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

3.9. Declaración de Aplicabilidad.

3.10. Objetivos de Seguridad de la información

3.11. Clausula 7: Soporte

3.12 Clausula 8: Operación

3.13 Clausula 9: Evaluación de rendimiento

3.14 Clausula 10: Mejora

3.9. Declaración de Aplicabilidad

La Declaración de Aplicabilidad o SoA, por sus siglas del inglés, es un documento que lista los controles establecidos en el Anexo A del estándar ISO 27.001 y en la que la organización establece cuales si y cuales no aplican a la misma.

Los controles aplicables provienen principalmente de tratamiento de los riesgos de la organización (ISO 27.001-A 6.1.3.d.) pero también puede incluir otras fuentes como:

- Requerimientos legales;
- Obligaciones contractuales;
- Requerimientos del negocio;
- Buenas prácticas u otros.

3.9. Declaración de Aplicabilidad

El SoA debe incluir además una justificación del porque no se implementará una medida.

Esta declaración puede ser modificada a lo largo el tiempo para adaptarse a nuevos requerimientos.

Este suele ser el documento utilizado por los auditores para el control de cumplimiento de los controles establecidos.

3.9. Declaración de Aplicabilidad

Declaración de Aplicabilidad

Vigente para:

Leyenda (para la selección de controles y razón por la que se seleccionaron)
LR: requerimientos legales, **CO**: obligaciones contractuales, **BR/BP**: requerimientos del negocio/mejores prácticas adoptadas , **RRA**: resultado de la valoración de riesgos, **TSE**: hasta cierto punto

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	seleccionados y razones de selección				Comentarios (Visión general de la implementación)
					LR	CO	BR/BP	RRA	
Cláusula	**Sección**	**Objetivo de Control / Control**							
5 Políticas de Seguridad	5,1	Dirección de la Alta Gerencia para la Seguridad de la Información							
	5.1.1	Políticas de Seguridad de la Información							
	5.1.2	Revisión de las Políticas de Seguridad de la Información							
6 Organización de la Seguridad de la Información	6,1	Organización Interna							
	6.1.1	Roles y Responsabilidad de Seguridad de la Información							
	6.1.2	Contacto con autoridades							
	6.1.3	Contacto con grupos de interés especial							
	6.1.4	Seguridad de la Información en la gestión de proyectos							
	6.1.5	Segregación de deberes							
	6,2	Dispositivos móviles y teletrabajo							
	6.2.1	Política de dispositivos móviles							
	6.2.2	Teletrabajo							
7 Seguridad en los Recursos Humanos	7,1	Previo al Empleo							
	7.1.1	Verificación de antecedentes							
	7.1.2	Términos y condiciones del empleo							
	7,2	Durante el Empleo							
	7.2.1	Responsabilidades de la Alta Gerencia							
	7.2.2	Conciencia, educación y entrenamiento de Seguridad de la Información							
	7.2.3	Proceso disciplinario							
	7,3	Terminación y Cambio de Empleo							
	7.3.1	Termino de responsabilidades o cambio de empleo							

3.10. Objetivos de Seguridad de la Información

ISO 27.001 - 6.2

La organización debe establecer los objetivos de seguridad de la información en funciones y niveles relevantes.

Los objetivos de seguridad de la información deben:

- Ser consistentes con la política de seguridad de la Información.
- Ser medibles.
- Tener en cuenta requerimientos de seguridad de la información aplicables y los resultados del análisis y tratamiento de riesgos.
- Ser comunicado.
- Actualizados cuando sea apropiado

3.10. Objetivos de Seguridad de la Información

ISO 27.001 - 6.2

Los Objetivos de Seguridad de la Información deben estar disponibles como información documentada.

En la planificación de cómo alcanzar los objetivos, se debe determinar:

- Qué se hará.
- Los recursos necesarios.
- Quien será el responsable.
- Cuando será completado.
- Quien evaluará los resultados.

3.10. Objetivos de Seguridad de la Información

ISO 27.001 - 6.2

Objetivos				Recoleccion de Datos		Evaluación de Resultados		
Objetivo	**Valor Minimo**	**Valor maximo**	**Recurso**	**Periodicidad**	**Responsable**	**Metodo**	**Periodicidad**	**Responsable**
Disponibilidad de la Conectividad	90%	100%	Herramienta de monitorización	Mensual	Operadores	Si menor >90% aplicar acción correctiva	Trimestral	Director de TI
Fortalecer Competencias	70%	100%	Curso de Capacitación	Según plan de capacitación	Oficial de SI	Control de asistencia. Resultados de examenes	Anual	Director de SI

3.11. CLAUSULA 7 – SOPORTE

7.1. Recursos

La organización debe determinar y proveer los recursos necesarios para establecer, implementar, mantener y mejorar contunuamente el SGSI

7.2. Competencias

La organización debe:

- Determinar la competencia necesaria de las personas cuyo trabajo afecta el rendimiento de la seguridad de la información.
- Asegurar que las personas son competentes en base a su educación entrenamiento o experiencia.

3.11. CLAUSULA 7 – SOPORTE

- Cuando sea necesario tomar acciones para adquirir la competencia necesaria, y evaluar la eficiencia de las medidas tomadas.
- Retener documentación apropiada como evidencia de la competencia.

Departamento	Seguridad de la Información
Responsabilidades	Elaborar y revisar normas y políticas de seguridad de la información
Experiencia	3 Años de experiencia en SI
Educación	Ing. Informatico, Lic. En Analisis de Sistemas Master en Seguridad Certificacion CISM o CISSP
Cualificaciones	Responsable - Trabajo en equipo - Autodidacta Conocimientos ISO 27.001

7.3. Awareness

Las personas que trabajan bajo el control de la organización deben estar capacitados en:

- Las políticas de seguridad de la información
- Su contribución a la eficiencia del SGSI, incluyendo los beneficios de mejorar el rendimiento de la Seguridad de la Información.
- Las implicaciones de no cumplir con los requerimientos del SGSI.

3.11. CLAUSULA 7 – SOPORTE

7.4. Comunicación.

La Organización debe determinar la necesidad de comunicaciones internas o externar relevantes al SGSI incluyendo:

- Que comunicar,
- Cuando comunicar,
- Con quien comunicar,
- Quien debe comunicar
- El proceso por el cual se hará la comunicación.

7.5. Información Documentada.

El SGSI de la Organización debe incluir:

- La información documentada requerida por el estándar.
- Y la información documentada determinada por la organización como necesaria para la eficiencia del SGSI

Estos deben tener en cuenta el tamaño, la complejidad de la organización y la competencia de las personas.

3.12. CLAUSULA 8 – OPERACIÓN

8.1. Planificación y control operacional.

La organización planificar, implementar y controlar los procesos necesarios para alcanzar los requerimientos de seguridad de la información.

La organización debe mantener la documentación necesaria para tener la confianza de que el proceso se esta llevando a cabo según lo planeado.

La organización debe controlar los cambios planeados y revisar las consecuencias de los cambios no deseados.

3.12. CLAUSULA 8 – OPERACIÓN

8.2. y 8.3 Análisis y tratamiento de riesgos

La organización debe realizar análisis de riesgos a intervalos planificados o cuando cambios significativos así lo requieran.

La organización debe implementar el plan de tratamiento de riesgos.

La organización debe mantener información documentada del analsis y el tratamiento

3.13. CLAUSULA 9 – EVALUACIÓN DE RENDIMIENTO

9.1. Monitoreo, medición, análisis y evaluación.

La organización debe evaluar el rendimiento y la eficiencia del SGSI y debe determinar:

- Que necesita ser monitoreado.
- El método de monitoreo, medición, análisis y evaluación.
- Cuando se monitorea y se miden los resultados.
- Quien monitorea y mide.
- Cuando se evalúan los resultados.
- Quien analizara los resultados.

La organización debe retener información documentada.

9.2. Auditoria Interna.

La organización debe conducir auditorias en intervalos planificados para proveer información de si el SGSI:

- Cumplen con que los requerimientos propios de la organización y del estándar.
- Esta eficientemente implementado y mantenido.

La organización debe planear, establecer, implementar y mantener un programa de auditoria.

9.3. Revisión por la dirección.

La alta dirección debe verificar el SGSI en intervalos planificados para asegurar la continua idoneidad, adecuación y eficiencia.

La dirección debe incluir consideraciones de:

- Es estatus de acciones de revisiones anteriores.
- Cambios en cuestiones internas o externas relevantes.
- Los feedbacks del rendimiento de la seguridad de la información
- Feedback de partes interesadas
- Resultado del análisis de riesgos.
- Oportunidades de mejora continua

3.14. CLAUSULA 10 – MEJORA

10.1. No conformidades y acciones correctivas.

Cuando ocurre una no conformidad, la organización debe:

- Reaccionar a la no conformidad.
- Evaluar la necesidad de acciones para eliminar la causa.
- Implementar las acciones necesarias.
- Revisar la efectividad de las acciones correctivas
- Hacer cambios al SGSI.

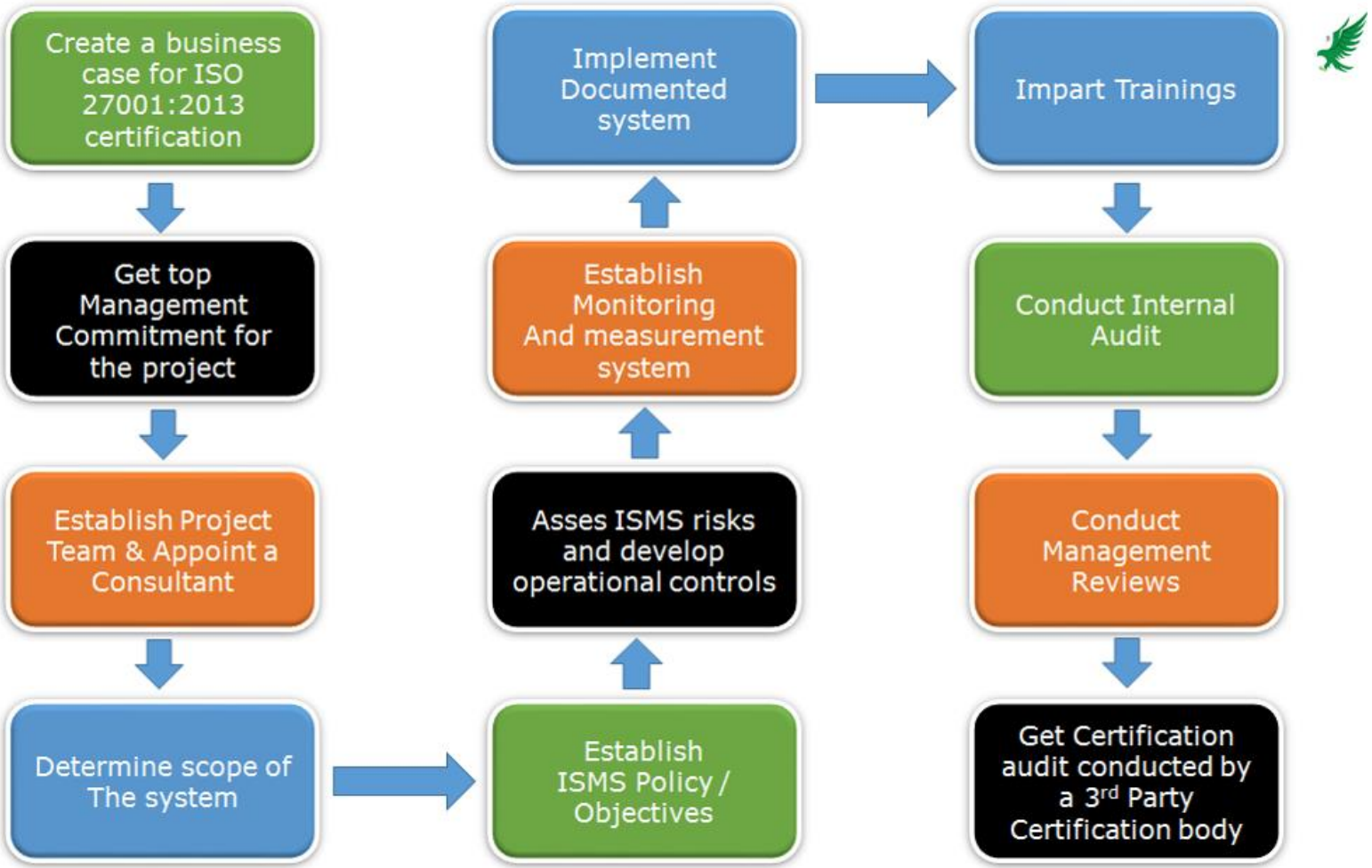
La organización debe mantener información documentada de las no conformidades y de las acciones correctivas

3.14. CLAUSULA 10 – MEJORA

10.2. Mejora Continua.

La organización debe continuamente mejorar la idoneidad, adecuación y eficacia del SGSI

EN RESUMEN


Create a business case for ISO 27001:2013 certification
Get top Management Commitment for the project
Establish Project Team & Appoint a Consultant
Determine scope of The system
Establish ISMS Policy / Objectives
Asses ISMS risks and develop operational controls
Establish Monitoring And measurement system
Implement Documented system
Impart Trainings
Conduct Internal Audit
Conduct Management Reviews
Get Certification audit conducted by a 3rd Party Certification body

5. Concienciación de usuarios en Seguridad de la Información

5.1. Planificación.

5.2. Concienciación.

5.3. Capacitación.

5.4. Evaluaciones y métricas.

5. Concienciación de usuarios en Seguridad de la Información

ISO 27.002 7.2.2.

Todos los empleados de la organización y, cuando sea relevante, los contratados deben recibir capacitación, educación y entrenamiento apropiados y actualizaciones regulares en políticas y procedimientos de seguridad de la información que son relevantes para sus labores.

5.1. PLANIFICACIÓN

Se debe elaborar un plan de capacitación y concienciación de seguridad de la información en el cual se establezcan:

- Formato en el cual se desarrollará.
- La periodicidad tanto del desarrollo como de la revisión del plan.
- Los temas a ser desarrollados.
- Los recursos necesarios.
- Como y cuando medir los resultados.
- El publico objetivo

CONSULTAS.

MUCHAS GRACIAS