PROGRAMA DE ESPECIALIZACIÓN EN CIBERDEFENSA Y CIBERSEGURIDAD ESTRATÉGICA
(PECCE)

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Ing. Miguel Toffoletti

AGENDA

1. Introducción
2. Sistemas de Gestión de la Seguridad de la información
3. SGSI basado en ISO 27001
4. Análisis de riesgos basados en objetivos de negocios
5. Concienciación de usuarios en Seguridad de la Información

3. SISTEMA DE GESTIÓN BASADO EN ISO 27.001

3.5. Clausula 4: Contexto de la Organización.

3.6. Clausula 5: Liderazgo

3.7. Clausula 6: Planificación

3.8. Plan de Proyecto Gantt

3.5. CLAUSULA 4 – CONTEXTO DE LA ORGANIZACIÓN

Determinar Cuestiones Internas y Externas

Cuestiones Internas: Son los factores el control directo de la organización.

Cuestiones Externas: Factores sobre los cuales la organización no tiene control, pero estas pueden ser anticipadas y adaptadas.

3.5. CLAUSULA 4 – CONTEXTO DE LA ORGANIZACIÓN

Determinar Cuestiones Internas y Externas

Cuestiones Internas

- Gobierno Corporativo
- Estructura Organizativa
- Roles
- Responsabilidades/Autoridades
- Capacidades
- Cultura de la Organización
- Relaciones Contractuales
- Sistemas y flujos de información

Cuestiones Externas

- Social y cultural
- Política
- Legal
- Economía
- Tecnología
- Entorno Internacional
- Entorno Natural
- Regulaciones

3.5. CLAUSULA 4 – CONTEXTO DE LA ORGANIZACIÓN

Entender las necesidades y expectativas de las partes interesadas.

Partes Interesadas Internas	Partes Interesadas Externas
• Empleados • Sindicatos • Partners • Contratados	• Legal • Clientes • Proveedoras • Competencia • Contratistas • Aseguradoras • Entidades Financieras

3.5. CLAUSULA 4 – ALCANCE DEL SGSI

La organización debe determinar las fronteras y la aplicabilidad del SGSI para establecer su alcance.

Cuando se determina el alcance la organización debe considerar las cuestiones internas y externas, los requerimientos de las partes interesadas y, las interfaces y dependencias entre las actividades llevadas a cabo por la organización.

El alcance debe estar disponible como información documentada.

3.5. CLAUSULA 4 – ALCANCE DEL SGSI

Ejemplo de Alcance

El Alcance del SGSI de XXXX aplica a la provisión de información de clientes a través de su pagina web administrada desde su edificio principal en Asunción – Paraguay. Cubre la gestión de la información y las actividades de la organización que soportan este servicio; de acuerdo a la declaración de aplicabilidad “SoA V. 1.0 de fecha 15/08/2019”

3.6. CLAUSULA 5 – LIDERAZGO

Liderazgo y compromiso

La alta gerencia debe demostrar liderazgo y compromiso con respecto al SGSI:

- Asegurando que la política y los objetivos de seguridad de la información han sido establecidos y son compatibles con la dirección estratégica de la organización;

- Asegurando que los requerimientos de integración del SGSI en los procesos del negocio;

- Asegurando que los recursos necesarios para el SGSI están disponibles;

3.6. CLAUSULA 5 – LIDERAZGO

- Comunicando la importancia de una efectiva gestión de seguridad de la información y en conformidad a los requerimientos del SGSI;

- Asegurando que el SGSI alcance los resultados esperados;

- Dirigiendo y apoyando a las personas a contribuir con la eficiencia del SGSI;

- Promoviendo la mejora continua;

- Apoyando a otros roles de gestión relevantes a demostrar su liderazgo en la aplicación en sus áreas de responsabilidad.

3.6. CLAUSULA 5 – LIDERAZGO

Política

La alta dirección debe establecer una política de seguridad de la información que:

- Sea apropiada a los propósitos de la organización;
- Incluya los objetivos de seguridad de la información o provea el framework para el establecimiento de los objetivos;
- Incluir un compromiso para satisfacer los requerimientos aplicables relativos a la seguridad de la información

3.6. CLAUSULA 5 – LIDERAZGO

Ejemplo de política de seguridad de la información:

Toda la información que viaja a través de las redes de computadoras de Texas Wesleyan que no han estado específicamente identificadas como de propiedad de otras partes serán tratadas como activos de Texas Wesleyan.

Esta es la política de Texas Wesleyan para prohibir acceso no autorizado, revelación, duplicación, modificación, destrucción, perdida, mal uso o robo de esta información. Adicionalmente esta es la política de Texas Wesleyan para proteger información de terceras partes que han sido confiadas a Texas Wesleyan en concordancia con su sensibilidad y los acuerdos aplicables

3.6. CLAUSULA 5 – LIDERAZGO

Roles Responsabilidades y Autoridades:

La alta dirección debe asegurar que las responsabilidades y autoridades para roles relevantes para la seguridad de la información son asignadas y comunicadas

La alta dirección debe asignar responsabilidades y autoridades para:

- Asegurar que el SGSI este conforme con los requerimientos del estándar internacional.

- Informe del rendimiento del SGSI a la alta dirección.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Análisis de riesgos

3.7. CLAUSULA 6 – PLANIFICACIÓN

Riesgo.

Posibilidad de ocurrencia de un evento adverso. Según ISO 27.000: El efecto de la incertidumbre el los objetivos.

Robo de objetos de valor.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Amenaza.

Según ISO: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización.

Ladrones altamente preparados.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Control o contramedida.

Según ISO: Medida que modifica un riesgo.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Control o contramedida.

Según ISO: Medida que modifica un riesgo.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Control o contramedida.

Según ISO: Medida que modifica un riesgo.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Control o contramedida.

Según ISO: Medida que modifica un riesgo.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Algunas metodologías de análisis de riesgos.

ISO 27005
RISK MANAGER

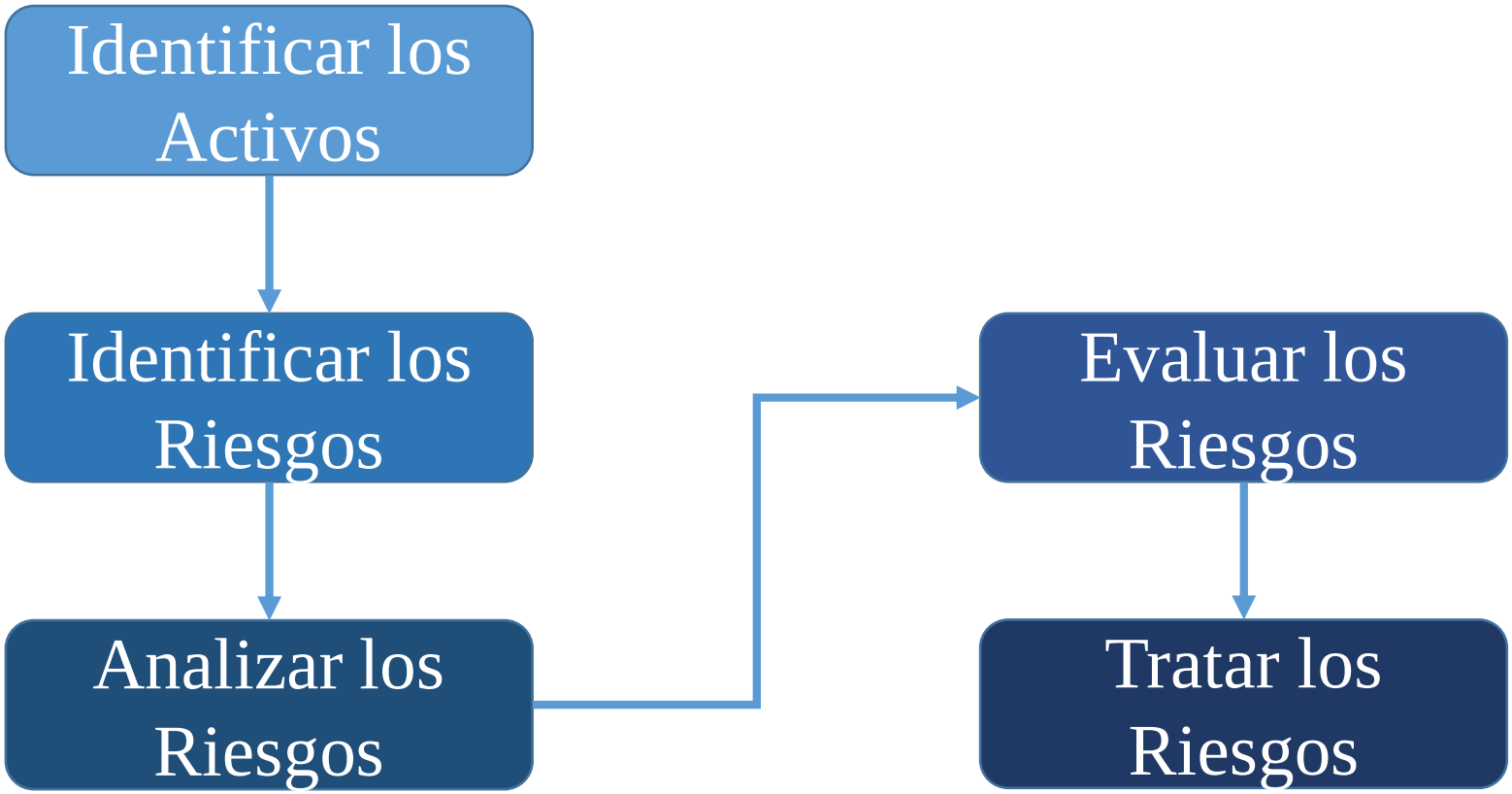
magerit
METHODOLOGY FOR INFORMATION SYSTEMS
RISK ANALYSIS AND MANAGEMENT

NIST SP 800-39
y SP 800-30r1

OCTAVE

3.7. CLAUSULA 6 – PLANIFICACIÓN

Definir metodología de gestión de riesgos



3.7. CLAUSULA 6 – PLANIFICACIÓN

Terminología.

Activo: Cualquier bien que tiene valor para la organización.
Activo de la Información: Información fundamental para el negocio.
Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización.
Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.
Apetito de Riesgo: Nivel de riesgos que la organización esta dispuesta a asumir.
Control: Medida que modifica el riesgo.
Criterio de Riesgo: Término de referencia con respecto a los cuales se evalúa la importancia del riesgo.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Terminología.

Evaluación de Riesgos: Proceso que compara los resultados del análisis de riesgos con el criterio de riesgos para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
Gestión de Riesgos: Proceso global de identificación de los riesgos, análisis de riesgos y evaluación del riesgo.
Impacto: Daño sobre el activo derivado de la materialización de la amenaza.
Identificación de activos: Bienes que están dentro del alcance del SGSI.
Identificación de riesgos: Proceso de buscar, identificar y describir los riesgos

3.7. CLAUSULA 6 – PLANIFICACIÓN

Terminología.

Nivel de Riesgo: Magnitud de un riesgo expresado en términos de la combinación de las consecuencias y las probabilidades.
Opciones de tratamiento: Aceptar, tratar, transferir y eliminar el riesgo.
Probabilidad: Posibilidad de que algo suceda.
Propietario del Riesgo: Persona o entidad con la responsabilidad para gestionar el riesgo.
Riesgo: Efecto de la incertidumbre sobre los objetivos.
Riesgo Residual: Riesgo que queda después del tratamiento de riesgos.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Terminología.

Tolerancia de Riesgo: Es el nivel de variación aceptable.
Tratamiento del Riesgo: Proceso para modificar el riesgo.
Vulnerabilidad: Debilidad de un activo o control que puede ser explotado.

3.7. CLAUSULA 6 – PLANIFICACIÓN

Valor del Activo - Impacto

1	2	3	4	5
• <= US$ 1.000	• Entre US$ 1.001 Hasta 5.000	• Entre US$ 5.001 y 10.000	• Entre US$ 10.001 y 100.000	• > US$ 100.000

3.7. CLAUSULA 6 – PLANIFICACIÓN

Valor de Frecuencia

1	2	3	4	5
• 1 vez o menos cada 5 años	• 1 vez cada 2 años	• 1 vez al año	• Cada 6 meses	• Cada 2 meses o menos

3.7. CLAUSULA 6 – PLANIFICACIÓN

Criterio de Riesgos

	MAPA DE NIVELES DE RIESGOS					
	PROBABILIDAD					
	#	1	2	3	4	5
IMPACTO	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	18
	5	5	10	15	20	25

BAJO	
MEDIO BAJO	
MEDIO	
MEDIO ALTO	
ALTO	

Apetito de Riesgo

Tolerancia de Riesgo

3.7. CLAUSULA 6 – PLANIFICACIÓN

Análisis de Riesgos

Activos	Impacto	Probabilidad			Nivel de Riesgo
	Valor del Activo	Vulnerabilidad	Amenaza	Frecuencia	
Servidor Host SR-X008	5	Falta de parches	Explotacion del CVE	5	25
Carpeta de archivos administrativos de la Gerencia General	4	Falta de controles de acceso	Acceso, modificación y/o eliminación de archivos no autorizados	3	12
Centro de Datos principal	5	Falta de mantenimiento estructural	Inundaciones	1	5

Evaluación de Riesgos

Nivel de Riesgo Vs. Apetito de Riesgos

Nivel de Riesgo	Apetito de Riesgo
25	12
12	12
5	12

Plan de tratamiento de Riesgos

Activos	Nivel de Riesgo	Control Aplicado	Valor	Riesgo Residual
Servidor Host SR-X008	25	A 12.6.1	14	11
Carpeta de archivos administrativos de la Gerencia General	12	A 9.2.2	6	6
Centro de Datos principal	5	--------	--------	--------

3.8. PLAN DE PROYECTO GANTT

									2019		2020			
Actividad	Control asociado	Fuente	Responsable	Horas Hom.	Costo	Duración	Fecha de inicio	Fecha Fin	Q3	Q4	Q1	Q2	Q3	Q4
Actualización de Software Servidor Host SR-X008	A 12.6.1	TR	DGTI	100	15.000	20 Días	15/9/2019	4/10/2019						
Aplicar control de acceso a carpeta de Archivos Administrativos de GG	A 9.2.2	TR	DSI	6	0	5	20/9/2019	25/9/2019						

CONSULTAS.

MUCHAS GRACIAS