Centro de Especializaciones Noeder

Diploma de Especialización Internacional

IMPLEMENTADOR Y AUDITOR SEGURIDAD DE LA INFORMACIÓN - ISO 27001 Y CONTINUIDAD DEL NEGOCIO - ISO 22301

MÓDULO II

IMPLEMENTACIÓN DE LA NORMA ISO 27001

CLASE 01

Mg. Ing. Julio Pereyra Rosales

1. Gestión del contexto organizacional

Plan de implementación del SGSI

ANÁLISIS DE BRECHA

- Requerimientos del negocio respecto a la SI.
- Requisitos de seguridad implementados y por implementar de acuerdo a la NTP ISO/IEC 27001:2022
- Plan Inicial de Implementación del SGSI, identificando los recursos para establecer el modelo de gestión de SI.

Planear

- Identificar el FODA del MTPE
- Identificar las interesados (necesidades y expectativas de SI).
- Definir el alcance del SGSI (límites a nivel estructura orgánica, física y de procesos)
- Establecer la Política y los objetivos de SI.
- Definir roles y responsabilidades para la gestión de la SI.
- Elaborar el Plan para cumplir los objetivos de SI, identificando los recursos.
- Definir Metodología de Riesgos de SI.
- Identificar, analizar y evaluar riesgos y oportunidades de SI
- Elaborar el Plan de Tratamiento de los riesgos y oportunidades de SI
- Elaborar Documento de Aplicabilidad.
- Elaborar el Plan de Capacitación y Concienciación en SI.
- Elaborar el Plan de Comunicación.
- Elaborar el plan para monitorear, medir y evaluar de la efectividad del SGSI.

Hacer

- Ejecutar el Plan para cumplir los objetivos de SI.
- Ejecutar el Plan de Tratamiento de los riesgos y oportunidades de SI
- Ejecutar el Plan de Capacitación y Concienciación en SI.
- Ejecutar el Plan de Comunicación.
- Implementar los controles del Anexo A de la Norma de acuerdo al Documento de aplicabilidad y al Plan de Tratamiento de riesgos: controles organizativos, de procesos y tecnológicos.
- Actualizar el Documento de aplicabilidad con los controles implementados
- Realizar evaluaciones de riesgos de SI cuando ocurran cambios significativos y actualizar el Plan de Tratamiento de riesgos.

Verificar

- Seguimiento al Plan de tratamiento de riesgos
- Ejecutar el Plan para monitorear, medir, analizar y evaluar la efectividad del SGSI.
- Realizar la auditoria interna del SGSI.
- Realizar la revisión del SGSI por el CDG de acuerdo a lo establecido en la clausula 9.3.

Actuar (Mejorar)

- Revisar y atender las No Conformidades e implementar las acciones correctivas detectadas en las auditorias, resultados de la revisión por la Dirección y/o tratamiento de los incidentes.
- Implementar y documentar la mejora continua.

CULTURA DE SEGURIDAD DE LA INFORMACIÓN
SEGURIDAD DE LA INFORMACIÓN GESTIONADA

SI: Seguridad de la Información

Plan de implementación del SGSI

Nº	Actividades	Responsable	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6				Mes 7				Mes 8				Mes 9			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	ETAPA 0 - INICIAL																																					
1	ELABORAR Y APROBAR PLAN DEL PROYECTO DETALLADO	OGETIC/CGTD																																				
2	ANALISIS DE BRECHA CON RESPECTO A LOS REQUISITOS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	OGETIC																																				
	ETAPA 1 - PLANIFICACIÓN																																					
3	ELABORAR EL MANUAL DEL SGSI	OSCD/OGPP																																				
4	REVISAR Y ACTUALIZAR DOCUMENTOS DE CONTEXTO	OGETIC/CGTD																																				
4.1	MATRIZ FODA	OGETIC																																				
4.2	MATRIZ DE PARTES INTERESADA	OGETIC																																				
4.3	MATRIZ DE REQUISITOS LEGALES	OGETIC																																				
4.4	MATRIZ DE PARTES INTERESADA	OGETIC																																				
5	ACTUALIZAR DOCUMENTO DE ALCANCE DEL SGSI	OGETIC																																				
6	ACTUALIZAR LA POLÍTICA Y OBJETIVOS DEL SGSI	OGETIC/CGTD																																				
7	ALINEACIÓN DE LA POLÍTICA DE SEGURIDAD A LOS OBJETIVOS ESTRATEGICOS (PEI)	OGETIC																																				
8	ELABORAR EL PLAN PARA LOGRAR LOS OBJETIVOS DEL SGSI	OGETIC																																				
9	ASIGNAR LOS ROLES Y RESPONSABILIDADES PARA LA GESTIÓN DEL SGSI	OGETIC/CGTD																																				
10	ACTUALIZAR UN PROGRAMA DE CAPACITACIÓN Y CONCIENCIACIÓN (INCLUIDO EN LA ESTRATEGIA DIGITAL)	OGETIC/OGRH/CGTD																																				
10.1	ELABORAR MATERIAL PARA LAS COMUNICACIONES DE TODO EL AÑO	OGETIC																																				
11	ELABORAR / ACTUALIZAR OTROS DOCUMENTOS																																					
12	REALIZAR UN INVENTARIO DE ACTIVOS	ORGANOS/UNIDADES ORGANICAS																																				
13	ANALIZAR Y EVALUAR LOS RIESGOS Y ELABORAR EL PLAN DE TRATAMIENTO	ORGANOS/UNIDADES ORGANICAS																																				
14	ELABORAR UN DOCUMENTO DE APLICABILIDAD (SI APLICA Y SI ESTA IMPLEMENTADO)	OSCD/OGETIC																																				
15	ELABORAR UN PLAN PARA MEDIR Y EVALUAR EL SGSI	OGETIC																																				
15.1	REVISAR Y ACTUALIZAR INDICADORES DEL SGSI	OGETIC																																				
	ETAPA 2 - IMPLEMENTACIÓN (HACER)																																					
12	EJECUTAR EL PLAN DE TRATAMIENTO DE RIESGOS	ORGANOS/UNIDADES ORGANICAS																																				
13	EJECUTAR EL PROGRAMA DE CAPACITACIÓN Y CONCIENCIACIÓN	OGETIC/OGRH/CGTD																																				
14	IMPLEMENTAR/VERIFICAR LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DEL ANEXO A	ORGANOS/UNIDADES ORGANICAS																																				
	ETAPA 3 - MONITOREO Y REVISIÓN																																					
15	MEDIR LOS INDICADORES DEL SGSI	ORGANOS/UNIDADES ORGANICAS																																				
16	REALIZAR EL SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS	OGETIC/CGTD																																				
17	EJECUTAR EL PLAN PARA MEDIR Y EVALUAR EL SGSI	OGETIC/CGTD																																				
18	EJECUTAR EL PLAN DE REVISIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	OGETIC/CGTD																																				
19	REALIZAR LA AUDITORIA INTERNA DEL SGSI	SERVICIO POR TERCEROS																																				
20	DESARROLLAR LA REVISIÓN POR LA DIRECCIÓN	OGETIC/CGTD																																				
	ETAPA 4 - MANTENER Y MEJORAR																																					
21	IMPLEMENTAR LAS ACCIONES CORRECTIVAS (Según NC y OBS)	ORGANOS/UNIDADES ORGANICAS																																				
22	REALIZAR EL INFORME DE CIERRE DE LA IMPLEMENTACIÓN DEL SGSI	OGETIC/CGTD																																				
23	AUDITORIA DE CERTIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) FASE I Y II (SUJETO A DECISIÓN DEL CGTD Y DISPONIBILIDAD PRESUPUESTAL)	SERVICIO POR TERCEROS																																				

Información documentada mínima en el SGSI

Alcance del Sistema de Gestión

Solicitado en la cláusula 4.3, requiere que la organización defina todos los aspectos, internos y externos, que tengan la capacidad de impedir el logro de los objetivos. Estos aspectos son **condiciones, circunstancias, leyes, acuerdos, requisitos de un organismo regulador, expectativas o solitudes de partes interesadas**.

Política de Seguridad de la Información

La Política de Seguridad de la Información es requerida en la cláusula 5.2 y la responsabilidad compete a la Alta Dirección. Es el documento que expresa la voluntad y el compromiso de la organización por preservar la Seguridad de la Información y cumplir con las obligaciones regulatorias. En ese sentido, debe **expresar también unos objetivos generales, en concordancia con los compromisos asumidos**.

Proceso de Gestión de Riesgos de SI

Este es un requisito establecido en la cláusula 6.1.2. El objetivo es documentar todo el trabajo de planificación, desarrollo de metodologías y herramientas de evaluación, así como el resultado de la Gestión de Riesgos de Seguridad de la Información.

Declaración de aplicabilidad

La declaración de aplicabilidad de la que habla la cláusula 6.1.3 d. es, dentro de la documentación en ISO 27001:2022, un documento obligatorio si se espera certificar el sistema. La aplicabilidad está directamente relacionada con los objetivos y los controles del Anexo A que la organización necesite para alcanzar esos objetivos.

Plan de gestión de riesgos

Las cláusulas 6.1.3 e, 6.2 y 8.3 solicitan la planificación de la gestión de riesgos, y la respectiva documentación de esa actividad.

Objetivos de Seguridad de la Información

Los objetivos que aquí deben documentarse, de conformidad con lo solicitado en la cláusula 6.2, son los específicos de la gestión que, a su vez, estarán vinculados a los controles respectivos del anexo A.

Informes de evaluación y de gestión de riesgos

Las conclusiones y resultados que arrojan las tareas de evaluación y gestión de riesgos deben documentarse según lo solicitado en las cláusulas 8.2 y 8.3.

Inventario de activos

No todos los requisitos de documentación en ISO 27001:2022 parten de una solicitud en una cláusula. **Este, y los subsiguientes en esta guía, son ejemplo de ello**. El inventario de activos, en particular, es requisito para la implementación del Control A.5.9. Por supuesto, en este y en los casos que siguen, se considerarán documentos obligatorios solo en el evento de que el control sea obligatorio para la organización.

Uso aceptable de los activos

Este documento se solicita en el Control A.5.10. También se podría denominar Política de Seguridad Informática, y está vinculado con los activos que se han inventariado en el documento anterior.

https://www.escuelaeuropeaexcelencia.com/2023/01/documentacion-en-iso-270012022-lista-actualizada-de-los-documentos-obligatorios-en-la-ultima-revision/

Información documentada mínima en el SGSI

Procedimiento de respuesta a incidentes

Control que lo solicita: A.5.26. El objetivo es documentar las acciones que prevé la organización ante la ocurrencia de un incidente o una infracción.

Requisitos reglamentarios, contractuales y legales

Un inventario de las leyes, normas, acuerdos o regulaciones a los que está obligada la organización, en materia de Seguridad de la Información o Protección de Datos, es lo que solicita documentar el control A.531.

Procedimientos Operativos de Seguridad para la Gestión de TI

El control A.5.37 es muy específico. Solicita documentar todos los procedimientos prácticos que se ponen en marcha para garantizar la Seguridad de la Gestión de TI.

Definición de roles y responsabilidades de seguridad de la información

Aunque la información que debe documentarse según los controles A.6.2 y A.6.6 **puede incluirse en la política o en la declaración de objetivos**, es bueno también crear un documento exclusivo, para satisfacer el requerimiento.

Definición de configuraciones de seguridad

Se refiere a procedimientos y configuraciones de seguridad en el área de TI, y se solicita en el Control A.8.9.

Principios de ingeniería de sistemas seguros

Finalmente, el control A.8.27 requiere una política de desarrollo seguro de sistemas de información.

https://www.escuelaeuropeaexcelencia.com/2023/01/documentacion-en-iso-270012022-lista-actualizada-de-los-documentos-obligatorios-en-la-ultima-revision/

Registros mínimos en el SGSI

- **Registros sobre capacitaciones, experiencia, calificaciones y habilidades**, que usualmente son certificados de programas de formación, CVs o evaluaciones de resultados de las capacitaciones impartidas.
- **Reportes, seguimiento y mediciones** de la efectividad de los controles o de la eficiencia de alguna acción correctiva.
- **Resultados de la auditoría interna** o del programa de auditorías.
- **Resultados de las inspecciones o revisiones** de la Alta Dirección.
- **Resultados de la implementación de acciones correctivas** u otro tipo de medidas tomadas para prevenir riesgos.
- **Actividades de usuarios** y otros registros automáticos en los diferentes sistemas de información.

https://www.escuelaeuropeaexcelencia.com/2023/01/documentacion-en-iso-270012022-lista-actualizada-de-los-documentos-obligatorios-en-la-ultima-revision/

4. Contexto de la organización

4.1 Comprensión de la organización y su contexto

Análisis DOFA SITECH	Oportunidades	Amenazas
	1. Crecimiento del mercado en torno a la tecnología. 2. Estilos de vida tecnológicos. 3. Oportunidades en el sector educativo.	1. Patrones y cambios en el mercado. 2. Tasa de cambio de moneda extranjera fluctuante. 3. Competencia desleal.
Fortalezas	**Estrategias FO**	**Estrategias FA**
1. Habilidad para responder a la tecnología Cambiante. 2. Agresividad para enfrentar la competencia. 3. Nivel tecnológico de la empresa. 4. Estabilidad laboral y nivel de pertenencia de la fuerza de trabajo. 5. Lealtad y satisfacción del cliente. 6. Facilidad de créditos y acuerdos de pago con proveedores.	1. Implementar estrategias de negocio para nichos de mercado en crecimiento. 2. Aprovechar la lealtad de los clientes para generar estabilidad y dedicar esfuerzo en incursionar en el sector educativo. 3. Generar un acercamiento a los prospectos de clientes mediante el uso de tecnología aprovechando el uso masivo de las redes sociales.	1. Generar planes de acción mediante el uso delos créditos y acuerdos de pagos a proveedores para superar la fluctuación de la moneda extranjera. 2. Fortalecer y socializar la ética en los empleados y clientes evitando los impactos de la competencia desleal. 3. Generar estrategias tecnológicas de cambio para responder oportunamente a las variaciones y requerimientos del mercado.
Debilidades	**Estrategias DO**	**Estrategias DA**
1. Falta de sistemas de control. 2. Alta Rotación de personal. 3. Falta de inversión de I&D de nuevos servicios. 4. Estabilidad de los costos.	1. Realizar pruebas piloto de tecnología con el personal internos, para motivarlos a conocer la línea de negocio, aprovechando el auge de la tecnología en los estilos de vida actuales. 2. Implementar las soluciones del sector educativo internamente para incentivar la I&D de nuevos servicios y capacitar al personal en general en el uso de las mismas. 3. Generar estrategias generales para estabilizar los costos de operación al contemplar el crecimiento de la organización junto con el del mercado.	1. Generar sistemas de control y verificación de procesos 2. Definir procesos documentados que le permita al personal generar estándares en busca de costos mínimos de reprocesos. 3. Implementar planes de incentivos para evitar la alta rotación de personal y la migración a la competencia.

FORTALEZAS	DEBILIDADES
Políticas de Seguridad Efectivas	Falta de Recursos
Tecnología Avanzada	Sistemas Desactualizados
Personal Capacitado	Capacitación Inadecuada
Cultura de Seguridad	Políticas Inconsistentes
OPORTUNIDADES	**AMENAZAS**
Avances Tecnológicos	Amenazas Avanzadas y Persistentes (APT)
Conciencia Creciente	Ransomware
Colaboración y Alianzas	Fugas de Información
Regulaciones y Normativas	Evolución de las Amenazas

4. Contexto de la organización

4.1 Comprensión de la organización y su contexto

N.º	FORTALEZAS
1	Se cuenta con servicios que brindan atención a jóvenes, ciudadanos y público en general brindándoles información sobre alternativas de generación de autoempleo, asimismo; el servicio también es accesible a extranjeros en general.
2	La entidad cuenta con procesos con certificación ISO 9001 e ISO 37001 y servicios certificados en Cartas de servicio.
3	EL MTPE ha registrado los Bancos de Datos Personales como lo establece la Ley de Protección de Datos Personales.
4	Se realizan programas de capacitación para el personal con el objeto de mejorar su desempeño profesional.
5	Colaboradores de la OGETIC altamente comprometidos y con conocimientos en diferentes especialidades del área de TI y experiencia en el sector público.
6	Visión integral y holística para gobernar y gestionar las TIC
7	Alta capacidad de adaptación a los cambios.
8	Capacidad de racionalización de recursos.

N.º	OPORTUNIDADES
1	La Pandemia incremento de uso de tecnologías de la información y comunicaciones, por motivos laborales, educativos, personales y de otra índole.
2	Incremento de canales digitales a través del uso de la Tecnologías de la Información y Comunicaciones a fin de brindar una mejor atención a los usuarios.
3	Apoyo y colaboración de la SEGTDI y el CNSD de la PCM para el desarrollo e implementación de nuevas soluciones tecnológicas, así como seguridad digital.
4	Utilización de marcos de referencia y buenas prácticas internacionales en materia de gobierno y gestión de las TIC
5	Conocimiento del ciudadano en el uso de las tecnologías de información (tecnología móvil, internet y otros) facilita la aplicación del Gobierno Digital.
6	Utilización de nuevas tecnologías para reducir costos.
7	Políticas públicas (como la Política Nacional de Transformación Digital) y las Plataformas de Interoperabilidad del Estado que fomentan el uso de herramientas tecnológicas y medios electrónicos, así como establecen la importancia de la seguridad digital.
8	A través del DS 029-2021-PCM Reglamento de la Ley de Gobierno Digital y la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD se indica que las entidades públicas deben implementar un Sistema de Gestión de Seguridad de la Información.

Nº	DEBILIDADES
1	Procedimiento de desarrollo de software poco maduros.
2	Poca toma de conciencia del personal del MTPE en Seguridad de la Información.
3	No se realiza aseguramiento de la calidad de las aplicaciones y/o sistemas de información que se desarrollan en el MTPE, incluyendo pruebas de seguridad.
4	No se cuenta con el personal y los recursos económicos suficiente en OTIC para afrontar la demanda de soluciones tecnológicas que provienen de los órganos internos, así como los requisitos y buenas prácticas de seguridad de la información.
5	Inexistencia de un entorno de contingencia ante incidentes que afecten la infraestructura física del datacenter.
6	No se cuenta con el presupuesto suficiente para atender los requerimientos de infraestructura, desarrollo de software y seguridad de la información del MTPE.
7	Falta de medición de los controles de seguridad implementados.
8	Insuficiente cultura institucional en gestión de riesgos.

Nº	AMENAZAS
1	Incremento de ataques informáticos como consecuencia de la masificación del uso de servicios en internet después de la Pandemia.
2	Los órganos del MTPE ven a la OTIC como una Oficina de Soporte cuando, en realidad, desempeña un rol estratégico.
3	Personal que deja de laborar en la OTIC se lleva el Know How (conocimiento) y dificulta la transferencia de conocimiento.
4	Emergencias debido a factores externo, tales como: desastres naturales.
5	Restricciones y recorte presupuestales afectan significativamente las actividades y proyectos ya programados.
6	Incumplimiento de regulaciones en materia de Tecnología de la Información y Comunicaciones.

4. Contexto de la organización

4.2 Comprensión de las necesidades y expectativas de partes interesadas

PARTES INTERESADAS		REQUISITOS DEL SGSI
INTERNAS	ACCIONISTAS	Maximizar la rentabilidad del negocio.
	GERENTES	Maximizar la rentabilidad del negocio. Garantizar la disponibilidad de los servicios entregados al cliente.
	COLABORADORES	Laborar en una empresa sólida y de prestigio. Proteger su información personal.
EXTERNAS	CLIENTE	Asegurar la confidencialidad, integridad y disponibilidad de su información
	PROVEEDORES	Alianzas estratégicas Proteger la continuidad de las operaciones Cumplimiento de los compromisos pactados
	GOBIERNO	Cumplir con las leyes Responsabilidad Social

4. Contexto de la organización

4.2 Comprensión de las necesidades y expectativas de partes interesadas

Nombre y cargo	Rol en el proyecto	Necesidades principales
Gerente General	Alta dirección	- Lograr la recertificación de la Empresa Soluciones Globales S.A.S en la Norma ISO 27001:2002 antes de finalizar el año 2024 - Obtener una guía práctica de transición de la versión 2013 a la versión 2022 de la Norma ISO 27001 para que el personal de su empresa pueda implementar fácilmente la nueva norma - Que la guía abarque todos los controles que exige la norma para los procesos más relevantes de la empresa - Cumplir los objetivos planteados en el direccionamiento estratégico de la empresa asociados con el Sistema de Gestión de la Seguridad de la Información
Directora de Sistemas Integrados	Sponsor	- Lograr la recertificación de la Empresa Soluciones Globales S.A.S en la Norma ISO 27001:2002 antes de finalizar el año 2024 - Obtener una guía práctica de transición de la versión 2013 a la versión 2022 de la Norma ISO 27001 para que el personal de su empresa pueda implementar fácilmente la nueva norma - Conocer los cambios de la Norma ISO27001:2022 con respecto a su versión anterior y el impacto que generaría en los procesos y herramientas actuales de la empresa - Identificar los elementos claves, incluyendo procesos y políticas para lograr la transición a la nueva versión de la Norma ISO27001:2022 - Definir los nuevos mecanismos tecnológicos requeridos para la implementación de la nueva versión de la Norma ISO27001:2022 - Que la guía práctica sea clara, precisa y de fácil interpretación para los técnicos encargados del proceso de implementación de la norma.

4. Contexto de la organización

4.3 Determinar el alcance del SGSI.

MAPFRE

ALCANCE

Luego de analizar los aspectos internos y externos, las necesidades y expectativas de las partes interesas y las interfaces y dependencias internas y externas de la empresa detallas en el documento SGSI.DC.01 Conocimiento de la organización y las partes interesadas, se determina el siguiente alcance para el SGSI:

"*Sistema de Gestión de Seguridad de la Información para el servicio de Facturación Electrónica, incluyendo PSE (Proveedor de Servicios Electrónicos) soportado por los procesos de Implantación, Soporte y Desarrollo de Software, de acuerdo con la declaración de aplicabilidad vigente*"

4. Contexto de la organización

4.3 Determinar el alcance del SGSI.

Certificado ES23/00001295

El sistema de gestión de

LEADER NETWORK MARKETING, S.L

Dirección Fiscal: C/ San Vicente Mártir,160, pta 2, 46007 Valencia

ha sido evaluado y certificado que cumple con los requisitos de

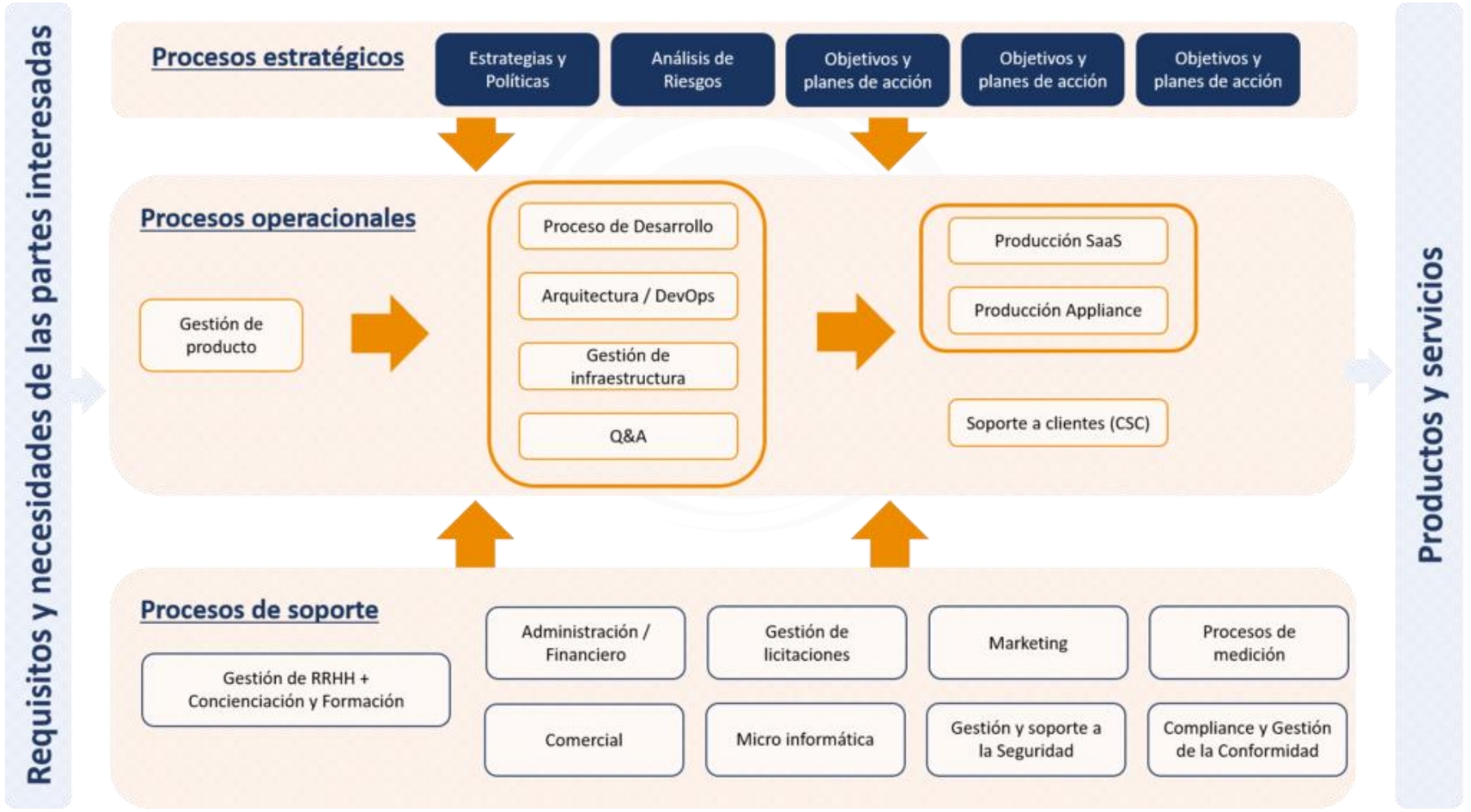
ISO/IEC 27001:2022

Para las siguientes actividades

Los sistemas de información que dan soporte a la implantación y asistencia técnica de soluciones de telecomunicaciones y seguridad; diseño,
programación y gestión de plataformas documentales de coordinación y control de accesos.
Según declaración de aplicabilidad Rev.2

4. Contexto de la organización

4.4 Sistema de gestión de seguridad de la información



2. Liderazgo y compromiso en el SGSI

5. Liderazgo

5.1 Liderazgo y compromiso

La Alta Dirección debe:

Establecer la política y objetivos del SGSI y que sean compatibles con la dirección estratégica.

Integración del SGSI en los procesos del negocio.

Apoyar a otros roles de la dirección para la eficacia del SGSI.

Asegurarse que los recursos necesarios del SGSI estén disponibles.

5. Liderazgo

5.1 Liderazgo y compromiso

La Alta Dirección debe:

- Comunicación de la importancia del SGSI.
- Asegurarse que el SGSI cumpla lo planificado.
- Comprometerse, dirigir y apoyar a las personas para contribuir a la eficacia de SGSI.
- Promover la mejora continua.

5. Liderazgo

5.2 Política

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La dirección de OBSS INGENIERÍA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para OBSS INGENIERÍA la protección de la información es fundamental y busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a OBSS INGENIERÍA según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de OBSS INGENIERÍA.
- Garantizar la continuidad del negocio frente a incidentes.

OBSS INGENIERÍA ha decidido junto con su equipo directivo apoyarse en en una consultoría para el diseño la definición y posterior implementación y operación de un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva. Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc.

Para abordar este punto es necesario remitirse a la "Guía de políticas específicas de seguridad y privacidad de la información" y mencionar aquellas que OBSS INGENIERÍA haya establecido como necesarias y primordiales.

5. Liderazgo

5.3 Roles, responsabilidades y autoridad

	PROCEDIMIENTO	Código: PRO.025	
	GESTIÓN DE ACTIVOS	Fecha: 08/03/2021	Versión: 1
		Página 1 de 5	

1. **OBJETIVO**

El presente documento establece los lineamientos a seguir para establecer, mantener y asegurar un nivel de protección adecuado para los activos de información de Core Business Corporation.

2. **ALCANCE**

Aplica a todo el personal de CORE BUSINESS CORPORATION.

3. **REFERENCIAS:**

- ISO 27001: Sistema de Gestión de Seguridad de la Información.
- ISO 27002: Técnicas de seguridad Código de prácticas para los controles de seguridad de la información

4. **DEFINICIONES**

- **Activo de información:** Es todo aquello que representa valor para la CBC desde software, hardware, información, servicios y colaboradores.
- **Integridad:** Resguardar la veracidad e integridad de la información y los métodos de procesamiento.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información.
- **Confidencialidad:** Asegurar que la información es accesible solo a aquellos que están autorizados.
- **Propietario del activo:** Cargo, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos se clasifiquen adecuadamente.
- **Usuario:** Responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Propietario del riesgo:** Es el responsable de la realización y ejecución de los controles.

5. **RESPONSABILIDADES**

5.1. **Oficial de Seguridad de la Información**

- Informar al Socio principal sobre el desempeño del SGSI.
- Dar seguimiento a los registros de SGSI.
- Organizar la realización de las auditorías internas y externas del SGSI.
- Promover la capacitación y concientización de los colaboradores acerca de la gestión de la seguridad de la información.
- Liderar los proyectos de mejora del SGSI.

5.2. **Propietario del Activo de Información**

- Controlar el uso y seguridad de los activos que le son asignados para la creación, procesamiento, transmisión y almacenamiento de información relacionadas al proceso o área que le compete.
- Entender y abordar los riesgos relacionados a la seguridad de la información de los activos del proceso o área de su responsabilidad.
- Asegurar que el activo de información se utiliza únicamente para los propósitos de la organización.

5.3. **Usuario del Activo de Información**

- Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos para el uso aceptable de los activos de información que le compete.
- Comunicar al propietario del activo de información las amenazas y vulnerabilidades que identifique durante el desarrollo de sus actividades.

	PROCEDIMIENTO	Código: PRO.023	
	GESTIÓN DE RIESGOS OPERACIONALES	Fecha: 5/10/21	Versión: 1
		Página 1 de 5	

1. **OBJETIVO**

Establecer el proceso para la identificación, análisis, evaluación y tratamiento de los riesgos relacionados con la seguridad de la información; asimismo, definir los controles que permitan mitigar o disminuir el riesgo identificados.

2. **ALCANCE**

Aplica a todos los procesos relacionados con el SIG.

Se considera los riesgos y oportunidades hacia los procesos que afecten a los activos de información.

3. **REFERENCIAS:**

- ISO 27001:2013. Requisitos de un Sistema de Seguridad de la Información.
- ISO 27002. Técnicas de seguridad Código de prácticas para los controles de seguridad de la información.
- ISO 3100. Gestión de Riesgos

4. **DEFINICIONES**

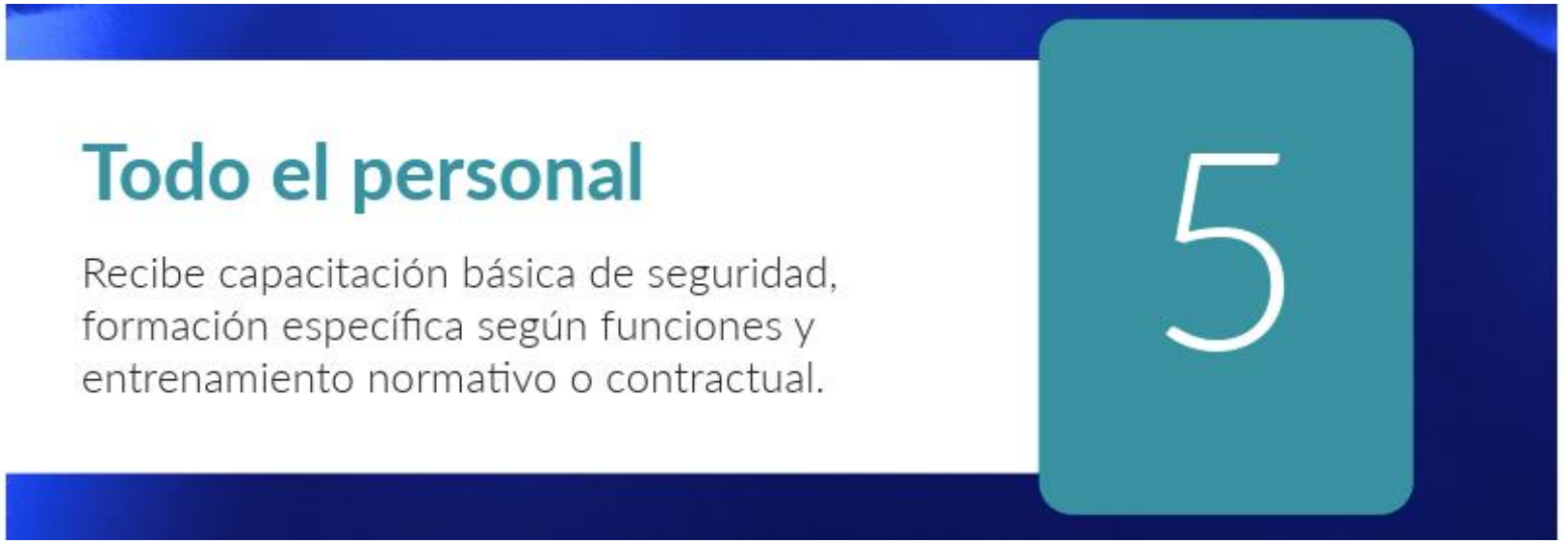
- **Activo de información:** Es todo aquello que representa valor para la Entidad desde software, hardware, información, servicios y personas.
- **Integridad:** Resguardar la veracidad e integridad de la información y los métodos de procesamiento.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información.
- **Confidencialidad:** Asegurar que la información es accesible solo a aquellos que están autorizados.
- **Riesgo aceptable:** es el riesgo que se ha conseguido reducir o mitigar de tal forma que pueda ser tolerado por la organización. Nivel de riesgo medio o bajo.
- **Riesgo residual:** riesgo restante después del tratamiento del riesgo.
- **Probabilidad:** Posibilidad de que el evento riesgoso ocurra de acuerdo con situaciones ya presentadas basadas en registros reales, datos, hechos o información conocida.
- **Amenaza:** Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática.
- **Impacto:** Consecuencia que pueda ocasionar en la empresa la materialización del riesgo.
- **Propietario:** Cargo, proceso o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos se clasifiquen adecuadamente.
- **Custodio:** Responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Vulnerabilidad:** Debilidad de los sistemas, ya sean equipos de cómputo, servidores, tanto hardware como software, sistema operativo, sistemas de información, aplicaciones, redes, etc. que puede ser utilizados o aprovechados por delincuentes informáticos, con el fin de ocasionar daño o extraer información confidencial y datos personales.
- **Consecuencia:** el resultado de un evento (amenaza) que afecta a los objetivos.
- **Propietario del riesgo:** Es el responsable de la realización y ejecución de los controles.

5. Liderazgo

5.3 Roles, responsabilidades y autoridad

5. Liderazgo

5.3 Roles, responsabilidades y autoridad



¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón