UNIVERSIDAD DE LIMA | 60 años

Conceptos generales (II)

Seguridad de Sistemas de TI
2022-1

Agenda

I. Arquitectura de Seguridad de la Información

II. Gobierno, Gobierno de TI, Gobierno de Seguridad de la Información

III. Estrategia de Seguridad de la Información

IV. Conclusiones

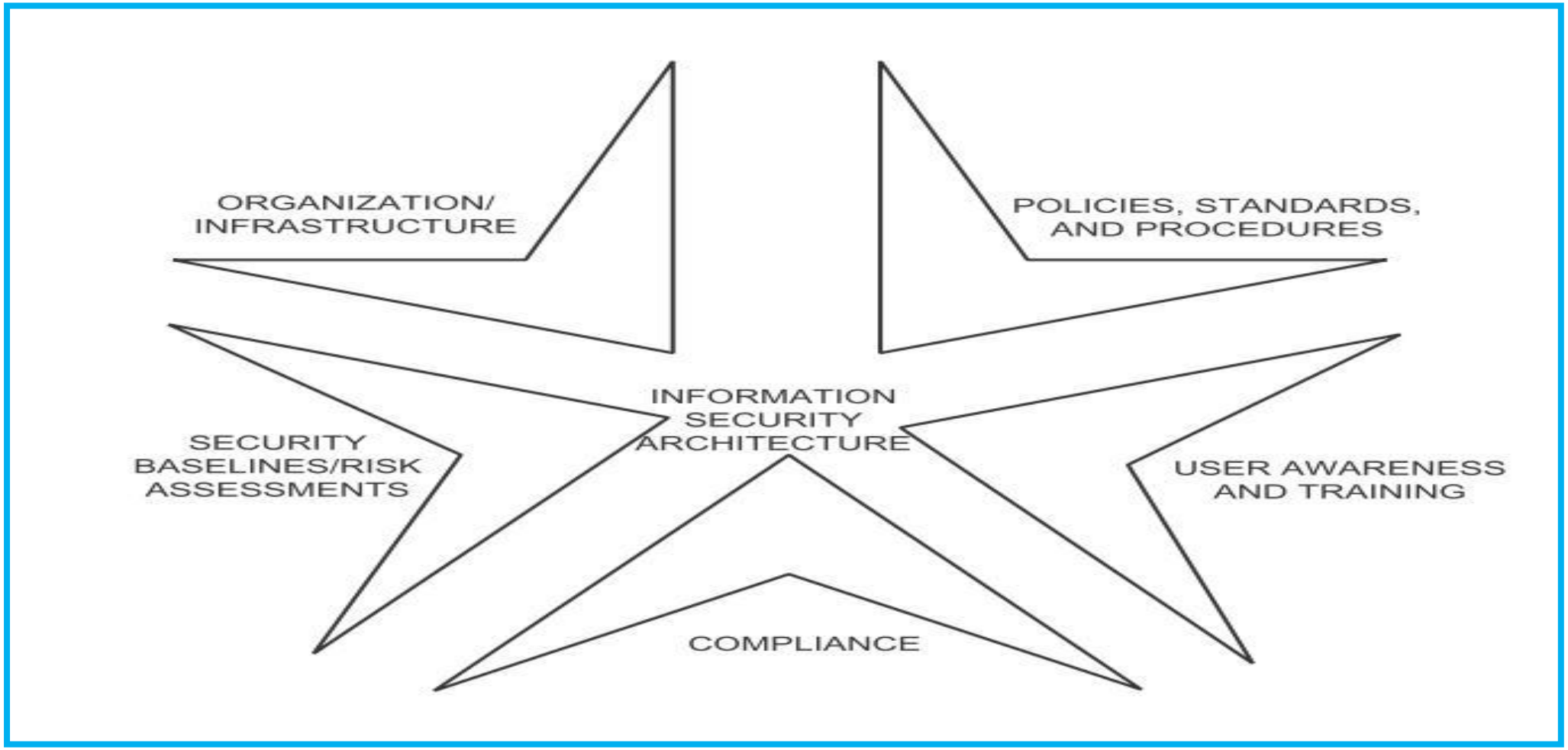
UNIVERSIDAD DE LIMA

I. Arquitectura de la seguridad de la información

Elementos de la Arquitectura de la Seguridad de la Información

1) Organización de la Seguridad / Infraestructura
2) Políticas, estándares y procedimientos de la seguridad
3) Línea base de la seguridad / Evaluación de riesgos
4) Programas de concientización y entrenamiento en seguridad
5) Cumplimiento

Arquitectura de la Seguridad de la Información (componentes)



UNIVERSIDAD DE LIMA

Organización de la Seguridad / Infraestructura

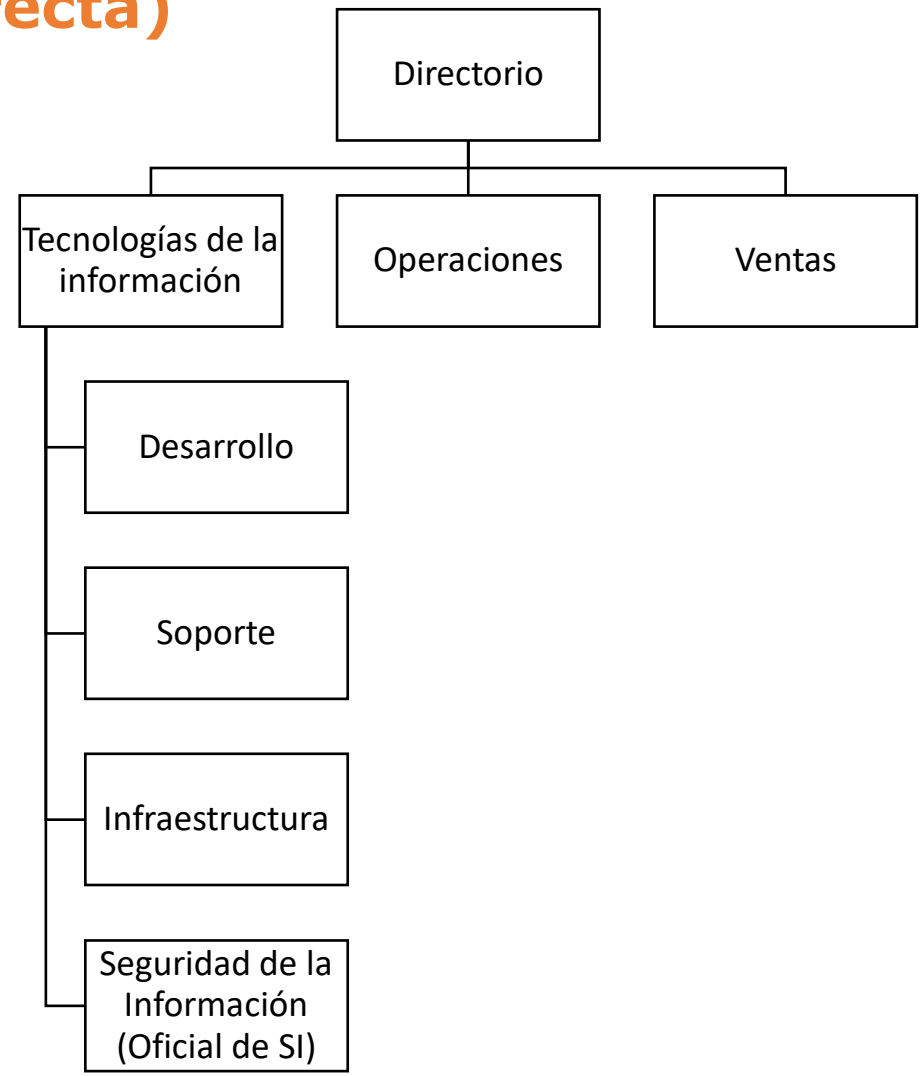
- Dentro del negocio debe haber una **Organización** con la responsabilidad de la Gestión de la Seguridad de la Información
- En lo más alto, el **Comité Directivo de la Seguridad de la Información**, responsable de proveer dirección estratégica y recursos para los componentes necesarios de la ASI

La Organización de la Seguridad

- El equipo que participa en la función de seguridad dependerá de varios factores:
  - Tamaño de la empresa
  - Entorno (centralizado vs. distribuido)
  - Estructura organizacional y administrativa
  - ¿Cómo están interconectadas las sedes?
  - Riesgo evaluado
  - Plan estratégico de TI
  - Presupuesto de TI

Ubicación del Oficial de Seguridad

(típica, pero no correcta)



UNIVERSIDAD DE LIMA

Madurez de la Organización de la Seguridad (I)

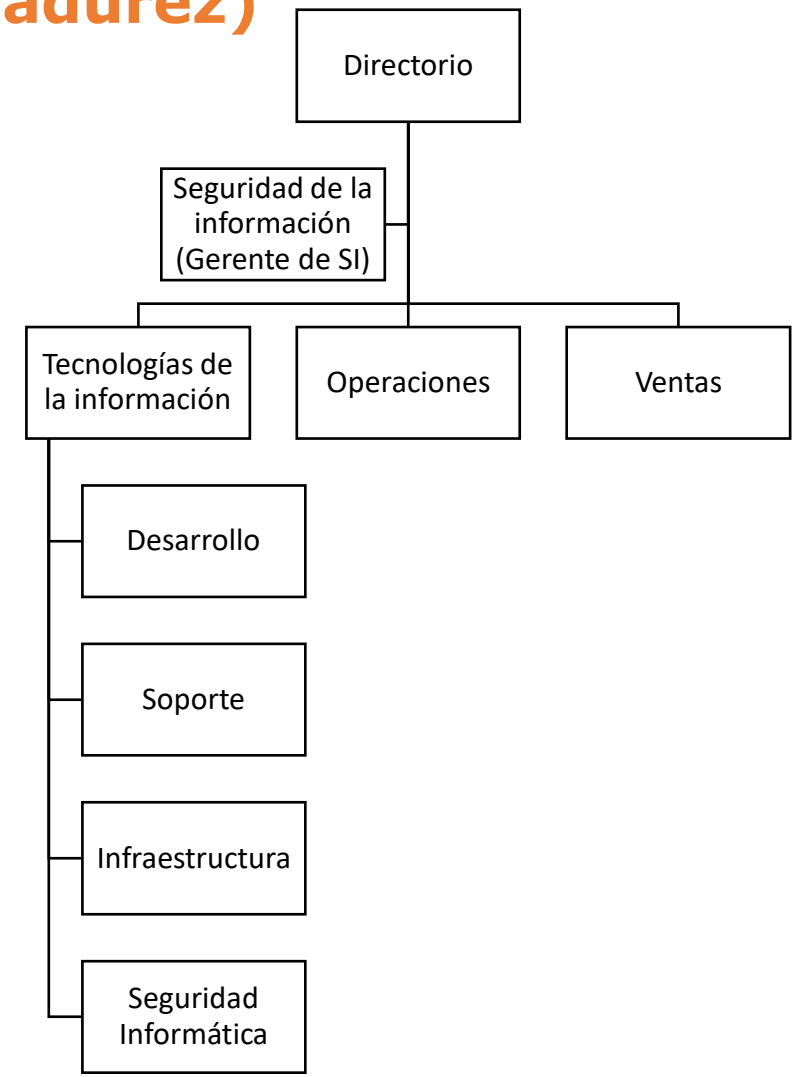
- La función principal del Gerente/Oficial de seguridad no es llevar a cabo funciones relacionadas a la seguridad, sino **asegurar que los esfuerzos de seguridad sean coordinados; que las políticas, procedimientos y estándares sean desarrollados y seguidos; y que el programa de seguridad sea implementado** efectivamente y actualizado de acuerdo a los cambios en el entorno de procesamiento y negocio

Madurez de la Organización de la Seguridad (II)

- El Gerente/Oficial de seguridad debe reportar a la administración de nivel ejecutivo (miembro del comité directivo de la seguridad de la información)
- Cuando la arquitectura de seguridad de la información ha madurado a través de varios ciclos de evaluación, mitigación, auditoría y cumplimiento efectivo, el rol de Gerente/Oficial de seguridad ***debe ser retirado*** del área de SI/TI y **reportar directamente al presidente, CEO, ó Junta de directores**

UNIVERSIDAD DE LIMA

Ubicación del Gerente/Oficial de Seguridad (Correcta, en una empresa con madurez)



UNIVERSIDAD DE LIMA

El Gerente/Oficial de Seguridad de la información

- En la década pasada casi todas las organizaciones crearon un puesto de Gerente y/o Oficial de seguridad de la información en algún nivel de la organización
- Cada día es mayor el número de organizaciones que crean departamentos centrales de seguridad de la información con el fin de resolver la creciente complejidad para proteger no solo los sistemas de TI sino toda la información sensible y crítica que de cualquier forma se procesa y manipula

¿Qué es una Política?

- Una política se diseña para informar a todos los individuos que operan en una **organización cómo deben comportarse con respecto a un tópico específico**, cuál es la posición de la dirección ejecutiva con respecto a ese tópico, y qué acciones específicas está preparada para tomar la organización en relación a dicho tópico
- Responden a las preguntas ¿Quién?, ¿Qué? y ¿Porqué?

UNIVERSIDAD DE LIMA

Políticas de Seguridad de la Información

- **Documento de Políticas de Seguridad**
  - Debe ser aprobado por la administración, publicado y comunicado a todos los empleados.
- **Revisión y Evaluación**
  - La política debe ser administrada por una persona quién es responsable de su mantenimiento y revisión de acuerdo a un proceso definido.

Justificación de una Política de Seguridad

- Establece **lo que se puede hacer y lo que no**, de forma escrita y formal. Se puede leer y es algo escrito y aceptado.
- Demuestra que la empresa se lo quiere tomar en serio. Implica un **compromiso con los directivos**.
- Útil frente a una auditoría, sobre todo si se siguen las normalizaciones.
- Útil para demostrar casos de intrusiones o delitos contra los sistemas informáticos.

Modelo de Política de Seguridad (I)

- Requerimientos de Seguridad de la Información para **adquisición de nuevo hardware.**
- ¿Qué consideraría Usted?

Policy 010101
Specifying Information Security Requirements for New Hardware

SUGGESTED POLICY STATEMENT

"All purchases of new systems hardware or new components for existing systems must be made in accordance with Information Security and other organisation Policies, as well as technical standards. Such requests to purchase must be based upon a User Requirements Specification document and take account of longer term organisational business needs."

EXPLANATORY NOTES

The purchase of new computers and peripherals requires careful consideration of your business needs because it is usually expensive to make subsequent changes.

Information Security issues to be considered when implementing your policy include the following:

- The system must have adequate capacity or else it may not be able to process your data.
- Data must be adequately protected; otherwise there is a risk of loss or accidental / malicious damage.
- Where hardware maintenance is poor or unreliable, you greatly increase the risk to the organisation, because, in the event of failure, processing could simply STOP.
- The system must be sufficiently 'resilient' to avoid unplanned *down-time*, which can have an immediate negative impact on your organisation.

Modelo de Política de Seguridad (II)

- Requerimientos para ingresar **(log-in)** y salir de su computador **(log-off)**.
- ¿Qué consideraría Usted?

Policy 010706
Logon and Logoff from your Computer

SUGGESTED POLICY STATEMENT

"Approved login procedures must be strictly observed and users leaving their screen unattended must firstly lock access to their workstation or log off."

EXPLANATORY NOTES

The access to the vast majority of systems is via a logon process. The security of the system is therefore highly dependant on suitable logon and logoff procedures. See also *Access Control*.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised access to systems may be gained via a valid user ID and password if these are not kept secure.
- Incorrect logon scripts and access rights may allow access to unauthorised areas.
- Unauthorised access to files may result in the confidentiality of data being compromised.
- Where the 'User Logon Register' or operator / administrator logs show incorrect or unusual entries, it could indicate that data has been accessed and therefore possibly lost or stolen.
- You may be unable to logon to the system and denied service.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.3.1(c) Clear desk and clear screen policy
9.2 User access management

Modelo de Política de Seguridad (III)

- Requerimientos de Seguridad de la Información para el **uso de computadoras portátiles.**
- ¿Qué consideraría Usted?

UNIVERSIDAD DE LIMA

Policy 010403
Using Laptop/Portable Computers

SUGGESTED POLICY STATEMENT

"Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks."

EXPLANATORY NOTES

Laptops and Portables have unique security issues, primarily because of their size and mobility.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data disclosed to unauthorised persons can damage the organisation.
- A virus threatens not only the data but also the system files on the laptop.
- A laptop connected to any network is open to hacking and is unlikely to have any effective security features enabled. Files and data could be stolen, damaged, or corrupted.
- A laptop left 'on' may be easy prey to opportunist access, despite your use of (say) a user password etc.
- Theft of a laptop computer usually results in additional cost to the organisation and potential loss of confidential data.
- Where a laptop is used by persons with differing *access control* privilege, residual data and / or other information could compromise the confidentiality of your information.
- When vital updates to the data files are lost or corrupted due to technical or user problems during transfer, the integrity of the entire database of records may be in question.
- Where a laptop is used by several persons, old / 'stale' data may still be present, risking unintentional actions / reactions to inaccurate data.

Políticas, estándares y procedimientos de la seguridad

- Se tiene que discutir los requerimientos, desarrollo é implementación de políticas, estándares y procedimientos de seguridad

¿Qué es un Estándar?

- Un estándar consiste en un **conjunto de reglas, procedimientos ó convenciones** que son acordados y aceptados por varias partes a fin de operar más **uniformemente y efectivamente.**
- Los estándares establecen un nivel de expectativa que debe ser alcanzado ó superado para cumplir con nuestras obligaciones y responsabilidades.

UNIVERSIDAD DE LIMA

¿Qué es un Procedimiento?

- Los procedimientos son **planes, procesos ú operaciones** que tratan el detalle de cómo llevar a cabo una acción particular.
- Permiten la transferencia de conocimiento entre individuos que realizan el mismo trabajo, que reemplazan a otros en períodos de ausencia, ó permiten una transmisión más "suave" y controlada durante cambios permanentes del staff.
- Responden las preguntas ¿Dónde?, ¿Cuándo? y ¿Cómo?

UNIVERSIDAD DE LIMA

Línea base de la Seguridad / Evaluación de Riesgos

- Para comprender el nivel de riesgo que existe en un ambiente operativo, se deben llevar a cabo evaluaciones periódicas de riesgo.
- Tanto **vulnerabilidades** como **agujeros de seguridad** y **puertas traseras** son descubiertas frecuentemente.
- Cuando se implementa un nuevo sistema se debe hacer una evaluación preliminar, denominada línea base de seguridad. Esta brinda un **punto de medida para los cambios** en configuración y mejoras del sistema.

Programas de concientización y entrenamiento en seguridad

- La concientización y el entrenamiento son quizás los elementos más significativos en un **programa de seguridad de la información**.
- Están diseñados para ayudar a **reducir el riesgo** de pérdida de propiedad intelectual y recursos de procesamiento.
- La responsabilidad de proteger estos recursos es transferida a cada individuo de la organización a través de estos programas.
- Deben abarcar varios frentes y ser consistentes con la cultura organizacional (y ser divertidos!!!)

UNIVERSIDAD DE LIMA

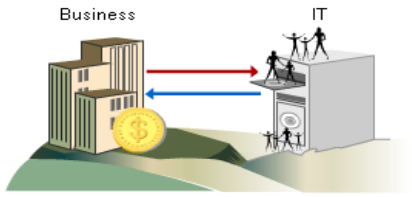
Cumplimiento

- El Cumplimiento mide el **grado en el cual las políticas, estándares y procedimientos definidos están siendo seguidos.**
- El cumplimiento incluye la **auditoría**, **monitoreo** é **investigación** en diferentes niveles de la organización.
- Ayuda a verificar que los controles preventivos y detectores están en su lugar y que están siendo empleados efectivamente.

UNIVERSIDAD DE LIMA

II. Gobierno

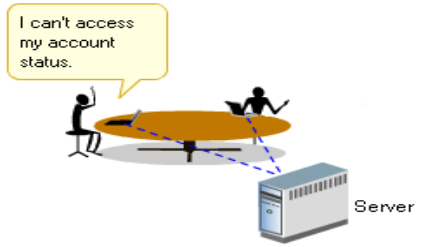
¿Por qué Gobierno de TI ?

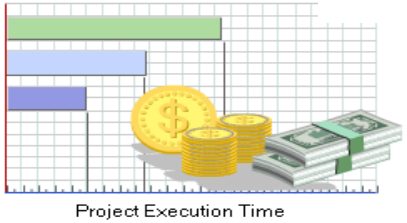


Strategic Alignment

Poor Security Assurances

Seguridad





Valor/Costo

Alinear T
Nego

Handling External Relationship

IS
e TI

Cumplir con
Requerimientos
Regulatorios

Las organizaciones requieren una aproximación estructurada para administrar estos y otros cambios.

Esto garantizará que existan objetivos acordes para TI, buenos controles de administración y un monitoreo efectivo del desempeño que mantenga el curso y evite resultados inesperados.

UNIVERSIDAD DE LIMA

¿Por qué se necesita un Framework de Gobierno de TI ?

- **¿Algunas de estas condiciones le suena familiar?**
  - Incremento de la presión para potenciar la tecnología en las estrategias de los negocios
  - Crecimiento de la complejidad del ambiente de TI
  - Infraestructuras de TI fragmentadas
  - Brechas de comunicación entre los gerentes de negocio y TI
  - Bajos niveles de servicios de TI
  - Costos de TI fuera de control
  - Falta de flexibilidad organizacional y rechazo al cambio
  - Frustración de los usuarios con requerimientos no satisfechos
  - Gerentes de TI trabajando como bomberos

La necesidad de Gobierno de TI

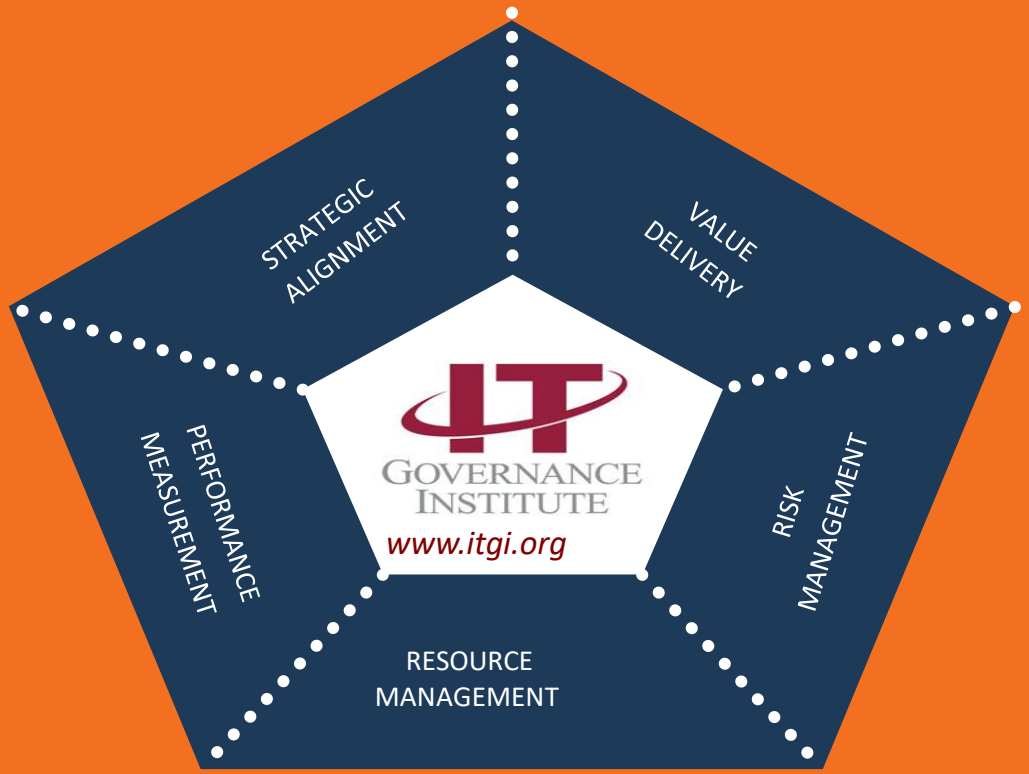
Gobierno Corporativo es un conjunto de responsabilidades y prácticas ejercidas por la junta directiva y administración ejecutiva con el objetivo de:

- Proporcionar dirección estratégica
- Garantizando que los objetivos sean alcanzados
- Estableciendo que los riesgos sean administrados apropiadamente
- Verificando que los recursos de la empresa son usados responsablemente

Gobierno de TI, según definición del ITGI

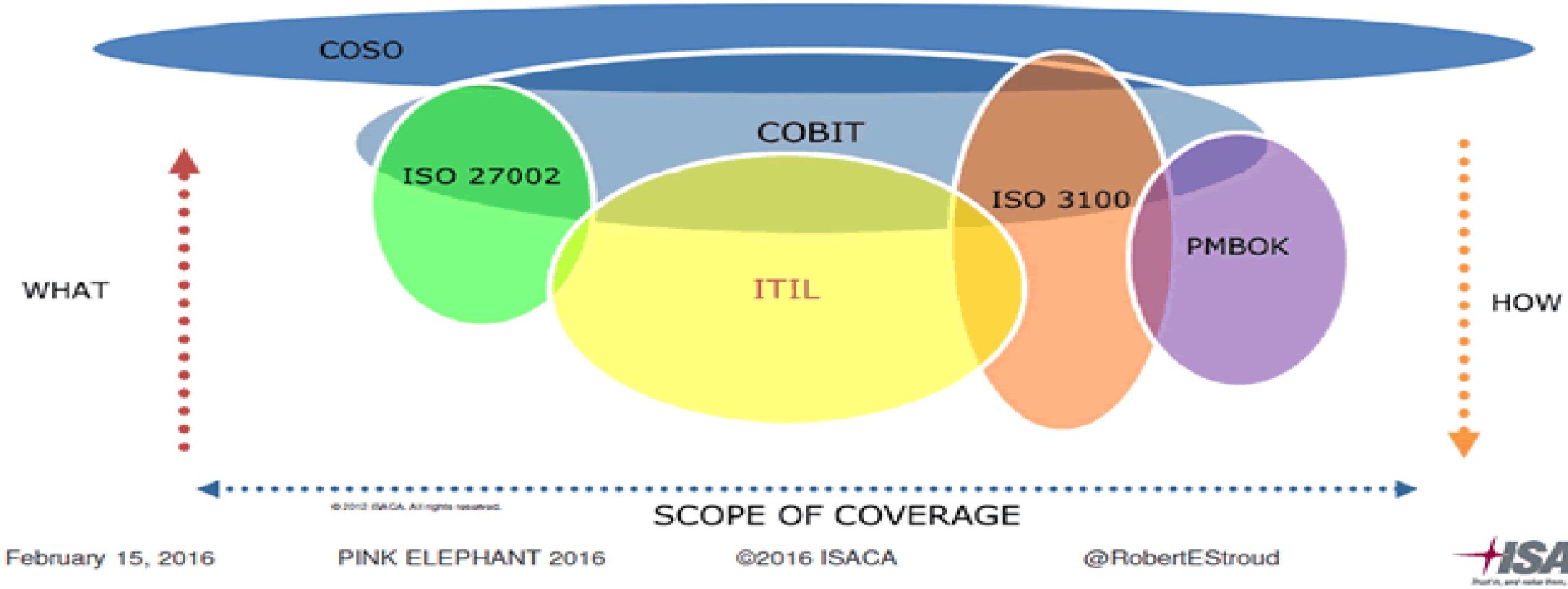
Gobierno de TI es:

- Responsabilidad de la junta directiva y la administración ejecutiva
- Una **parte integral** de gobierno corporativo, y consta de liderazgo, estructuras organizacionales y procesos que aseguran que la TI de la empresa **sustenta y extiende las estrategias y objetivos organizacionales**



UNIVERSIDAD DE LIMA

Estándares v Frameworks



UNIVERSIDAD DE LIMA

Gobierno de la Seguridad de la Información

- El objetivo del Gobierno de la Seguridad de la Información es **desarrollar y gestionar un programa** que alcance los siguientes resultados:
  - Alineación estratégica
  - Gestión de riesgos
  - Entrega de valor
  - Gestión de recursos
  - Medición del desempeño
  - Integración

UNIVERSIDAD DE LIMA

Alineación estratégica

- **Alinear la Seguridad de la Información con la estrategia de negocio** para apoyar los objetivos organizacionales, tales como:
  - Requerimientos de seguridad dirigidos por requerimientos de la empresa
  - Ajuste de las soluciones de seguridad a los procesos de la empresa que tomen en cuenta la cultura, estilo de gobierno, la tecnología y estructura de la organización
  - Inversión en seguridad de la información que sea congruente con la estrategia de la empresa

Gestión de riesgos

- **Ejecutar medidas apropiadas para mitigar los riesgos y reducir el posible impacto** que tendrían en los recursos de información a un nivel aceptable, tales como:
  - Entendimiento colectivo del perfil de amenaza, vulnerabilidad y riesgo de la organización
  - Entendimiento de la exposición al riesgo
  - Conciencia de las prioridades
  - Suficiente mitigación de riesgos
  - Aceptación/transferencia del riesgo

UNIVERSIDAD DE LIMA

Entrega de valor

- **Optimizar las inversiones en la Seguridad** en apoyo a los objetivos de negocio, tales como:
  - Un conjunto estándar de prácticas de seguridad
  - Un esfuerzo debidamente priorizado y distribuido
  - Soluciones institucionalizadas y estandarizadas
  - Soluciones completas que abarquen a la organización, el proceso y la tecnología
  - Una cultura de mejora continua

Gestión de recursos

- Utilizar el conocimiento y la infraestructura de Seguridad de la Información con **eficiencia y efectividad** para:
  - Asegurar que los conocimientos sean captados y están disponibles
  - Documentar los procesos y prácticas
  - Desarrollar arquitecturas de seguridad

Medición del desempeño

- **Monitorear y reportar procesos de seguridad** de la información para garantizar que se alcancen los objetivos, entre otros:
  - Un conjunto de medidas definidas, acordadas y significativas
  - Un proceso de medición que identifique deficiencias y brinde realimentación de avances
  - Aseguramiento independiente por evaluaciones y auditorías externas

Integración

- **Integrar todos los factores de aseguramiento relevantes** para garantizar que los procesos operan de acuerdo con lo planeado de principio a fin:
  - Determinar todas las funciones organizacionales de aseguramiento
  - Desarrollar relaciones formales con otras funciones de aseguramiento
  - Coordinar todas las funciones de aseguramiento
  - Coincidencia de roles y responsabilidades
  - Enfoque sistémico

III. Estrategia de seguridad de la información

Estrategia de Seguridad de la Información

¿Qué es estrategia?

–Kenneth Andrews describe la estrategia corporativa como

"el patrón de decisiones en una compañía que determina y revela sus objetivos, propósitos, o metas, genera las principales políticas y planes para alcanzar dichas metas y define el rango de negocio que debe perseguir la compañía, el tipo de organización económica y humana que es o pretende ser y la naturaleza de la contribución tanto económica como no económica que pretende hacer a sus accionistas, empleados, clientes y comunidades"

UNIVERSIDAD DE LIMA

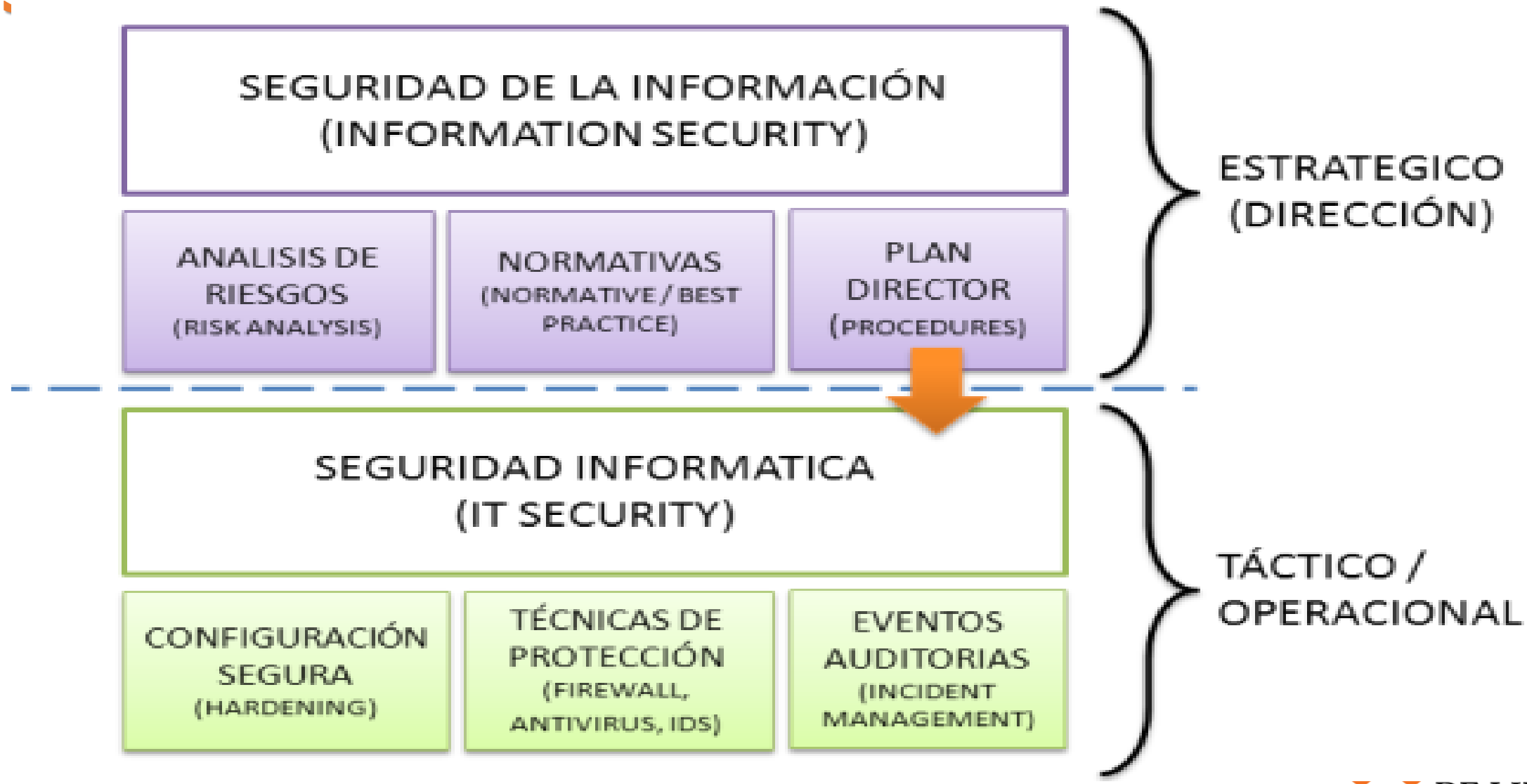
Estrategia de Seguridad de la Información

Una estrategia de seguridad de la información:

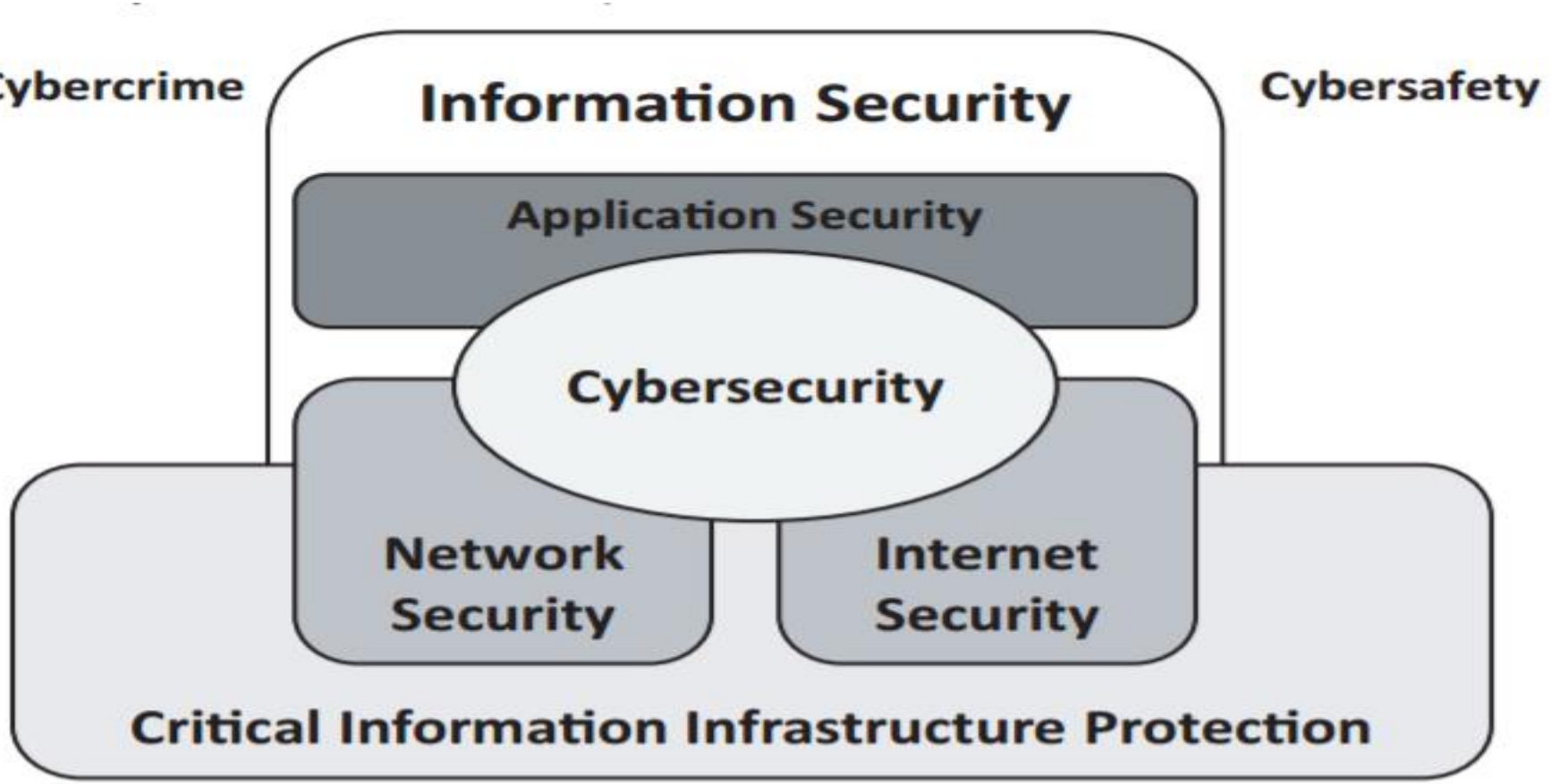
- Establece objetivos/propósitos/metas
- Alinea las principales políticas y planes para alcanzar los objetivos/propósitos/metas
- Define
  - El ámbito del negocio
  - Estado deseado para el negocio
- Proporciona la base para los planes de acción
  - Cada plan de acción debe formularse con base en los recursos disponibles y las limitaciones
  - Los planes de acción deben contener disposiciones para monitoreo y métricas definidas para determinar el nivel de éxito

UNIVERSIDAD DE LIMA

Participantes en la aplicación de la Estrategia de Seguridad de la Información



Relación de Seguridad de la información y ciberseguridad



Fuente: ISO/IEC 27032:2012

UNIVERSIDAD DE LIMA

IV. conclusiones