Strategos
Consulting Services

# Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27001:2013 para entidades públicas del estado peruano.

Abril 2015

# Agenda

- ¿Por qué implementar un Sistema de Gestión de Seguridad de la Información en entidades públicas?
- Seguridad de la Información en entidades públicas.
- ¿Por qué fallan los SGSI en las entidades públicas?
- Lo nuevo de la ISO/IEC 27001:2013
- Implementación de la ISO/IEC 27001:2013.
- Adecuación de la ISO/IEC 27001: 2005 a la 2013 o NTP ISO/IEC 27001:2008 a la NTP ISO/IEC 27001:2014
- Nuestros Servicios.

Strategos
Consulting Services

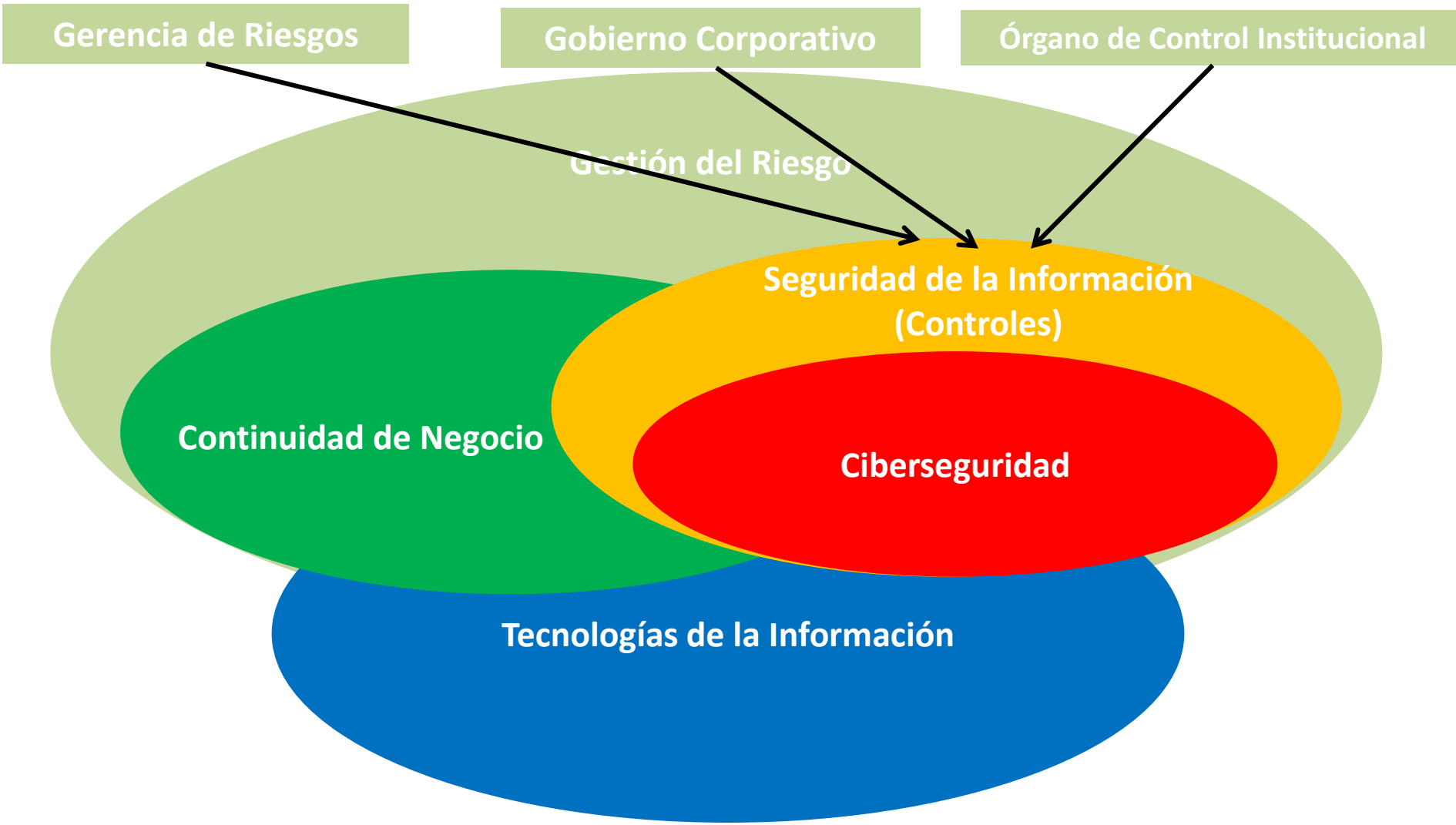
# ¿Por qué implementar un Sistema de Gestión de Seguridad de la Información en entidades públicas?

# ¿Por qué implementar un Sistema de Gestión de Seguridad de la Información en entidades públicas?

- Cumplimiento de Resolución Ministerial 129-2012-PCM: La PCM desde el año 2012 ha solicitado la implementación de un Sistema de Gestión de Seguridad basado en la NTP ISO/IEC 27001:2008. Actualmente, la norma internacional es la ISO/IEC 27001:2013 y se encuentra en revisión la NTP ISO/IEC 27001:2014 correspondiente a la ultima versión internacional.
- Aseguramiento de la información del ciudadano: Todo impacto contra la disponibilidad, integridad y confidencialidad de la información afecta la perspectiva del ciudadano generando malestar del servicio, perdida de imagen a la institución publica e investigaciones por Contraloría. Algunas amenazas de la información de una institución pública son:
  - Personal interno descontento o mal intencionado
  - Cibercriminales
  - Malware
  - Desastres naturales
  - Hacktivistas
  - Fraude
  - BYOD
- Gobierno Corporativo: La seguridad de la información brinda controles que puedan ser supervisados por el directorio y la alta dirección. Así mismo es considerado una herramienta antifraude y permite obtener evidencias para el control interno.

# Seguridad de la Información en el Negocio en entidades públicas

# Seguridad de la Información en entidades públicas.




Strategos Consulting Services

Gerencia de Seguridad de la Información

# ¿Por qué fallan los SGSI en las entidades públicas?

# ¿Por qué fallan los SGSI en entidades públicas?

- Los procesos del alcance del SGSI:
  - No son eficientes.
  - Son de TI y no críticos de negocio.
  - No son analizados desde la perspectiva del ciudadano o usuarios.
- Poco apoyo de la dirección y recursos.
- La entidad pública cree que la responsabilidad de la seguridad es solo del Jefe de seguridad de la información.
- Cultura Organizacional inadecuada.
- Ausencia de Liderazgo y Compromiso para promover la seguridad de la información por la alta dirección.

La seguridad de la información mal implementada genera ineficiencia y disconformidad en toda la organización y en la perspectiva del servicio al ciudadano, por consiguiente, incumplimiento constante y aumento del riesgo.

**Procesos mal diseñados + Tecnología = Desastre Organizacional**

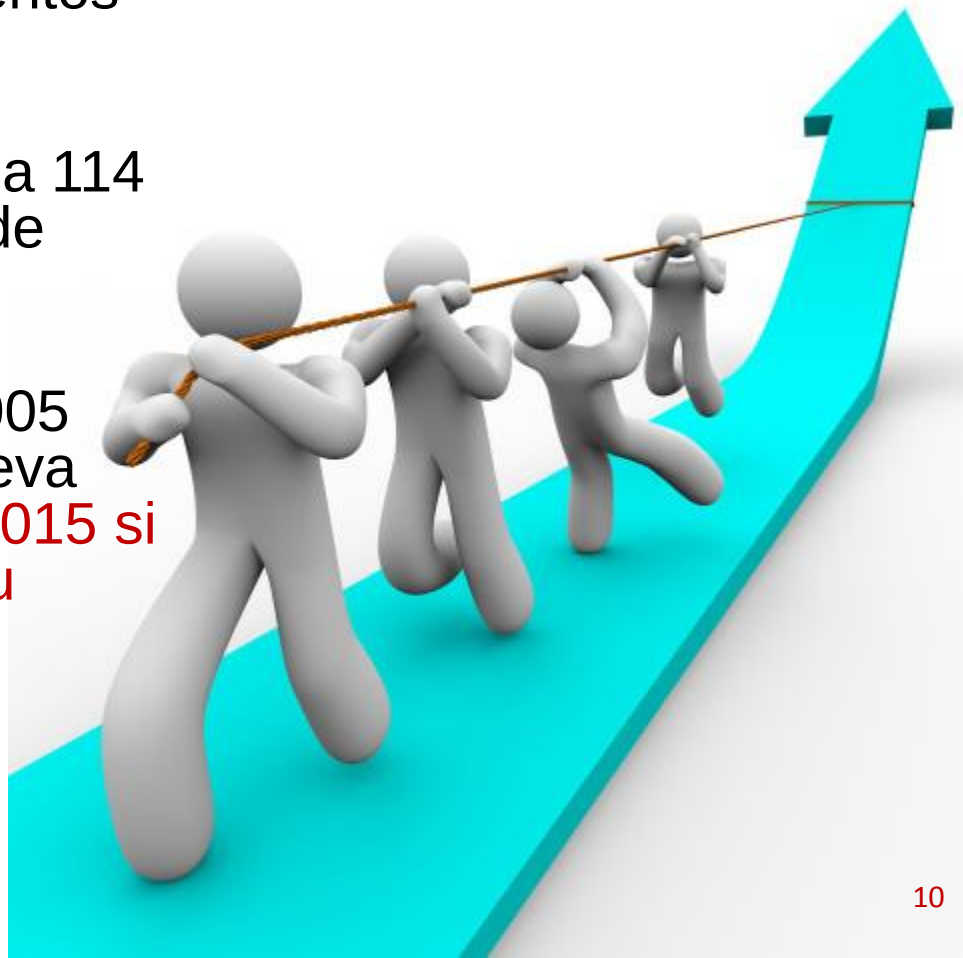
**Procesos mal diseñados + Tecnología + Seguridad = Catástrofe Organizacional**

Strategos
Consulting Services

# Lo nuevo de la ISO/IEC 27001:2013

# Cambios de la versión 2005 a la 2013

- Se cambio la estructura de la norma.
- Nuevos conceptos incorporados.
- Se eliminaron algunos requerimientos y la documentación de algunos procedimientos.
- El anexo A ha disminuido de 133 a 114 controles y aumento la cantidad de secciones de 11 a 14.
- Las empresas que han sido certificadas en ISO/IEC 27001:2005 deben hacer la transición a la nueva revisión 2013 hasta septiembre 2015 si quieren mantener la validez de su certificación.



Strategos
Consulting Services

# Estructura ISO/IEC 27001:2013

| PLAN | | | | DO | CHECK | ACT |
|---|---|---|---|---|---|---|
| 4. Contexto de la organización | 5. Liderazgo | 6. Planificación | 7. Apoyo | 8. Operación | 9. Evaluación de desempeño | 10. Mejora |
| 4.1 Comprender la organización y su contexto | 5.1 Liderazgo y compromiso | 6.1 Acciones para abordar los riesgos | 7.1 Recursos | 8.1 Control y planificación | 9.1 Monitoreo, medición, análisis y evaluación | 10.1 No conformidades y acciones correctivas |
| 4.2 Comprender las necesidades y expectativas de las partes interesadas | 5.2 Política | 6.2 Objetivos de seguridad de la información y planificación para lograrlos | 7.2 Competencias | 8.2 Evaluación del riesgo de la seguridad de la información | 9.2 Auditoría Interna | 10.2 Mejora continua |
| 4.3 Determinar el alcance del sistema de gestión de la seguridad de la información | 5.3 Roles organizacionales, responsabilidades y autoridades | | 7.3 Conocimiento | 8.3 Tratamiento del riesgo de seguridad de la información | 9.3 Revisión de la gestión | |
| 4.4 Sistema de gestión de seguridad de la información | | | 7.4 Comunicación | | | |
| | | | 7.5 Información documentada | | | |

Strategos
Consulting Services

# Nuevos conceptos incorporados

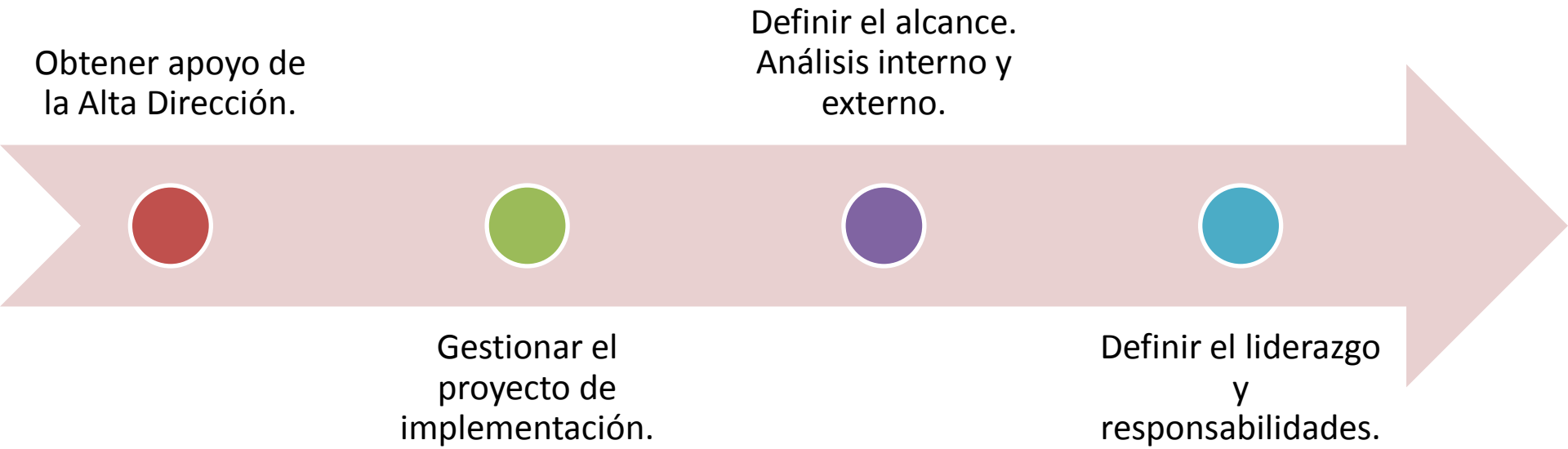
| Concepto Nuevo o Actualizado | Explicación |
|---|---|
| Contexto de la Organización | El ambiente interno o externo en el cual la organización opera. |
| Problemas, riesgos y oportunidades | Reemplaza a la acción preventiva. |
| Partes interesadas | Reemplaza a los stakeholders. El termino en ingles es “más amplio”. |
| Liderazgo | Requerimientos específicos para la alta gerencia. |
| Comunicación | Existen requerimientos explícitos para las comunicaciones internas y externas. |
| Objetivos de seguridad de la información | Los objetivos de seguridad tienen una función mas relevante en esta versión. |
| Dueño del riesgo | Reemplaza al dueño del activo. |
| Plan de tratamiento del riesgo | La efectividad del plan de tratamiento del riesgo es mas importante que la efectividad de los controles. |
| Controles | Los controles son determinados durante el proceso de tratamiento del riesgo en vez de ser seleccionados del Anexo A. |
| Información documentada | Reemplaza a los documentos y registros. |
| Evaluación de rendimiento | Cubrir la medición del SGSI y de la efectividad del plan del tratamiento del riesgo. |
| Mejora Continua | Se pueden utilizar otras metodologías diferentes al Plan, Do, Check, Act. |

# Información Documentada “Obligatoria” ISO/IEC 27001:2013

- 4.3 Alcance del SGSI
- 5.2 Política de Seguridad de la Información
- 6.1.2 Proceso de evaluación de riesgo
- 6.1.3 Proceso de tratamiento del riesgo
- 6.1.3.d Documento de aplicabilidad
- 6.2 Objetivos de seguridad
- 7.2.d Evidencia de Competencias.
- 7.5.1.b Información documentada sobre la efectividad del SGSI
- 8.1. Plan y control operacional
- 8.2. Resultados de la evaluación del riesgo
- 8.3 Resultados del tratamiento del riesgo
- 9.1 Evidencia del monitoreo y resultado de mediciones
- 9.2.g Evidencia de programas de auditoria y resultados de auditoria
- 9.3 Evidencia de resultados de revisiones gerenciales
- 10.1.f Evidencia de la naturaleza de no conformidades y acciones a tomar.
- 10.1.g Evidencia de resultados de acciones correctivas.

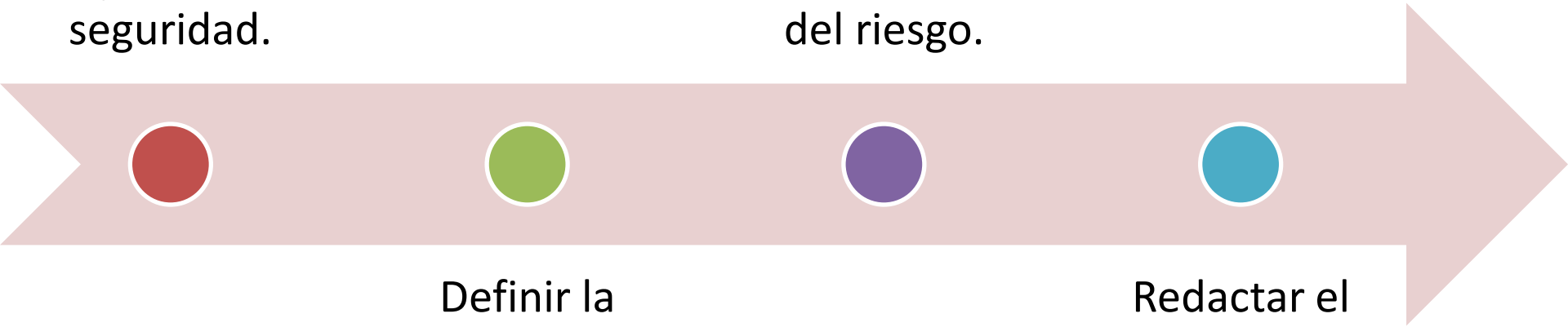
# Implementación de la ISO/IEC 27001:2013

# Implementación de la ISO/IEC 27001:2013



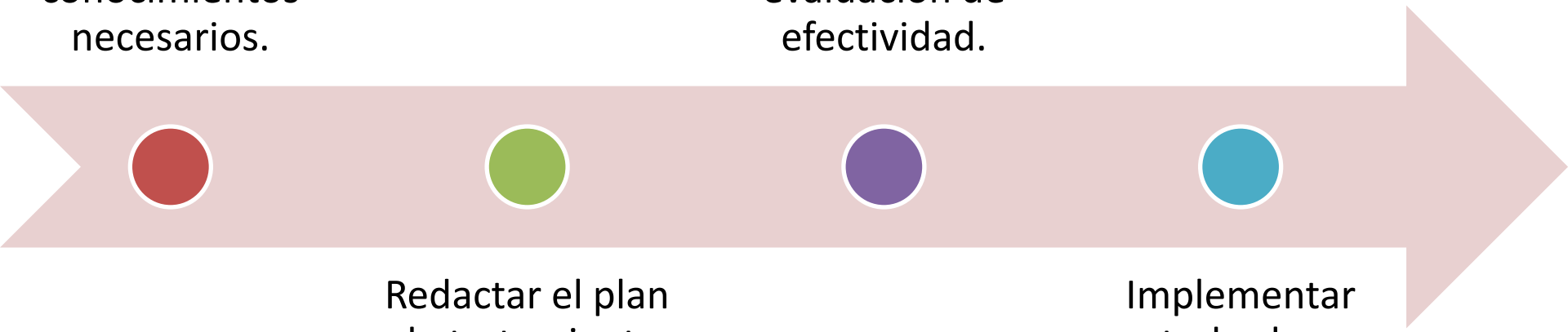

Strategos
Consulting Services

# Implementación de la ISO/IEC 27001:2013




Strategos
Consulting Services

# Implementación de la ISO/IEC 27001:2013



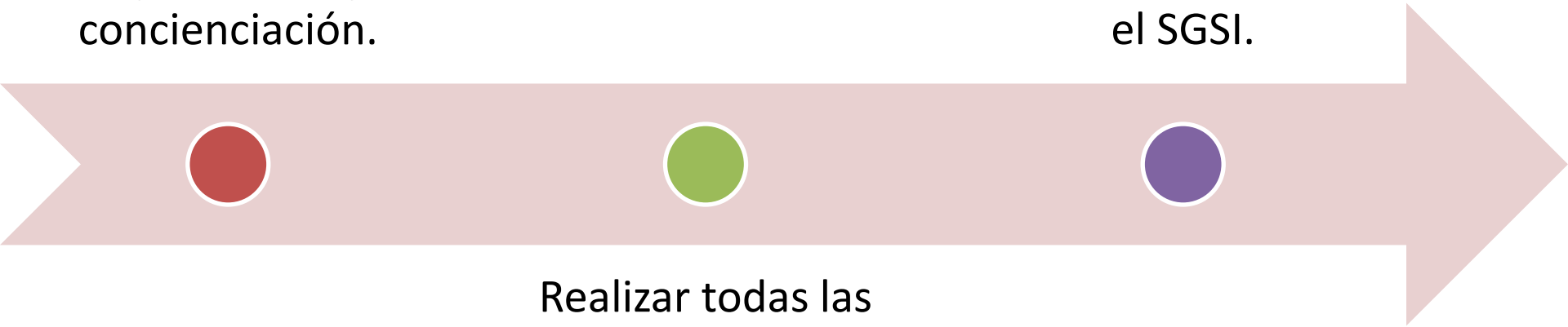

Strategos
Consulting Services

# Implementación de la ISO/IEC 27001:2013

Implementar programas de capacitación y concienciación.

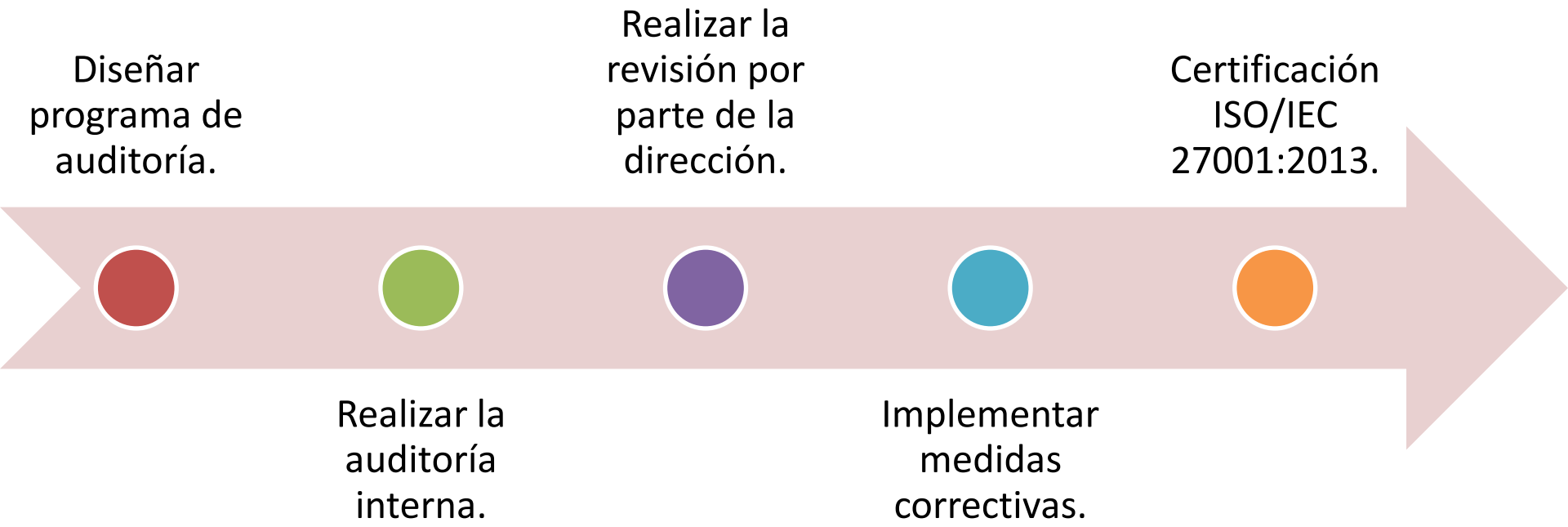
Realizar todas las operaciones diarias establecidas en la documentación de su SGSI.

Monitorear y medir el SGSI.



Strategos
Consulting Services

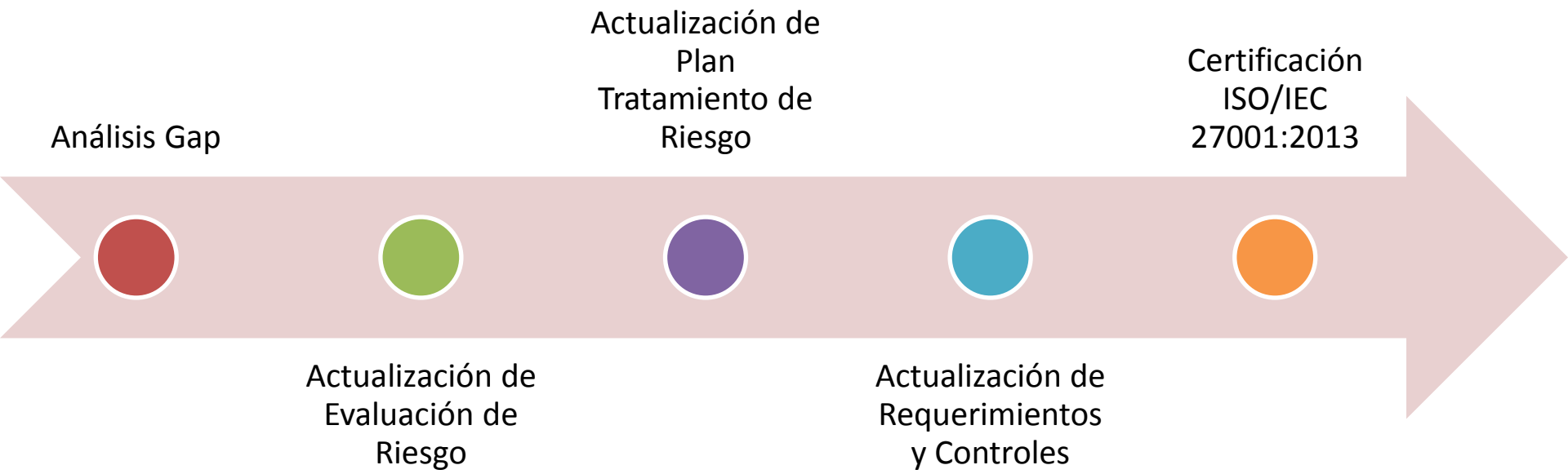
# Implementación de la ISO/IEC 27001:2013




Strategos
Consulting Services

# Adecuación de la ISO/IEC 27001: 2005 a la 2013 o NTP ISO/IEC 27001:2008 a la 2014

# Adecuación de la ISO/IEC 27001: 2005 a la 2013




Strategos
Consulting Services

# Nuestros Servicios

# Nuestros Servicios

- Implementación integral ISO/IEC  27001:2013.
- Diagnostico ISO/IEC 27001:2013 o Análisis Gap.
- Monitoreo o Evaluación de Controles del SGSI.
- Monitoreo del Plan de tratamiento de riesgo.
- Gestión de Proyecto de la ejecución del plan de tratamiento de riesgo en la organización.
- Outsourcing
- Diseño y elaboración de información documentada del SGSI.
- Pre-auditorías para la certificación ISO/IEC 27001:2013: Análisis documental y auditoría in-situ.

Strategos
Consulting Services

# Nuestros Diferenciadores

# Nuestros Diferenciadores

- Aseguramos la certificación ISO/IEC 27001:2013.
- Contamos con Alianzas de Negocio con BSI Group y Tuv Rehinland (entidades certificadoras)
- Nuestros profesionales ISO/IEC 27001 Lead Auditor, CISM, CISA, CRISC, ISF ISO/IEC 27002
- Proponemos precios competitivos en el mercado.
- Generamos una cultura de seguridad de la información en la organización antes de la implementación.
- Nuestro enfoque es entregar una propuesta de valor desde la perspectiva del usuario final o ciudadanos.

bsi.

Strategos
Consulting Services

# *CONTACTO*

Strategos
Consulting Services

Raúl Díaz | Socio IT & Information Security Services
**CISM, CISA, ISO/IEC 27002, CEH, CHFI, ECSA, ECSP, ITIL(F), CPTE**
raul.diaz@strategoscs.com
@rauldiazp
Skype: raul.diaz.com
Cel: +51-994521461
RPM: #0032737
www.strategoscs.com
www.rauldiazparra.com