Ciberseguridad – Posicionándola en el Nivel Estratégico

Germán Pancho Carrera
DIRECTOR MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Germán Pancho Carrera: Profile

Máster en Gerencia de Sistemas

Areas de Compencia

- Arquitectura Empresarial
- Seguridad de la Información - Ciberseguridad
- Transformación Digital
- Estrategia Tecnológica
- Gestión por Procesos
- Estándares y Buenas Prácticas: TI - Negocio

Rol/Cargo

- Arquitecto Empresarial
- Consultor Empresarial
- Director de la Maestrías
  - Gerencia de Sistemas y Tecnología Empresarial
  - Gestión de la Seguriodad de la Información

2020 -2021: Años sin precedentes

POSGRADOS | udla

- Todas las industrias fueron afectada por la pandemia: unos ganaron, otros perdieron
- Estrategia y modelos de negocio cambiaron y siguen cambiando
- En este contexto, hay presión sobre ciertos roles:
  - CIOs: generar mayor valor al negocio con el uso de tecnología (acelerar la digitalización)
  - La función de seguridad de la información debe también responder
  - Los CISOs deben reposicionarse

Gestión de Ciberseguridad Ágil y Dinámica

- El cibercrimen ha evolucionado rápidamente en los últimos 5 años.
- Existe un nivel de profesionalización de los cibercriminales y representan un riesgo a gobierno e industria
- La ciberseguridad se ha elevado a un estatus de “crítica”. Hay incremento de phishing attacks, malware y online scams.
- No es possible tener estrategias estáticas de ciberseguridad, sino un efoque ágil de ciber estrategia, roadmap y riesgo

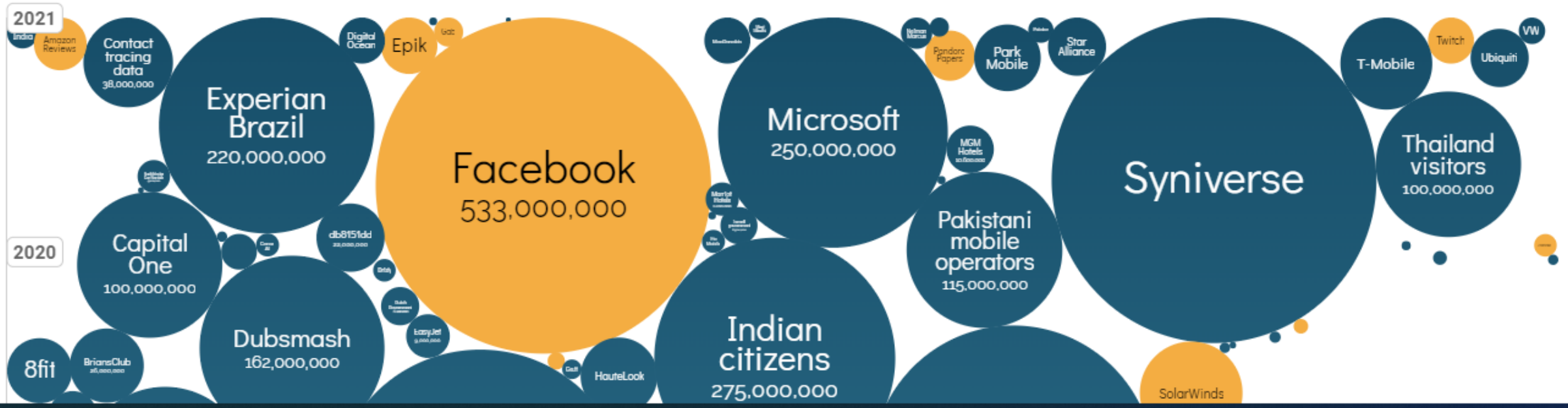
World's Biggest Data Breaches & Hacks

interesting story

Selected events over 30,000 records

UPDATED: Oct 2021

size: records lost filter search...



Agilidad en Ciberseguridad

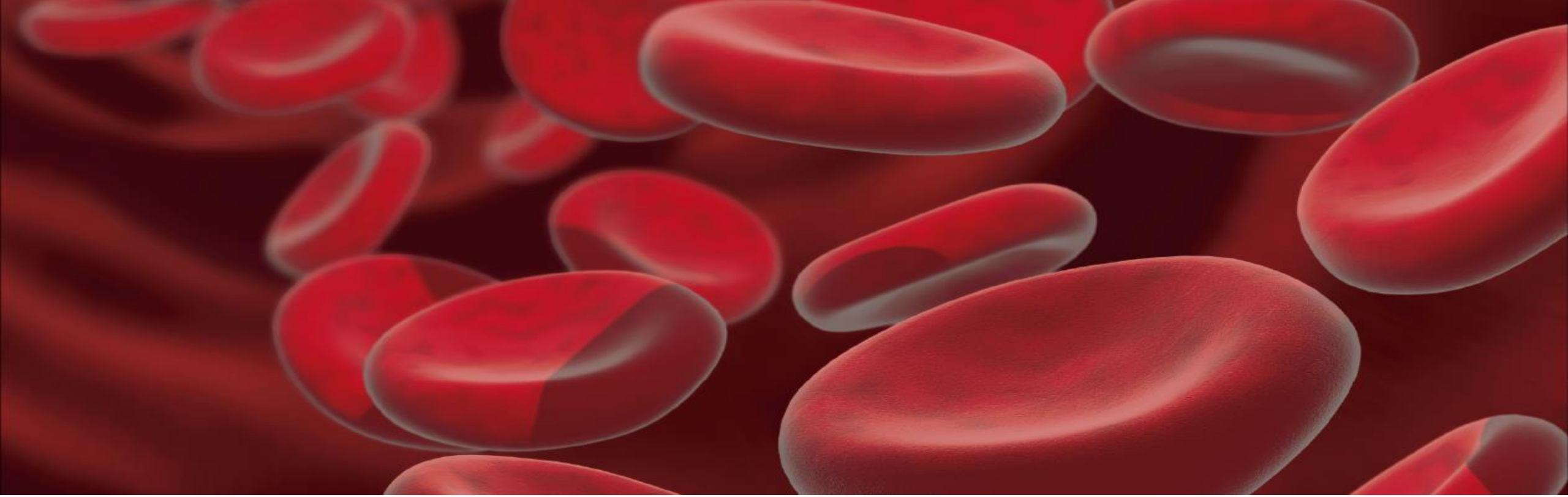
POSGRADOS | udla

- Ágil es una palabra de moda. Ciberseguridad debe repensar su papel
- Realidad: los productos y servicios son cada vez más digitales
- La seguridad de la información es un objetivo móvil que a la transformación digital
- La seguridad de la información es parte del valor de marca de las organizaciones

Frente a esta complejidad es común…

- **Organizaciones: diseñan, adquieren e implementan soluciones de seguridad de la información desde una perspectiva operativa/táctica.**

- **Es decir:**
  - **Se identifica requerimiento**
  - **Se desarrolla especificación**
  - **Se busca una solución**
  - **Se implementa**



Enfoque Ágil:

Mixtura de soluciones técnicas ad-hoc, con diseños independientes que no aseguran compatibilidad e interoperabilidad. Sin TCO claro.

Hay agilismo, pero no hay oportunidad de encontrar una dimensión estratégica de ciberseguridad

- Cómo posicionar a nivel estratégico la ciberseguridad?.
- Cómo alinear las soluciones de ciberseguridad con los objetivos de negocio?
- Cómo tener una visión sistémica y articulada de los retos de ciberseguridad?

Framework: Arquitectura de Ciberseguridad

POSGRADOS | udla

- Que maneje la complejidad
- Que parta de las motivaciones de negocio
- Que articule dimensiones
- Agnóstico tecnología
- Escalable – crecimiento incremental
- Multi-industria
- Que se complemente y armonice con otros estándares

Una buena Arquitectura …

- Soporta decisiones correctas en cuanto a las soluciones
- Mejor gestión del riesgo: balance entre amenazas y oportunidades
- Habilitador del objetivos de negocio y no solamente de seguridad/ cyber seguridad
- Ayuda a priorizar y decidir que hacer y en que orden "Hacer las cosas correctas“
- “Hacer las cosas correctamente”

Pero además…

Con un enfoque estratégico que prevenga eventos disruptivos, hasta donde sea posible y mitigue los posibles impactos sobre los sistemas de información, operaciones de negocio y partes interesadas

Visión Holística desde el negocio hasta las soluciones

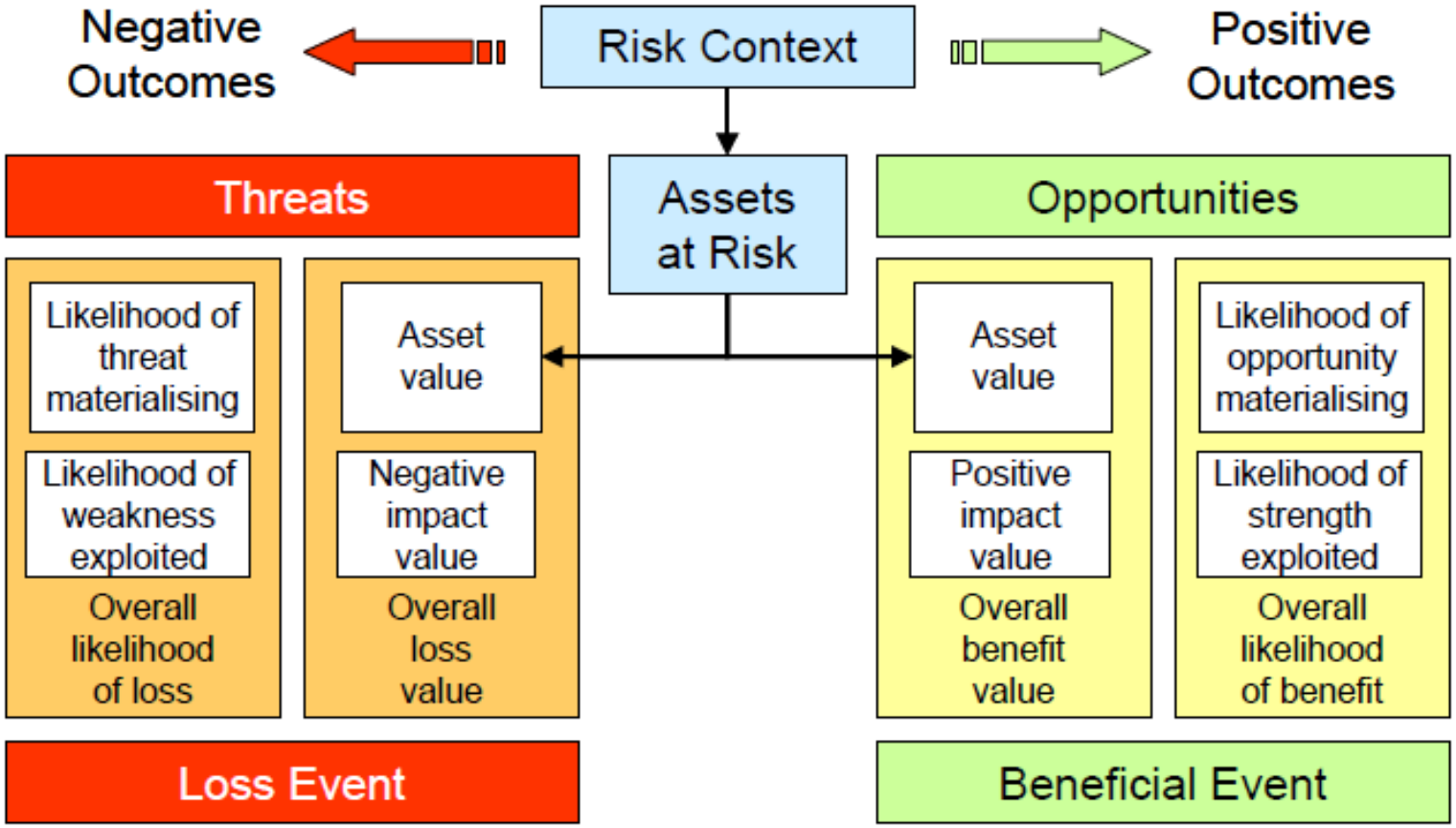
	Perspectiva	Se enfoca a...
Arquitectura Contextual	Del negocio	Requerimientos de negocio
Arquitectura Conceptual	Del arquitecto	Visión estratégica de alto nivel
Arquitectura Lógica	Del diseñador	Servicios de seguridad
Arquitectura Física	Del implementador	Mecanismos de seguridad
Arquitectura de Componente	De proveedor de soluciones	Productos de seguridad y herramientas
Arquitectura Operacional	Del Jefe de Infraestructura	Administración y operación de la seguridad

Ref: Sherwood Applied Business Security Architecture (SABSA)

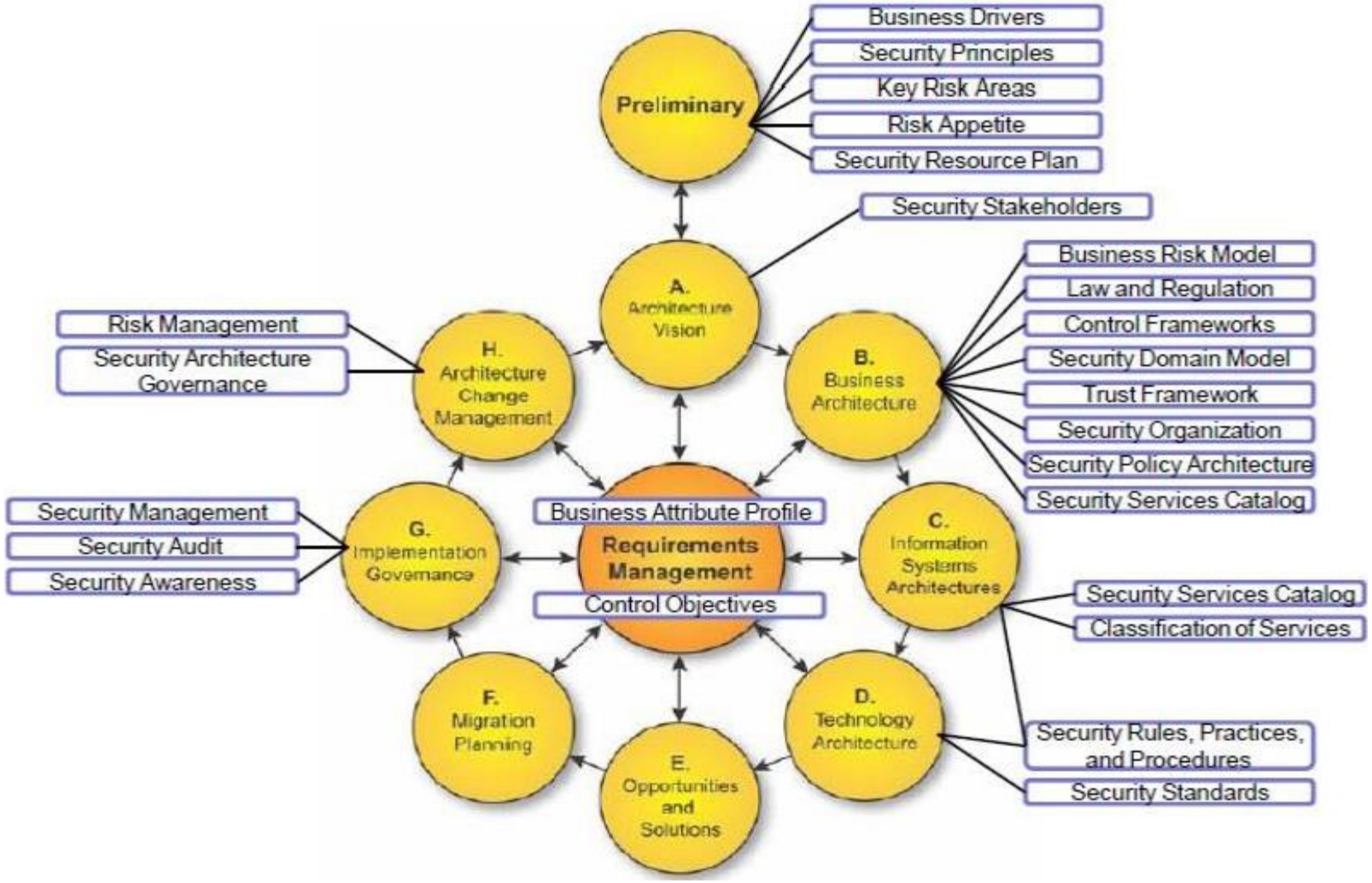
	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Ref: Sherwood Applied Business Security Architecture (SABSA)

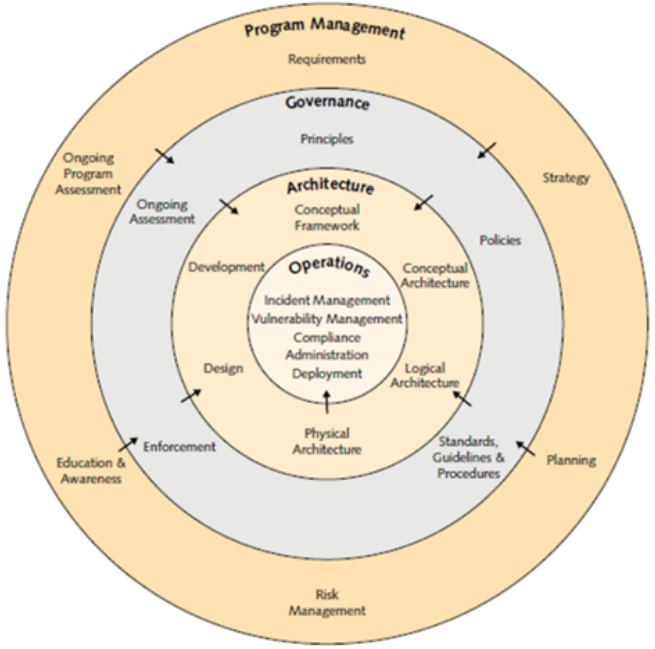
Balance entre Riesgos y Oportunidades



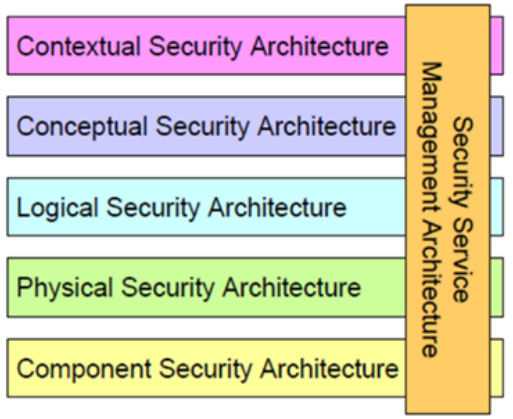
Más allá de las Capas – Hay que articular



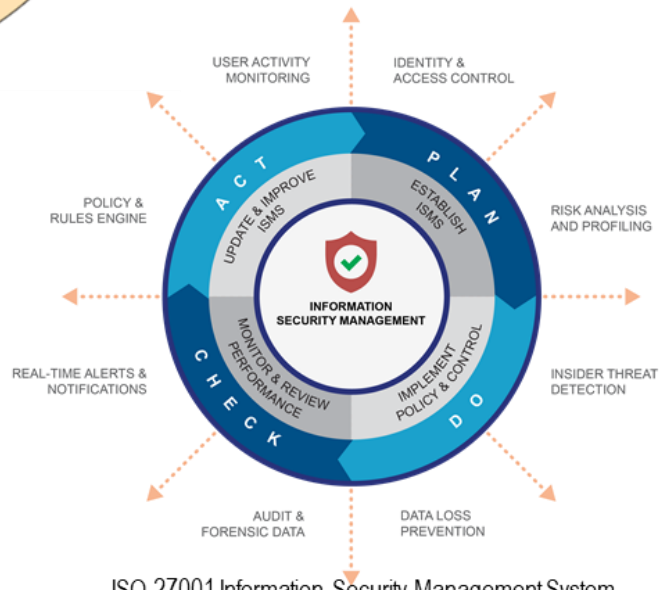
Complementar con otros Estándares



TOGAF O-ESA – Enterprise security program model



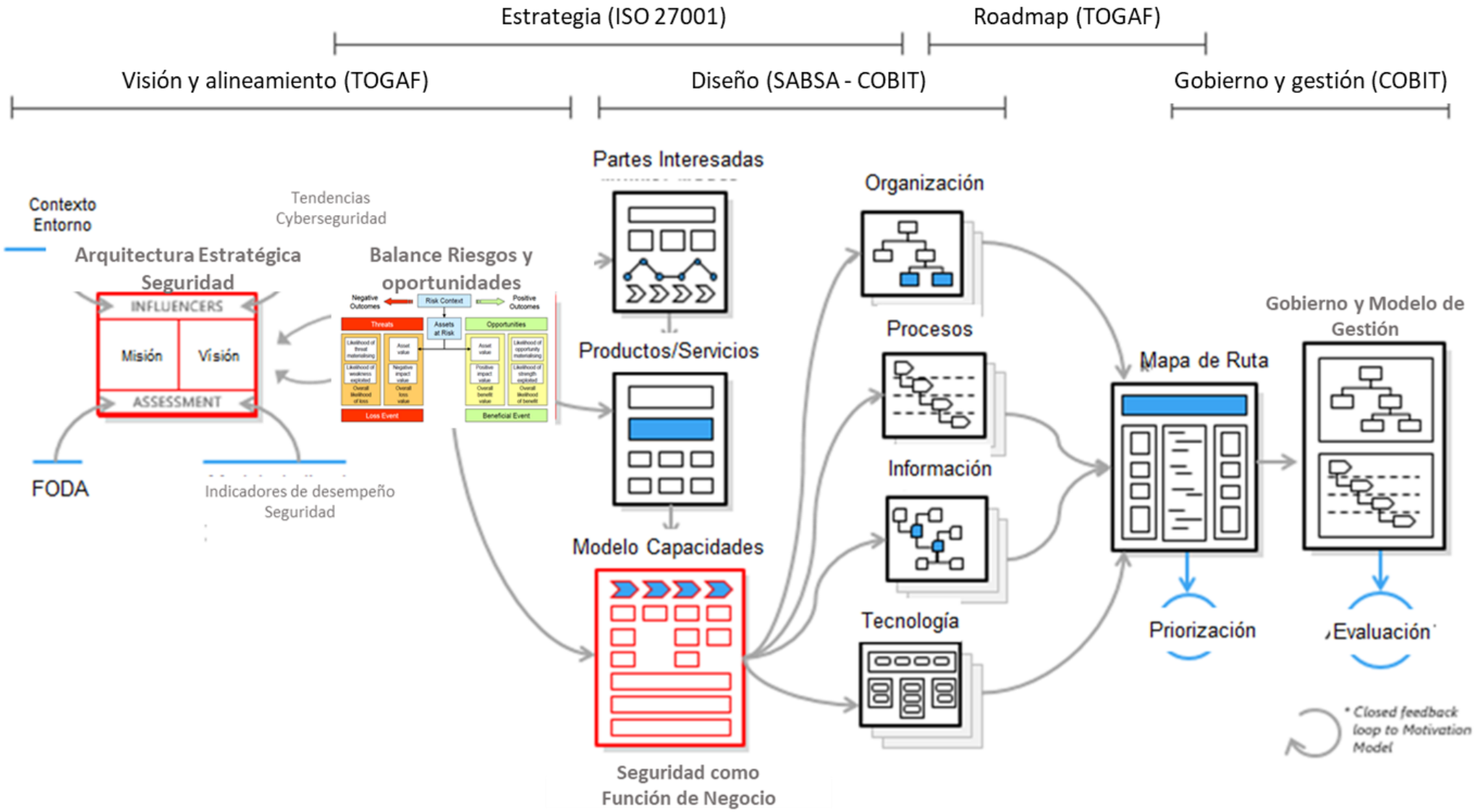
SABSA Design Framework



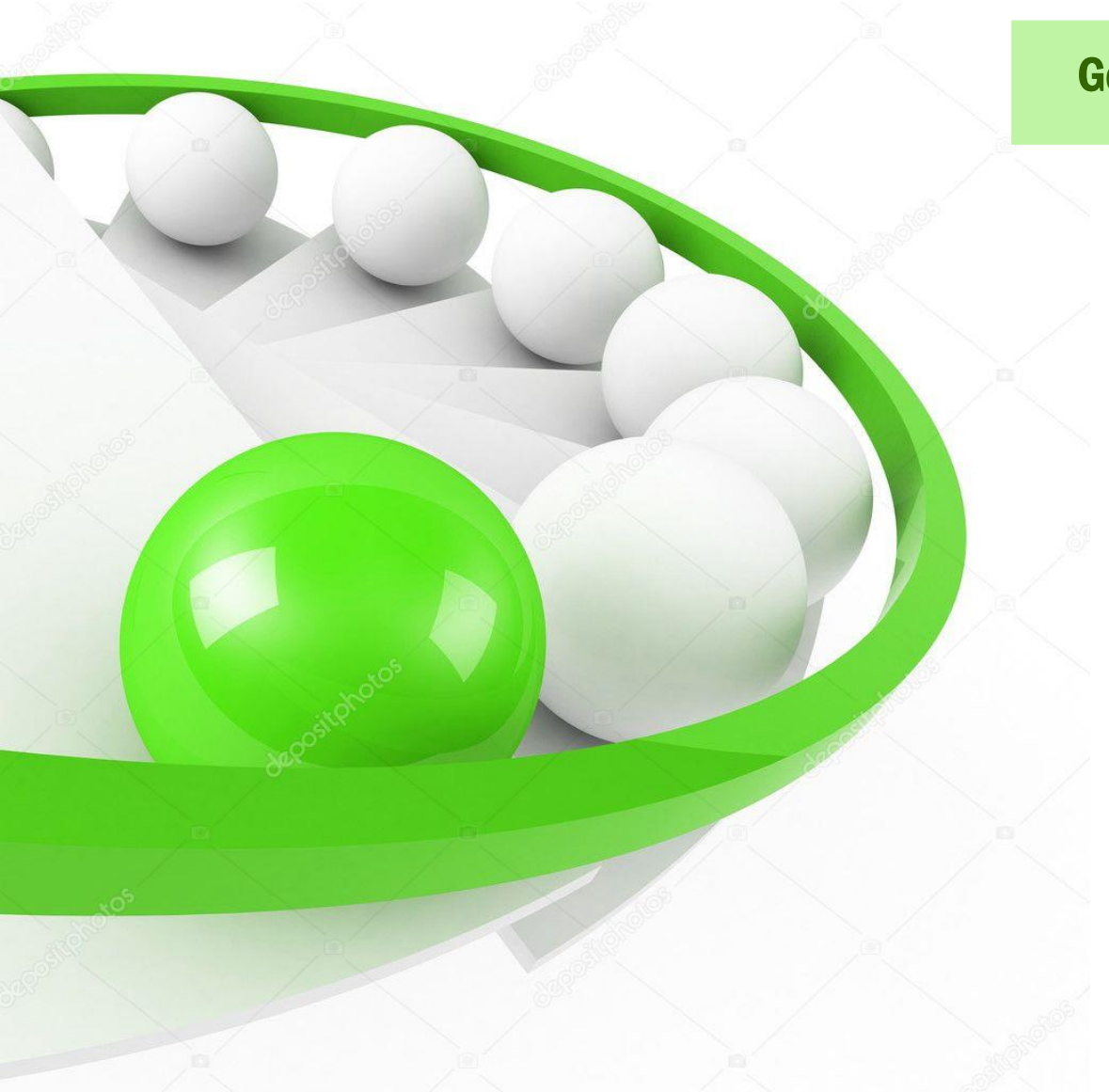
ISO 27001 Information Security Management System

COBIT 2019 Governance System Components

Modelo y arquitectura de ciberseguridad en la práctica



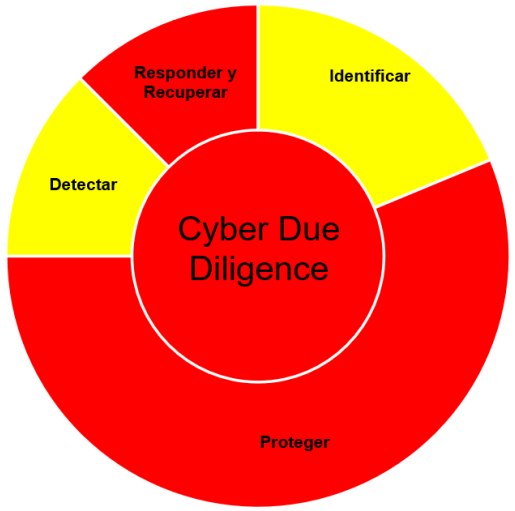
Ciberseguridad: Función de Negocio

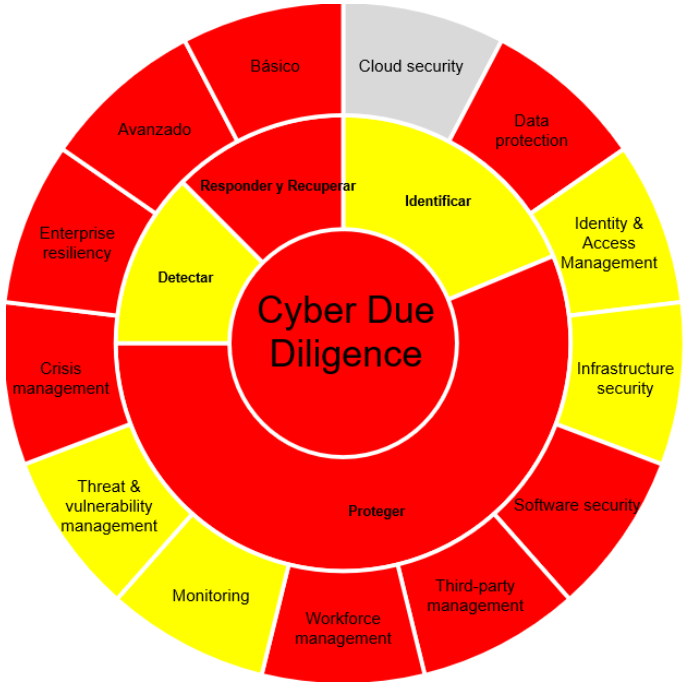


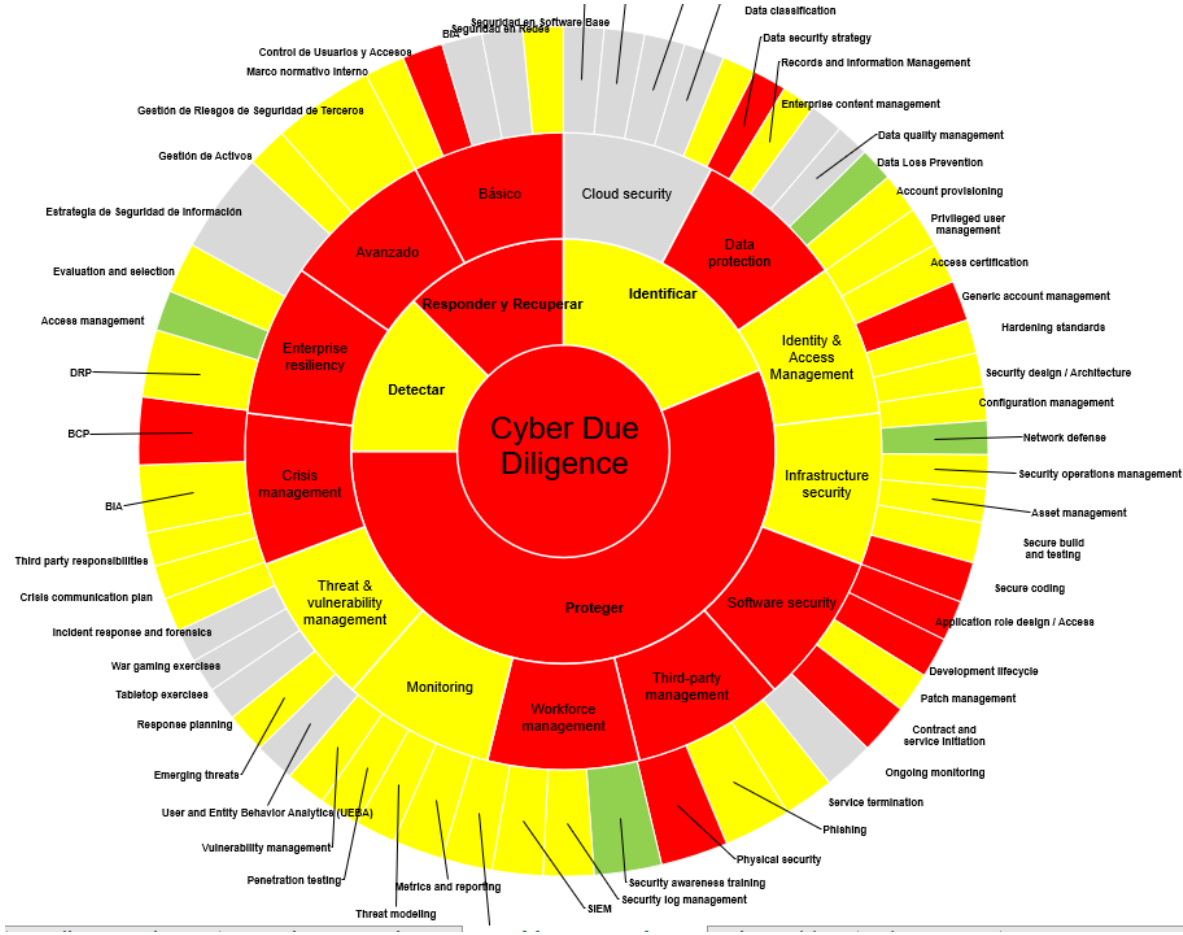
- Gobernanza
- Patrocinio Ejecutivo
- Cultura comprometida con el riesgo
- Tratamiento del Riesgo y la Cyberseguridad

Modelo de Gobierno de Ciberseguridad

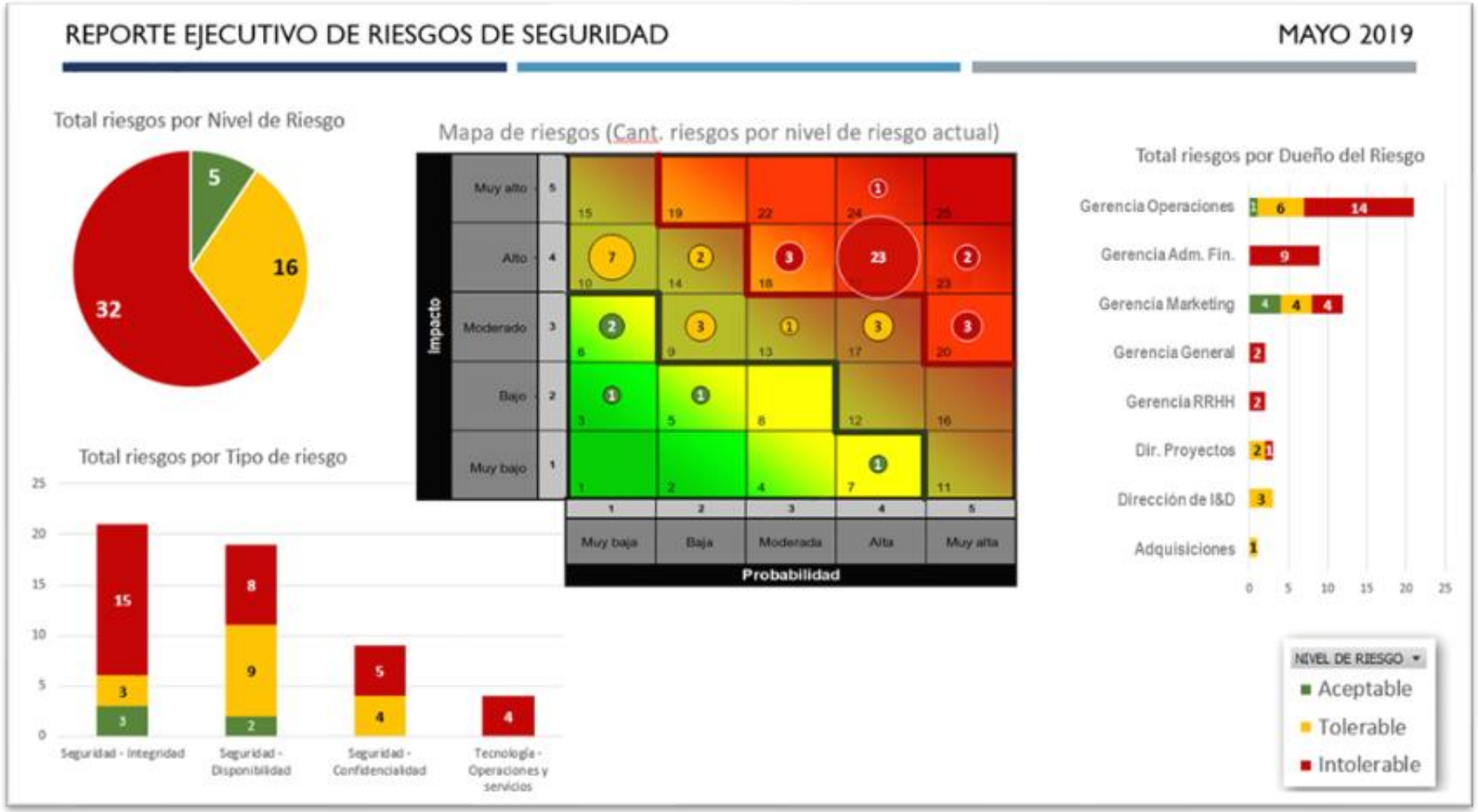
Dashboard Dinámico de Vulnerabilidades, Controles y Riesgos



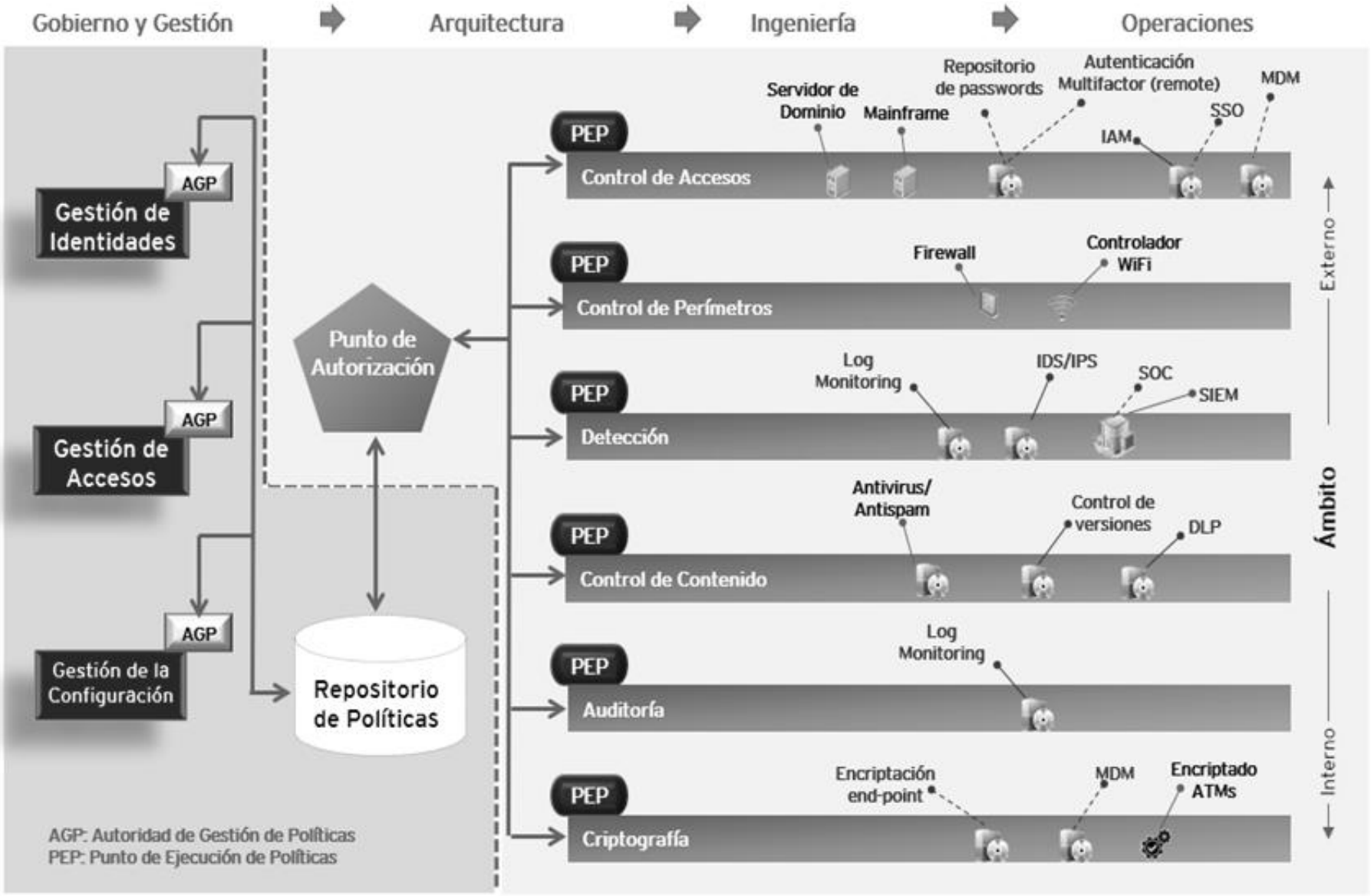




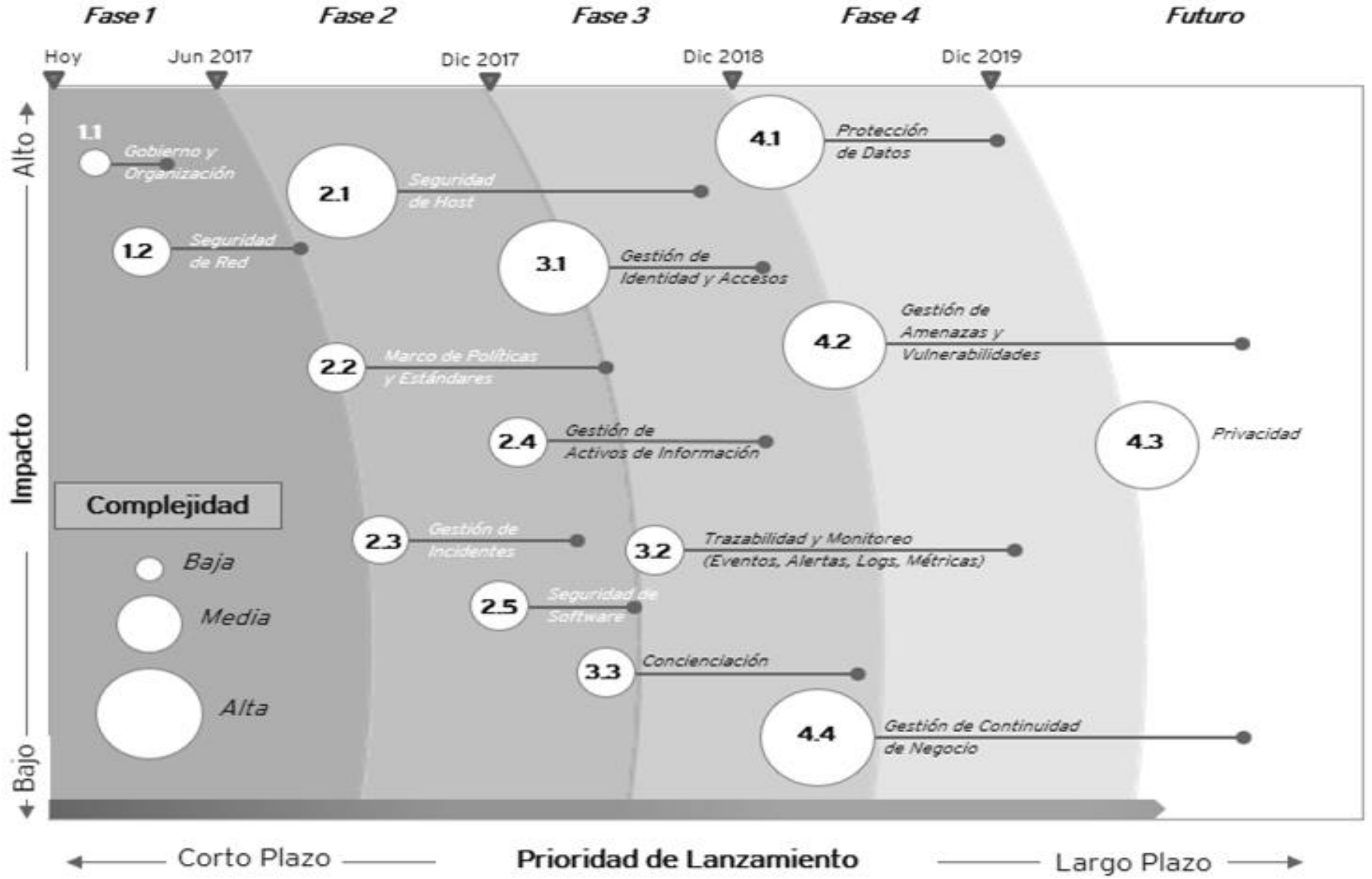
Dashboard Dinámico de Vulnerabilidades, Controles y Riesgos



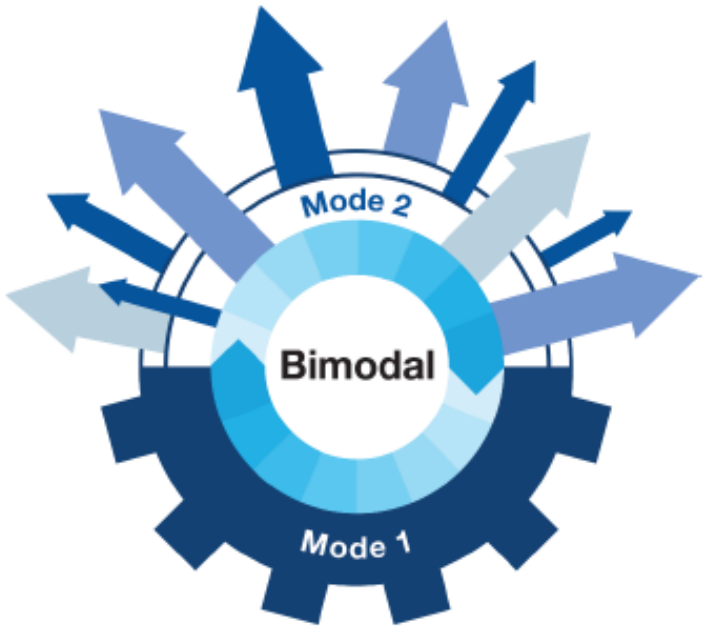
Modelo de Gestión Integrada



Hoja de Ruta Estratégica priorizada



Adopción Bimodal de la Ciberseguridad



Percentage of Respondents Who Use a Bimodal Approach

68%	43%	17%
Top performers (n = 160)	Typical performers (n = 1,894)	Trailing performers (n = 153)

Average Bimodal Adoption	38%	43%
	2016	2017

CISO
Fortalecer competencias

POSGRADOS | udla

Adaptabilidad

Demostrar flexibilidad, agilidad y la habilidad para responder efectivamente al cambio de entorno

Enfoque al Negocio

Demuestra conciencia de la dinámica interna y externa con una precisión acerca de los impactos sobre el negocio

Destreza digital

Es capaz de aprovechar la información y la tecnología de formas únicas e innovadoras

Enfoque a resultados

Enfoque en los resultados y metas del negocio. Define nuevos desafíos

Colaboración/sinergia

Colabora con terceros de manera formal e informal

Ideas de Cierre

- El gobierno/gestión de ciberseguridad es un habilitante de la transformación digital.
- Importante desplegar un enfoque bimodal a esta problemática.
- Visión que enlace lo estratégico y operativo, pero articulado
- Gestión ciberseguridad debe ser vista como una función de negocio que parte no de la gestión de vulterabilidades, sino del propio apetito del riesgo.
- Hay que apoyarse en estándares y buenas prácticas
- No hay oportunidad para improvisar.

Ideas de Cierre

- Mantenga perspectiva de mediano plazo, pero siempre esté preparado para revisar, actualizar y cambiar su estrategia
- Tener una hoja de ruta es excelente, pero hay que establecer ajustes rápidos en función del panorama de amenazas externas
- Elaborada la estrategia cibernética y su hoja de ruta para ponerla en práctica, puede comenzar con la gestión de riesgos empresariales.
- Se pueden tener ejercicios regulares de gestión de riesgos y auditoría, pero para construir una estrategia de ciberseguridad verdaderamente ágil, las actualizaciones de la gestión de riesgos deben realizarse en tiempo real.

Ideas Finales

- Si Usted no comunica, está en un ambiente inseguro. La colaboración elimina los silos, conecta a las personas, procesos y la tecnología; consume menos recursos, mejora la eficiencia y transparenta los resultados
- La gestión de seguridad de la información es una capacidad empresarial que transforma los eventos, incidentes y amenazas en acciones inteligentes de prevención, análisis, detección y respuesta

Preguntas

- **Escríbame … sus comentarios me interesan**

german.pancho@udla.edu.ec

Celular: 0998120443