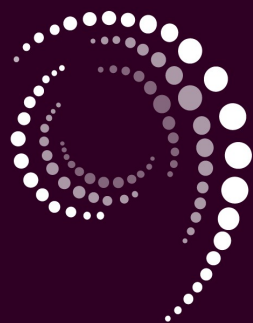




MINISTERIO DE LA PRESIDENCIA
ESTADO PLURINACIONAL DE BOLIVIA



AGETIC

agencia de gobierno electrónico y
tecnologías de información y comunicación

Plan de seguridad institucional

CTIC – Consejo para las Tecnologías de
Información y Comunicación

Grupo de trabajo: Seguridad

El Centro de Gestión de Incidentes Informáticos CGII

MISIÓN

Establecer los lineamientos para la protección de los activos de información críticos del Estado y promover la conciencia en seguridad de la información de manera que prevenga y responda a incidentes de seguridad.

VISIÓN

Ser un centro de respuesta a incidentes en seguridad informática y seguridad de la información y un referente a nivel internacional.

El Centro de Gestión de Incidentes Informáticos CGII

FUNCIONES

Evaluar la seguridad de los sistemas de información de las entidades del sector público, a solicitud de las mismas;

Monitorear los sitios Web gubernamentales y la aplicación de las políticas y lineamientos definidos por la AGETIC

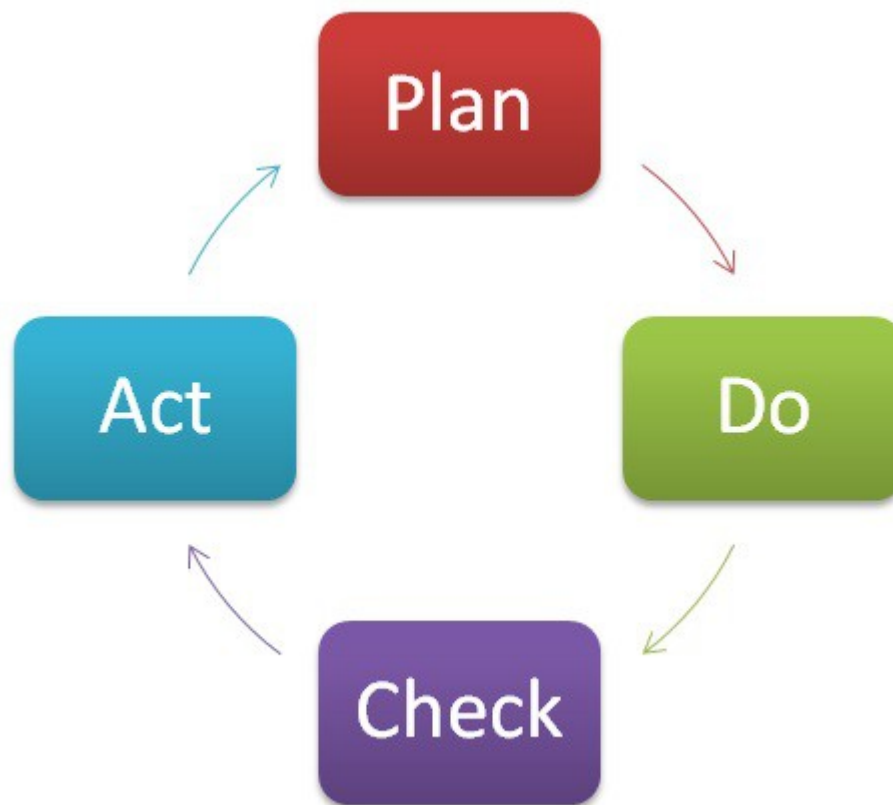
Sistema de Gestión de Seguridad de la Información

El SGSI es el concepto central sobre el que se construye ISO 27001.

Un SGSI es una herramienta de gran utilidad para la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio

Establecimiento y gestión del SGSI

Uso del ciclo de mejora continua



Establecimiento del SGSI

- Definir alcances y límites.
- Definir una política del SGSI.
- Identificar los riesgos.
 - Inventario de activos

Código	Activo
P1	Usuarios externos
P2	Usuarios internos
S1	Repositorio de archivos
SW1	Sistema Gestor de base de datos

Inventario de activos (Magerit)

Establecimiento del SGSI

- Analizar y evaluar los riesgos.

	Valor	Abreviat ura	Descripción
Valoración de los activos	Valor > 200'	MA	Muy alto
	200' > valor > 100'	A	Alto
	100' > valor > 50'	M	Medio
	50' > valor > 10'	B	Bajo
	10' > valor > 1'	MB	Muy bajo

Establecimiento del SGSI

- Analizar y evaluar los riesgos

RIESGO		Impacto				
		MA	A	M	B	MB
Frecuencia	EF	MA	MA	MA	MA	MA
	MF	MA	MA	A	A	M
	F	A	A	M	M	B
	PF	M	M	B	B	MB
	MPF	B	B	MB	MB	MB
	D	MB	MB	MB	MB	MB

Matriz de riesgos

Establecimiento del SGSI

- Identificar y evaluar las opciones para el tratamiento de los riesgos.
 - Aplicar controles adecuados
 - Aceptar el riesgo
 - Evitar el riesgo
 - Transferir el riesgo
- Obtener aprobación de la dirección de los riesgos residuales propuestos.

Implementación y operación

- Implementar un plan para el tratamiento de riesgos.
 - ISO 27001.- 14 Dominios, 35 objetivos de control, 114 controles
- Implementar los controles seleccionados.
- Implementar programas de formación y toma de conciencia.
- Gestionar la operación del SGSI.
- Gestionar los recursos del SGSI.

Seguimiento y revisión

- Emprender revisiones regulares de la eficacia.
 - Definir métricas para los dominios seleccionados
 - Deben medir cosas significativas para el organismo.
 - Deben ser reproducibles.
 - Deben ser objetivas e imparciales.
 - Deben ser capaces de medir algún tipo de progresión en el tiempo.
- Revisar las valoraciones de los riesgos.
- Actualizar los planes de seguridad.
- Emprender una revisión del SGSI

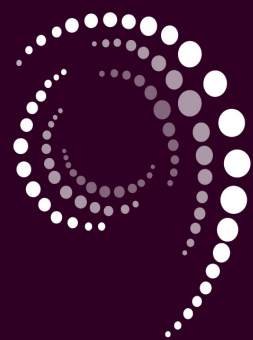


Mantenimiento y mejora

- Implementar mejoras identificadas.
- Empezar las acciones correctivas y preventivas.
- Comunicar las acciones y mejoras a las partes interesadas.
- Asegurar que las mejoras logran los objetivos previstos.



MINISTERIO DE LA PRESIDENCIA
ESTADO PLURINACIONAL DE BOLIVIA



AGETIC

agencia de gobierno electrónico y
tecnologías de información y comunicación

GRACIAS POR SU ATENCIÓN