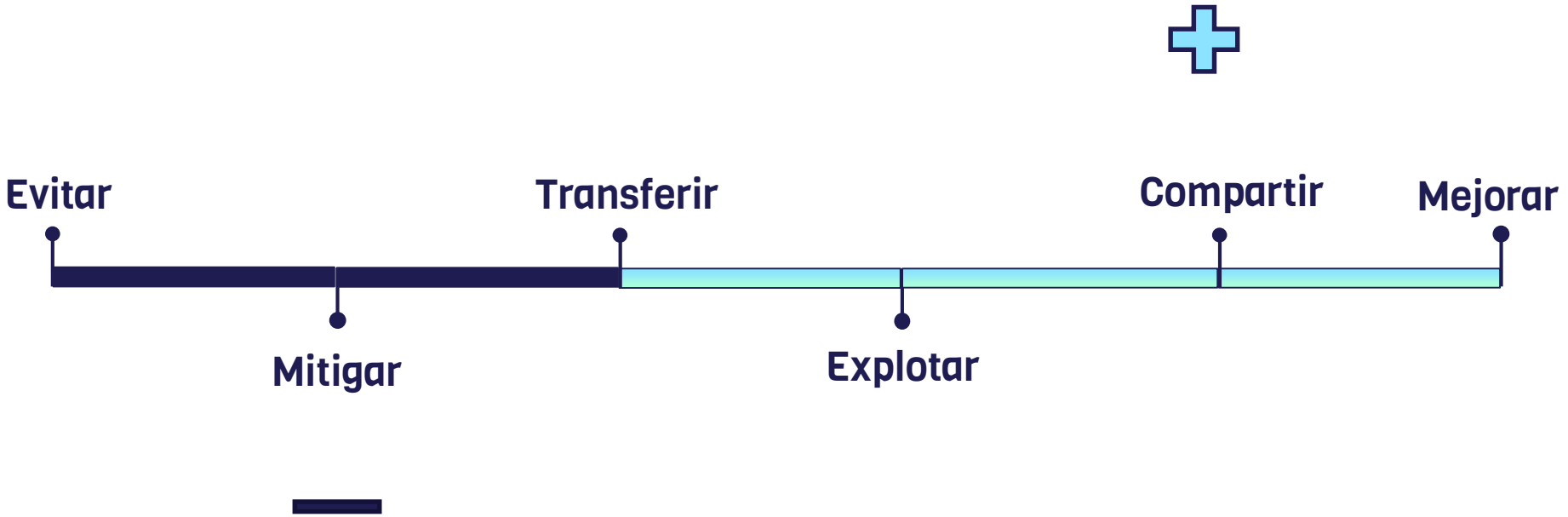


Perdidas Intangibles (Marca, Categorización)





Respuestas al Riesgo (Estrategias)




ISO/IEC 27001

TUTORIAS
Tu Certificación a un Click

03. ISO / IEC 27001

Estándar internacional que define una serie de requerimientos para la gestión de seguridad de la información, donde la evaluación del riesgo es el punto mas importante.

Es una solución de mejora continua en base al cual puede desarrollarse un SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI) que permite evaluar los riesgos o susceptibilidades que puedan poner en peligro a una organización tanto propia como de terceros.

- Permite establecer controles y estrategias adecuadas para poder eliminar riesgos o minimizar su impacto dentro de la organización.

Importancia en la organización (Empresa)

La información, junto a los procesos y los sistemas que hacen uso de ella, son activos demasiado importantes para la empresa, de dicha información puede ser esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la empresa necesarios para conseguir los objetivos de la empresa y asegurase de que haya beneficios económicos.

El cumplimiento de la legislación, la adaptación dinámica y de forma puntual de todas las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar que se obtiene el máximo beneficio son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las empresas.

04. SGSI (Sistema de Gestión de Seguridad de la Información)

SGSI es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información

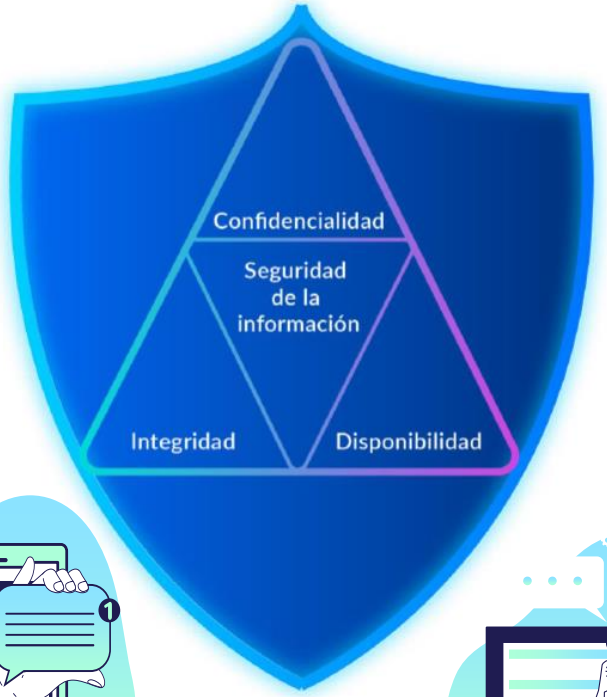
Podemos entender por información todo el conjunto de datos que se organizan en una organización y otorgan valor añadido para ésta, de forma independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración.

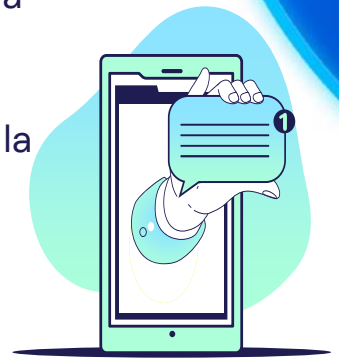
El Sistema de Gestión de Seguridad de la Información, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

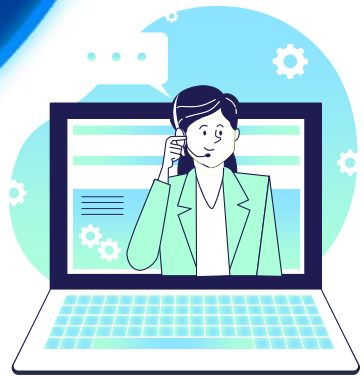
Triada CID

Un SGSI define 3 dimensiones principales

- Disponibilidad – la información debe ser accesible y utilizable
- Confidencialidad – la información debe estar disponible para los usuarios de la organización, siempre y cuando tengan la autorización para su uso/manejo
- Integridad – propiedad de salvaguardar la exactitud y estado de los activos







Beneficios – Aplicación SGSI

- Generación de conciencia en la organización en la necesidad de la seguridad de la información
- Asignación de responsabilidades en seguridad de la información
- Compromiso de la Alta Dirección
- Gestión de Riesgos para determinar controles y acciones adecuadas
- Establecer a la seguridad de la información como componente esencial de los procesos de la organización
- Mejora continua de los procesos a través de la seguridad de la información

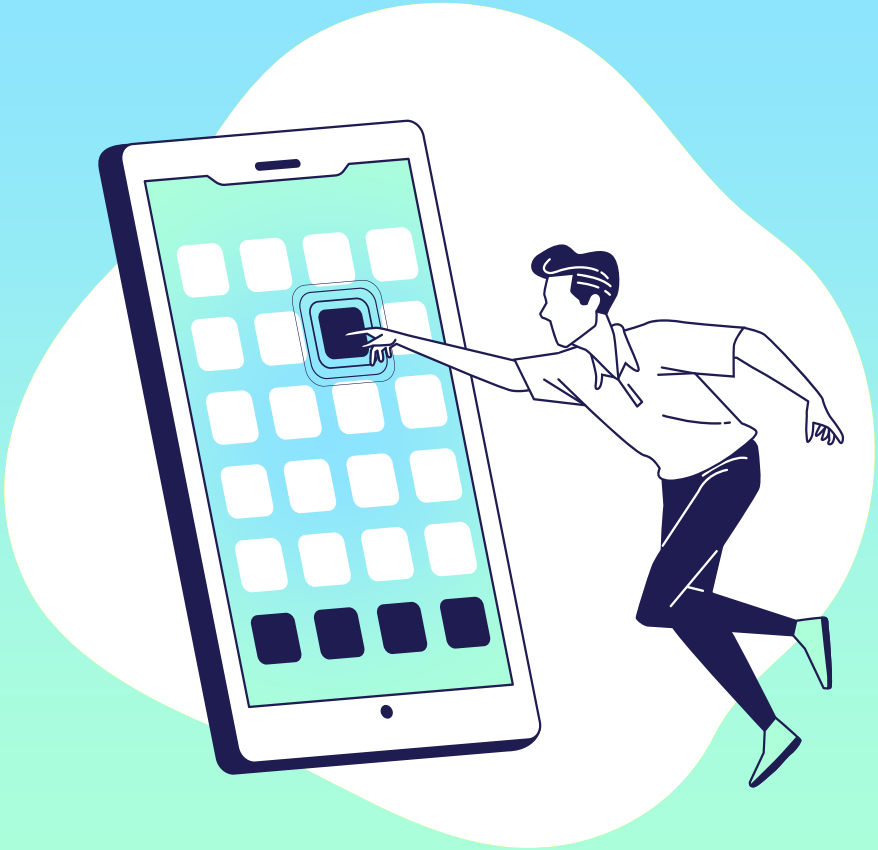
05. ESTRUCTURA DEL SGSI

TUTORIAS
Tu Certificación a un Click

Estructura ISO/IEC 27001

1. Introducción
2. Alcance
3. Referencia normativa
4. Términos y definiciones
5. Contexto de la Organización
6. Liderazgo
7. Planificación
8. Soporte
9. Operación
10. Evaluación de desempeño
11. Mejora

Estructura ISO/IEC 27001



Gracias!

website: www.tutorias.ec

Síguenos en nuestras redes

Tutorias Ec

@tutoriasecuador

@tutorias_ec