



# SGSI: ¿Qué es?


# ¿Quien soy?


**Rodolfo Schonhals**

**Técnico Superior en Programación**
**Licenciado en Sistemas**

**Auditor Interno ISO 9001 y 27001**

**Incursionando en ISO 22301 e IRAM 90600**

**Miembro de LUG Paraná desde 2005**


# SGSI: ¿Qué es?


¿La información es un activo de la organización?


# ¿Cual es el problema?


- La información y los sistemas se encuentran expuestos a amenazas físicas y lógicas.
- Aún se mantiene la idea que la información no es un activo


# ¿Qué se propone?


Implantar un **S**istema de **G**estión de **S**eguridad de la **I**nformación

# SGSI: ¿Qué es?

Es un proceso sistemático, documentado y conocido por toda la organización desde un enfoque de riesgo empresarial

# CID

La seguridad de la Información,
según ISO 27001,
consiste en la preservación
de tres pilares fundamentales


# CID


# Confiabilidad

La información no se pone a disposición ni se revela a individuos, procesos y terceros no autorizados


# CID


# Integridad

El mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.


# CID


## Disponibilidad

Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.


## SGSI: ¿Qué es?


# ¿Porqué es necesario un SGSI?

# ¿Es necesario?

Para mantener los niveles de competitividad, rentabilidad, imagen y conformidad legal necesarios para el logro de los objetivos organizacionales asegurando los beneficios económicos


# ¿Es necesario?


Para gestionar la seguridad de forma efectiva, tomando parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

# ¿Es necesario?

Para planificar e implantar controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

# Riesgos


Amenazas
Aprovechan
Vulnerabilidades
Protegen de
Aumentan
Aumentan
Exponen
Controles
Disminuyen
Riesgos
Activos
Imponen
Marcan
Impactan si se materializan
Aumenta
Tienen
Requerimientos de seguridad
Valor de los activos
Fuente: www.ISO27000.es


# SGSI: ¿Qué es?


¿Cómo está compuesto un SGSI?

# SGSI: ¿Qué es?


PIRAMIDE DOCUMENTAL
Política SGI
1
Manual SGI
1
Procedimiento y programas
31
Instructivos
10
Formatos/Registros
50
93 Documentos

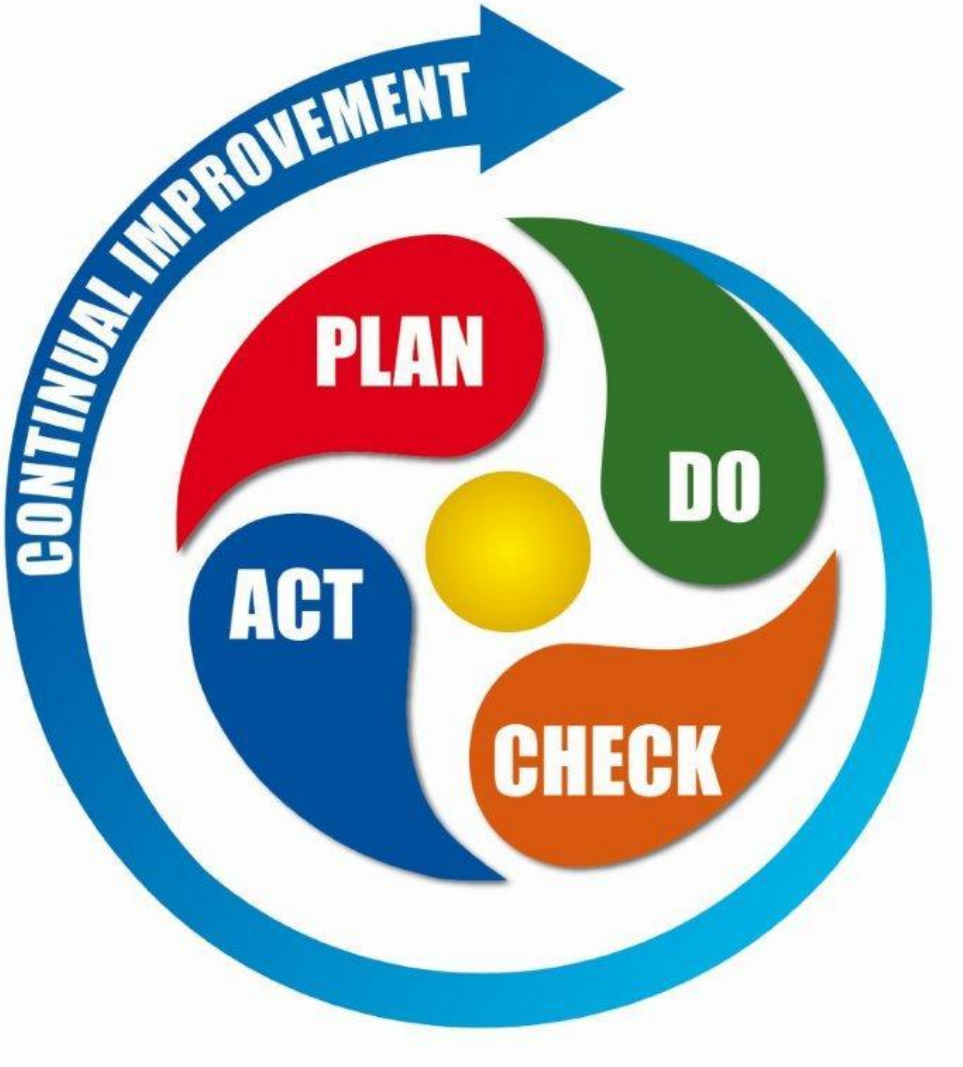

# SGSI: ¿Qué es?


¿Cómo se implanta y mantiene un SGSI?

ISO 27001

# Mejora continua!

PARANA CONF




# Mejora continua!


## Plan (planear)


# PLAN


- Alcance
- Política
- Identificación y evaluación de riesgos
- SOA
- Elección de controles


# Mejora continua!


## Do (hacer)

# DO

- Definir e implantar el plan de tratamiento de riesgos
- Implantar controles
- Formación y concienciación
- Gestionar operaciones y recursos


# Mejora continua!


## Check (Verificar)


# CHECK


- Ejecución y monitoreo de procedimientos para:
  - detectar errores
  - identificar incidentes y brechas
  - detectar y prevenir incidentes mediante indicadores
  - etc...


# CHECK


- Realizar auditorías internas
- Revisar el SGSI por parte de la dirección
- Actualizar planes de seguridad


# Mejora continua!


## Act (Actuar)

# ACT

- Implantar las mejoras encontradas
- Realizar acciones preventivas y correctivas pertinentes
- Comunicar las acciones y mejoras a las partes interesadas

# Conclusiones


- Gestión de proyectos, recursos del proyecto
- El cambio organizacional requiere recursos de la organización
- Diseño, desarrollo, pruebas, implementación
- Certificación y visitas de seguimiento
- Operación y mantenimiento en curso

Fuente: Iso27000.es

- Reduce los riesgos de seguridad de la información
- Reduce la probabilidad y el impacto de los incidentes de seguridad
- La certificación de un estándar internacional
- Ventajas de marketing/marca
- Enfoque coherente, estructurado
- Evaluación integral de riesgos
- Focaliza el gasto en seguridad de la información donde produce mayor ventaja
- Gobernanza demostrable


# SGSI: ¿Qué es?


¿Preguntas?

# SGSI: ¿Qué es?

Fuentes:

www.iso27000.es

www.incibe.es

www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en