



Instituto Superior
Tecnológico del Azuay



Centro de Investigación
y Desarrollo Ecuador



Centro de Estudios
Transdisciplinarios Bolivia
CET-BOLIVIA

Aseguramiento de Tecnologías de Información. Una perspectiva integradora

Congreso Internacional de
**DESARROLLO
DE SOFTWARE**



EXPOSITOR



Centro de Investigación
y Desarrollo Ecuador



Centro de Estudios
Transdisciplinarios Bolivia
CET-BOLIVIA



- **Francisco Javier Valencia Duque**
- **PhD en Ingeniería, Industria y Organizaciones**
- **CISA/CRISC/CF/LA 27001**
- **Universidad Nacional de Colombia**
- **fjvalenciad@unal.edu.co**

Congreso Internacional de
**DESARROLLO
DE SOFTWARE**

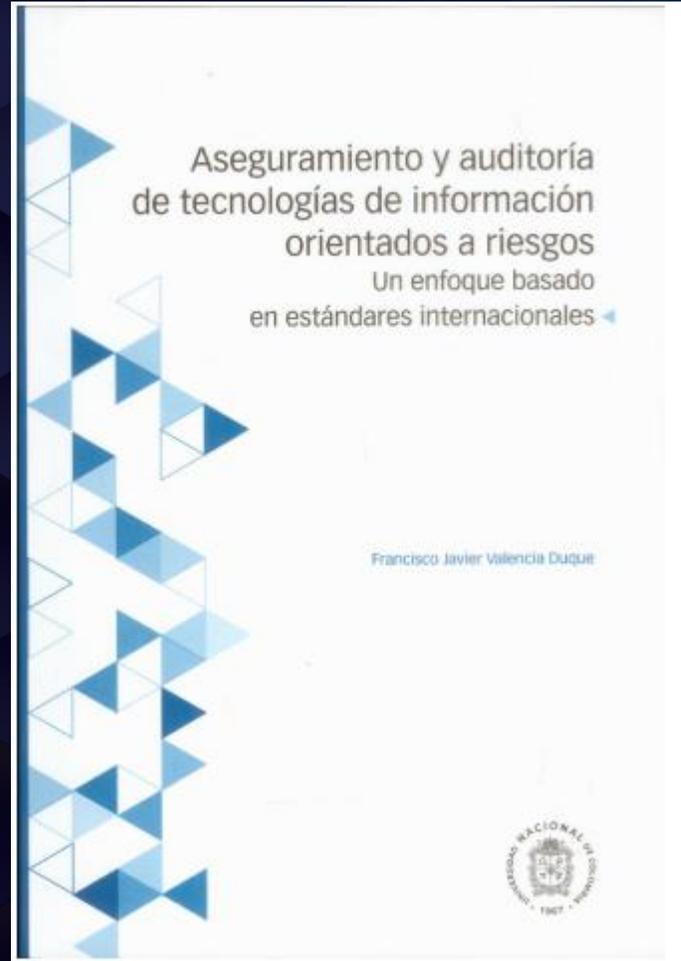


INTRODUCCIÓN





INTRODUCCIÓN



<http://www.uneditorial.com/review/product/list/id/381559/>



Congreso Internacional de
**DESARROLLO
DE SOFTWARE**

QUE ES ASEGURAMIENTO

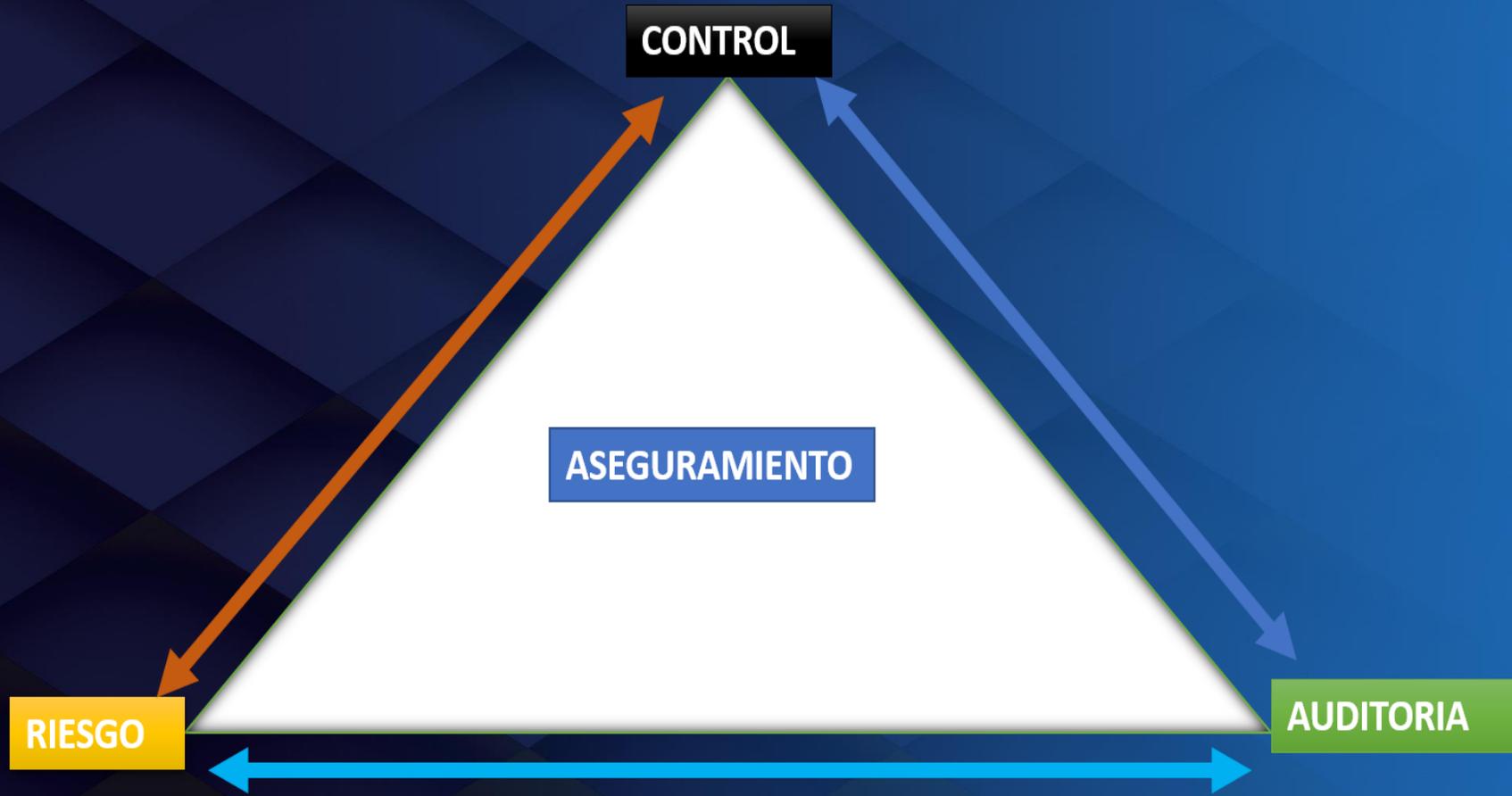
De acuerdo con Spears, Barki, & Barton (2013) el aseguramiento tiene diversos significados, dependiendo de la fuente, la audiencia y la interpretación

La función de aseguramiento es definida por el Instituto de Auditores Internos, como “aquella función que provee aseguramiento sobre la efectividad del gobierno, administración de riesgos y control” (The Institute of Internal Auditors, 2016,p. 5),

El aseguramiento es una función organizacional diseñada para mejorar el grado de confianza que se tiene sobre un asunto en particular, de allí que pueden existir diferentes tipos de aseguramiento, ejecutados por diferentes actores. Entre los diferentes servicios de aseguramiento se encuentran la autoevaluación, los servicios de auditoría interna y los servicios de auditoría externa (ISACA, 2013b)



QUE ES ASEGURAMIENTO



ALGUNOS PERFILES DEL ASEGURAMIENTO

DISCIPLINA	A NIVEL ORGANIZACIONAL	A NIVEL TECNOLÓGICO
RIESGOS	CRO (Chief Risk Officer) o CRMO (Chief Risk Management Officer)	CIRO (Chief Information Risk Officer)
CONTROL	CSO (Chief Security Officer)	CISO (Chief Information Security Officer)
AUDITORÍA	CAO (Chief Audit Officer) o CAE (Chief Audit Executive)	CISA* (Chief Information System Auditor)

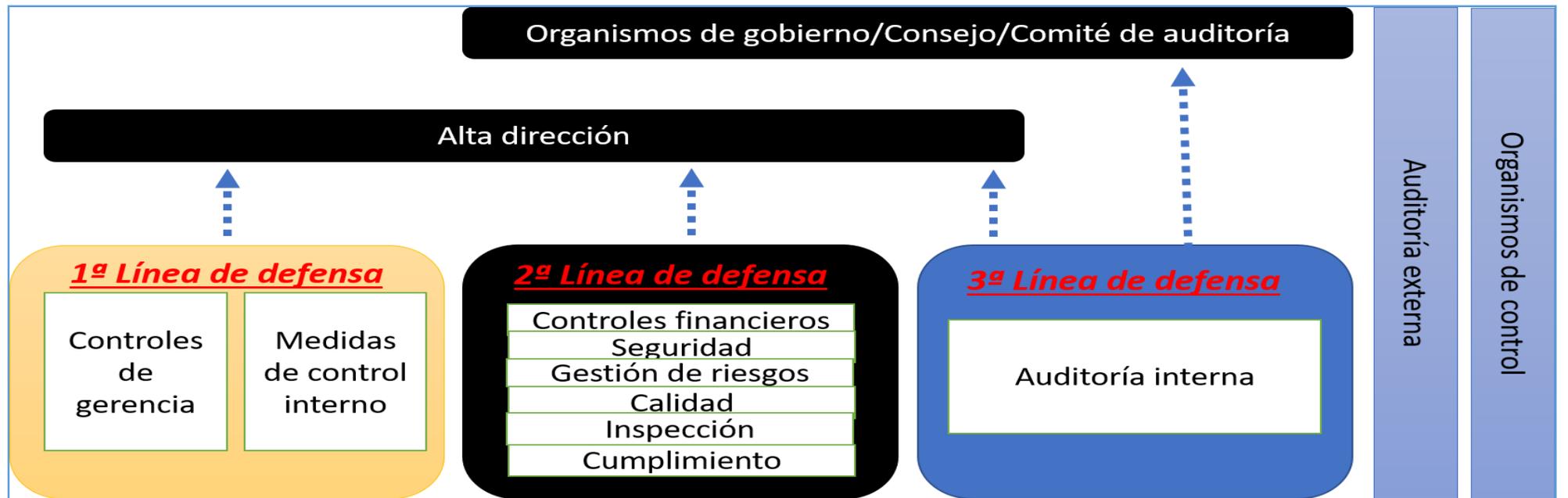
*La sigla CISA es referida con mayor frecuencia a Certified Information System Auditor, certificación internacional de ISACA.

PRINCIPALES MARCOS DE REFERENCIA DE ASEGURAMIENTO CORPORATIVO

Governance, Risk and Compliance (GRC)

OCEG (Open Compliance and Ethics Group)

Modelo de tres líneas de defensa



PRINCIPALES MARCOS DE ASEGURAMIENTO CORPORATIVO



El estándar de auditoría internacional del IIA 2050 relacionado con la coordinación, establece que el director ejecutivo de auditoría debe compartir información y coordinar actividades con otros proveedores internos y externos de aseguramiento y servicios de consultoría relevantes para asegurar una cobertura adecuada y minimizar la duplicidad de esfuerzos



Fuente: Diseñado a partir de (Huibers, 2015)

PRINCIPALES MARCOS DE ASEGURAMIENTO CORPORATIVO

MAPAS DE ASEGURAMIENTO

Es una herramienta diseñada con el fin de establecer una adecuada coordinación de los diferentes actores internos y externos relacionados con la función de aseguramiento en una organización, y de esta forma minimizar la duplicidad de esfuerzos y dar una cobertura adecuada a las diferentes tareas relacionadas con el riesgo, control y auditoría.

El consejo para la práctica de auditoría 2050-2 del IIA está orientado al establecimiento de mapas de aseguramiento,

PRINCIPALES MARCOS DE ASEGURAMIENTO TECNOLÓGICO

I.T.

G.

R.

C.

GOBIERNO CORPORATIVO

GOBIERNO DE TIC

GESTIÓN DE **R**IESGOS EMPRESARIALES

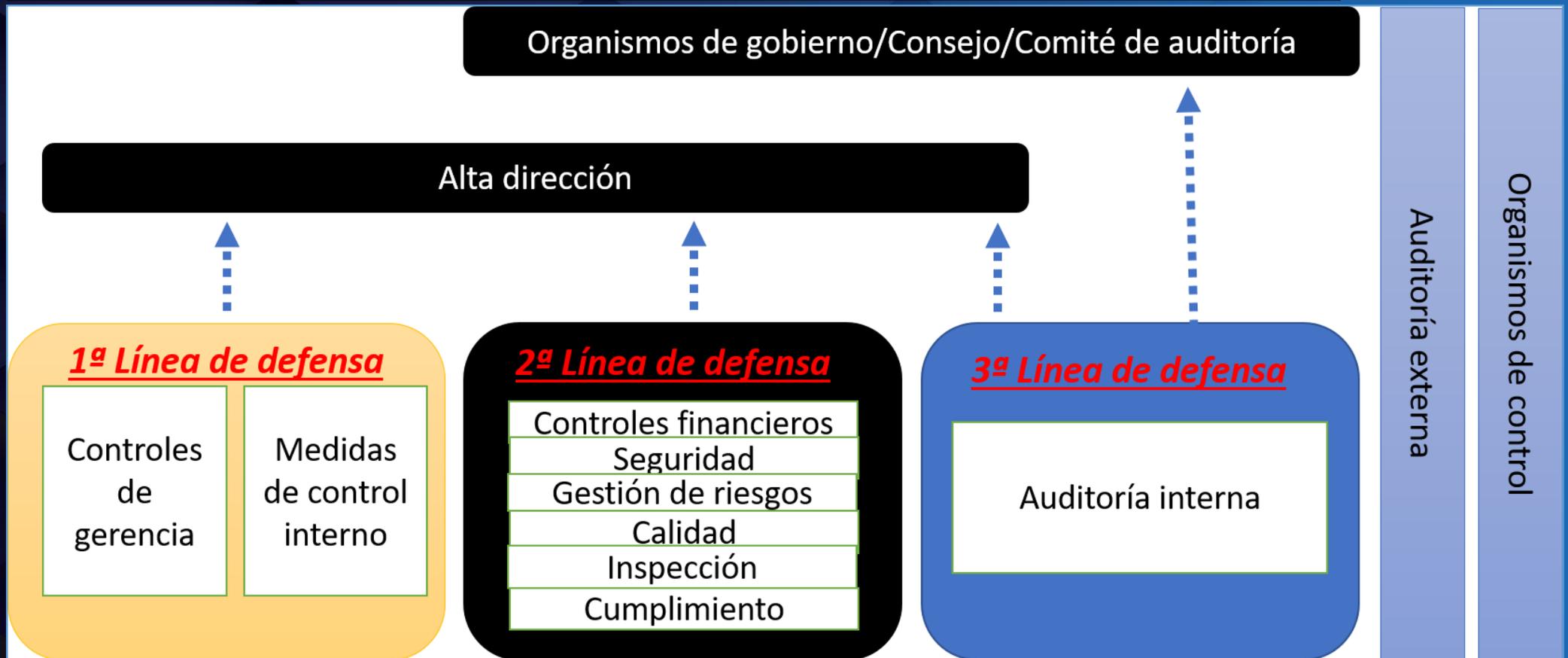
GESTIÓN DE RIESGOS
DE TIC

CUMPLIMIENTO

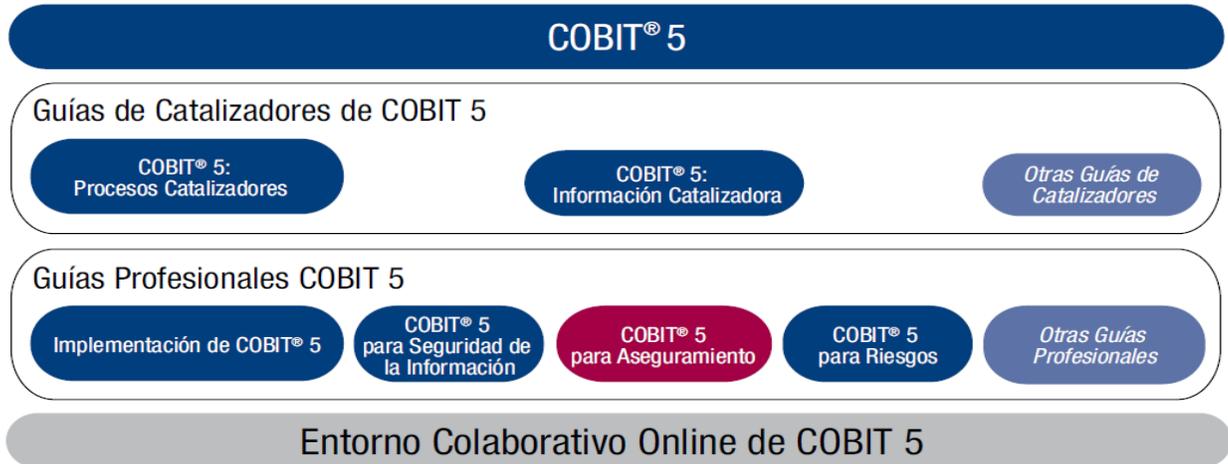
CUMPLIMIENTO DE
TIC

PRINCIPALES MARCOS DE ASEGURAMIENTO TECNOLÓGICO

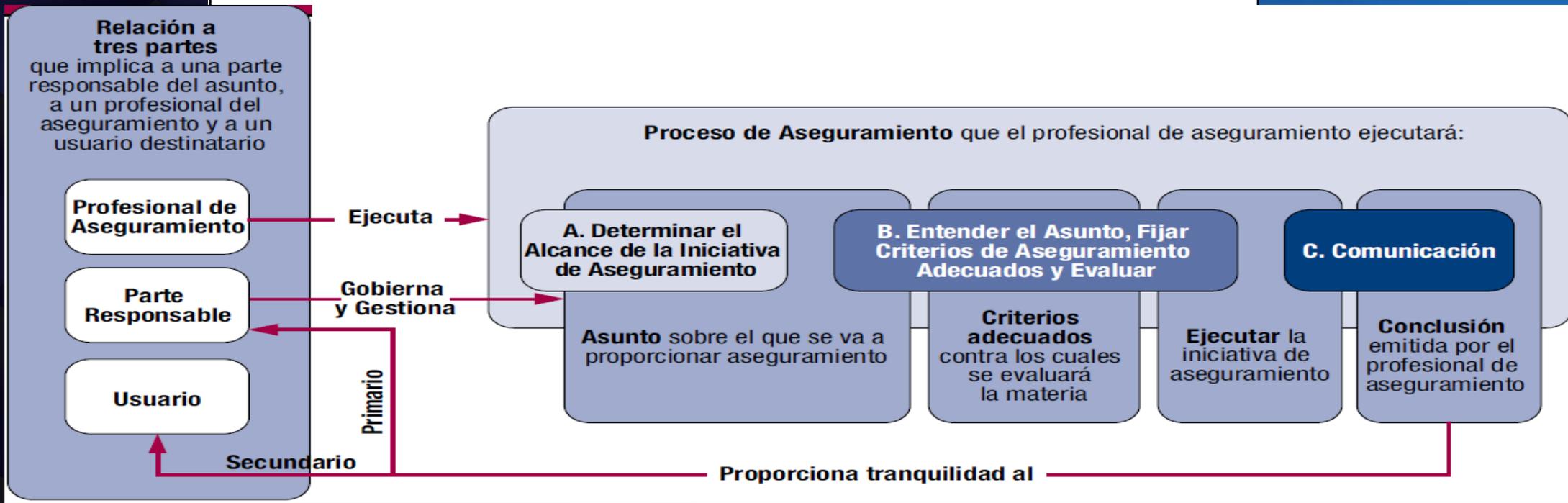
LAS TRES LÍNEAS DE DEFENSA EN EL CONTEXTO DE LAS TIC



PRINCIPALES MARCOS DE ASEGURAMIENTO TECNOLÓGICO



COBIT 5 PARA ASEGURAMIENTO



VISIÓN INTEGRADA DEL ASEGURAMIENTO CORPORATIVO Y TECNOLÓGICO

NEGOCIO

OBJETIVOS EMPRESARIALES

PROCESOS DE GOBIERNO Y GESTIÓN EMPRESARIAL

RECURSOS EMPRESARIALES

MODELOS DE ASEGURAMIENTO EMPRESARIAL

RIESGOS
(ISO 31000, COSO ERM...)

CONTROLES
(COSO, COCO, SOX, MECI, MECIP..)

AUDITORÍA
(ISO 19011, IIA)

FUNCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

OBJETIVOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

PROCESOS DE GOBIERNO Y GESTIÓN DE TIC
(ISO 38500, ITIL, ISO 20000, ISO 12207, COBIT 5, MOF...)

RECURSOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
(SISTEMAS DE INFORMACIÓN, INFRAESTRUCTURA TECNOLÓGICA, PERSONAL...)

MODELOS DE ASEGURAMIENTO TECNOLÓGICO

RIESGOS DE TIC
(RISK IT, ISO/IEC 27005, MAGERIT, OCTAVE, NIST...)

CONTROLES DE TIC
(COBIT, ISO/IEC 27002, NIST...)

AUDITORÍA DE TIC
(IT ASSURANCE, ISO 19011, ISO 2700X...)

A
L
I
N
E
A
C
I
O
N

PLANEACIÓN

EJECUCIÓN

REPORTE

SEGUIMIENTO

PROCESO DE AUDITORÍA Y ASEGURAMIENTO



Muchas gracias

Congreso Internacional de
**DESARROLLO
DE SOFTWARE**



Ingresa a:

www.cidecuador.com

Al finalizar este evento podrás encontrar esta presentación en su respectiva página web.

Congreso Internacional de
**DESARROLLO
DE SOFTWARE**