La nueva versión ISO 27001:2013

Un cambio en la integración de los sistemas de gestión

Auspicia:

PRIME Asesoría y Desarrollo Integral PROFESIONAL

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los equipos"

Kevin Mitnick

AGENDA

I. ¿Qué es la ISO?
II. La nueva estructura ISO 27001:2013.
III. Nuevos conceptos.
IV. La ISO 27002:2013.
V. Conclusiones

I. ¿Qué es la ISO?

International Organization for Standardization

La ISO y sus principios de gestión

Es una federación mundial de organismos nacionales de normalización alrededor de 160 países, trabajan a nivel de Comités Técnicos, tienen al menos 19,000 estándares publicados desde 1947 (creación), 1951 (publicación).

Trabaja en función a 8 principios de gestión:

1. Orientación al cliente.
2. Liderazgo.
3. Participación del personal.
4. Enfoque de procesos.
5. Enfoque de sistemas de gestión.
6. Mejora Continua.
7. Enfoque de mejora continua.
8. Relación mutuamente beneficiosa con el proveedor.

La ISO y sus estándares

Incremento de la demanda en las empresas por implementar sistema de gestión estandares (ISO 9001, ISO 27001, ISO 22301, ISO 20000 otras).
Los estandares ISO son aplicables a cualquier tipo y tamaño de empresa.

Name of standard	Number of certificates in 2011	Number of certificates in 2010	Evolution	Evolution in %
ISO 9001	1 111 698	1 118 510	-6 812	-1%
ISO 14001	267 457	251 548	15 909	6%
ISO 50001	461	0		
ISO/IEC 27001	17 509	15 626	1 883	12%
ISO 22000	19 980	18 580	1 400	8%
ISO/TS 16949	47 512	43 946	3 566	8%
ISO 13485	20 034	18 834	1 200	6%
TOTAL	**1 484 651**	**1 467 044**	**17 607**	**1%**

(Source: iso.org)

La ISO y como nace la ISO 27001:2013

Causas:

Los estandres ISO se revisan cada 4 o 5 años.

Los controles de la ISO 27002 muchos son obsoletos.

La necesidad de integrar los sistemas de gestión (Anexo SL, PAS 99).

Historia:

- El proyecto nace con la aprobación de un articulo en el New Work Item (NWI) el 19 de mayo 2009.
- Lo primeros 3 borradores de trabajo conservan la estructura de 1ra edición.
- La estructura común y el texto básico actual aplican al draft 4 en oposición de varios organismos nacionales.
- El 2012-02-15 el Consejo de Gestión Técnica de ISO (TMB) decidió que la norma ISO 27001 tiene que seguir la nueva estructura, unificado, pero que las desviaciones justificadas se admiten.
- La alianza para elevar el nivel de abstracción se logró
- La alianza para dejar caer la Declaración de aplicabilidad falló.
- Los intentos para matar el proyecto hasta el final fracasaron.

II. La nueva estructura de la ISO 27001:2013

ANEXO SL

INTEGRAR LAS NORMAS Y TERMINOS COMUNES

- ***ISO 30301:2011**, Información y documentación - Sistemas de gestión de documentos - Requisitos (armonizado con el anexo SL)*
- ***ISO 22301:2012**, la seguridad societaria - Los sistemas de gestión de continuidad de negocio - Requisitos (armonizado con el anexo SL)*
- ***ISO 20121:2012**, sistemas de gestión de la sostenibilidad de eventos - Requisitos con orientación para su uso (armonizado con el anexo SL*
- ***ISO 27001:2013**, sistemas de gestión de la seguridad de la información.*

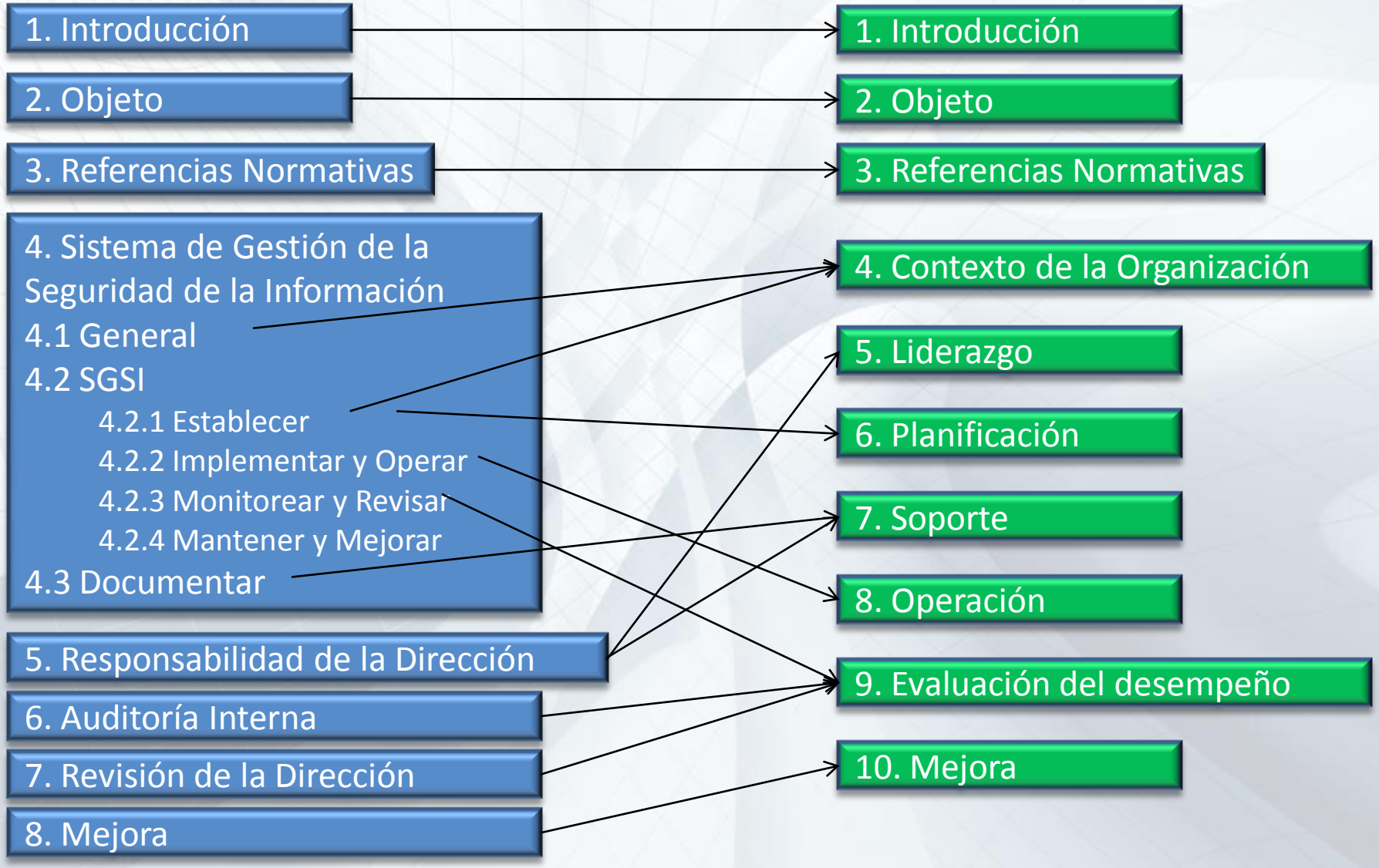
Annex SL common terms

organization	process
interested party (preferred term)	performance
stakeholder (admitted term)	outsource (verb)
requirement	monitoring
management system	measurement
top management	audit
effectiveness	conformity
policy	nonconformity
objective	correction
risk	corrective action
competence	continual improvement
documented information	

Norma ISO 30301:2011	Norma ISO 9001:2015
PROLOGO INTRODUCCIÓN	PROLOGO INTRODUCCIÓN
1. OBJETO Y CAMPO DE APLICACIÓN	1. OBJETO Y CAMPO DE APLICACIÓN
2. REFERENCIAS NORMATIVAS	2. REFERENCIAS NORMATIVAS
3. TÉRMINOS Y DEFINICIONES	3. TÉRMINOS Y DEFINICIONES
4. CONTEXTO DE LA ORGANIZACIÓN 4.1 Comprensión de la organización y su contexto 4.2 Requisitos de negocio, legales y de otra índole 4.3 Definición del alcance del SGD	4. CONTEXTO DE LA ORGANIZACIÓN 4.1. Conocimiento de la organización y de su contexto 4.2. Comprensión de las necesidades y expectativas de las partes interesadas 4.3. Determinación del alcance del sistema de gestión de la calidad 4.4. Sistema de gestión de calidad
5. LIDERAZGO 5.1 Compromiso de la dirección 5.2 Política 5.3 Roles organizativos, responsabilidades y competencias	5. LIDERAZGO 5.1. Liderazgo y compromiso 5.2. Política 5.3. Roles, responsabilidades y autoridades en la organización
6. 6 PLANIFICACIÓN 6.1 Acciones para el tratamiento de riesgos y oportunidades 6.2 Objetivos de gestión documental y planes para alcanzarlos	6. PLANIFICACIÓN 6.1. Acciones para tratar riesgos y oportunidades 6.2. Objetivos de calidad y planificación para lograrlos
7. SOPORTE 7.1 Recursos 7.2 Capacitación 7.3 Concienciación y formación 7.4 Comunicación 7.5 Documentación	7. SOPORTE 7.1. Recursos 7.2. Competencia 7.3. Toma de conciencia 7.4. Comunicación 7.5. Información documentada 7.5.1. Generalidades 7.5.2. Creación y actualización 7.5.3. Control de la información documentada
8. OPERACIÓN 8.1 Planificación y control de operaciones 8.2 Diseño de los procesos de gestión documental 8.3 Implementación de las aplicaciones de gestión documental	8. OPERACIÓN 8.1. Planificación y control operacional
9. 9 EVALUACIÓN DEL DESEMPEÑO DEL SGD 9.1 Supervisión, medición, análisis y evaluación 9.2 Sistema de auditoría interna 9.3 Revisión por la dirección	9. EVALUACIÓN DEL DESEMPEÑO DEL SGD 9.1. Supervisión, medición, análisis y evaluación 9.2. Auditoría interna 9.3. Revisión por la dirección
10. 10 MEJORA 10.1 Control de las no conformidades y acciones correctivas 10.2 Mejora continua	10. MEJORA 10.1. No conformidades y acciones correctivas 10.2. Mejora continua
ANEXO A (Normativo) PROCESOS Y CONTROLES	

Fuente Anexo SL

ISO 27001:2005 Y LA 27001:2013



VENTAJAS Y DESVENTAJAS

VENTAJAS	DESVENTAJAS
Facilita la integración de los sistemas de gestión, debido a que es una estructura de alto nivel, donde los términos y definiciones ayudan a implementar.	Es una abstracción y es un nivel alto, no es tan detallado.
Todas las definiciones vienen del estándar ISO 27000 y las inconsistencias se han removido.	Los requisitos son un tanto mas difícil para interpretar, debido a los nuevos conceptos.
Los riesgos en la seguridad de la información en su conjunto deben ser abordados.	No se menciona el enfoque PDCA.
Los documentos requeridos están claramente establecidos, hace referencia al tamaño y complejidad.	No se menciona las políticas del SGSI.
Menciona que las acciones preventivas no van.	No hay una descripción detallada de la identificación del riesgo.

ALGUNOS DATOS

ISO 27001:2013	ISO 27001:2005
7 CLAUSULAS: La mas resaltante es el contexto de la organización.	5 CLAUSULAS:
154 requerimiento	178 requerimientos
32 nuevos requerimientos	
El anexo A tiene 14 categorías de control (del 5 al 18)	El anexo A tiene 11 categorías de control (del 5 al 15)
Menciona a la ISO 31000 en la clausula 6.1 Acciones para la dirección de riesgos y oportunidades	No menciona la ISO 31000 u otro estándar.

NUEVOS REQUERIMIENTOS

4.2 Entendiendo las necesidades y expectativas de las partes interesadas.
4.3 Determinar los objetivos del SGSI.
5.1 Liderazgo y compromiso.
6.1 Acciones para direccionar los riesgos y las oportunidades.
6.2 Los objetivos de seguridad de la información y la planificación para alcanzarlos.
7.3 Sensibilización.
7.4 Comunicación.
7.5 Información documentada.
8.1 Planificación y control operativo.
9.1 Seguimiento, medición, análisis y evaluación.
9.3 Revisión de la Dirección.
10.1 No-conformidades y acciones correctivas.

III. Nuevos conceptos

¿Qué es Información?

Las cuentas bancarias, estados de cuenta, deuda tributaria, resultados de análisis clínicos, configuración de un equipo de red, códigos de un sistema, tipo de cambio, la propuesta técnica y económica, estado financiero, el CV, la compra de una empresa, las imágenes de una cámara, los sueldos, correos, grabación de un teléfono, logs de auditoría, contratos, examen de admisión, identificación, resultados electorales, la comunicación telefónica, …

La **información** es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Para sus actividades diarias, operaciones de su trabajo, para cumplir con sus funciones, el cual puede equivocarse o no, o hacer el bien o el mal. La información tienen estructura que modificará las sucesivas interacciones del ente que posee dicha información con su entorno.

¿Qué es Seguridad de la Información?

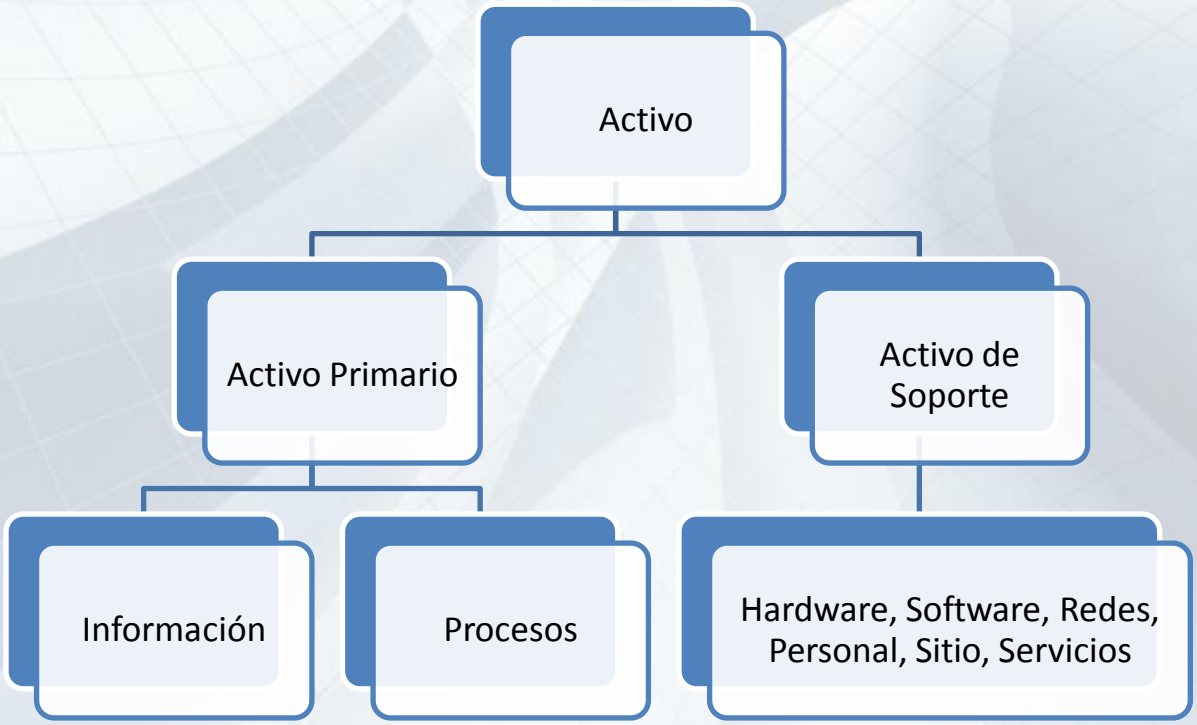
La información es un recurso que, como el resto de los activos, tiene **valor para una organización y por consiguiente debe ser debidamente protegida**. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La información puede existir en muchas formas. Puede estar **impresa o escrita en papel, almacenada electrónicamente, transmitida por un medio electrónico, presentada en imágenes, o expuesta en una conversación**. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

ACTIVOS

ISO 27002:2013 Clausula 8.1

Activos relacionados con las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de los activos deberá estar redactado y mantenido.

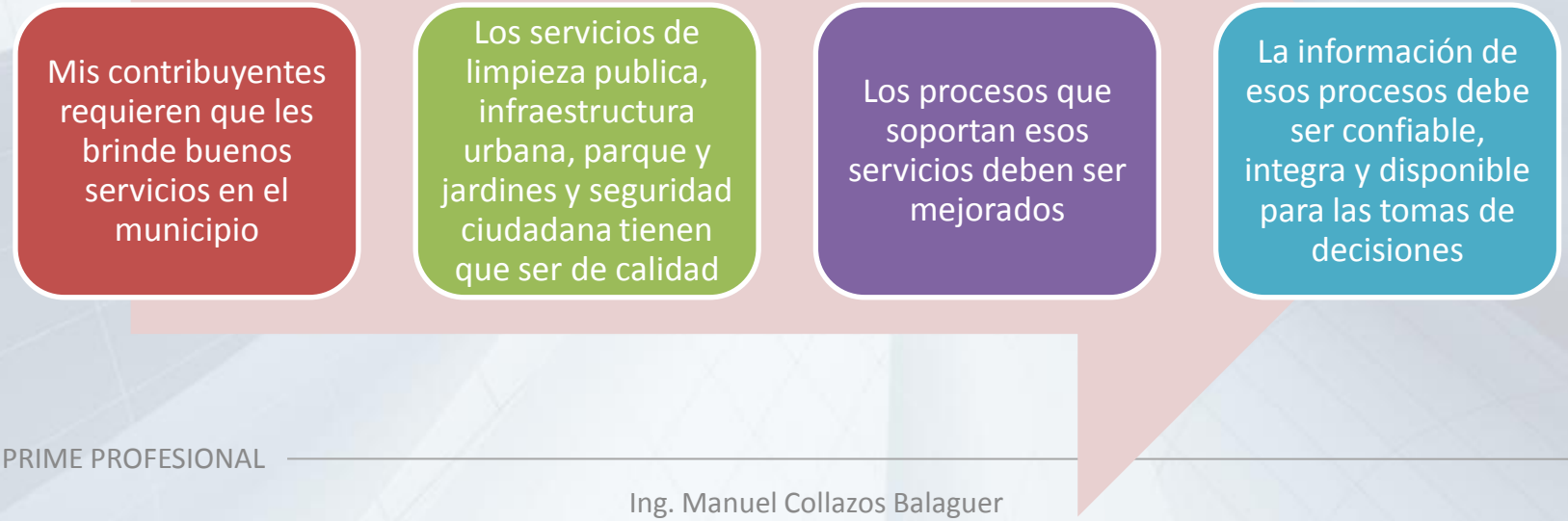


PARTES INTERESADAS

ISO 27001:2013 Clausula 4.2

Entendiendo las necesidades y expectativas de las partes interesadas

a) las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información, y
b) los requisitos de estas partes interesadas pertinentes a la seguridad de la información.



RIESGOS

ISO 27001:2013 Clausula 6.1.2 Evaluación de los riesgos de la seguridad de la información.

c) identifica los riesgos de seguridad de la información:

1) aplicar el proceso de evaluación de riesgos de seguridad de información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información en el ámbito del sistema de gestión de la seguridad de información, y

2) identificar a los propietarios de los riesgos;

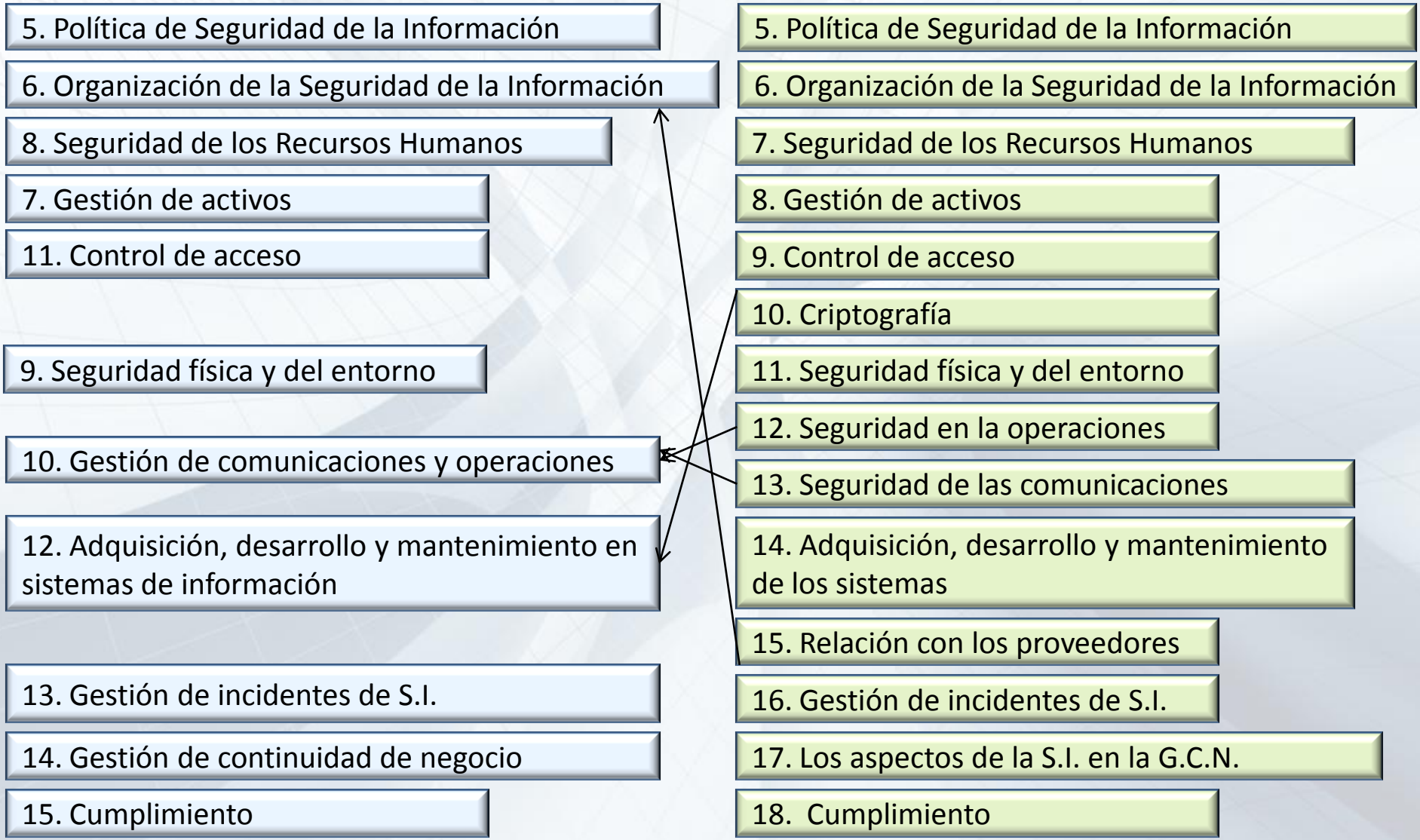
LIDERAZGO

ISO 27001:2013 Clausula 5.3 Roles de organización, responsabilidades y autoridades

La alta dirección debe asegurarse de que las responsabilidades y autoridades para las funciones pertinentes a la seguridad de información se asignen y se comuniquen.

IV. La ISO 27002:2013

ISO 27002:2005 Y LA ISO 27002:2013



ISO 27002:2005 Y LA ISO 27002:2013

ISO 27002:2005	ISO 27002:2013
11 Clausulas de controles de seguridad de la información	14 Clausulas de controles de seguridad de la información
39 Categorías de control	35 Categorías de control
133 controles	111 controles
21 controles borrados	14 nuevos controles
	Cerca de 20 controles fuertemente revisados
	Mas de 30 controles actualizados
	Varios controles fusionados

ISO 27002:2005 Y LA ISO 27002:2013

Controles eliminados	Controles nuevos
6 .1.2 Coordinador de seguridad de la información	6.1.5 Seguridad de la información en la gestión de proyectos
10.4.2 Control de código móvil	12.6.2 Restricciones en la instalación de software
11.4.2 Autenticación de usuarios en las conexiones externas	14.2.5 Principios en Ingeniería de seguridad de los sistemas
11.4.4 Diagnostico remoto y protección de la configuración de los puertos	14.2.8 Prueba de la seguridad de los sistemas
11.4.6 Control de las conexiones de las redes	17.1.2 Implementar la continuidad de la seguridad de la información
12.2.2 Control en el procesamiento interno	15.1.3 Tecnología de información y comunicación en la cadena de suministro

V. Conclusiones

CONCLUSIONES

Se nos viene un gran reto en la gestión de la seguridad de la información con la nueva ISO 27001:2013

Los conceptos que debemos reforzar: Partes interesadas, Liderazgo, Sensibilización, Comunicación, Capacidades, Propietario del riesgo, Activos, Gestión de Riesgos y Oportunidades, entre otros.

Se tiene un año para las empresas certificadas en adaptar este nueva versión de la ISO 27001:2013

La ISO 27003, 27004 y 27005 deben asumir nuevos roles bajo la óptica de la ISO 27001:2013

La ISO 27002:2013 tiene menos controles en cantidad y en método hay menos controles tecnológicos, adicionalmente se cuentan con políticas de control mas claras.

Las empresas que han realizado el esfuerzo de implementar la ISO 27001:2005, deben tomar estrategias para alinear su implementación a la ISO 27001:2013

PRIME Asesoría y Desarrollo Integral PROFESIONAL

Muchas Gracias por su atención!

Ing. Manuel Collazos Balaguer
MASTER IMPLEMENTADOR Y AUDITOR LIDER ISO 27001,
AUDITOR LIDER BS 25999
IMPLEMENTADOR LIDER ISO 22301
manuel.collazos@prime.pe

Calles Las Begonias 52839 Lince. Lima – Perú.
Central: (511) 222-1249
Directo: (511) 222-1249
Fax: (511) 273-2501
Celular: (511) 998-117-438
www.prime.pe
www.capacitacionprime.pe