ISO/IEC 27001

Sistema de Gestión
de Seguridad de la Información

Juan Carlos Morales, CISA, CISM, CRISC, CGEIT

Instructor

Juan Carlos Morales

Magister Artium

Ingeniero de Sistemas

UFM universidad FRANCISCO MARROQUÍN

Bachiller en Ciencias y Letras

ISACA

COBIT 5 AN ISACA FRAMEWORK

APM GROUP

Instructor autorizado de COBIT 5 acreditado por APMG

Miembro de ISACA poseedor de las cuatro certificaciones

CISA Certified Information Systems Auditor

CISM Certified Information Security Manager

CGEIT Certified in the Governance of Enterprise IT

CRISC Certified in Risk and Information Systems Control

Instructor

Juan Carlos Morales

Faceta como escritor

amazon

Smashwords

SOPHOS
por el placer de leer

BARNES&NOBLE
BN.com

Trabajos desempeñados

BAYER

Walmart

Actualmente

Consultor e Instructor de Tecnología de la Información

Docencia

UFM
FRANCISCO MARROQUÍN

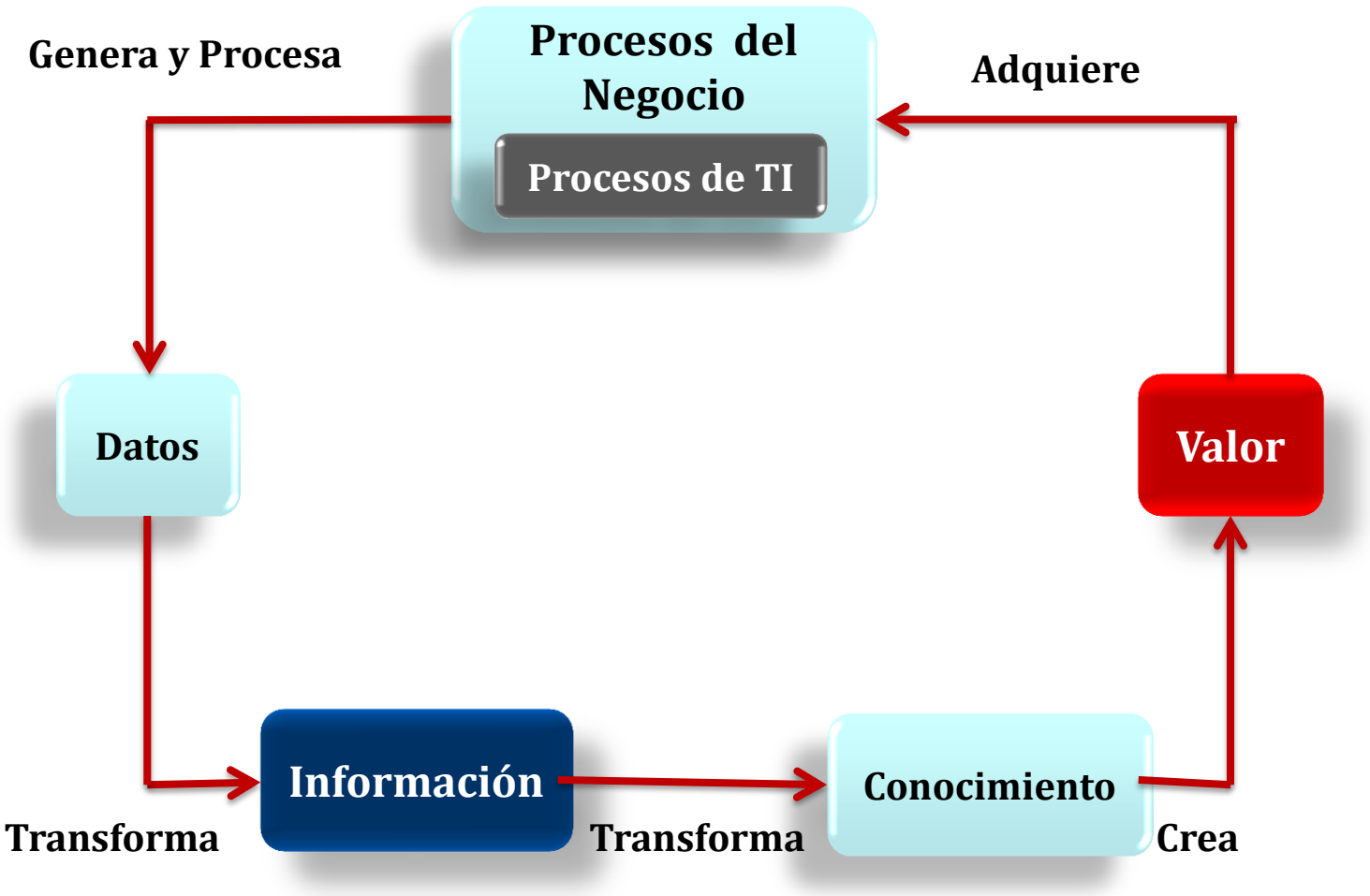
Universidad Rafael Landívar

ISACA

ITLearning

BDO ESENFA

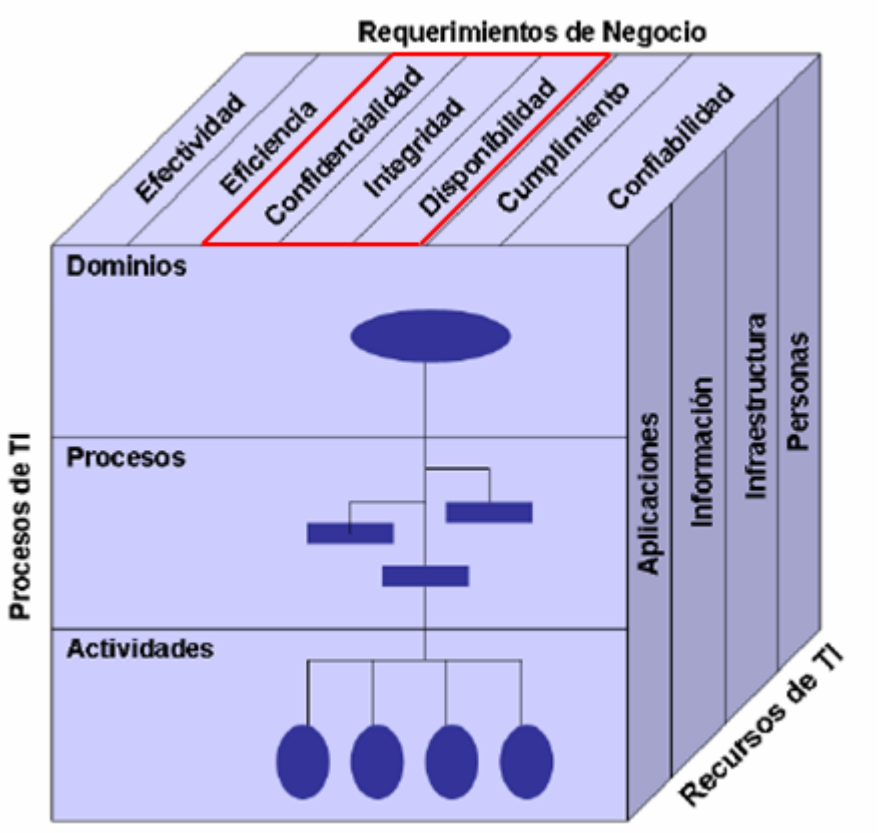
¡Se trata de información!



Seguridad de la Información

- ❑ Confidencialidad
- ❑ Integridad
- ❑ Disponibilidad

Criterios de la información



ISO/IEC 27001:2013

- Especifica los requerimientos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información en el contexto de la organización.
- Incluye los requerimientos para evaluar y tratar los riesgos de seguridad de información de acuerdo a las necesidades de la organización.
- Los requerimientos establecidos en la norma ISO/IEC 27001:2013 son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.

COBIT 5

APO13 Gestionar la Seguridad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	
Propósito Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.	

APO13 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
APO13.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	**De**	**Descripción**	**Descripción**	**A**
	Fuera del Ámbito de COBIT	Enfoque de seguridad de la empresa	Política de SGSI	Interno
			Declaración de alcance del SGSI	APO01.02 DSS06.03

ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

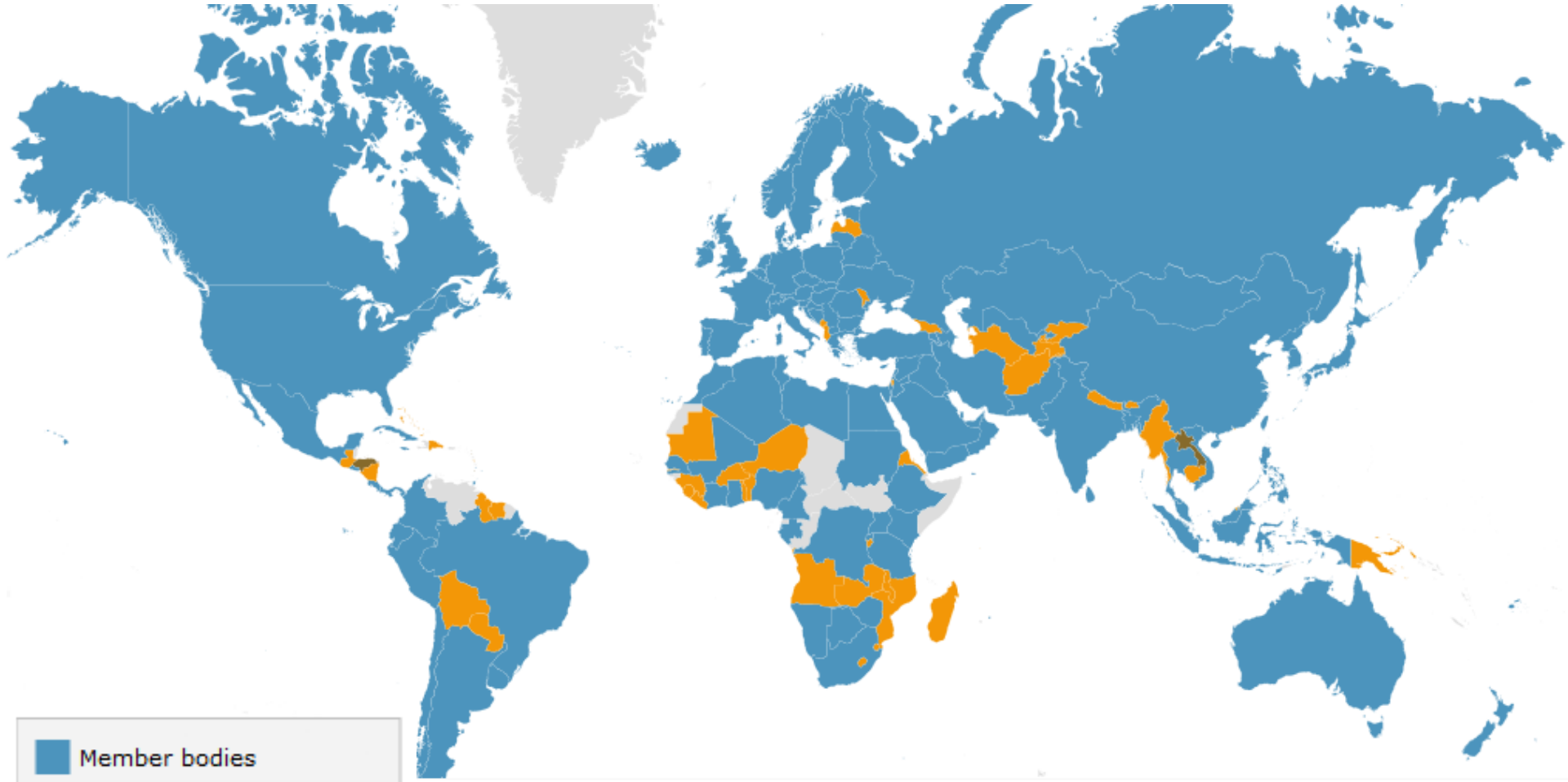
© ISO/IEC 2013

Introducción

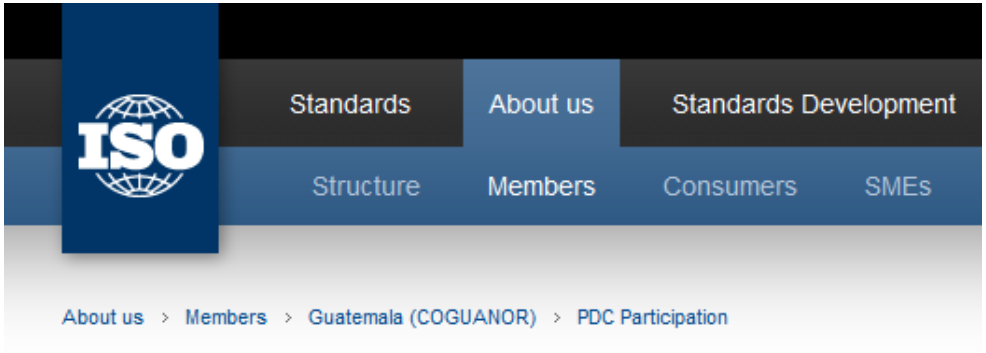
ISO/IEC

- ISO: Organización Internacional de Normalización
- IEC: Comisión Electrotécnica Internacional

Miembros ISO



Guatemala es miembro corresponsal



Participation in PDCs

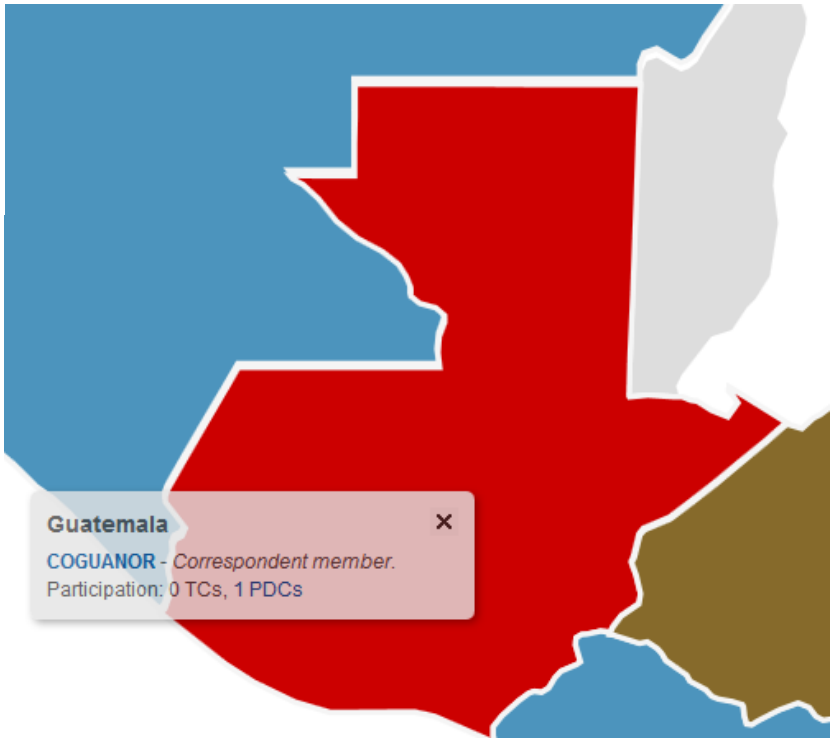
Guatemala (COGUANOR)

ISO/DEVCO - Committee on developing country matters (*O-Member*)

Comisión Guatemalteca de Normas
Calzada Atanasio Tzul 27-32 zona 12
GT-Guatemala C.A. 010012

Tel: +502 2247 2654
Fax: +502 2247 2687
E-mail: info-coguanor@mineco.gob.gt
Web: www.coguanor.gob.gt

- La Comisión Guatemalteca de Normas (COGUANOR), adscrita al Ministerio de Economía, fue creado por el Decreto N º 1523 del Congreso Nacional en 1962.
- COGUANOR ha sido miembro de la ISO desde 1997



Estándares de TI en Guatemala

- Comisión Guatemalteca de Normas, del Ministerio de Economía.
- De la estructura de COGUANOR forma parte el Comité Técnico de Normalización 71 (CTN/71) relativo a Tecnología de la información (TI).
- Este Comité es homólogo al ISO/IEC/JTC1.

Recursos ISO

ISO Resources

ISO's Website (in English and French, with top levels in Russian and individual publications in other languages)
www.iso.org

***ISO Focus+* magazine**
(10 editions annually in English and French)
www.iso.org/iso/iso-focus-plus

ISO videos
www.youtube.com/PlanetISO

ISO Café
www.iso.org/isocafe

Follow us on **Twitter**!
www.twitter.com/isostandards

Join us on **Facebook**!
www.facebook.com/isostandards

Contact the ISO member in your country:

www.iso.org/isomembers

ISO/IEC JTC 1

- Los organismos nacionales miembros de ISO e IEC participan en el desarrollo de normas internacionales a través de comités técnicos
- En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto: ISO / IEC JTC 1

ISO/IEC 27001:2013

- Provee los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información
- La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización
- Incluye los requisitos para la evaluación y tratamiento de los riesgos de seguridad de información, adaptados a las necesidades de la organización

El SGSI se ve influencia por:

- Necesidades de la organización
- Objetivos
- Requisitos de seguridad
- Procesos organizativos
- Tamaño y estructura de la organización

El SGSI

- El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos.
- Las partes interesadas tendrán la confianza de que los riesgos se gestionan adecuadamente.

El SGSI

- Es importante que el sistema de gestión de seguridad de la información esté integrado con los procesos de la organización y con la estructura de gestión.

El SGSI

- Es importante que la seguridad de información se considere en el diseño de:
  - Procesos
  - Sistemas de información
  - Controles

El SGSI

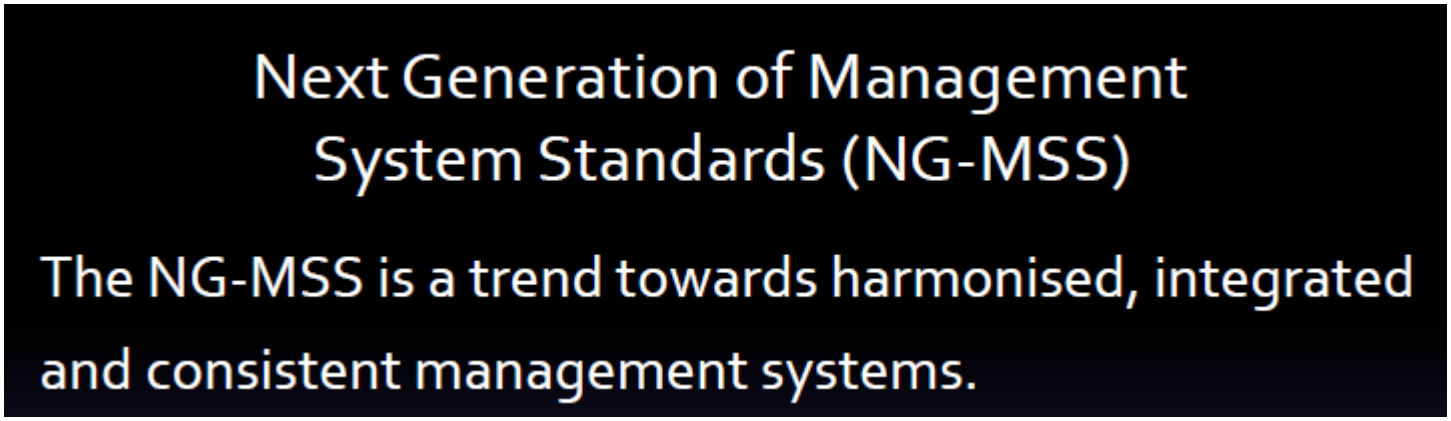
- Se espera que la implementación del sistema de gestión de seguridad de la información se amplíe de acuerdo con las necesidades de la organización

ISO/IEC 27001:2013

- Esta Norma Internacional la pueden utilizar las partes internas y externas para evaluar la capacidad de la organización para cumplir con los requisitos de seguridad de la información propios de la organización

Compatibilidad con otras normas

- ISO/IEC 27001:2013 aplica la estructura de alto nivel, los títulos de sub-capítulos idénticos, texto idéntico, términos comunes y definiciones básicas definidas en el Anexo SL de la Directiva ISO/IEC, y por lo tanto mantiene la compatibilidad con otras normas de sistemas de gestión que han adoptado el Anexo SL.



ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Alcance

Alcance de la norma ISO/IEC 27001:2013

- Los requisitos establecidos en la norma internacional son genéricos y se pretende que sean aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.
- Excluir alguno de los requisitos especificados en las cláusulas 4 a 10 no es aceptable cuando una organización afirma conformidad con esta norma internacional.

Referencias de COBIT

AP013 Guías relacionadas	
Estándares relacionados	**Referencia Detallada**
ISO/IEC 27001:2005	Sistemas de gestión de seguridad de información – Requisitos, Sección 4
ISO/IEC 27002:2011	
NIST (National Institute of Standards and Technology) SP800-53 Rev 1	Controles de Seguridad Recomendados para Sistemas de Información Federales de EE.UU.
ITIL V3 2011	Diseño de Servicio, 4.7 Gestión de la Seguridad de la Información.

ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Referencias Normativas

Referencias normativas

- El siguiente documento está normativamente referenciado en ISO/IEC 27001:2013 y es indispensable para su aplicación:
  - ISO/IEC 27000 Sistema de gestión de seguridad de la información - Información general y vocabulario

ISO/IEC 27000:2014

- Describe la visión de conjunto y el vocabulario del sistema gestión de seguridad de la información, que hacen referencia a la familia de sistemas de gestión de seguridad de la información de las normas, incluyendo ISO/IEC 27003, ISO/IEC 27004 y la ISO/IEC 27005, con términos y definiciones relacionados.

ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Términos y definiciones

Términos y definiciones

- Se aplican los términos y definiciones dados en la norma ISO / IEC 27000.
  - ISO/IEC 27000 Sistema de gestión de seguridad de la información - Información general y vocabulario

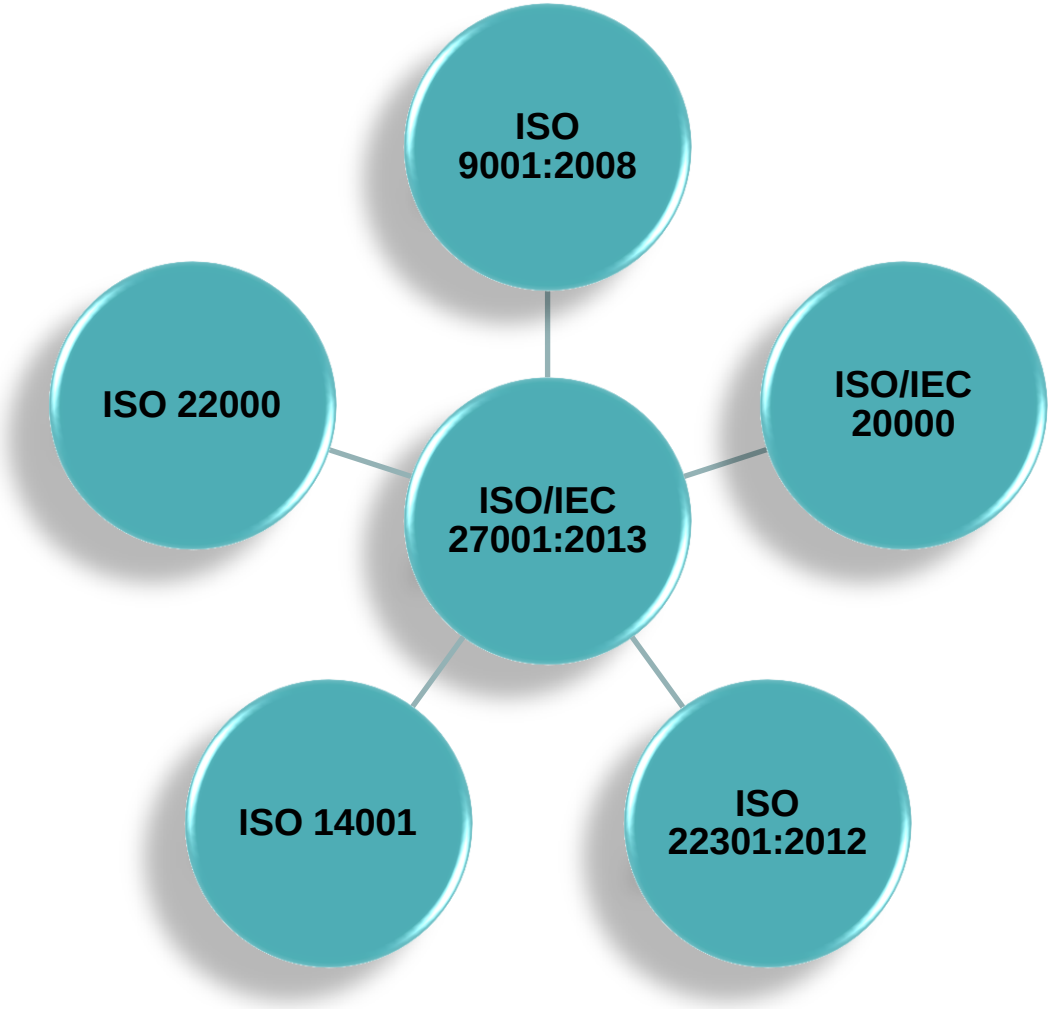
Los principales cambios a la norma

- Cambios introducidos en la evaluación de riesgos (cláusula 6.1.2)
- Propietarios de riesgos (cláusula 6.1.2 y 6.2)
- Más importancia dada a las partes interesadas (cláusula 4.2)
- Ya no se enfoca únicamente en el riesgo técnico, ahora le presta atención al riesgo estratégico (identificación de oportunidades como parte del proceso de gestión de riesgos)

Los principales cambios a la norma

- Cambio en el número de secciones y controles
- Mejora de la comunicación acerca de seguridad de la información (cláusula 7.4)
- Mejorar de la supervisión de la gestión a través del monitoreo de los controles
- Valor añadido al estar alineado con otras normas de sistemas de gestión

Alineación con otros sistemas de gestión



Caso de negocio

- Crimen cibernético: Un SGSI ayudará a mejorar la protección de la organización contra las amenazas del crimen organizado
- Minimizando el riesgo de pérdida o corrupción de la información como resultado de errores humanos
- Mejora del gobierno corporativo al reducir la exposición financiera al riesgo de pérdidas causadas por fallas en los sistemas de TI
- Alineación de la gestión del riesgo de seguridad de la información con ERM

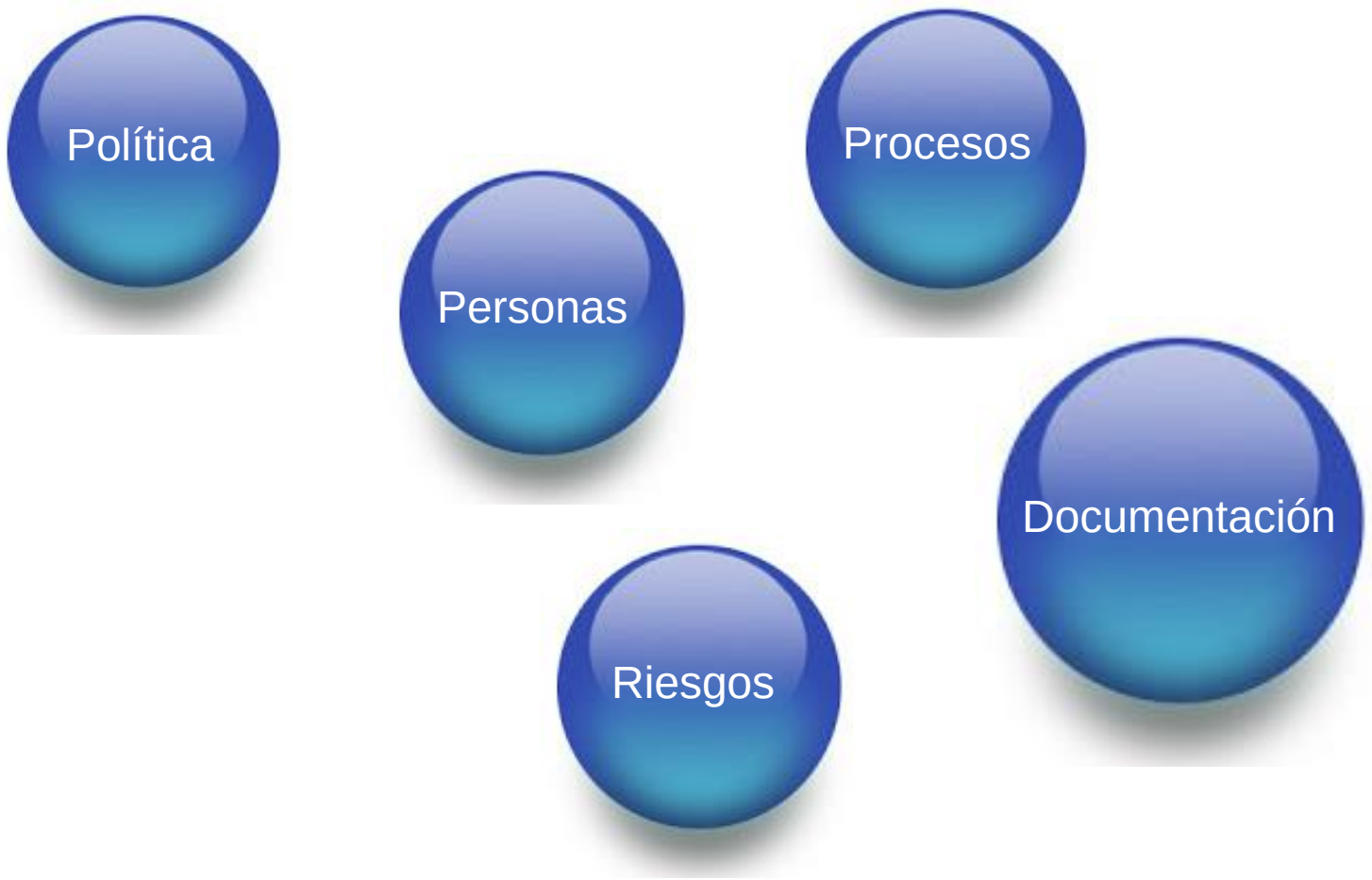
COSO ERM


Estratégicos
Operaciones
Reporte
Cumplimiento
Ambiente de Control
Establecimiento de Objetivos
Identificación de Eventos
Evaluación de Riesgos
Respuesta al Riesgo
Actividades de Control
Información y Comunicación
Monitoreo
Nivel de Entidad
División
Unidad de Negocios
Subsidiaria

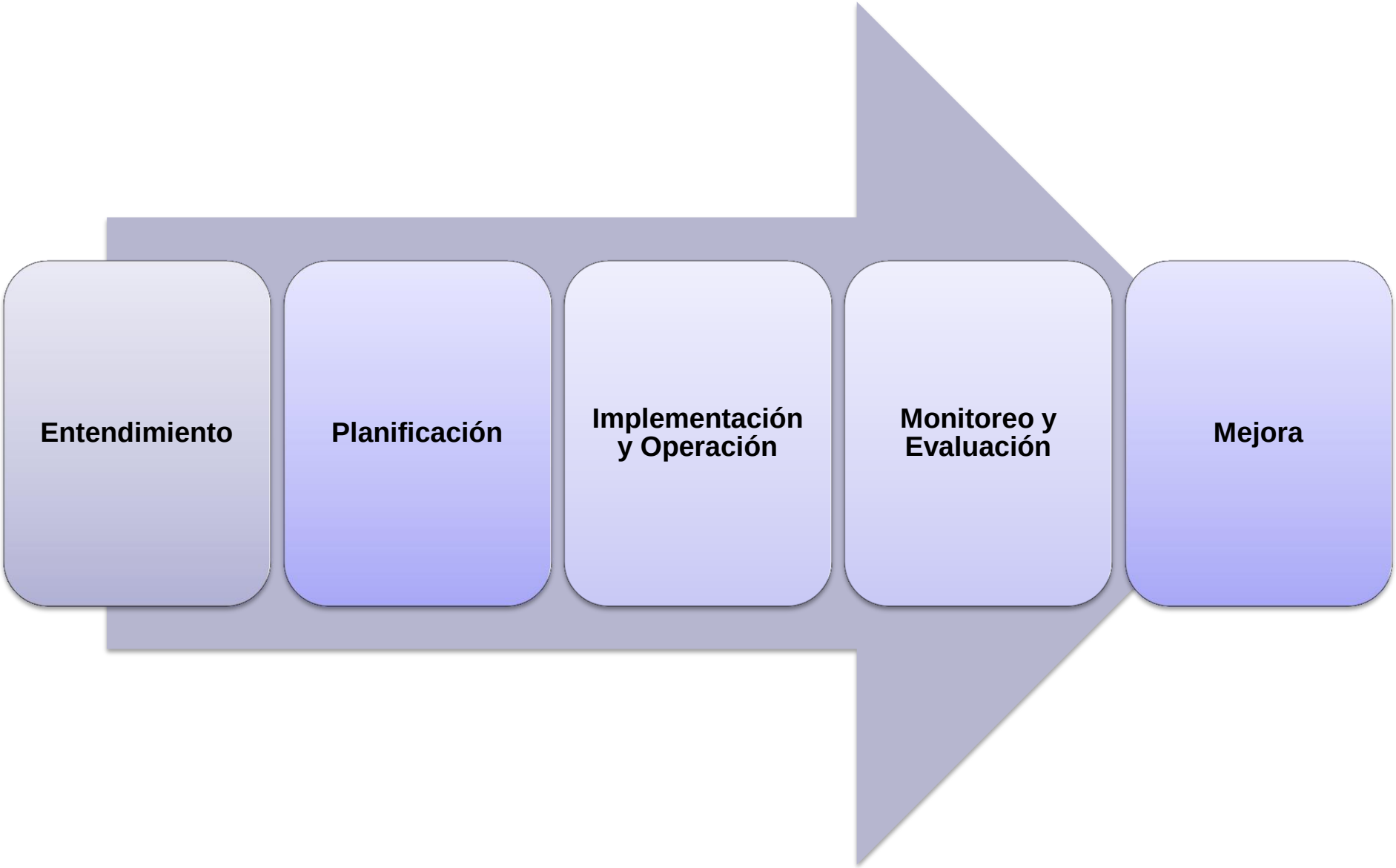
Contenido


Introducción
Alcance
Referencias normativas
Términos y definiciones
Planear
Organización
Entendimiento de la organización y su contexto
Expectativas de las partes interesadas
Alcance del SGSI
Liderazgo
Liderazgo y compromiso de la Alta Dirección
Políticas, roles, responsabilidades y autoridades
Planeación
Acciones para atender riesgos y oportunidades
Objetivos de seguridad de la información
Soporte
Recursos, Competencias, Conciencia
Comunicación, Documentación
Hacer
Operación
Planeación y control operacional
Evaluación de riesgos de seguridad
Revisar
Evaluación de desempeño
Monitoreo, medición, análisis y evaluación
Auditoría interna y Revisión gerencial
Actuar
Mejora
No conformidad y acciones correctivas
Mejora continua

Componentes de un Sistema de Gestión



Fases


Entendimiento
Planificación
Implementación y Operación
Monitoreo y Evaluación
Mejora

Fases

- Entendimiento de los requerimientos de la organización y de la necesidad de establecer una política de seguridad de la información y objetivos de seguridad.
- Planificación
- Implementación y operación de controles para la gestión de riesgos de la organización relacionadas con seguridad de la información
- Monitoreo, evaluación y revisión del desempeño y la eficiencia del SGSI
- Mejora continua basada en mediciones objetivas

ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

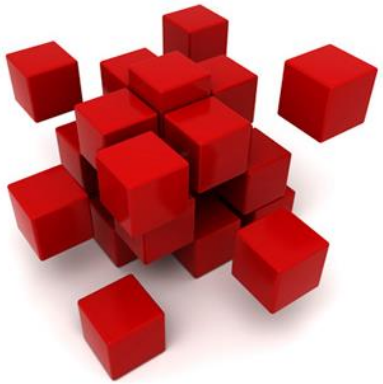
Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Organización

Contexto de la organización

- La organización debe determinar los problemas externos e internos que son relevantes para su propósito y que afectan su capacidad para lograr el resultado deseado de su sistema de gestión de seguridad de la información.



Contexto externo

Problemas

- de la Naturaleza
- Sociales
- Culturales
- Políticos
- Económicos
- Legales
- Tecnológicos
- de la Competencia

Contexto interno

Problemas

- en las políticas
- en los procesos
- organizacionales
- culturales
- de información
- en los servicios
- en las aplicaciones
- en la infraestructura
- en las competencias

Comprensión de las partes interesadas

- Identificar a las partes interesadas externas e internas que son relevantes para el sistema de gestión de seguridad de la información
- Determinar los requerimientos de estas partes interesadas pertinentes a la seguridad de la información

AP013 Gestionar la Seguridad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos

Ejercicio

- Identifique los principales "*stakeholders*" en su organización, tanto internos como externos
- Elabore una lista indicando aquellos con los que se deberá entrevistar o llevar a cabo una reunión o workshop para determinar los requerimientos del SGSI

Determinación del alcance del SGSI

- La organización debe determinar los límites y aplicabilidad del sistema de gestión de seguridad de la información para establecer su ámbito de aplicación.
  - Productos y servicios
  - Procesos
  - Estructura organizacional
  - Ubicación física
  - Legal
  - Contractual
  - Tecnológico

Consideraciones para definir el alcance

- Los problemas externos e internos de la organización
- Los requerimientos de las partes interesadas
- Las interfaces y las dependencias entre las actividades realizadas por la organización, y las que son realizados por otras organizaciones.

Alcance

- El alcance deberá estar disponible como información documentada.

SGSI

- La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, de conformidad con los requisitos de ISO/IEC 27001:2013.

¿Qué es un SGSI?

- Un Sistema de Gestión de Seguridad de la Información (SGSI) consta de políticas, procedimientos, guías, recursos y actividades asociadas, administradas colectivamente por una organización, en la búsqueda de la protección de sus activos de información.

¿Qué es un SGSI?

- Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr sus objetivos de negocio.

Principios de un SGSI

- Conciencia de la necesidad de seguridad
- Asignación de responsabilidades para la seguridad
- La incorporación del compromiso de la dirección y de los requerimientos de las partes interesadas
- Evaluaciones de riesgo que determinen los controles adecuados para alcanzar niveles aceptables de riesgo
- Seguridad de la información incorporada como un elemento esencial en la organización
- Prevención y detección de incidentes de seguridad
- Reevaluación continua de la seguridad de la información

Consideraciones en la planificación

- Contexto externo e interno de la organización
- Requerimientos de las partes interesadas
- Determinación de riesgos y oportunidades

Riesgos y oportunidades

- Asegurar que el sistema de gestión de seguridad de la información puede lograr su resultado previsto
- Prevenir o reducir los efectos no deseados
- Lograr la mejora continua
- La organización debe planificar: las acciones para hacer frente a estos riesgos y oportunidades
- Integrar y poner en práctica las acciones en los procesos del sistema de gestión de seguridad de la información
- Evaluar la eficacia de las acciones

ISO/IEC 27001:2013


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Liderazgo

Liderazgo y compromiso

- Asegurándose de que la política de seguridad de la información y los objetivos de seguridad sean establecidos y que sean compatibles con la dirección estratégica de la organización;
- Garantizando la integración de los requerimientos del sistema de gestión de seguridad de la información con los procesos de la organización;
- Velar por que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;

Liderazgo y compromiso

- Comunicando la importancia de una gestión eficaz de seguridad de la información y de adaptarse a los requisitos del sistema de gestión de seguridad de la información;
- Garantizando que el sistema de gestión de seguridad de la información alcance su resultado previsto;
- Dirigiendo y apoyando a las personas para contribuir a la eficacia del sistema de gestión de la seguridad de la información;

Liderazgo y compromiso

- Promoviendo la mejora continua
- Apoyando a otras funciones de gestión pertinentes para demostrar su liderazgo ya que se aplica a su áreas de responsabilidad.

Liderazgo y compromiso

AP013 Gestionar la Seguridad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	
Propósito Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.	

AP013 Prácticas, Entradas/Salidas y Actividades del Proceso				
Práctica de Gestión	**Entradas**		**Salidas**	
	De	**Descripción**	**Descripción**	**A**
AP013.01 Establecer y mantener un SGSI. Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	Fuera del Ámbito de COBIT	Enfoque de seguridad de la empresa	Política de SGSI	Interno
			Declaración de alcance del SGSI	AP001.02 DSS06.03

Liderazgo y compromiso

- La alta dirección debe establecer una política de seguridad de la información

Política de seguridad de la información

- Que sea apropiada para el propósito de la organización;
- Que incluya los objetivos de seguridad de la información o proporcione el marco para establecer los objetivos de seguridad información;
- Que incluya un compromiso de cumplir con los requisitos aplicables relacionados con la seguridad de la información;
- Que incluya un compromiso de mejora continua del sistema de gestión de seguridad de la información

Política de seguridad de la información

- Disponible como información documentada;
- Comunicada dentro de la organización;
- A disposición de las partes interesadas, según corresponda

Liderazgo y compromiso

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

Responsabilidad y autoridad para:

- Garantizar que el sistema de gestión de seguridad de la información se ajusta a los requisitos de la norma Internacional ISO/IEC 27001:2013
- Informar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección

Roles y Responsabilidad

- Propietarios de la información
- Dueños de procesos
- Propietarios del sistema
- Propietarios de la infraestructura

Definición de Gobierno Corporativo de TI

- El sistema por el cual el uso actual y futuro de TI es dirigido y controlado.
- El gobierno corporativo de TI implica evaluar y dirigir el uso de TI para apoyar la organización y el seguimiento de este uso para lograr los planes.
- Incluye la estrategia y las políticas para el uso de TI en una organización.

Alineación Estratégica

- La alineación de TI requiere de liderazgo y el compromiso de los más altos niveles de la empresa.
- Requiere la participación activa del director ejecutivo (CEO) y de la Junta Directiva

Alineación Estratégica

- Requiere que la Junta Directiva tome la responsabilidad de:
  - Asegurarse de que la estrategia de TI esté alineada con la estrategia del negocio
  - Asegurarse de que los entregables de TI estén alineados con la estrategia
  - Dirigir la estrategia de TI a balancear adecuadamente las inversiones entre los sistemas que soportan el negocio, y los que lo transforman y lo hacen crecer
  - Tomar decisiones informadas acerca del enfoque y la prioridad para el uso de los recursos de TI

¿Por qué es importante la alineación de TI?

- La investigación llevada a cabo por Price Waterhouse Coopers en octubre del 2003 a nombre de ITGI ha puesto en relieve los principales problemas relacionados con TI, a los que se enfrentan los ejecutivos de las empresas, debido a la falta de alineación de la estrategia de TI con la estrategia del negocio.

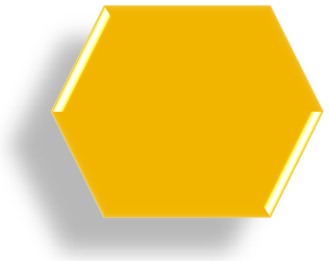
Principales problemas

- Incorrecto enfoque de los recursos de TI
- La incapacidad de la empresa para alcanzar su pleno potencial
- Falta de identificación y capitalización de las oportunidades de negocio que puedan ser habilitadas por TI
- Mayores costos de operación y desventaja competitiva debido a la falta de automatización
- Mayores costos generales
- Erosión de valor para los accionistas a través del tiempo

Principios de la norma ISO/IEC 38500

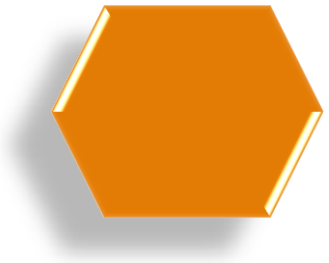
Principio 1: Responsabilidad

- Los individuos y grupos dentro de la organización comprenden y aceptan las acciones que tienen bajo su responsabilidad respecto a la oferta y la demanda de TI, y tienen la autoridad para llevarlas a cabo.



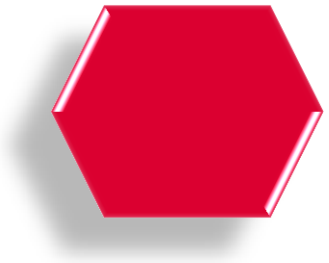
Principio 2: Estrategia

- La estrategia de la organización toma en cuenta las capacidades de TI, tanto actuales como futuras. Los planes estratégicos de TI satisfacen las necesidades actuales de la estrategia de negocios de la organización.



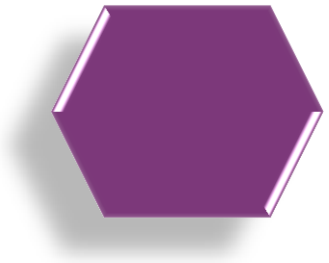
Principio 3: Adquisición

- Las adquisiciones de TI se hacen por razones válidas, sobre la base de un análisis apropiado y con una toma de decisiones clara y transparente. Existe un equilibrio adecuado entre los beneficios, oportunidades, costos y riesgos, tanto en el corto, como en el largo plazo.



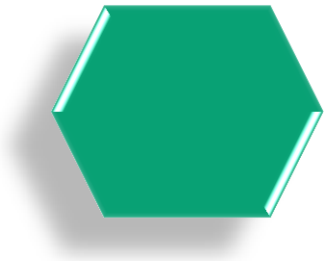
Principio 4: Desempeño

- TI es apto para el propósito de apoyar a la organización, prestando los servicios, los niveles de servicio y la calidad de servicio requerida para cumplir con los requerimientos actuales y futuros del negocio.



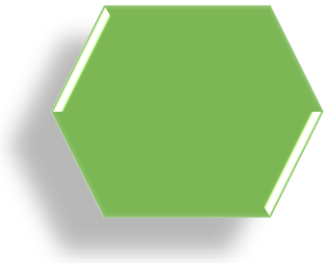
Principio 5: Conformidad

- TI cumple con todas las leyes y reglamentos obligatorios. Las políticas y las prácticas están claramente definidas, implementadas y aplicadas.



Principio 6: Comportamiento Humano

- Las políticas de TI, las prácticas y las decisiones demuestran respeto por el comportamiento humano, incluyendo las necesidades actuales y futuras de todas las personas involucradas.



Principios ISO/IEC 38500

1. Responsabilidad
2. Estrategia
3. Adquisición
4. Desempeño
5. Cumplimiento
6. Comportamiento Humano

King III

- El Informe King lidera las mejores prácticas internacionales de gobierno corporativo.
- A la fecha, el Comité de Gobierno Corporativo de Sudáfrica ha publicado tres informes: en 1994 King I, en 2002 King II, y en 2009 King III.
- El cumplimiento de los Informes King es un requisito para las empresas que cotizan en la Bolsa de Valores de Johannesburgo.
- El informe enfatiza la importancia del liderazgo y la sostenibilidad en el logro del desempeño económico, social y ambiental de las organizaciones.

Informe King III

Capítulos de King III

- Liderazgo ético y de ciudadanía corporativa
- El consejo y los directores
- Los comités de auditoría
- Gobierno de riesgos
- Gobierno de la tecnología de la información
- El cumplimiento de las leyes y normas
- Auditoría interna
- Gobierno de relaciones con los interesados
- Informes integrados y su divulgación

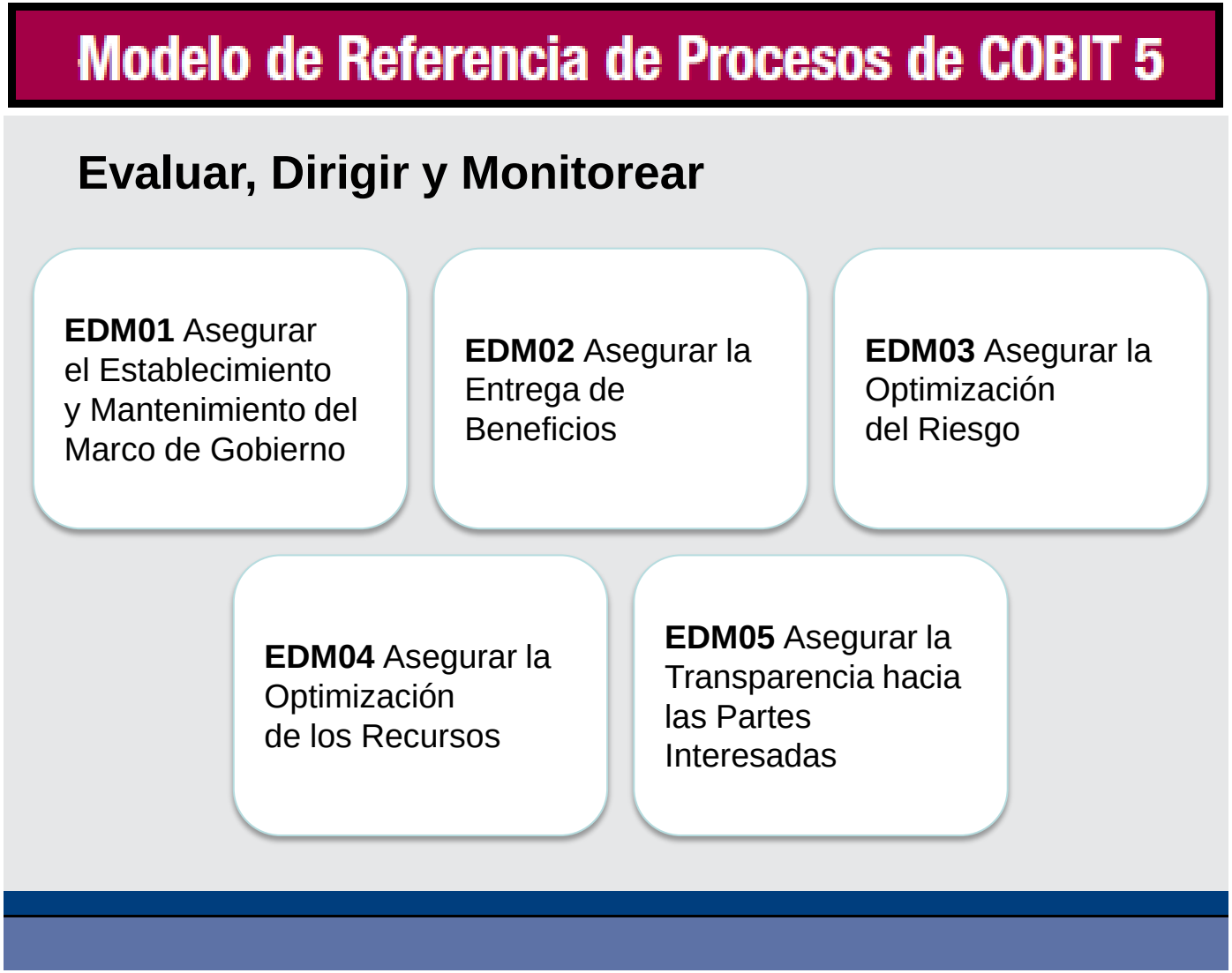
Gobierno de la tecnología de información

- Tecnología de la información se ha convertido en un elemento estratégico para crear oportunidades, innovación y ventaja competitiva, pero a su vez conlleva riesgos inherentes relacionados con la confidencialidad, integridad y disponibilidad de la información que requieren atención.

Los principios para el gobierno de la tecnología de información que plantea King III son los siguientes:

1. La junta directiva debe ser responsable del gobierno de tecnología de la información.
2. TI debe estar alineada con los objetivos de desempeño y de sostenibilidad de la empresa.
3. La junta directiva debe delegar en la gerencia la responsabilidad de la implementación de un marco de gobierno de TI.
4. La junta directiva debe supervisar y evaluar las inversiones y los gastos significativos en TI.
5. TI debe formar parte integral de la gestión de riesgos de la compañía.
6. La junta directiva debe asegurar que los activos de información se gestionen de manera eficaz.
7. Un comité de riesgos y un comité de auditoría deben ayudar a la junta directiva en el desempeño de sus responsabilidades de TI

Dominio de Gobierno



ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Planeación

Evaluación de riesgos

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

Riesgo

- Efecto de la incertidumbre en los objetivos
- Un efecto es una desviación de lo esperado - positiva o negativa.
- La incertidumbre es el estado, aunque sea parcial, de la deficiencia de información relacionada con, la comprensión o el conocimiento de un evento, su consecuencia, o probabilidad.

Riesgo

- El riesgo se caracteriza a menudo por referencia a los acontecimientos y las consecuencias potenciales, o una combinación de éstos.
- El riesgo se expresa a menudo en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la probabilidad de ocurrencia asociada.

Riesgo

- En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden ser expresado como efecto de la incertidumbre en los objetivos de seguridad de la información.

Riesgo

- El riesgo para la seguridad de información se asocia con la posibilidad de que las amenazas explotarán vulnerabilidades de un activo de información o un grupo de activos de información y por lo tanto causan daño a la organización.

Riesgo inherente

- Es el riesgo de una actividad cuando no existen controles o factores mitigantes.

Riesgo residual

- Es el riesgo que permanece después de que se han tomado en consideración los controles existentes o cualquier otro factor mitigante.

Riesgo residual

Riesgo inherente

Riesgo residual

Perfil del riesgo

- Riesgo inherente de una organización, en total, lo que representan las características de riesgo de una organización que están presentes en un momento dado.

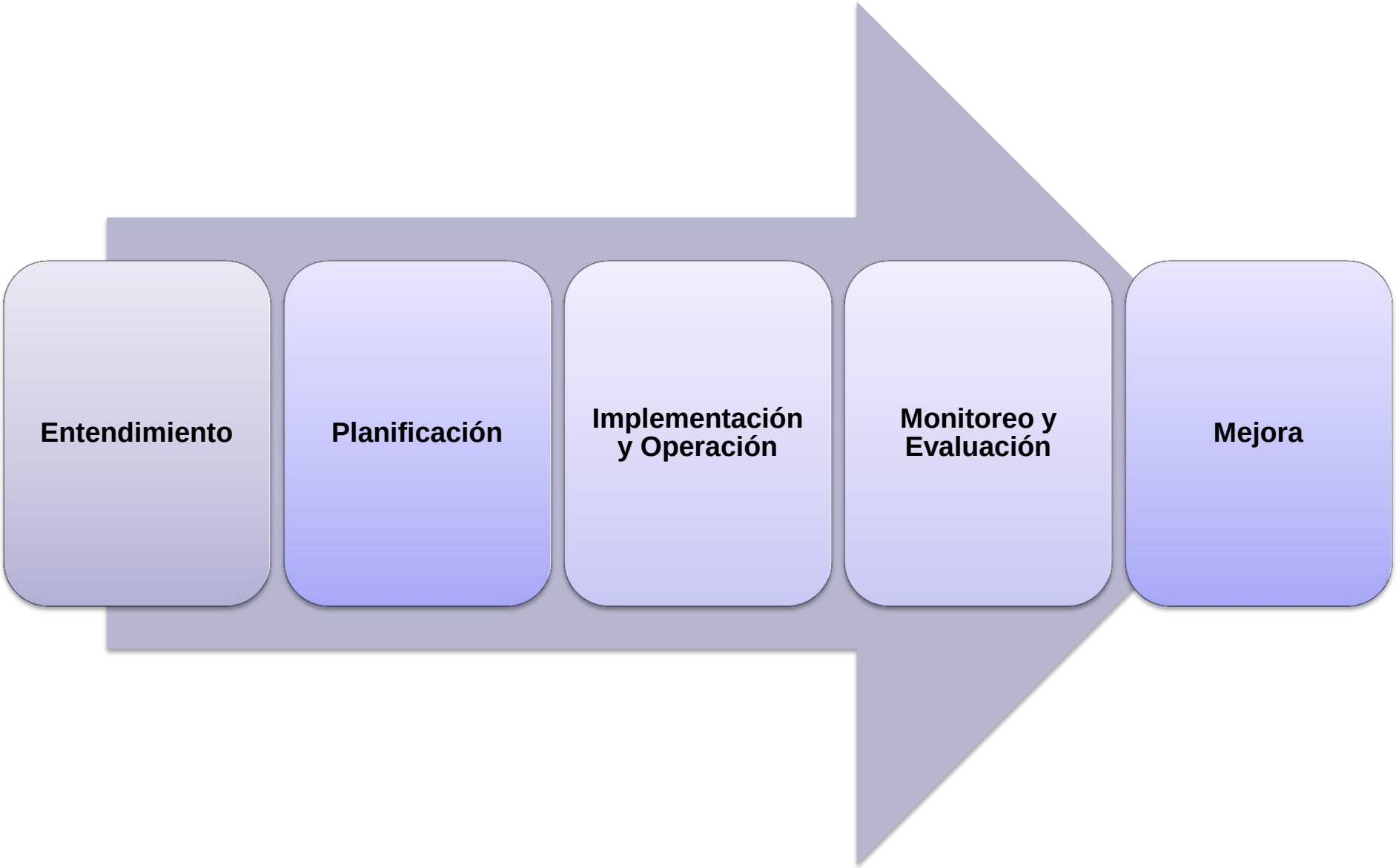
Características del riesgo

- Impacto
- Probabilidad de ocurrencia
- Velocidad
- Duración

Contenido


Introducción
Alcance
Referencias normativas
Términos y definiciones
Planear
Organización
Entendimiento de la organización y su contexto
Expectativas de las partes interesadas
Alcance del SGSI
Liderazgo
Liderazgo y compromiso de la Alta Dirección
Políticas, roles, responsabilidades y autoridades
Planeación
Acciones para atender riesgos y oportunidades
Objetivos de seguridad de la información
Soporte
Recursos, Competencias, Conciencia
Comunicación, Documentación
Hacer
Operación
Planeación y control operacional
Evaluación de riesgos de seguridad
Revisar
Evaluación de desempeño
Monitoreo, medición, análisis y evaluación
Auditoría interna y Revisión gerencial
Actuar
Mejora
No conformidad y acciones correctivas
Mejora continua

Fases


Entendimiento
Planificación
Implementación y Operación
Monitoreo y Evaluación
Mejora

Mentalidad demasiado negativa

Se crea valor únicamente evitando las consecuencias negativas

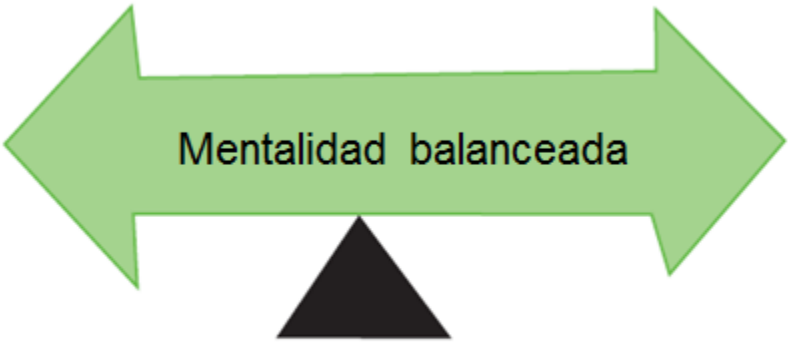
The Internal Auditor's GUIDE TO RISK ASSESSMENT

RICK A. WRIGHT JR., CIA

Mentalidad demasiado positiva

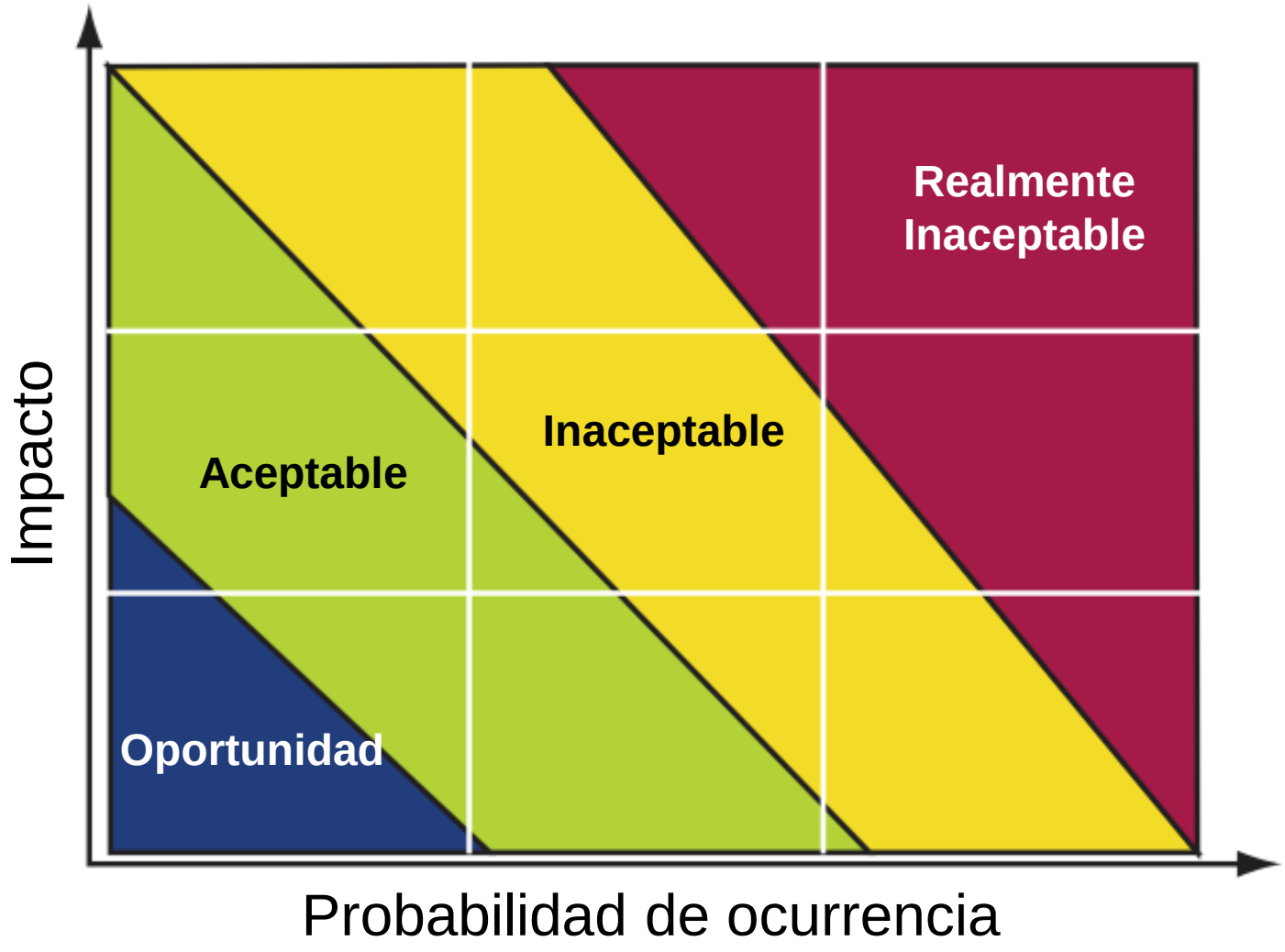
El valor se crea mediante el fomento de las consecuencias positivas, pero se erosiona por las consecuencias negativas sin respuestas apropiadas para los riesgos.

Mentalidad balanceada

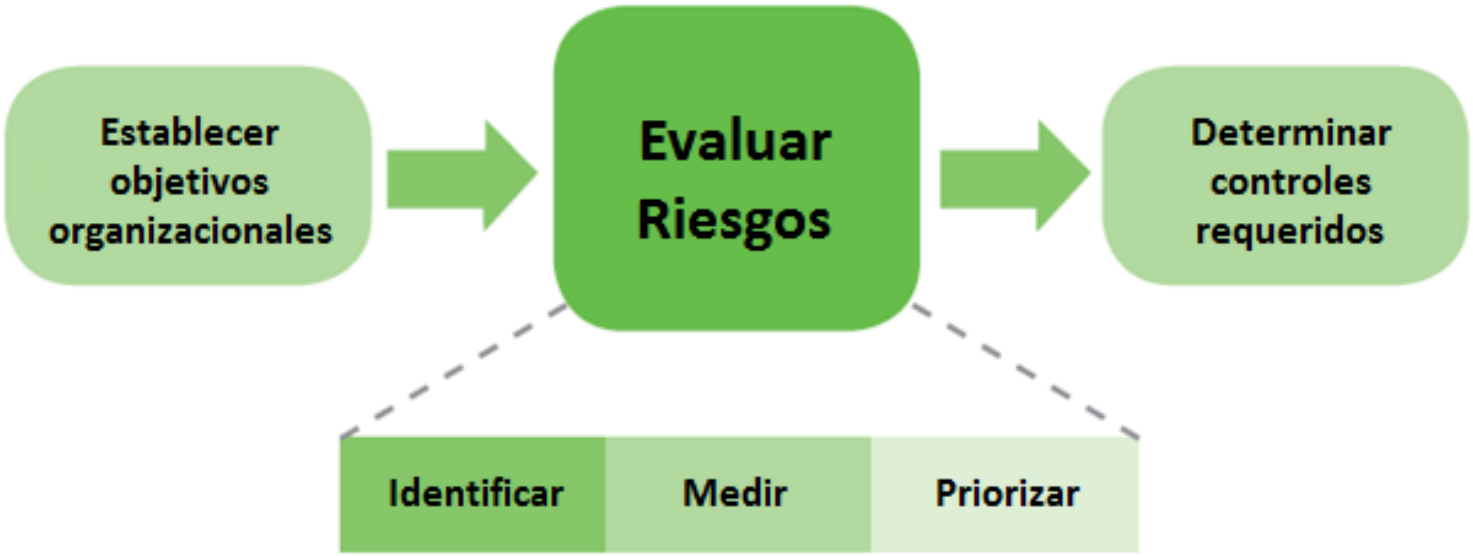


Se crea valor minimizando las consecuencias negativas a la vez que aprovechando las oportunidades

Apetito del riesgo



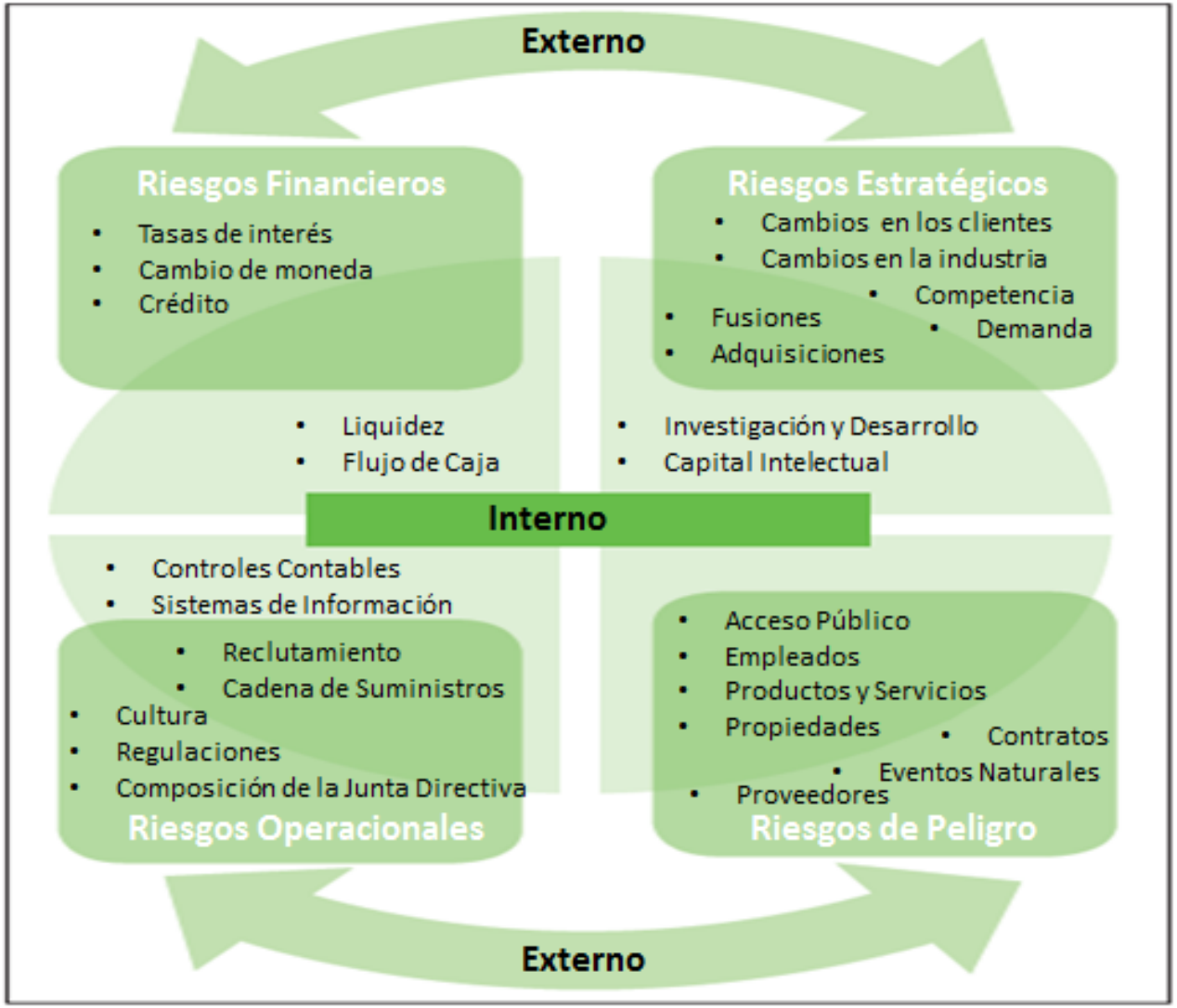
Proceso de Evaluación de Riesgos



Emitir un juicio acerca de los riesgos

- Proceso general de
  - la identificación del riesgo,
  - el análisis de riesgo y
  - la evaluación del riesgo

Identificación de riesgos



Identificación de riesgos

- Proceso de encontrar, reconocer y describir los riesgos.
- La identificación del riesgo implica la identificación de las fuentes de riesgo, eventos, sus causas y sus posibles consecuencias.
- La identificación de riesgos puede implicar datos históricos, análisis teórico, opiniones informadas y de expertos, y las necesidades de las partes interesadas.

Identificación de riesgos

- 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 la información
- Identificar a los propietarios de los riesgos;

Criterios de riesgos

- Términos de referencia con el que se evalúa la importancia del riesgo.
- Los criterios de riesgo se basan en objetivos de la organización, y el contexto externo e interno.
- Los criterios de riesgo se pueden derivar de las normas, leyes, políticas y otros requisitos.

Análisis de riesgos

- Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- El análisis de riesgos es la base para la evaluación de riesgos y las decisiones sobre el tratamiento del riesgo.
- El análisis de riesgos incluye la estimación del riesgo.

Análisis de riesgos

- Evaluar las posibles consecuencias que resultarían si los riesgos identificados fueran a materializarse
- Evaluar la probabilidad realista de la ocurrencia de los riesgos identificados
- Determinar los niveles de riesgo

Evaluación del riesgo

- Proceso de la comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable
- La evaluación del riesgo ayuda a tomar la decisión acerca del tratamiento del riesgo.

Evaluación de riesgos

- Establece y mantiene los criterios de riesgo de la información de seguridad que incluyen:
  1. Criterios de aceptación del riesgo
  2. Criterios para la realización de las evaluaciones de riesgos de seguridad de la información

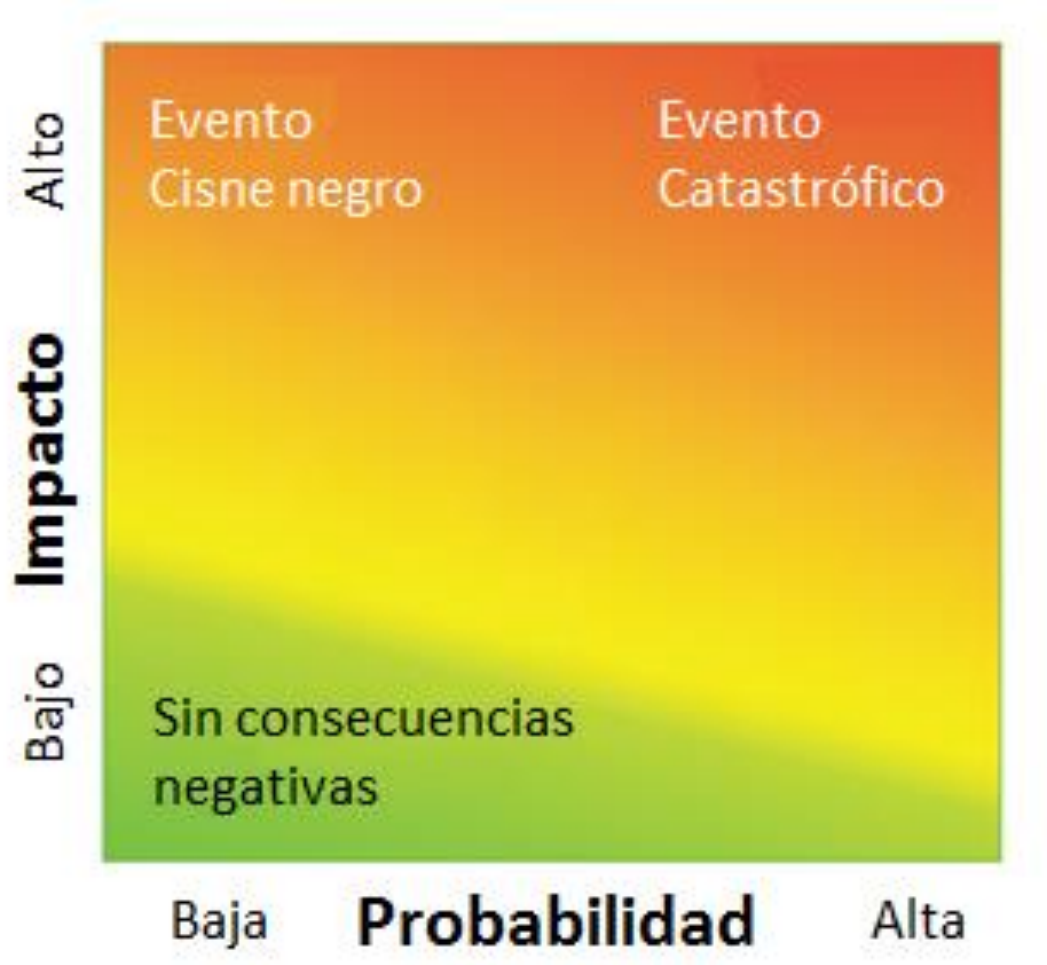
Evaluación de riesgos

- Asegurarse de que las evaluaciones de riesgos de seguridad de la información repetidas producen resultados comparables, consistentes y válidos

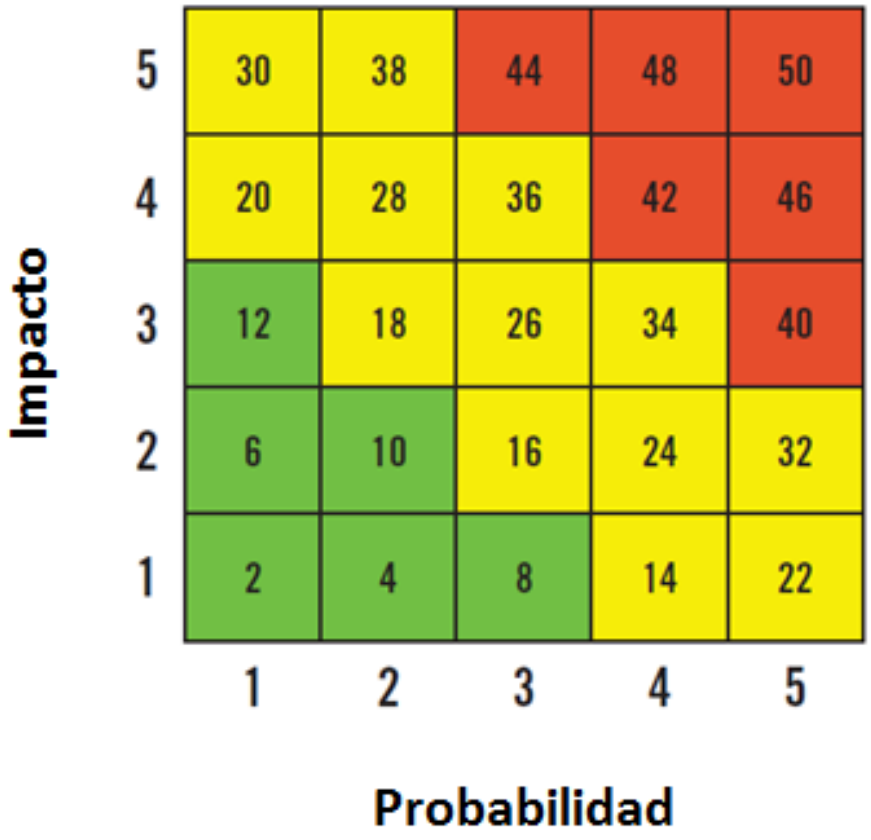
Evaluación de riesgos

- Comparar los resultados del análisis de riesgos a los criterios de riesgo establecidos
- Clasificación de los riesgos analizados para el tratamiento de riesgos
- La organización conservará información documentada acerca del proceso de evaluación de los riesgos de seguridad de información

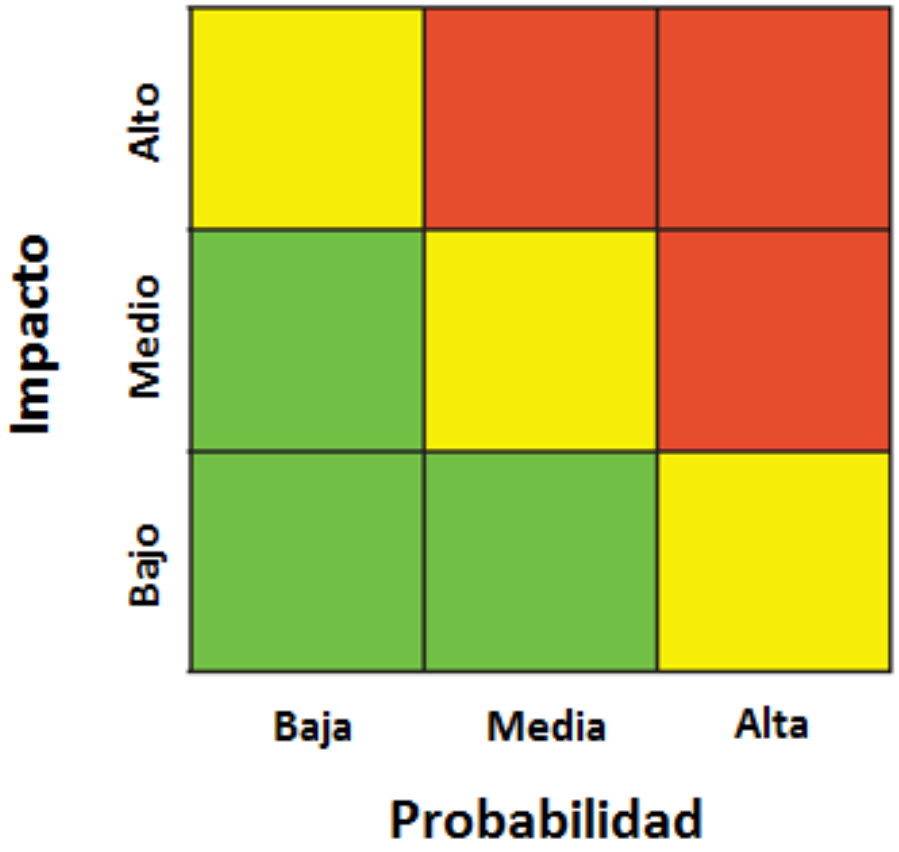
Mapa de calor de riesgos



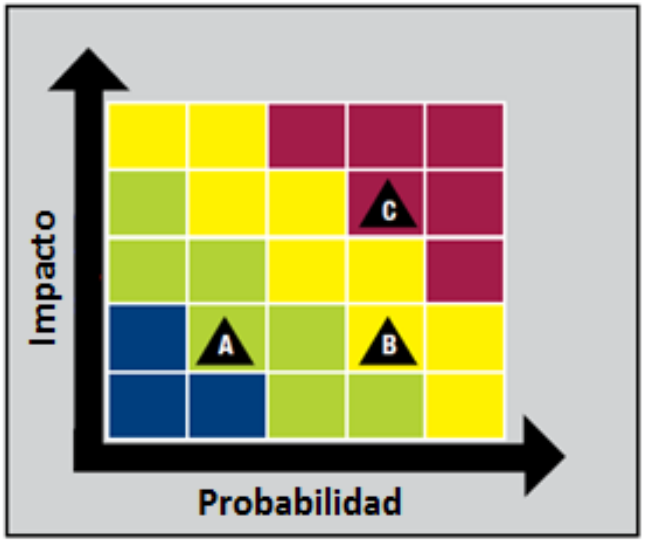
Mapa de calor de riesgos con puntuación

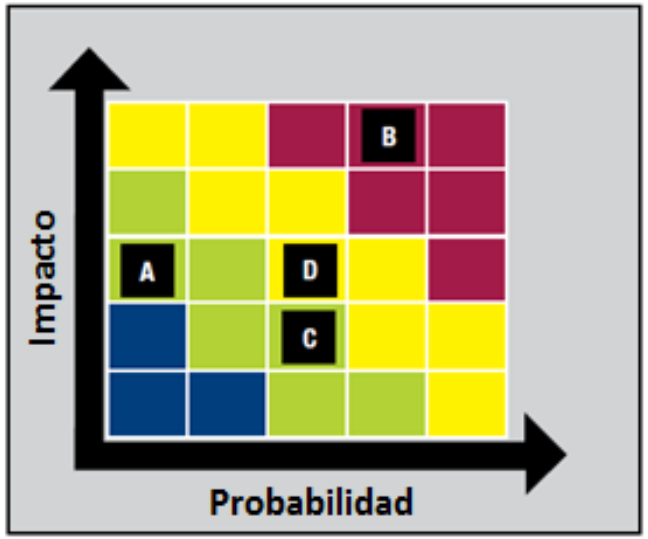


Mapa de calor de riesgos cualitativo

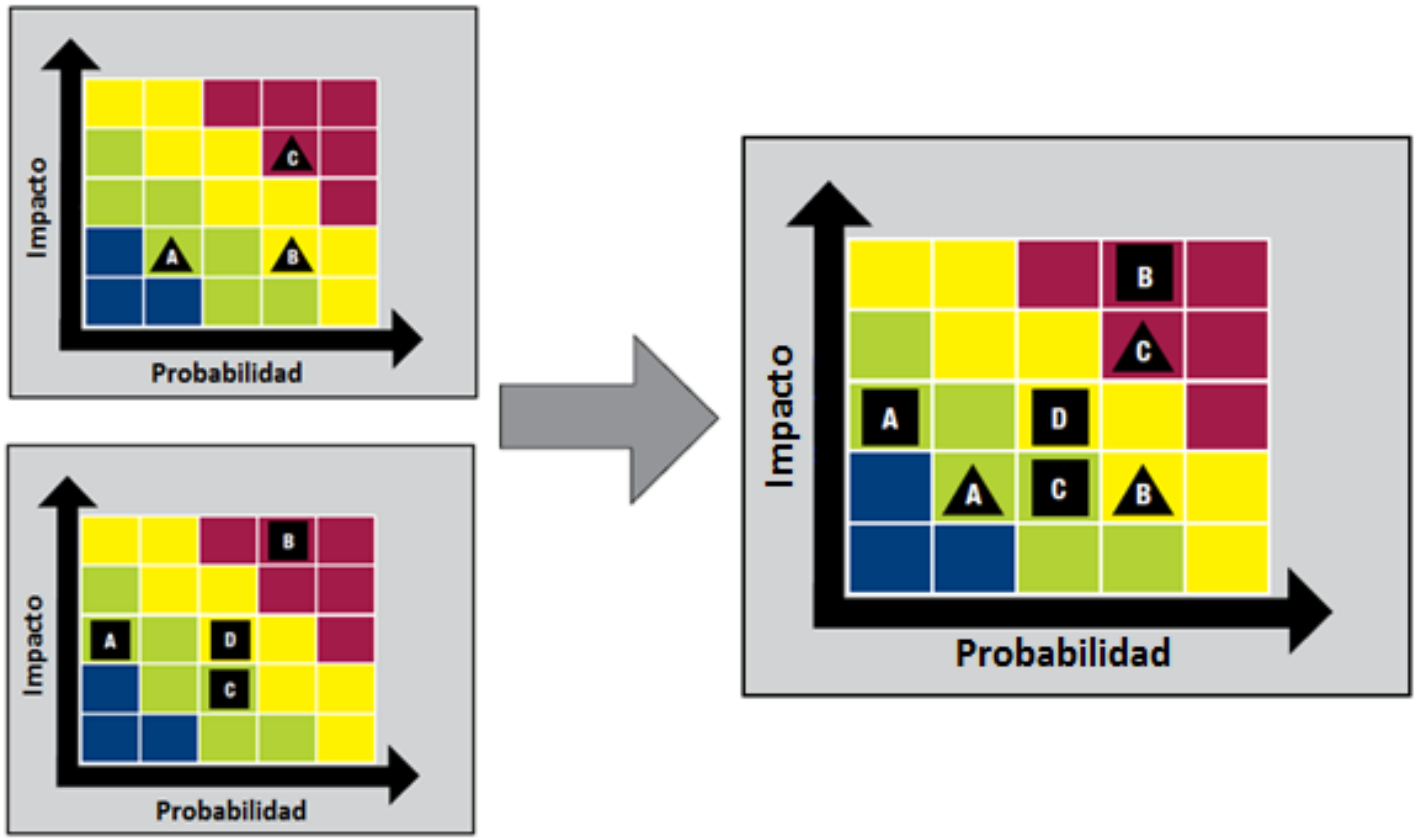


Agregación de riesgos disjuntos

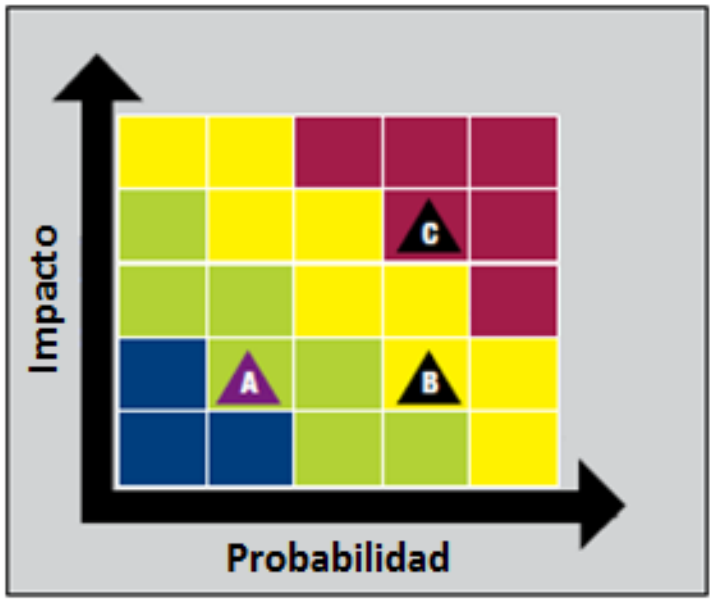


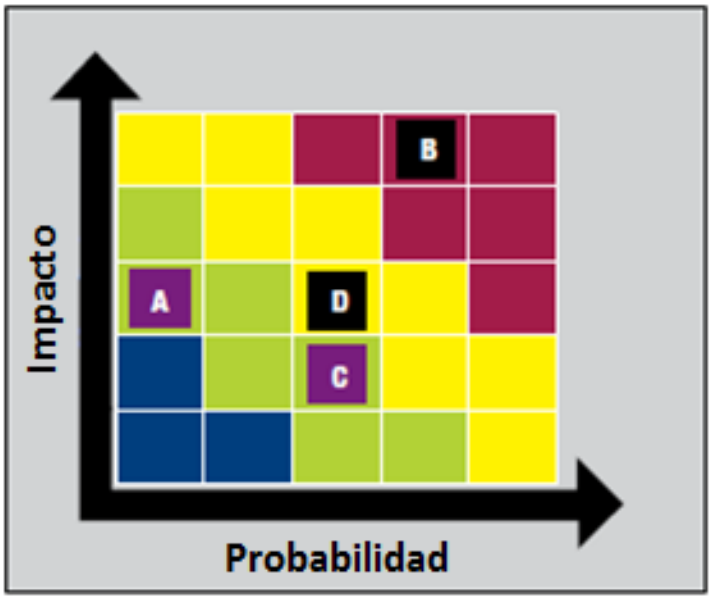


Agregación de riesgos disjuntos

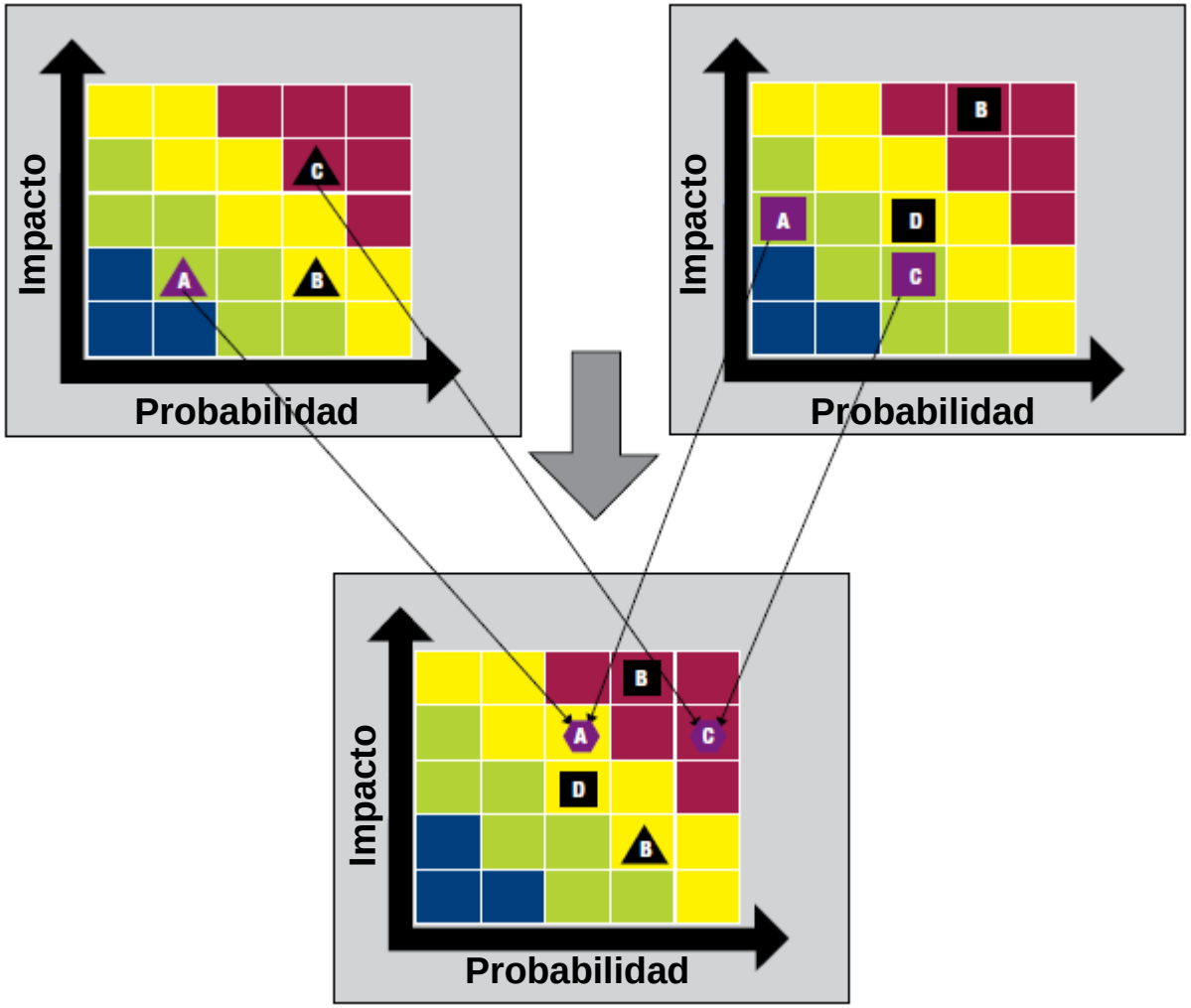


Agregación de riesgos compartidos





Agregación de riesgos compartidos



Evaluación de Riesgos

Principio COSO		Proceso COBIT	Relación con el Principio COSO
7	La organización debe identificar, analizar y evaluar sus riesgos para gestionarlos.	EDM03 APO12	COBIT 5 aborda el tema de gobierno y gestión de riesgos en su guía de procesos. Específicamente en los procesos EDM03 Asegurar la Optimización del Riesgo, y en APO12 Gestionar el Riesgo. Estos procesos incluyen las prácticas y las actividades que se requieren para gobernar y gestionar el riesgo efectivamente, incluyendo su identificación, análisis y evaluación.

Estructura de escenarios de riesgos

Tratamiento de riesgos

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

Prácticas de Gestión	Entradas		Salidas	
	De	Descripción	Descripción	A
AP013.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información. Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	AP002.04	Diferencias y cambios necesarios para alcanzar la capacidad objetivo	Plan de tratamiento de riesgos de seguridad de la información	Todo EDM Todo APO Todo BAI Todo DSS Todo MEA
	AP003.02	Descripciones de dominios de partida y definición de arquitectura	Casos de negocio de seguridad de información	AP002.05
	AP012.05	Propuestas de proyectos para reducir el riesgo		

Respuestas al riesgo

- Evitar
- Transferir o compartir
- Aceptar
- Mitigar

Tratamiento de riesgos

- Seleccionar las opciones apropiadas para el tratamiento de riesgos de seguridad de información teniendo en cuenta los resultados de la evaluación de riesgos
- Determinar todos los controles que sean necesarios para implementar la opción elegida para el tratamiento de los riesgos de seguridad de información
- Comparar los controles determinados anteriormente con los del Anexo A y comprobar que no se han omitido controles que sean necesarios

Tratamiento de riesgos

- Producir una Declaración de Aplicabilidad que contenga los controles necesarios y la justificación de las inclusiones, se estén aplicando o no, y la justificación de las exclusiones de controles del Anexo A.

Tratamiento de riesgos

- Obtener la aprobación de los dueños de los riesgos del plan de tratamiento de riesgos de seguridad de la información y la aceptación del riesgo residual.
- La organización deberá conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

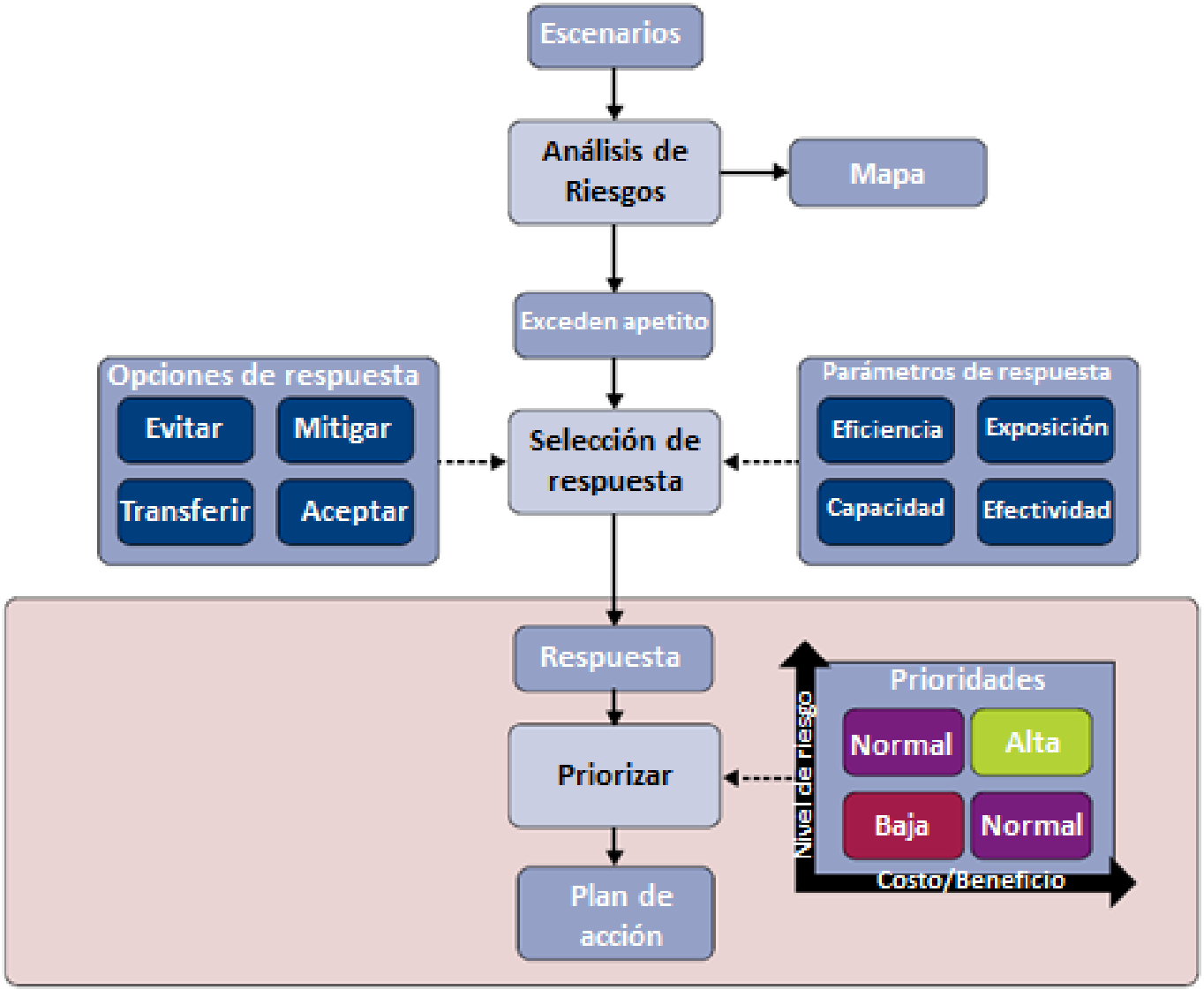
Aceptación de riesgos

- Decisión informada para tomar un riesgo en particular
- La aceptación de riesgos puede ocurrir sin tratamiento de riesgos o durante el proceso de tratamiento de riesgos.
- Los riesgos aceptados están sujetos al monitoreo y revisión.

Criterios de riesgos

- Términos de referencia con el que se evalúa la importancia del riesgo.
- Los criterios de riesgo se basan en objetivos de la organización, y el contexto externo e interno.
- Los criterios de riesgo se pueden derivar de las normas, leyes, políticas y otros requisitos. Repetido

Respuesta a los riesgos



Líneas de defensa contra los riesgos

Líneas de defensa contra los riesgos

Errores que hay que evitar

- Equiparar la complejidad con el valor
- Asignar el personal incorrecto
- Herramientas inadecuadas para recopilación de datos

Retos que hay que anticipar

- Resultados inconsistentes en la medición de riesgos
- Recursos inadecuados
- Falta de compromiso de la dirección

Ejercicio

- Defina un universo de riesgos
- Defina una tabla de criterios de aceptación de riesgos
- Identifique 5 riesgos
- Haga un análisis cualitativo para determinar el impacto y la probabilidad de ocurrencia y determine el nivel de riesgo
- Dibuje los riesgos en un diagrama de temperatura
- Compare sus resultados contra la tabla de criterio e indique si los riesgos pueden aceptarse o si requieren un tratamiento

Contenido


Introducción
Alcance
Referencias normativas
Términos y definiciones
Planear
Organización
Entendimiento de la organización y su contexto
Expectativas de las partes interesadas
Alcance del SGSI
Liderazgo
Liderazgo y compromiso de la Alta Dirección
Políticas, roles, responsabilidades y autoridades
Planeación
Acciones para atender riesgos y oportunidades
Objetivos de seguridad de la información
Soporte
Recursos, Competencias, Conciencia
Comunicación, Documentación
Hacer
Operación
Planeación y control operacional
Evaluación de riesgos de seguridad
Revisar
Evaluación de desempeño
Monitoreo, medición, análisis y evaluación
Auditoría interna y Revisión gerencial
Actuar
Mejora
No conformidad y acciones correctivas
Mejora continua

Objetivos y planificación para alcanzarlos

- Se deben definir los objetivos de seguridad de la información y la planificación para alcanzarlos

Objetivos y planificación para alcanzarlos

- La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Objetivos de seguridad de la información

Los objetivos de seguridad de la información deberán:

- Ser coherentes con la política de seguridad de la información
- Ser medibles (si esto es posible)
- Tener en cuenta los requisitos de seguridad de la información aplicable, así como los resultados de la evaluación de riesgos y el tratamiento del riesgos
- Ser comunicados
- Actualizarse según corresponda

Objetivos de seguridad de la información

- La organización conservará información documentada sobre los objetivos de seguridad de la información.

Objetivos de seguridad de la información

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

- Qué se hará
- Los recursos que serán necesarios
- Quién será responsable
- Cuándo se completará
- Cómo se evaluarán los resultados

Marco COSO de control interno

Marco COSO ERM

Objetivos empresariales

Metas Corporativas de COBIT 5				
		Relación con los Objetivos de Gobierno		
Dimensión del CMI	Meta Corporativa	Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

Cuadro de Mando Integral – CMI

- Balanced Scorecard – BSC fue presentado en el número de enero/febrero de 1992 de la revista Harvard Business Review.
- Sus autores, Robert Kaplan y David Norton, plantean que el CMI es un sistema de administración que va más allá de la perspectiva financiera con la que los gerentes acostumbran evaluar la marcha de una empresa

Cuadro de Mando Integral – CMI

Cuadro de Mando Integral – CMI

ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Soporte

Recursos

- La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

Competencia

La organización deberá:

- Determinar las competencias necesarias que afecten el desempeño relacionado con la seguridad de la información
- Asegurarse de que las personas sean competentes sobre la base de una educación adecuada, capacitación o experiencia
- En su caso, tomar las acciones para adquirir la competencia necesaria, y evaluar la eficacia de las acciones tomadas
- Retener la información documentada apropiada como evidencia de la competencia

Concientización

Se deberá concientizar acerca de:

- La política de seguridad de la información
- La contribución a la eficacia del sistema de gestión de seguridad de la información
- Los beneficios de un mejor desempeño de seguridad de información
- Las consecuencias de que no se cumpla con los requisitos del sistema de gestión de seguridad de la información

Comunicación

La organización debe determinar la necesidad de las comunicaciones internas y externas pertinentes para el sistema de gestión de seguridad de la información, lo cual incluye:

- Con que comunicarse
- Cuándo comunicarse;
- Con quién comunicarse;
- Qué se comunicará y
- Los procesos por medio de los cuales la comunicación se llevará a cabo

Comunicación

APO13 Gestionar la Seguridad	Área: Gestión Dominio: Alinear, Planificar y Organizar

Meta del Proceso	Métricas Relacionadas
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa • Número de soluciones de seguridad que se desvían del plan • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa

Información documentada

El Sistema de gestión de seguridad de la información de la organización deberá incluir:

- Información documentada requerida por ISO/IEC 27001
- Información documentada que la organización determine como necesaria para la efectividad del sistema de gestión de seguridad de la información

Información documentada

El alcance de la información documentada para un sistema de gestión de seguridad de la información puede ser diferente de una organización a otra debido a :

- El tamaño de la organización y su tipo de actividades, procesos, productos y servicios
- La complejidad de los procesos y sus interacciones
- La competencia de las personas

Creación y actualización

Al crear y actualizar la información documentada de la organización se deberá garantizar que los siguientes elementos sean apropiados:

- La identificación y descripción (por ejemplo, un título, fecha, autor, o el número de referencia)
- El formato (por ejemplo, el idioma, la versión del software, gráficos) y de los medios de comunicación (por ejemplo, papel, electrónico)
- La revisión y aprobación por la idoneidad y adecuación

Control de la información documentada

Para asegurar:

- Que está disponible y que es adecuada para su uso, donde y cuando sea necesaria
- Que esté protegida de forma adecuada (por ejemplo, de pérdida de confidencialidad, uso inadecuado, o la pérdida de la integridad).

Control de la información documentada

Para el control de la información documentada, la organización debe responder a las siguientes actividades, según sea el caso:

- La distribución, acceso, recuperación y uso
- Almacenamiento y conservación, incluyendo la preservación de la legibilidad
- El control de cambios (por ejemplo, control de versiones)
- La retención y disposición

Control de la información documentada

- La información documentada de origen externo, que la organización determine como necesaria para la planificación y operación del sistema de gestión de seguridad de la información, deberá será debidamente identificada y controlada.

- NOTA El acceso implica una decisión sobre el permiso para ver la información documentada solamente, o el permiso y la autoridad para ver y cambiar la información documentada, etc.

ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Operación

Planificación y control operacional

- La organización deberá planificar, ejecutar y controlar los procesos necesarios para cumplir con los requerimientos de seguridad de información, y para poner en práctica las acciones determinadas para responder a los riesgos y oportunidades.
- La organización deberá aplicar también los planes para alcanzar los objetivos de seguridad de la información.

Planificación y control operacional

- La organización deberá mantener información documentada en la medida que esto sea necesario para tener la confianza de que los procesos se han llevado a cabo según lo previsto.

APO13 Gestionar la Seguridad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Meta del Proceso	**Métricas Relacionadas**
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad • Número de incidentes de seguridad causados por la no observancia del plan de seguridad • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

Planificación y control operacional

- La organización deberá controlar los cambios previstos, y revisar las consecuencias de los cambios no deseados, y la adopción de medidas para mitigar los posibles efectos adversos, según sea necesario.

Planificación y control operacional

- La organización deberá asegurarse de que los procesos externalizados se determinan y controlan.

Evaluación de riesgos

- La organización deberá llevar a cabo evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se producen cambios significativos, teniendo en cuenta los criterios establecidos para la realización de evaluaciones y aceptación del riesgo.

Evaluación de riesgos

- La organización conservará la información documentada de los resultados de la evaluaciones de riesgos de seguridad de la información.

Información acerca del tratamiento de riesgos

- La organización deberá implementar el plan de tratamiento de riesgos de seguridad de la información.
- La organización deberá conservar la información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

ISO/IEC 27001:2013


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Evaluación del desempeño

Evaluación del desempeño

- La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información.

Seguimiento, medición, análisis y evaluación

La organización debe determinar:

- Lo que necesita ser monitoreado y medido, incluyendo los procesos de seguridad de la información y los controles
- Los métodos de monitoreo, medición, análisis y evaluación, para garantizar resultados válidos

Seguimiento, medición, análisis y evaluación

La organización debe determinar:

- Cuando se deberán llevar a cabo el monitoreo y la medición
- Quien deberá monitorear y hacer la medición
- Cuando deberán ser analizados y evaluados los resultados de monitoreo y medición
- Quien deberá analizar y evaluar los resultados

Seguimiento, medición, análisis y evaluación

- La organización deberá conservar información documentada apropiada como evidencia de los resultados del monitoreo y la medición.

Auditoría interna

La organización debe realizar auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

Cumple

- Las propias necesidades de la organización para su sistema de gestión de seguridad de la información
- Los requisitos de la norma internacional ISO/IEC 27001

Auditoría interna

La organización debe realizar auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

- ❑ Se ha implementado y se mantiene de manera eficaz.

Responsabilidades de la organización

- La organización debe planificar, establecer, implementar y mantener un programa de auditoría, incluida la periodicidad, los métodos, responsabilidades, requisitos de planificación y presentación de informes.
- El programa de auditoría debe tener en cuenta la importancia de los procesos y los resultados de auditorías anteriores.

Responsabilidades de la organización

- Definir los criterios de auditoría y el alcance de cada auditoría
- Seleccionar a los auditores
- Garantizar la objetividad e imparcialidad del proceso de auditoría

Responsabilidades de la organización

- Asegurarse de que los resultados de las auditorías se reportan a la gerencia pertinente
- Conservar la información documentada como prueba del programa de auditoría y de los resultados de la auditoría

Revisión de la gerencia

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

Prácticas de Gestión	Entradas		Salidas	
APO13.03 Supervisar y revisar el SGSI. Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.	**De**	**Descripción**	**Descripción**	**A**
	DSS02.02	Incidentes clasificados y priorizados y requerimientos de servicios	Informes de auditoría del SGSI	MEA02.01
			Recomendaciones para mejorar el SGSI	Interno

Revisión de la gerencia

La revisión de la gerencia deberá incluir la consideración de:

- El estado de las acciones de revisiones previas de la gerencia
- Los cambios en el contexto externo e interno que sean relevantes para el sistema de gestión de seguridad de la información

Revisión de la gerencia

La revisión de la gerencia deberá incluir la consideración de la retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en:

- Las no conformidades y acciones correctivas
- Monitoreo y medición a los resultados
- Los resultados de auditoría
- El cumplimiento de los objetivos de seguridad de la información

Revisión de la gerencia

La revisión de la gerencia deberá incluir la consideración de:

- La retroalimentación de las partes interesadas
- Los resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos
- Las oportunidades de mejora continua

Revisión de la gerencia

- Los informes de revisión de la gerencia deberán incluir las decisiones relacionadas con las oportunidades de mejora continua y las necesidades de cambios en el sistema de gestión de seguridad de la información.
- La organización conservará información documentada como evidencia de los resultados de las revisiones de la gerencia.

ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Mejora

No conformidad y acciones correctivas

Cuando se produce una no conformidad, la organización deberá:

Reaccionar a la no conformidad, y según sea el caso:

- ❑ Tomar medidas para controlarlo y corregirlo
- ❑ Hacer frente a las consecuencias

No conformidad y acciones correctivas

Cuando se produce una no conformidad, la organización deberá evaluar la necesidad de acciones para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir o producirse en otros lugares, por:

- La revisión de la no conformidad
- Determinar las causas de la no conformidad
- Determinar si existen incumplimientos similares o podrían producirse

No conformidad y acciones correctivas

Cuando se produce una no conformidad, la organización deberá:

- Poner en práctica las medidas oportunas
- Revisar la eficacia de las medidas correctivas tomadas
- Realizar cambios en el sistema de gestión de seguridad de la información, si es necesario

No conformidad y acciones correctivas

- Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

No conformidad y acciones correctivas

La organización conservará información documentada como evidencia de:

- La naturaleza de las no conformidades y de cualquier acción tomada posteriormente
- Los resultados de cualquier acción correctiva

Mejora continua

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

ISO/IEC 27001:2013

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Anexo

Seguridad de la información

Secciones


Organizacional
Lógica
Legal
Física
Políticas de seguridad
Organización de la seguridad
Gestión de activos
Continuidad del negocio
Gestión de incidentes de seguridad
Cumplimiento
Recursos humanos
Seguridad física y ambiental
Adquisición, desarrollo y mantenimiento de sistemas
Relaciones con proveedores
Control de acceso
Criptografía
Seguridad operacional
Seguridad en comunicaciones

Secciones

A.5 Políticas de seguridad de la información

A.6 Organización de seguridad de la información

A.7 Seguridad de recursos humanos

A.8 Gestión de activos

A.9 Control de acceso

A.10 Criptografía

A.11 Seguridad física y ambiental

Secciones

A.12 Seguridad de Operaciones

A.13 Seguridad en las comunicaciones

A.14 Adquisición, desarrollo y mantenimiento de sistemas

A.15 Relaciones con proveedores

A.16 Gestión de incidentes de seguridad de la Información

A.17 Seguridad de la gestión de continuidad del negocio

A.18 Cumplimiento

Documentos requeridos

Documento	Referencia
Alcance del SGSI	4.3
Política y objetivos de seguridad	5.2, 6.2
Metodología de evaluación de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3 d)
Plan de tratamiento de riesgos	6.1.3 e), 6.2
Informe de evaluación de riesgos	8.2
Definición de roles y responsabilidades de seguridad	A.7.1.2, A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos operativos para la gestión de TI	A.12.1.1

©2013 Information Security & Business Continuity Academy

Documentos requeridos

Documento	Referencia
Principios de ingeniería de sistemas seguros	A.14.2.5
Política de seguridad del proveedor	A.15.1.1
Procedimiento de gestión de incidentes	A.16.1.5
Procedimientos de contingencia	A.17.1.2
Requerimientos legales, reglamentarios y contractuales	A.18.1.1

©2013 Information Security & Business Continuity Academy

Registros requeridos

Registro	Referencia
Registros de capacitación, habilidades, experiencia y las cualificaciones	7.2
Resultados del monitoreo y medición	9.1
Programa de auditoría interna	9.2
Resultados de las auditorías internas	9.2
Resultados de la revisión efectuada por la dirección	9.3
Resultados de las acciones correctivas	10.1
Registros de actividades de usuarios, excepciones y eventos de seguridad	A.12.4.1, A.12.4.3

©2013 Information Security & Business Continuity Academy

Documentos referidos en la norma

Documento	Referencia
Procedimiento de control de documentos	7.5
Controles para la gestión de documentos	7.5
Procedimiento para la auditoría interna	9.2
Procedimiento para las acciones correctivas	10.1
Política Traiga su propio dispositivo (BYOD)	A.6.2.1
Política de dispositivo móvil y teletrabajo	A.6.2.1
Política de clasificación de información	A.8.2.1, A.8.2.2, A.8.2.3
Política de contraseñas	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
Política de eliminación y destrucción	A.8.3.2, A.11.2.7

©2013 Information Security & Business Continuity Academy

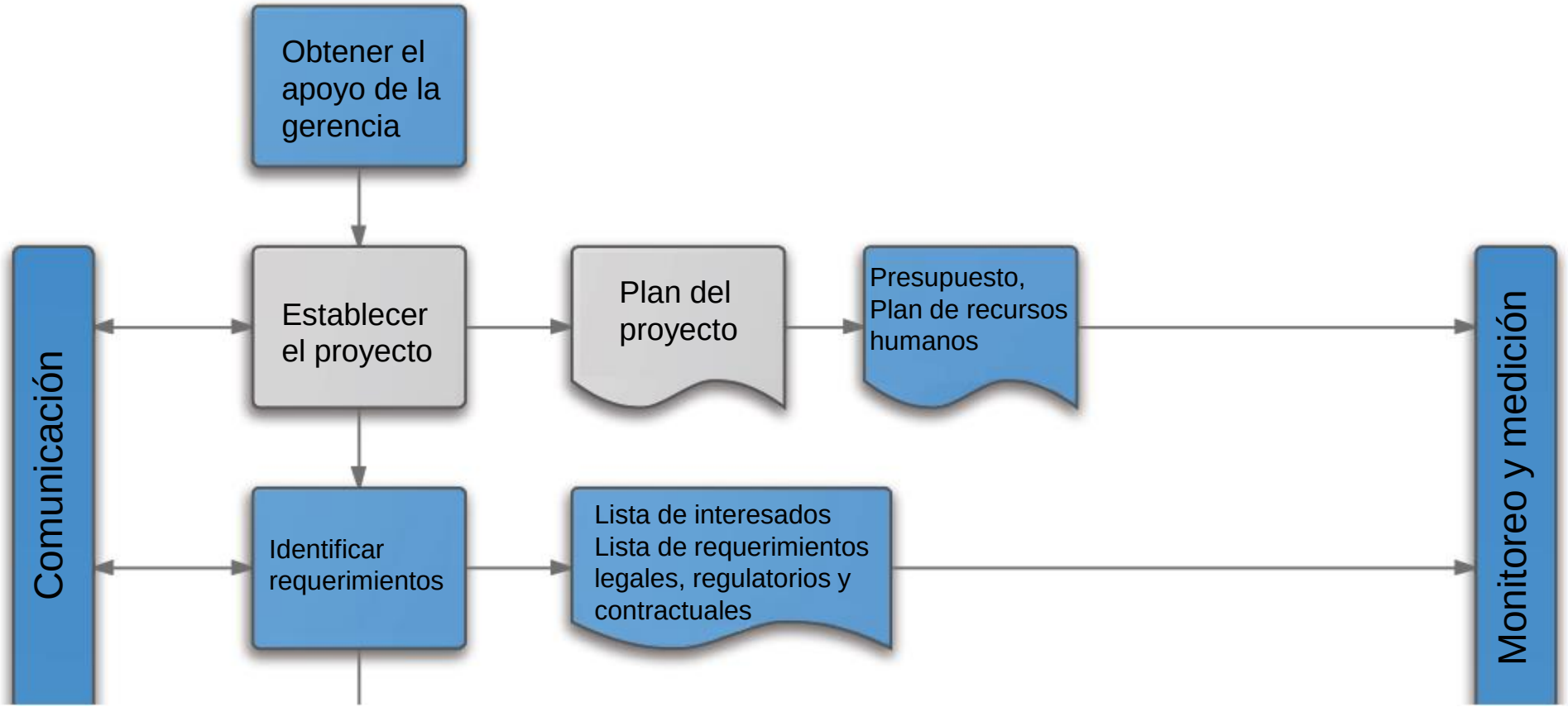
Documentos referidos en la norma

Documento	Referencia
Procedimientos de trabajo en áreas seguras	A.11.1.5
Política de escritorio y pantalla despejados	A.11.2.9
Política de gestión de cambios	A.12.1.2, A.14.2.4
Política de copias de seguridad	A.12.3.1
Política de transferencia de información	A.13.2.1, A.13.2.2, A.13.2.3
Análisis del impacto	A.17.1.1
Plan de pruebas	A.17.1.3
Plan de revisión y mantenimiento	A.17.1.3
Estrategia de continuidad del negocio	A.17.2.1

©2013 Information Security & Business Continuity Academy

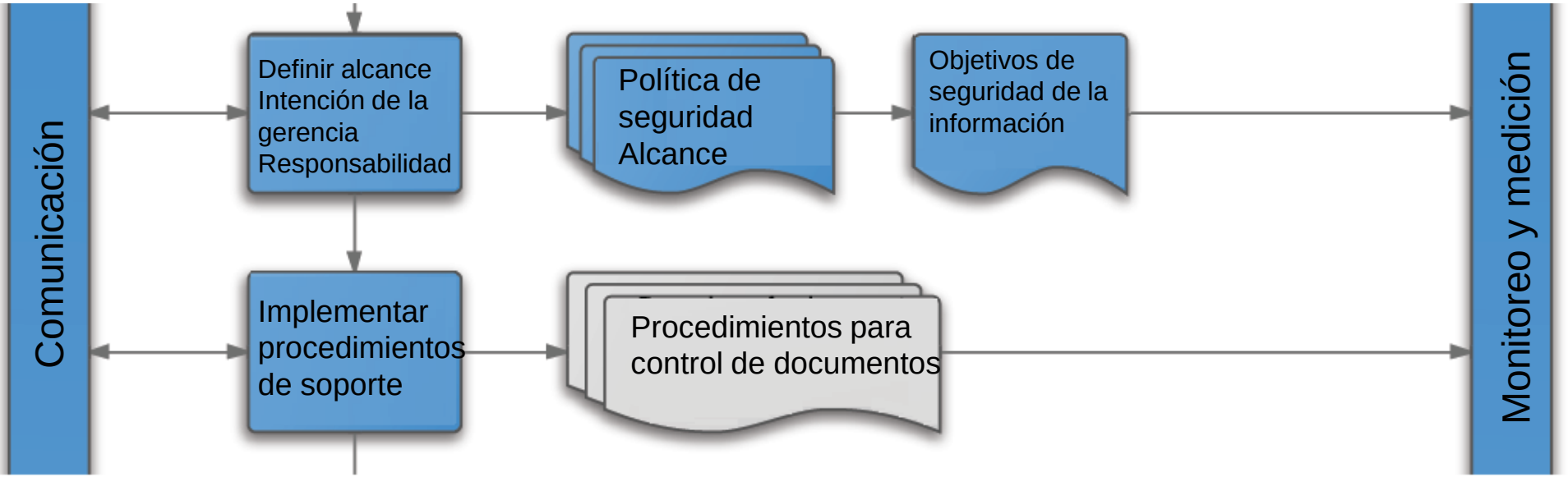
Proceso de implementación

Proceso de implementación



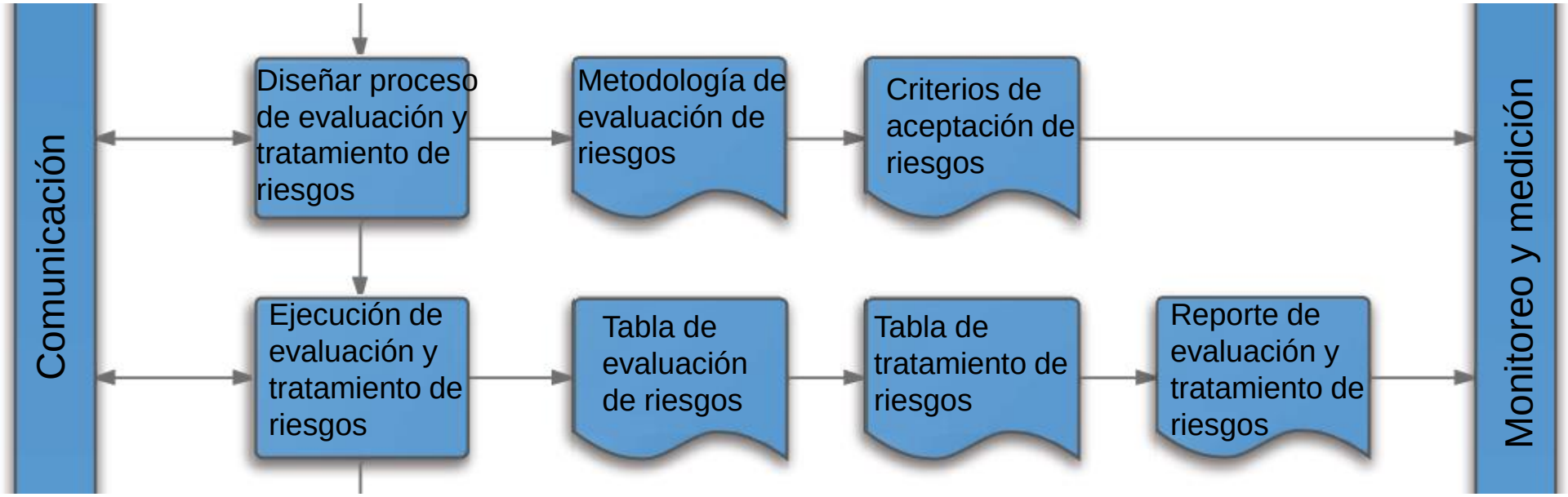
©2013 Information Security & Business Continuity Academy

Proceso de implementación



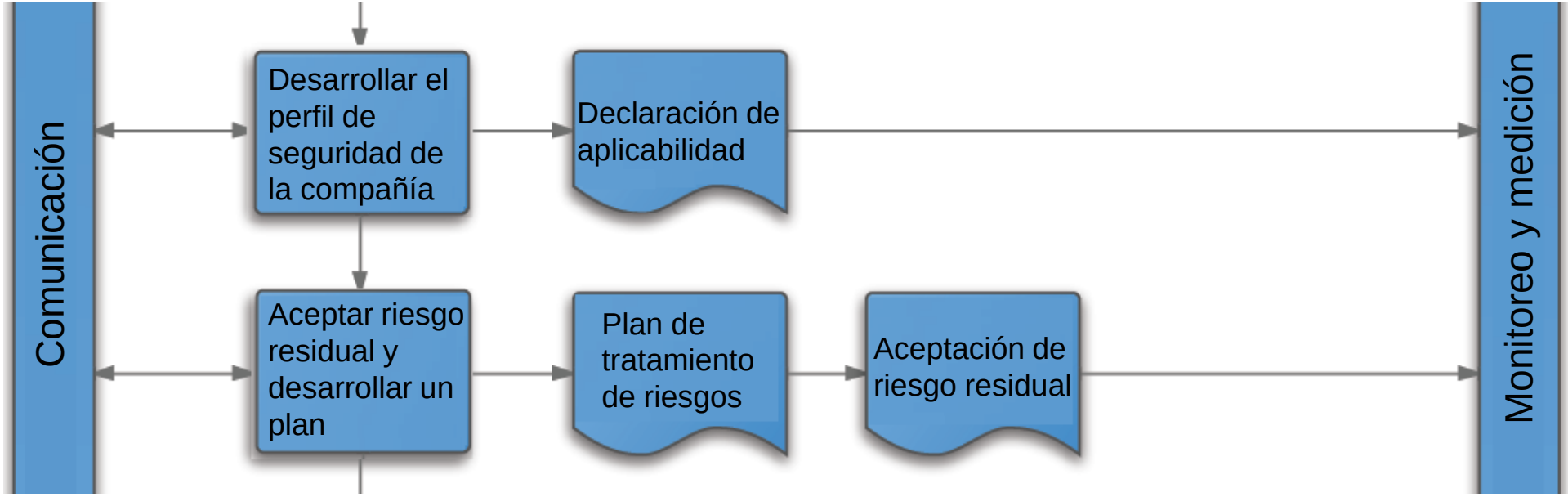
©2013 Information Security & Business Continuity Academy

Proceso de implementación



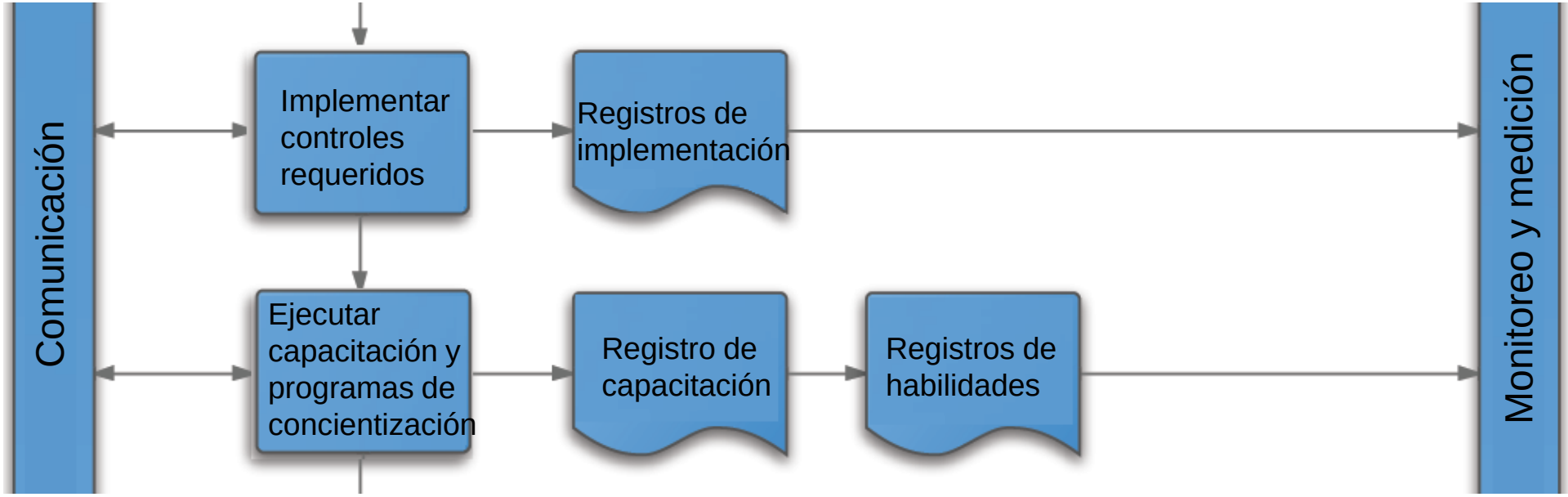
©2013 Information Security & Business Continuity Academy

Proceso de implementación



©2013 Information Security & Business Continuity Academy

Proceso de implementación

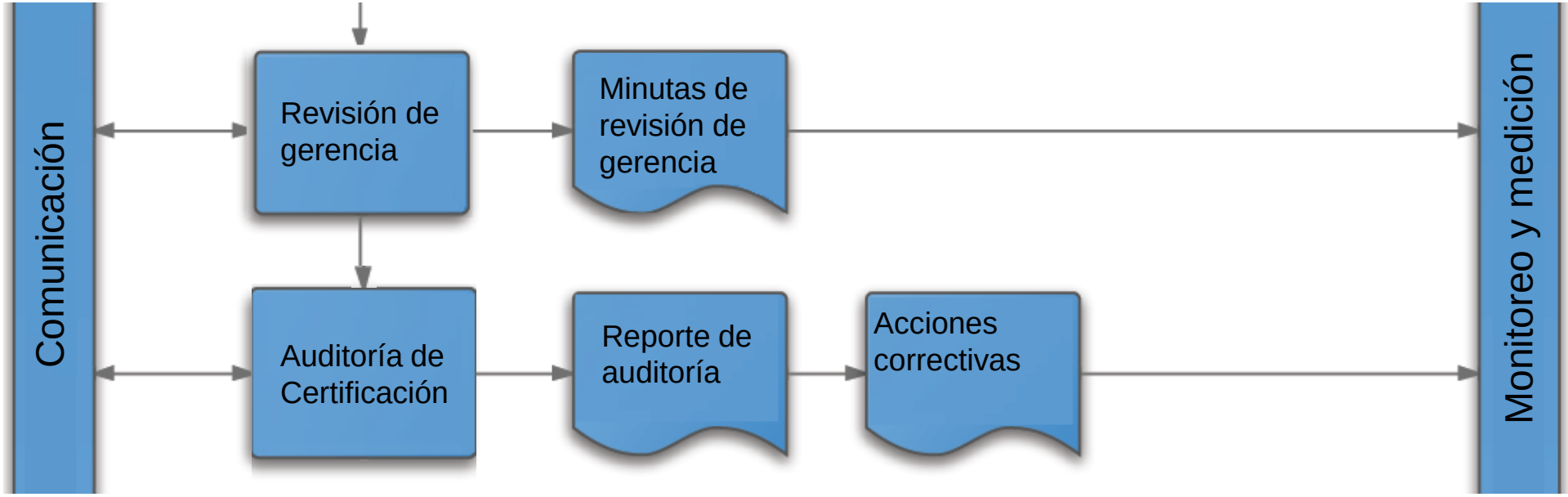


©2013 Information Security & Business Continuity Academy

Proceso de implementación

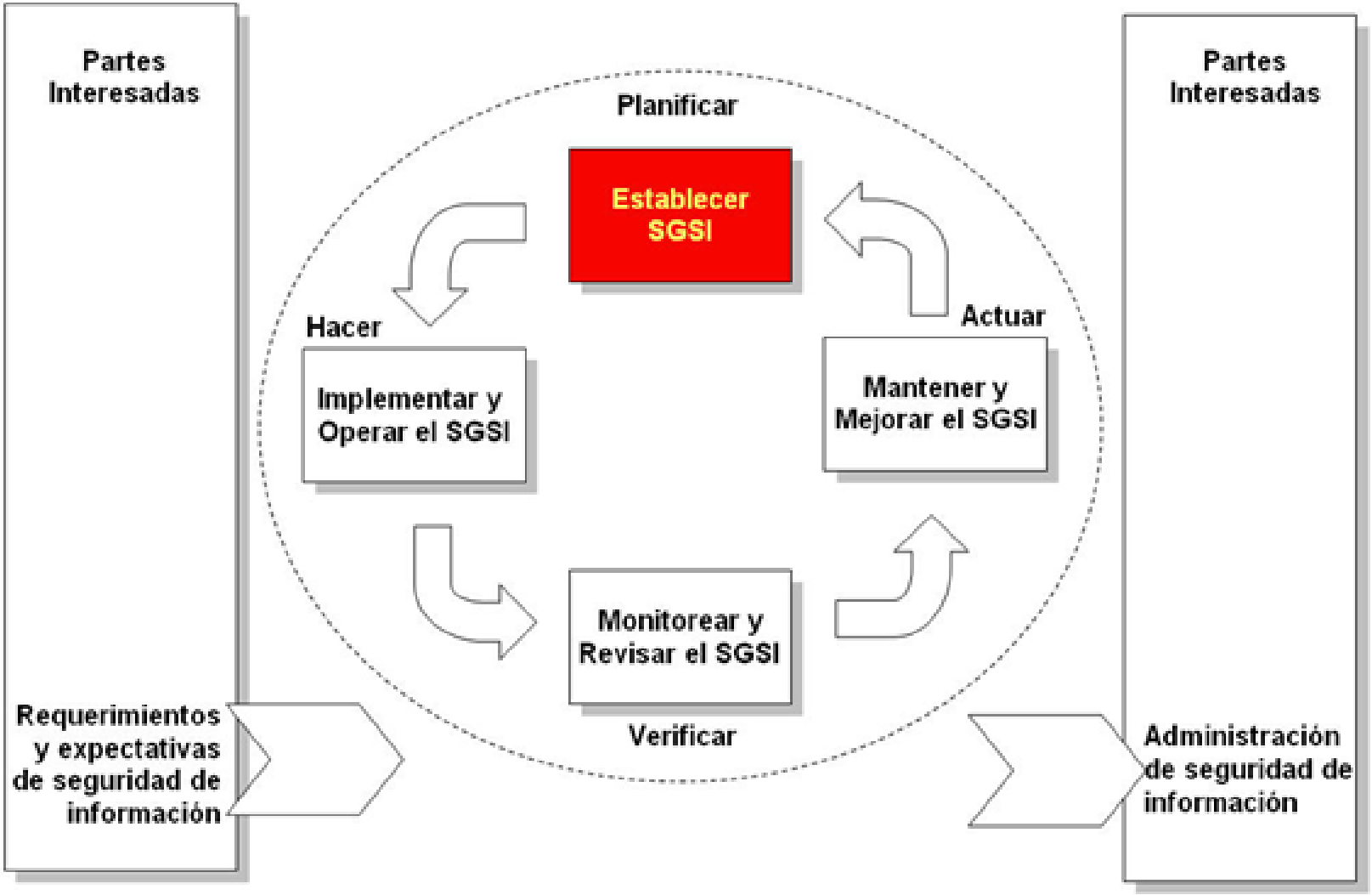
©2013 Information Security & Business Continuity Academy

Proceso de implementación



©2013 Information Security & Business Continuity Academy

Implementación



Implementación

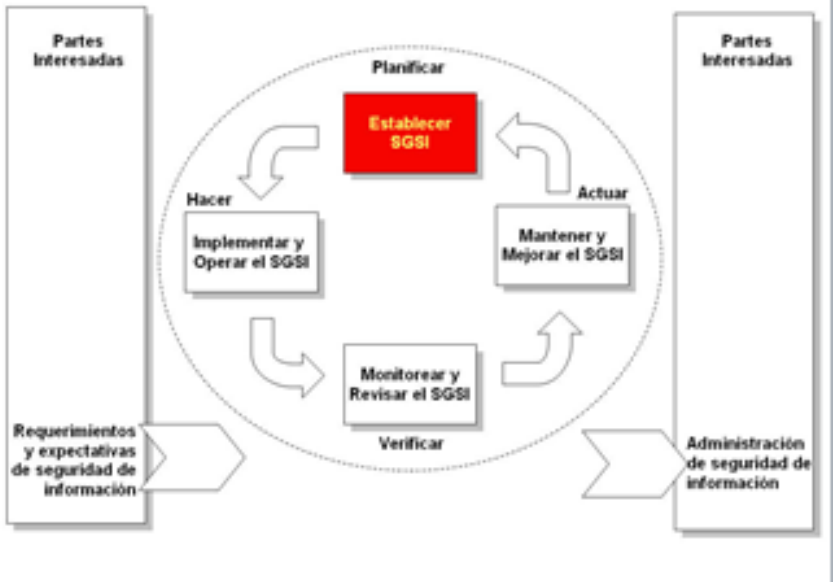
Guía Proceso "Planificar"

Estableciendo el alcance del SGSI

Formulando las políticas de SGSI y Seguridad de Información

Realizando la valoración de riesgos

Y tomando decisiones en el tratamiento de riesgos



Implementación

Guía Proceso "Hacer"

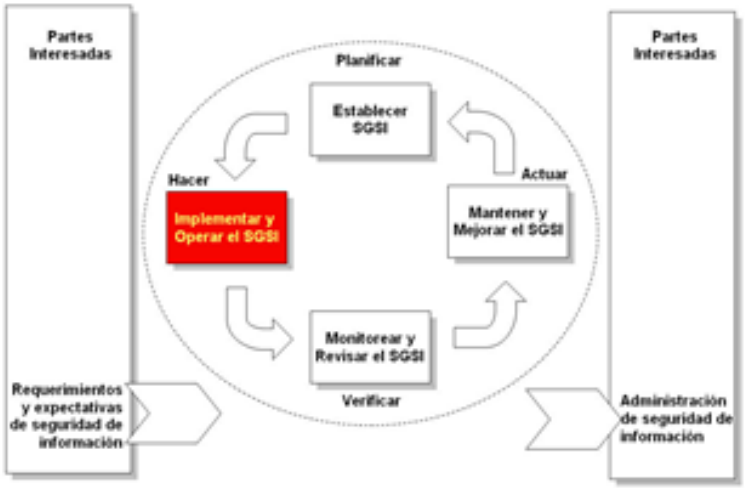
Creando e Implantando el Plan de Tratamiento de Riesgos

Implementado los controles

Capacitación y sensibilización

Implementando un programa de manejo de incidentes de seguridad de información

Administrando los recursos



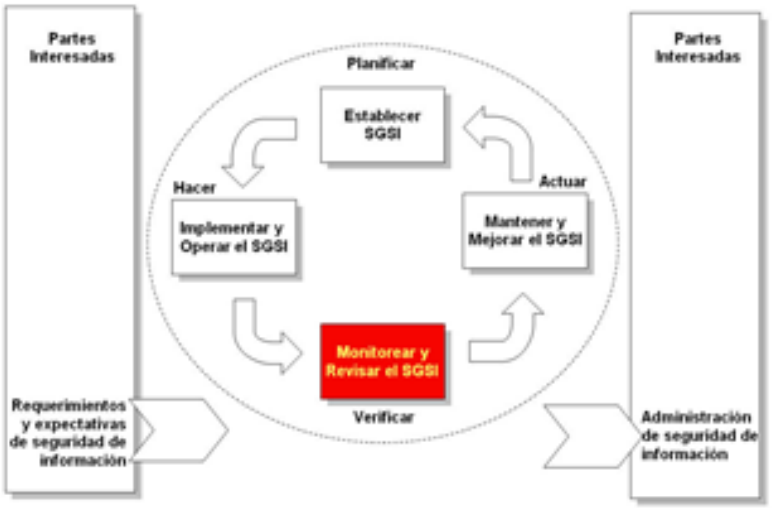
Implementación

Guía Proceso "Verificar"

Monitoreo

- *Chequeo rutinario*
- *Self-policing procedures*

Revisiones
Haciendo Auditorias internas del SGSI
Ejecutando revisiones administrativas
Midiendo el SGSI
Analizando tendencias
Controlando documentación y registros



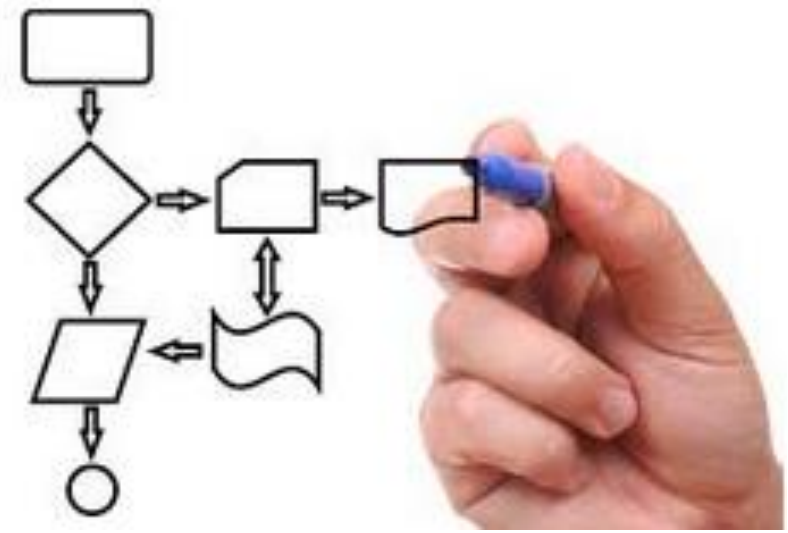
Implementación

Guía Proceso "Actuar"

Implementando mejoras
Identificando no-conformidades
Identificando e implementado acciones preventivas y correctivas
Asegurando mejora continua.
Probando
Comunicando cambios y mejoras

Ejercicio

- Con base a los ejemplos anteriores elabore un diagrama de procesos que se adapte a su organización.



Familia SGSI

Vocabulario	Requerimientos	Guías
ISO/IEC 27000:2016 Información general y vocabulario		**ISO/IEC 27002:2013** Código de buenas prácticas
	ISO/IEC 27001:2013 Requerimientos SGSI	**ISO/IEC 27003:2010** Guía de implementación
		ISO/IEC 27004:2009 Medición
		ISO/IEC 27005:2011 Gestión del riesgo de seguridad de la información

Familia SGSI

Vocabulario

ISO/IEC 27000:2016
Información general y vocabulario

Requerimientos

ISO/IEC 27001:2013
Requerimientos SGSI

ISO/IEC 27006:2015
Requisitos para los organismos que realizan la auditoría y certificación

Guías

ISO/IEC 27002:2013
Código de buenas prácticas

ISO/IEC 27003:2010
Guía de implementación

ISO/IEC 27004:2009
Medición

ISO/IEC 27005:2011
Gestión del riesgo de seguridad de la información

ISO/IEC 27007:2011
Directrices para la auditoría de SGSI

ISO/IEC TR 27008:2011
Directrices para los auditores sobre los controles de seguridad de la información

ISO/IEC 27013:2015
Orientación sobre la aplicación integrada de ISO / IEC 27001 e ISO / IEC 20000-1

ISO/IEC 27014:2013
Gobierno de seguridad de la información

ISO/IEC TR 27016:2014
Economía de las Organizaciones

Familia SGSI

Sector Específico

ISO/IEC 27010:2012
Comunicaciones inter-sectoriales e inter-institucionales

ISO/IEC TR 27015:2012
Servicios Financieros

ISO/IEC 27011:2008
Organismos de telecomunicaciones

ISO/IEC CD 27017
Servicios de Computación en la Nube

Control Específico

ISO/IEC 2703x

ISO/IEC 2704x

ISO / IEC 27000:2014

- Proporciona la visión general de los sistemas de información de gestión de la seguridad (SGSI), y los términos y las definiciones utilizadas en la familia de normas de SGSI.
- Es aplicable a todos los tipos y tamaños de organización (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).

ISO / IEC 27006:2011

- Especifica los requisitos y proporciona una guía para los organismos que realizan la auditoría y certificación de un sistema de gestión de seguridad de la información (SGSI), además de los requisitos contenidos en la norma ISO / IEC 17021 e ISO / IEC 27001.
- Está pensado principalmente para apoyar la acreditación de organismos que ofrecen la certificación del SGSI.
- Cualquier organismo que proporciona la certificación del SGSI debe demostrar competencia y fiabilidad.

ISO / IEC 27002:2013

- Proporciona directrices para la gestión de seguridad de la información, incluida la selección, implementación y gestión de los controles, considerando los riesgos de la organización.
- Está diseñado para ser utilizado por las organizaciones que pretenden:
  - seleccionar los controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO / IEC 27001;
  - implementar controles de seguridad de la información generalmente aceptados;
  - desarrollar sus propias directrices de gestión de seguridad de información.

ISO / IEC 27003:2010

- Se centra en los aspectos críticos necesarios para el éxito del diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO / IEC 27001:2005.

ISO/IEC 27004:2009

- Proporciona orientación sobre el desarrollo y uso de las métricas con el fin de evaluar la eficacia de un sistema de gestión de la seguridad información (SGSI) y de los controles o grupos de controles, como se especifica en la norma ISO / IEC 27001.

ISO / IEC 27005:2011

- Proporciona directrices para la gestión de riesgos de seguridad de la información.
- Es compatible con los conceptos generales especificados en la norma ISO / IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO / IEC 27007:2011

- Proporciona orientación en la realización de las auditorías, y en la competencia de los auditores, además de las directrices contenidas en la norma ISO 19011.
- ISO / IEC 27007:2011 es aplicable a aquellos que necesitan comprender o realizar auditorías internas o externas de un SGSI o para gestionar un programa de auditoría SGSI.

ISO / IEC TR 27008:2011

- Proporciona orientación sobre la revisión de la implementación y operación de los controles, incluyendo la comprobación del cumplimiento técnico de los controles del sistema de información, de conformidad con las normas establecidas de seguridad de información de una organización.

ISO / IEC 27013:2012

- Proporciona directrices sobre la aplicación integrada de ISO / IEC 27001 e ISO / IEC 20000-1 para las organizaciones que tienen la intención de la aplicación integrada de ISO / IEC 27001 e ISO / IEC 20000-1.

ISO / IEC 27014:2013

- Proporciona orientación sobre los conceptos y principios para la gobernanza de la seguridad de la información, mediante el cual las organizaciones pueden evaluar, dirigir, controlar y comunicar las actividades relacionadas con la seguridad de la información dentro de la organización.

ISO / IEC TR 27016:2014

- Proporciona directrices sobre cómo una organización puede tomar decisiones para proteger la información y entender las consecuencias económicas de estas decisiones en el contexto de las necesidades que compiten por los recursos.

ISO / IEC 27010:2012

- Proporciona controles y orientaciones relativas específicamente a iniciar, implementar, mantener y mejorar la seguridad de la información en las comunicaciones inter-institucionales e inter-sectoriales.
- Es aplicable a todas las formas de intercambio y difusión de información sensible, tanto públicas como privadas, nacionales e internacionales, dentro de la misma industria o sector del mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y el intercambio en relación con el suministro, el mantenimiento y la protección de la infraestructura crítica de una organización o del Estado.

ISO/IEC 27011:2008

- Provee directrices que fomenten la aplicación de la gestión de seguridad de la información en las organizaciones de telecomunicaciones.
- La adopción de esta norma permitirá a las organizaciones de telecomunicaciones satisfacer las necesidades básicas para la gestión de seguridad de la información.

ISO / IEC TR 27015:2012

- Proporciona información complementaria al ISO / IEC 27002:2005 para iniciar, implementar, mantener y mejorar la seguridad de la información en organizaciones que prestan servicios financieros.

ISO/IEC 27001

Sistema de Gestión
de Seguridad de la Información

Juan Carlos Morales, CISA, CISM, CRISC, CGEIT

ISO/IEC 27001:2013

Controles y Objetivos de Control

Juan Carlos Morales, CISA, CISM, CRISC, CGEIT

Seguridad de la información

INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Actualización 2013

Seguridad de la información

Nuevos controles

A.6.1.5 Seguridad de la información en gestión de proyectos

A.14.2.1 Política de desarrollo seguro

A.14.2.5 Principios de ingeniería de sistemas seguros

A.14.2.6 Ambiente de desarrollo seguro

A.14.2.8 Pruebas de seguridad del sistema

A.16.1.4 Evaluación y decisión en los eventos de seguridad de la información

A.17.2.1 Disponibilidad de instalaciones para el procesamiento de la información

Secciones

A.5 Políticas de seguridad de la información

A.6 Organización de seguridad de la información

A.7 Seguridad de recursos humanos

A.8 Gestión de activos

A.9 Control de acceso

A.10 Criptografía

A.11 Seguridad física y ambiental

Secciones

A.12 Seguridad de Operaciones

A.13 Seguridad en las comunicaciones

A.14 Adquisición, desarrollo y mantenimiento de sistemas

A.15 Relaciones con proveedores

A.16 Gestión de incidentes de seguridad de la Información

A.17 Seguridad de la gestión de continuidad del negocio

A.18 Cumplimiento

COBIT 5

DSS05 Gestionar Servicios de Seguridad	Área: Gestión Dominio: Entrega, Servicio y Soporte
Descripción del Proceso Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	
Declaración del Propósito del Proceso Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.	

Seguridad de la información

Sección A.5
Políticas de seguridad de la información

Objetivo de Control A.5.1
Dirección de la gestión de seguridad de la información

A.5.1.1
Políticas de seguridad de la información

A.5.1.2
Revisión de las políticas de seguridad de la información

Ejercicio

- A continuación se presentan las secciones, objetivos de control y controles contenidos en el anexo A de la norma ISO/IEC 27001:2013. Para cada uno de ellos usted deberá determinar si aplica o no a su organización, lo cual le servirá como base para su declaración de aplicabilidad (SOA).

Controles y Objetivos de Control

Sección

- A.5 Políticas de seguridad de la información

Objetivo de Control

- A.5.1 Dirección de gestión de seguridad de la información

Descripción del Objetivo de Control

- Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y reglamentos pertinentes.

Controles y Objetivos de Control

Control

- A.5.1.1 Políticas de seguridad de la información

Descripción del Control

- Se definirá un conjunto de políticas de seguridad de la información, aprobado por la gerencia, publicado y comunicado a los empleados y partes externas relevantes.

Controles y Objetivos de Control

Control

- A.5.1.2 Revisión de las políticas de seguridad de la información

Descripción del Control

- Las políticas de seguridad de la información, deberán revisarse periódicamente de acuerdo a un plan, o en caso se produzcan cambios significativos para asegurar su continua idoneidad, adecuación y eficacia.

Controles y Objetivos de Control

Sección

- A.6 Organización de seguridad de la información

Objetivo de Control

- A.6.1 Organización interna

Descripción del Objetivo de Control

- Establecer un marco de gestión para iniciar y controlar la aplicación y el funcionamiento de seguridad de la información dentro de la organización.

Controles y Objetivos de Control

Control

- A.6.1.1 Roles y responsabilidades de seguridad de la información

Descripción del Control

- Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.

Controles y Objetivos de Control

Control

- A.6.1.2 Segregación de funciones

Descripción del Control

- Las funciones en conflicto y las áreas de responsabilidad deben estar separadas para reducir las oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.

Controles y Objetivos de Control

Control

- A.6.1.3 Contacto con las autoridades

Descripción del Control

- Se mantendrán los contactos apropiados con las autoridades pertinentes.

Controles y Objetivos de Control

Control

- A.6.1.4 Contacto con grupos de interés especial

Descripción del Control

- Se deberá mantener un contacto apropiado con grupos de interés especial o con foros de seguridad y asociaciones profesionales.

Controles y Objetivos de Control

Control

- A.6.1.5 Seguridad de la información en gestión de proyectos

Descripción del Control

- La seguridad de la información deberá ser atendida al gestionar proyectos, independientemente del tipo del proyecto.

Controles y Objetivos de Control

Sección

- A.6 Organización de seguridad de la información

Objetivo de Control

- A.6.2 Dispositivos móviles y el teletrabajo

Descripción del Objetivo de Control

- Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

Controles y Objetivos de Control

Control

- A.6.2.1 Política de dispositivo móvil

Descripción del Control

- Se deberá adoptar una política y apoyo a las medidas de seguridad necesarias para gestionar los riesgos derivados del uso de dispositivos móviles.

Controles y Objetivos de Control

Control

- A.6.2.2 Teletrabajo

Descripción del Control

- Se deberá implementar una política y apoyo a las medidas de seguridad para proteger la información accedida, procesada o almacenada en sitios de teletrabajo.

Controles y Objetivos de Control

Sección

- A.7 Seguridad de recursos humanos

Objetivo de Control

- A.7.1 Antes de empleo

Descripción del Objetivo de Control

- Asegurar que los empleados y contratistas entiendan sus responsabilidades y que las mismas sean adecuadas para las funciones a las que hayan sido considerados.

Controles y Objetivos de Control

Control

- A.7.1.1 Verificación de candidatos

Descripción del Control

- Los controles de verificación de antecedentes de todos los candidatos a empleo, se deberán llevar a cabo de conformidad con las leyes, regulaciones, y la ética y deberán ser proporcionales a los requerimientos del negocio, a la clasificación de la información que se accederá y al riesgo percibido.

Controles y Objetivos de Control

Control

- A.7.1.2 Términos y condiciones

Descripción del Control

- Los acuerdos contractuales con los empleados y los contratistas deberán establecer sus responsabilidades respecto a seguridad de la información y las responsabilidades de la organización.

Controles y Objetivos de Control

Sección

- A.7 Seguridad de recursos humanos

Objetivo de Control

- A.7.2 Durante el empleo

Descripción del Objetivo de Control

- Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades de seguridad de la información.

Controles y Objetivos de Control

Control

- A.7.2.1 Responsabilidades de la gerencia

Descripción del Control

- La gerencia deberá requerir a todos los empleados y contratistas, aplicar la seguridad de la información de acuerdo con las políticas establecidas y procedimientos de la organización.

Controles y Objetivos de Control

Control

- A.7.2.2 Concientización, educación y formación acerca de Seguridad de la Información

Descripción del Control

- Todos los empleados de la organización y, cuando sea pertinente, los contratistas deberán ser concientizados y recibir educación y formación adecuada, y actualizaciones regulares acerca de las políticas y procedimientos de la organización que sean relevantes para su función de trabajo.

Controles y Objetivos de Control

Control

- A.7.2.3 Proceso disciplinario

Descripción del Control

- Deberá existir un proceso disciplinario formal y comunicado para tomar acciones en contra de aquellos empleados que hayan cometido una violación a la seguridad de la información.

Controles y Objetivos de Control

Sección

- A.7 Seguridad de recursos humanos

Objetivo de Control

- A.7.3 Terminación y cambio de empleo

Descripción del Objetivo de Control

- Se deberán proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

Controles y Objetivos de Control

Control

- A.7.3.1 Terminación o cambio de las responsabilidades laborales

Descripción del Control

- Las responsabilidades de seguridad de la Información y los deberes que siguen vigentes después de la terminación o cambio de empleo, deberán ser definidos y comunicados al empleado o contratista y asegurar su cumplimiento.

Controles y Objetivos de Control

Sección

- A.8 Gestión de activos

Objetivo de Control

- A.8.1 Responsabilidad de los activos

Descripción del Objetivo de Control

- Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

Controles y Objetivos de Control

Control

- A.8.1.1 Inventario de activos

Descripción del Control

- Los activos relacionados con la información y las instalaciones para su procesamiento deberán ser identificados e inventariados. El inventario debe mantenerse actualizado.

Controles y Objetivos de Control

Control

- A.8.1.2 Propiedad de los activos

Descripción del Control

- Todos los activos del inventario deben tener asignado un propietario.

Controles y Objetivos de Control

Control

- A.8.1.3 Uso aceptable de bienes

Descripción del Control

- Las normas para el uso aceptable de la información, de los activos asociados con la información y las instalaciones para su procesamiento, deberán ser identificadas, documentadas e implementadas.

Controles y Objetivos de Control

Control

- A.8.1.4 Retorno de los activos

Descripción del Control

- Todos los empleados y usuarios externos deberán devolver todos los activos de la organización en su poder al término de su empleo, contrato o acuerdo.

Controles y Objetivos de Control

Sección

- A.8 Gestión de activos

Objetivo de Control

- A.8.2 Clasificación de la información

Descripción del Objetivo de Control

- Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

Controles y Objetivos de Control

Control

- A.8.2.1 Clasificación de la información

Descripción del Control

- La información se clasificará en función de los requisitos legales, valor, criticidad y sensibilidad a la divulgación no autorizada o modificación.

Controles y Objetivos de Control

Control

- A.8.2.2 Etiquetado de la información

Descripción del Control

- Se deberá desarrollar e implementar un conjunto de procedimientos apropiados para el etiquetado de información, de acuerdo con el sistema de clasificación de la información adoptado por la organización.

Controles y Objetivos de Control

Control

- A.8.2.3 Manejo de activos

Descripción del Control

- Se deberán desarrollar e implementar procedimientos para el manejo de los activos, de acuerdo con el esquema de clasificación de la información adoptado por la organización.

Controles y Objetivos de Control

Sección

- A.8 Gestión de activos

Objetivo de Control

- A.8.3 Manejo de Medios

Descripción del Objetivo de Control

- Evitar la divulgación no autorizada, modificación, eliminación o destrucción de información contenida en los medios de almacenamiento.

Controles y Objetivos de Control

Control

- A.8.3.1 Gestión de medios de almacenamiento removibles.

Descripción del Control

- Se deberán desarrollar e implementar procedimientos para la gestión de medios de almacenamiento removibles, de conformidad con el sistema de clasificación adoptado por la organización.

Controles y Objetivos de Control

Control

- A.8.3.2 Eliminación de los medios de almacenamiento

Descripción del Control

- Los medios de almacenamiento deberán ser desechados de forma segura cuando ya no se necesiten, utilizando procedimientos formales.

Controles y Objetivos de Control

Control

- A.8.3.3 Transferencia física de medios

Descripción del Control

- Los medios que contienen información deberán ser protegidos contra el acceso no autorizado, el uso indebido o la corrupción durante el transporte.

Controles y Objetivos de Control

Sección

- A.9 Control de acceso

Objetivo de Control

- A.9.1 Requerimientos del negocio acerca del control de acceso

Descripción del Objetivo de Control

- Limitar el acceso a la información y a las instalaciones para su procesamiento.

Controles y Objetivos de Control

Control

- A.9.1.1 Política de control de acceso

Descripción del Control

- Se establecerá una política de control de acceso, documentada y revisada con base a los requerimientos de seguridad del negocio y los requerimientos de seguridad de la información.

Controles y Objetivos de Control

Control

- A.9.1.2 Acceso a las redes y servicios de red

Descripción del Control

- Los usuarios sólo deberán disponer de acceso a la red y a los servicios de la red a los que han sido específicamente autorizados para su uso.

Controles y Objetivos de Control

Sección

- A.9 Control de acceso

Objetivo de Control

- A.9.2 Gestión del acceso de los usuarios

Descripción del Objetivo de Control

- Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.

Controles y Objetivos de Control

Control

- A.9.2.1 Registro y eliminación de usuarios

Descripción del Control

- Se deberá implementar un proceso formal para el registro y la eliminación de usuarios, permitiendo así la correcta asignación de derechos de acceso.

Controles y Objetivos de Control

Control

- A.9.2.2 Provisión de acceso a los usuarios

Descripción del Control

- Se deberá implementar un proceso formal para proveer el acceso a los usuarios, para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

Controles y Objetivos de Control

Control

- A.9.2.3 Gestión de los derechos de acceso con privilegio

Descripción del Control

- La asignación y utilización de los derechos de acceso privilegiados deberán ser restringidas y controladas.

Controles y Objetivos de Control

Control

- A.9.2.4 Gestión de la información secreta para la autenticación de los usuarios

Descripción del Control

- La asignación de la información secreta para la autenticación deberá ser controlada por medio de un proceso formal de gestión.

Controles y Objetivos de Control

Control

- A.9.2.5 Revisión de los derechos de acceso de los usuarios

Descripción del Control

- Los propietarios de los activos deberán revisar los derechos de acceso de los usuarios a intervalos regulares.

Controles y Objetivos de Control

Control

- A.9.2.6 Remoción o ajuste de derechos de acceso

Descripción del Control

- Los derechos de acceso a la información y a las instalaciones para su procesamiento (de todos los empleados y usuarios externos) deberán ser removidos cuando termine su relación de empleo, contrato o acuerdo, o deberán ser ajustados cuando dicha relación cambie.

Controles y Objetivos de Control

Sección

- A.9 Control de acceso

Objetivo de Control

- A.9.3 Responsabilidades de los usuarios

Descripción del Objetivo de Control

- Lograr que los usuarios se responsabilicen de salvaguardar su información de autenticación.

Controles y Objetivos de Control

Control

- A.9.3.1 Uso de la información secreta para la autenticación

Descripción del Control

- A los usuarios se les deberá exigir que sigan las prácticas de la organización en el uso de la información secreta para la autenticación.

Controles y Objetivos de Control

Sección

- A.9 Control de acceso

Objetivo de Control

- A.9.4 Control de acceso a los sistemas y a las aplicaciones

Descripción del Objetivo de Control

- Evitar el acceso no autorizado a los sistemas y a las aplicaciones.

Controles y Objetivos de Control

Control

- A.9.4.1 Restricción de acceso a la información

Descripción del Control

- El acceso a la información y a las funciones de los sistemas de aplicación deberá ser restringido de conformidad con la política de control de acceso.

Controles y Objetivos de Control

Control

- A.9.4.2 Procedimientos de inicio de sesión seguros

Descripción del Control

- Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones deberá ser controlado por un procedimiento de inicio de sesión seguro.

Controles y Objetivos de Control

Control

- A.9.4.3 Sistema para gestión de contraseñas

Descripción del Control

- Los sistemas para gestión de contraseñas deberán ser interactivos y asegurar la calidad de las contraseñas.

Controles y Objetivos de Control

Control

- A.9.4.4 Uso de programas utilitarios privilegiados

Descripción del Control

- El uso de programas utilitarios que podrían ser capaces de anular los controles del sistema y de las aplicaciones deberá ser restringido y estrictamente controlado.

Controles y Objetivos de Control

Control

- A.9.4.5 Control acceso al código fuente de los programas

Descripción del Control

- El acceso al código fuente de los programas deberá ser restringido.

Controles y Objetivos de Control

Sección

- A.10 Criptografía

Objetivo de Control

- A.10.1 Controles criptográficos

Descripción del Objetivo de Control

- Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad y la autenticidad y / o la integridad de la información.

Controles y Objetivos de Control

Control

- A.10.1.1 Política acerca del uso de controles criptográficos

Descripción del Control

- Se deberá elaborar e implementar una política acerca del uso de controles criptográficos para la protección de la información.

Controles y Objetivos de Control

Control

- A.10.1.2 Gestión de claves

Descripción del Control

- Se deberá elaborar e implementar una política acerca del uso, la protección y la duración de las claves criptográficas, aplicable a todo su ciclo de vida.

Controles y Objetivos de Control

Sección

- A.11 Seguridad física y ambiental

Objetivo de Control

- A.11.1 Asegurar las áreas

Descripción del Objetivo de Control

- Evitar el acceso físico no autorizado , el daño e interferencia a la información de la organización y a las instalaciones para su procesamiento.

Controles y Objetivos de Control

Control

- A.11.1.1 Perímetro de la seguridad física

Descripción del Control

- Se deberán definir y utilizar perímetros de protección para las áreas que contienen información sensible o crítica y de igual manera para las instalaciones en que se procesa.

Controles y Objetivos de Control

Control

- A.11.1.2 Controles de entrada física

Descripción del Control

- Las áreas seguras deberán ser protegidas mediante controles de entrada que sean apropiados para asegurar que se le permita el acceso sólo al personal autorizado.

Controles y Objetivos de Control

Control

- A.11.1.3 Asegurar oficinas, salas e instalaciones

Descripción del Control

- La seguridad física para oficinas, salas e instalaciones deberá ser diseñada y aplicada.

Controles y Objetivos de Control

Control

- A.11.1.4 Protección contra amenazas

Descripción del Control

- La protección física contra los desastres naturales, ataques maliciosos o accidentes deberá ser diseñada y aplicada.

Controles y Objetivos de Control

Control

- A.11.1.5 Trabajo en las áreas seguras

Descripción del Control

- Se deberán diseñar y aplicar procedimientos para trabajar en las áreas seguras.

Controles y Objetivos de Control

Control

- A.11.1.6 Áreas de entrega y carga

Descripción del Control

- Los puntos de acceso , tales como las zonas de entrega y de carga y otros puntos donde las personas no autorizadas puedan entrar en los locales deberán ser controlados y, si es posible, aislados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.

Controles y Objetivos de Control

Sección

- A.11 Seguridad física y ambiental

Objetivo de Control

- A.11.2 Equipo

Descripción del Objetivo de Control

- Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

Controles y Objetivos de Control

Control

- A.11.2.1 Emplazamiento y protección del equipo

Descripción del Control

- El equipo deberá estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y la posibilidad de acceso no autorizada.

Controles y Objetivos de Control

Control

- A.11.2.2 Servicios

Descripción del Control

- El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en los servicios.

Controles y Objetivos de Control

Control

- A.11.2.3 Seguridad del cableado

Descripción del Control

- El cableado de la energía eléctrica y el de las telecomunicaciones que transporta datos o que apoya los servicios de información, deberá estar protegido contra la intercepción, interferencia o daño.

Controles y Objetivos de Control

Control

- A.11.2.4 Mantenimiento del equipo

Descripción del Control

- Se deberá dar correcto mantenimiento al equipo para asegurar su continua disponibilidad e integridad.

Controles y Objetivos de Control

Control

- A.11.2.5 Retiro de los activos

Descripción del Control

- Los equipos, la información o el software no podrá ser retirado fuera de las instalaciones sin previa autorización.

Controles y Objetivos de Control

Control

- A.11.2.6 Seguridad de los equipos y de los activos fuera de las instalaciones

Descripción del Control

- Los activos que se retiren fuera de las instalaciones, deberán ser protegidos con medidas de seguridad apropiadas, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización.

Controles y Objetivos de Control

Control

- A.11.2.7 Eliminación segura o reutilización de equipo

Descripción del Control

- Todos los componentes del equipo que contengan capacidad de almacenamiento, deberán ser revisados para garantizar que los datos sensibles y el software con licencia han sido removidos o sobrescritos de forma segura, antes de la eliminación o reutilización del equipo.

Controles y Objetivos de Control

Control

- A.11.2.8 Equipo (de los usuarios) desatendido

Descripción del Control

- Los usuarios deberán asegurarse de que el equipo desatendido tenga la protección adecuada.

Controles y Objetivos de Control

Control

- A.11.2.9 Política de pantallas y escritorios limpios

Descripción del Control

- Se deberá adoptar una política de escritorio limpio de papeles y de medios de almacenamiento removibles y una política de pantalla limpia, en las instalaciones donde se procese información. El término pantalla limpia se refiere a la buena práctica de evitar la posibilidad de que personas ajenas puedan ver la información desplegada en la pantalla, especialmente cuando el usuario se retira momentáneamente de su puesto de trabajo.

Controles y Objetivos de Control

Sección

- A.12 Seguridad de Operaciones

Objetivo de Control

- A.12.1 Procedimientos y responsabilidades de operaciones

Descripción del Objetivo de Control

- Asegurar operaciones correctas y seguras en las instalaciones de procesamiento de información.

Controles y Objetivos de Control

Control

- A.12.1.1 Procedimientos de operación documentados

Descripción del Control

- Los procedimientos de operación deberán estar documentados y puestos a disposición de todos los usuarios que los necesiten.

Controles y Objetivos de Control

Control

- A.12.1.2 Gestión del cambio

Descripción del Control

- Se deberán controlar los cambios que afecten la seguridad de la información. Esto comprende cambios en la organización, en los procesos del negocio, en las instalaciones para procesamiento de la información y en los sistemas.

Controles y Objetivos de Control

Control

- A.12.1.3 Capacidad

Descripción del Control

- El uso de los recursos deberá ser monitoreado, ajustado y se deberán hacer proyecciones de requerimientos futuros de capacidad, para asegurar el desempeño que se necesite de los sistemas.

Controles y Objetivos de Control

Control

- A.12.1.4 Separación de los ambientes de desarrollo, de pruebas y de operación

Descripción del Control

- Los ambientes de desarrollo, de pruebas y de operación deberán estar separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.

Controles y Objetivos de Control

Sección

- A.12 Seguridad de Operaciones

Objetivo de Control

- A.12.2 Protección del Malware

Descripción del Objetivo de Control

- Asegurar que la información y las instalaciones para su procesamiento están protegidos contra el malware.

Controles y Objetivos de Control

Control

- A.12.2.1 Controles contra el malware

Descripción del Control

- Se deberán implementar controles de detección, prevención y recuperación, conjuntamente con una campaña de concientización de los usuarios, para protegerlos contra el malware.

Controles y Objetivos de Control

Sección

- A.12 Seguridad de Operaciones

Objetivo de Control

- A.12.3 Copia de seguridad

Descripción del Objetivo de Control

- Evitar la pérdida de datos.

Controles y Objetivos de Control

Control

- A.12.3.1 Copia de seguridad de la información

Descripción del Control

- Las copias de seguridad de la información, software e imágenes del sistema deberán realizarse y probarse periódicamente de acuerdo con lo establecido en la política de respaldos.

Controles y Objetivos de Control

Sección

- A.12 Seguridad de Operaciones

Objetivo de Control

- A.12.4 Registro de eventos y monitoreo

Descripción del Objetivo de Control

- Registrar eventos y generar evidencia.

Controles y Objetivos de Control

Control

- A.12.4.1 Registro de eventos

Descripción del Control

- Se deberán registrar bitácoras de eventos de seguridad de la información, actividades de los usuarios, excepciones y fallas. Las bitácoras se deberán conservar y revisar periódicamente.

Controles y Objetivos de Control

Control

- A.12.4.2 Protección de las bitácoras

Descripción del Control

- Se deberá proteger contra manipulación y acceso no autorizado, a la información contenida en las bitácoras y las instalaciones en las que éstas se encuentren.

Controles y Objetivos de Control

Control

- A.12.4.3 Bitácora del administrador y del operador

Descripción del Control

- Las actividades del administrador y del operador del sistema deberán ser registradas en bitácoras. Las bitácoras deberán estar protegidas y ser revisadas periódicamente.

Controles y Objetivos de Control

Control

- A.12.4.4 Sincronización del reloj

Descripción del Control

- Los relojes de todos los sistemas de procesamiento de información relevantes en la organización o dominio de seguridad se deberán sincronizar con una única fuente de referencia de tiempo.

Controles y Objetivos de Control

Sección

- A.12 Seguridad de Operaciones

Objetivo de Control

- A.12.5 Control de software operativo

Descripción del Objetivo de Control

- Garantizar la integridad de los sistemas en operación.

Controles y Objetivos de Control

Control

- A.12.5.1 Instalación de software en sistemas en operación

Descripción del Control

- Se deberán implementar controles de la instalación de software en sistemas en operación.

Controles y Objetivos de Control

Sección

- A.12 Seguridad de Operaciones

Objetivo de Control

- A.12.6 Gestión de vulnerabilidades técnicas

Descripción del Objetivo de Control

- Evitar la explotación de vulnerabilidades técnicas.

Controles y Objetivos de Control

Control

- A.12.6.1 Gestión de vulnerabilidades técnicas

Descripción del Control

- La información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan deberá ser obtenida de manera oportuna. Se deberá evaluar la exposición que tiene la organización a este tipo de vulnerabilidades y se deberán adoptar medidas apropiadas para responder al riesgo asociado.

Controles y Objetivos de Control

Control

- A.12.6.2 Restricciones en la instalación de software

Descripción del Control

- Se deberán establecer e implementar normas que rijan la instalación de software por parte de los usuarios.

Controles y Objetivos de Control

Sección

- A.12 Seguridad de Operaciones

Objetivo de Control

- A.12.7 Consideraciones de auditoría de sistemas de información

Descripción del Objetivo de Control

- Minimizar el impacto de las actividades de auditoría en los sistemas en operación.

Controles y Objetivos de Control

Control

- A.12.7.1 Controles de auditoría de Sistemas de información

Descripción del Control

- Los requerimientos y las actividades relacionadas con las auditorías de sistemas en operación deberán ser cuidadosamente planificados y acordados para reducir al mínimo las interrupciones en los procesos del negocio.

Controles y Objetivos de Control

Sección

- A.13 Seguridad en las comunicaciones

Objetivo de Control

- A.13.1 Gestión de la seguridad en la Red

Descripción del Objetivo de Control

- Garantizar la protección de la información en las redes y en las instalaciones para su procesamiento.

Controles y Objetivos de Control

Control

- A.13.1.1 Controles de red

Descripción del Control

- Las redes deberán ser gestionadas y controladas para proteger la información de los sistemas y de las aplicaciones.

Controles y Objetivos de Control

Control

- A.13.1.2 Seguridad de los servicios de red

Descripción del Control

- Los mecanismos de seguridad, niveles de servicio y la gestión de los requerimientos de todos los servicios de la red, deberán ser identificados e incluidos en acuerdos de servicios de red, no importando si estos servicios se proporcionan en la misma empresa o se subcontratan.

Controles y Objetivos de Control

Control

- A.13.1.3 Segregación en las redes

Descripción del Control

- Los grupos de servicios de información, usuarios y los sistemas de información deberán estar segregados en las redes.

Controles y Objetivos de Control

Sección

- A.13 Seguridad en las comunicaciones

Objetivo de Control

- A.13.2 Transferencia de información

Descripción del Objetivo de Control

- Mantener la seguridad de la información que se transfiere dentro de la organización y con cualquier entidad externa.

Controles y Objetivos de Control

Control

- A.13.2.1 Políticas y procedimientos de transferencia de información

Descripción del Control

- Deberán existir políticas, procedimientos y controles formales para la protección de la transferencia de información a través de cualquier medio de comunicación.

Controles y Objetivos de Control

Control

- A.13.2.2 Acuerdos sobre transferencia de la información

Descripción del Control

- Los acuerdos deberán considerar la necesidad de contar con una transferencia segura de información empresarial entre la organización y las partes externas.

Controles y Objetivos de Control

Control

- A.13.2.3 Mensajería electrónica

Descripción del Control

- La información involucrada en la mensajería electrónica deberá estar debidamente protegida.

Controles y Objetivos de Control

Control

- A.13.2.4 Acuerdos de confidencialidad o de no divulgación

Descripción del Control

- Se deberán identificar, revisar y documentar regularmente, los requerimientos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información.

Controles y Objetivos de Control

Sección

- A.14 Adquisición, desarrollo y mantenimiento de sistemas

Objetivo de Control

- A.14.1 Requerimientos de seguridad para los sistemas de información

Descripción del Objetivo de Control

- Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo su ciclo de vida. Esto también incluye los requerimientos para los sistemas de información que proporcionan servicios a través de redes públicas.

Controles y Objetivos de Control

Control

- A.14.1.1 Análisis y especificación de requerimientos de seguridad de la información

Descripción del Control

- Los requerimientos relacionados con la seguridad de la información deberán ser incluidos como parte de los requerimientos de los nuevos sistemas de información o de las mejoras de los sistemas de información existentes.

Controles y Objetivos de Control

Control

- A.14.1.2 Seguridad de los servicios de aplicación en redes públicas

Descripción del Control

- La información involucrada en los servicios de aplicaciones que pasa por redes públicas, deberá estar protegida de la actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.

Controles y Objetivos de Control

Control

- A.14.1.3 Protección de transacciones de servicios de aplicación

Descripción del Control

- La información involucrada en las transacciones de los servicios de aplicación deberá ser protegida para evitar la transmisión incompleta, mal encaminamiento, alteración de mensajes sin autorización, la divulgación no autorizada, duplicación de mensajes sin autorización, o repetición.

Controles y Objetivos de Control

Sección

- A.14 Adquisición, desarrollo y mantenimiento de sistemas

Objetivo de Control

- A.14.2 Seguridad en los procesos de desarrollo y soporte

Descripción del Objetivo de Control

- Garantizar que la seguridad de la información se ha diseñado e implementado en el desarrollo del ciclo de vida de los sistemas de información.

Controles y Objetivos de Control

Control

- A.14.2.1 Política de desarrollo seguro

Descripción del Control

- Se deberán establecer e implementar normas para el desarrollo de software y sistemas dentro de la organización.

Controles y Objetivos de Control

Control

- A.14.2.2 Procedimientos para el control de cambios de los sistemas

Descripción del Control

- Los cambios en los sistemas dentro del ciclo de desarrollo se deberán controlar utilizando procedimientos formales de control de cambios.

Controles y Objetivos de Control

Control

- A.14.2.3 Revisión técnica de aplicaciones después de cambios en la plataforma operativa

Descripción del Control

- Cuando se realicen cambios en las plataformas de operación, se deberán revisar y aprobar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones de la organización o en la seguridad.

Controles y Objetivos de Control

Control

- A.14.2.4 Restricciones a los cambios en paquetes de software

Descripción del Control

- Se deberán desincentivar las modificaciones a los paquetes de software, limitando los mismos a cambios necesarios. Todos los cambios deberán ser estrictamente controlados.

Controles y Objetivos de Control

Control

- A.14.2.5 Principios de ingeniería de sistemas seguros

Descripción del Control

- Se deberán establecer , documentar, y mantener principios para la ingeniería de sistemas seguros, aplicables para cualquier esfuerzo de implementación de sistemas de información.

Controles y Objetivos de Control

Control

- A.14.2.6 Ambiente de desarrollo seguro

Descripción del Control

- Las organizaciones deberán establecer y proteger adecuadamente los entornos de desarrollo seguro, para los esfuerzos de desarrollo de sistemas e integración que cubren todo el ciclo de vida de desarrollo de sistemas.

Controles y Objetivos de Control

Control

- A.14.2.7 Desarrollo de terceros

Descripción del Control

- La organización deberá supervisar y monitorear las actividad de desarrollo de sistemas realizadas por terceros. Esto es cuando el desarrollo de sistemas se da en outsourcing.

Controles y Objetivos de Control

Control

- A.14.2.8 Pruebas de seguridad del sistema

Descripción del Control

- Las pruebas de la funcionalidad de la seguridad se deberán llevar a cabo durante el desarrollo.

Controles y Objetivos de Control

Control

- A.14.2.9 Pruebas de aceptación del sistema

Descripción del Control

- Se deberán establecer programas de pruebas de aceptación y los criterios relacionados, para los nuevos sistemas de información, actualizaciones y nuevas versiones.

Controles y Objetivos de Control

Sección

- A.14 Adquisición, desarrollo y mantenimiento de sistemas

Objetivo de Control

- A.14.3 Datos de prueba

Descripción del Objetivo de Control

- Garantizar la protección de los datos utilizados para las pruebas.

Controles y Objetivos de Control

Control

- A.14.3.1 Protección de datos de prueba

Descripción del Control

- Los datos de prueba deberán seleccionarse cuidadosamente, protegerse y controlarse.

Controles y Objetivos de Control

Sección

- A.15 Las relaciones con proveedores

Objetivo de Control

- A.15.1 Seguridad de la información en relaciones con los proveedores

Descripción del Objetivo de Control

- Garantizar la protección de los activos de la organización que sean accedidos por los proveedores.

Controles y Objetivos de Control

Control

- A.15.1.1 Política de seguridad de la información para relaciones con proveedores

Descripción del Control

- Los requerimientos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deberán ser acordados con el proveedor y documentados.

Controles y Objetivos de Control

Control

- A.15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores

Descripción del Control

- Todos los requisitos pertinentes de seguridad de la información se deberán establecer y acordar con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.

Controles y Objetivos de Control

Control

- A.15.1.3 Cadena de suministro de tecnología de la información y comunicación

Descripción del Control

- En los acuerdos con proveedores se deberán incluir los requisitos para responder a los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicación y la cadena de suministro de productos.

Controles y Objetivos de Control

Sección

- A.15 Las relaciones con proveedores

Objetivo de Control

- A.15.2 Gestión de la entrega de servicios del proveedor

Descripción del Objetivo de Control

- Mantener y acordar el nivel de seguridad de la información y prestación de servicios, tomando como base los acuerdos con el proveedor.

Controles y Objetivos de Control

Control

- A.15.2.1 Monitoreo y revisión de los servicios de proveedores

Descripción del Control

- Las organizaciones deberán supervisar, revisar y auditar, periódicamente, la prestación de servicios de los proveedores.

Controles y Objetivos de Control

Control

- A.15.2.2 Gestión de cambios en servicios de proveedores

Descripción del Control

- Los cambios en la prestación de servicios por parte de los proveedores, incluyendo mantenimiento y mejora de las políticas de seguridad de la información existentes, procedimientos y controles, deberán ser gestionados, teniendo en cuenta la criticidad de la información comercial, sistemas y procesos que intervienen y la reevaluación de los riesgos.

Controles y Objetivos de Control

Sección

- A.16 Gestión de incidentes de seguridad de la Información

Objetivo de Control

- A.16.1 Gestión de incidentes de seguridad de la información y mejoras

Descripción del Objetivo de Control

- Garantizar un enfoque coherente y eficaz para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

Controles y Objetivos de Control

Control

- A.16.1.1 Responsabilidades y procedimientos

Descripción del Control

- Las responsabilidades y los procedimientos de gestión se deberán establecer para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Controles y Objetivos de Control

Control

- A.16.1.2 Reportar los eventos de seguridad de la información

Descripción del Control

- Los eventos de seguridad de la información deberán ser reportados lo más rápidamente posible, a través de los canales de gestión apropiados.

Controles y Objetivos de Control

Control

- A.16.1.3 Reportar las debilidades de seguridad de la información

Descripción del Control

- A los empleados y contratistas que utilicen la información de la organización, se les deberá requerir que anoten y reporten cualquier debilidad de seguridad de la información en los sistemas o servicios (ya sea observada o sospechada).

Controles y Objetivos de Control

Control

- A.16.1.4 Evaluación y decisión en los eventos de seguridad de la información

Descripción del Control

- Los eventos de seguridad de la información deberán ser evaluados y se deberá decidir si van a ser clasificados como incidentes de seguridad de la información.

Controles y Objetivos de Control

Control

- A.16.1.5 Respuesta a los incidentes de seguridad de la información

Descripción del Control

- Se deberá responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

Controles y Objetivos de Control

Control

- A.16.1.6 Aprender de los incidentes de seguridad de la información

Descripción del Control

- Los conocimientos adquiridos a partir del análisis y la solución de los incidentes de seguridad de la información deberá ser utilizado para reducir la probabilidad o el impacto de los incidentes en el futuro.

Controles y Objetivos de Control

Control

- A.16.1.7 Acopio de pruebas

Descripción del Control

- La organización deberá definir y aplicar procedimientos para la identificación, colección, adquisición y conservación de la información, que puede servir como evidencia.

Controles y Objetivos de Control

Sección

- A.17 Aspectos de seguridad Información de la gestión de continuidad del negocio

Objetivo de Control

- A.17.1 Continuidad de seguridad de la información

Descripción del Objetivo de Control

- La continuidad de la seguridad de la información deberá incorporarse a los sistemas de gestión de la continuidad del negocio en la organización.

Controles y Objetivos de Control

Control

- A.17.1.1 Planificación de la continuidad de la seguridad de la Información

Descripción del Control

- La organización deberá determinar sus requerimientos de seguridad de la información y de la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

Controles y Objetivos de Control

Control

- A.17.1.2 Implementación de la continuidad de la seguridad de la Información

Descripción del Control

- La organización deberá establecer, documentar, implementar y mantener procesos, procedimientos y controles que garanticen el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

Controles y Objetivos de Control

Control

- A.17.1.3 Verificar, revisar y evaluar la continuidad de la seguridad de la Información

Descripción del Control

- La organización deberá verificar el establecimiento y la aplicación de controles de continuidad de seguridad de la información a intervalos regulares, para asegurarse de que son válidos y eficaces durante situaciones adversas.

Controles y Objetivos de Control

Sección

- A.17 Aspectos de seguridad Información de la gestión de continuidad del negocio

Objetivo de Control

- A.17.2 Redundancias

Descripción del Objetivo de Control

- Asegurar la disponibilidad de instalaciones de procesamiento de información.

Controles y Objetivos de Control

Control

- A.17.2.1 Disponibilidad de instalaciones para el procesamiento de la información

Descripción del Control

- Las instalaciones de procesamiento de información deberán contar con suficiente redundancia para satisfacer los requisitos de disponibilidad.

Controles y Objetivos de Control

Sección

- A.18 Cumplimiento

Objetivo de Control

- A.18.1 Cumplimiento con los requisitos legales y contractuales

Descripción del Objetivo de Control

- Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales en materia de seguridad de la información y de cualquier requisito de seguridad.

Controles y Objetivos de Control

Control

- A.18.1.1 Identificación de legislaciones y requisitos contractuales aplicables

Descripción del Control

- Todos los requisitos pertinentes legislativos estatutarios, reglamentarios, contractuales, y el enfoque de la organización para cumplir con estos requisitos deberán identificarse de forma explícita, documentarse y mantenerse al día para cada sistema de información y la organización.

Controles y Objetivos de Control

Control

- A.18.1.2 Derechos de propiedad intelectual

Descripción del Control

- Se deberán aplicar los procedimientos apropiados para garantizar el cumplimiento con los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario.

Controles y Objetivos de Control

Control

- A.18.1.3 Protección de registros

Descripción del Control

- Los registros deberán estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y la liberación no autorizada, de conformidad con, requisitos reglamentarios, contractuales y leyes comerciales.

Controles y Objetivos de Control

Control

- A.18.1.4 Privacidad y protección de información personal identificable

Descripción del Control

- La privacidad y protección de la información personal identificable deberá garantizarse de acuerdo con lo dispuesto en la legislación y reglamentación cuando sea aplicable.

Controles y Objetivos de Control

Control

- A.18.1.5 Reglamento de controles de cifrado

Descripción del Control

- Los controles criptográficos se deberán utilizar en cumplimiento con todos los acuerdos , leyes y reglamentos.

Controles y Objetivos de Control

Sección

- A.18 Cumplimiento

Objetivo de Control

- A.18.2 Revisión de seguridad de la información

Descripción del Objetivo de Control

- Garantizar que la seguridad de la información sea implementada y operada de acuerdo con las políticas y procedimientos de la organización.

Controles y Objetivos de Control

Control

- A.18.2.1 Revisión independiente de seguridad de la información

Descripción del Control

- El enfoque de la organización para la gestión de seguridad de la información y su puesta en práctica (es decir, los objetivos de control , controles , políticas, procesos y procedimientos para la seguridad de la información) se deberán revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos.

Controles y Objetivos de Control

Control

- A.18.2.2 Cumplimiento de políticas y normas de seguridad

Descripción del Control

- Los gerentes deberán comprobar periódicamente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas de seguridad apropiadas, normas y cualquier otro requerimiento de seguridad.

Controles y Objetivos de Control

Control

- A.18.2.3 Revisión de cumplimiento técnico

Descripción del Control

- Los sistemas de información deberán ser revisados periódicamente para asegurar su cumplimiento con las políticas y estándares de seguridad de la información de la organización.

ISO/IEC 27001:2013

Controles y Objetivos de Control

Juan Carlos Morales, CISA, CISM, CRISC, CGEIT