GLOBAL Quality CORP

WEBINAR ISO 27001

Gratuito

Estructura de la norma ISO 27001:2013 SGSI

ISO 27001:2013
Estructura

CLAUSULA	CONTENIDO **/ DESCRIPCIÓN**
1	Alcance
2	Referencias Normativas
3	Términos y definiciones
4	Contexto de la organización
5	Liderazgo
6	Planeación
7	Soportes e Información Documentada
8	Operación
9	Evaluación del desempeño
10	Mejora
Anexo **A Normativo**	14 Clausulas de Seguridad, en 35 Categorías y 114 Controles de Seguridad

CAMBIO ESTRUCTURAL

Apéndice 3
(Normativo)

Estructura de alto nivel, texto esencial idéntico, términos y definiciones esenciales comunes

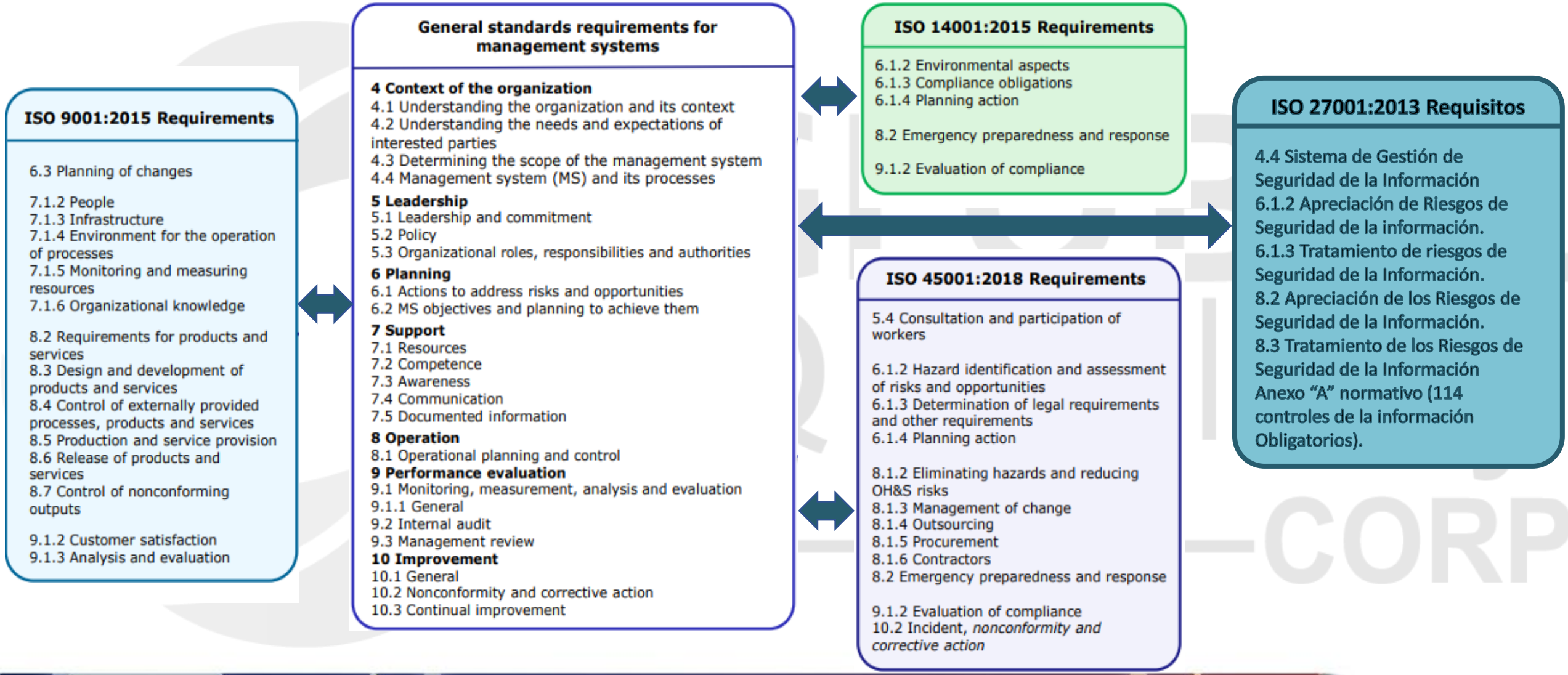
NOTA En las propuestas de texto idéntico, XXX designa un calificador de Norma de Sistemas Gestión específico para la disciplina (por ejemplo, energía, seguridad del tráfico por carretera, seguridad de TI, inocuidad de los alimentos, seguridad de los ciudadanos, medio ambiente, calidad) que es necesario incluir. El texto azul en cursiva se proporciona como recomendaciones a quienes redactan las normas.

INTRODUCCIÓN

NOTA Específico de la disciplina

La estructura de Alto Nivel.

1. Objetivo y campo de aplicación
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Apoyo
8. Operación
9. Evaluación del desempeño
10. Mejora

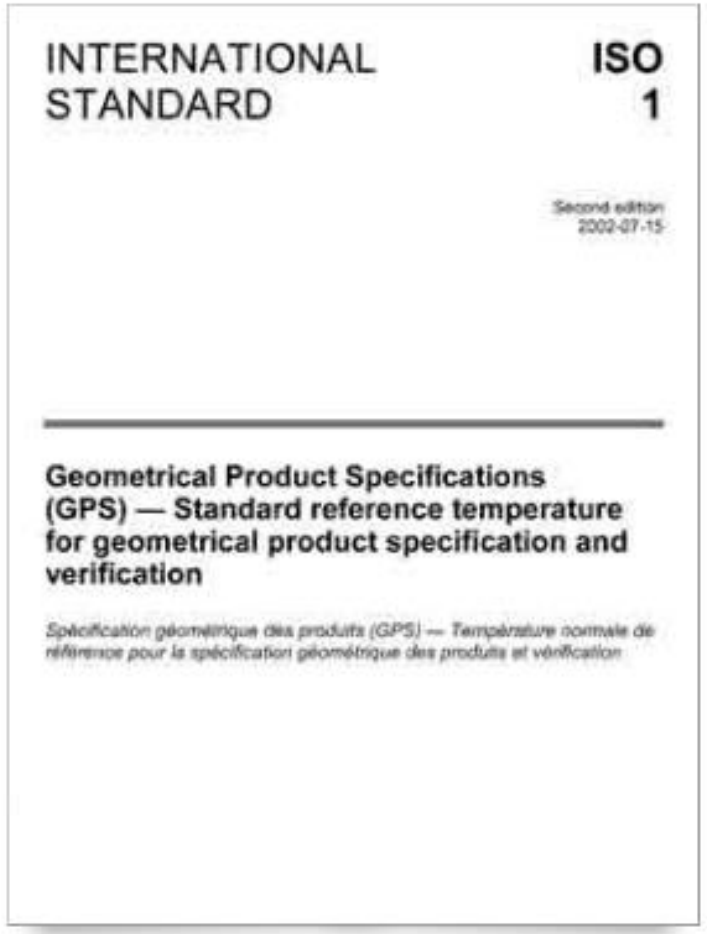

ISO 9001:2015 Requirements
6.3 Planning of changes
7.1.2 People
7.1.3 Infrastructure
7.1.4 Environment for the operation of processes
7.1.5 Monitoring and measuring resources
7.1.6 Organizational knowledge
8.2 Requirements for products and services
8.3 Design and development of products and services
8.4 Control of externally provided processes, products and services
8.5 Production and service provision
8.6 Release of products and services
8.7 Control of nonconforming outputs
9.1.2 Customer satisfaction
9.1.3 Analysis and evaluation
General standards requirements for management systems
4 Context of the organization
4.1 Understanding the organization and its context
4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the management system
4.4 Management system (MS) and its processes
5 Leadership
5.1 Leadership and commitment
5.2 Policy
5.3 Organizational roles, responsibilities and authorities
6 Planning
6.1 Actions to address risks and opportunities
6.2 MS objectives and planning to achieve them
7 Support
7.1 Resources
7.2 Competence
7.3 Awareness
7.4 Communication
7.5 Documented information
8 Operation
8.1 Operational planning and control
9 Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation
9.1.1 General
9.2 Internal audit
9.3 Management review
10 Improvement
10.1 General
10.2 Nonconformity and corrective action
10.3 Continual improvement
ISO 14001:2015 Requirements
6.1.2 Environmental aspects
6.1.3 Compliance obligations
6.1.4 Planning action
8.2 Emergency preparedness and response
9.1.2 Evaluation of compliance
ISO 45001:2018 Requirements
5.4 Consultation and participation of workers
6.1.2 Hazard identification and assessment of risks and opportunities
6.1.3 Determination of legal requirements and other requirements
6.1.4 Planning action
8.1.2 Eliminating hazards and reducing OH&S risks
8.1.3 Management of change
8.1.4 Outsourcing
8.1.5 Procurement
8.1.6 Contractors
8.2 Emergency preparedness and response
9.1.2 Evaluation of compliance
10.2 Incident, nonconformity and corrective action
ISO 27001:2013 Requisitos
4.4 Sistema de Gestión de Seguridad de la Información
6.1.2 Apreciación de Riesgos de Seguridad de la información.
6.1.3 Tratamiento de riesgos de Seguridad de la Información.
8.2 Apreciación de los Riesgos de Seguridad de la Información.
8.3 Tratamiento de los Riesgos de Seguridad de la Información
Anexo "A" normativo (114 controles de la información Obligatorios).

Estructura de la norma y Antecedentes

La historia de ISO
(Organización Internacional de Estandarización)

Nace en Londres, en 1946, con 65 delegados de 25 países, los cuales se reúnen para discutir el futuro de la Normalización Internacional.

En 1947, ISO se creó oficialmente con 67 comités técnicos (grupos de expertos que se centran en un tema específico).



INTERNATIONAL STANDARD

ISO 1

Second edition
2002-07-15

Geometrical Product Specifications (GPS) — Standard reference temperature for geometrical product specification and verification

Spécification géométrique des produits (GPS) — Température normale de référence pour la spécification géométrique des produits et vérification

En 1951 Nace el Primer estándar de ISO

En 1951 , se publica el primer estándar ISO (denominado:

Temperatura de referencia estándar para mediciones de longitud industrial.

FAMILIA ISO/IEC 27001

- **ISO 27000:2018** Información general y vocabulario
- **ISO 27001:2013** Requisitos (Certificable)
- **ISO 27002:2013** Código buenas practicas (Controles)
- **ISO 27003:2014** Guía de implementación
- **ISO 27004:2016** Mediciones
- **ISO 27005:2018** Administración de riesgos
- **ISO 27006:2015** Requerimientos para organismos de certificación
- **ISO 27007:2020** Lineamientos de auditoria
- **ISO 27007:2020** Directrices para los auditores sobre los controles de seguridad de la información

LÍNEA DE TIEMPO

Revisada en 1999 por la ISO

BS 7799

1995

BS 7799-1 / BS7799-2

1998

ISO 17799

2002

1.ra Edición

ISO/IEC 27001_2005

1995

2.da Edición

ISO/IEC 27001_2013

2013

GLOBAL Quality CORP

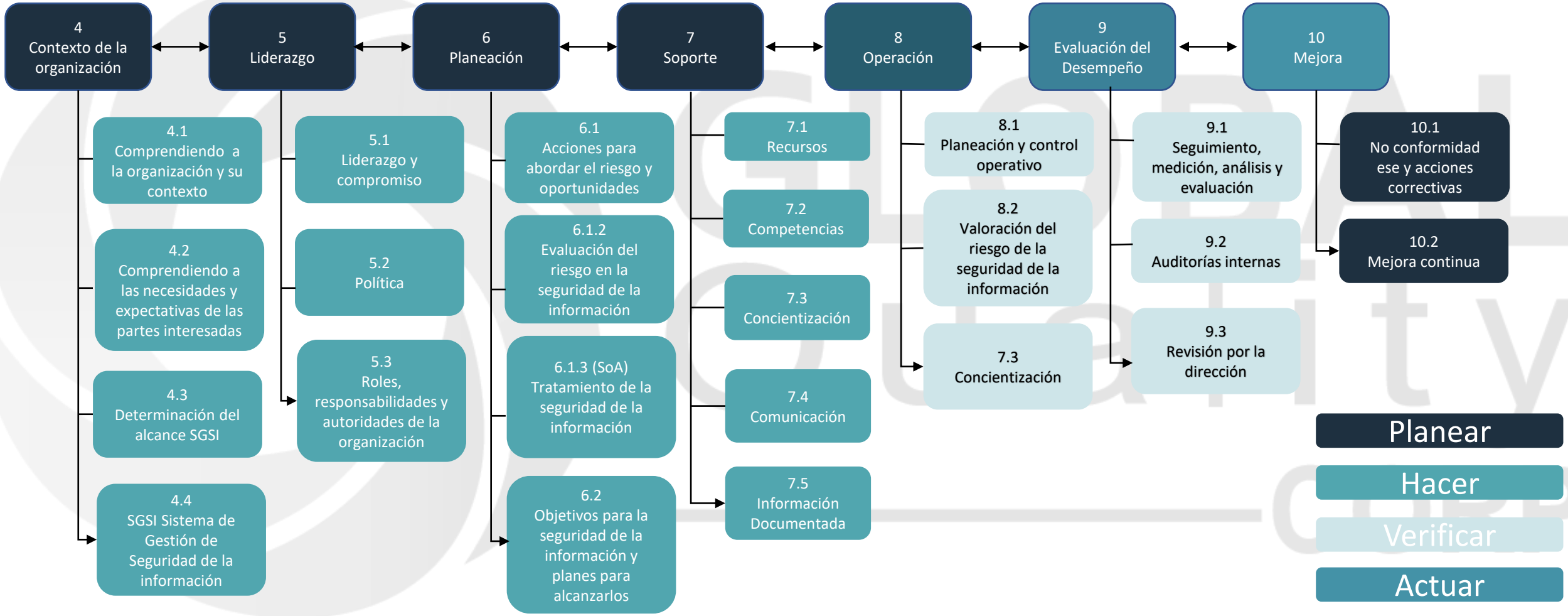
WEBINAR

ISO 27001

Estructura de la norma ISO 27001:2013 SGSI

Contenido de la Norma ISO/IEC 27001:2013

ESTRUCTURA ISO/IEC 27001



Lo primero que hay que tener en consideración en que el activo mas importante de la Organización es la Información y que la información puede ser:

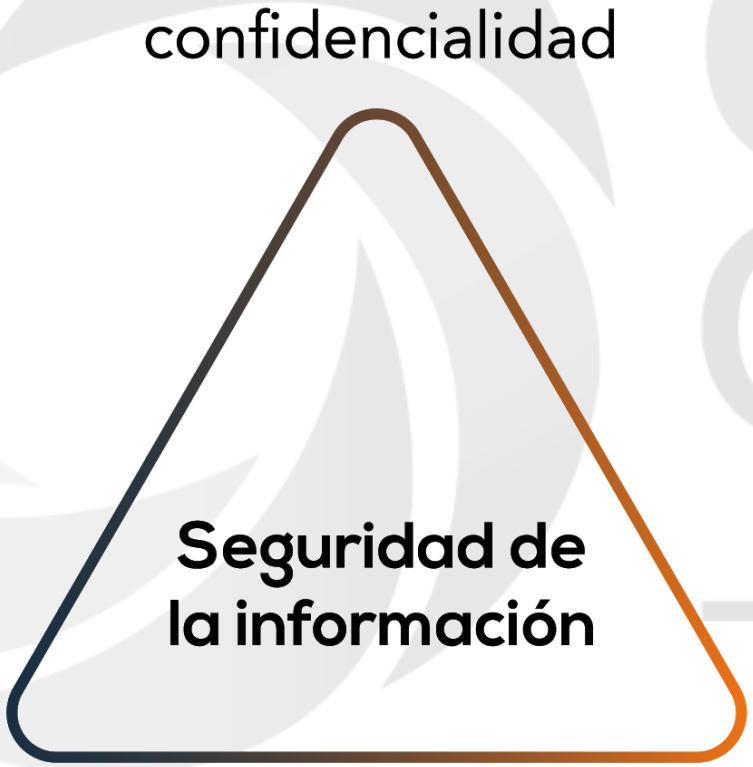
PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

confidencialidad

Integridad

Disponibilidad

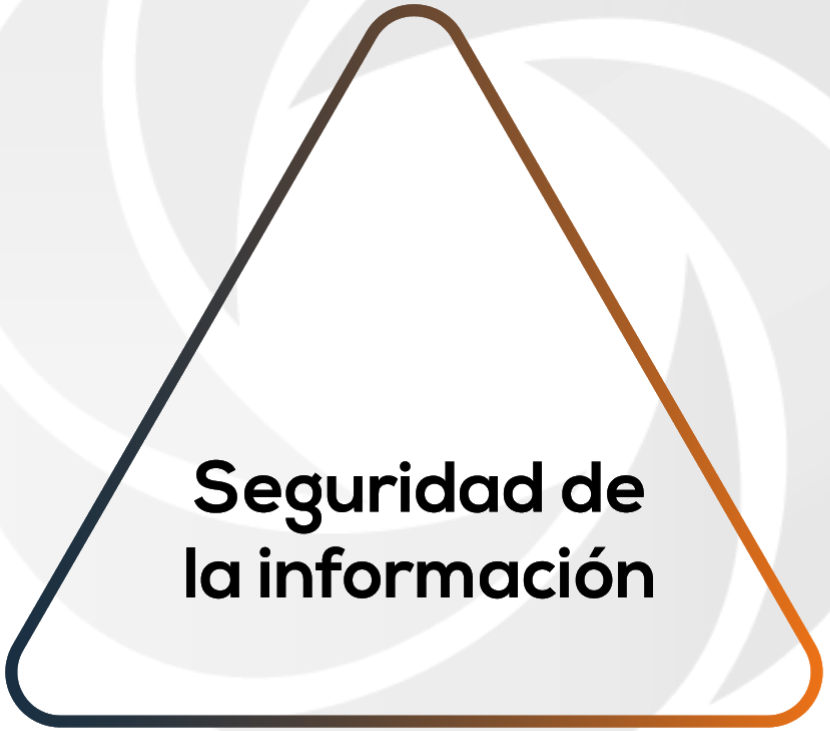
PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN



CONFIDENCIALIDAD:

Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados

PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN



DISPONIBILIDAD:

Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.

Disponibilidad

PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

INTEGRIDAD:

Propiedad de exactitud y completitud.

PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

NO REPUDIO:

Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron.

PERSONAL

Sensibilización y formación.

Obligaciones y responsabilidades del personal.

Control y supervisión.

Personal a considerar:
Directivos, Administradores, usuarios, personal interno y externo.

LEGISLACION

Análisis identificación y gestión del marco legal aplicable:

Propiedad intelectual.

Derechos del personal

Protección de datos personales.

S.G.S.I

TECNOLOGIA

Selección de instalaciones, hardware, software.

Controles de Cifrado.

Uso y desarrollo de aplicaciones.

ORGANIZACION

Políticas, Normas, Manales y Procesos.

Planes de Tratamientos,

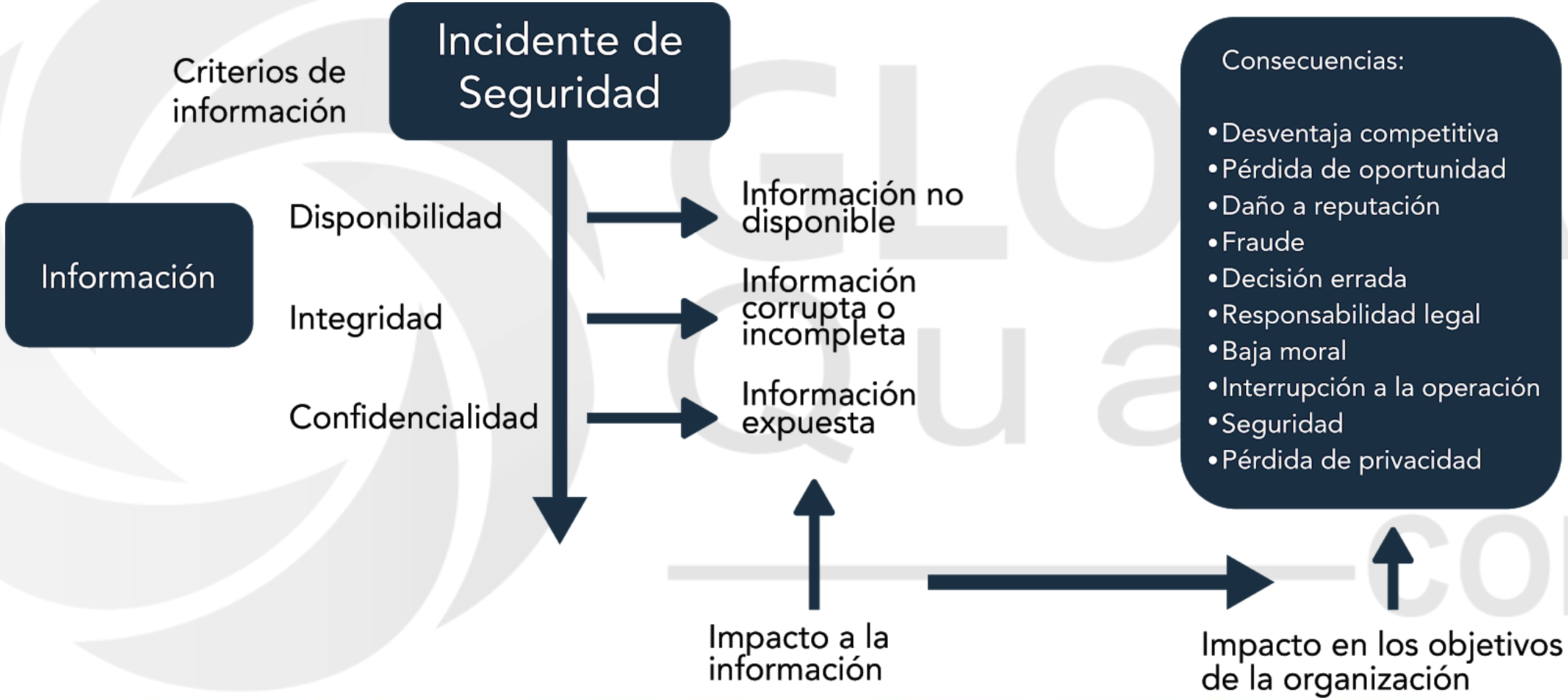
Planes de contingencia y respuesta a incidentes.

Gestión de las relaciones con terceros y proveedores.

SGSI / ISMS

- Sistema de gestión de seguridad de la información

“ Podemos definirlo como el conjunto de actividades, recursos y procesos entre las que se encuentran, políticas, procedimientos, estructura organizacional, infraestructura y activos de tecnologías, recurso humano y apego legislativo.”


Incidente de Seguridad
Criterios de información
Información
Disponibilidad
Integridad
Confidencialidad
Información no disponible
Información corrupta o incompleta
Información expuesta
Consecuencias:
• Desventaja competitiva
• Pérdida de oportunidad
• Daño a reputación
• Fraude
• Decisión errada
• Responsabilidad legal
• Baja moral
• Interrupción a la operación
• Seguridad
• Pérdida de privacidad
Impacto a la información
Impacto en los objetivos de la organización

GLOBAL Quality CORP

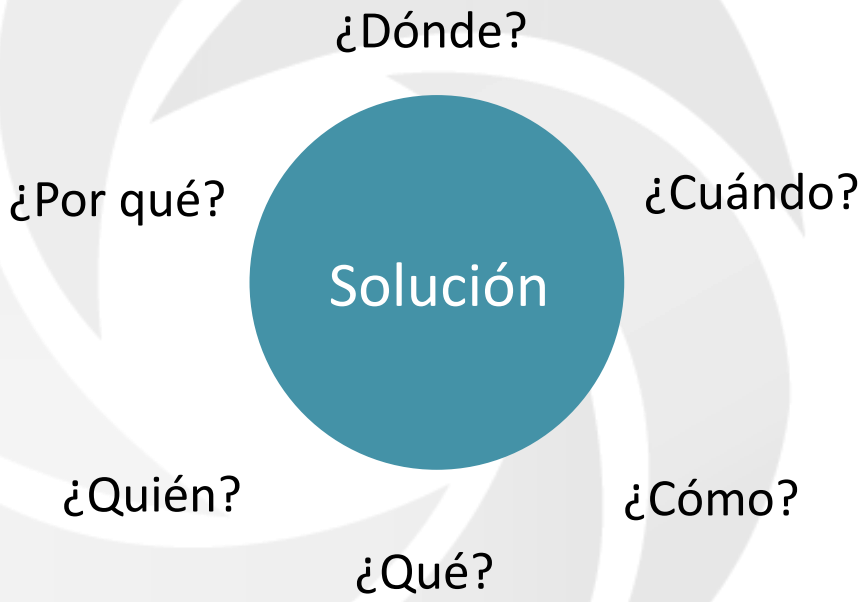
WEBINAR ISO 27001

Estructura de la norma ISO 27001:2013 SGSI

Entendiendo el Contexto de la Organización

Para que una organización cuente con un sistema de gestión eficaz (SG), el SG deben estar alineados con su dirección estratégica y tomar en cuenta los problemas internos y externos que son relevantes, en la planificación para lograr sus objetivos, así como el contexto actual y cambiante y el uso y gestión de las tecnologías de la información (TIC´s)

4.1 ENTENDIENDO EL CONTEXTO DE LA ORGANIZACIÓN



El contexto de la organización se ve afectado por muchos factores, que podemos agrupar en factores externos e internos. Aunque a veces nos puede costar definir si un factor es interno o externo.

4.1 Comprendiendo a la Organización

ISO 31000:2009 principios y directrices para la administración del riesgo, 5.3.2 el contexto externo.

Al establecer el contexto externo se puede incluir

- Legal
- Regulatorio
- Financiero
- Social y cultural
- Tecnológico
- Relaciones con entes externos que impacten a los procesos dentro del SGSI.

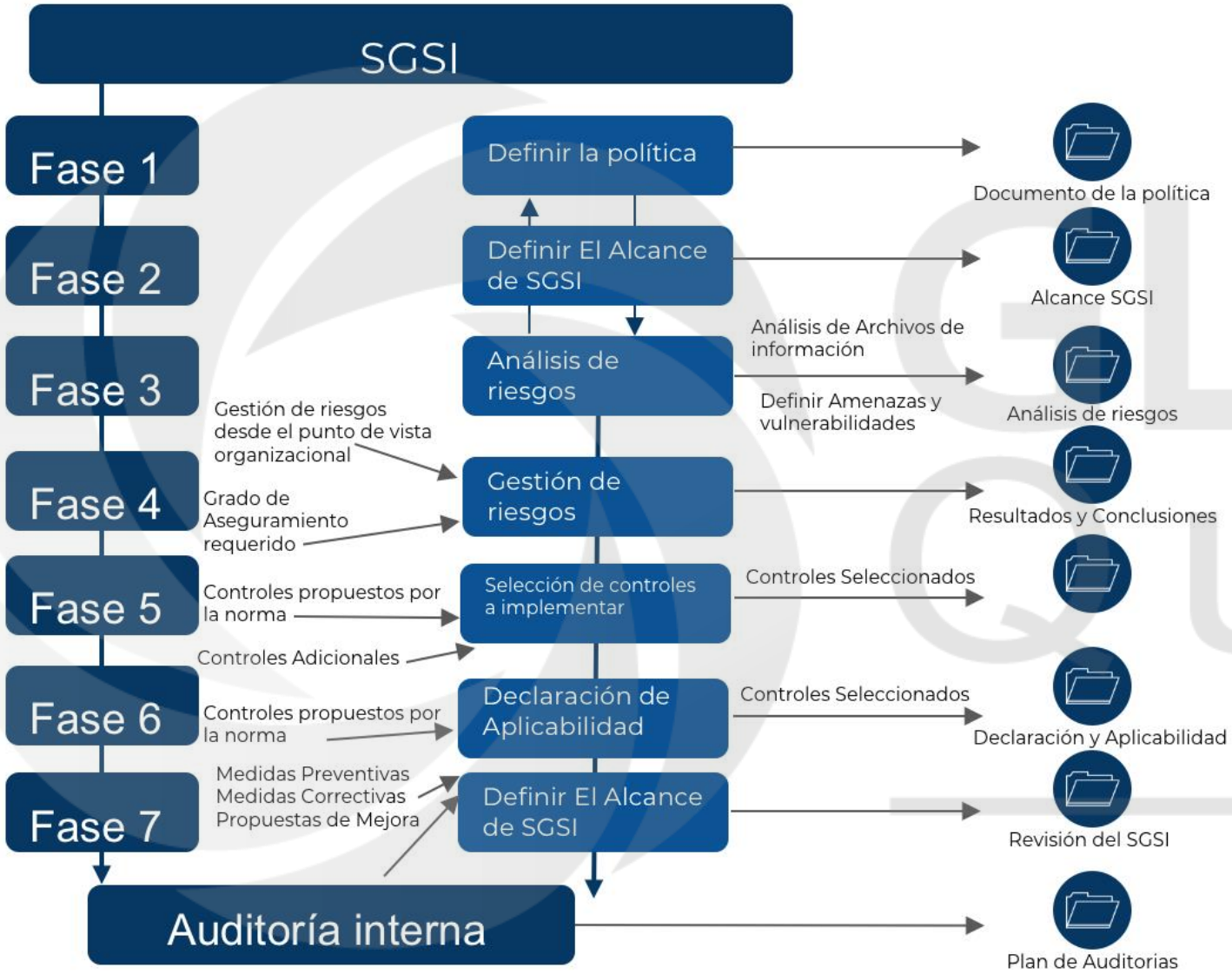
4.1 Comprendiendo a la Organización

ISO 31000:2009 principios y directrices para la administración del riesgo, 5.3.3 el contexto interno.

Al establecer el contexto interno se puede incluir

- Políticas, objetivos y lineamientos estratégicos existentes
- Conocimiento del capital humano en el contexto de la organización
- Normas o modelos regulatorios adoptados por la organización
- Cultura organizacional
- Conocimiento de partes interesadas entre las áreas internas

NOTA: las referencias presentadas no son limitativas



4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

- 59 **debes** dentro de las cláusulas del l 4 al 10
- 114 **debes** correspondientes a los 114 controles de seguridad
- 130 requisitos dentro de las cláusulas del l 4 al 10

4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

y sus procesos:

La extensión (alcance) del SG debería ser evidente en la información documentada apoyar el enfoque del proceso, que soporta la implementación del SG.

- diagramas de proceso (entrada - proceso - salida)
- diagramas que muestran vínculos de proceso (entradas / salidas / cliente)
- superposiciones que muestran las ubicaciones de las actividades
- identificación de procesos externalizados
- diagramas de recursos (por ejemplo, análisis de la capacidad, de mapeo de flujo de valor, “pobre” ...).
- programas
- Identificación de tecnologías de la información y sistemas de procesamiento de Información

4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

ISO 27001 no exige que las empresas documenten el contexto de la organización a través de un documento separado; solo se deben documentar ciertos elementos de problemas internos y externos.

Para problemas internos, debe documentar los relevantes como parte de sus objetivos de seguridad de la información y los resultados de la evaluación de riesgos , y mantener registros de la competencia de sus empleados. (Consulte aquí una Lista de documentos obligatorios requeridos por ISO 27001 (revisión de 2013) .)

GLOBAL Quality CORP

WEBINAR

ISO 27001

Estructura de la norma ISO 27001:2013 SGSI

Acciones para abordar el riesgo y las oportunidades

6.1.1 Consideraciones generales

Al planificar el SGSI, la organización debe considerar:

- 4.1 Asuntos externos
- 4.2 Asuntos internos
- determinar los riesgos y oportunidades que deben dirigirse a:

  a) asegurar que en el SGSI se puede lograr el resultado(s) previsto (s)
  b) prevenir o reducir los efectos no deseados, y
  c) lograr una mejora continua

La organización debe planificar:

d) las acciones para hacer frente a estos riesgos y oportunidades, y

e) cómo. (Como lograrlos y llevar a cabo las actividades inherentes)

1) integrar y poner en práctica las acciones en sus procesos del SGSI, y

2) evaluar la efectividad de estas acciones.

Evaluación del Riesgo

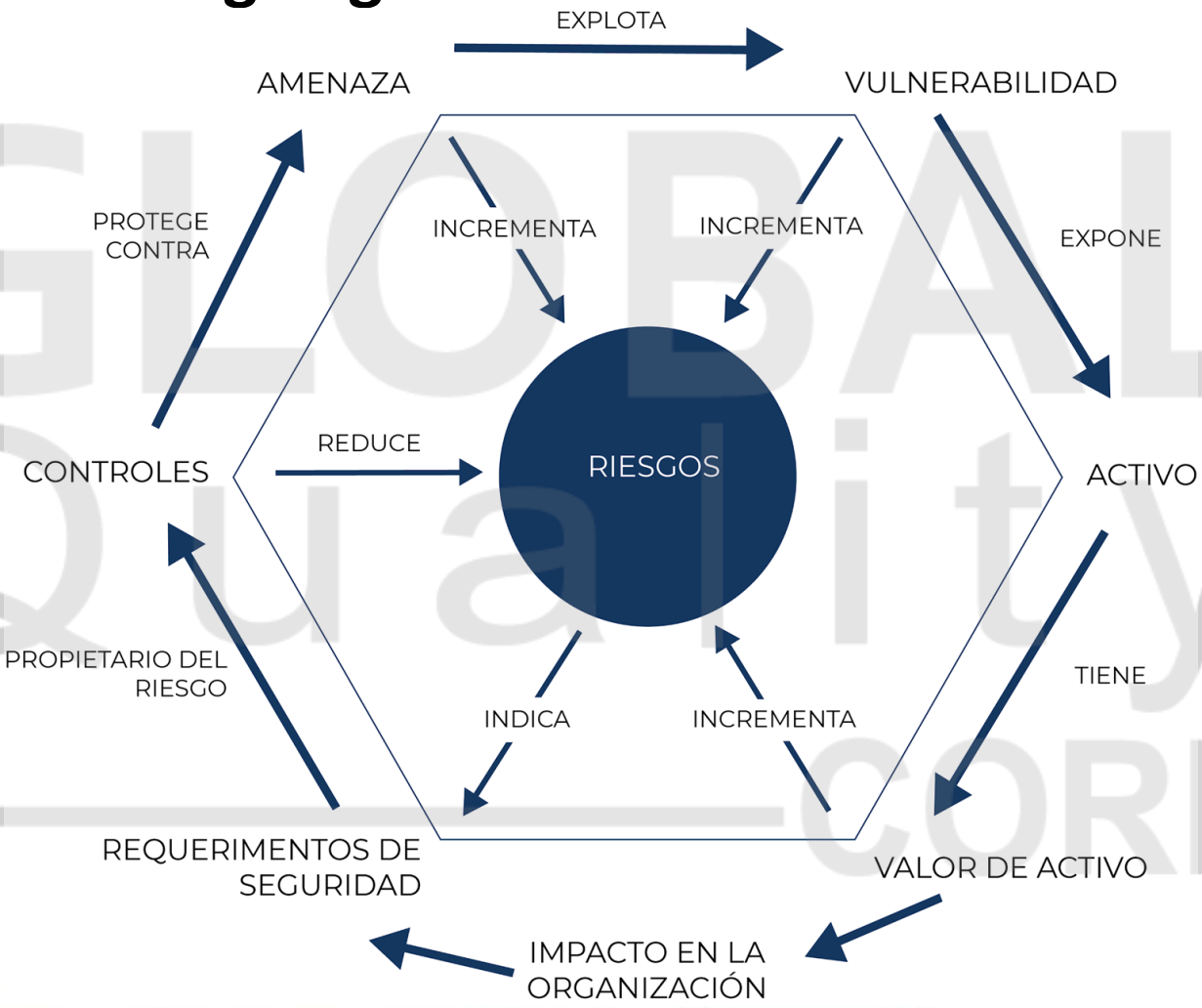
Es necesario un enfoque sistemático para la gestión del riesgo de la seguridad de la información para identificar las necesidades organizativas con respecto a los requisitos de la seguridad de la información y crear un sistema de gestión de la seguridad de la información (SGSI).

La gestión del riesgo de la seguridad de la información debe ser una parte integral de todas las actividades de la gestión de la seguridad de la información y debe aplicarse tanto a la implementación como a la operación en curso de un SGSI.

6.1.2 Evaluación del Riesgo ligado al SGSI

La organización debe definir y aplicar un proceso de evaluación de riesgos de seguridad de la información.

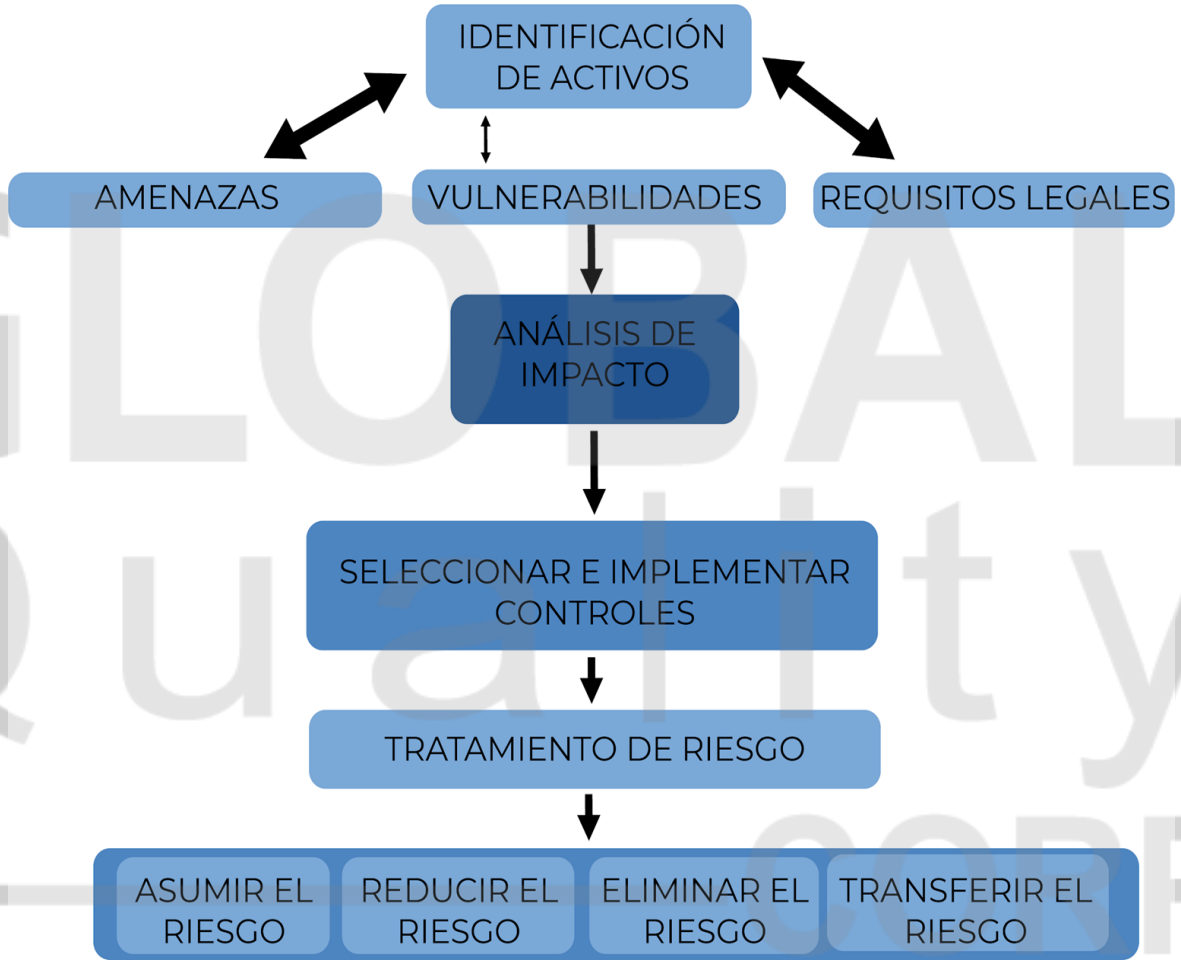
- Criterios evaluación
- Criterios de aceptación
- Impacto a la CID
- Consecuencias
- Posibilidad de ocurrencia
- Nivel del riesgo (ponderación)
- Resultados comparables
- Clasificación (establecimiento de prioridades)



NOTA: identificar y asignar al dueño (propietario) del riesgo.

6.1.3 Tratamiento del Riesgo ligado al SGSI

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información a:



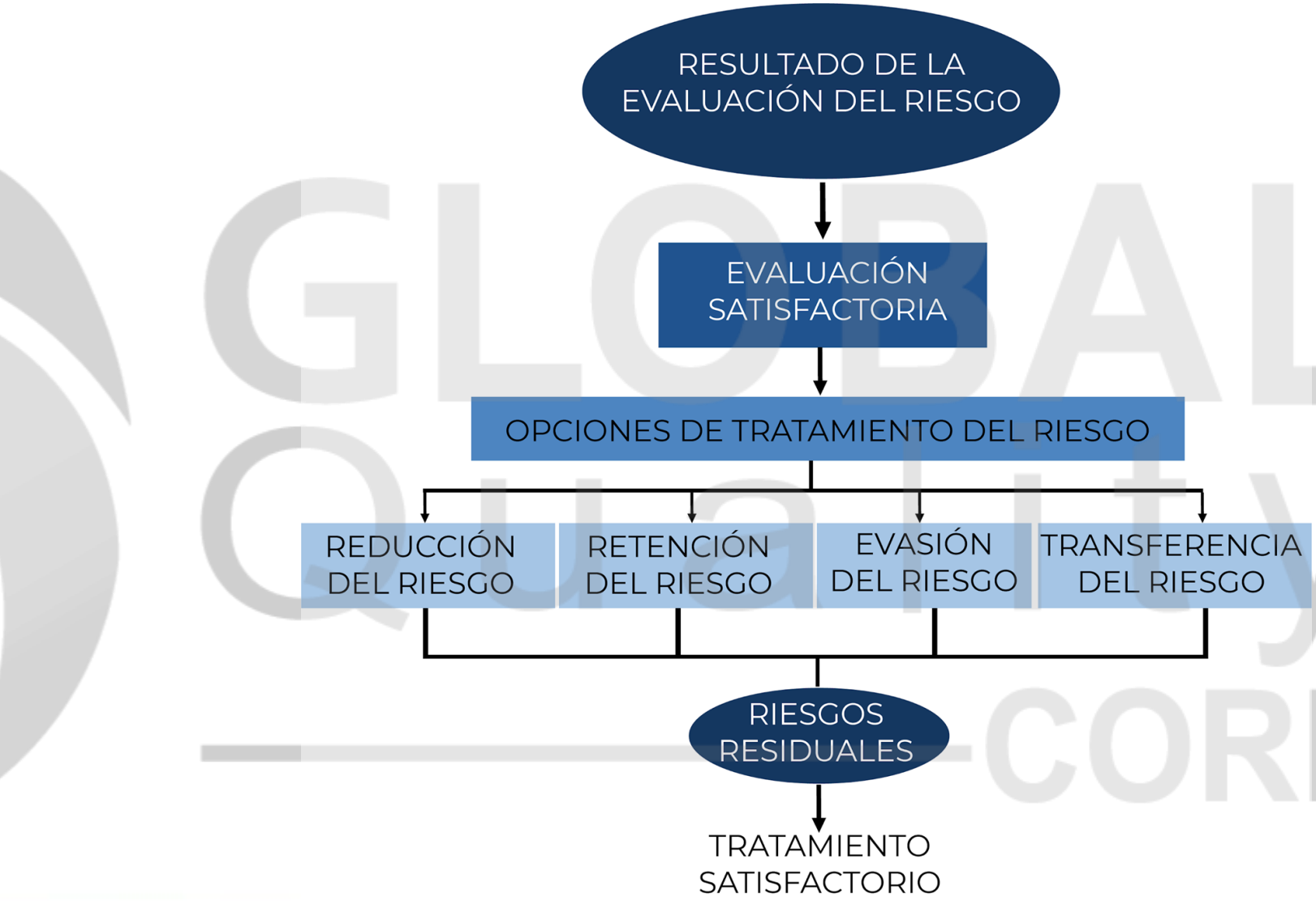
NOTA: la organización puede diseñar controles según sea necesario, considerando aquellos detectados en cualquier búsqueda.

Tratamiento del Riesgo ligado al SGSI

Las opciones del tratamiento del riesgo deben seleccionarse basadas en el resultado de la evaluación del riesgo, los costos esperados para implementar estas opciones y los beneficios esperados de estas opciones.

Cuando las reducciones grandes en los riesgos pueden obtenerse con un gasto bajo relativamente, tales opciones deben implementarse. Las opciones adicionales para mejoras pueden ser necesidades no-económicas y legales para ejercitarse sí son justificables.

Tratamiento del Riesgo ligado al SGSI



Tratamiento del Riesgo ligado al SGSI

Los planes del tratamiento del riesgo deben describir como los riesgos evaluados son tratados para cumplir con el criterio de aceptación del riesgo (véase 7.2, Criterio de aceptación del riesgo).

Es importante para los gerentes responsables revisar y aprobar los planes propuestos de tratamiento del riesgo y riesgos residuales resultantes, y registrar algunas condiciones asociadas con tal aprobación.

Tratamiento del Riesgo ligado al SGSI
IDENTIFICACION DE ACTIVOS

Activo de Procesamiento de información						
Clasificación	No.	Activo	Descripción	Ubicación	Dueño	Custudio
Proceso de negocio	1	Administración de nómina y personal	Dentro de este proceso se considera las actividades inherentes a la administración de personal de diferentes empresas	Instalaciones de la ORG	Organización	Área de nómina y personal

Generar una lista de activos de procesamiento de información considerando, hardware, software, personal, instalaciones, bases de datos, documentos físicos etc.

Tratamiento del Riesgo ligado al SGSI
VALOR ORGANIZACIONAL

Valor Organizacional de Activos				
Confidencialidad	**integridad**	**Disponibilidad**	**Costo de reposición (M.N)**	**Valor institucional (M.N)**
Reservado	Medio	Medio	$40,000.00	$320,000.00

A cada activo de procesamiento de la información asignar una categoría de confidencialidad, y valores de integridad y disponibilidad

Tratamiento del Riesgo ligado al SGSI
VALORACION DEL RIESGO Y VULNERABILIDADES

Análisis de riesgos

Amenazas	Controles Existenciales	Probabilidad	Vulnerabilidades	Degradación			Valor Impacto	Impacto	Valor de Riesgo	Valor de riesgo
				C	I	D				
7.10 cruce de información (Envío de información de un cliente a otro)	N/A	Baja	5.3 Falla de identificación del remitente/ receptor	x	x		8	Medio	2	Bajo
7.18 Falla en el respaldo de datos y documentos	N/A	Media	4.29 Falta de verificación en la integridad del respaldo		x	x	8	Medio	4	Medio
5.38 Virus de archivos	N/A	Baja	4.12 Control de descargas inadecuado	x	x	x	9	Medio	2	Bajo
7.27 Incumplimiento de la legislación	N/A	Media	7.12 Inadecuado seguimiento de cambio legislativo		x		7	Medio	4	Medio
6.2 Error del personal operativo (confundir nombre de empleados)	N/A	Media	2.7 Falta de controles operativos y /o tecnología para el manejo de información y vigilancia		x		1	Bajo	2	Bajo

Realizar la identificación de amenazas y vulnerabilidades aplicables por activo de procesamiento de información identificando también posibles controles existentes probabilidad de impacto y degradación a la CID

Tratamiento del Riesgo ligado al SGSI
TRATAMIENTO DE RIESGOS

Tratamiento de riesgos							
Acción	Control de la norma ISO	Responsable	Riesgo			Responsable de supervisión	Plan de tratamiento de riesgos
			Grado de aseguramiento	Riesgo Residual	Descripción de riesgo residual		
Reducir			Medio	Medio			
Aceptar			Medio	Medio			
Aceptar			Medio	Medio			
Aceptar			Medio	Medio			
Aceptar			Medio	Medio			
Aceptar			Medio	Medio			

Con base en los resultados de la evaluación de riesgos asignar controles del anexo A de la norma y buenas practicas para el establecimiento de planes de tratamiento

Al planificar cómo alcanzar los objetivos de seguridad de la información, la organización debe determinar:

f) lo qué se hará;

g) los recursos que serán necesarios;

h) quien será responsable;

i) cuando se completará, y

j) cómo se evaluarán los resultados.

Los objetivos de Seguridad de la Información deberían establecerse en las funciones, niveles y procesos pertinentes, según sea apropiado, para asegurar el despliegue eficaz de la dirección estratégica de la organización y de su política de la calidad considerando los niveles aceptables de Confidencialidad, Integridad y Disponibilidad de a información y requisitos de partes interesadas.

Los objetivos de la Seguridad de la Información deberían establecerse y medirse usando técnicas adecuadas, como SMART, (es decir, establecer objetivos de la calidad que son Específicos, Medibles, Alcanzables, Relevantes y acotados en el Tiempo), cuadros de mando integrales, o paneles de control; los objetivos de la calidad deberían actualizarse o añadirse según sea necesario, para reflejar cualquier cambio implementado.

GLOBAL Quality CORP

WEBINAR ISO 27001

Estructura de la norma ISO 27001:2013 SGSI

7. Soporte

- 7.1 Recursos: La organización debe determinar y proveer de los recursos necesarios para la implementación mantenimiento y mejora continua del SGSI.
- 7.2 Competencias: Determinar, evaluar y ejecutar las acciones pertinentes para asegurar y satisfacer los requisitos de competencias establecidos.
- 7.3 Concientización: Del personal de la organización sobre la política, su contribución y rol dentro del SGSI y las consecuencias del incumplimiento.
- 7.4 Comunicación: determinar los lineamientos y necesidades de comunicación internas y externas, considerando las partes interesadas.

- 7.5.1 Generales
- 7.5.2 Creación y Actualización
- 7.5.3 Gestión y control de la información documentada

7.5 Información documentada

Generalidades

Cuando la Norma ISO/IEC 27001:2013 hace referencia a “mantener la información documentada”, significa asegurarse de que la información se mantiene actualizada; por ejemplo, la información contenida en los procedimientos documentados, manuales, formularios y listas de verificación, información que podría almacenarse en la nube y descargarse a un teléfono inteligente u otro dispositivo electrónico, y otra información documentada (como la política y los objetivos de la Seguridad de la Información).

Requisitos de Documentación Del SGSI

CLAUSULA	DOCUMENTACIÓN
4.3	Alcance del SGSI
5.2	Política de seguridad de la información
6.1.2	Proceso de evaluación del riesgo
6.1.3	Proceso de tratamiento del riesgo
6.1.3 d)	Acuerdo de Aplicabilidad (SoA)
6.2	Objetivos de Seguridad
7.2 d	Evidencias de competencias (RH)
7.5.1 b)	Información documentada (que la organización considere pertinente y necesaria para evidenciar y asegurar ña eficacia del SGSI)
8.1	Planeación y control operativo

Requisitos de Documentación Del SGSI

CLAUSULA	DOCUMENTACIÓN
8.2	Resultado de la evaluación del riesgo
8.3	Resultados del tratamiento del riesgo
9.1	Evidencias(registros) de los resultados del monitoreo y medición
9.2 g)	Evidencia de las auditorias su programación resultados y seguimiento
9.3	Evidencias de ejecución y resultados de revisiones por la dirección
10. 1 f)	Evidencia y seguimiento a las no conformidades y la naturaleza de estas
10.1 g)	Evidencia de los resultados delas acciones correctivas

GLOBAL Quality CORP

WEBINAR

ISO 27001

Estructura de la norma ISO 27001:2013 SGSI

8. Operaciones

➢ 8.1 Planificación y control operacional:

- Implementación y control de procesos
- Mantener documentación necesaria para asegurar el apego a los procesos planeados
- Control de cambios y las consecuencias de estos
- Controlar los procesos externos y subcontratados que impacten al SGSI

8.2 EVALUACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

- Ejecución de evaluaciones a intervalos planificados Considerando 6.1.2 a)
- Evidencia de los resultados de las evaluaciones del riesgo

- Implementación de planes de tratamiento
- Evidencia de los resultados y planes de tratamiento del riesgo

Una manera útil de abordar el desarrollo de normas de política y procedimientos operacionales respecto a la seguridad de la información es considerar cada punto de orientación para la implementación de la norma ISO / IEC 27001: 2013 e ISO / IEC 27002:, que se considera aplicable (en base a los resultados de la evaluación de riesgos), y describir con precisión la forma en que se debe aplicar cada política y/i procedimiento documentado.

GLOBAL Quality CORP

WEBINAR

ISO 27001

Estructura de la norma ISO 27001:2013 SGSI

9. Evaluación del Desempeño

- **9.1 Seguimiento, medición, análisis y evaluación**
  - Que necesita ser monitoreado
  - Determinar el método de monitoreo, evaluación que garanticé resultados validos y reproducibles
  - Cuando realizar la evaluación
  - Quien evaluara
  - Cuando analizar los datos resultados de la evaluación
  - Quien analizara y evaluara los resultados

Evaluar el desempeño y eficacia del SGSI

Información documentada Como evidencia de los resultados de la evaluación

La intención de este apartado es que la organización analice y evalúe los datos y la información de los resultados del seguimiento y medición a fin de determinar si los procesos, productos y servicios cumplen los requisitos, y determinar cualquier acción necesaria y las oportunidades de mejora.

Las salidas del análisis y evaluación toman a menudo la forma de información documentada como análisis de tendencias o informes, cuadros de mando integral, paneles de control, y se convierten en una entrada para la revisión por la dirección o para reuniones que consideren esa salida.

Por este motivo, debería estar en un formato que permita determinar si es necesario tomar acciones para mejorar el sistema de gestión de la Seguridad de la Información.

9.2 AUDITORIA INTERNA

La organización debe:

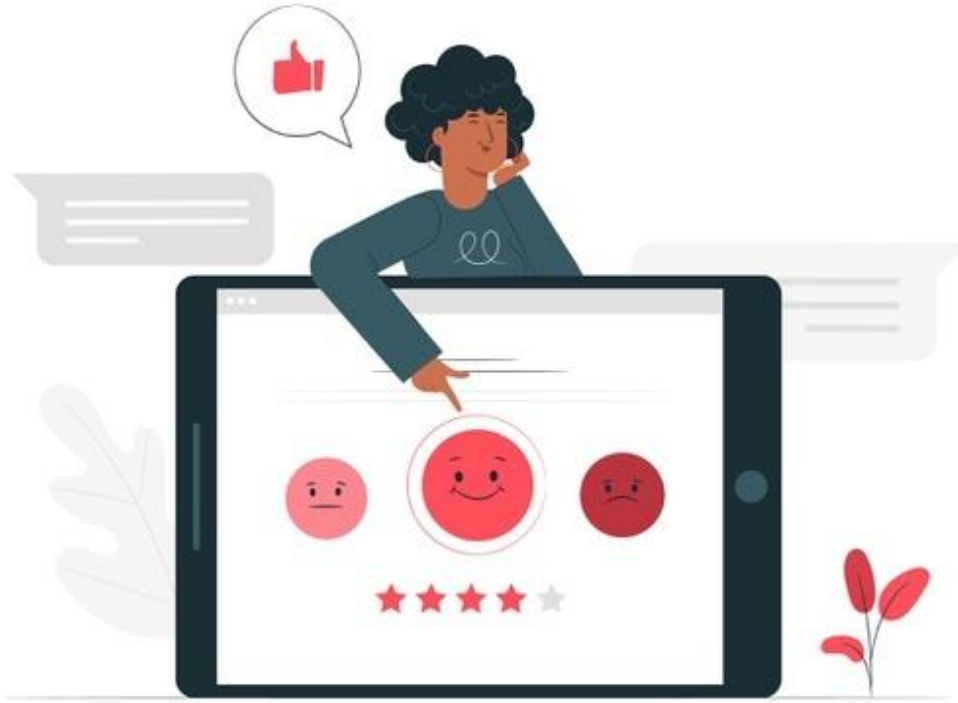
c) planificar, establecer, implementar y mantener un programa (s) de auditoría, incluida la periodicidad los métodos, responsabilidades, requisitos de planificación y presentación de informes. Las auditorías programadas) deberán tomar en consideración la importancia de los procesos en cuestión y los resultados de auditorías anteriores;

9.3 REVISIÓN POR LA DIRECCIÓN

La alta dirección debe revisar el sistema de gestión de seguridad de la información, de la organización a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia.

Se debe asegurar que la revisión por la dirección proporciona salidas e información sobre el desempeño y eficacia del sistema de gestión de la Seguridad de la Información, y sobre todas las decisiones y acciones necesarias.

Las salidas de la revisión por la dirección incluyen decisiones y acciones relacionadas con las oportunidades para la mejora (véase el apartado 10 de la Norma ISO/IEC 27001:2013), cambios necesarios en el sistema de gestión de la Seguridad de la Información (véase el apartado 6.3 de la Norma ISO/IEC 27001:2013), y recursos necesarios (véase el apartado 7.1 de la Norma ISO/IEC 27001:2013.



GLOBAL Quality CORP

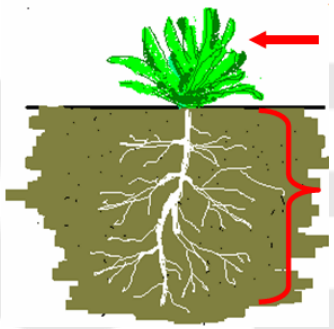
WEBINAR

ISO 27001

Estructura de la norma ISO 27001:2013 SGSI

10. Mejora y Acción Correctiva

10 Mejora



SINTOMA
PROBLEMA

CASA
RAIZ

➢ 10.1 No conformidades y acciones correctivas

La organización debe:

- reaccionar ante la no conformidad
- Evaluar la necesidad de toma de acciones
- Implementar las medidas oportunas
- Contemplar posibles cambios al SGSI si es necesario
- Conservar información documentada como evidencia de las acciones.

10.2 MEJORA CONTINUA

La organización debe mejorar continuamente la conveniencia,
adecuación y eficacia del sistema de gestión de seguridad de la información.

La intención de este apartado es asegurar que la organización mejora continuamente la idoneidad, adecuación y eficacia de su sistema de gestión de la Seguridad de la Información.

La mejora continua puede incluir acciones para incrementar la coherencia de las salidas, productos y servicios, a fin de incrementar el nivel de salidas conformes, mejorar la capacidad de los procesos y reducir las variaciones en los procesos.

Existen varias metodologías y herramientas que la organización puede considerar para realizar actividades de mejora continua (kaizen). Los ejemplos pueden incluir, pero no se limitan a: metodologías Seis Sigma; iniciativas “Lean / manufactura esbelta”; los estudios comparativos con las mejores prácticas (benchmarking), y el uso de modelos de autoevaluación.

GLOBAL Quality CORP

WEBINAR ISO 27001

Estructura de la norma ISO 27001:2013 SGSI

Anexo A: Controles

Anexo A Controles de la ISO/IEC 27001:2013

- 14 clausulas de seguridad
- 35 Categorías de Seguridad
- 114 Controles de seguridad

Clausula

Categoría

A.5 Política de seguridad de la información		
A.5.1 Dirección de la gestión para la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo a la gestión de la seguridad de la información conforme a los requisitos del negocio, leyes y reglamentos pertinentes (relevantes)		
A.5.1.1	Política de la seguridad de la información	Control La gerencia deberá definir y aprobar un conjunto de políticas de seguridad dela información que deberán ser publicadas y comunicadas a los empleador y a las partes externas relevantes.
A.5.1.2	Revisión de la política de la seguridad de la información	Control Las políticas de seguridad de la información se deberán revisar a intervalos planeados o si ocurren cambios considerables para asegurar su conveniencia, adecuación y eficacia.

DOMINIO 5

Política de seguridad de la información

- Definición de políticas aprobadas comunicadas interna y externamente a las partes interesadas, las cuales deberán ser revisadas a intervalos regulares.
- Proporcionar orientación y apoyo a la gestión de seguridad de la información con apego a los requerimientos de la organización leyes y reglamentos pertinentes.

DOMINIO 6

Organización de la seguridad de la información

- Establecer una gestión y estructura de trabajo para la implementación y gestión del SGSI
- Designación de roles y responsabilidades ligaras a la seguridad de la información

Seguridad ligada a dispositivos móviles y teletrabajo

DOMINIO 7

Seguridad en el Recurso Rumano (RH)

- Previo al empleo (selección)
- Durante el empleo
- Posterior al empleo

DOMINIO 8

Seguridad en la gestión de activos e información

- Inventario de activos (identificando al propietario)
- Reglas de uso aceptable de activos (manejo de activos)
- Retorno de activos
- Clasificación de la información (etiquetado)
- Gestión y eliminación de medios

DOMINIO 9

Control de acceso

- Gestión de acceso físico y lógico
- Registro de los accesos
- Gestión de privilegios
- Revisión de derechos
- Modificación y remoción de privilegios
- Responsabilidad del usuario

DOMINIO 10

Control de criptográfico

- Gestión de políticas para uso de controles criptográficos
- Gestión y administración de claves

DOMINIO 11

Seguridad física y ambiental

- Áreas seguras
- Ubicación y seguridad de los activos
- Seguridad en el cableado
- Mantenimiento y traslado de equipo
- Reciclado y eliminación segura de activos
- Equipo desatendido
- Pantalla y escritorio limpio

DOMINIO 12

Seguridad en las operaciones y medios para este fin

- Procedimientos operacionales
- Gestión de cambios y capacidades
- Ambientes de pruebas
- Seguridad ante código malicioso (virus-worm´spam)
- Respaldos
- Registros y evidencias
- Control de acceso al sistema operacional
- Gestión del riesgo operacional y vulnerabilidad técnica

DOMINIO 13

Seguridad y gestión en las comunicaciones

- Gestión y control de RED
- Segmentación de redes(operacional- visitas)
- Gestión en el intercambio de información
- Gestión de los mensajes electrónicos (correos)
- Acuerdos de confidencialidad

DOMINIO 14

Seguridad y gestión en el desarrollo de software

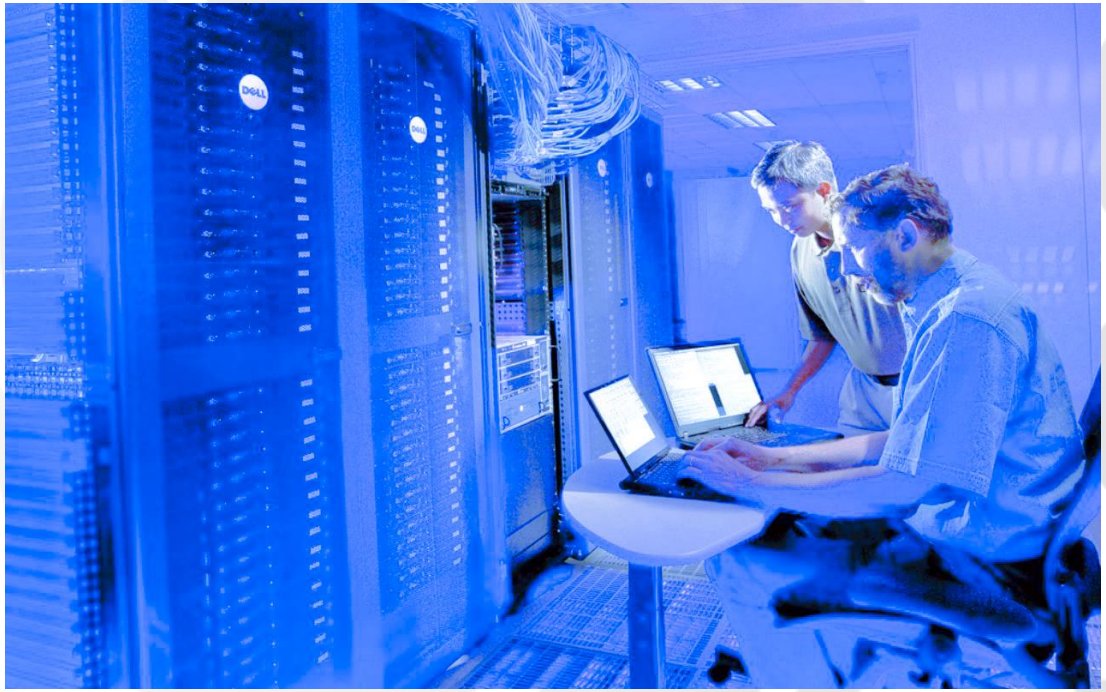
- Gestión y análisis de especificaciones
- Gestión de la seguridad en redes publicas
- Gestión de la seguridad en el desarrollo
- Gestión de la seguridad en la subcontratación del desarrollo
- Gestión de pruebas y entorno de desarrollo
- Gestión y políticas para proveedores

DOMINIO 15

Seguridad ligada a los proveedores

- Gestión y monitoreo de los servicios contratados
- Acuerdos con proveedores
- Seguridad y políticas ligados al proveedor

DOMINIO 16



Seguridad y gestión de incidentes

- Gestión y registro de incidentes de seguridad
- Responsabilidades ante incidentes
- Evaluación de las incidencias
- Aprendizaje de las incidencias
- Recolección de evidencias

DOMINIO 17

Seguridad y gestión de la continuidad del negocio

- Gestión de la seguridad de la información y la continuidad
- Generación e implementación de un plan de continuidad
- Verificación de la continuidad de las operaciones
- Gestión de la redundancia
- Disponibilidad de los recursos e instalaciones para la continuidad

DOMINIO 18

Gestión del cumplimiento legislativo

- Gestión de la legislación aplicable
- Derechos de propiedad intelectual
- Protección de los registros
- Protección de los datos personales
- Regulación de los controles criptográficos (legislación)
- Revisiones a la seguridad de la información

Gracias

Por seleccionarnos como tu centro capacitador de confianza, en nombre de todos los que conformamos:

GLOBAL Quality CORP

Estamos a tus ordenes para cualquier duda y/o comentario en nuestros correos y teléfonos:

francisco.h@globalqualitycorp.com

(55) 2791 6389

Síguenos en nuestras redes sociales:

¿Qué aprenderás durante el curso?

- Estructura de Alto Nivel
- SOA (anexo de la norma)
- Controles

PONENTES:

Si este curso te gusto, ayúdanos a llegar a mas personas:

¡Reseña este Curso Webinar!