DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Unidad 3: Planeando la ciberseguridad

Sistemas de gestión de la seguridad

Profesor
Juan Ignacio Iturbe A.

Frameworks de Seguridad

- En este punto ya sabemos que necesitamos cumplir (CIA).
- Conocemos que herramientas usar (controles administrativos, técnicos y físicos)
- Y las definiciones que hay que manejar (vulnerabilidades, amenazas, riesgo, control).
- Ahora se necesita construir un programa de seguridad para lo amplio de la organización.

Frameworks de Seguridad

- Primero, ¿Qué **NO** hacer?
  - Seguridad a través de la oscuridad (se asume que mis enemigos no son tan listos como uno). Ej:
    - Un vendedor que diga que sus productos son mejores que uno *opensource*, ya que los de él son compilados y no se puede ver el código fuente.
    - Un algoritmo criptográfico hecho en casa (Lo mejor es utilizar algoritmos ampliamente reconocidos)
    - Remapear puertos (fácilmente detectable con herramientas)

Frameworks de Seguridad

- Entonces, ¿Qué hacer?
  - Construir una fortaleza (También llamado “Programa de seguridad”) de muchas piezas:
    - Mecanismos de protección lógicos, administrativos, físicos, procedimientos, procesos de negocio y personas.
    - Todos de gran importancia para el marco de trabajo.
    - Si una falla, todo el marco de trabajo se ve comprometido.
    - Este se construye en capas, cada capa da soporte a la siguiente.
    - Se necesitan los planos de la estructura de la fortaleza, por suerte existen estándares en la industria.

Estándares, mejores prácticas y frameworks

- Desarrollo de un programa de seguridad
  - Serie ISO/IEC 27000 estándares internacionales de cómo desarrollar y mantener un ISMS.
- Desarrollo de un arquitectura corporativa (no necesariamente orientado a la seguridad).
  - Zachman framework
  - TOGAF (The Open Group)
  - DoDAF (U.S. Department of Defense)
  - MODAF (British Ministry of Defense)

Estándares, mejores prácticas y frameworks

- Desarrollo de una arquitectura de **seguridad corporativa**
  - SABSA model
- Desarrollo de Controles de Seguridad
  - CobiT
  - SP 800-53 (NIST)
- Gobierno corporativo
  - COSO
- Gestión de procesos
  - ITIL, Six Sigma, CMMI

Serie ISO/IEC 27000

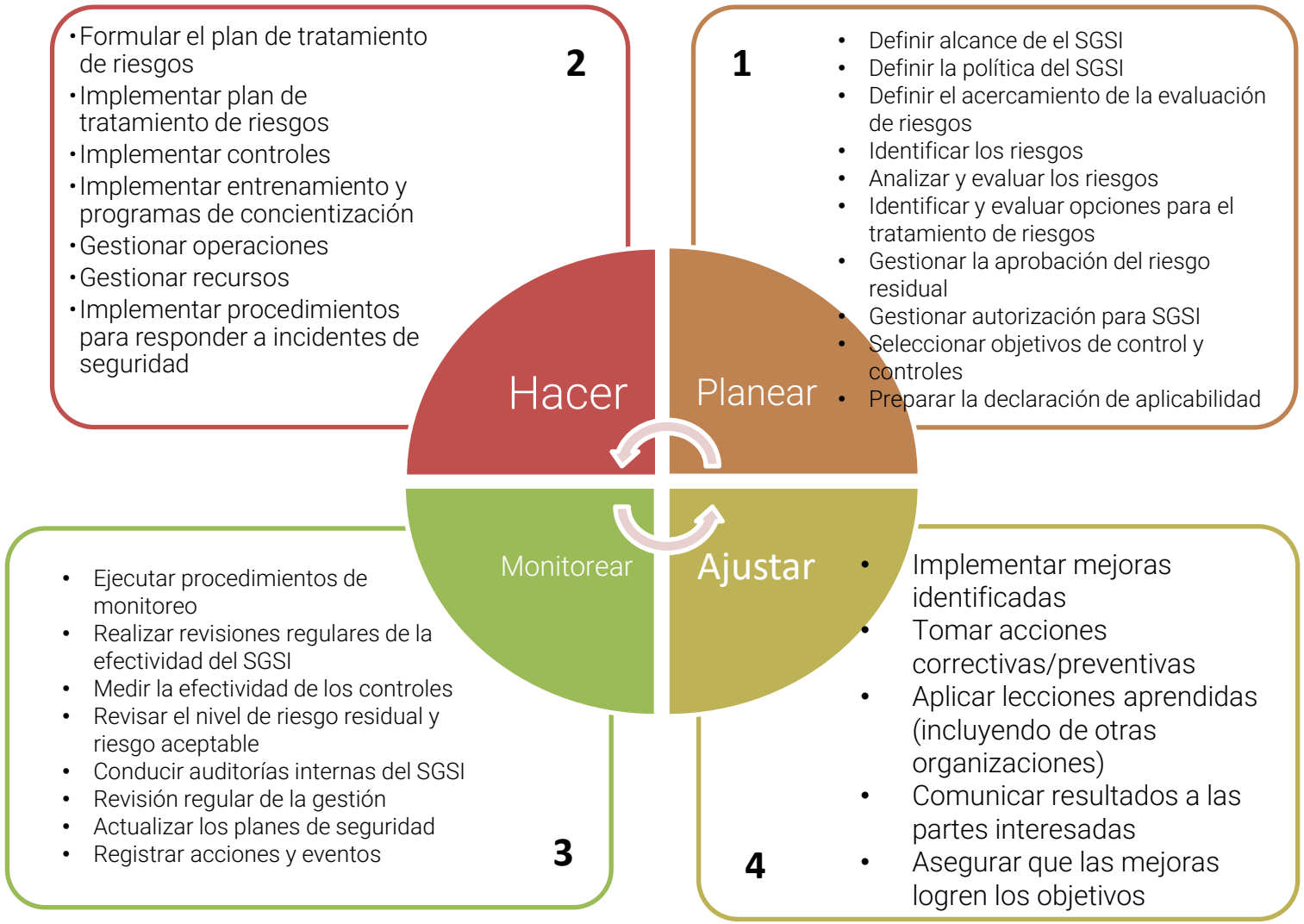
- Nace desde el estándar británico BS7799
- Este estándar delinea de qué trata un ISMS o SGSI (aka programa de seguridad). Y como debe ser este mantenido.
- El objetivo de este es :
  - proveer una guía de cómo diseñar, implementar y mantener políticas, procesos y tecnologías para manejar riesgos y activos con información sensible.
- Se tiene el manejo de los controles de seguridad centralmente **(no adhoc)**.

Serie ISO/IEC 27000

- El BS7799 fue actualizado y derivo en el BS7799v1, BS7799v2, ISO 17799, BS7799-3:2005,etc.
- Finalmente se llego a la serie ISO/IEC 27000 que trata de modularizar y separar los componentes necesarios para el desarrollo de un ISMS.
- ISO sigue el ciclo Plan – DO – Check - Act

Serie ISO/IEC 27000

- Se busca:
  - Políticas de seguridad de la información (IS) para la organización
  - Creación de una infraestructura de IS
  - Clasificación de activos y controles
  - Seguridad del personal
  - Seguridad física y ambiental.
  - Manejo de las comunicaciones y operaciones
  - Control de acceso
  - Desarrollo y mantenimiento de sistemas
  - Manejo de la continuidad de negocio
  - Cumplimiento legales


Hacer
Planear
Monitorear
Ajustar
2
•Formular el plan de tratamiento de riesgos
•Implementar plan de tratamiento de riesgos
•Implementar controles
•Implementar entrenamiento y programas de concientización
•Gestionar operaciones
•Gestionar recursos
•Implementar procedimientos para responder a incidentes de seguridad
1
• Definir alcance de el SGSI
• Definir la política del SGSI
• Definir el acercamiento de la evaluación de riesgos
• Identificar los riesgos
• Analizar y evaluar los riesgos
• Identificar y evaluar opciones para el tratamiento de riesgos
• Gestionar la aprobación del riesgo residual
• Gestionar autorización para SGSI
• Seleccionar objetivos de control y controles
• Preparar la declaración de aplicabilidad
3
• Ejecutar procedimientos de monitoreo
• Realizar revisiones regulares de la efectividad del SGSI
• Medir la efectividad de los controles
• Revisar el nivel de riesgo residual y riesgo aceptable
• Conducir auditorías internas del SGSI
• Revisión regular de la gestión
• Actualizar los planes de seguridad
• Registrar acciones y eventos
4
• Implementar mejoras identificadas
• Tomar acciones correctivas/preventivas
• Aplicar lecciones aprendidas (incluyendo de otras organizaciones)
• Comunicar resultados a las partes interesadas
• Asegurar que las mejoras logren los objetivos

Serie ISO/IEC 27000

- ISO/IEC:
  - 27000 Revisión y vocabulario.
  - 27001 Requerimientos de un ISMS
  - 27002 Código de práctica para el manejo de la IS
  - 27003 Guía para la implementación ISMS
  - 27004 Guía para la IS del manejo de la medidas y métricas
  - 27005 Guía para el manejo de riesgo del IS
  - 27032 Guía para la ciberseguridad
  - …
  - 27034 Guía para la Seguridad de aplicaciones
  - 27035 Guía para la seguridad del manejo de incidentes
  - 27036 Guía para el manejo del outsourcing
  - 27037 Guía para la identificación, recolección, adquisición y preservación de evidencia digital.

Actualización ISO/IEC 27002:2022

- La actualización de la ISO 27002:2022 los organiza en:
  - Organizativos
  - Humanos
  - Físicos
  - Tecnológicos
- Además, los tipifica en:
  - **Preventivo:** el control que pretende evitar la ocurrencia de un incidente de seguridad de la información.
  - **Detectivo:** el control actúa cuando se produce un incidente de seguridad de la información.
  - **Correctivo:** el control actúa después de que se produzca un incidente de seguridad de la información.

- Para cada control se tiene:
  - **Título del control**: Nombre corto del control;
  - **Tabla de atributos**: Una tabla muestra el valor o valores de cada atributo para el control dado;
  - **Control**: Qué control es;
  - **Propósito**: Por qué debería implementarse el control;
  - **Orientación**: Cómo debería implementarse el control;
  - **Información adicional:** Texto explicativo o referencias a otros documentos relacionados.

5.1 Políticas para la seguridad de la información

Tipo de control	Dimensiones de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernanza	#Gobernanza_Ecosistema #Resiliencia

Ejemplo de control

REVISEMOS UN CONTROL

A tener en cuenta

- Cuando se tiene un requerimiento **habilitador de negocio** sobre la arquitectura de seguridad de la empresa, hay que recordar que el objetivo de las empresas es generar dinero. Estas no existen solamente para ser seguras.
- La seguridad no se debe interponer sobre el negocio, pero debe ser implementada de la mano con el negocio.
- La seguridad debe ayudar a realizar a la organización proveyendo mecanismos para hacer las nuevas cosas de forma segura.

A tener en cuenta

- Por ejemplo una compañía puede querer habilitar que su servicio de atención al cliente y soporte trabajen desde la casa.
  - Esto trae un montón de ahorro por ejemplo en arriendo de oficinas, servicios y gastos generales.
- La compañía debe moverse a este nuevo modelo con la utilización de VPN, firewalls, filtrado de contenidos, etc.
- Entonces, la seguridad habilita a la compañía a moverse a un diferente modelo de trabajo proveyendo los mecanismos de protección necesarios.

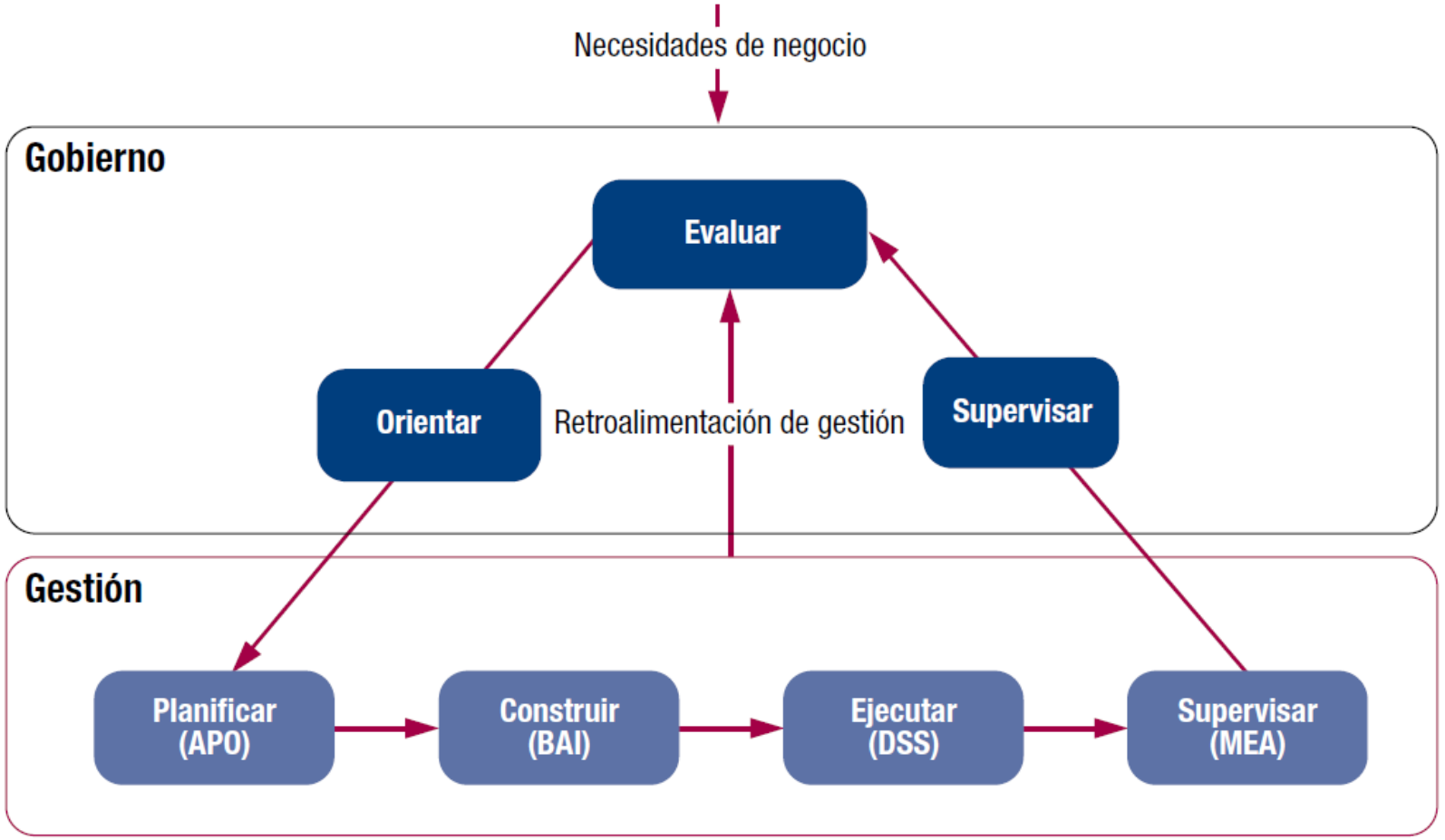
Desarrollo de controles de seguridad

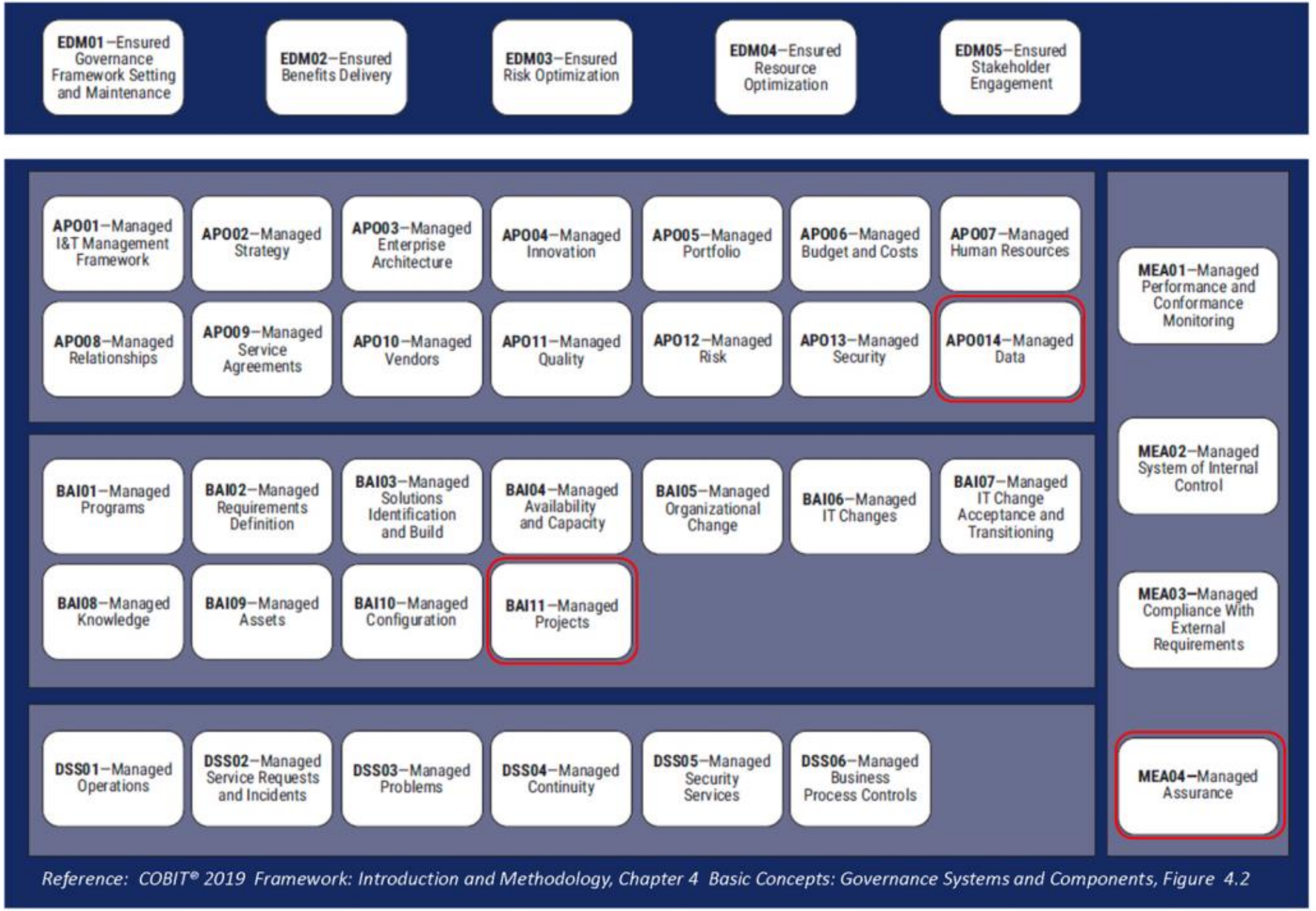
- Hasta ahora se tiene la serie 27000, la cual describe los componentes necesarios de un programa de seguridad de la organización.
- También se tiene la arquitectura de seguridad corporativa, lo cual ayuda a integrar los requisitos descritos en la estructura empresarial existente.
- Ahora nos centraremos en los **objetivos de control** que se podrán en marcha para lograr los objetivos planteados en el programa de seguridad y la arquitectura corporativa.

COBIT

- Desarrollado por ISACA
- Es un marco de gobierno de las tecnologías de información que entrega una serie de herramientas para que la alta dirección pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos de negocio.
- Define los objetivos para los controles que se deben utilizar para la gobernanza y gestión adecuadamente TI y garantizar que TI soporte lo que el negocio requiera.
- Enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio.

Áreas claves de Gobierno y Gestión de COBIT





Ej. COBIT 2019

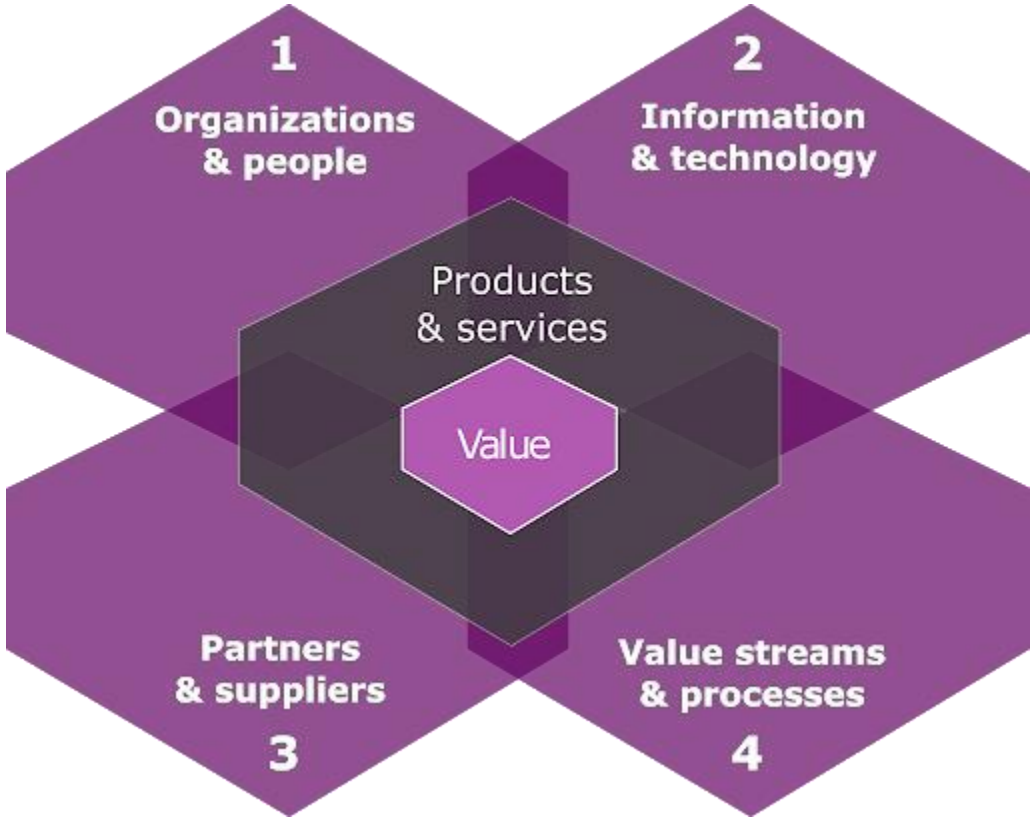
Importante

- Una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas.
- Empresas más pequeñas pueden tener pocos procesos;
- Empresas más grandes y complejas pueden tener numerosos procesos, pero todos con el ánimo de cubrir las mismas metas.

ITIL

- El *Information Technology Infraestructure Library* (ITIL)
- Estándar de facto de las mejores prácticas para el manejo de los servicios de TI.
- Creado por la dependencia entre las necesidades del negocio y las TI.
- Es un conjunto de libros que proveen los objetivos a largo plazo y las actividades necesarias para conseguir estos objetivos.
- Es orientado a brindar, internamente en una empresa, un SLA adecuado.

ITIL v4: Dimensiones

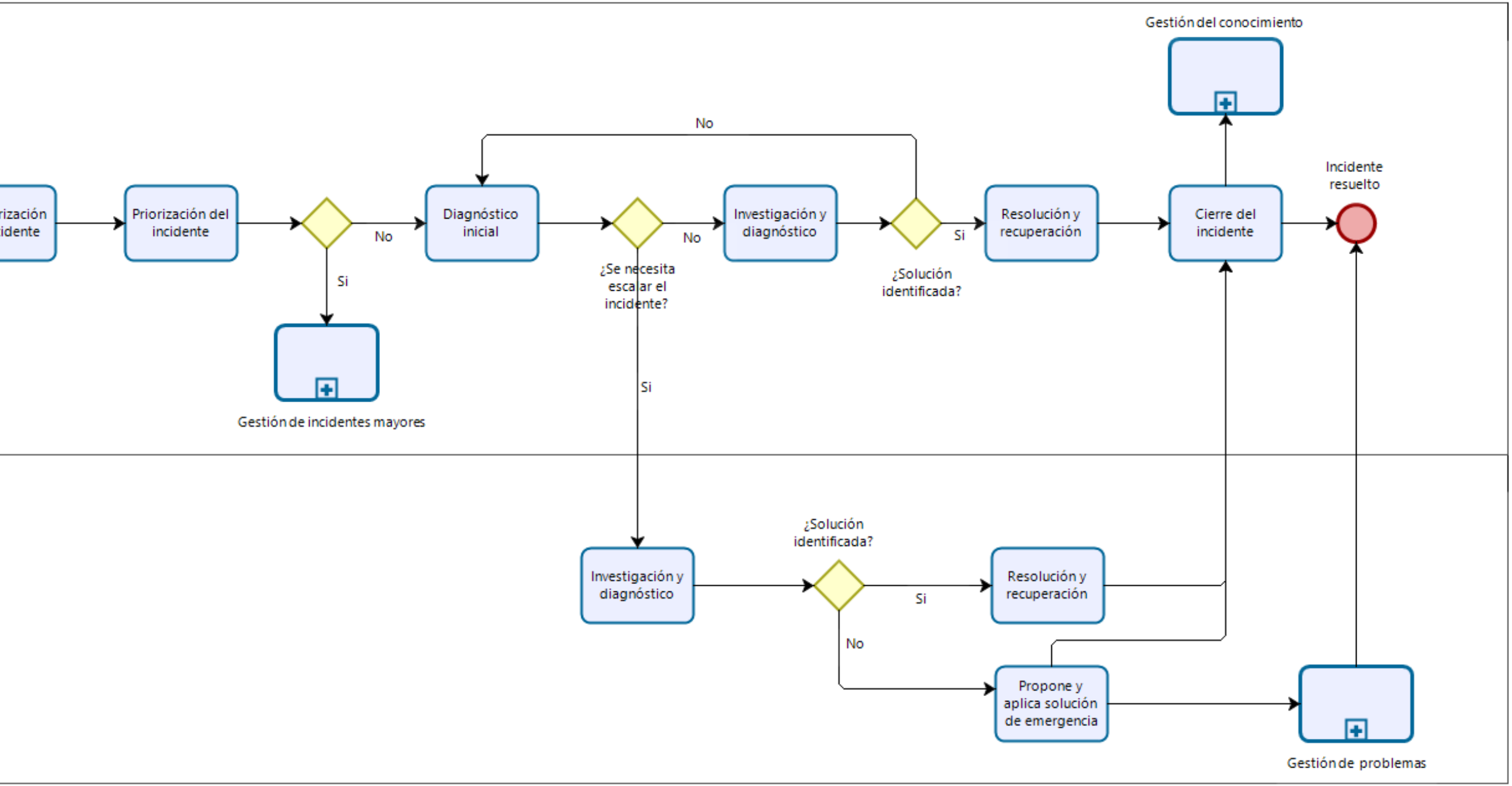


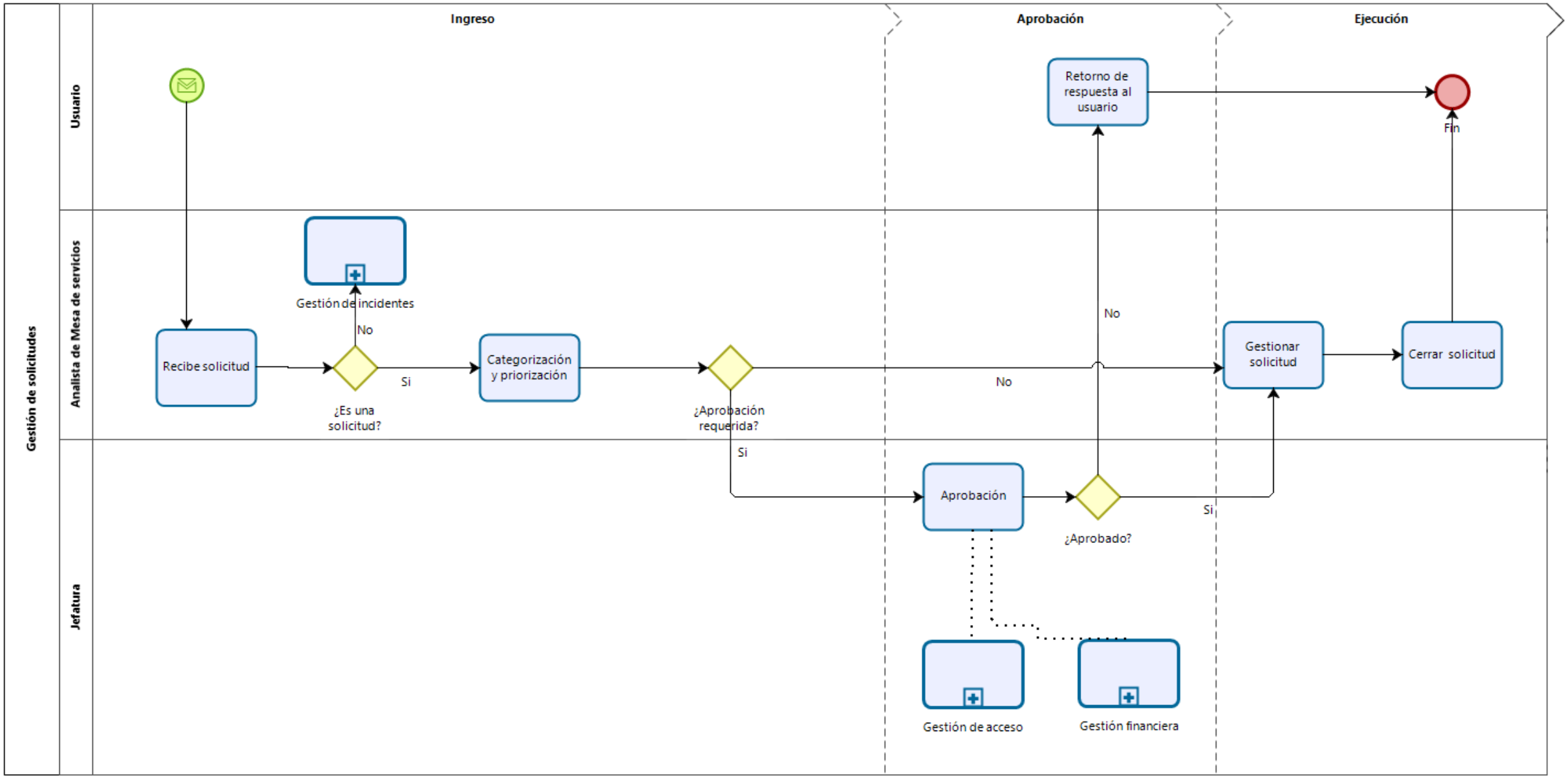
https://www2.deloitte.com/es/es/pages/technology/articles/itil-v4-que-hay-de-nuevo-viejo.html

ITIL v4: Prácticas

General Management Practices	Service Management Practices	Technical Management Practices
Architecture management	Availability management	Deployment management
Continual improvement	Business analysis	Infrastructure & Platform management
Information security management	Capacity & Performance management	Software development & management
Knowledge management	Change control	
Measurement & reporting	Incident management	
Organisational change management	IT asset management	
Portfolio management	Monitoring & even management	
Project management	Problem management	
Relationship management	Release management	
Risk management	Service catalogue management	
Service financial management	Service configuration management	
Strategy management	Service continuity management	
Supplier management	Service design	
Workforce & talent management	Service desk	
	Service request management	
	Service validation & testing	

https://www2.deloitte.com/es/es/pages/technology/articles/itil-v4-que-hay-de-nuevo-viejo.html





Controles CIS

- Los controles CIS (*Center for Internet Security*) son un conjunto de acciones priorizadas y altamente focalizadas.
- Colectivamente forman un conjunto de mejores prácticas de defensa.
- Mitigan los ataques más comunes contra sistemas y redes.
- **La información disponible** para los profesionales de seguridad sobre lo que deberían hacer para proteger su infraestructura **no es escasa**.

Controles CIS

- Como defensores, tenemos acceso a una extraordinaria variedad de información y tecnología:
  - herramientas de seguridad
  - hardware
  - estándares de seguridad
  - entrenamientos y clases
  - certificaciones
  - bases de datos de vulnerabilidad
  - orientación, mejores prácticas
  - catálogos de controles de seguridad
  - innumerables listas de verificación de seguridad
  - puntos de referencia
  - recomendaciones

Controles CIS

- Para la comprensión de las amenazas:
  - *feeds* de información de amenazas
  - informes
  - herramientas
  - servicios de alerta
  - estándares
  - *frameworks* de intercambio de amenazas

Controles CIS

- Para colmo, estamos rodeados de:
  - requisitos de seguridad
  - marcos de gestión de riesgos
  - regímenes de cumplimiento
  - mandatos regulatorios
  - Etc

¿Cuáles son las áreas más críticas que debemos abordar y cómo debe una empresa dar el primer paso para madurar su programa de gestión de riesgos?

¿Dónde y cómo empiezo?

¿cómo podemos encaminarnos con una hoja de ruta de fundamentos y una guía para medir y mejorar?

¿Qué pasos defensivos tienen el mayor valor?

Los controles CIS

- Estos son los tipos de problemas que provocaron y ahora conducen los controles CIS.
- Los controles de CIS han sido madurados por una comunidad internacional de personas e instituciones que:
  - comparten información sobre ataques y atacantes, herramientas, ayudas de trabajo y traducciones.
  - identifican problemas comunes.
  - mapean los Controles de CIS a los marcos regulatorios y de cumplimiento.
  - documentan historias de adopción y compartir herramientas para resolver problemas.

Principios de diseño de los CIS Controls

1. *La ofensiva informa a la defensa:* aprender continuamente y usar aquello demostrado.
2. *Objetivo*: Identificar los puntos más críticos que deben hacer para detener los ataques.
3. *Factibilidad:* Todas las recomendaciones individuales (Salvaguardias) deben ser específicas y prácticas de implementar.
4. *Métricas:* Todos los controles CIS deben ser medibles.
5. *Adaptado:* Crear y demostrar una “Coexistencia pacífica” con otros esquemas.

Grupos de implementación (IG)

- Desde la versión 7.1 de los CIS Controles introduce los grupos de implementación (IG).
- Históricamente, los Controles CIS utilizaron su orden para enfocar las actividades de ciberseguridad.
- Muchas de las prácticas dentro de los controles de higiene cibernética CIS pueden ser difíciles de implementar para organizaciones con recursos limitados.
- Por lo que CIS actualizó su guía para priorizar la utilización del Control CIS.
- El IG 1 es definido como “Ciber Higiene Básico”

Grupos de implementación

- Cada IG identifica un subconjunto de los Controles CIS para una organización con un perfil de riesgo y recursos similares.
- Cada IG se basa en el anterior.
- Las organizaciones deben implementar salvaguardias (ó sub-controles en v7.1) en IG1, seguidos por IG2 y luego IG3.

- Una empresa IG1 es de tamaño pequeña a mediana.
- Experiencia limitada en TI y ciberseguridad.
- La principal preocupación de estas empresas es mantener el negocio operativo.
- La sensibilidad de la información que ellas tratan de proteger es baja.
- Las Salvaguardas implementables con limitada experiencia en ciberseguridad
- Dirigidas a frustrar ataques generales y no dirigidos.
- Salvaguardas se diseñan para trabajar en conjunto con software y hardware disponible de fuentes comerciales.

- Una empresa IG2 emplea a individuos responsables de administrar y proteger la infraestructura de TI.
- Estas empresas se apoyan de múltiples departamentos con distintos perfiles de riesgo.
- Almacenan procesos e información sensible sobre el cliente o información empresarial.
- Pueden soportar breves interrupciones de servicios.
- La mayor preocupación es la pérdida de la confianza del público si se produce una brecha.
- Las Salvaguardas ayudan a los equipos de seguridad a hacer frente al incremento de la complejidad operacional.
- Algunas Salvaguardas están sujetas al grado de tecnología y nivel empresarial, experiencia especializada para ser instaladas y configuradas correctamente.

- Una empresa IG3 emplea expertos en seguridad los cuales se especializan en diferentes facetas de la ciberseguridad.
- Los activos e información contienen información sensible o funciones que están sujetas a supervisión regulatoria y de cumplimiento.
- Deben abordar la disponibilidad y la confidencialidad e integridad de los datos sensibles.
- La materialización de los ataques puede causar un daño significativo al bienestar público.
- Las Salvaguardas deben reducir los ataques dirigidos por un adversario sofisticado y reducir el impacto de los ataques de día cero.

Estructura del documento de los Controles CIS

La presentación de cada Control en este documento incluye los siguientes elementos:

- **Resumen:** Una breve descripción de la intención del Control y su utilidad como acción defensiva
- **¿Por qué es Crítico este Control?** Una descripción de la importancia del Control en el bloqueo, mitigación o identificación de ataques, y la explicación de cómo los atacantes activamente explotan la ausencia de este control
- **Procedimientos y Herramientas:** Una descripción técnica de los procesos y tecnologías disponibles y automatización para este Control
- **Salvaguardas:** Un listado de acciones específicas que las empresas deben tomar para implementar el Control

Controles CIS: ¿Qué es lo que deberíamos estar todos haciendo?

Ejemplo de control

REVISEMOS UN CONTROL

Conclusiones (1/2)

- Todo programa de seguridad debe seguir un acercamiento Top-Down.
  - Este asegura que la administración de la empresa está preocupada por proteger sus activos.
  - Se suministran los recursos necesarios para su construcción.
  - Se asegura el seguimiento de las políticas generadas.
- Un acercamiento Bottom-up
  - es menos efectivo.
  - No abarca todos los riesgos
  - Y finalmente falla estrepitosamente

Conclusiones (2/2)

- Ninguna organización va a colocar todos los estándares vistos anteriormente en práctica.
- Pero estas son buenos *toolbox* de donde sacar las herramientas **adecuadas** para nuestra organización.
- A medida que el programa de seguridad madura, se van utilizando.
- Toda organización es distinta, pero todas están compuestas de **gente, procesos, datos y tecnologías** y cada una de ellos debe ser protegidos.

Actividad formativa: Controles CIS

- De acuerdo al caso de estudio:
  - Seleccione el mayor riesgo del caso de estudio.
  - Seleccione uno o más controles CIS para mitigar dicho riesgo.
  - Justifique la disminución del impacto y la probabilidad en función del control seleccionado.
  - Desarrolle un análisis de riesgos cualitativo y súbalo a la actividad formativa.

Recursos bibliográficos

- Alineando CobiT 4.1, ITILv3 e ISO 27002 en beneficio del negocio [Link]
- Cobit 5 en español. [Link]
- Introducción a COBIT 5 [Link]
- Cobit 4.1