Modelo de Arquitectura de Seguridad de la Información –MASI–

A. Flórez , J. A. Calvo and D. J. Parada,

Facilitador

Diego Javier Parada Serrano

Escuela de Ingeniería
Facultad de Ingeniería Informática
Universidad Pontifica Bolivariana

Agenda

- Objetivos
- Introducción
- Definición de Arquitectura
- Modelo de Arquitectura de Seguridad de la Información – MASI –
- MASI
  - ✓ Elementos
- Conclusiones

Objetivo General

Desarrollar un modelo conceptual que permita la administración y gestión de la Seguridad de la Información mediante el involucramiento de la alta gerencia en los procesos de negocio.

Objetivos Específicos

- Definir los elementos que conforman el Modelo de Arquitectura de Seguridad de la Información MASI mediante la revisión del estado del arte de modelos existentes.

.

Objetivos Específicos

- Establecer los insumos que permitan la ejecución de las actividades establecidas en el modelo para facilitar la implementación del MASI en las organizaciones

Introducción

Actualmente en el **contexto de las TI** es común encontrarse con un **gran número de conceptos** como:

- ✓ Gobierno de TI
- ✓ Gobierno de la SI
- ✓ Arquitectura de TI
- ✓ Arquitectura de SI
- ✓ Seguridad Informática
- ✓ Seguridad de la Información
- ✓ Análisis de Riesgos
- ✓ Continuidad de Negocio, entre otros;

Conceptos con un **campo de acción específico** frente al apoyo en la administración de **TI** como aquel proceso inherente a la idea de negocio.

Introducción (cont.)

¿Existe un modelo para administración de la Seguridad de la Información?

Dicho modelo debe en **elementos genéricos** y debe estar soportar en un **proceso lógico y sistemático** que permita alinear:

- ✓ Procesos de negocio
- ✓ Procesos de TI

→

- ✓ Lenguaje
- ✓ Compromiso

¿Qué es una Arquitectura?

Es habitual que al hablar de arquitectura se traiga a acotación términos como **diseñar, planear, construir** lo que es apenas normal, muestra de ello es el análisis etimológico que así lo demuestra:

Etimología de la palabra Arquitectura:

- Arquitectura → del latín *architectūra* (técnica de diseñar y construir)
- Arquitecto → del griego *ἀρχιτέκτων* (Arkhitekton)

  ἀρχ (Arkhi) → jefe

  ιτέκτων (tekton) → constructor

¿Qué es una Arquitectura? (cont.)

Dependiendo del contexto, se pueden encontrar diseños o arquitecturas de tipo:

- ✓ Eléctrico
- ✓ Electrónico
- ✓ Red de datos
- ✓ Diseño de máquinas
- ✓ Diseño industrial
- ✓ Diseño de redes de acueducto, entre otros.

El diseño permite definir un esquema que vislumbre:

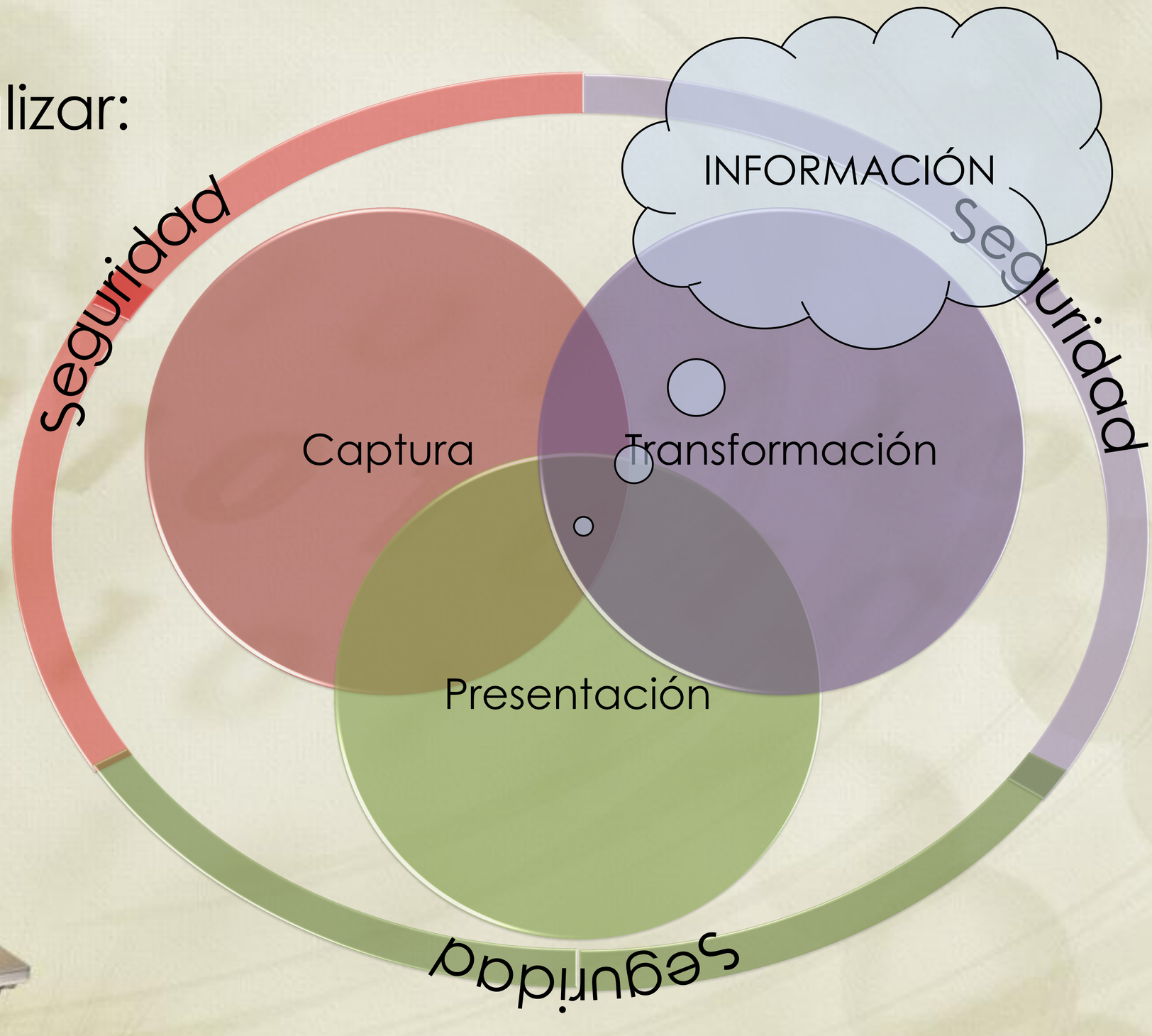
- Armonía
- Interacción

} → Componentes → Funcionalidad Sistema

Qué es una Arquitectura? (cont.)

¿Cuál es la necesidad que se vislumbra?

Operacionalizar:



Qué es una Arquitectura?? (cont.)

El Dr. Jeimy Cano, quien ha desarrollado investigación en el contexto de TI, establece que una arquitectura es: "*la organización lógica para los procesos, estructuras y acuerdos de una corporación que reflejan la integración y regulación de los requerimientos del modelo operacional de la misma*".

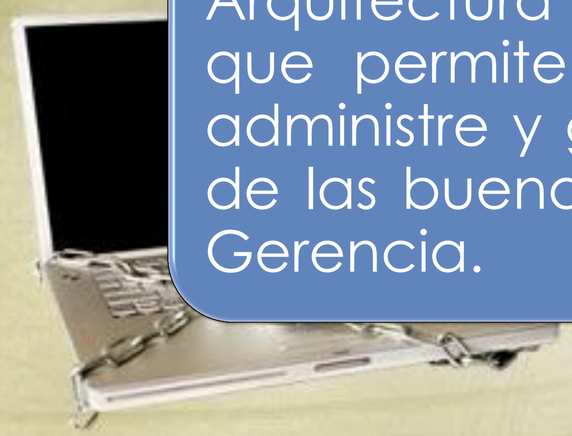
Introducción:
Arquitectura de Seguridad de la Información

Arquitectura : palabra estrechamente relacionada con el diseño.

+

Seguridad de la Información: "*proceso que busca proteger la información contra una gama amplia de amenazas, busca asegurar la continuidad del negocio, disminuir los posibles daños y maximizar el retorno de inversión.*" *[1]*

=



Arquitectura de Seguridad de la Información: correlación de los elementos que permiten diseñar y construir un esquema gerencial que: organice, administre y gestione los procesos de la organización bajo los fundamentos de las buenas prácticas de la SI alineados con las expectativas de la Alta Gerencia.

Introducción:
Arquitectura de Seguridad de la Información

Las estrategias de seguridad deben ser desplegadas:

- ✓ Estratégico: formulación de la expectativas del negocio, en términos de los compromisos en seguridad.
- ✓ Táctico: instrumentalización de la arquitectura a través de estándares, normas o *frameworks*.
- ✓ Operacional: definición del comportamiento de los actores del negocio (usuarios, alta gerencia, clientes, proveedores, entre otros) en la ejecución de sus funciones, detallando el cómo se realizan los procesos definidos en la arquitectura.

Gestión de Continuidad del Negocio

Negocio

Razón de ser de la organización

Misión de la organización

Definición de indicadores del cumplimiento de las metas trazadas

Plan de desarrollo

Proyección del negocio

Visión de la organización

Conocimiento del Negocio

Sistema de planeación y gestión estratégica

Balanced Scorecard (BSC) (Cuadro de Mando Integral)

Metas de la organización

Expectativas del negocio

Proceso Negocio

ENTRADAS
(De otros procesos)

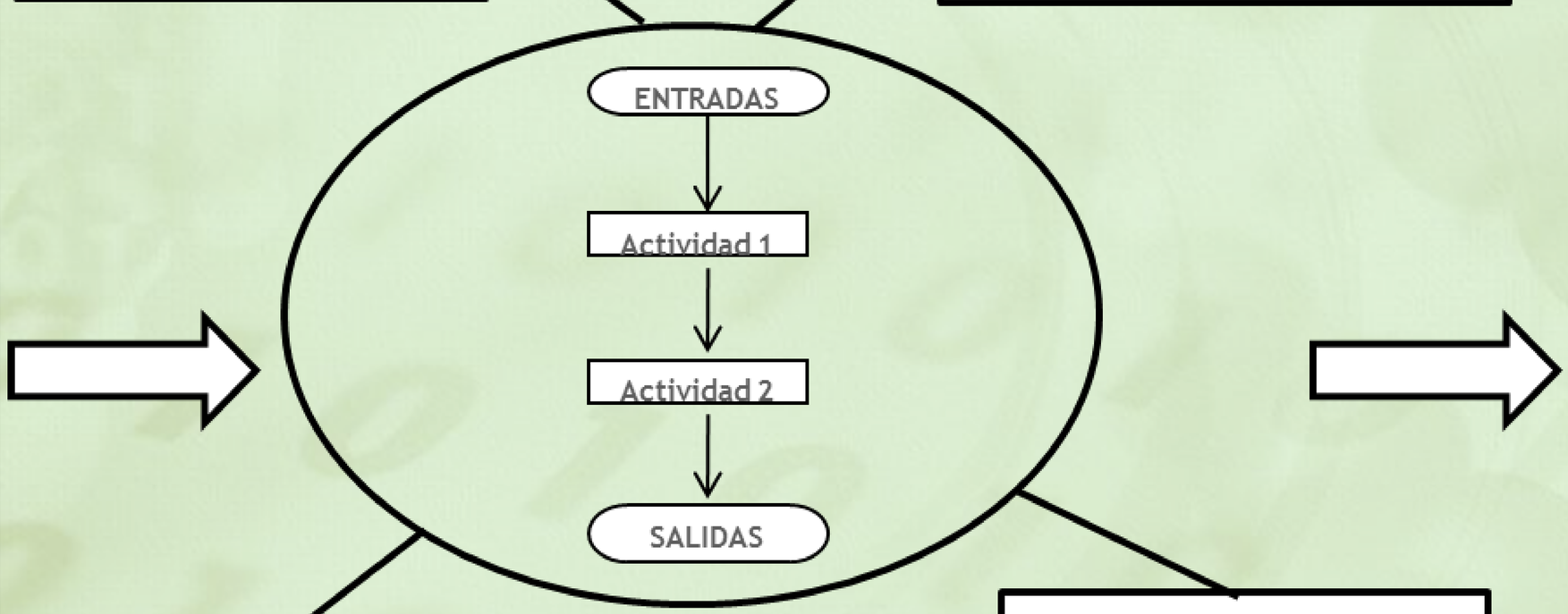
- Misión
- Visión
- Plan de Desarrollo
- Mapa de procesos
- Balanced Scorecard

¿Con qué?

Sistemas de información:
- DSS
- GDSS
- EIS

¿Con quién?

Involucrados:
- Alta Dirección
- Arquitecto SI
- Dueños y custodios de los procesos misionales



Recursos:
Herramienta de gestión de información de la Empresa

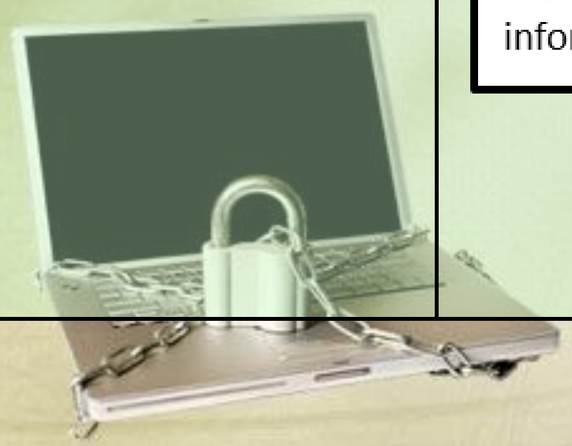
¿Cómo?

$$\frac{Met.Cum.}{M.Def.} + \frac{Doc.Act.}{Doc.Exist.} + Nu.Proc.$$

Indicadores

SALIDAS

- Entendimiento del negocio a nivel estratégico
- Entendimiento del negocio a nivel operativo
- Alineación de las expectativas de la alta dirección con respecto a los objetivos de la arquitectura



Marco Normativo

Marco Normativo y Legal de SI

Política

Directrices

Normas

Procedimientos

Normativa Corporativa

Normativa Jurídica

Normativa Jurídica

Normativa Jurídica

Proceso Normativa de Seguridad

ENTRADAS
(De otros procesos)

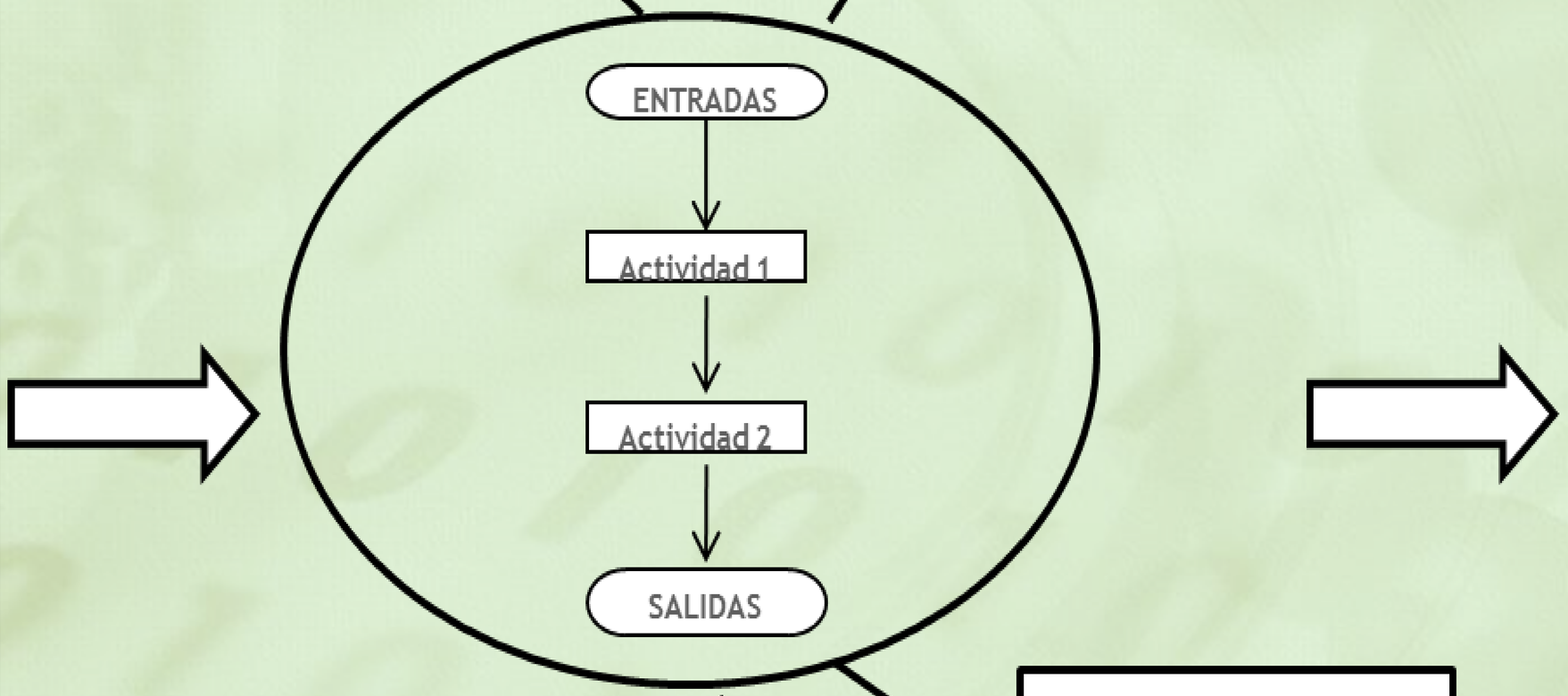
- Políticas organizacionales y contractuales
- Procedimientos de TI
- Legislación aplicable
- Información de incidentes

¿Con qué?

Sistema de información:
- Help Desk
- Portal Web Informativo

¿Con quién?

Involucrados:
- Alta Dirección
- Arquitecto SI
- Abogados



- Equipos de Help Desk
- Consultoría o asesoría jurídica.

¿Cómo?

$$\frac{\text{Nº Proyectos Aprobados}}{\text{Nº Proyectos Sugeridos}}$$

Indicadores

SALIDAS

- Política de, Directrices, Normas, Procedimientos de SI.
- Código de ética
- Redefinición del reglamento interno de trabajo y contractual
- Norma antifraude

MASI: Acuerdos

Alinear la agenda interna

Determinan

- Nivel de Compromiso
- Competencias y Habilidades
- Prioridades
- Nivel de Inversión

Alta Gerencia

Arquitecto de SI

Proceso Acuerdos

ENTRADAS
(De otros procesos)

Comunicación en Cascada

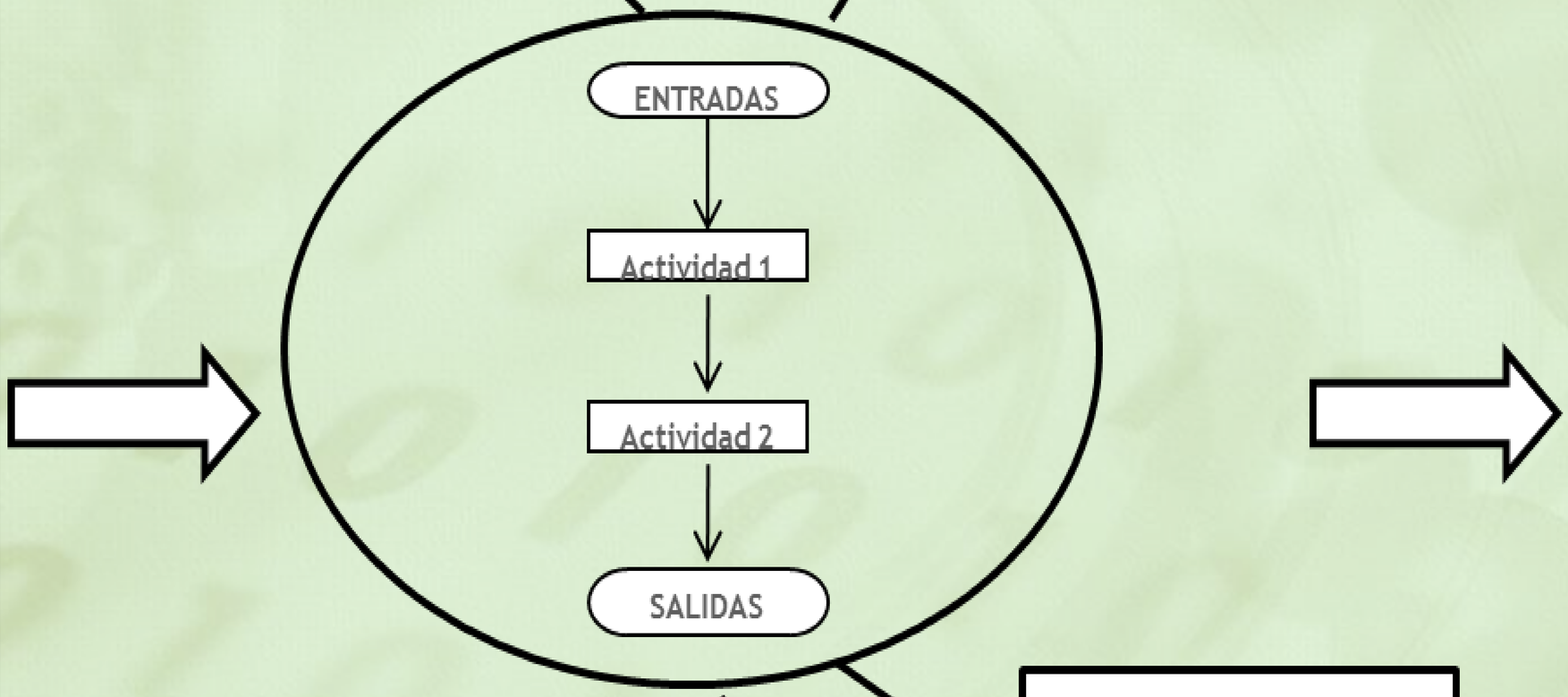
¿Con qué?

Sistema de información para la atención de requerimientos de seguridad.

¿Con quién?

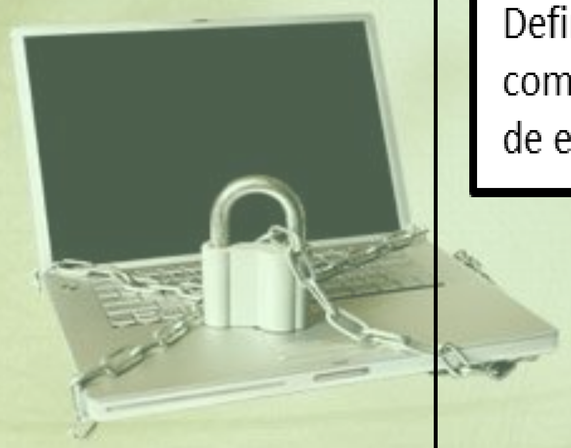
Involucrados:

- Alta Dirección
- Arquitecto
- Actores



SALIDAS

- Comunicación Top-Down
- Prioridades
- Compromisos
- Presupuesto de Inversión



Definición de flujo de comunicación y cumplimiento de expectativas.

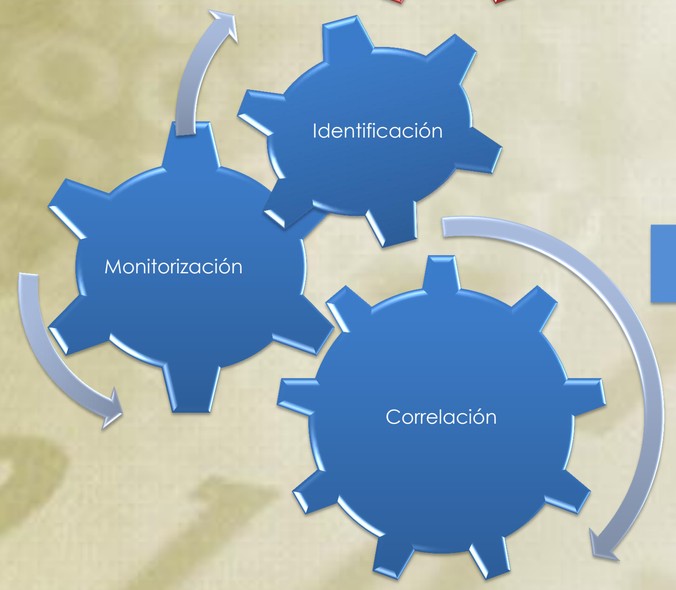
¿Cómo?

$$\frac{\text{Nº Proyectos Aprobados}}{\text{Nº Proyectos Sugeridos}}$$

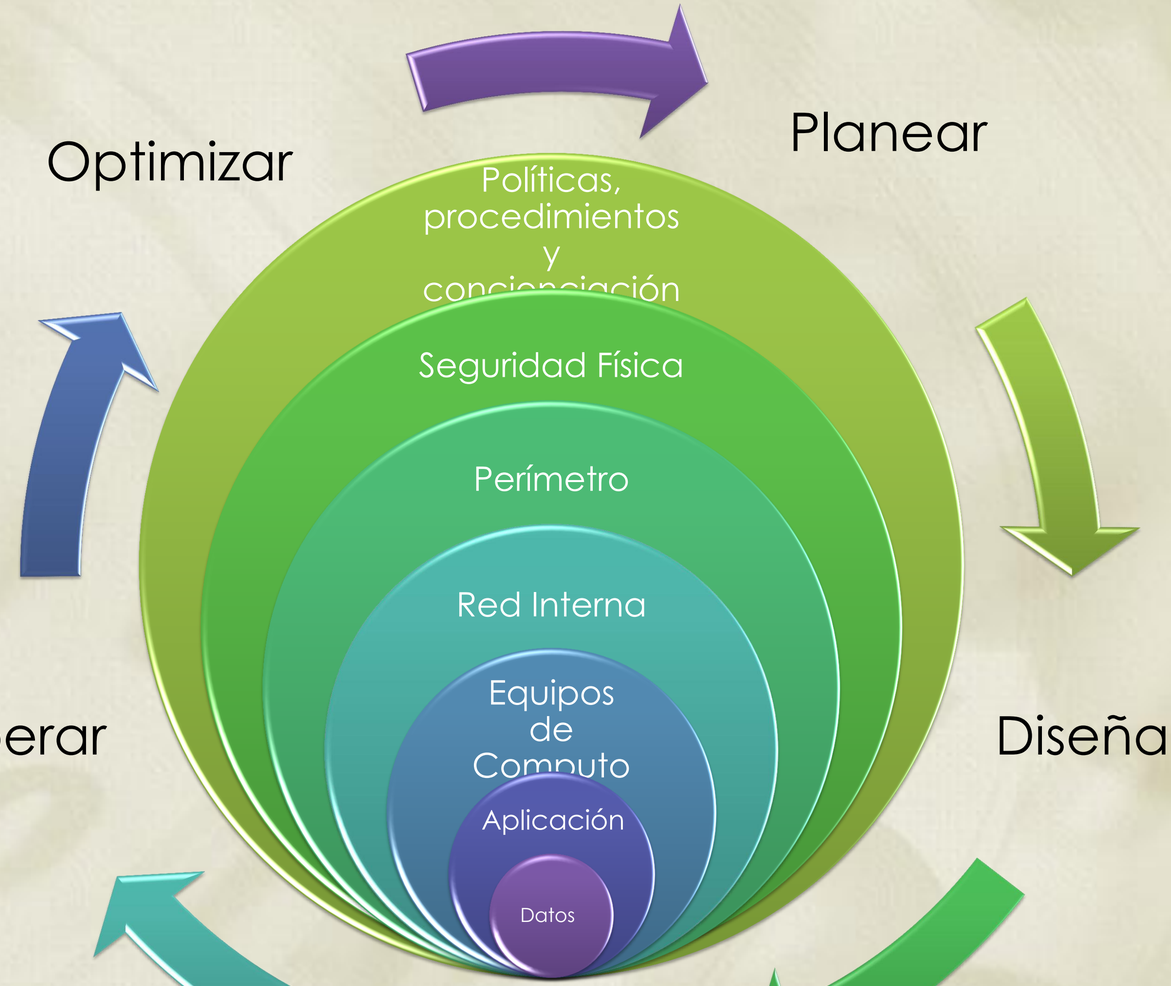
Indicadores

Infraestructura de Seguridad de la Información

Control



Visibilidad



Documentación los procedimientos de operación

Gestión de Conocimiento

Perímetro	Red Interna	Equipos de Computo	Aplicación	Datos
• Firewalls • Proxy (Reverso y Web) • IDS / IPS • VPN	• Seguridad de la Red • VLANs • NIDS / NIPS • DAC (ACLs) • SSL • SSH	• HIDS / HIPS • Actualización SO (parches) • Antivirus • Líneas Base • MAC (permisos)	• Firewall (WAF) • Buenas Prácticas de Programación • RBAC (perfiles)	• Cifrado • Prevención de fugas de Información • EFS • Borrado Seguro
Seguridad Física: CCTV, Smart Cards, Biométricos, Controles Ambientales (HVAC)				
Políticas, Procedimientos y Concienciación: Marco Normativo, Entrenamiento (Gestión de la Seguridad de la Información)				

Proceso Infraestructura

ENTRADAS (De otros procesos)

- Diagramas de red
- Diagramas de infraestructura tecnológica de seguridad
- Inventario de Activos
-

¿Con qué?

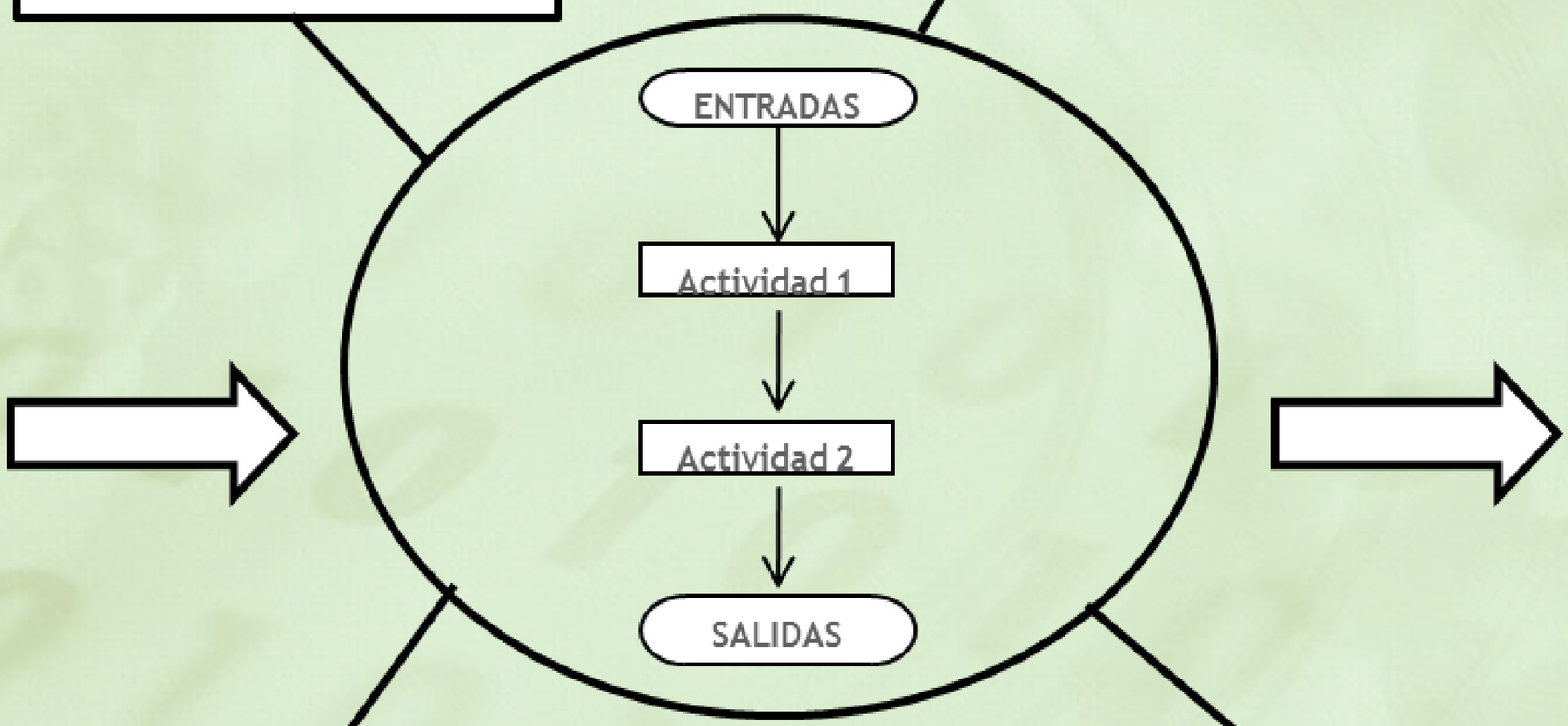
Sistema de información:

- Gestión de la plataforma tecnológica
- SLA

¿Con quién?

Involucrados:

- Arquitecto SI
- CISO
- CIO
- Proveedores



A nivel lógico y físico:

- Hardening
- Actualizaciones
- Expertos

¿Cómo?

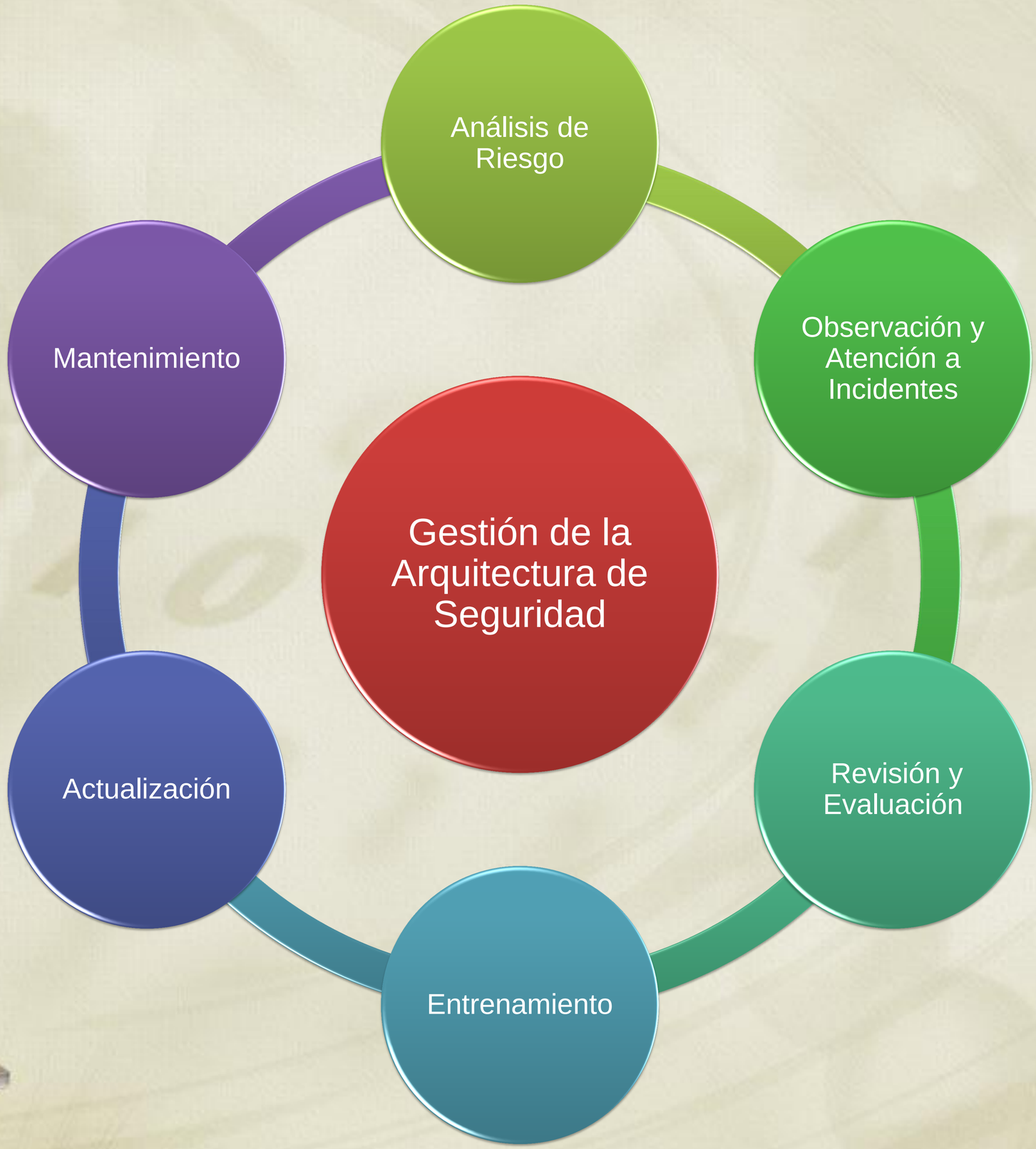
$$\frac{Nº\ Controles\ Ejecutados}{Nº\ Controles\ Implantados}$$

Indicadores

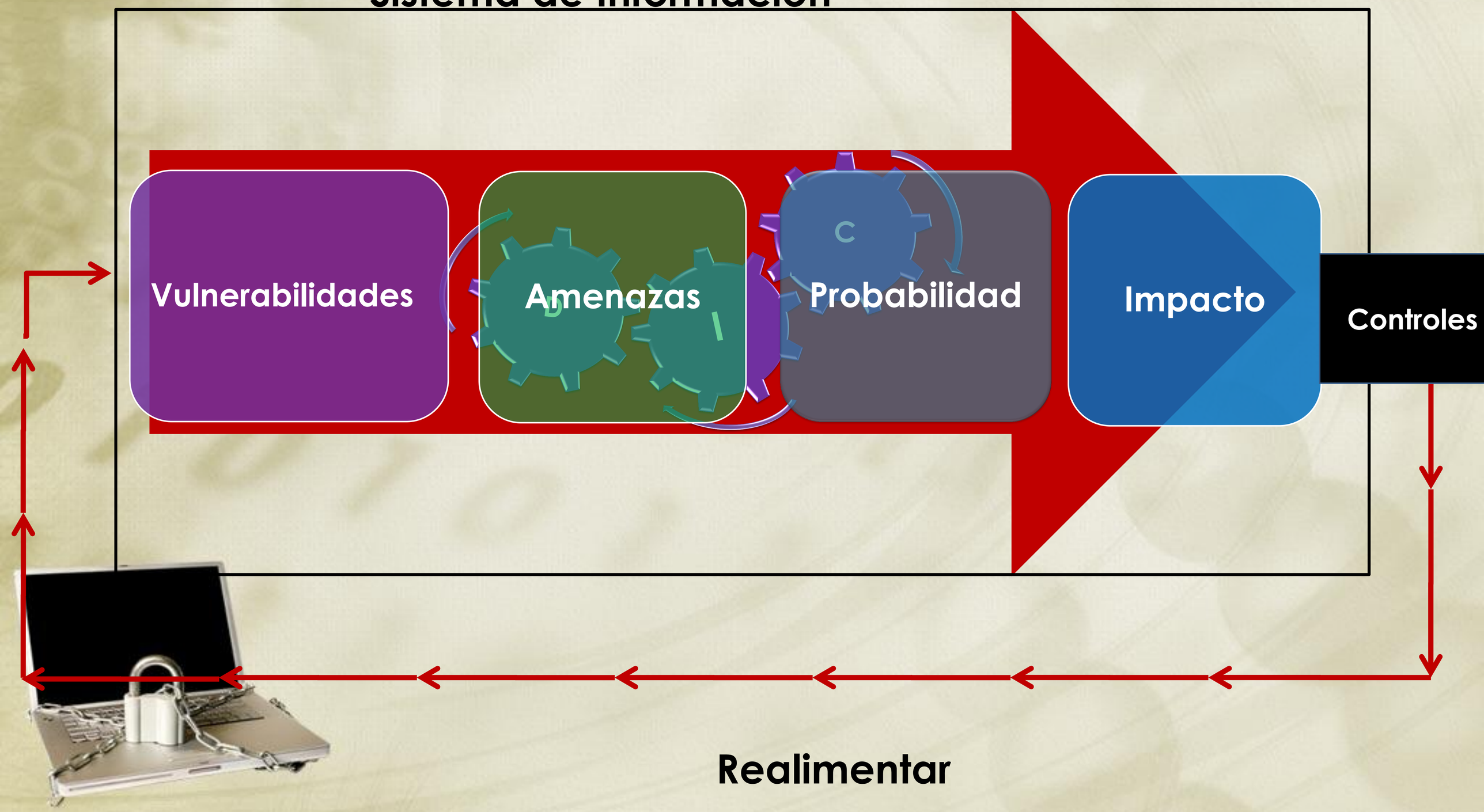
SALIDAS

. Nuevos requerimientos, procesos o elementos de MASI implantados.

Gestión de la Arquitectura de Seguridad de la Información



MASI: Gestión de la Seguridad (Análisis de Riesgos)



Proceso Gestión de Riesgo

ENTRADAS (De otros procesos)

- Inventario de activos de información
- Análisis de Riesgos
- Atención de incidentes

¿Con qué?

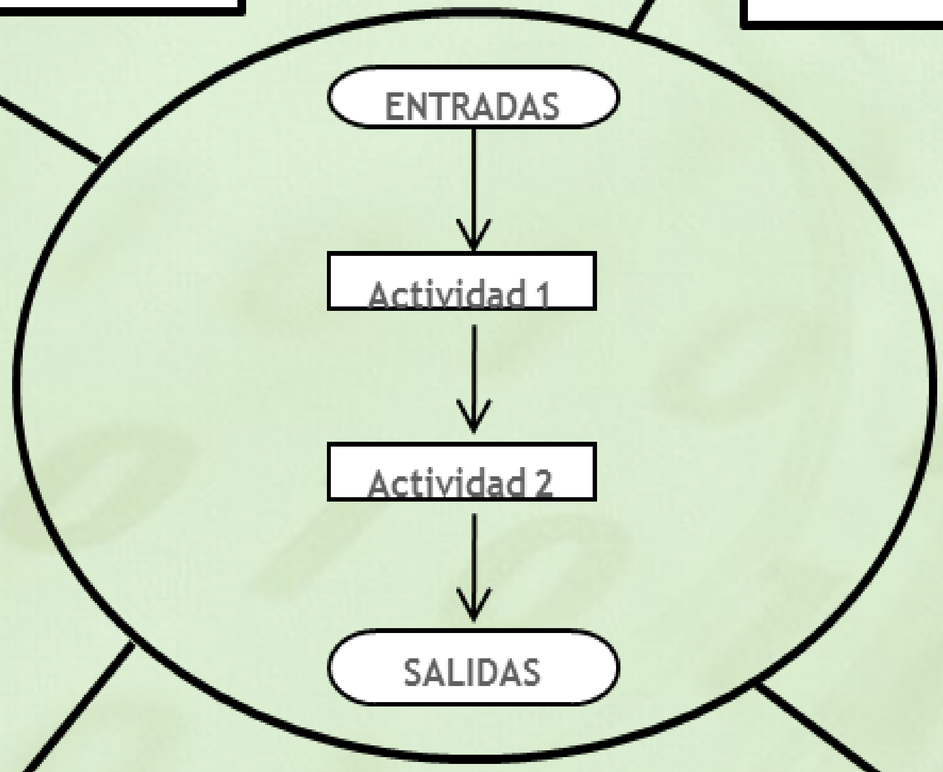
Sistema de información:

- Herramienta para la gestión de riesgos
- Herramienta de gestión de incidentes

¿Con quién?

Involucrados:

- Arquitecto SI
- CISO
- CIO
- Usuario



SALIDAS

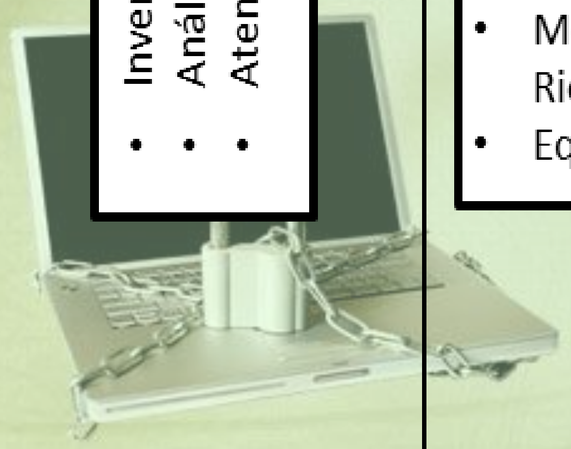
- Matriz de riesgos
- Planes de tratamiento para los riesgos
- Pólizas de seguro (riesgo transferido)

- Metodología para Análisis de Riesgos
- Equipo analista de riesgos

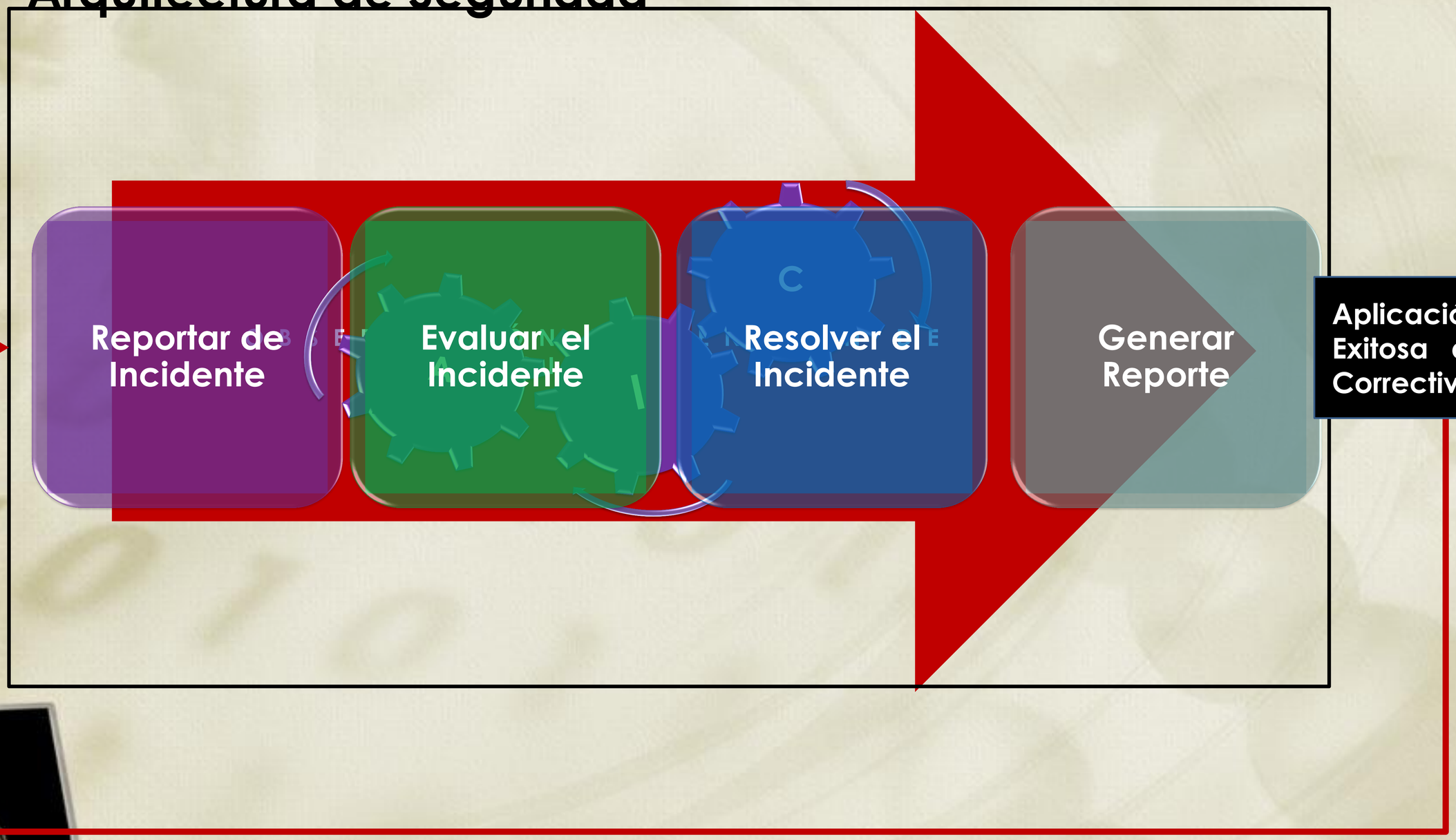
¿Cómo?

$$\frac{\text{Nº Controles Aprobados}}{\text{Nº Controles Sugeridos}}$$

Indicadores



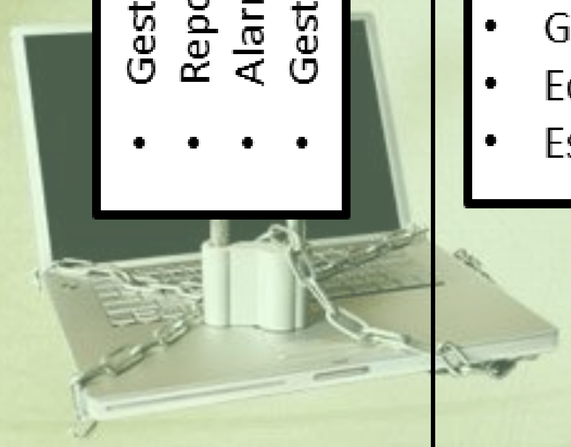
MASI: Gestión de la Seguridad (Observación y Atención de Incidentes)



Proceso Observación y Atención de Incidentes

ENTRADAS (De otros procesos)

- Gestión de riesgos
- Reporte de Incidentes
- Alarmas de equipos de seguridad
- Gestión de logs



¿Con qué?

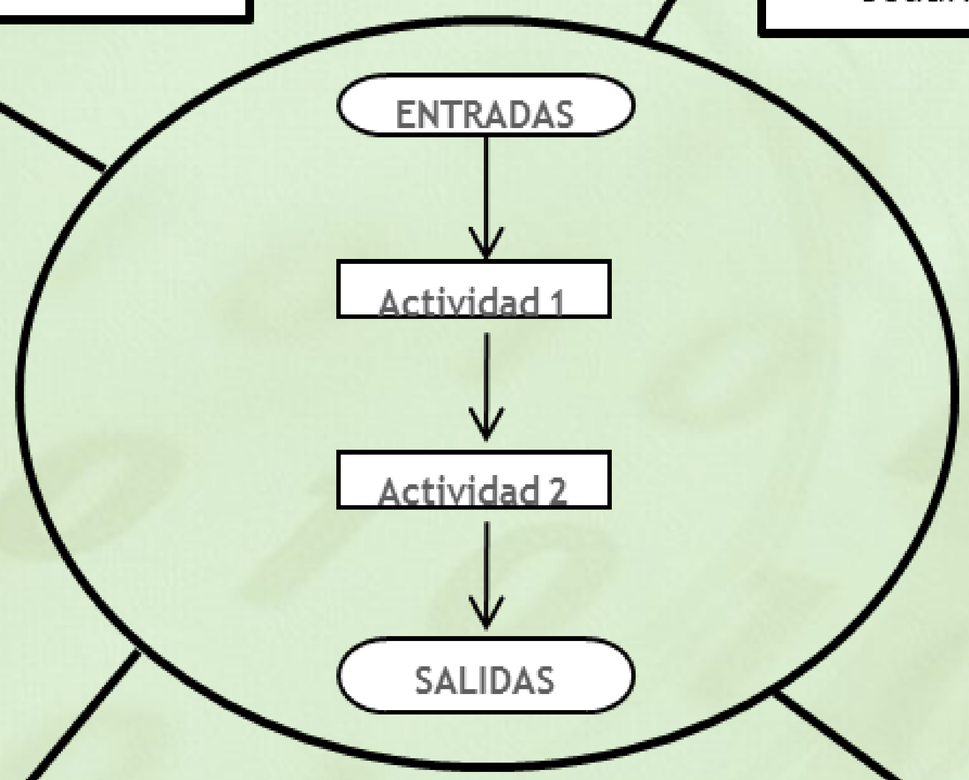
Sistema de información:

- Herramienta de atención de Incidentes
- Herramienta de gestión de log

¿Con quién?

Involucrados:

- Arquitecto SI
- CISO
- CIO
- Usuario



- Gestión de Riesgos
- Equipo de atención
- Escalar a la persona encargada

¿Cómo?

$$\frac{Nº\ Incidentes\ Solucionados}{Nº\ Incidentes\ Reportados}$$

Indicadores

SALIDAS

- Incidente atendido solucionado
- Informe con el reporte de la solución o atención del incidente

MASI: Gestión de la Seguridad (Revisión y Evaluación)

Proceso Revisión y Evaluación

ENTRADAS (De otros procesos)

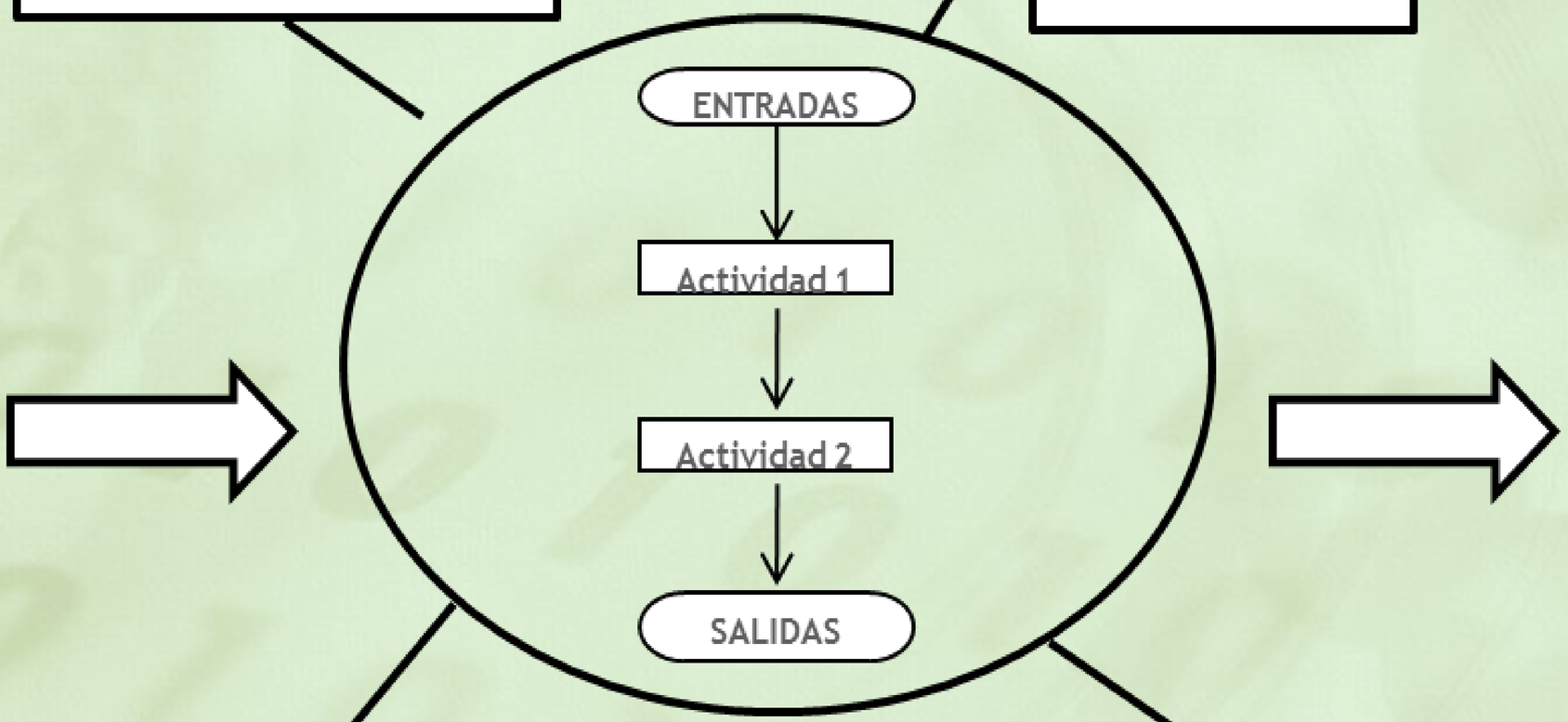
- Documentación de los elementos y procesos de MASI

¿Con qué?

Sistema de información:
- Encuestas
- Pruebas de Concepto

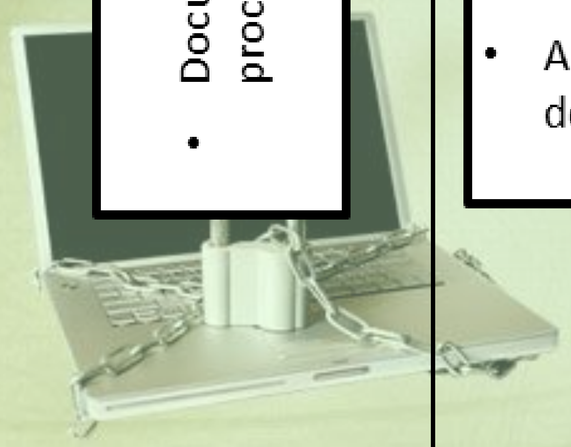
¿Con quién?

Involucrados:
- Arquitecto SI
- Alta Gerencia
- Auditor



SALIDAS

- Identificación de necesidades como oportunidad de mejora.



- Auditoria a los procesos y documentos de MASI

¿Cómo?

$$\frac{\text{Nº Doc. o Proc. para Actualizar}}{\text{Nº Doc. o Proc. Existentes}}$$

Indicadores

MASI: Gestión de la Seguridad (Entrenamiento)

Arquitectura de Seguridad

Entrenamiento

Generación de Expectativa

Necesidades

Plan de entrenamiento

Oportunidades de mejora

Realimentar

Proceso Entrenamiento

ENTRADAS (De otros procesos)

- Levantamiento de requerimientos según expectativas
- Análisis GAP de conocimiento
- Política, Directrices, Normas y Procedimientos
-

¿Con qué?

Sistema de información:

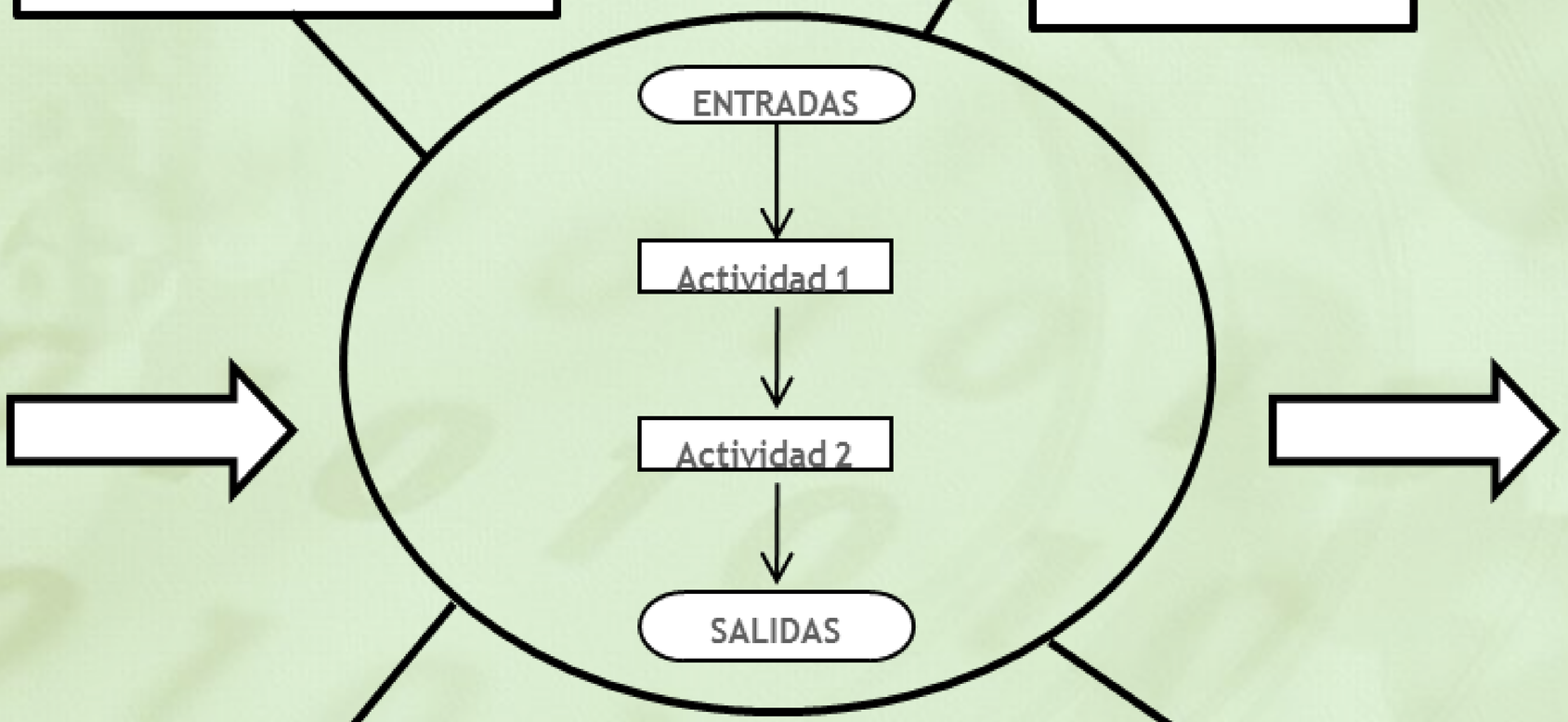
- Portal Web
- Correo electrónico

Otros Medios

¿Con quién?

Involucrados:

- Arquitecto SI
- Alta Gerencia
- Comunicaciones



- Charlas
- Cursos
- Seminarios

¿Cómo?

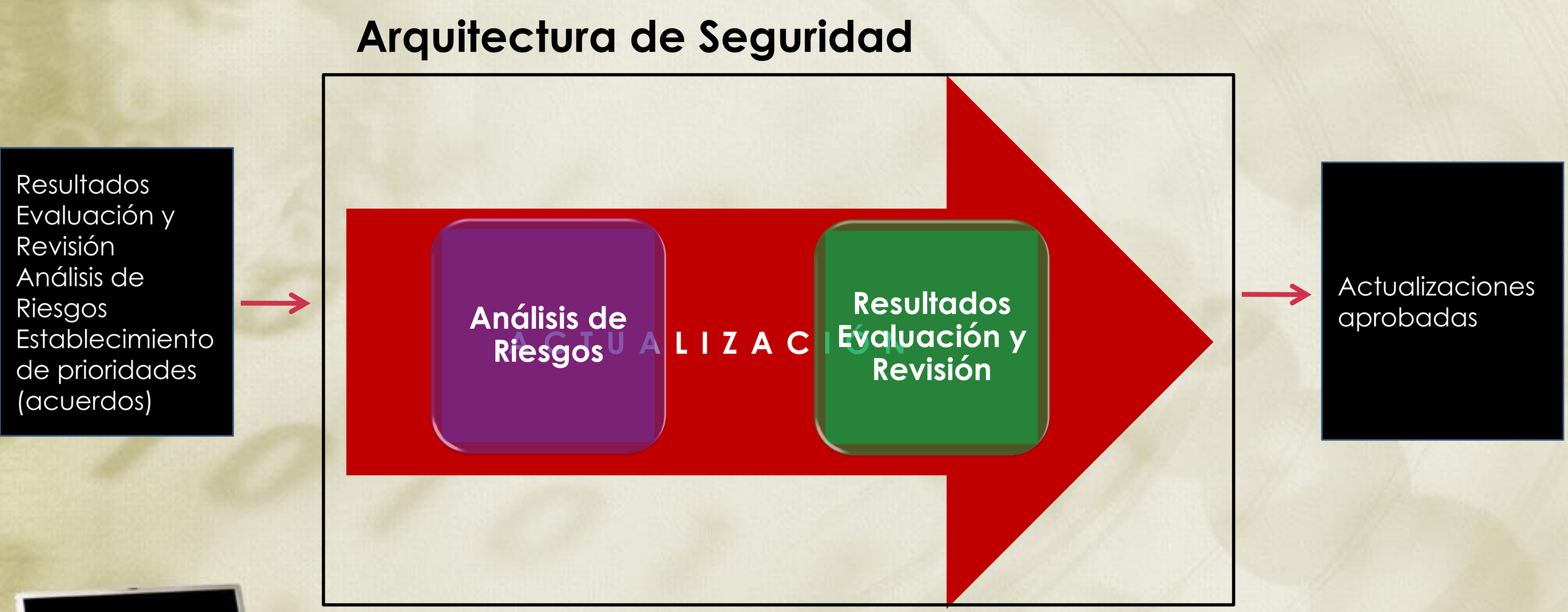
$$\frac{Nº\ Asistentes}{Nº\ Actores} * \frac{Nº\ Horas\ Cap.}{Nº\ Hrs.Asistidas}$$

Indicadores

SALIDAS

- Actores (alta gerencia, jefes de unidad, usuario final, clientes, interesados) capacitados y sensibilizados,
-

MASI: Gestión de la Seguridad (Actualización)



Proceso Revisión y Evaluación

ENTRADAS (De otros procesos)

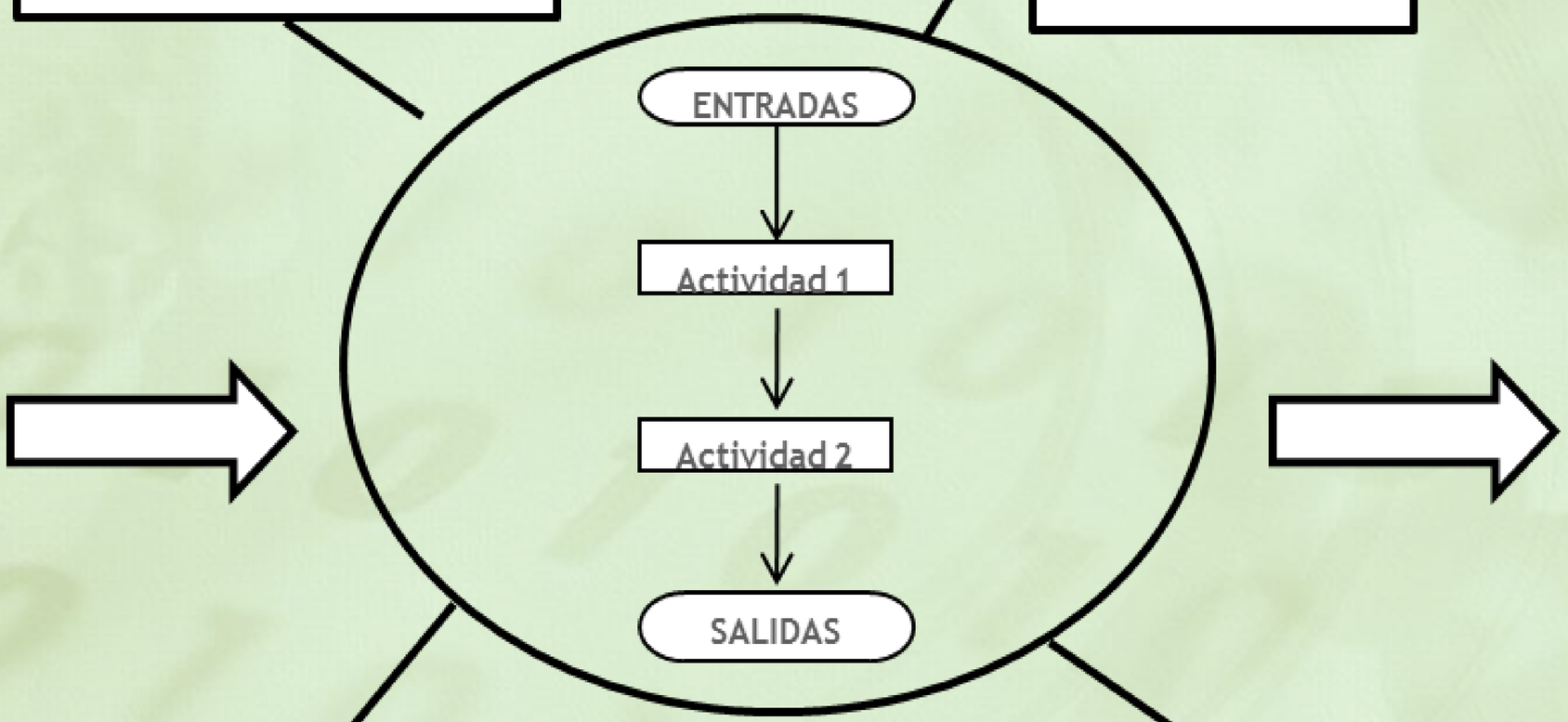
- Documentación de los elementos y procesos de MASI

¿Con qué?

Sistema de información:
- Encuestas
- Pruebas de Concepto

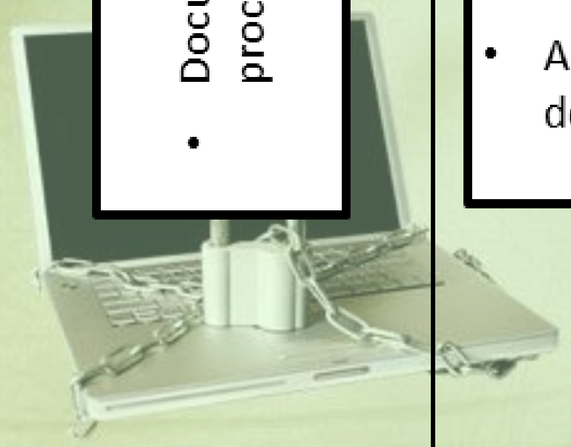
¿Con quién?

Involucrados:
- Arquitecto SI
- Alta Gerencia
- Auditor



SALIDAS

- Identificación de necesidades como oportunidad de mejora.



- Auditoria a los procesos y documentos de MASI

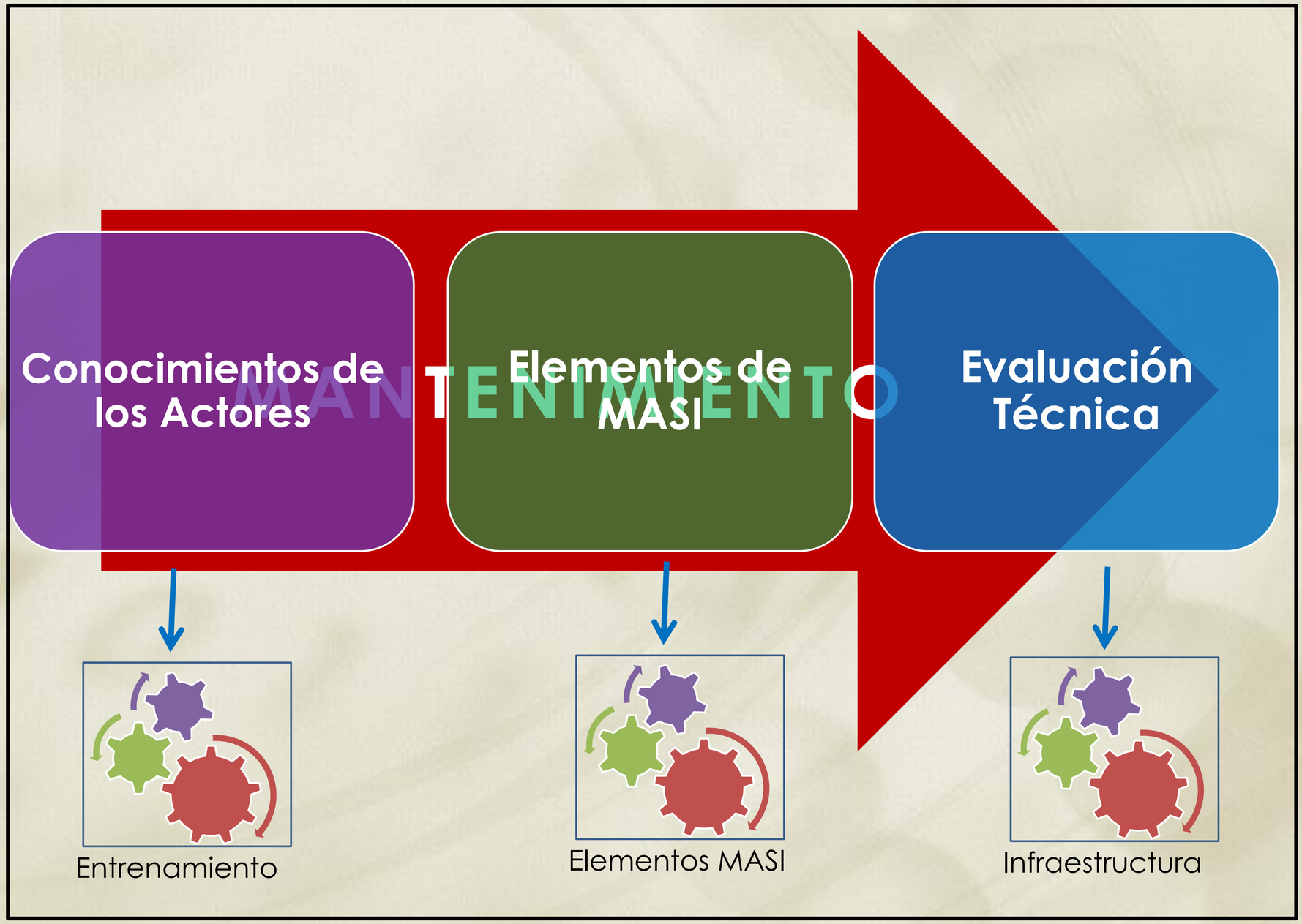
¿Cómo?

$$\frac{\text{Nº Doc. o Proc. para Actualizar}}{\text{Nº Doc. o Proc. Existentes}}$$

Indicadores

MASI: Gestión de la Seguridad (Mantenimiento)

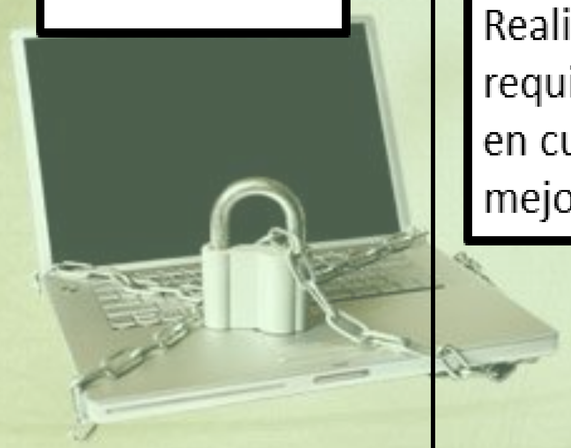
Arquitectura de Seguridad



Proceso Mantenimiento

ENTRADAS (De otros procesos)

- Actualizaciones Aprobadas
- Tiempos de implementación
- Presupuesto de Inversión



¿Con qué?

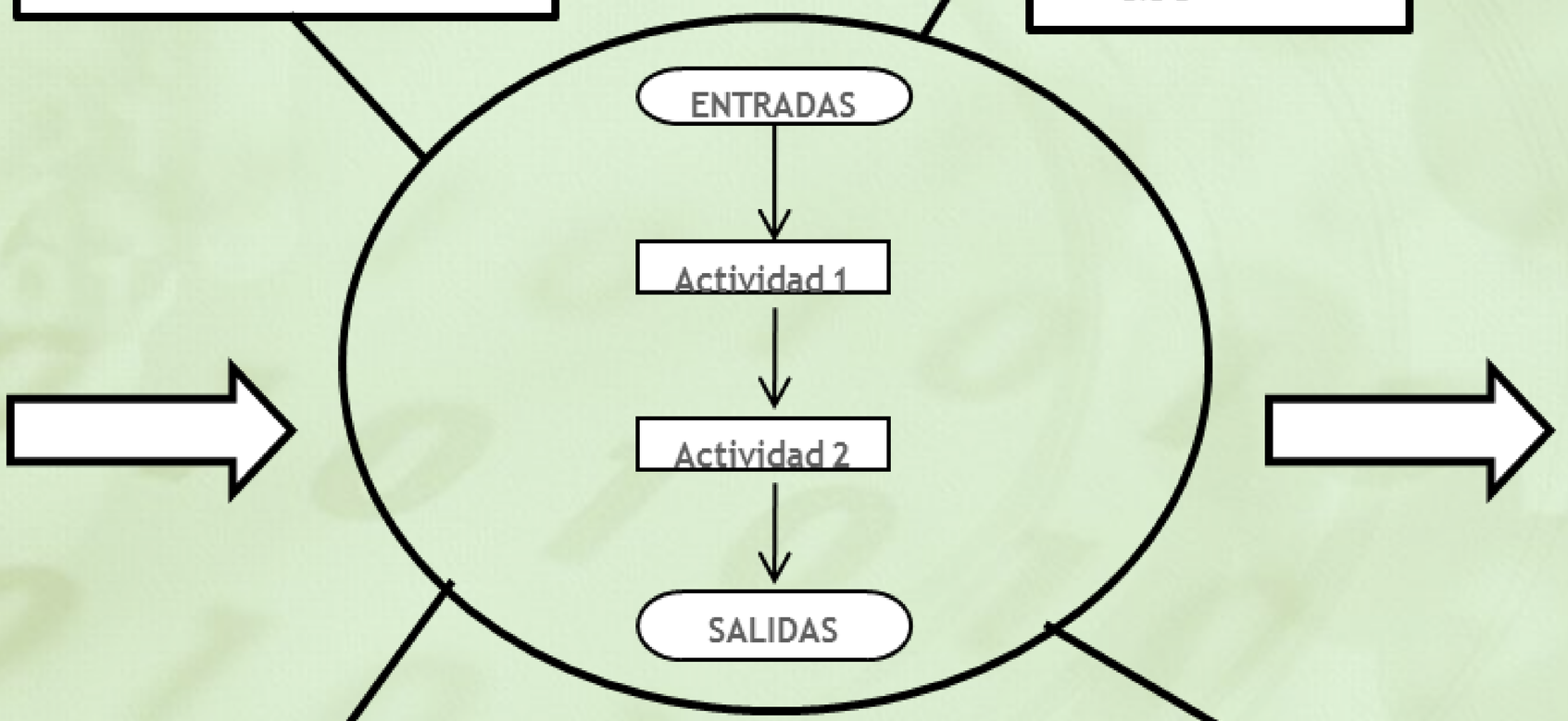
Sistema de información:

- Gestión de MASI
- GDSS o EIS
- Inversión ejecutada

¿Con quién?

Involucrados:

- Arquitecto SI
- Alta Gerencia
- Jurídica
- CISO



¿Cómo?

Realizar las actualizaciones que requiere la arquitectura teniendo en cuenta las oportunidades de mejora identificadas.

Indicadores

$$\frac{\text{Nº Actualizaciones Aprobadas}}{\text{Nº Actualizaciones Implantadas}}$$

SALIDAS

Nuevos requerimientos, procesos o elementos de MASI implantados.

7 × 24 × 365 = Cont. De Negocio

Proceso Gestión Continuidad del Negocio

ENTRADAS (De otros procesos)

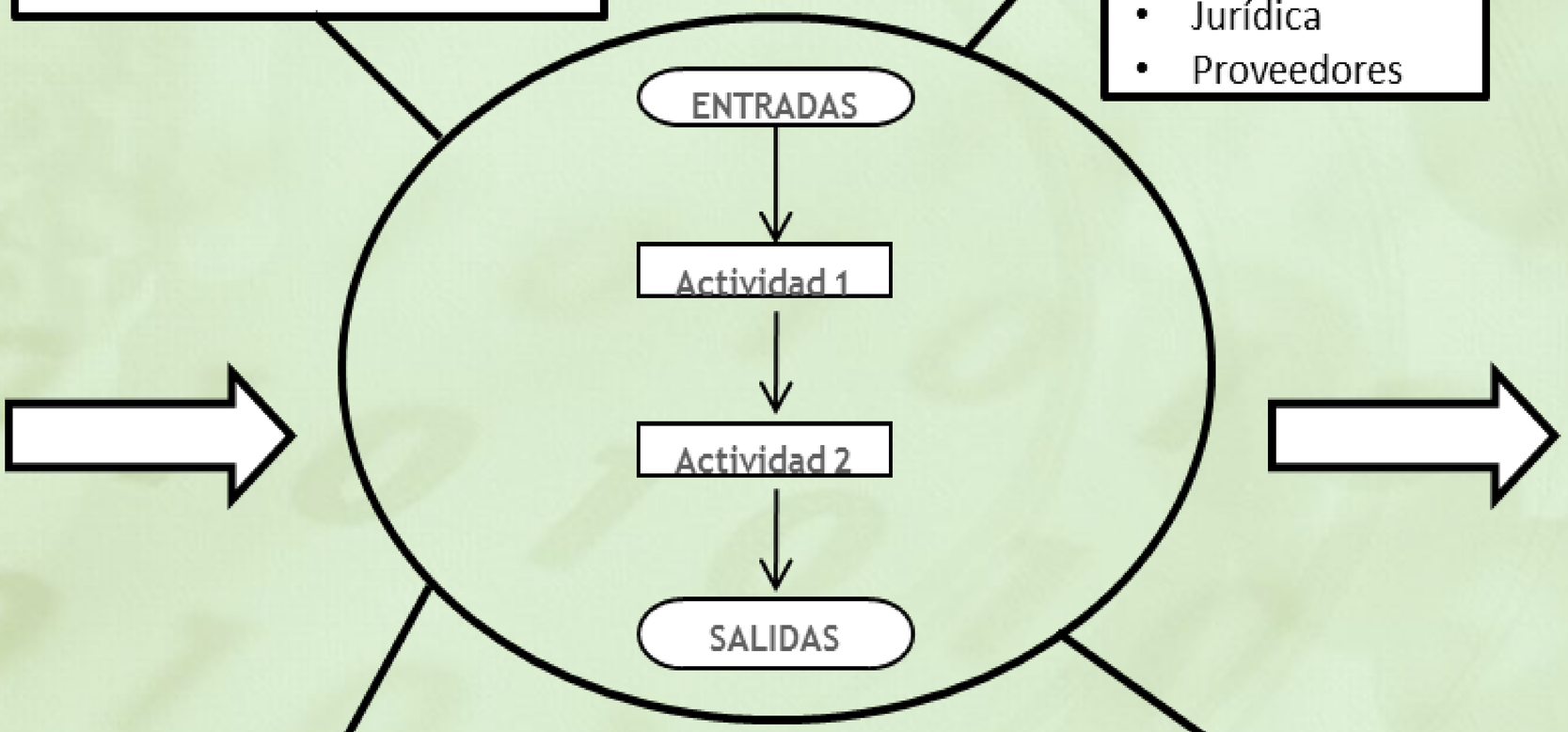
- Análisis de Riesgos
- Análisis del Impacto al Negocio
- Plan de Recuperación ante Desastres
- Mapa de procesos

¿Con qué?

Replicación:
- Física → Infraestructura SI
- Lógica → Servicios
- Seguros

¿Con quién?

Involucrados:
- Alta Gerencia
- Arquitecto
- CISO
- CIO
- Jurídica
- Proveedores



SALIDAS

- Maximizar el tiempo de interrupción
- Identificación de procesos críticos
- Plan de implementación y pruebas del proceso
-

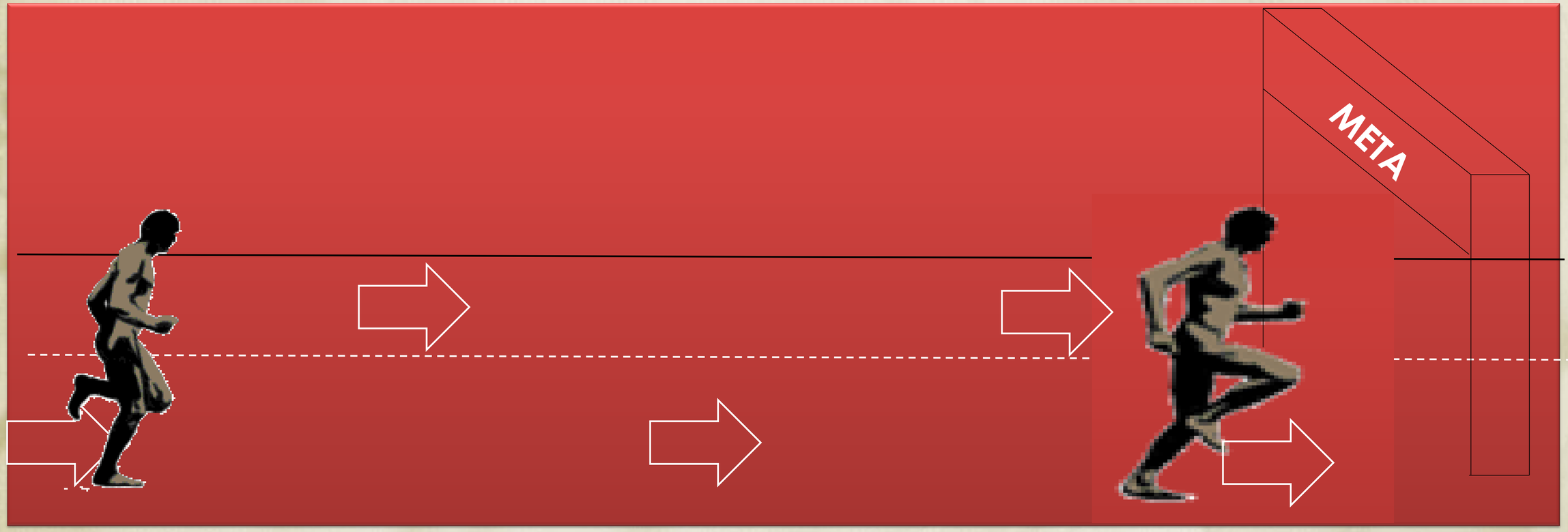
Definición de Planes:
- Continuidad de la operación de los procesos
- Continuidad de la operación de la plataforma tecnológica

¿Cómo?

$$\left(\frac{Nº\ Proyectos\ Propuestos}{Nº\ Proyectos\ Aprobados}\right) * \left(\frac{Recursos}{Tiempo}\right)$$

Indicadores

Metodología → El cómo…



Se puede definir la metodología como una serie de pasos ordenados que van a permitir seguir un camino para lograr determinado fin [19].

Conclusiones

La gestión del modelo de arquitectura de seguridad de la información permite el mejoramiento continuo de los diferentes elementos que lo componen, por tanto es indispensable que las actividades definidas en el mismo se ejecuten de manera sistemática.

Conclusiones

MASI permite establecer el canal de comunicación necesario para alinear la agenda interna de la Alta Gerencia con la del Arquitecto de SI, con el ánimo de atender las necesidades e invertir en los asuntos concernientes a la Seguridad de la Información.

Recomendaciones

Incentivar en todos los actores (usuarios, proveedores, clientes, entre otros,) el cumplimiento de la normativa, así como la colaboración para lograr un ambiente adecuado para el funcionamiento de la arquitectura de seguridad de la información y los procesos de la misma.

Recomendaciones

Definir reuniones de seguimiento en intervalos planificados para la realimentación de la Arquitectura de Seguridad de la Información, de tal manera que se pueda revisar que lo definido ha sido o no acertado para el mejoramiento continuo tanto del negocio como de la Arquitectura de Seguridad de la información.

Recomendaciones

Desarrollar un plan de trabajo mancomunado entre las Directivas y el Arquitecto de Seguridad de la Información, que permita la inclusión y priorización de los temas concernientes a la Seguridad de la Información, y con ello materializar el compromiso y los niveles de inversión que está dispuesta a asumir la Alta Gerencia con respecto a la Seguridad de la Información y el funcionamiento del MASI.

Preguntas????

Referencias

[1]INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. NTC-ISO/IEC 27002. Bogotá. ICONTEC, 2007.

[2] CANO, Jeimy. Arquitecturas de Seguridad Informática: *Entre la administración y el gobierno de la Seguridad de la Información*. En: SEMINARIO DE ACTUALIZACIÓN EN SEGURIDAD INFORMÁTICA. (2008: Bucaramanga). Documento Modulo I Seminario de Actualización en Seguridad Informática. Bucaramanga: Facultad de Ingeniería Informática, 2008, p 28.

[3]KILLMEYER, Jan. Information Security Architecture: An Integrated Approach to Security in the Organization. 2ª edición. Estados Unidos: Auerbach, 2006. 393p

[4] IYER, Bala. GOTTLIEB, Richard. The Four-Domain Architecture: An approach to support enterprise architecture design. *Julio 21 de 2004*.Disponible en Web: http://www.research.ibm.com/journal/sj/433/iyer.html

[5] INTERNATIONAL PROFESSIONAL ASSOCIATION THAT DEALS WITH IT GOVERNANCE. COBIT 4.1. Estados Unidos. ISACA, 2007.

[6] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. NTC-ISO/IEC 27001. Bogotá. ICONTEC, 2006.

[7] SysAdmin Audit, Networking and Security Institute. Information Systems Security Architecture: A Novel Approach to Layered Protection. Estados Unidos. SANS, 2004.

[8] PARADA, Diego. CALVO, July. Diseño de la arquitectura de seguridad de la red de la Universidad Pontificia Bolivariana. Bucaramanga, 2008, 219p. Proyecto de grado (Ingeniería en Informática). Universidad Pontificia Bolivariana. Facultad de Ingeniería Informática.

[9] "Definición de Metodología", Enero de 2010. Disponible: http://definicion.de/metodologia/