Ciberseguridad en el sector asegurador

Medidas y controles para gestionar y proteger la información de los asegurados derivado de ataques cibernéticos.

Seminario Regional de Capacitación sobre Supervisores de Seguros ASSAL – IAIS 2024

Ciberseguridad en el Sector asegurador

Medidas y controles para gestionar y proteger la información de los asegurados derivado de ataques cibernéticos.

David Ricardo Rodríguez Calderón, Panelista
Supervisor de TI SUGESE

Ingeniero en Sistemas y Máster en Administración de empresas con énfasis en Gerencia de Proyectos, cursando el Master en IA aplicada a los negocios de Lead University.

Auditor CISA Internacional certificado por ISACA.
Agente de Cambio de la Fundación Friedrich-Ebert-Stiftung en América Central.
Es miembro el Colegio de Profesionales en Informática de Costa Rica (CPIC) desde el 2004, de la Asociación Costarricense de Auditores en Informática (ACAI – ISACA) desde el 2016, y desde el 2020 forma parte del Comité sobre Fintech-Regtech-Suptech (TC FRS CoP) del Toronto Centre.

Tiene más de 15 años de experiencia en el ámbito público y privado en Gestión de TI, control interno, supervisión y auditoría.

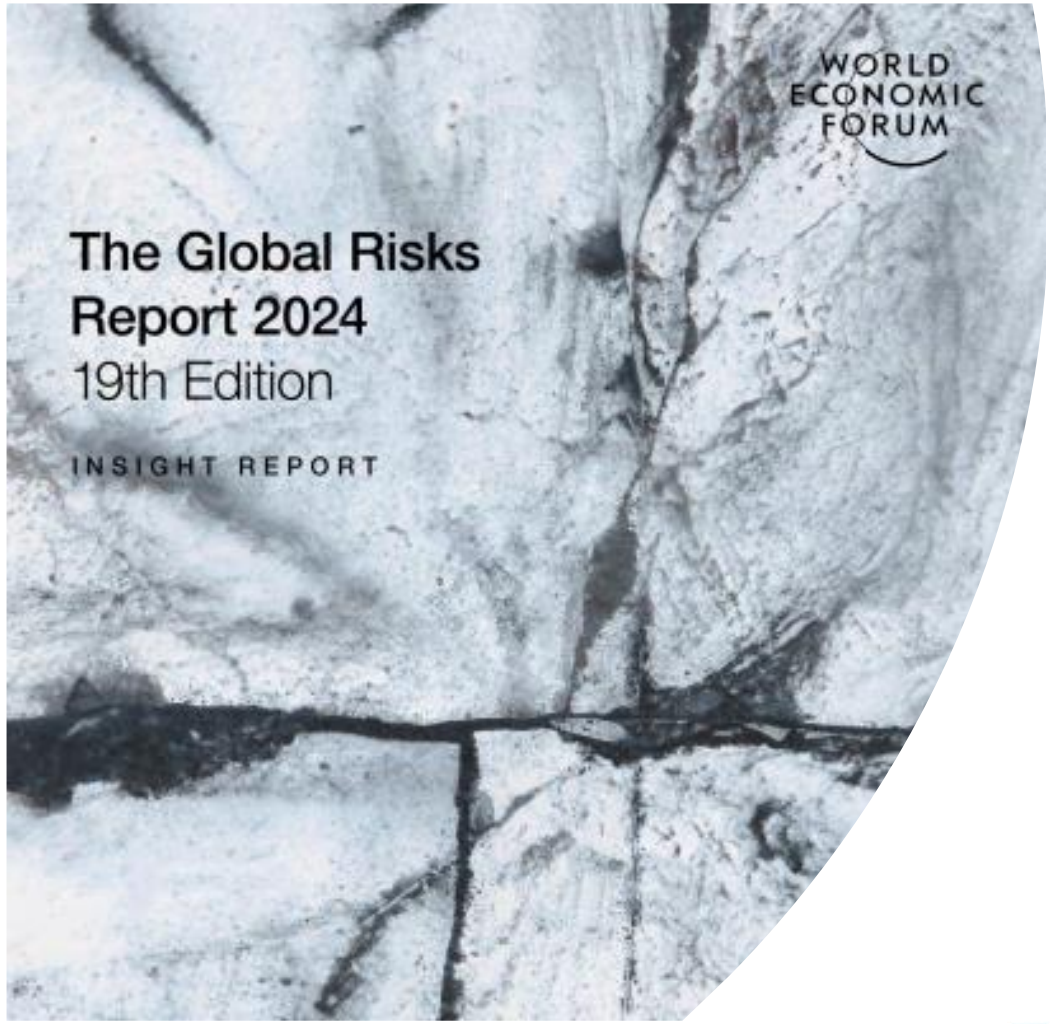
Más de 10 años como líder de proyectos e implementador de marcos de referencia, normas y estándares internacionales, tales como: ISO 9001, ISO (27001, 27002, 27032), ISO 22301, ISO 31000, ISO 17065 (Sistemas de Gestión de Calidad para certificación de productos), ISO 21001 (Sistemas de Gestión de Calidad para Instituciones Educativas), SUGEF 14-09, y 14-17, CobiT 4.1, CobiT 5.0, y 2019 así como el diseño e implementación de Sistemas de Control Interno, documental y de gobierno corporativo.

www.davidrrc.com
In/davidricardorodriguezc/

Panorama de riesgos globales

Introducción y contexto

¿Estamos seguros ante los avances y el uso indiscriminado de la tecnología?

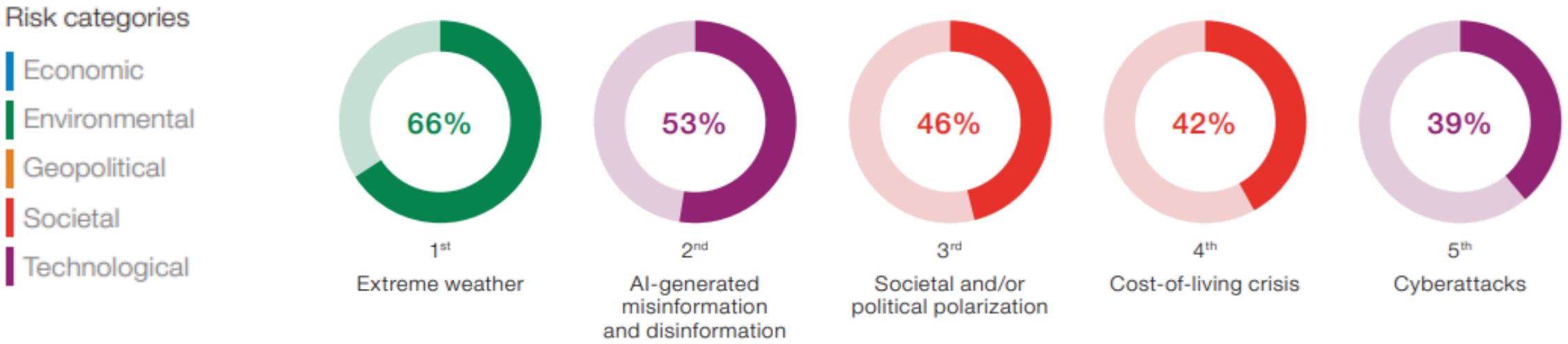


Fuente: Foro Económico Mundial (The Global Risks Report 2024)

Cambios actuales

Transformación digital afecta todos los aspectos de nuestras vidas.

Panorama de riesgos para el 2024



Fuente: Foro Económico Mundial (The Global Risks Report 2024)

Panorama de riesgos corto y largo plazo

Fuente: Foro Económico Mundial (The Global Risks Report 2024)

¿Cuál es el origen y evolución de la Seguridad de la Información y la Ciberseguridad?

1960
Primeros intentos

1960
- MIT
- Confidencialidad datos en Red

1969
- ARPANET

1970
Desarrollo de redes y protocolos

1970
- Control de acceso
- ★ Modelo Bell-LaPadula

1973
- Protocolo TPC-IP

1980
Primeros virus
Concepto de seguridad

1983
- Primer virus (Creeper)
- Primer antivirus (Reaper)
- ARPANET

1986
- Computer Fraud and Abuse Act (CFAA)
- EE.UU.

1990
Expansión del Internet
Estándares de Seguridad

1991
- World Wide Web
- Hace a Internet accesible al público

1995
- ISO 17799
- Gestión de la seguridad de la información

2000
Sofisticación de Ataques
Protección de IC*

2000
- Virus ILoveYou
- 50 Millones de usuarios a nivel global
- Daños por 10 mil millones de USD

2001
- ISO 27001
- Gestión de la seguridad de la información

2007
- Ataque de virus Stuxnet
- Ciberataque a IC

2010
Conciencia global sobre privacidad y ciberseguridad

2013
- Filtraciones de la Agencia de Seguridad Nacional de EEUU
- Caso: Snowden

2014
- Ataques cibernéticos masivos
- Sony Pictures daños por 200 millones USD
- NIST CSF v 1

2016
- Ataque de virus WannaCry
- Ciberataque a IC

2020
Prioridad estratégica
Auge de la IA

2020
- Ataques por phishing y ransomware
- Covid-19

2021
- Ataque de cadena de suministros de proveedores de Software
- SolarWinds

2023
- ISO 27001 y 27002
- NIST CSF 2.0
- Uso de IA y Blockchain para protección de datos personales

* IC: Infraestructuras críticas

Algunos datos relevantes

Fuente: Foro Económico Mundial (The Global Risks Report 2022)

Fundamentos teóricos

Conceptos generales

Marcos de supervisión y regulación internacional sobre ciberseguridad

Seguridad de la información

- Es el conjunto de **medidas preventivas y reactivas** que afectan al tratamiento de los datos almacenados y que permite almacenar y proteger la información.

Seguridad informática

- Es la disciplina que en encarga de **proteger la integridad y la privacidad de la información** almacenada y utilizada en los sistemas informáticos de cibercriminales

Ciberseguridad

- Es la **práctica de defender**, con tecnologías o prácticas ofensivas, las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, redes y los datos **de ataques maliciosos**.

Ciberresiliencia

- Es la capacidad para **prepararse, responder** y **recuperarse** de **ataques cibernéticos** y **violaciones de datos** mientras continúa operando de manera efectiva.

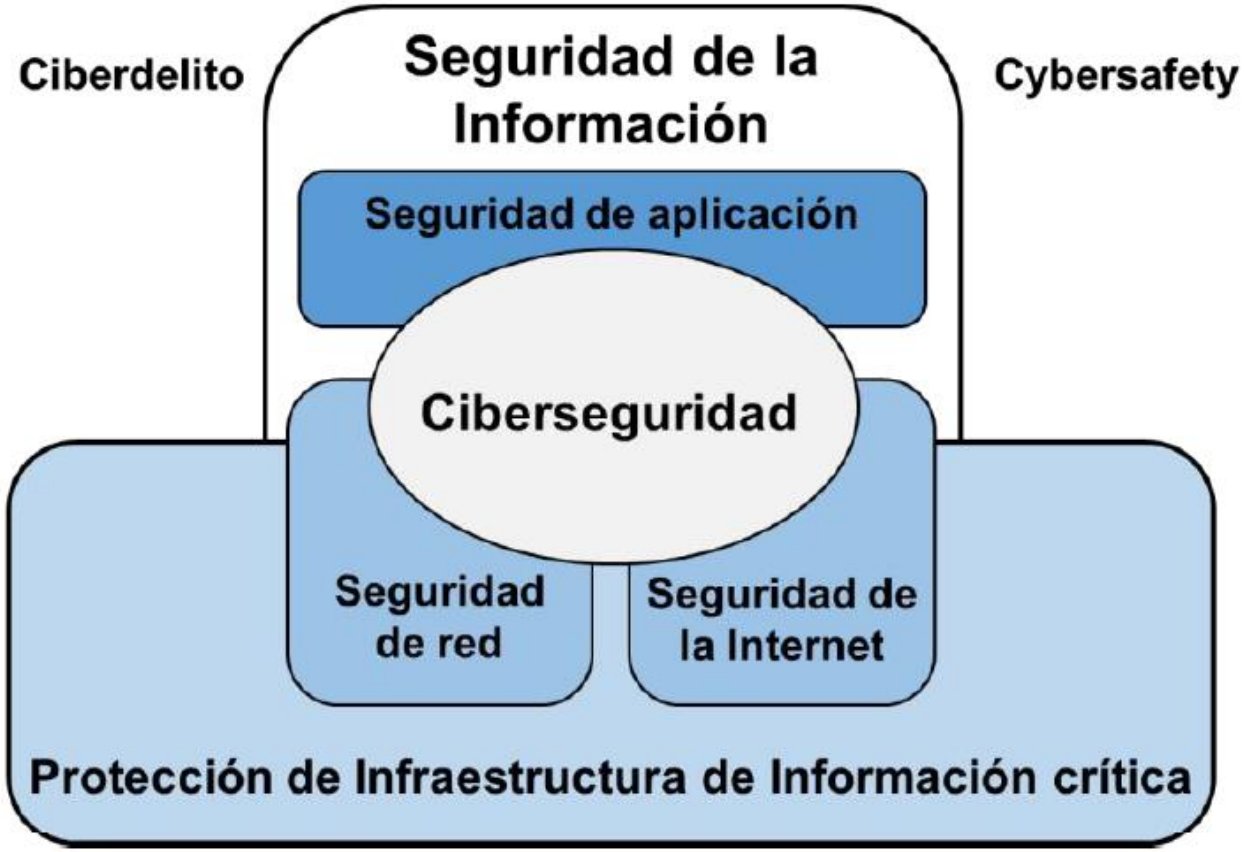
CobiT

- APO12 Gestionar los riesgos
- APO13 Gestionar la seguridad
- DSS02 Gestionar las peticiones e incidentes
- DSS04 Gestionar la continuidad
- DSS05 Gestionar los servicios de seguridad

Fuentes: ISO/IEC 27032:2017; Cyber Lexicon del Financial Stability Board; ISACA CobiT

¿Cuál es la relación de la Seguridad de la Información y la Ciberseguridad?

Internet



La Internet

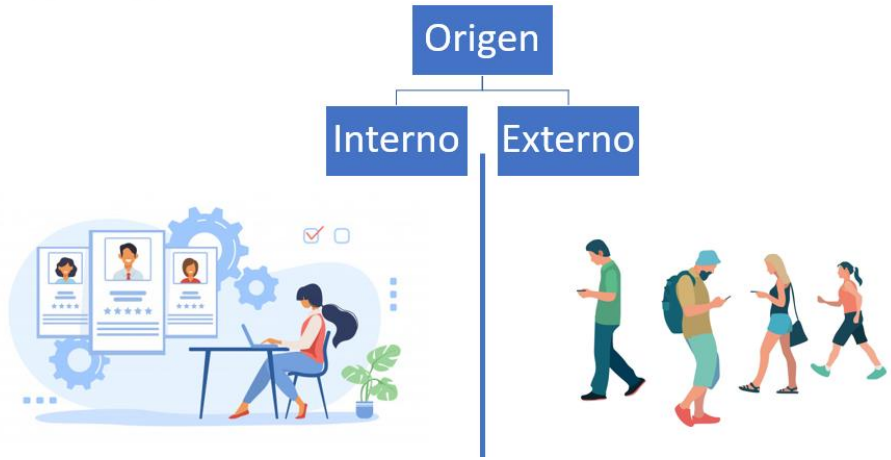
Figura 1 - Relación entre la ciberseguridad y otros dominios de seguridad

Fuente: ISO/IEC 27032:2017

Riesgos Cibernéticos

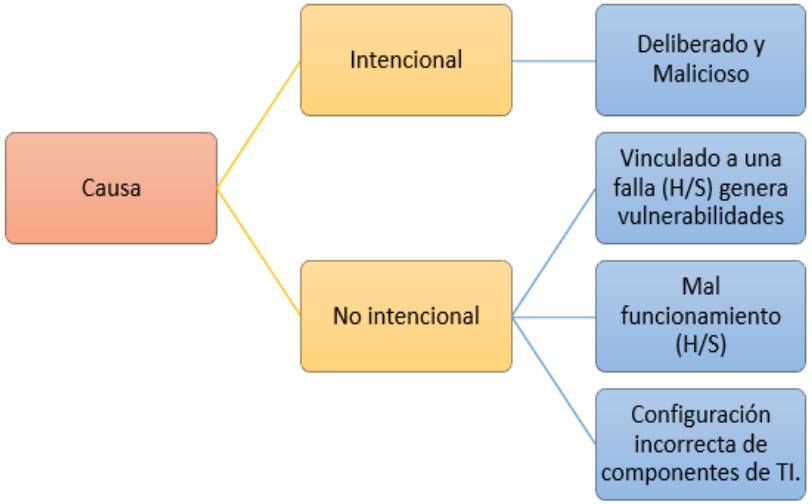
Caracterización e interrelaciones

Caracterización e interrelaciones



Actores

- Personal no capacitado
- Empleados descontentos
- Empleados deshonestos
- Competidores
- Delincuentes internacionales
- Crimen organizado
- Activistas ("hacktivistas")
- Entidades patrocinadas por el gobierno



Análisis del impacto

- Generalmente se analiza de forma independiente
- Un evento de riesgo cibernético **no está aislado** ni confinado, sino que a menudo desencadena una serie de eventos consecuentes
- La **evaluación** del impacto del posible riesgo cibernético, dentro del marco más amplio de gestión de riesgos

SUGESE
Superintendencia General de Seguros

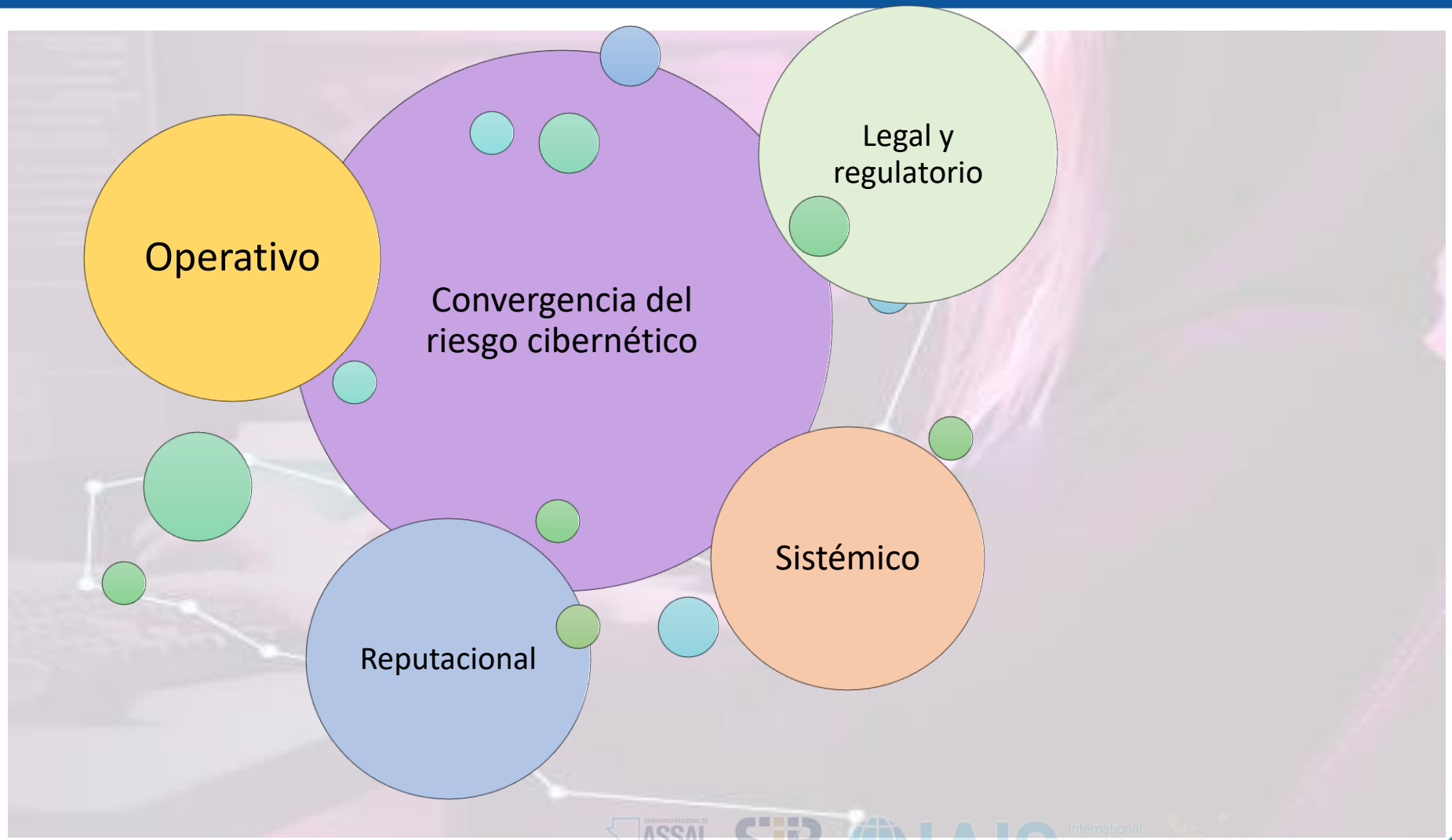
Caracterización e interrelaciones

Principales tipos de ataques

- Ransomware
- Robo de datos
- Ataque a terceros
- Exposición de información por vulnerabilidades de software
- Filtración de datos por ex - empleados

Fuente: https://www.marsh.com/mx/risks/global-risk.html

Caracterización e interrelaciones



Marcos y modelos de supervisión

Relacionados con la ciberseguridad

¿Cuál son Marcos y modelos de supervisión – Relacionados con la ciberseguridad ?

(2016 – abr)

"Documento temático sobre riesgo cibernético al sector de seguros" (**IAIS**)

(2016 – oct)

"Elementos fundamentales de ciberseguridad para el sector financiero" (**El G7**)

(2017)

"Enfoques regulatorios para mejorar los marcos de ciberseguridad de los bancos" (**BIS**)

(2019 – abr)

"Directrices sobre la gestión de riesgos de TIC y seguridad" Autoridad Bancaria Europea (**ABE**)

(2020 – set)

Reglamento del **Parlamento Europeo** y del consejo sobre la resiliencia operativa digital del sector financiero

"Orientación sobre resiliencia cibernética para infraestructuras de mercados financieros" (**BIS**) (**IOSCO**)

(2016 – jun)

"Iniciativa de Fortalecimiento de la Ciberseguridad (CFI)" Hong Kong Monetary Authority (**HKMA**)

(2016 – dic)

"Supervisión del riesgo de seguridad cibernética" (**Toronto Centre**)

(2018 – dic)

"Prácticas efectivas para la respuesta y recuperación de incidentes cibernéticos" El Consejo de Estabilidad Financiera (**FSB**)

(2020 – oct)

"Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad" (**SFC**)

(2020 – nov)

Enfoques regulatorios para mejorar los marcos de ciberseguridad de los bancos (BSI)

Ciberseguridad como un elemento específico

Ciberseguridad desde un **enfoque holístico**

Marcos y mejores prácticas de referencia

Relacionados con la ciberseguridad

Marcos de supervisión y regulación internacional sobre ciberseguridad

Estándares del NIST

- NIST CSF (National Institute of Standards and Technology - Cybersecurity Framework) - Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología.

Ciberresiliencia INCIBE

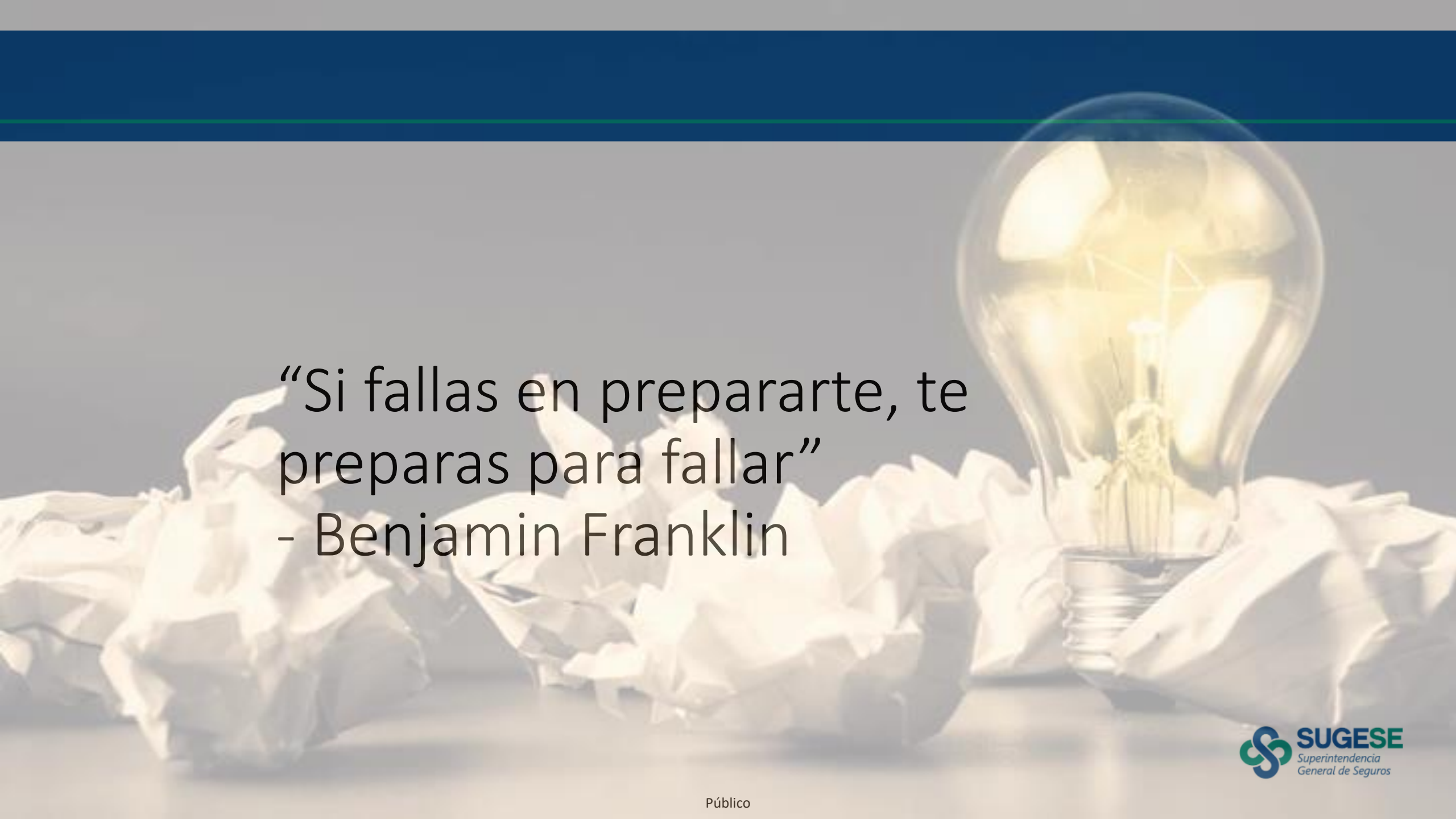
ISO / IEC Familia de Normas 27000

HITRUST CSF (Health Information Trust Alliance - Cybersecurity Framework)

Cloud Security Alliance (CSA) Cloud Controls Matrix

Critical Security Control (CIS Control) del Center for Internet Security

COBIT 4 – 5 – 19


“Si fallas en prepararte, te preparas para fallar”
- Benjamin Franklin

Ciberseguridad a nivel país

Costa Rica

Ciberseguridad a nivel país

Decreto Ejecutivo número 37052-MICIT del 9 de marzo de 2012

- Creación del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) ente coordinador de la ciberseguridad y seguridad de la información nacional.

Directriz No 133-MP-MICITT abril 2012

- Cumplir con lo que realice el CSIRT-CR
- Resiliencia de la infraestructura

Protocolo de Ciberseguridad del MICITT-ICE-CNE (Alineado al NIS CSF)

Estrategia Nacional de Ciberseguridad (ENC) 2017 – 2021

- Objetivos 2030 para el Desarrollo Nacional
- PND 2014-2018
- PND Telecomunicaciones 2015-2021

Alerta Técnica de Ciberseguridad MICITT-DGD-DRR-AT-079-2020 Malware “Drovorub”

Presentación de Resultados de la Revisión de la Estrategia Nacional de Ciberseguridad de Costa Rica 14-dic-2021

Normas Técnicas de Tecnología de Información (CobiT 2019)

ASAMBLEA LEGISLATIVA de la República de Costa Rica

Proyecto de Ley de ciberseguridad (2022)

Supervisión Basada en Riesgos y Cumplimiento Normativo

Regulación del Sistema Financiero

Evolución del cumplimiento regulatorio de la supervisión de TI

Hasta el 2009

SUGEF

- Autoevaluación
- Calificación

2009

SUGEF

- SUGEF 14-09
- Marco de Gestión (CobiT 4)
- Modelo de Madurez para calificación

2015

SUGESE

- Propuesta de Supervisión

2022

CONASSIF

- Reglamento General de Gestión de TI
  En proceso análisis temas de ciberseguridad
- Áreas de importancia o Interés de TI

CONASSIF

- Reglamento General de Gestión de TI
  SUGEF 14-17
- Marco de Gestión (CobiT 5)
- Modelo de cumplimiento a un Modelo de principios
- Principio de proporcionalidad
- Permite su alineación a SBR

Ciberataques a Infraestructuras críticas a nivel país

Sitios web y exfiltración de datos

¡Nos encontramos trabajando para habilitar el servicio!

TIC@ y ATV

EDUS

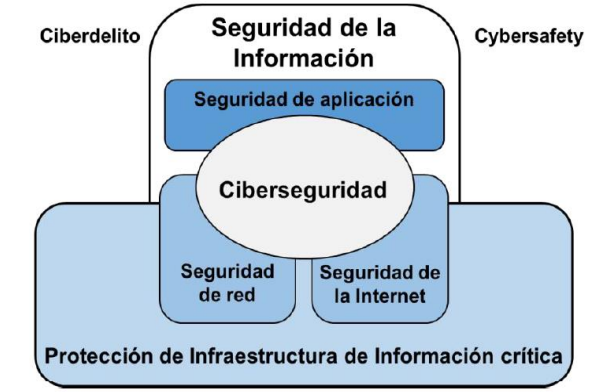


Figura 1 - Relación entre la ciberseguridad y otros dominios de seguridad

Enfoque para regulación y supervisión

Ciberseguridad como un elemento específico

Ciberseguridad desde un enfoque holístico

Abordaje de la regulación

Ciberseguridad desde un enfoque especifico

- NIST CSF v2.0
  - Gobernar
  - Identificar
  - Proteger
  - Detectar
  - Responder
  - Recuperar

Ciberseguridad desde un enfoque holístico

Gobernanza y Gestión de TI

- CobiT
- Refuerzo del SGSI
  - ISO 27001 (Administrativos)
  - ISO 27002 (Técnicos)
    - NIST CSF
    - CIS Controls
    - Otros estándares del NIST

¿Cómo se aliena el NIST CSF con el modelo de procesos del Reglamento de Gobierno y Gestión de TI?

- (P) Gestionar la seguridad cibernética
  - Funciones de seguridad cibernética del NIST

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

(106 Subcategorías)

Controles

CobiT 2019
(Objetivos de Control y sus prácticas y actividades)

- (P) Gestionar la seguridad
  - Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).
    - Definir el alcance y contexto de la organización a nivel local y global.
    - Diseño de Políticas, considerando el contexto.
    - Realizar una declaración de aplicación de controles según el contexto.
    - Definir y comunicar roles y responsabilidades de la seguridad de la información.
    - Comunicar la estrategia de SGSI.

ISO 27002:2022
(93 Controles)

¿Cómo se aliena el NIST CSF con el modelo de procesos del Reglamento de Gobierno y Gestión de TI?

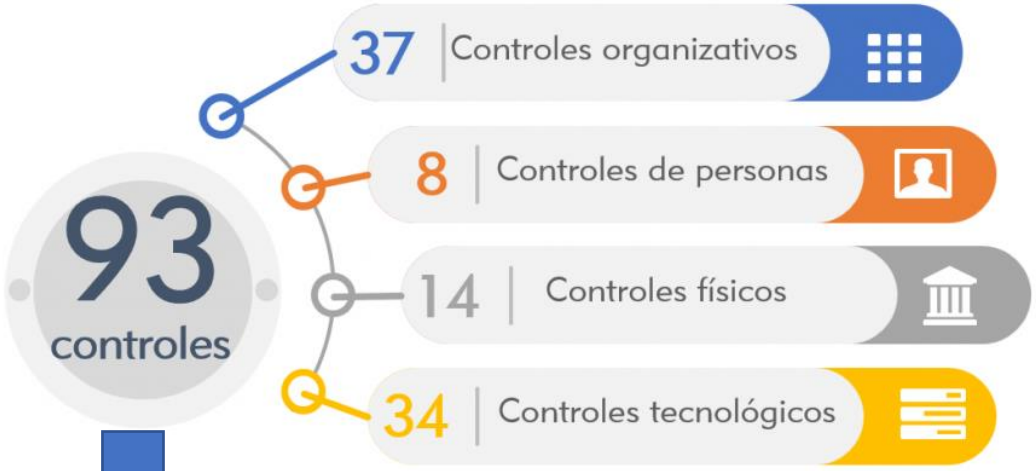
- (P) Gestionar la seguridad cibernética
  - Funciones de seguridad cibernética del NIST

(106 Subcategorías)

Controles

- (P) Gestionar la seguridad
  - Establecer y mantener un sistema de gestión de seguridad de la información (SGSI).
    - Definir el alcance y contexto de la organización a nivel local y global.
    - Diseño de Políticas, considerando el contexto.
    - Realizar una declaración de aplicación de controles según el contexto.
    - Definir y comunicar roles y responsabilidades de la seguridad de la información.
    - Comunicar la estrategia de SGSI.

ISO 27002:2022
(93 Controles)



CobiT 2019
(Objetivos de Control y sus prácticas y actividades)

Atributos de cada control de la ISO 27002:2022

Permiten hacer vistas de los controles según la necesidad de la audiencia

Tipo de Control	Propiedades de seguridad de la información	Funciones de seguridad cibernética	Dominios de Seguridad
•#Preventivo •#Detectivo •#Correctivo	•#Confidencialidad •#Integridad •#Disponibilidad	•#Gobernar (v.2.0) •#Identificar •#Proteger •#Identificar •#Responder •#Recuperar	•#Gobernanza_y_Ecosistema •#Protección •#Defensa •#Resiliencia

Reglamento General de Gobierno y Gestión de la Tecnología de Información

Capítulo I. Disposiciones generales

- Artículo 1 Objeto
- Artículo 2 Alcance
- Artículo 3 Regulación proporcional
- Artículo 4 Definiciones y abreviaturas
- Artículo 5 Lineamientos Generales

Capítulo II. Gobierno y Gestión de TI

- Sección I: Marco de gobierno y gestión de TI (2 artículos)
- Sección II Responsabilidades del Órgano de Dirección (3 artículos)
- Sección III Responsabilidades de la Alta Gerencia y del Comité de TI o de la función equivalente (3 artículos)
- Sección IV Responsabilidades de los Órganos de control (2 artículos)

Capítulo III. Organización de las tecnologías de información

- Sección I Generalidades de la unidad de TI (2 artículos)
- Sección II: Tratamiento de datos y aplicaciones (3 artículos)
- Sección III: Gestión de la computación en la nube (3 artículos)
- Sección IV: Tercerización de bienes y servicios de TI (6 artículos)

Capitulo IV. Gestión de la seguridad de la información y de la seguridad cibernética

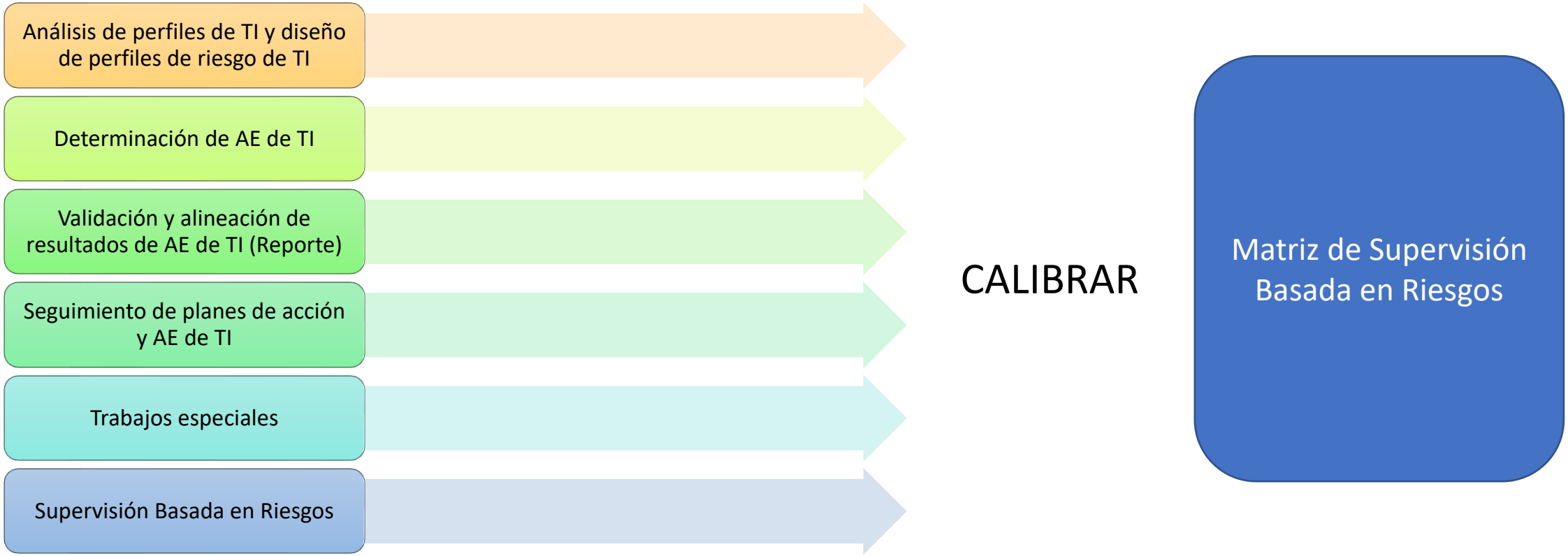
- Sección I: Gestión de la seguridad de la información y de la seguridad cibernética (5 artículos)
- Sección II: Incidentes de seguridad cibernética (6 artículos)

Capitulo V . Auditoría Externa de TI

- Sección I: Perfil tecnológico (4 artículos)
- Sección II: Auditoría externa (6 artículos)
- Sección III: Reporte de supervisión y plan de acción (3 artículos)
- Sección VI: Prorrogas (2 artículos)

Disposiciones adicionales (2 disposición)
Disposiciones transitorias (2 disposiciones)
Disposiciones derogatorias (1 disposición)

Supervisión de TI



Modelo de SBR aplicado a TI

SBR							
1. Actividad significativa	2. Riesgo Inherente - Operativo -	3 . Gestión	4 . Funciones de Control				
		Gestión Operativa de TI	Cumplimiento Normativo	Gestión de Riesgo	Auditoría Interna	Alta Gerencia -Gerencia General- -Director de TI-	Organo de Dirección
TI	Perfil tecnológico	MGTI Conocimiento informado	MGTI Conocimiento informado	MGTI Conocimiento informado	MGTI Conocimiento informado	MGTI Conocimiento informado	MGTI Conocimiento informado

Fortalezas

Debilidades

Riesgos

Oportunidades de mejora

Matriz del Modelo SBR alineado al Marco de Gestión

SBR								MARCO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN		
1. Actividad significativa	2. Riesgo Inherente - Operativo -	3. Gestión Operativa de TI	4 . Funciones de Control					IDENTIFICADOR	PROCESOS	AÑO
			Cumplimiento Normativo	Gestión de Riesgo	Auditoría Interna	Alta Gerencia -Gerencia General- -Director de TI-	Organo de Dirección			
TI	Perfil tecnológico					X	X	1.1	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	1
						X	X	1.2	Asegurar la Entrega de Beneficios	1
				X		X	X	1.3	Asegurar la Optimización del Riesgo	1
						X	X	1.4	Asegurar la Optimización de Recursos	1
						X	X	1.5	Asegurar la Transparencia hacia las Partes Interesadas	1
						X		2.1	Gestionar el Marco de Gestión de TI	1
						X		2.2	Gestionar la Estrategia	1
						X		2.3	Gestionar la Arquitectura Empresarial	4
		X						2.4	Gestionar el portafolio de servicios	4
						X		2.5	Gestionar el presupuesto y los costos	3
						X		2.6	Gestionar los recursos humanos	4
						X		2.7	Gestionar las relaciones entre TI y el negocio	4
		X						2.8	Gestionar los acuerdos de niveles de servicio	1
						X		2.9	Gestionar los servicios de los proveedores de TI	1
						X		2.10	Gestionar la Calidad	5
		X		X		X		2.11	Gestionar el riesgo de TI	2
						X		2.12	Gestionar la seguridad	2
						X		3.1	Gestionar programas y proyectos	1
		X						3.2	Gestionar la definición de requerimientos	4
		X						3.3	Gestionar la identificación y construcción de soluciones	3
		X						3.4	Gestionar la disponibilidad y capacidad	3
		X						3.5	Gestionar los cambios	2
		X						3.6	Gestionar la aceptación del cambio y la transición	4
		X						3.7	Gestionar los activos de TI	3
		X						3.8	Gestionar la configuración	3
		X						4.1	Gestionar las operaciones	3
		X						4.2	Gestionar peticiones e incidentes de servicio	1
		X						4.3	Gestionar los problemas	3
						X		4.4	Gestionar la continuidad	2
		X						4.5	Gestionar servicios de seguridad de la información	2
						X		4.6	Gestionar controles de proceso de negocio	2
						X		5.1	Supervisar, evaluar y valorar el rendimiento y la conformidad	5
			X		X			5.2	Supervisar, evaluar y valorar el sistema de control interno	2
			X		X			5.3	Supervisar, evaluar y valorar la conformidad con los requerimientos externos	5

Fortalezas

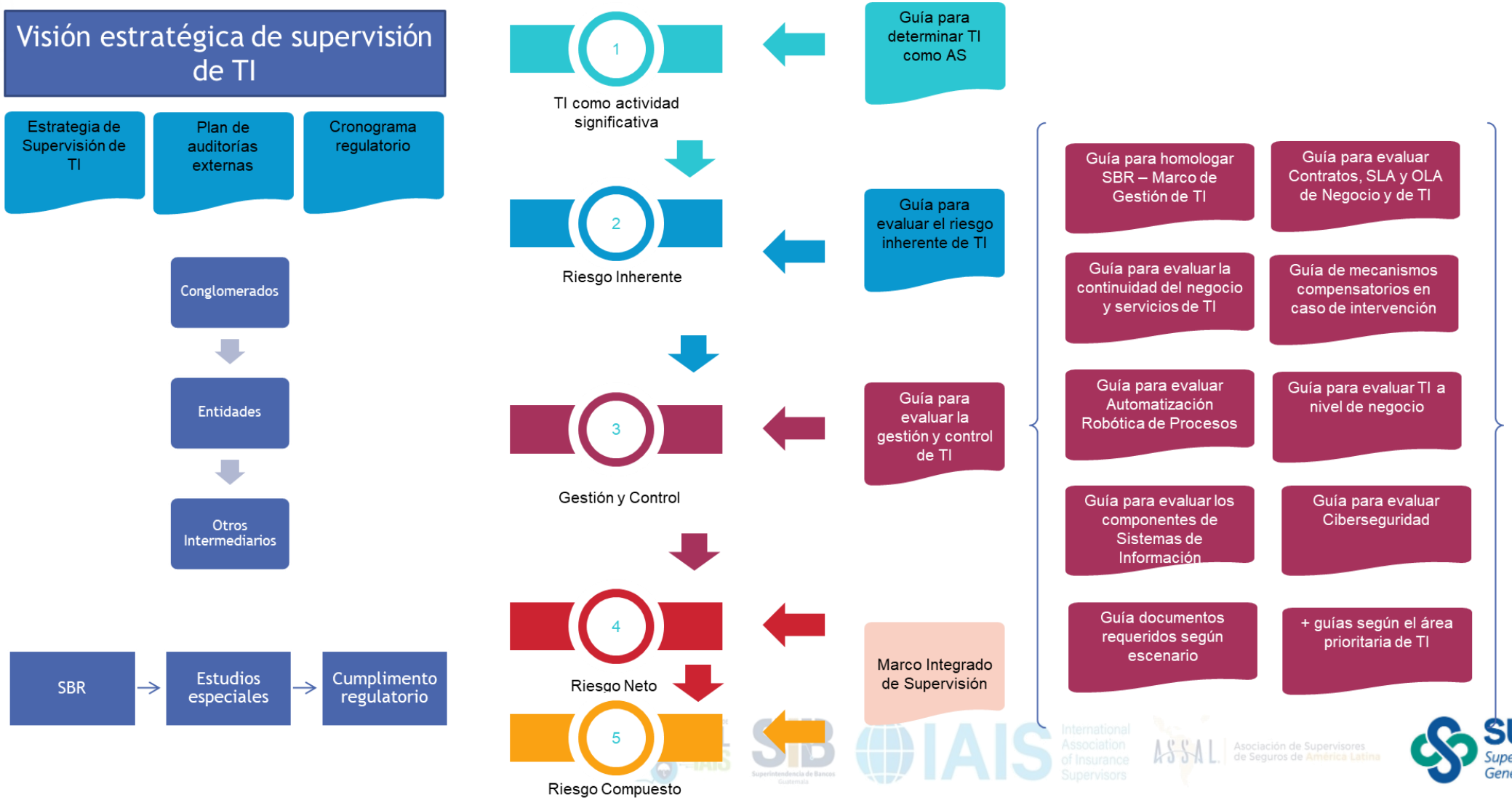
Debilidades

Riesgos

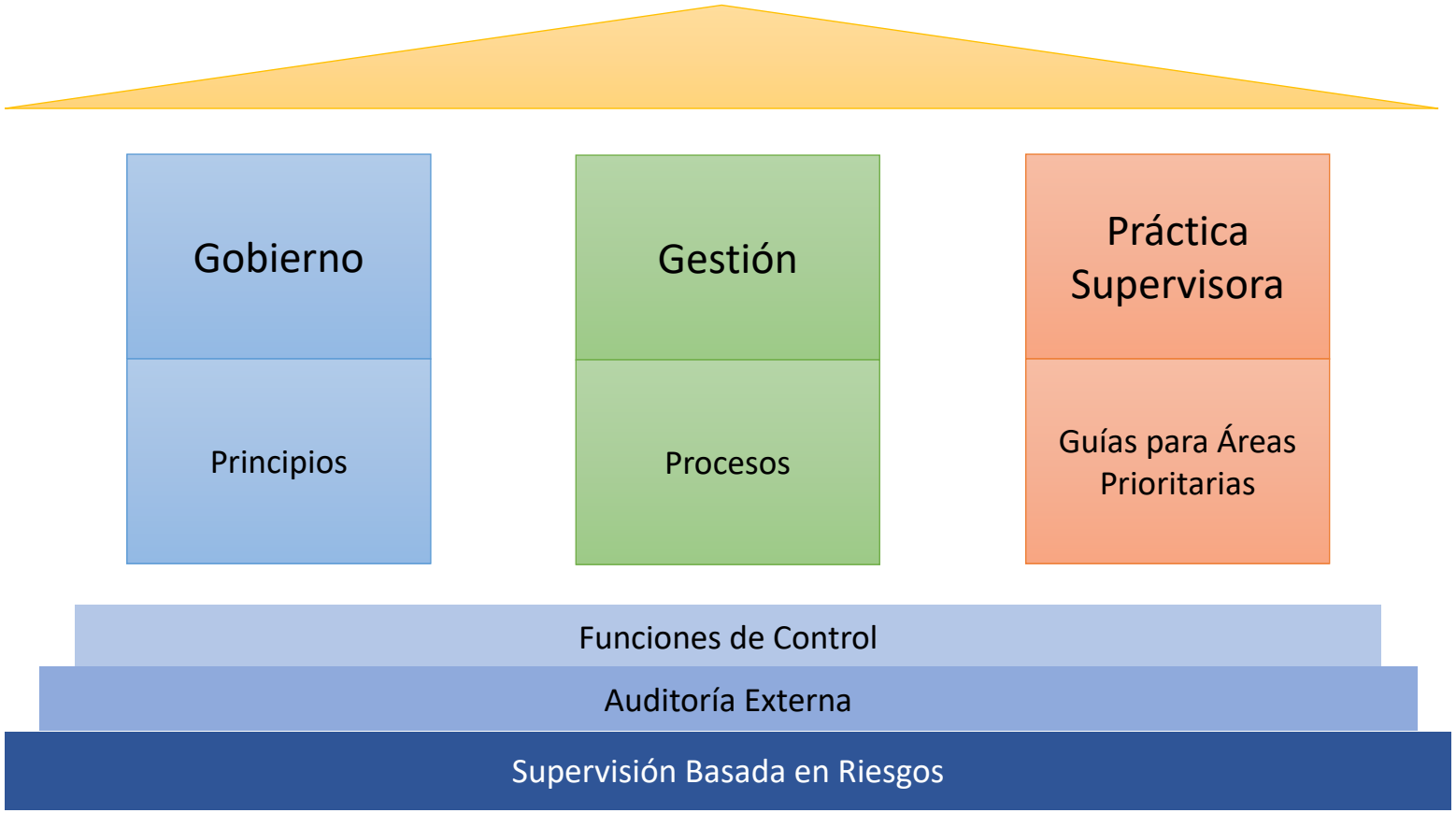
Oportunidades de mejora

SUGESE Superintendencia General de Seguros

Proceso de SBR de TI – Ciberseguridad y otras áreas prioritarias



Pilares de la regulación y supervisión



Propuesta de regulación

1 Gobierno

Principios

2 Gestión

Procesos

3 Práctica Supervisora

Enfoque en Áreas Prioritarias

Áreas Prioritarias 4

IA	RPA
Machine Learning	Big Data
Cloud Computing	Blockchain
API's	IoT

Ciberseguridad

Ciber delincuentes

5 Centro de Respuesta de Incidentes de Seguridad Informática

Protección de la Cadena de Proveedores Críticos de Suministros de Información y de Servicios de TI

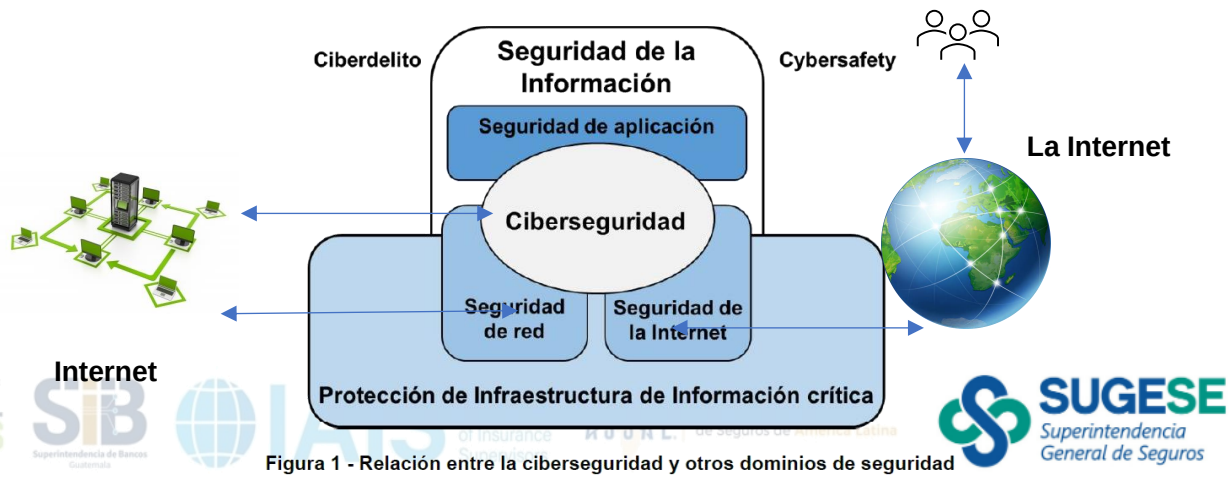


Figura 1 - Relación entre la ciberseguridad y otros dominios de seguridad

Reflexiones finales

- Los modelos de supervisión internacional sobre ciberseguridad tienen dos enfoques
  - Ciberseguridad dentro de un enfoque Holístico.
    - Aplicable cuando existe regulación que incorporar marcos de gestión de TI.
  - Ciberseguridad como un elemento especifico dentro de la regulación.
    - Aplicable cuando no existe regulación sobre marcos de gestión de TI, y se requiere implementar los mecanismos de control específicos.
- Un reglamento con un enfoque holístico permite mejorar la gobernanza y gestión de las entidades supervisadas.

- El Reglamento General de Gobierno y Gestión de la TI permite alinear las **áreas de enfoques más relevantes** de TI dentro del modelo de supervisión basada en Riesgo.
  - Seguridad/Ciberseguridad/Ciberresiliencia
  - IoT/IA/RAP
  - DevOp
- TI como actividad significativa dentro del modelo de SBR, permite alineación de estándares, prácticas y marcos de referencia.

- Las AE de TI, los trabajos especiales y de SBR permiten calibrar los resultados de la matriz de SBR de cada entidad, a partir del conocimiento informado de la entidad y los resultados de pruebas técnicas de seguridad de la información y seguridad cibernética.

- Se debe supervisar la adopción, adaptación y cumplimiento del Marco de gobierno y gestión de TI, de conformidad con el principio de proporcionalidad, el apetito de riesgo, los objetivos y su modelo de negocio.

¡Muchas Gracias!

La seguridad de la información y la seguridad cibernética o ciberseguridad es responsabilidad de todos no solo de las áreas de TI