Exacta
Consulting Training Solutions

Evaluación de controles internos informáticos

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

DGRV
Confederación Alemana de Cooperativas

CONTENIDO

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

DGRV Confederación Alemana de Cooperativas

Exacta Consulting Training Solutions

CAPÍTULO 0: Introducción a la Gestión de Riesgos Tecnológicos

Definición de servicios

ITIL define Servicio como “Un medio de entregar valor a los clientes, facilitando los resultados que el cliente quiere *sin ser los propietarios de los costes ni de los riesgos específicos*”.

Tipos de servicios

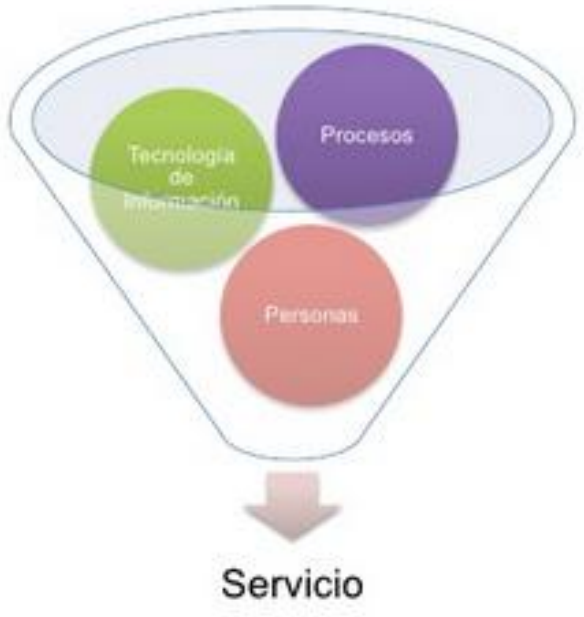
Los servicios pueden ser:

- **Servicios Internos:** son servicios entregados entre departamentos o Unidades de Negocio de la misma organización.
- **Servicios Externos:** son servicios ofrecidos a clientes externos.

Otros tipos de servicios

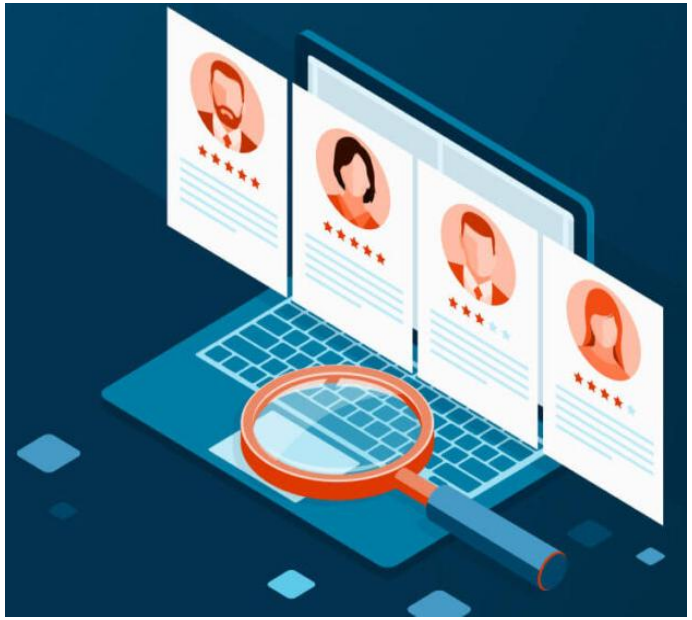
- Además de los servicios internos y externos, los servicios también pueden ser de los siguientes tipos:

Servicio de TI	• Está formado por las tecnologías de la información, personas y procesos. Un Proveedor de Servicios de TI ofrece este servicio a uno o más clientes para prestar apoyo a sus procesos de negocio.
Servicios principales	• Representan el valor que los clientes necesitan y por el que están dispuestos a pagar. • Ofrecen los resultados básicos que necesitan uno o más clientes. • Representan la propuesta de valor para el cliente y proporcionan la base para su utilización y satisfacción continuas.
Servicios internos/ habilitantes	• Son necesarios para ofrecer un servicio elemental. • Son los “factores básicos” que permiten que los clientes reciban el servicio “real”.
Servicios complementarios	• Son servicios que son añadidos a un servicio elemental para atraer a los clientes para que adquieran un servicio. • No son cruciales para la prestación de un servicio elemental porque son añadidos solamente como factores de “entusiasmo”.



Tipos de clientes

Internos	Externos
Son clientes que trabajan en la misma organización que el Proveedor de Servicios de TI.	Son clientes que trabajan para otra organización o son entidades jurídicamente independientes que constituyen contratos o convenios legalmente vinculantes con los Proveedores de Servicios.
"…..el departamento de marketing es un cliente interno de la organización de TI porque usa servicios TI. El director de marketing y el director de TI dependen del consejero delegado. Si TI cobra por sus servicios, el dinero pagado es una transacción interna en el sistema de contabilidad de la organización, es decir, no son ingresos reales".	"…una compañía aérea podría obtener servicios de consultoría de una gran empresa consultora. Dos tercios del valor del contrato se pagan en efectivo y un tercio se paga en billetes de avión de un valor equivalente".



Partes interesadas en la Gestión de Servicio

Las partes interesadas internas son funciones, grupos y equipos en la organización que ofrecen servicios.

- Las partes interesadas externas son:

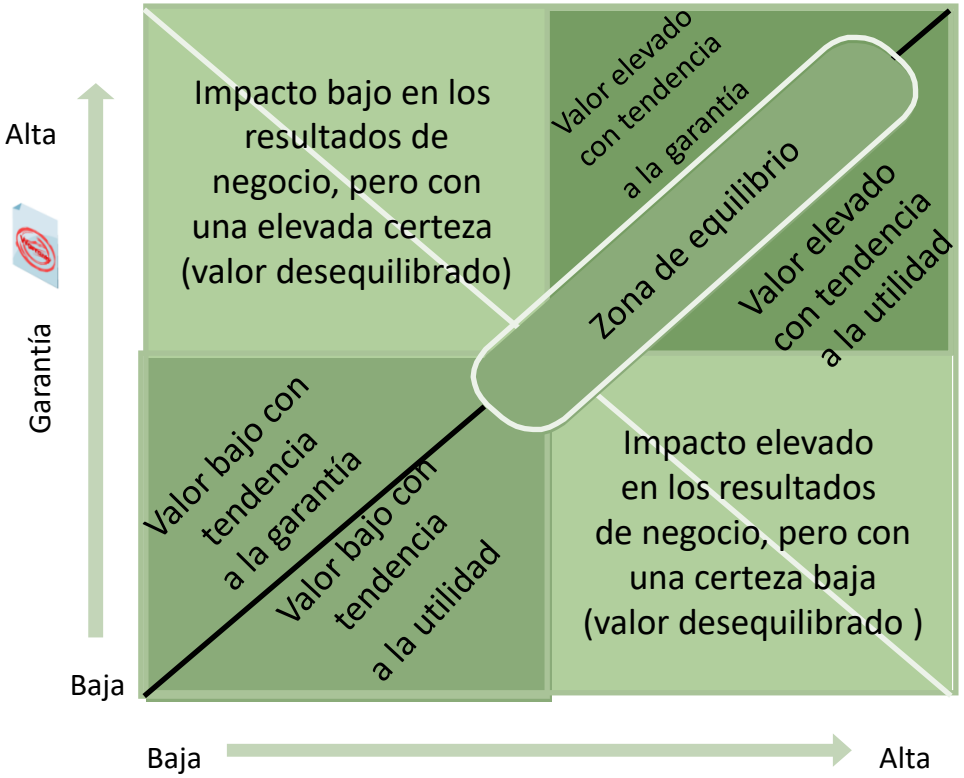
Clientes	• Compran productos o Servicios. • Definen y aceptan los objetivos de nivel del Servicio
Usuarios	• Son personas que usan el Servicio a diario. • Usan los Servicios de TI directamente. • A veces son clientes que usan estos Servicios.
Proveedores (Suppliers)	• Son terceras partes responsables de suministrar los productos o Servicios necesarios para ofrecer Servicios de TI. • Algunos ejemplos son los proveedores de hardware y software básicos, los proveedores de red y de telecomunicaciones y las organizaciones que externalizan los Servicios.

Utilidad y garantía

- Los conceptos de Utilidad y Garantía son claves para entender la perspectiva del cliente sobre el valor:

Utilidad = **Ajustado a la utilidad**: la funcionalidad ofrecida por un producto o servicio para satisfacer una necesidad en particular

Garantía = **Ajustado al uso**: una promesa o garantía de que tanto la disponibilidad, capacidad, continuidad y seguridad satisfacen las expectativas del cliente



Gobierno y Gestión

Proceso

Aplicación/ Servicio de TI /Canal

SISTEMAS OPERATIVOS

BASES DE DATOS

REDES Y COMUNICACIONES

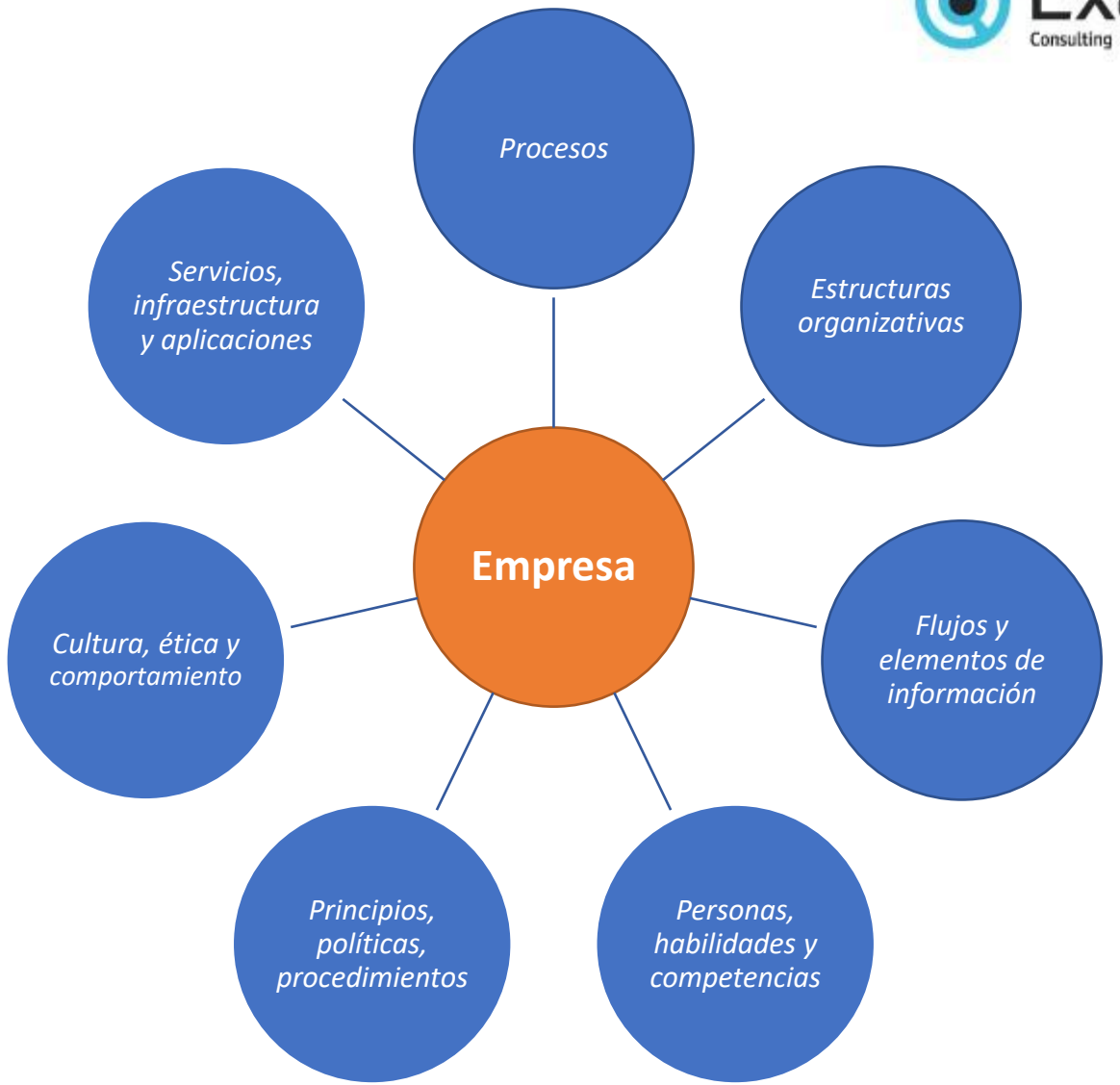
SERVIDORES Y OTRA INFRAESTRUCTURA

DISPOSITIVOS CLIENTE

INSTALACIONES FISICAS

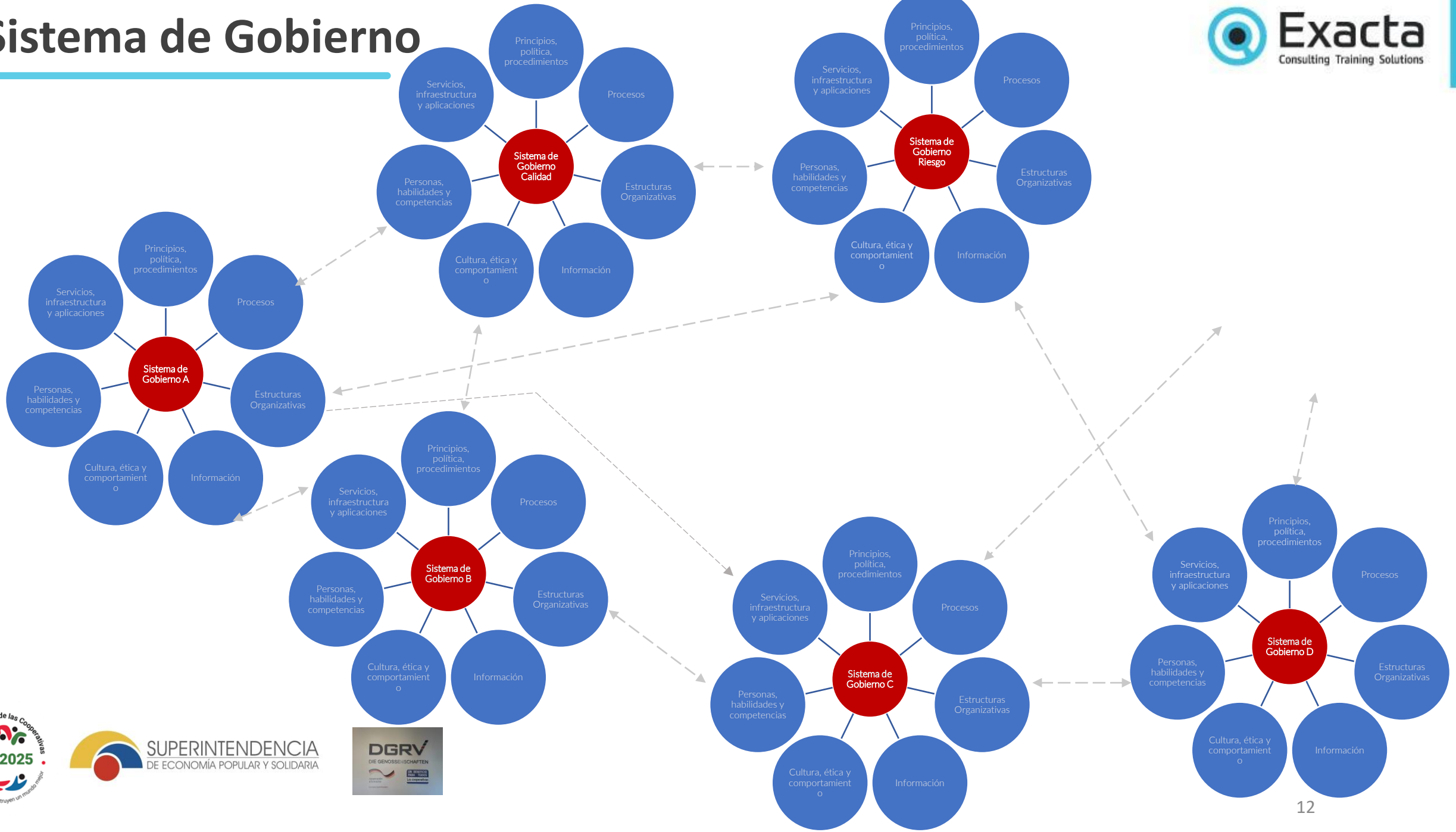
Personas

Componentes de un sistema de Gobierno

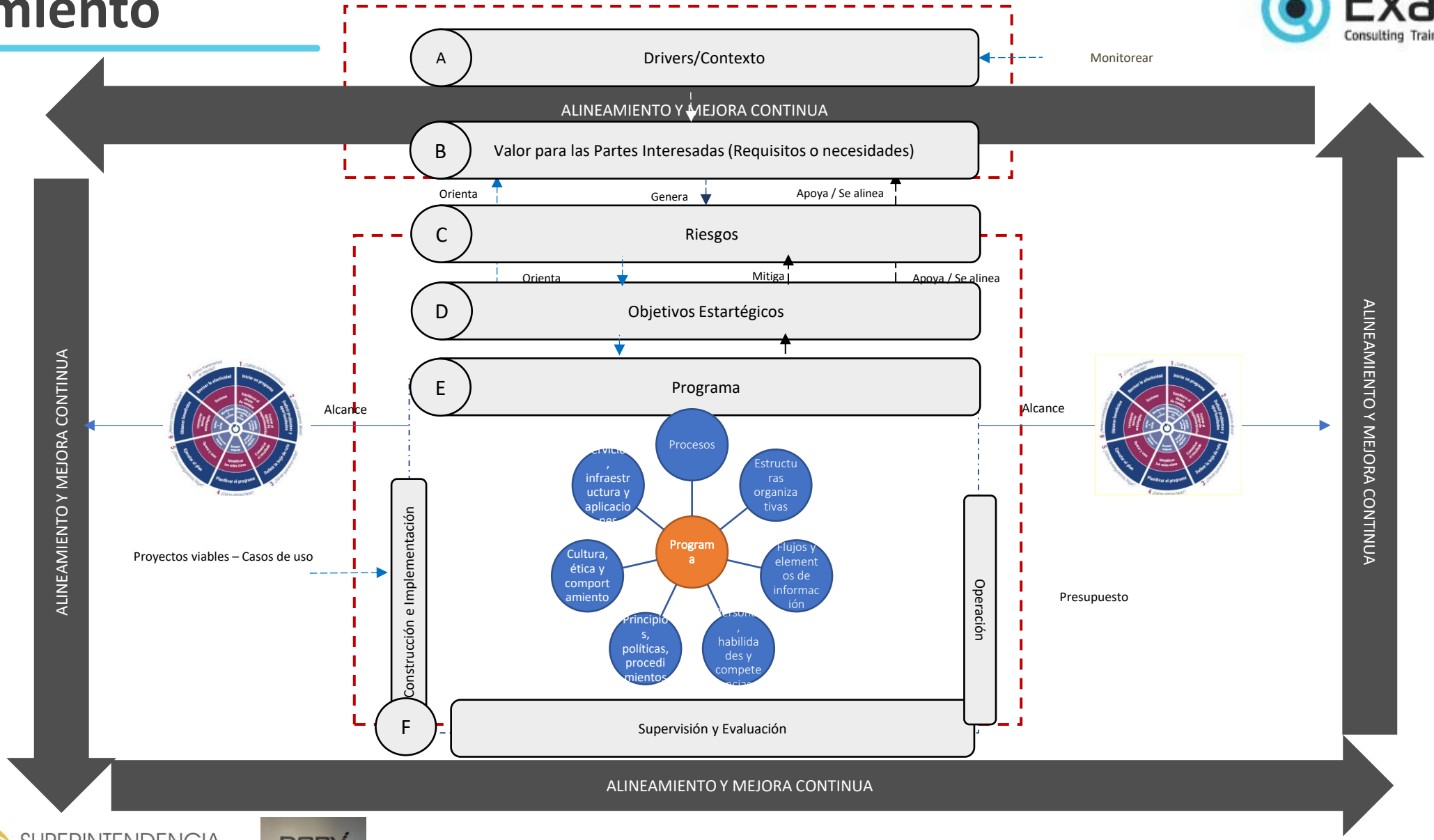


Referencia: Marco de referencia COBIT 2019: Conceptos básicos: Sistemas de gobierno y componentes, Capítulo 4

Sistema de Gobierno

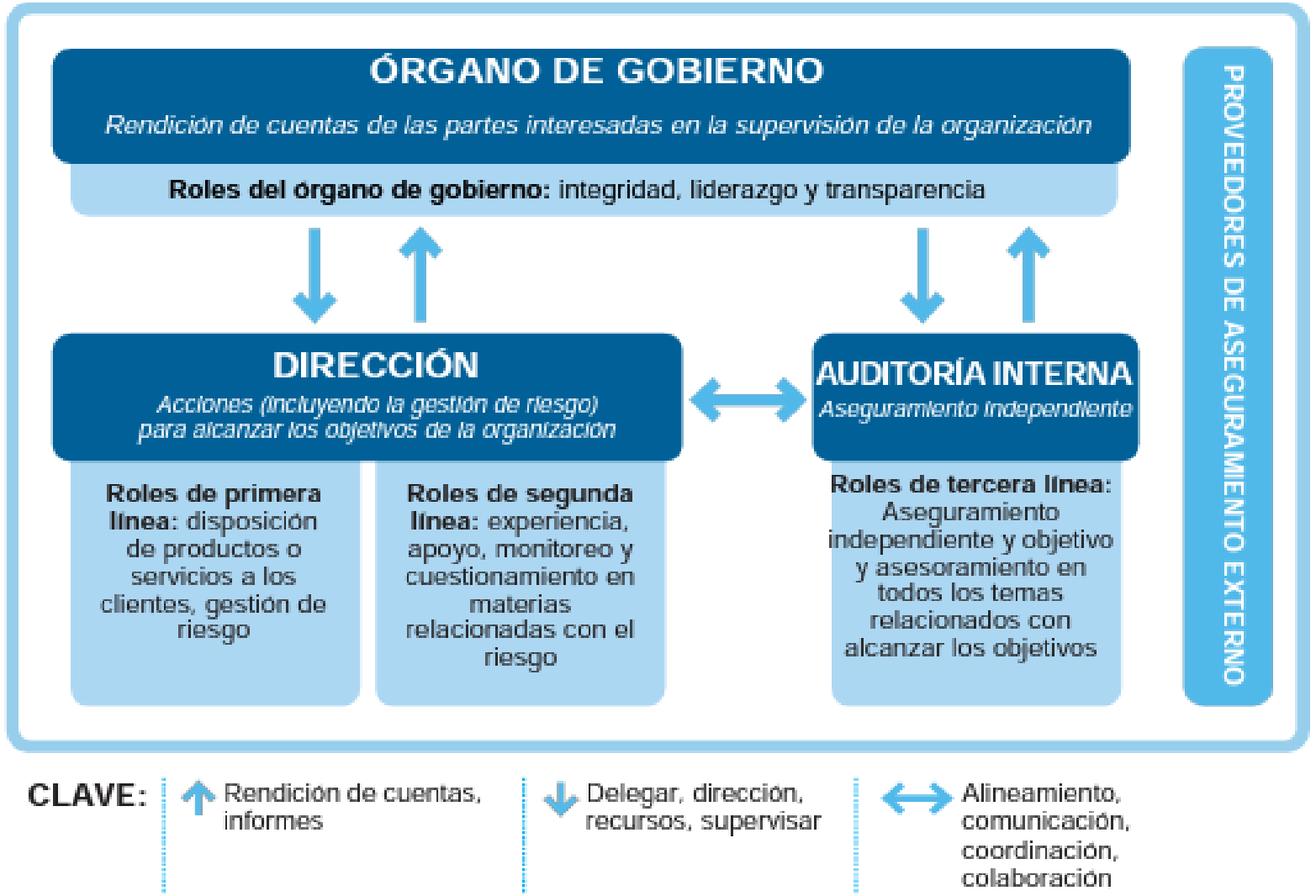


Alineamiento

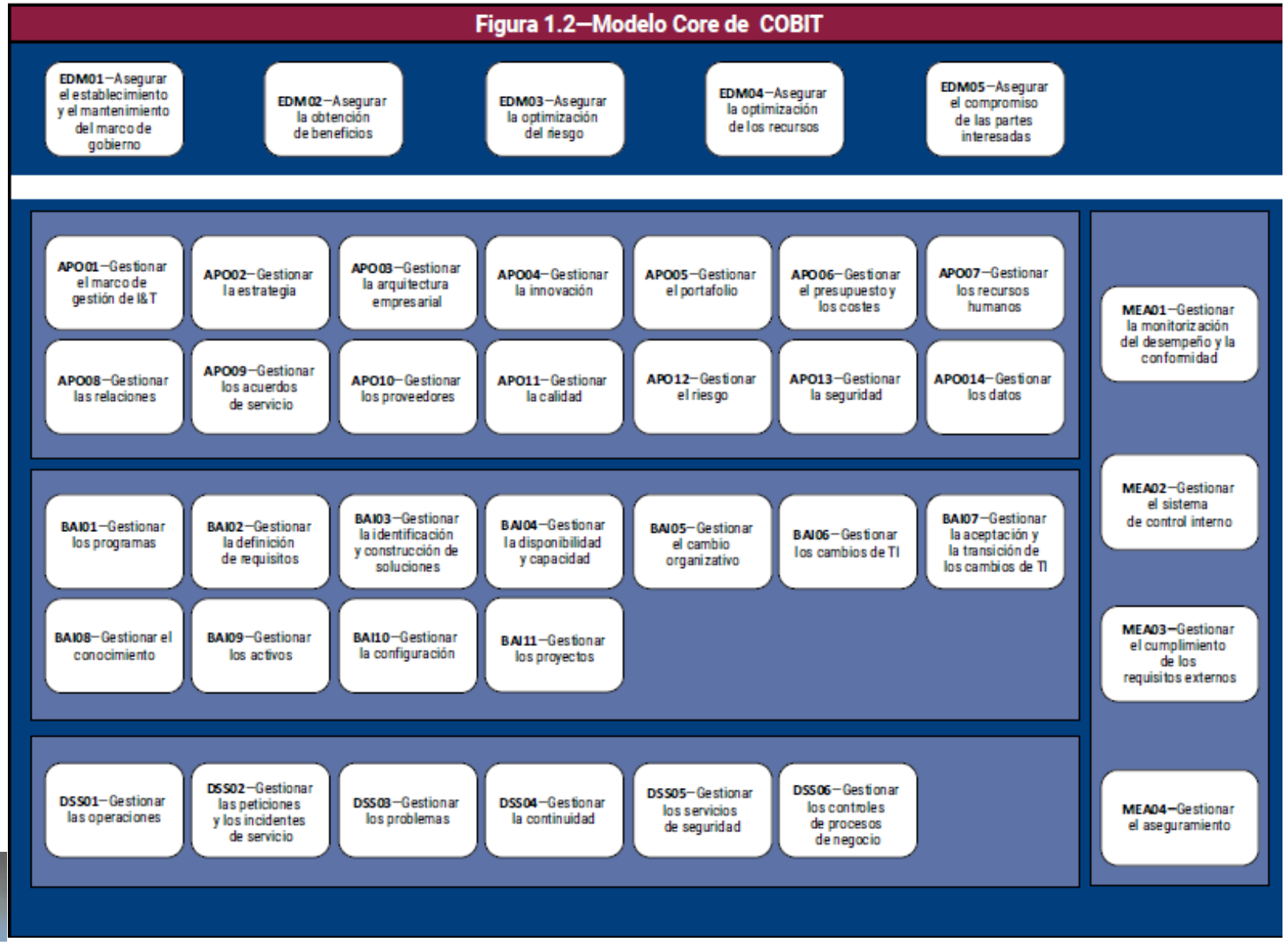


13

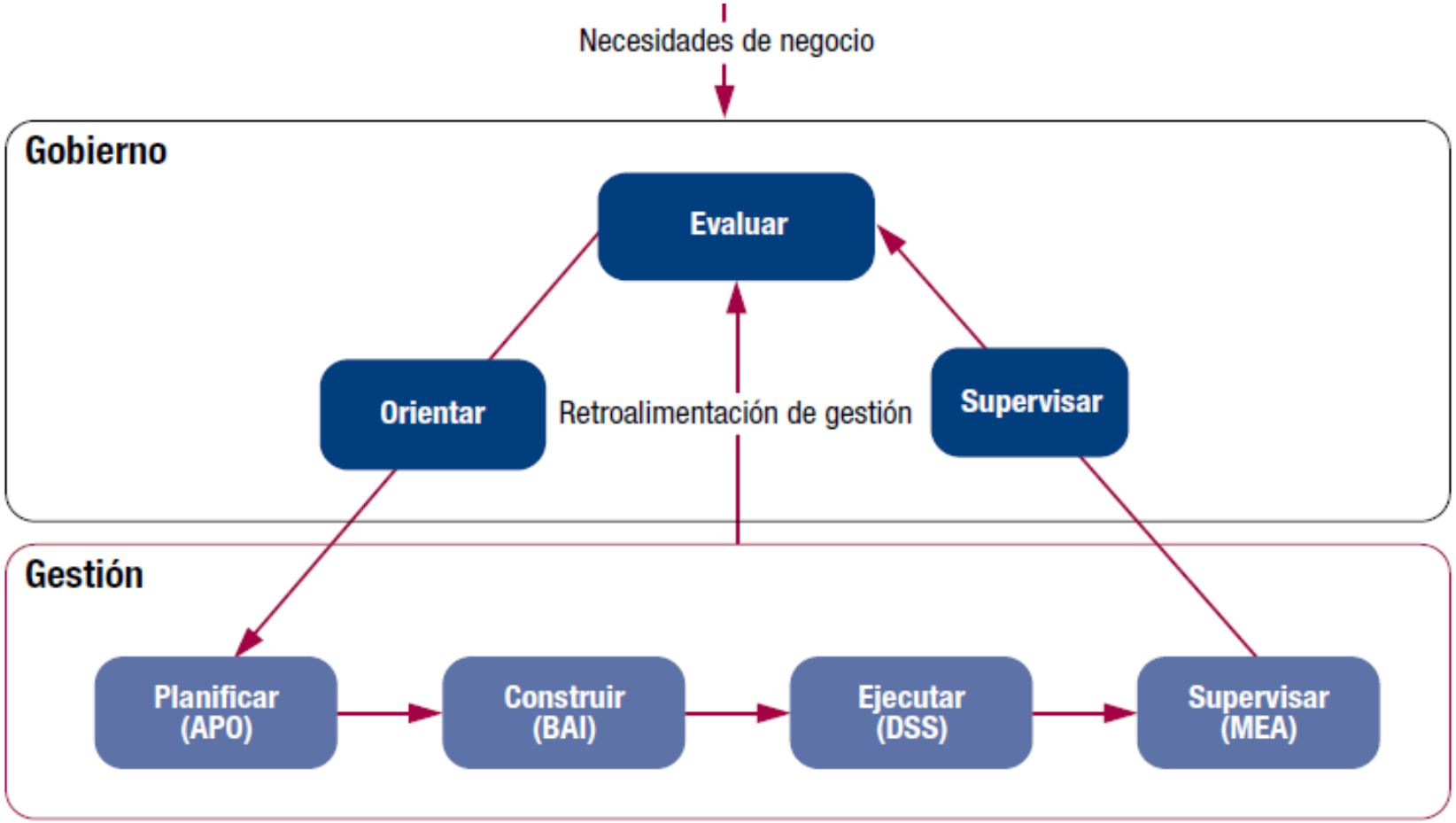
Modelo de las tres líneas del IIA



Controles generales



Separación Gobierno de Gestión



Sistema de Gobierno Integro (End to End)

1. La Norma de Ciberseguridad

Es la regulación específica más importante para el área de tecnología. Establece que la ciberseguridad no es solo un tema técnico, sino de gobierno corporativo.

- Sistema de Gestión de Seguridad de la Información → Obliga a implementar un sistema basado en las buenas prácticas internacionales (generalmente se usa como referencia la ISO/IEC 27001/27002).
- Roles Obligatorios → Las entidades grandes (Segmentos 1 y 2) deben tener un Oficial de Seguridad de la Información (CISO) independiente del área de TI, y un Comité de Seguridad de la Información.
- Clasificación de la Información → Debes inventariar y clasificar tus activos (crítico, confidencial, público, etc.).
- Gestión de Accesos → Políticas estrictas sobre quién entra a qué sistema.

2. La Norma de Gestión de Riesgos

Esta norma, vigente desde 2024, integra la tecnología como un factor de riesgo.

Gestión de Vulnerabilidades	Exige explícitamente realizar escaneos periódicos para identificar fallos de seguridad técnica y aplicar parches (updates) de seguridad.
Eventos de Riesgo	Obliga a reportar incidentes tecnológicos (caídas de sistema, hackeos) como eventos de riesgo operativo.
Continuidad del Negocio	Requiere tener planes de contingencia (DRP/BCP) probados para asegurar que la cooperativa siga operando si falla la tecnología.

3. La Norma de Seguridad Física y Canales

Se enfoca en la protección tangible y los canales electrónicos.

Cajeros Automáticos y Agencias

↓

Regula las cámaras, alarmas y blindajes.

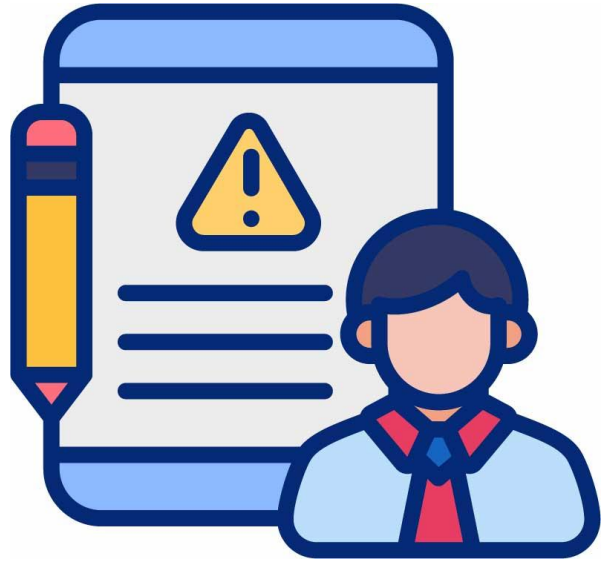
Canales Electrónicos

↓

Establece requisitos de seguridad para la Banca Web y Móvil (doble factor de autenticación, monitoreo de transacciones inusuales para prevenir fraudes).

Matriz de Requisitos de Gobierno

Requisito	Segmentos 1 y 2 (Grandes)	Segmentos 3, 4 y 5 (Medianas/Pequeñas)
Oficial de Seguridad (CISO)	Obligatorio y debe ser un rol exclusivo.	Puede ser asignado a un responsable (a veces compartido, según el caso).
Comité de Seguridad	Obligatorio reuniones periódicas y actas.	Generalmente gestionado por el Consejo de Administración directamente.
Auditoría de TI	Auditoría externa anual obligatoria con alcance en TI.	Revisiones simplificadas.
Estándar	Cumplimiento robusto alineado a ISO 27001.	Cumplimiento de controles mínimos esenciales.



Estructura de Gobernanza: Tecnología, Seguridad y Continuidad

1. Comité de Tecnología de la Información	**Aprobación del PETI:** Revisar y recomendar al Consejo de Administración el Plan Estratégico de Tecnología de la Información (PETI). **Priorización de Proyectos:** Decidir qué proyectos se ejecutan primero (ej: ¿Cambiamos el Core Bancario o lanzamos la App Móvil primero?). **Gestión de Presupuesto:** Aprobar y vigilar las inversiones en hardware, software y licencias. **Monitoreo de Niveles de Servicio (SLA):** Revisar que el departamento de TI esté cumpliendo con los tiempos de respuesta prometidos a las agencias y socios.
2. Comité de Seguridad de la Información	**Gestión del SGSI:** Impulsar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI). **Aprobación de Políticas**: Revisar las políticas de seguridad (ej: política de contraseñas, política de escritorio limpio) antes de que suban al Consejo de Administración. **Revisión de Incidentes:** Analizar los reportes del Oficial de Seguridad (CISO) sobre intentos de hackeo, fugas de información o infecciones de virus y decidir acciones correctivas. **Cultura de Seguridad:** Aprobar los planes de capacitación y concientización para los empleados (evitar ingeniería social/phishing
3. Comité de Continuidad del Negocio	**Análisis de Impacto (BIA):** Validar cuáles son los procesos críticos que no pueden detenerse (ej: cajas, banca móvil) y cuánto tiempo pueden estar caídos (RTO). **Aprobación de Planes (BCP/DRP):** Revisar el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP). **Simulacros:** Evaluar los resultados de las pruebas de continuidad (ej: ¿Qué pasó cuando apagamos el servidor principal? ¿Funcionó el alterno?). **Declaratoria de Crisis:** En una situación real (un terremoto o un ciberataque masivo), este comité suele transformarse en el Comité de Crisis para tomar decisiones de emergencia

Principio de Proporcionalidad SEPS y Caracterización de Comités

Segmentos 1 y 2 (Grandes):

La SEPS exige que estos comités existan formalmente, con actas de reunión separadas y miembros definidos (deben incluir vocales del Consejo de Administración).

Segmentos 3, 4 y 5 (Medianas/Pequeñas):

A menudo la SEPS permite que estas funciones sean absorbidas directamente por el Consejo de Administración o un único "Comité de Riesgos", siempre y cuando en las actas se diferencien los temas tratados.

Característica	Comité de Tecnología	Comité de Seguridad	Comité de Continuidad
Pregunta Clave	¿Tenemos las herramientas para competir?	¿Están seguros nuestros datos?	¿Podemos seguir operando si algo falla?
Enfoque	Eficiencia y Estrategia.	Confidencialidad, Integridad y Disponibilidad.	Resiliencia y Recuperación.
Principal Entregable	Plan Estratégico de TI (PETI).	Políticas de Seguridad y Matriz de Riesgos.	Plan de Continuidad (BCP) y Recuperación (DRP).
Liderado usualmente por	Gerencia General / Jefe de TI.	Oficial de Seguridad (CISO) / Riesgos.	Gerencia de Riesgos / Operaciones.

1. Gerencia de Tecnología (Primera Línea de Defensa)

- Es el órgano ejecutor.
- Son los dueños de la operación técnica diaria.

Su objetivo es que los sistemas funcionen, estén disponibles y apoyen al negocio.

Responsabilidades según la norma:

Implementación del PETI	Es responsable de ejecutar el Plan Estratégico de Tecnología de la Información (PETI). Debe asegurar que los proyectos tecnológicos se cumplan en tiempo y presupuesto
Gestión de la Infraestructura	Administrar servidores, redes, bases de datos y enlaces de comunicación para garantizar la disponibilidad de los servicios (que el sistema no "se caiga").
Ejecución de Controles de Seguridad	El Oficial de Seguridad define las políticas, pero la Gerencia de Tecnología las implementa.
Gestión de Proveedores TI	Administrar los contratos y niveles de servicio (SLA) con proveedores de software (Core Bancario) o internet.
Soporte y Mesa de Ayuda	Atender los requerimientos operativos de los usuarios internos y socios.
Continuidad Operativa	Ejecutar las pruebas técnicas del Plan de Recuperación ante Desastres (DRP) y asegurar que los respaldos (backups) se realicen correctamente.

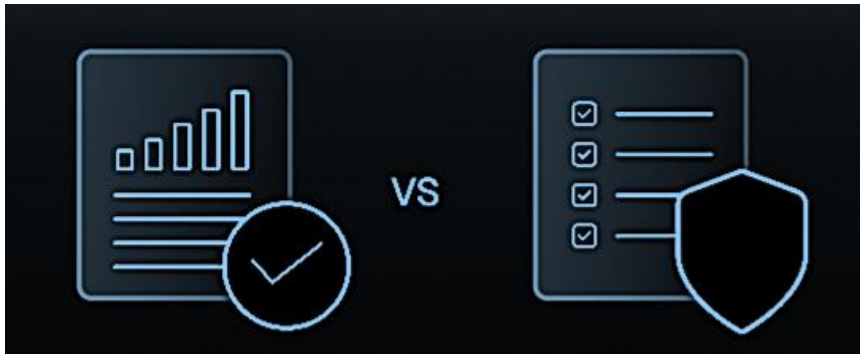
2. Auditoría Informática (Tercera Línea de Defensa)

Es el órgano evaluador independiente. No tocan los servidores, no configuran redes y no solucionan problemas. Su objetivo es asegurar que los controles funcionen y que la Gerencia de TI esté diciendo la verdad sobre el estado de los sistemas.

Responsabilidades según la norma:

Evaluación Independiente	Verificar el cumplimiento de las normativas de la SEPS (Resoluciones 002, 116, entre otras) y las políticas internas de la cooperativa.
Revisión del SGSI	La norma SEPS-2022-002 exige que la Auditoría realice una evaluación periódica (anual) de la eficacia del Sistema de Gestión de Seguridad de la Información.
Validación de Vulnerabilidades	Verificar que las vulnerabilidades detectadas (por ejemplo, en un Hacking Ético) hayan sido realmente cerradas por el área de Tecnología.
Auditoría de Proyectos	Revisar si los grandes proyectos de tecnología (como un cambio de Core) siguieron la metodología adecuada y gestionaron bien los riesgos.
Informe de Hallazgos	Emitir informes formales detallando debilidades, incumplimientos y recomendaciones.

Roles Complementarios



Aspecto	Gerencia de Tecnología (TI)	Auditoría Informática
Acción Principal	Operar y Construir.	Verificar y Reportar.
Sobre los Controles	Los implementa y configura (ej: configura el Firewall).	Prueba si funcionan (ej: revisa los logs del Firewall).
Sobre los Riesgos	Es el "dueño" del riesgo tecnológico (debe mitigarlo).	Evalúa si el riesgo está bien gestionado.
Sobre el PETI	Lo elabora y ejecuta.	Evalúa si se está cumpliendo lo planeado.
Relación con SEPS	Prepara la información técnica que pide la SEPS.	Valida que esa información sea veraz antes de enviarla.

Puntos Críticos de Revisión bajo Normativa SEPS

1. Gestión de Vulnerabilidades y Parches

No basta con ver si tienen antivirus. Auditoría debe pedir la evidencia de los escaneos de vulnerabilidades periódicos y, lo más importante, el informe de remediación.
Acción: Selecciona una muestra de 5 servidores críticos y pide al área de TI que demuestre cuándo fue la última vez que instalaron parches de seguridad. Si el último parche es de hace 6 meses, es un hallazgo crítico.
Base Normativa: Artículo sobre gestión de vulnerabilidades técnicas (Res. SEPS-2022-002).

2. Pruebas de Continuidad y Respaldos (Restauración)

Muchos hacen respaldos, pocos prueban que sirven. Auditoría no debe revisar si el backup se hizo, sino si se puede restaurar.
Acción: Pide la "Bitácora de Pruebas de Restauración". Si no existe, solicita una prueba en vivo: "Por favor, restaure un archivo aleatorio de hace 2 semanas". Si el área de TI no puede hacerlo o tarda horas, es un hallazgo mayor. También verifica el acta de la última prueba del plan de continuidad (DRP).
Base Normativa: Capítulo de Continuidad del Negocio (Res. SEPS-2024-0116).

3. Gestión de Accesos y Usuarios Privilegiados

El abuso de usuarios administradores es la causa #1 de fraudes internos.
Acción: Pide el listado de usuarios activos del Core Bancario y crúzalo con la nómina de Recursos Humanos.
- ¿Hay usuarios activos de empleados que renunciaron el mes pasado?
- ¿Hay usuarios genéricos tipo cajero1 o admin compartidos por varias personas? (Esto está prohibido).

Base Normativa: Control de Accesos (Res. SEPS-2022-002).

Puntos Críticos de Revisión bajo Normativa SEPS

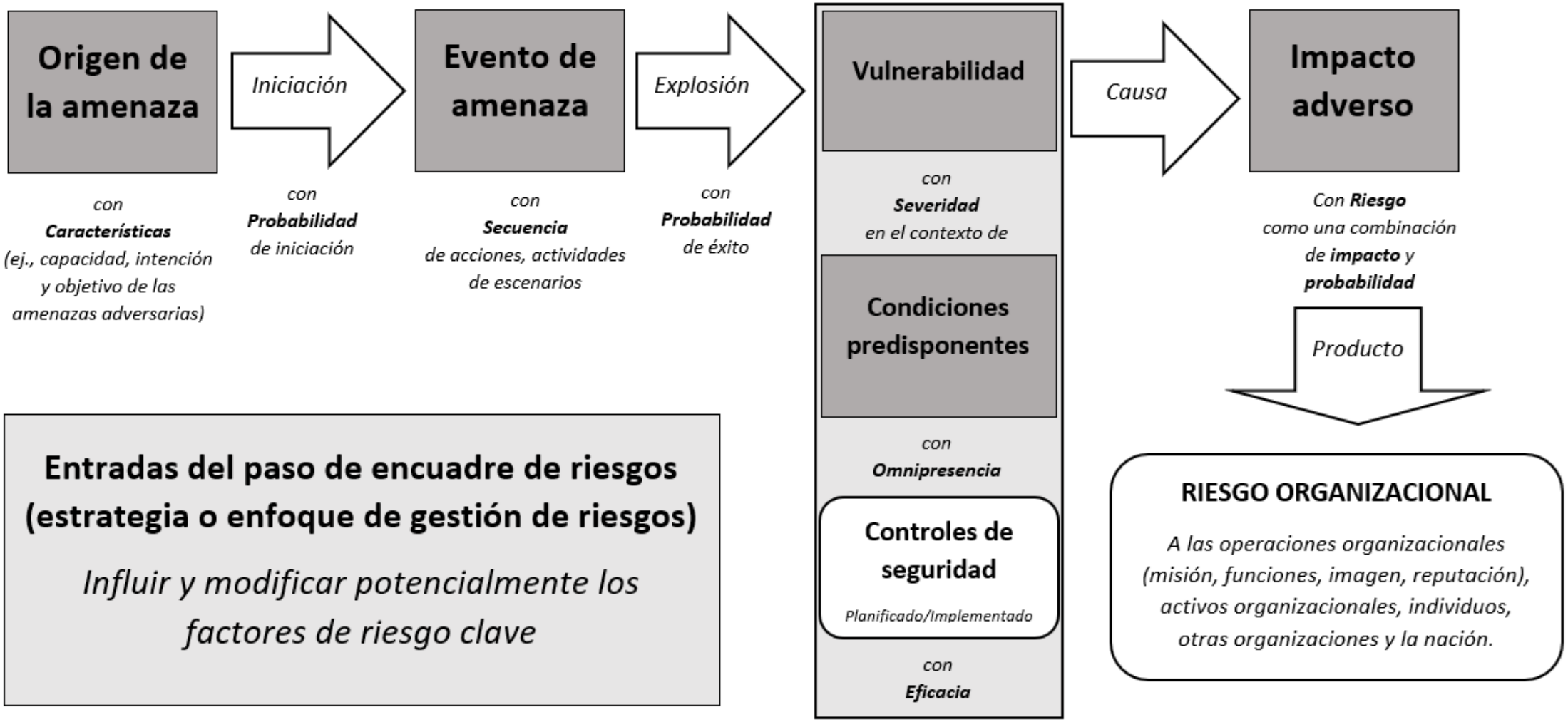
4. Segregación de Ambientes (Desarrollo vs. Producción)

Que los programadores no tengan poder absoluto.
Acción: Verifica si el personal de desarrollo tiene permisos para modificar datos reales en el ambiente de Producción.
Auditoría debe buscar evidencias de pasos a producción sin aprobación. Un programador nunca debe poder pasar su propio código a producción sin un control de calidad intermedio.
Base Normativa: Seguridad en el Ciclo de Desarrollo y Adquisición (Res. SEPS-2022-002).

5. Proveedores Críticos de Tecnología

La cooperativa es responsable por lo que hagan sus proveedores (nube, enlace de datos, core externo).
Acción: Revisa los contratos y los informes de cumplimiento de SLA (Niveles de Servicio).
¿El proveedor del Core Bancario ha entregado su certificación de seguridad o informe de auditoría anual?
¿Existe un acuerdo de confidencialidad (NDA) firmado vigente?
Base Normativa: Gestión de Relaciones con Proveedores (Res. SEPS-2024-0116).

Contexto del riesgo - Método



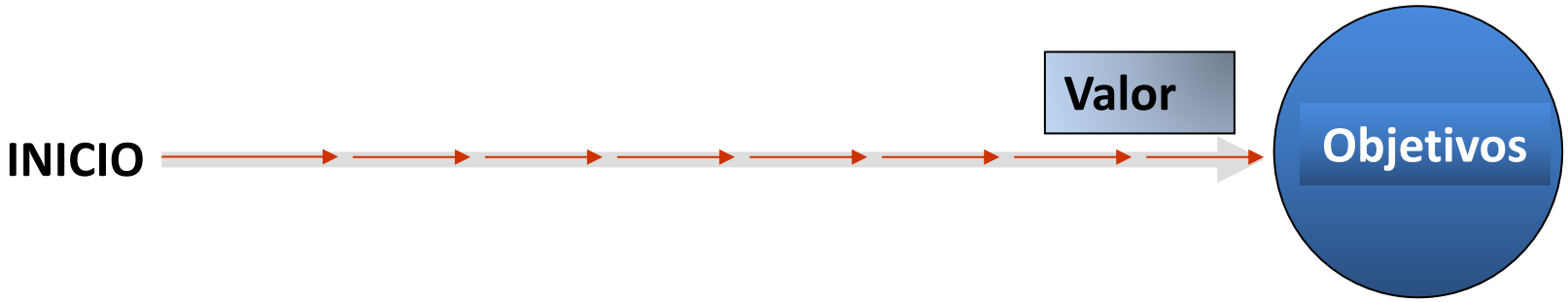
DEFINIENDO LA GESTIÓN DE RIESGOS

Todo nace con un objetivo o fin…

INICIO → **Objetivos**

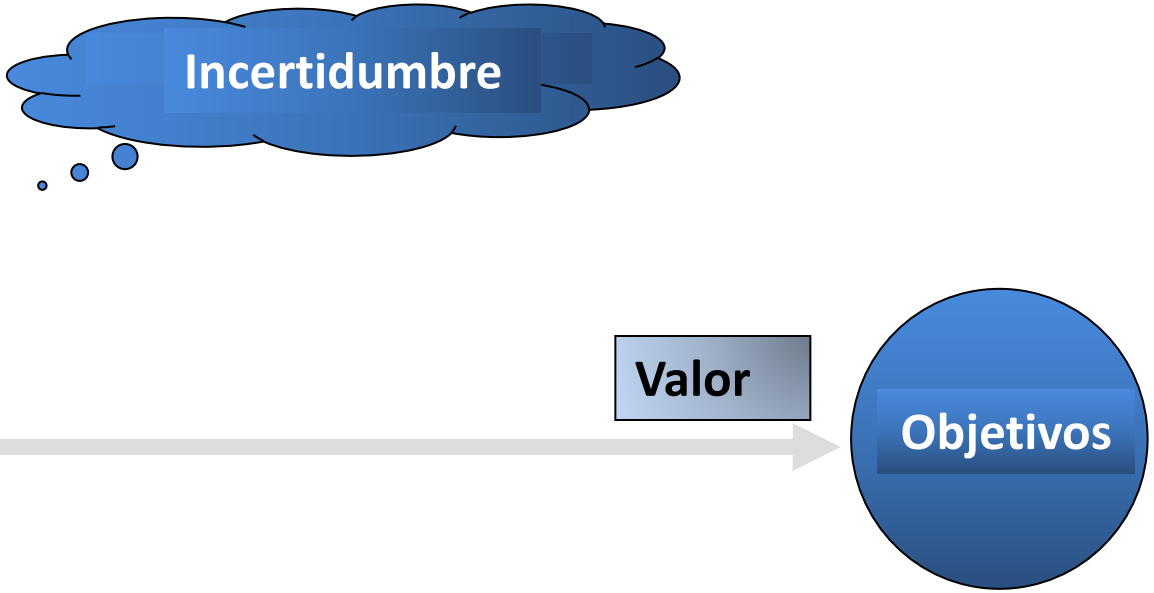
DEFINIENDO LA GESTIÓN DE RIESGOS

Los objetivos se consiguen generando valor



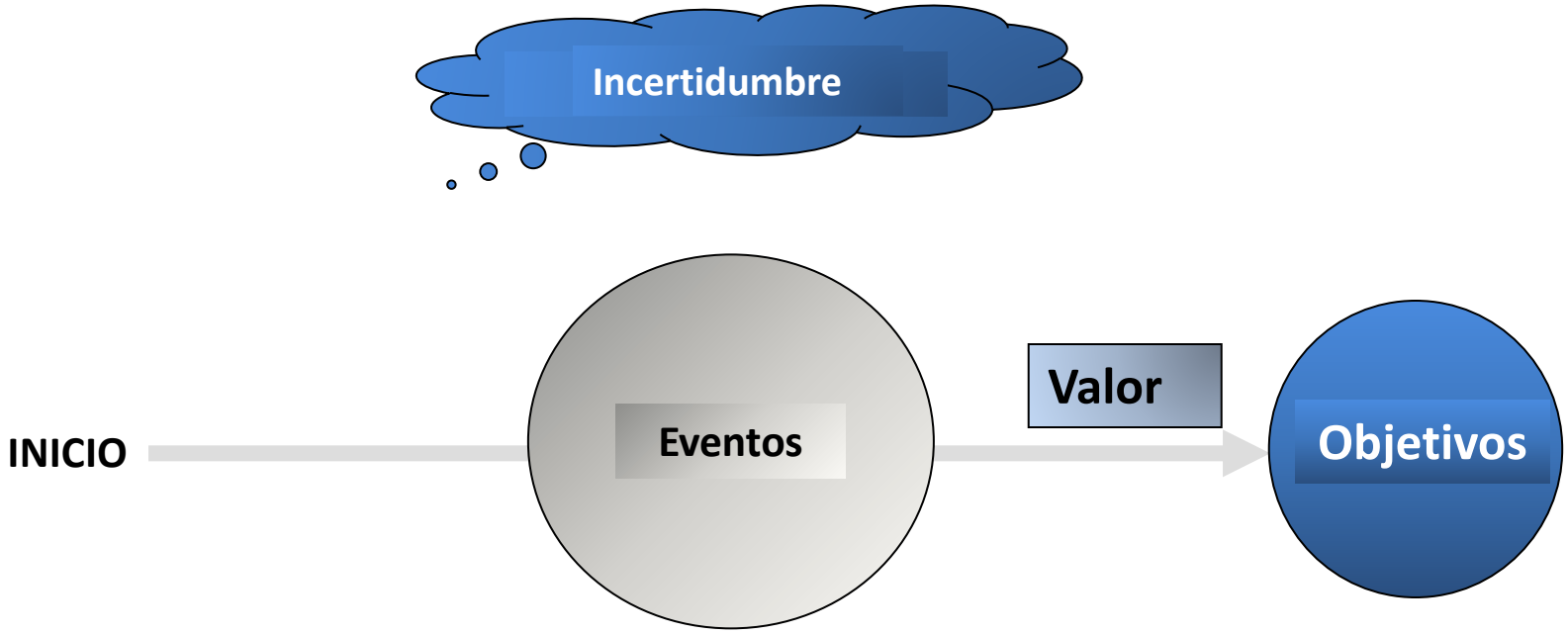
DEFINIENDO LA GESTIÓN DE RIESGOS

pero se pueden presentar eventos…



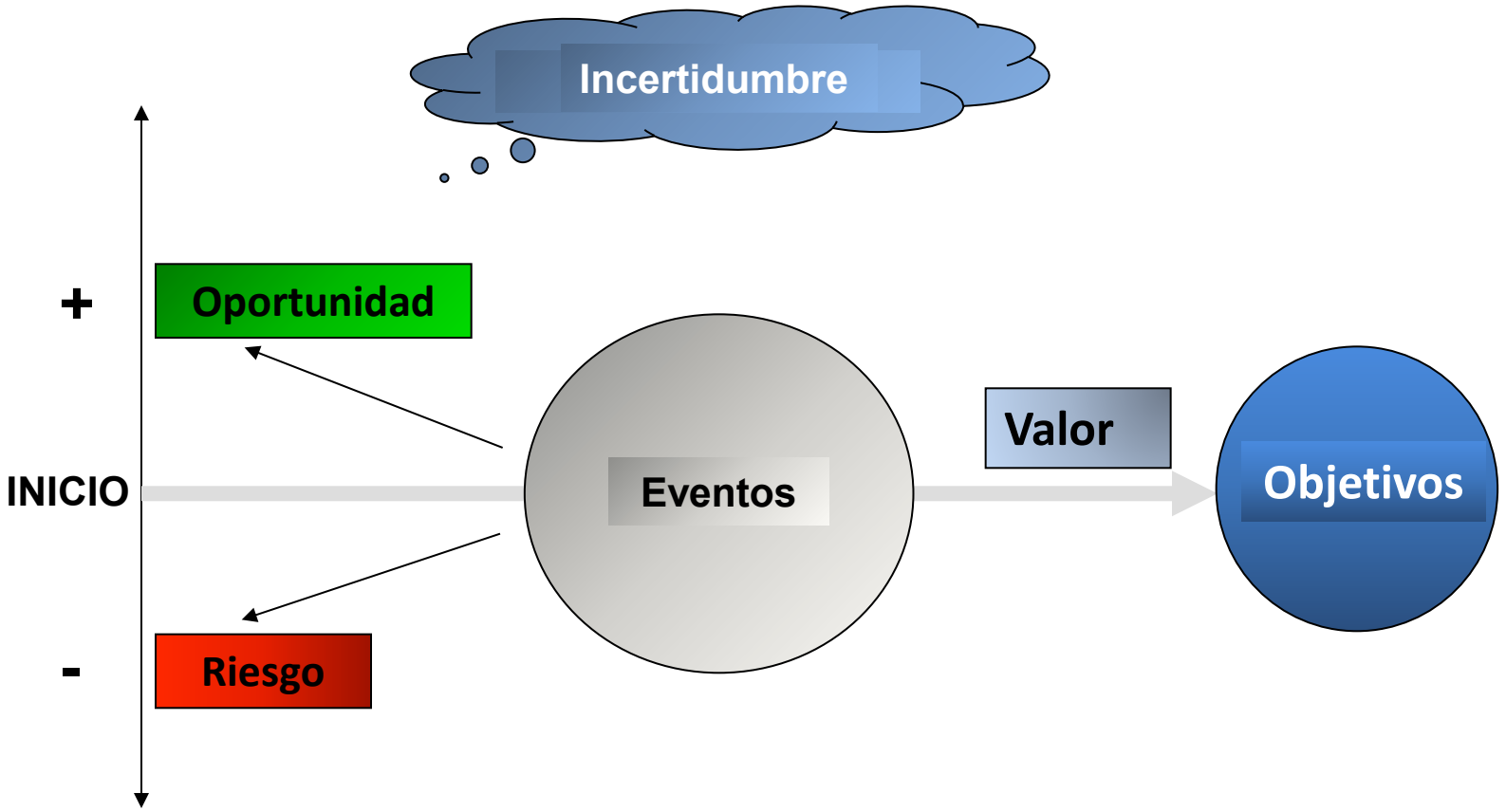
DEFINIENDO LA GESTIÓN DE RIESGOS

Estamos en constante incertidumbre…



DEFINIENDO LA GESTIÓN DE RIESGOS

No sabemos que pasará y sus consecuencias…



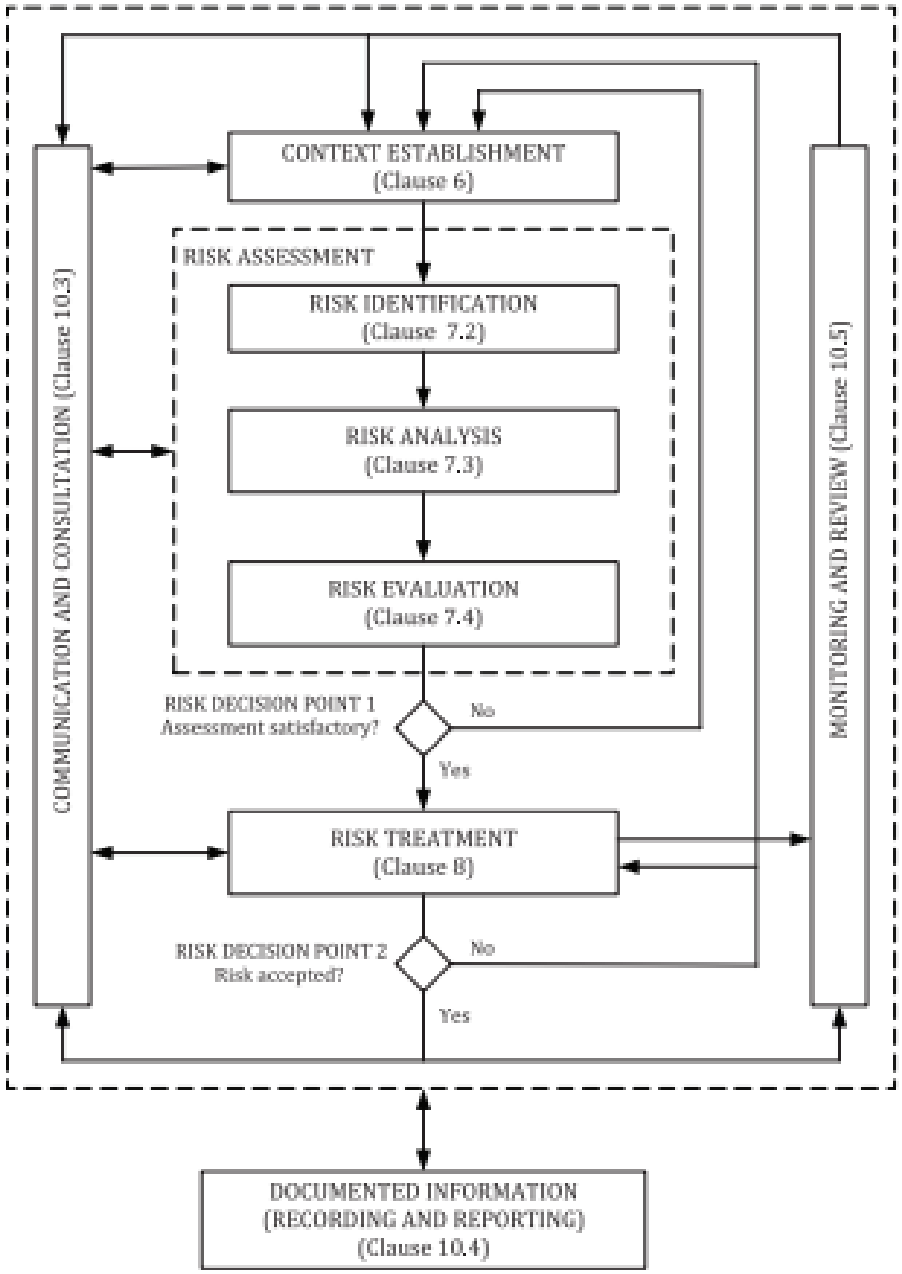
Riesgo y Gestión de Riesgos empresariales

La estrategia y los objetivos de negocio de una entidad pueden verse afectados por eventos potenciales. La falta de previsibilidad completa de un evento que ocurre (o no) y su impacto relacionado crea incertidumbre para una organización. Existe incertidumbre para cualquier entidad que se proponga alcanzar estrategias futuras y objetivos organizacionales.

En este contexto, el riesgo se define como:

La posibilidad de que los eventos ocurran y afecten el logro de la estrategia y los objetivos de la organización.

Gestión de riesgos

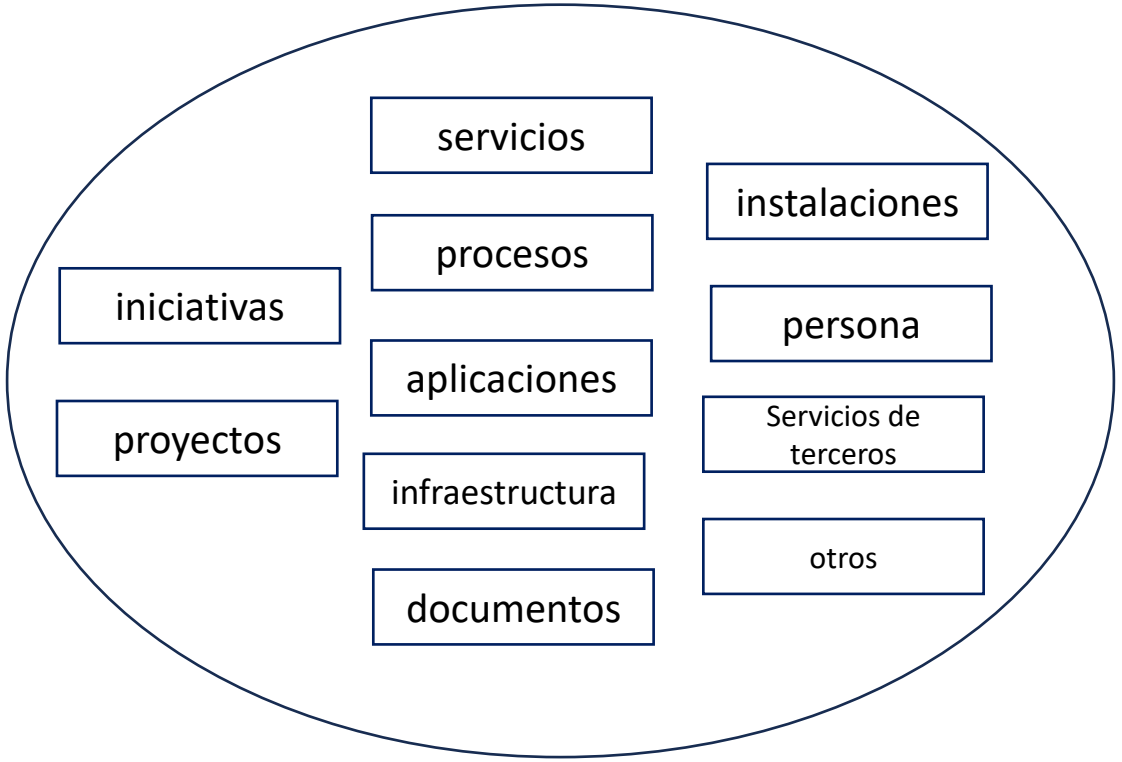


Ciclos de gestión de riesgos

Estratégico

Operacional

Tratamiento



Apetito al Riesgo - Cultura

Muchos factores dan forma a la cultura de la entidad.

Los factores internos incluyen, entre otras cosas, el nivel de juicio y autonomía otorgado al personal, cómo los empleados de la entidad interactúan entre sí y con sus gerentes, las normas y reglas, la disposición física del lugar de trabajo y el sistema de recompensas establecido.

Los factores externos incluyen los requisitos reglamentarios y las expectativas de los clientes, los inversores y otros elementos.

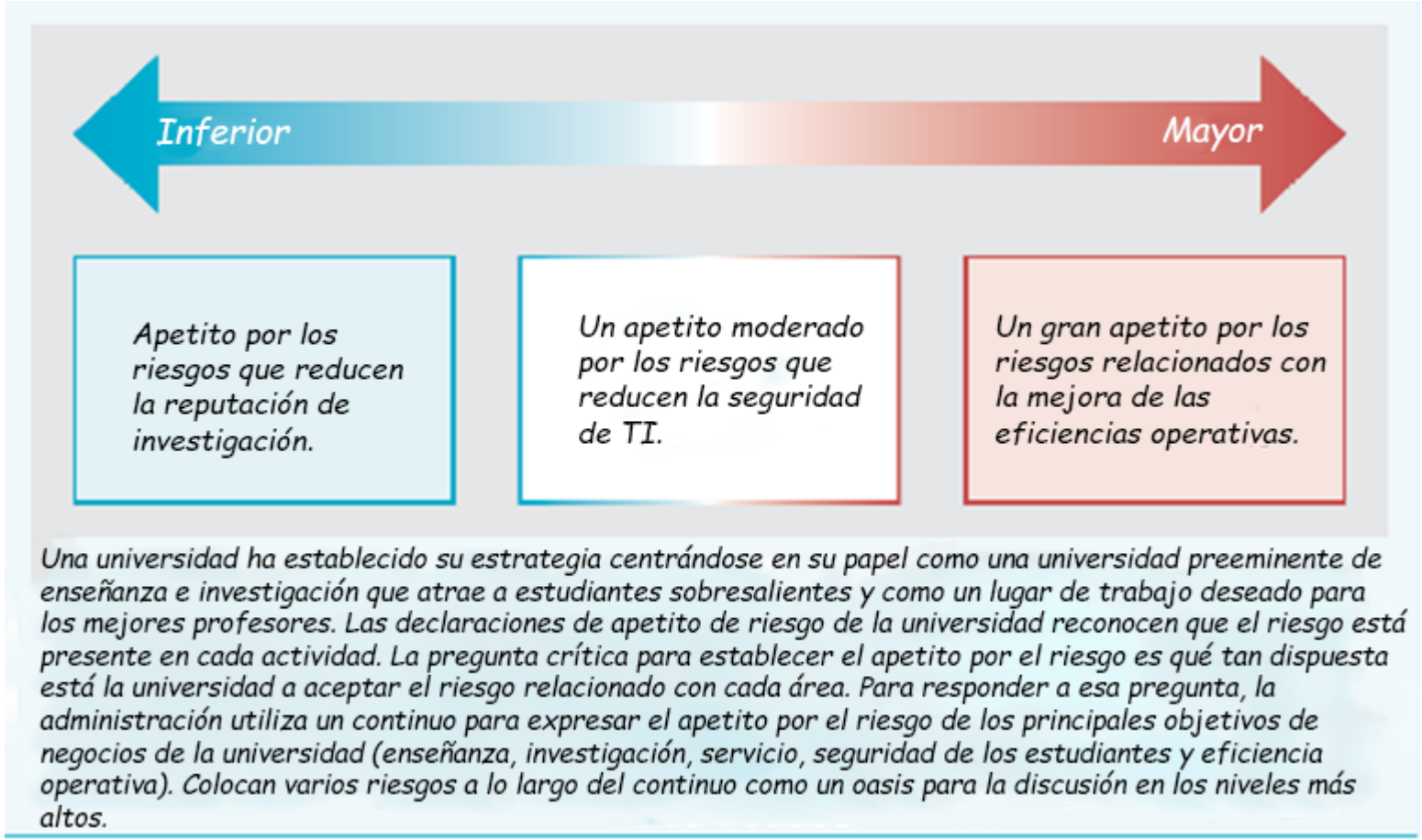
Todos estos factores influyen donde la entidad se posiciona en el espectro de la cultura, que va desde el riesgo adverso al riesgo agresivo (ver Figura). Cuanto más cerca esté una entidad del riesgo del extremo agresivo del espectro, mayor será su propensión y aceptación de los diferentes tipos y una mayor cantidad de riesgo para lograr la estrategia y los objetivos organizacionales (consulte el Ejemplo).

Ejemplo: Dos extremos del espectro de la cultura

Una planta de energía nuclear probablemente tendrá una cultura contraria al riesgo en sus operaciones diarias. Tanto la gerencia como las partes interesadas externas esperan que las decisiones con respecto a las nuevas tecnologías y sistemas se tomen con cuidado y con gran atención a los detalles y la seguridad para proporcionar una expectativa razonable de la confiabilidad de la planta. No es deseable que las plantas de energía nuclear inviertan fuertemente en tecnologías innovadoras y no probadas críticas para la gestión de las operaciones.

En contraste, un administrador de capital privado es más probable que sea una entidad agresiva en cuanto al riesgo. La administración y los inversionistas externos tendrán altas expectativas de desempeño que requieren asumir riesgos potencialmente graves, mientras que aún se encuentran dentro del apetito de riesgo definido de la entidad.

Definir el apetito al riesgo



Una universidad ha establecido su estrategia centrándose en su papel como una universidad preeminente de enseñanza e investigación que atrae a estudiantes sobresalientes y como un lugar de trabajo deseado para los mejores profesores. Las declaraciones de apetito de riesgo de la universidad reconocen que el riesgo está presente en cada actividad. La pregunta crítica para establecer el apetito por el riesgo es qué tan dispuesta está la universidad a aceptar el riesgo relacionado con cada área. Para responder a esa pregunta, la administración utiliza un continuo para expresar el apetito por el riesgo de los principales objetivos de negocios de la universidad (enseñanza, investigación, servicio, seguridad de los estudiantes y eficiencia operativa). Colocan varios riesgos a lo largo del continuo como un oasis para la discusión en los niveles más altos.

Algunas organizaciones articulan el apetito de riesgo como un solo punto; otros como un continuo (ver Ejemplo).

Riesgo inherente, objetivo y residual

Como parte de la evaluación del riesgo, la dirección considera el riesgo inherente, el riesgo residual objetivo y el riesgo residual real.

- El **riesgo inherente** es el riesgo para una entidad en ausencia de cualquier acción directa o enfocada por parte de la administración para alterar su gravedad.

- El **riesgo residual objetivo** es la cantidad de riesgo que una entidad prefiere asumir en la búsqueda de su estrategia y objetivos de negocio, sabiendo que la dirección implementará, o ha implementado, acciones directas o enfocadas para alterar la gravedad del riesgo.

- El **riesgo residual real** es el riesgo restante después de que la administración haya tomado medidas para alterar su gravedad. El riesgo residual real debe ser igual o inferior al riesgo residual objetivo. Cuando el riesgo residual real supere el riesgo objetivo, se deben identificar acciones adicionales que permitan a la administración alterar aún más la gravedad del riesgo.

Contexto del riesgo (tratamiento)

Tipo de Tratamiento	Descripción (Acción)
1. Modificar el Riesgo (Mitigación)	Implementar controles para cambiar la probabilidad de ocurrencia o alterar las consecuencias
2. Evitar el Riesgo	Decidir no iniciar o no continuar con la actividad que genera el riesgo
3. Compartir el Riesgo	Distribuir el riesgo con otras partes (terceros), mediante contratos o mecanismos de financiamiento.
4. Retener el Riesgo	Asumir o mantener el riesgo de manera informada, aceptando sus posibles consecuencias.

Contexto del riesgo (tratamiento)

Flujo de Decisión:

1. Riesgo Inaceptable (Fuera de Tolerancia): Si el Riesgo Residual (el riesgo que queda después de aplicar controles existentes) excede el Criterio de Aceptación, la organización está obligada a aplicar los tratamientos de Modificar (invertir más en controles para reducirlo) o Evitar (si la modificación es imposible).
    - *Ejemplo:* Si el Criterio de Aceptación establece que la probabilidad de un incidente debe ser < 1%, pero el riesgo residual es del 5%, ese 5% es Intolerable. La empresa debe Mitigar o Evitar.
2. Riesgo Aceptable (Dentro de Tolerancia): Si el Riesgo Residual es igual o inferior al Criterio de Aceptación, el riesgo se gestiona mediante el tratamiento de Retener el Riesgo. En este punto, la organización decide simplemente monitorearlo.
3. Riesgo Estratégico (Transferible): La decisión de Compartir el Riesgo (ej., comprar un seguro) se toma generalmente cuando el Impacto es muy alto, incluso si la probabilidad es baja. Es una decisión financiera que busca reducir el impacto monetario sin modificar necesariamente la probabilidad de ocurrencia del evento.

Ejemplo de escala de evaluación con matriz de riesgo de tres colores

Nivel de riesgo	Evaluación del riesgo	Descripción
Bajo (verde)	Aceptable tal como está	El riesgo puede ser aceptado sin necesidad de acciones adicionales.
Moderado (ámbar)	Aceptable bajo control	Debe hacerse un seguimiento en términos de gestión de riesgos y establecer acciones en el marco de mejora continua a mediano y largo plazo.
Alto (rojo)	Inaceptable	Deben tomarse medidas para reducir el riesgo en el corto plazo. De lo contrario, toda o parte de la actividad debe ser rechazada.

Ejemplo de escala de consecuencias

Consecuencias	Descripción
5 - Catastrófico	Consecuencias sectoriales o regulatorias más allá de la organización. Ecosistema(s) sectorial(es) sustancialmente afectados, con consecuencias que pueden ser duraderas. Y/o: dificultad para el Estado, e incluso una incapacidad, para garantizar una función reguladora o una de sus misiones de vital importancia. Y/o: consecuencias críticas para la seguridad de las personas y bienes (crisis sanitaria, gran contaminación ambiental, destrucción de infraestructuras esenciales, etc.).
4 - Crítico	Consecuencias desastrosas para la organización. Incapacidad de la organización para asegurar toda o parte de su actividad, con posibles consecuencias graves para la seguridad de las personas y bienes. La organización probablemente no superará la situación (su supervivencia está amenazada), y los sectores o estados en los que opera probablemente se vean levemente afectados, sin consecuencias duraderas.
3 - Grave	Consecuencias sustanciales para la organización. Alta degradación en el desempeño de la actividad, con posibles consecuencias significativas para la seguridad de las personas y bienes. La organización superará la situación con serias dificultades (operación en un modo altamente degradado), sin impacto en sectores o el Estado.
2 - Significativo	Consecuencias significativas pero limitadas para la organización. Degradación en el desempeño de la actividad sin consecuencias en la seguridad de las personas y bienes. La organización superará la situación pese a algunas dificultades (operación en modo degradado).
1 - Menor	Consecuencias insignificantes para la organización. Sin consecuencias en las operaciones o en el desempeño de la actividad ni en la seguridad de las personas y bienes. La organización superará la situación sin demasiada dificultad (se consumirán los márgenes).

Ejemplo de escala de consecuencias

Probabilidad	Descripción
5 - Casi cierto	La fuente del riesgo casi con certeza alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy alta.
4 - Muy probable	La fuente del riesgo probablemente alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es alta.
3 - Probable	La fuente del riesgo puede alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es significativa.
2 - Poco probable	La fuente del riesgo tiene pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es baja.
1 - Improbable	La fuente del riesgo tiene muy pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy baja.

Ejemplo de enfoque cualitativo para criterios de riesgo

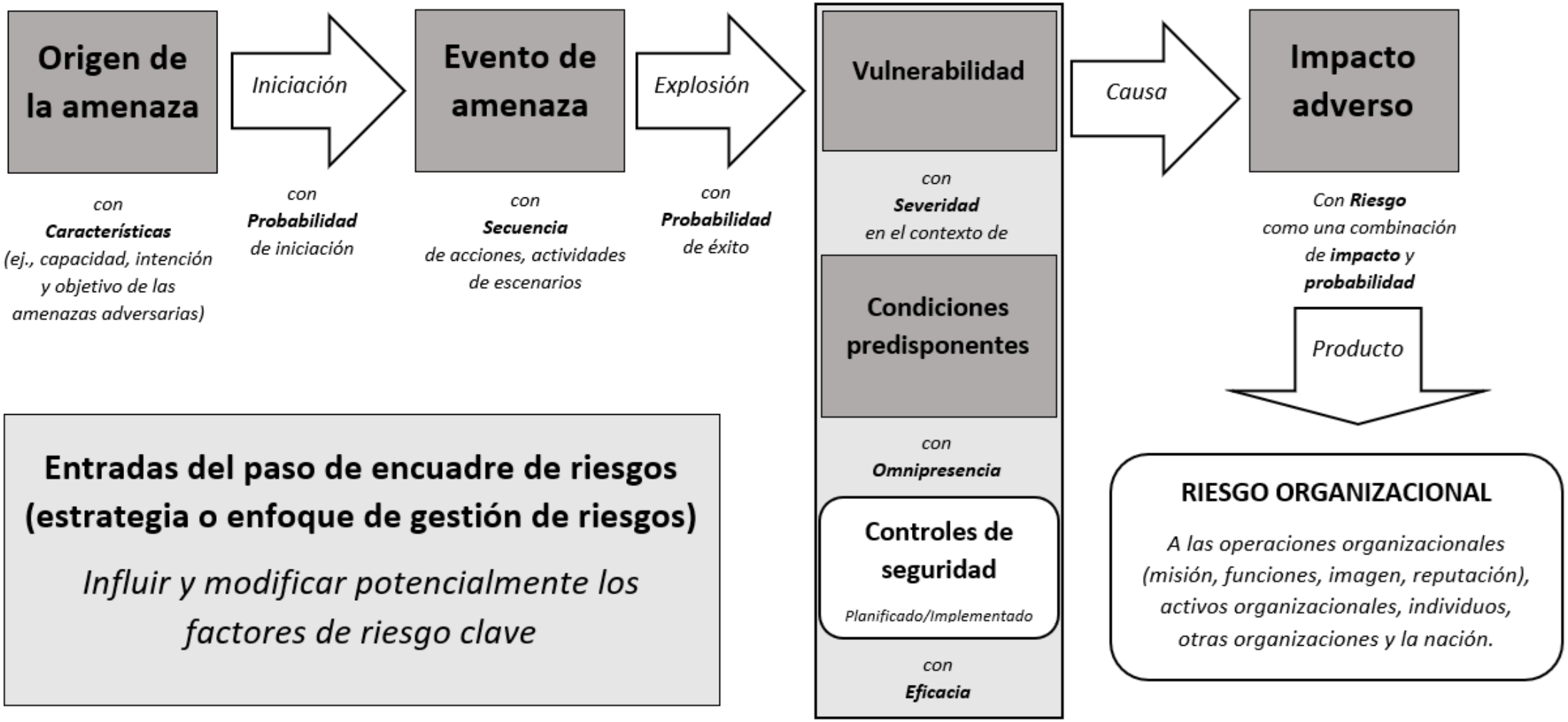
Probabilidad	Catastrófico	Crítico	Grave	Significativo	Menor
Casi cierto	Muy alto	Muy alto	Alto	Alto	Medio
Muy probable	Muy alto	Alto	Alto	Medio	Bajo
Probable	Alto	Alto	Medio	Bajo	Bajo
Poco probable	Medio	Medio	Bajo	Muy bajo	Muy bajo
Improbable	Bajo	Bajo	Bajo	Muy bajo	Muy bajo

Contexto del riesgo

Elección de un método y criterios apropiados

- **Consistencia**: las evaluaciones de los mismos riesgos realizadas por diferentes personas, o por la misma persona en diferentes momentos, en el mismo contexto, deben producir resultados similares.
- **Comparabilidad:** los criterios de evaluación de riesgos deben definirse de manera que las evaluaciones realizadas para diferentes riesgos produzcan resultados comparables cuando representen niveles de riesgo equivalentes.
- **Validez:** las evaluaciones deben generar resultados que se correspondan lo más fielmente posible con la realidad.

Contexto del riesgo - Método



Clasificación de activos de información

La clasificación de los activos de información es necesaria para determinar la sensibilidad relativa y la criticidad de los activos de información, a veces denominados colectivamente como valor comercial. Críticamente se mide por el impacto en la organización debido a la pérdida de un activo (es decir, qué tan importante es el activo para el negocio). La sensibilidad se basa en el daño potencial a la organización debido a la divulgación no autorizada.

Metodologías de clasificación de información & calificación de activos de información (1/6)

- Identificación, registro y asignación de Entidades
- Identificación, registro y asignación de tipos de Información a entidades
- Clasificación de los tipos de información identificados
- Identificación, registro de activos de información y asignación de tipos de información
- Calificación de los activos de información

Metodologías de clasificación de información & calificación de activos de información (2/6)

Identificación, registro y asignación de dueños de Entidades

NOMBRE DE LA ENTIDAD	DUEÑO DE LA ENTIDAD
Prospecto	CEO / CCO
Cliente	Vice presidente de Servicio al Cliente
Póliza	Gerente de Operaciones
Siniestro	Director de siniestros
Proveedor	Gerente de Contabilidad
Empleados	Director Regional

Identificar y registrar entidades de Información institucional

Identificar dueños de las entidades de información y asignar responsabilidades de dichas entidades

Una entidad de información es una agrupación de información mantenida en una Institución, es todo de lo que se puede generar, almacenar, transmitir y compartir información

Metodologías de clasificación de información & calificación de activos de información (3/6)

Identificación, registro y asignación de tipos de Información a entidades

NOMBRE DE LA ENTIDAD	DUEÑO DE LA ENTIDAD	NOMBRE DEL TIPO DE INFORMACIÓN
Prospecto	CEO / CCO	Información de contacto del prospecto
		Datos generales del prospecto
		Posición financiera del prospecto
		Información legal del prospecto
		Información médica del prospecto
		Información de siniestralidad del prospecto
Cliente	Vice presidente de Servicio al Cliente	Información de contacto del cliente
		Datos Generales del cliente
		Posición financiera del cliente
		Información legal del cliente
		Información de vinculación / compliance del cliente
		Información médica del cliente
		Información bancaria de cliente
		Información de siniestralidad del cliente

Identificar y registrar todos tipos de Información* institucional

Identificar la entidad a la que pertenece cada tipo de información identificada y registrar dicha relación

Un tipo de información es una agrupación de datos que pertenecen a una misma entidad con una calificación de importancia similar

Metodologías de clasificación de información & calificación de activos de información (4/6)

Clasificación de los tipos de información identificados

NOMBRE DE LA ENTIDAD	DUEÑO DE LA ENTIDAD	NOMBRE DEL TIPO DE INFORMACIÓN	CONFIDENCIALIDAD
Prospecto	CEO / CCO	Información de contacto del prospecto	ALTO
		Datos generales del prospecto	BAJO
		Posición financiera del prospecto	BAJO
		Información legal del prospecto	BAJO
		Información médica del prospecto	MEDIO
		Información de siniestralidad del prospecto	BAJO
Cliente	Vice presidente de Servicio al Cliente	Información de contacto del cliente	MEDIO
		Datos Generales del cliente	MEDIO
		Posición financiera del cliente	MEDIO
		Información legal del cliente	MEDIO
		Información de vinculación / compliance del cliente	CRÍTICO
		Información médica del cliente	CRÍTICO
		Información bancaria de cliente	MEDIO
		Información de siniestralidad del cliente	MEDIO

Clasificar la información (los tipos de información), de acuerdo con criterios de confidencialidad, disponibilidad e integridad. Esta clasificación de la información se la puede llevar a cabo considerando estándares, buenas prácticas, metodologías previamente definidas o aplicando metodologías propias de la Institución

En el gráfico, se ejemplifica utilizando el criterio de confidencialidad; sin embargo, la evaluación de los tipos de información se la debe hacer los criterios de confidencialidad, disponibilidad, integridad y privacidad

Metodologías de clasificación de información & calificación de activos de información (5/6)

Identificación, registro de activos de información y asignación de tipos de información

Una vez calificados los tipos de información, identificar y registrar todos los activos de Información institucional

Asignar los tipos de información que contiene cada activo de información

NOMBRE ACTIVO DE INFORMACIÓN	TIPO DE INFORMACIÓN QUE CONTIENE
Sistema de gestión de prospectos	Datos generales del prospecto
	Información de contacto del prospecto
	Posición financiera del prospecto
Carpeta Compartida prospectos y clientes	Datos Generales del cliente
	Información de contacto del cliente
	Posición financiera del cliente
	Información legal del prospecto
	Información bancaria de cliente
	Información médica del cliente
	Información de siniestralidad del cliente
	Información de vinculación / compliance del cliente
	Información General de la compañía de seguros
	Información de condiciones particulares de la póliza
Carpeta compartida área comercial	Datos generales del prospecto
	Información de contacto del prospecto
	Posición financiera del prospecto
	Información legal del prospecto
	Información de negociación de pólizas
	Información General de la compañía de seguros
	Información de vinculación / compliance del cliente
	Información de siniestralidad del prospecto
	Información médica del prospecto
	Datos Generales del cliente
	Información de contacto del cliente
	Posición financiera del cliente
	Información legal del cliente
	Información de siniestralidad del cliente
	Información médica del cliente

Metodologías de clasificación de información & calificación de activos de información (6/6)

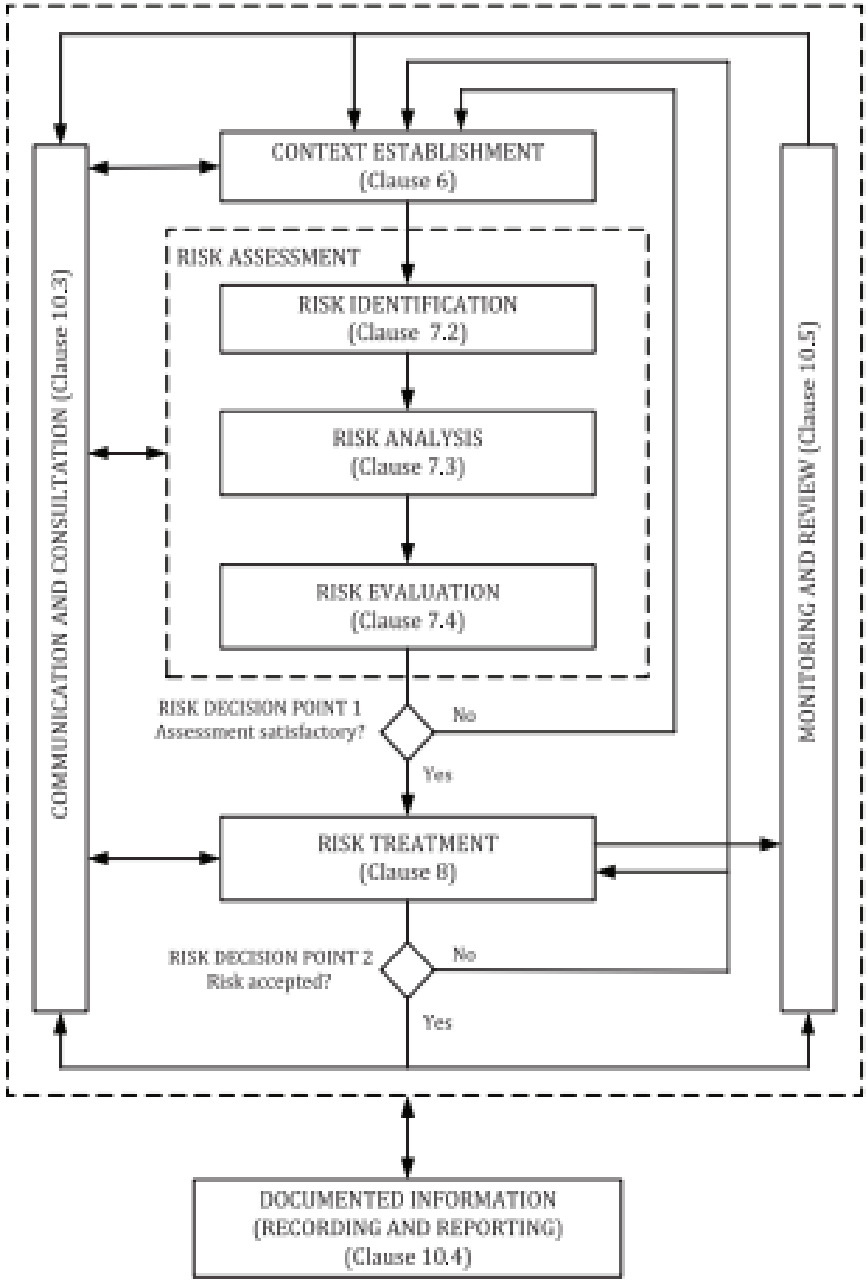
Calificación de los activos de información

NOMBRE ACTIVO DE INFORMACIÓN	TIPO DE INFORMACIÓN QUE CONTIENE	CLASIFICACIÓN DEL TIPO DE INFORMACIÓN	CALIFICACIÓN DEL ACTIVO DE INFORMACIÓN
Sistema de gestión de prospectos	Datos generales del prospecto	BAJO	ALTO
	Información de contacto del prospecto	ALTO	
	Posición financiera del prospecto	BAJO	
Carpeta Compartida prospectos y clientes	Datos Generales del cliente	BAJO	CRÍTICO
	Información de contacto del cliente	MEDIO	
	Posición financiera del cliente	MEDIO	
	Información legal del prospecto	BAJO	
	Información bancaria de cliente	MEDIO	
	Información médica del cliente	CRÍTICO	
	Información de siniestralidad del cliente	MEDIO	
	Información de vinculación / compliance del cliente	CRÍTICO	
	Información General de la compañía de seguros	BAJO	
	Información de condiciones particulares de la póliza	BAJO	
Carpeta compartida área comercial	Datos generales del prospecto	BAJO	CRÍTICO
	Información de contacto del prospecto	ALTO	
	Posición financiera del prospecto	BAJO	
	Información legal del prospecto	BAJO	
	Información de negociación de pólizas	MEDIO	
	Información General de la compañía de seguros	BAJO	
	Información de vinculación / compliance del cliente	CRÍTICO	
	Información de siniestralidad del prospecto	BAJO	
	Información médica del prospecto	MEDIO	
	Datos Generales del cliente	MEDIO	
	Información de contacto del cliente	MEDIO	
	Posición financiera del cliente	MEDIO	
	Información legal del cliente	MEDIO	
	Información de siniestralidad del cliente	MEDIO	
	Información médica del cliente	CRÍTICO	

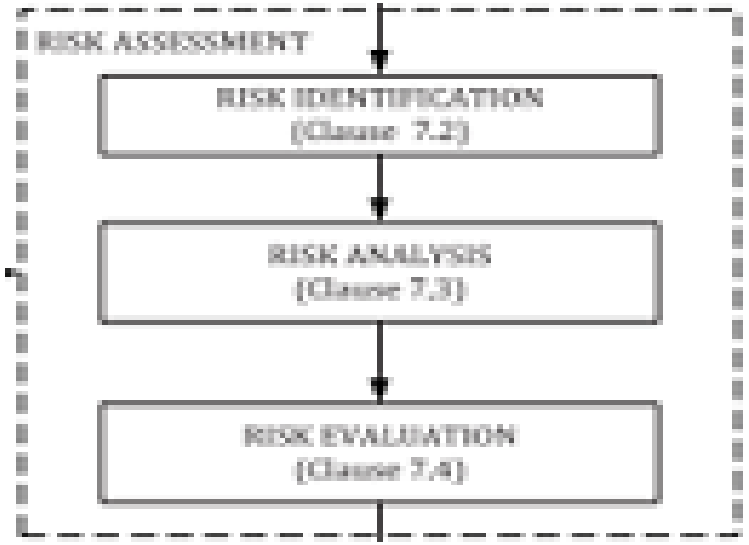
Asignar calificación de criticidad a los activos de información identificados, para esto se evalúa las clasificaciones de todos los tipos de información que contiene el activo. El activo de información tendrá la calificación del tipo de información de mayor criticidad; es decir, si el activo contiene al menos un tipo de información crítica, dicho activo será crítico.

Como se puede ver en el gráfico, los activos de información tienen la calificación dependiendo de la clasificación del tipo de información de mayor criticidad contenida en dicho activo

Gestión de riesgos

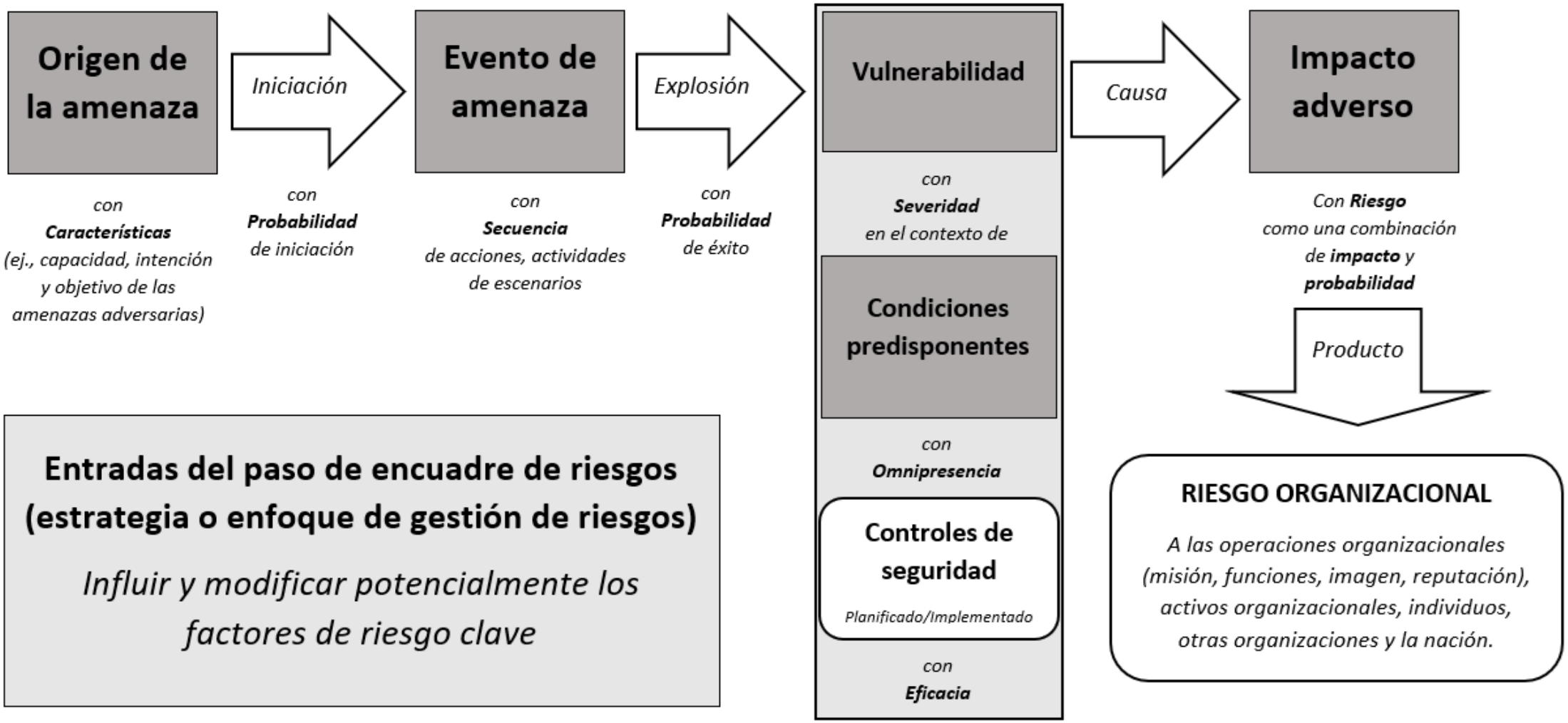


Gestión de riesgos



Concepto	Definición
3.2.3 Apreciación del riesgo	Es el Proceso general de identificación, análisis y evaluación de riesgos.
3.2.4 Identificación de riesgos	Es el Proceso de encontrar, reconocer y describir riesgos.
3.2.5 Análisis de riesgos	Es el Proceso para comprender la naturaleza del riesgo y determinar su nivel.
3.2.6 Evaluación de riesgos	Es Comparar resultados del análisis con criterios de riesgo para decidir si son aceptables.

Evaluación de riesgos de ciberseguridad



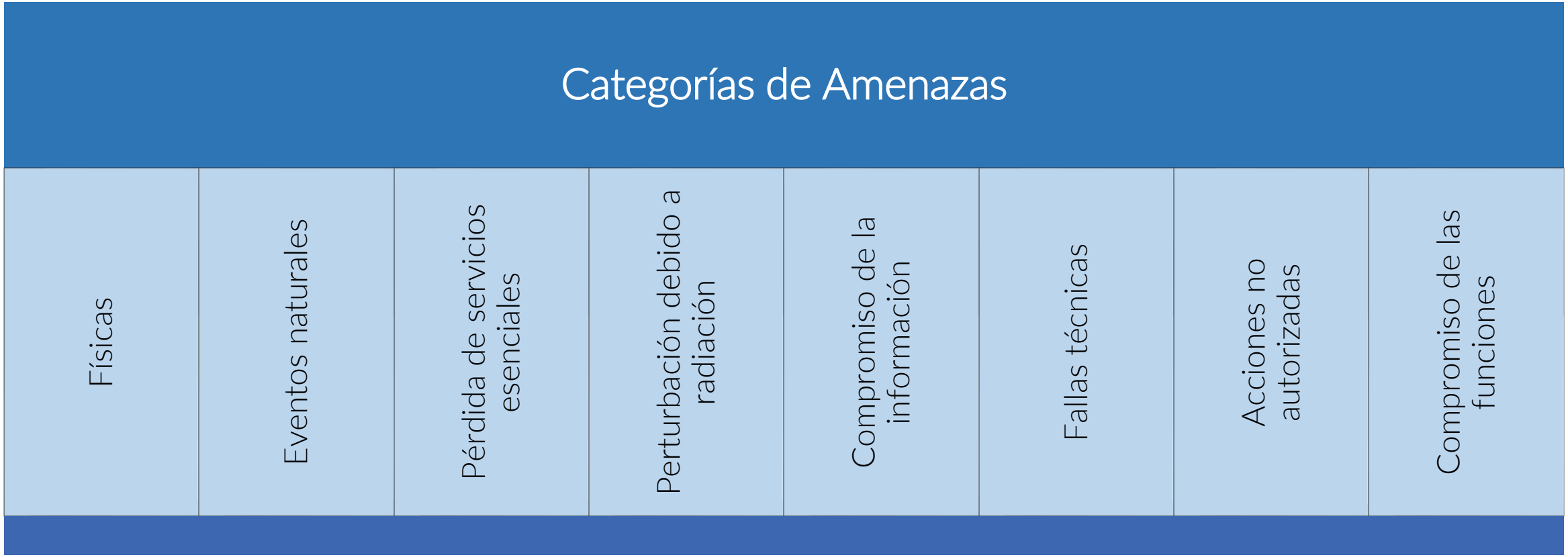
Amenazas

¿Qué es una Amenaza?

Son circunstancias o eventos que tienen la probabilidad de ocasionar daño a un recurso (ACTIVO DE INFORMACIÓN) de información al explotar vulnerabilidades en el sistema

Amenazas

Categorías de Amenazas



Amenazas

Amenazas Internas

En el proceso de contratación es necesario revisar las calificaciones y aptitudes de los posibles empleados.

- La persona puede enviar información incorrecta y alegar educación, certificación o experiencia que en realidad no posee

Llevar a cabo revisiones y/o validaciones de referencias y desempeño, verificación de antecedentes (siempre y cuando la legislación lo permita)

En el desarrollo de sus funciones, se debe recordar a los empleados las políticas de la organización y sus responsabilidades, mediante charlas de concientización y revisiones periódicas

Uno de los mejores controles basado en los empleados es la interacción con ellos y entender sus quejas, frustraciones o problemas y tratar de resolverlos

Al momento de terminar la relación laboral, el empleado debe devolver todos los activos de la organización y eliminar inmediatamente los accesos a sistemas, red e instalaciones

Amenazas

Amenazas Externas

En un entorno de red donde los datos se almacenan fuera del sitio o los alojan proveedores de servicios en la nube, las amenazas provenientes de fuera de la organización pueden originarse desde cualquier lugar y adoptar distintas formas

Amenazas externas				
Actos criminales	Fallas en las instalaciones (congelamiento de tuberías/rotura de tuberías)	Accidentes industriales	Sabotaje	Interrupción en la cadena de suministros
Corrupción de datos	Incendio	Pérdida de activos	Actividad sísmica	Terrorismo
Enfermedad (epidemia)	Inundación	Fallas mecánicas	Tormentas severas	Robo
Espionaje	Fallas de hardware	Sobretensión/falla en el suministro del servicio	Errores de software	

Amenazas

Amenaza Persistente Avanzada

Una APT hace referencia a atacantes altamente capacitados y avanzados que son determinados o persistentes en sus intentos por explotar sistemas y redes. Las APT presentan un riesgo significativo para las organizaciones de caso todos los tipos a nivel mundial.
Según la publicación 800-39 de la NIST, una APT se define así:

"Una APT es un adversario que posee niveles sofisticados de experiencia e importantes recursos que le permiten crear oportunidades para lograr sus objetivos utilizando múltiples vectores de ataques (Por ejemplo, cibernéticos, físicos y engaños). Estos objetivos normalmente, incluyen establecer y extender los puntos de apoyo dentro de la infraestructura de TI de las organizaciones atacadas con el propósito de extraer información, perjudicar o dificultar los aspectos críticos de una misión, programa u organización; o posicionarse para llevar a cabo estos objetivos en el futuro."

Amenazas

Fuentes típicas de APT

Amenaza	Lo que buscan	Impacto al negocio
Agencias de inteligencia	Secretos comerciales, de defensa o políticos	Pérdida de secretos comerciales o ventajas competitivas y comerciales
Grupos criminales	Información sobre identidad personal, oportunidades de extorsión, transferencias de dinero o cualquier otro secreto para una potencial venta posterior	Pérdida financiera, violación de datos de socios y clientes a gran escala o pérdida de secretos comerciales
Grupos terroristas	Terror ampliamente generalizado a través de la muerte, destrucción y perturbación	Pérdida de producción y servicios, irregularidades en el mercado de valores y riesgo potencial para la vida humana
Grupos activistas	Información confidencial o interrupción de servicios	Violación de datos importante o pérdida de servicio
Fuerzas armadas	Inteligencia o posicionamiento para respaldar ataques futuros sobre infraestructuras nacionales críticas	Daños graves a las instalaciones en caso de conflicto militar

Amenazas

Ciclo de vida Amenaza Persistente Avanzada

Ciclo de Vida de APT	Fase	Descripción
	Compromiso social	Los atacantes utilizan ingeniería social y spear phishing por correo electrónico, utilizando un virus de día cero. Puede instalar malware en un sitio web que sea probable que los empleados de la víctima visiten
	Establecimiento de punto de apoyo	Los atacantes pueden instalar SW de administración remota en la red de la víctima o crear túneles y puertas traseras que permitan el acceso furtivo a su infraestructura
	Escalado de privilegios	Las APT utilizan vulnerabilidades conocidas de SW y violaciones de contraseñas para adquirir privilegios de administrador en la PC de la víctima y posiblemente ampliarlos para cuentas de administrador de dominio de Windows
	Reconocimiento interno	Los atacantes recolectan información sobre infraestructura circundante, relaciones de confianza y estructura de dominios de Windows
	Movimiento lateral	Los atacantes amplían el control hacia otras estaciones de trabajo, servidores y elementos de la infraestructura y realizan extracción de datos de los mismos
	Conservación de presencia	Las APT garantizan el control continuo en los canales de acceso y las credenciales adquiridas en los pasos anteriores
	Completar la misión	Los atacantes retiran los datos robados de la red de la víctima

Amenazas

Amenazas emergentes

Las indicaciones de una amenaza emergente pueden incluir una actividad inusual en el sistema, alarmas repetitivas, rendimiento lento del sistema o la red, o una actividad nueva o excesiva en los registros

La falta de monitoreo efectivo, en combinación con una amenaza, puede llevar a una violación

La tecnología suele ser una fuente de nuevas vulnerabilidades, incluso puede ser un agente de amenazas dentro del sistema de información

El responsable de riesgos debe estar alerta del surgimiento de las nuevas tecnologías y prepararse para introducirlas en la organización

Amenazas

¿Qué es una vulnerabilidad?

La vulnerabilidad también es conocida como debilidad	Los activos son vulnerabilidades en distintos grados	Debe considerarse el grado de exposición, ya que afecta la probabilidad que una vulnerabilidad sea comprometida	Se deben hacer distinciones al momento de establecer prioridades de los esfuerzos de gestión de riegos y determinar el nivel de riesgo dentro de un escenario y al trata de explicar a la alta gerencia
Muchas vulnerabilidades son condiciones que existen en los sistemas y que deben identificarse para poder abordarlas	La identificación de vulnerabilidades permite encontrar problemas antes que alguien más pueda explotarlos	Es necesario realizar pruebas de penetración y evaluaciones periódicas de vulnerabilidades	La evaluación de vulnerabilidades debe considerar las debilidades de procesos y procedimientos y debilidades lógicas

Amenazas

Clasificación/Categorización de vulnerabilidades

Amenazas

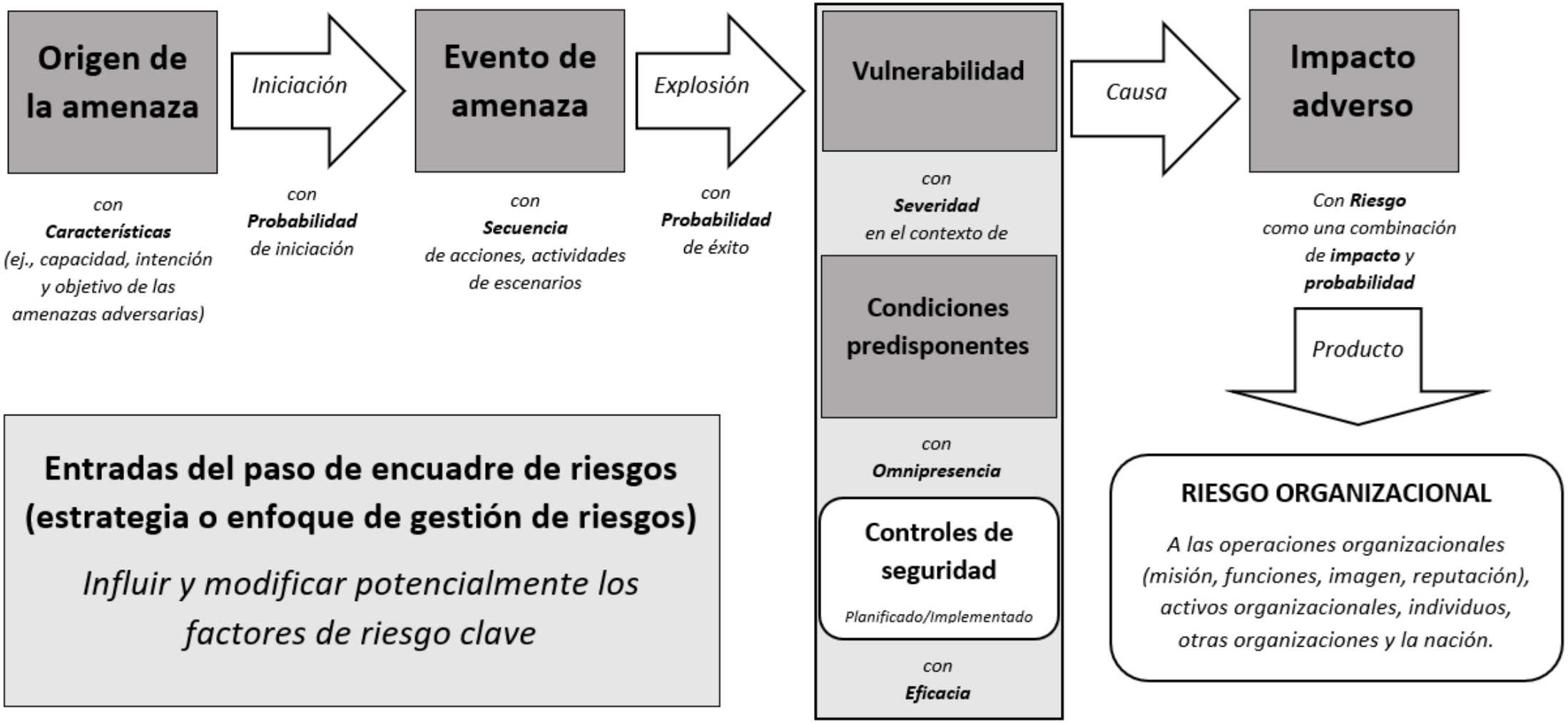
Ejemplos de vulnerabilidades

Fuentes de amenazas, vulnerabilidades y controles

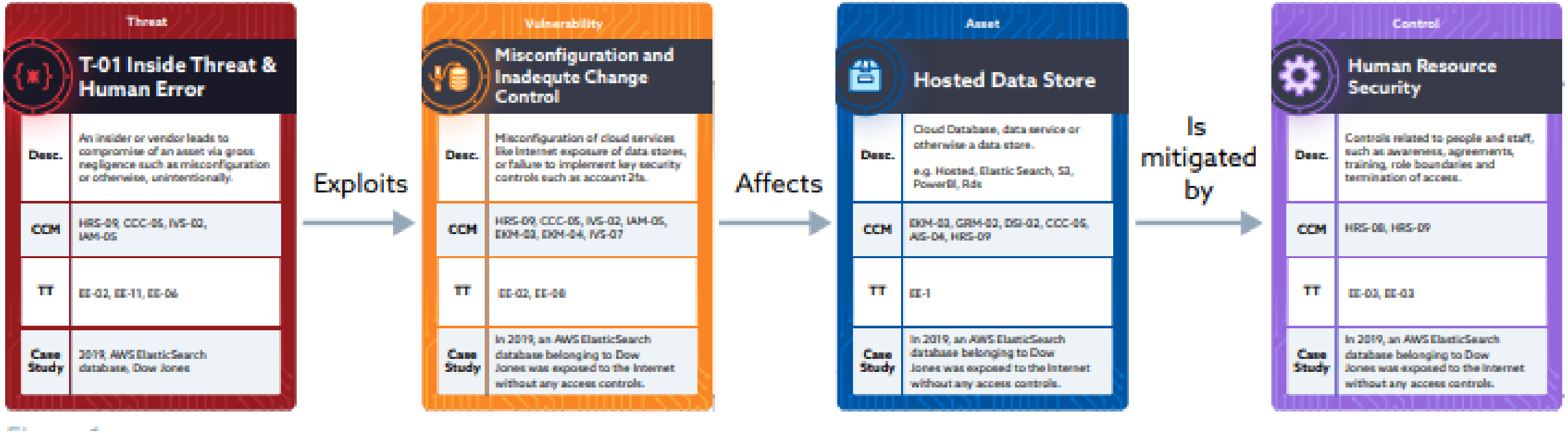
Fuente (Organismo)	Orientación General y Enfoque	Utilidad para el Riesgo PDP	Enlace de Referencia
1. ISO/IEC 27002	Controles de Seguridad. Guía detallada que describe más de 90 controles de seguridad de la información. Se enfoca en la implementación práctica de medidas técnicas y organizacionales.	Controles: Proporciona la taxonomía de controles estándar para mitigar vulnerabilidades y tratar riesgos (ej., gestión de privilegios, seguridad criptográfica, continuidad del negocio).	Buscar la publicación del estándar en ISO.org (Sujeto a compra).
2. NIST SP 800-53	Controles de Sistemas Federales (EE. UU.). Amplio catálogo de controles de seguridad y privacidad. Muy detallado y enfocado en el rigor del cumplimiento normativo.	Vulnerabilidades y Controles: Excelente para identificar vulnerabilidades operacionales y técnicas en sistemas de misión crítica. La versión moderna incluye controles de privacidad (P-Controls).	Buscar "NIST SP 800-53" en el sitio web de NIST.
3. OWASP Top 10	Riesgos de Aplicaciones Web. Publicación anual que lista las 10 vulnerabilidades de seguridad más críticas que se encuentran en aplicaciones web.	Vulnerabilidades y Amenazas Técnicas: Identifica las vulnerabilidades más explotadas por atacantes que afectan directamente la Confidencialidad e Integridad de los datos a través de *front-ends* (ej., *SQL Injection*, *Broken Access Control*).	Buscar "OWASP Top 10" en el sitio web de OWASP.
4. CVSS (Common Vulnerability Scoring System)	Sistema de Puntuación. Metodología estándar y abierta para calificar la gravedad de las vulnerabilidades de *software* (CVEs). Se enfoca en la probabilidad de explotación.	Análisis: Permite al analista priorizar las vulnerabilidades técnicas de acuerdo con su criticidad real y su impacto potencial en el sistema.	Buscar "CVSS Score" en el sitio web de FIRST.org o NIST NVD.
5. NVD (National Vulnerability Database)	Base de Datos de Referencia. Repositorio gubernamental de EE. UU. que agrega todas las vulnerabilidades de seguridad conocidas públicamente (CVEs) y asigna un puntaje de riesgo.	Amenazas y Vulnerabilidades Técnicas: Fuente de consulta obligatoria para la fase de Identificación y Análisis de riesgos, ya que cataloga las debilidades reales del *software* y *hardware*.	Buscar "NVD" en el sitio web de NIST.
6. LOPDP (Ley Orgánica de Protección de Datos Personales, Ecuador)	Marco Legal de Cumplimiento. Ley que establece la totalidad de los derechos y principios de PDP en Ecuador.	Impacto (Consecuencia): Define el impacto máximo (daño legal) y los factores de riesgo de consecuencia (datos especiales, gran escala, perfilamiento automatizado).	Buscar la Ley Orgánica de Protección de Datos Personales en el Registro Oficial de Ecuador.

ESCENARIO

Evaluación de riesgos de ciberseguridad



Referencia del modelo de amenazas en la nube



Referencia del modelo de amenazas en la nube

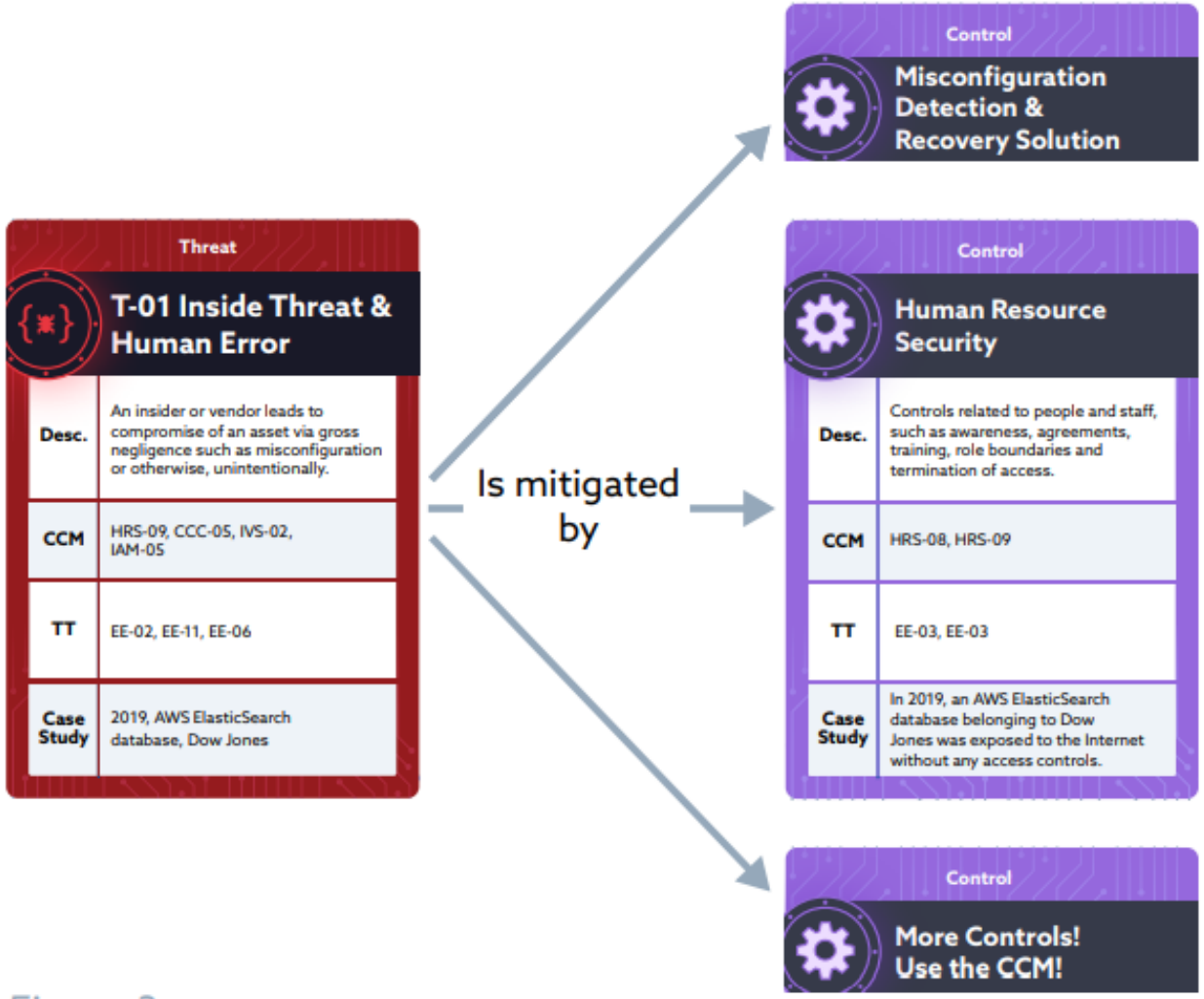


Figure 2

CAPÍTULO 1: Fundamentos de Controles Internos Informáticos

Definición y Objetivos del Control Interno Informático (CII)

Definición

Conjunto de políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable de que los objetivos de negocio se alcanzarán y los eventos no deseados se prevendrán o detectarán.

CAPÍTULO 2: Taxonomía de Controles y Buenas Prácticas

- **Clasificación General**

Taxonomía de Controles: Preventivo, Detectivo y Correctivo

La clasificación más importante se basa en el momento en que actúa el control respecto al incidente.

Preventivo: Actúa ANTES del incidente (evita que ocurra).

Detectivo: Actúa DURANTE o INMEDIATAMENTE DESPUÉS (alerta sobre el incidente).

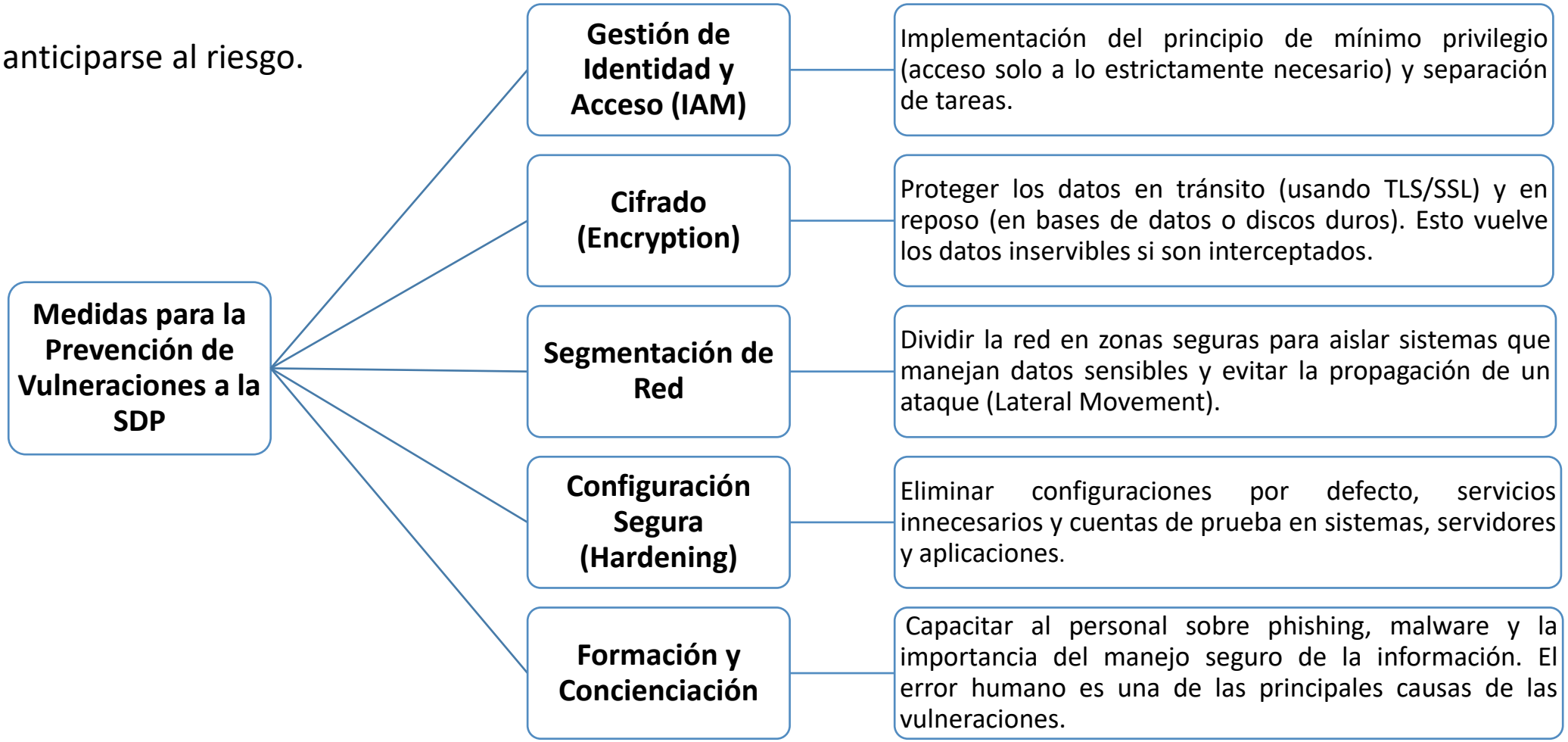
Correctivo: Actúa DESPUÉS (reduce el impacto y recupera).

CAPÍTULO 2: Taxonomía de Controles y Buenas Prácticas

- **Controles Preventivos Clave (Énfasis ISO 27002)**

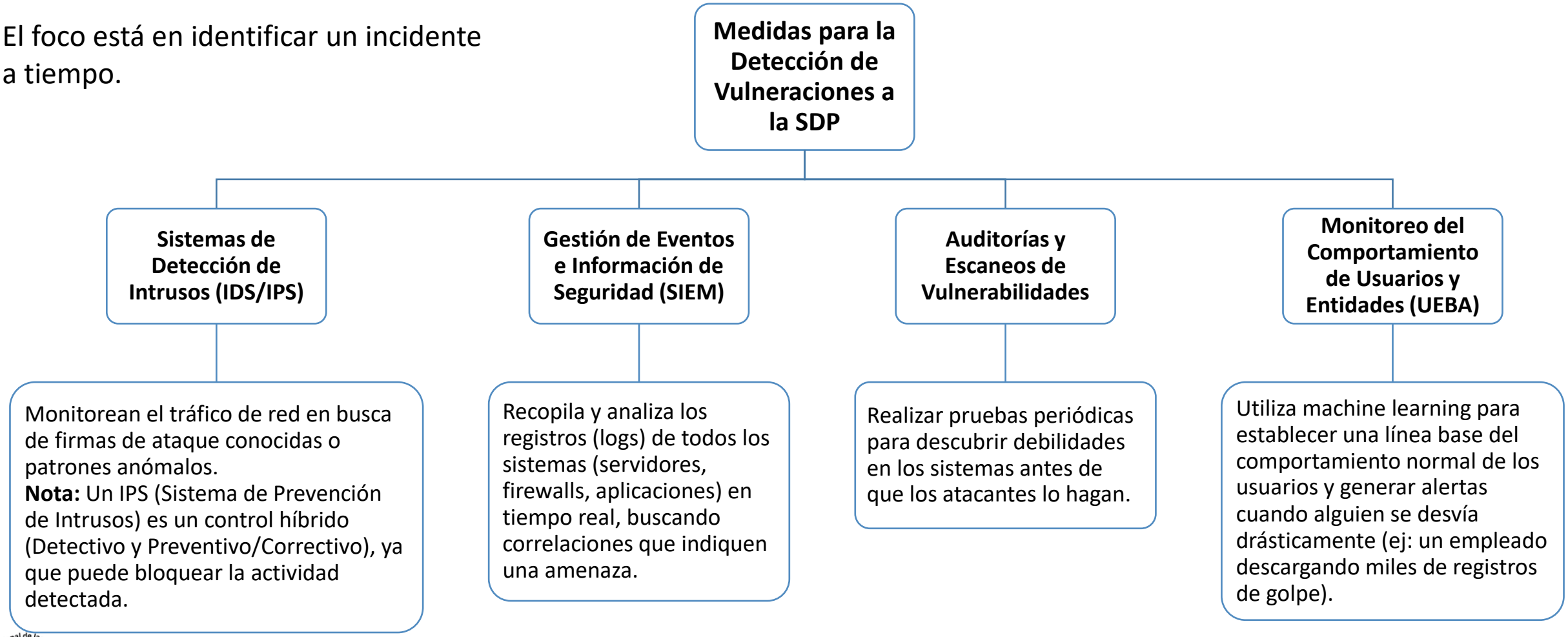
A. Medidas para la Prevención de Vulneraciones a la Seguridad de Datos Personales

El foco está en anticiparse al riesgo.



B. Medidas para la Prevención de Vulneraciones a la Seguridad de Datos Personales

El foco está en identificar un incidente a tiempo.



C. Medidas para la Respuesta a Vulneraciones

El foco es la contención, erradicación y recuperación.

Medidas para la Respuesta a Vulneraciones

- **Plan de Respuesta a Incidentes (IRP)**
  - Un documento formal con roles, responsabilidades y pasos a seguir, que incluye:
  - **1. Preparación:** Asegurar que los recursos de respuesta están listos.
  - **2. Detección y Análisis:** Confirmar el incidente y su alcance.
  - **3. Contención:** Aislar los sistemas afectados para evitar más daños (ej: desconectar un servidor de la red).
  - **4. Erradicación:** Eliminar la causa raíz (ej: malware o la vulnerabilidad explotada).
  - **5. Recuperación:** Restaurar la operación normal y validar la seguridad.
  - **6. Lecciones Aprendidas:** Revisar el proceso para mejorar los controles futuros.
- **Notificación a Autoridades y Afectados**
  - En cumplimiento con leyes como el RGPD o CCPA, se debe notificar a la autoridad de protección de datos y, a menudo, a los titulares de los datos sobre la vulneración.
- **Análisis Forense Digital**
  - Recopilar evidencia de manera legalmente admisible para entender qué pasó, cómo y quién fue responsable.

D. Interdependencias entre los Controles de Riesgos

Los controles nunca operan de forma aislada; forman una defensa en profundidad (Defense in Depth) donde las capas se apoyan mutuamente.

Ejemplo 1 (Prevención y Detección)

- Si la política de acceso (Preventivo/Administrativo) falla y un atacante obtiene credenciales, el SIEM (Detectivo/Técnico) debe monitorear los logs y alertar sobre un acceso sospechoso.

Ejemplo 2 (Detección y Respuesta):

- Un IDS (Detectivo) identifica un ataque, lo que automáticamente dispara la ejecución del Plan de Respuesta a Incidentes (Correctivo/Administrativo), llevando al equipo a aislar el sistema.

La base Administrativa

- Una buena Política de Seguridad de la Información (Administrativo) es la base que justifica e impulsa la compra e implementación de un Firewall (Técnico/Preventivo).

E. Evaluación del Rendimiento de las Medidas de Seguridad en el Tiempo

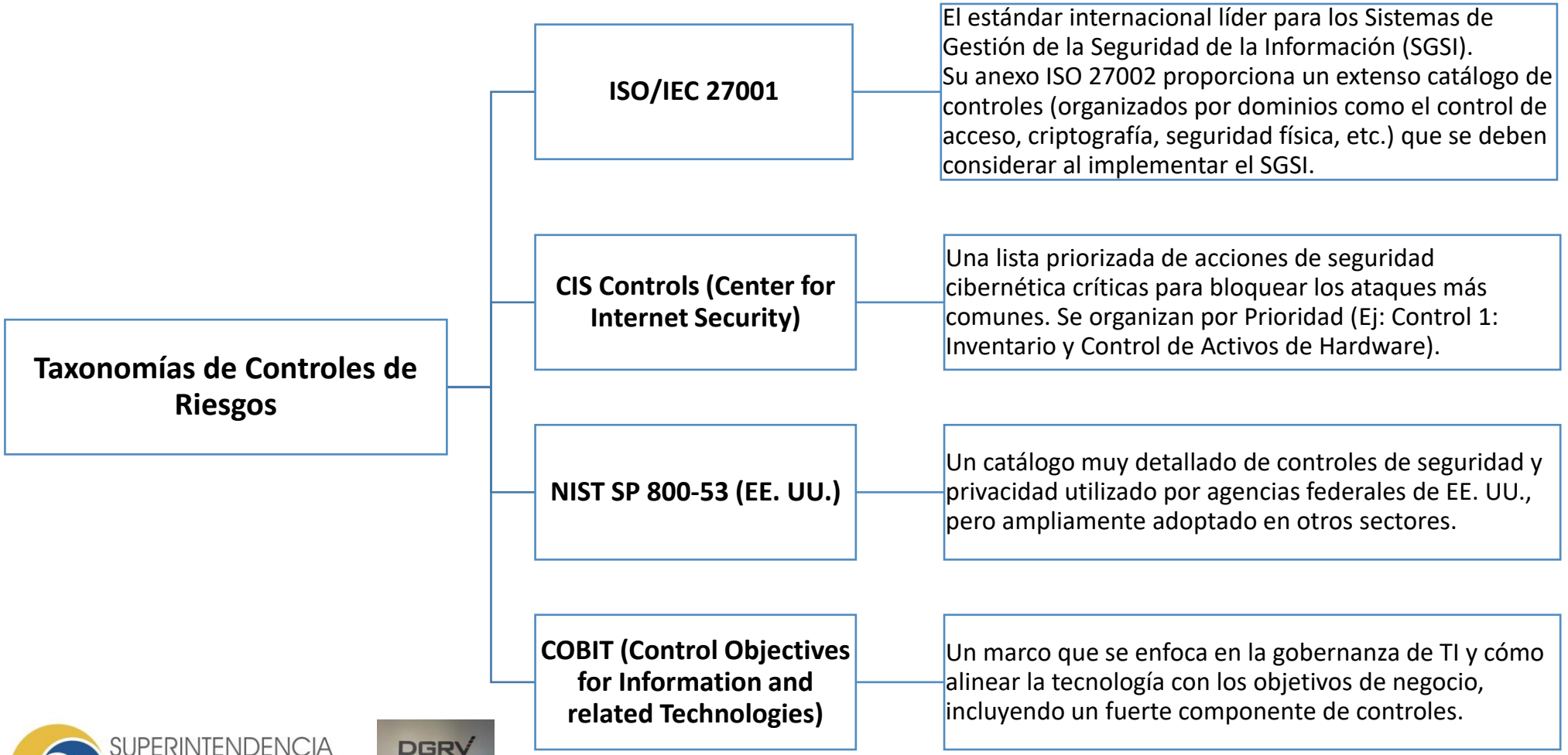
Un control es inútil si no se valida que funciona y sigue siendo relevante.

Evaluación del Rendimiento de las Medidas de Seguridad en el Tiempo

Métricas e Indicadores Clave de Riesgo (KRI) y Rendimiento (KPI)		Pruebas de Penetración (Penetration Testing)	Auditorías Internas y Externas
KPIs: Miden la eficacia del control (ej: Porcentaje de empleados que completan la formación de seguridad; Tiempo promedio para aplicar un parche).	**KRIs:** Miden el riesgo residual (ej: Número de incidentes críticos por mes; Número de vulnerabilidades de alto riesgo no mitigadas).	Simulación de un ataque real por un tercero para probar la solidez de los controles técnicos y administrativos.	Verificar el cumplimiento de las políticas de seguridad y los marcos normativos (como el RGPD o leyes locales de protección de datos).

F. Taxonomías de Controles de Riesgos (Ej: ISO/IEC 27001, CIS Controls, entre otras)

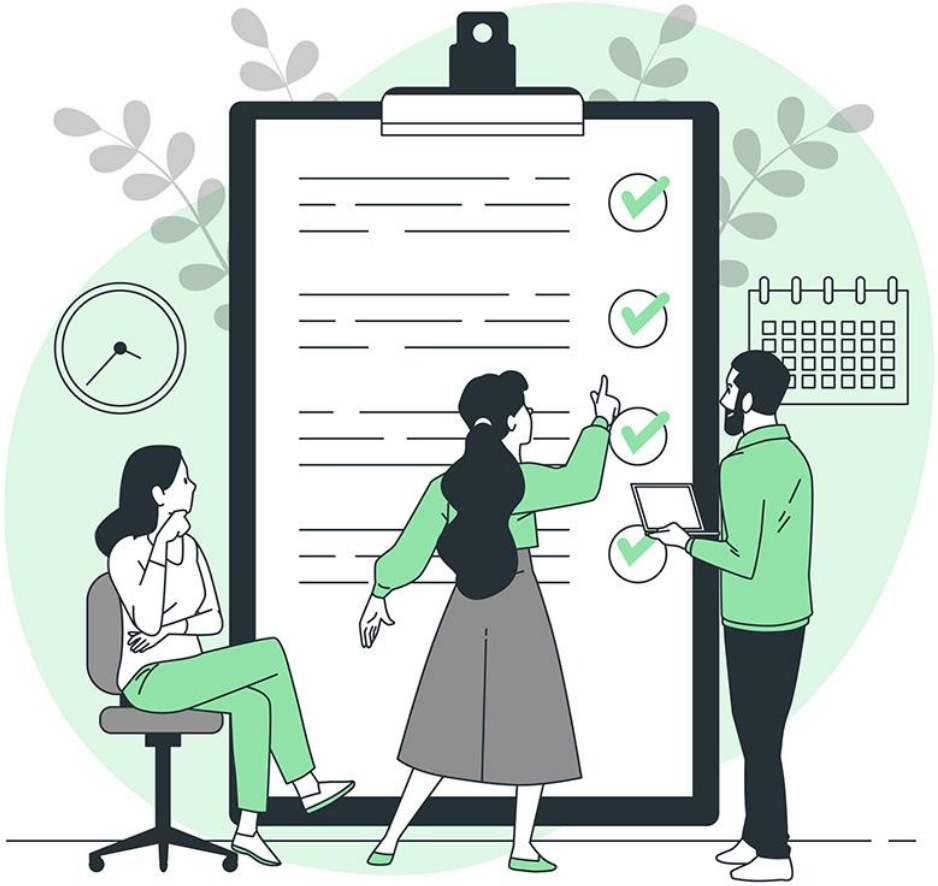
Las taxonomías son marcos de referencia que organizan los controles para asegurar una cobertura completa de los riesgos.



CAPÍTULO 3: Marco de Referencia y Normativas para la Evaluación

Marcos de Referencia Internacionales para la Evaluación

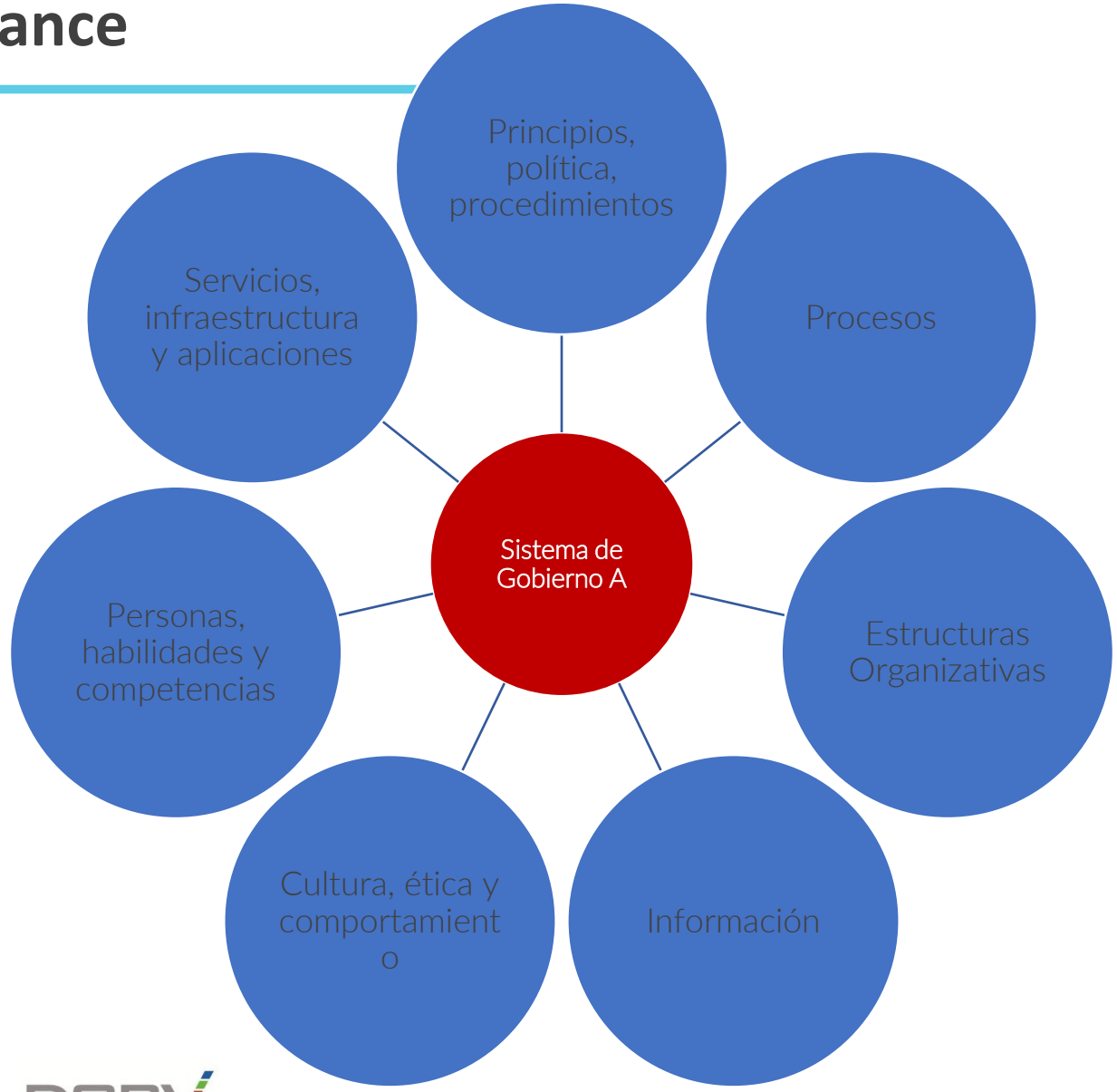
- ¿Contra qué evaluamos? No podemos evaluar "al vacío".
- Necesitamos un Criterio (una "regla" o "buena práctica") para comparar lo que vemos.
- **Marcos Clave:** COBIT (Gobernanza), ISO 27001/2 (Seguridad), NIST CSF (Ciberseguridad).



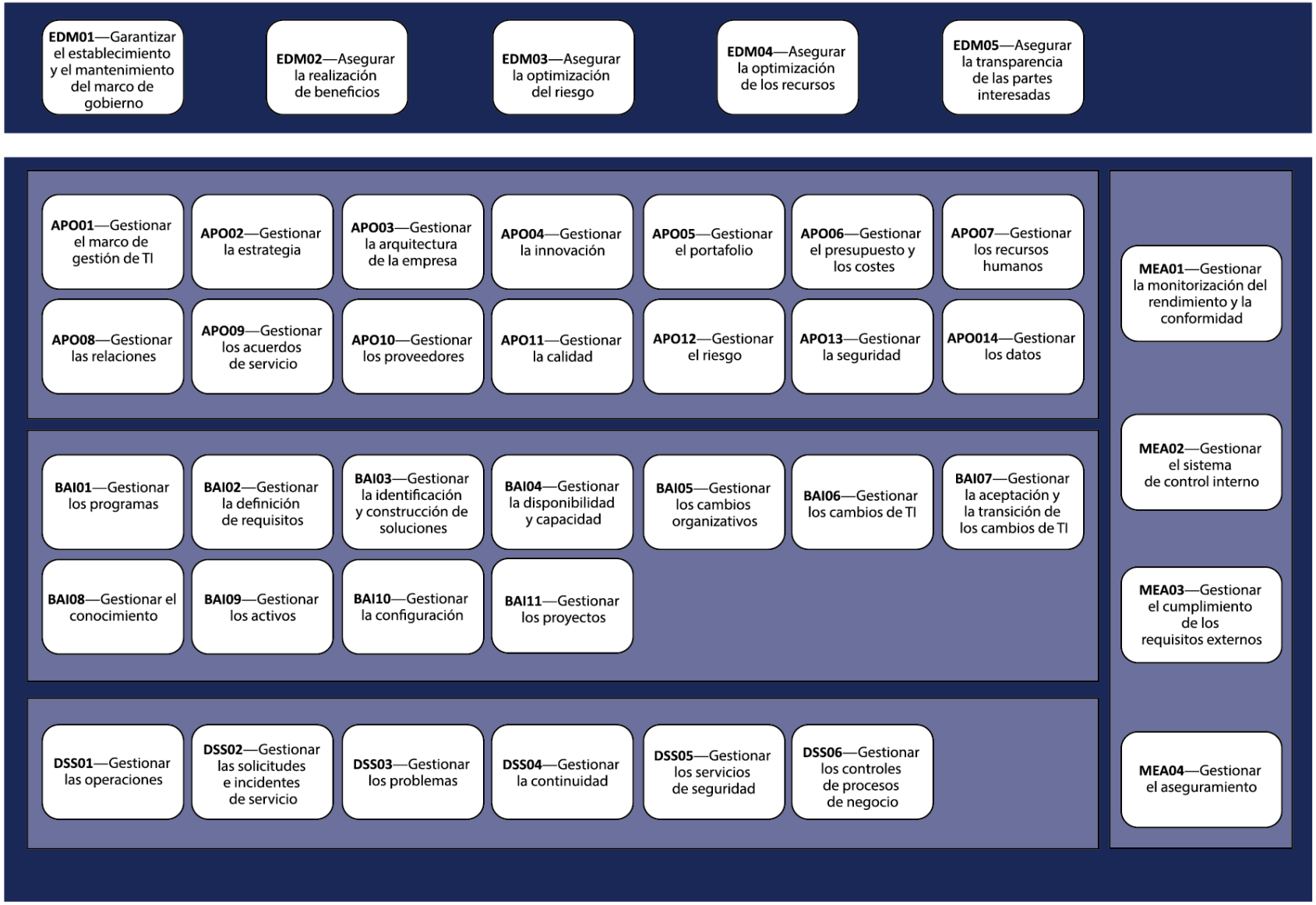
COBIT 2019: Uso de Objetivos de Gestión en la Evaluación

- **Enfoque:** Gobernanza y Gestión de TI.
- **Uso en Evaluación:** Se usa para evaluar la madurez de un proceso (ej. DSS05 "Gestionar Servicios de Seguridad"). ¿Está el proceso en Nivel 1 (Básico) o Nivel 5 (Optimizado)?
- Es ideal para evaluaciones a nivel estratégico y de procesos.

Identificar el alcance



Identificar el alcance



Controles generales

Mínimos

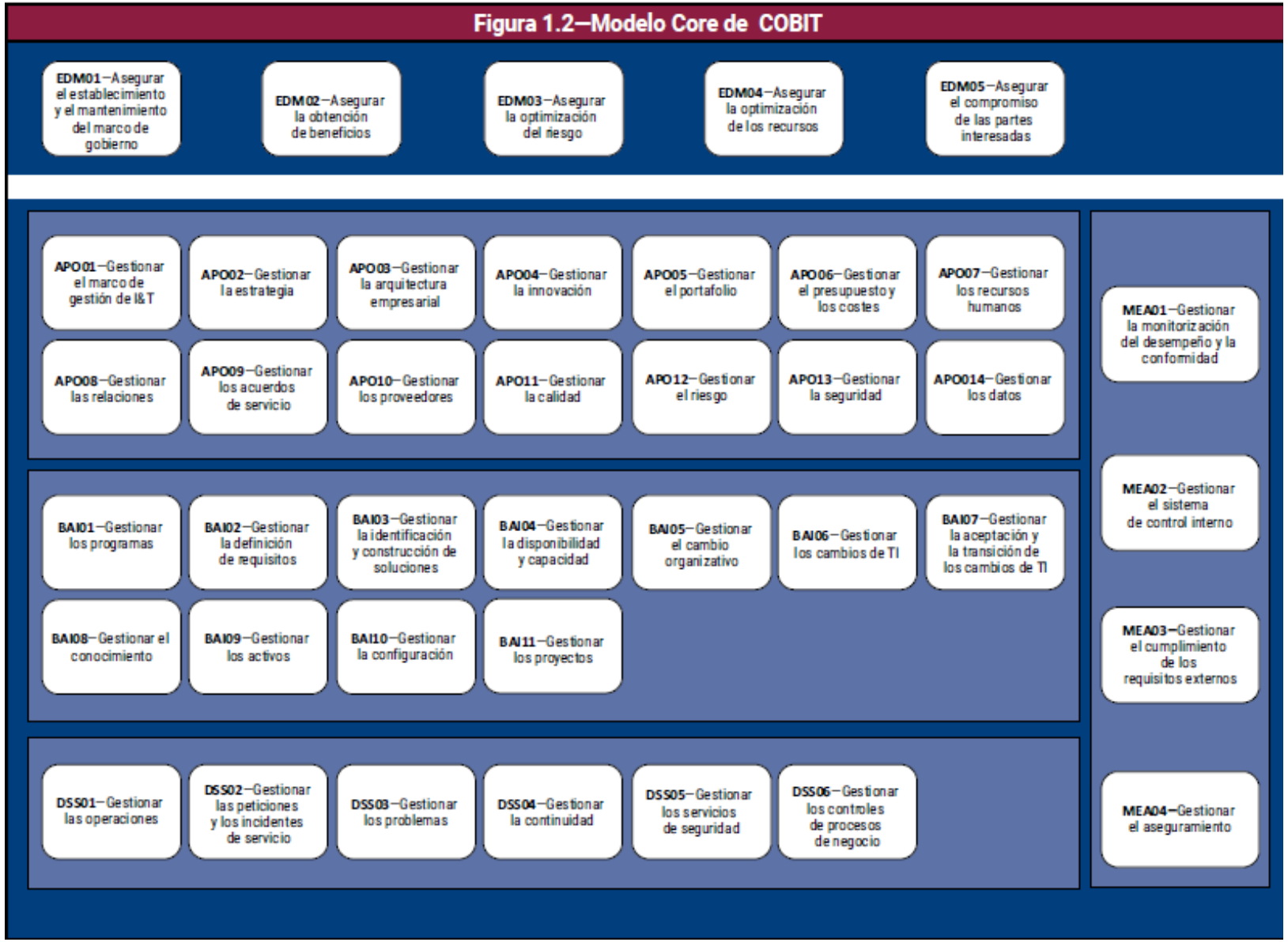
- Gestión de Seguridad
- Gestión de Construcción (Desarrollo y cambios)
- Gestión de Operación
  - Gestión de Incidentes
  - Gestión de Continuidad

Otros

- Gestión de problemas
- Gestión de configuración
- Gestión de proveedores

Controles generales : Seguridad de la Información

Seguridad de la Información



Controles generales : Seguridad de la Información

CONCEPTOS GENERALES		PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la Seguridad	**Descripción** Definir, operar y monitorizar un sistema de gestión de seguridad de la información.	1. Establecer y mantener un sistema de gestión de seguridad de la información (SGSI	Establecer y mantener un sistema de gestión de seguridad de la información (SGSI) que proporcione un enfoque estándar, formal y continuo para la gestión de la seguridad de la información, mediante la habilitación de tecnología segura y procesos de negocio alineados con los requisitos del negocio
	Propósito Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa	2 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad	Mantener un plan de seguridad de la información que describa cómo se debe manejar el riesgo de seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura de la empresa. Asegurar que las recomendaciones para implementar mejoras a la seguridad se basen en casos de negocio aprobados, implementados como una parte integral del desarrollo de servicios y soluciones, y que operen como una parte integral de la operación del negocio
	Metas de alineamiento • Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad	3. Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI).	Mantener y comunicar periódicamente la necesidad y los beneficios de una mejora continua de seguridad de la información. Recopilar y analizar datos sobre el sistema de gestión de seguridad de la información (SGSI) y mejorar su efectividad. Corregir los incumplimientos para evitar la recurrencia

Controles generales : Seguridad de la Información

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los servicios de seguridad		
Descripción Proteger la información de la empresa para mantener el nivel de riesgo de la seguridad de la información aceptable para la empresa, conforme con la política de seguridad. Establecer y mantener roles y privilegios de acceso de seguridad de la información. Realizar una monitorización de la seguridad.	1. Proteger contra software malicioso	Implementar y mantener en toda la empresa medidas preventivas, detectivas y correctivas (especialmente parches de seguridad y control de virus actualizados) para proteger los sistemas de información y la tecnología del software malicioso (p. ej., ransomware, malware, virus, gusanos, spyware y spam).
	2 Gestionar la seguridad de la conectividad y de la red	Usar medidas de seguridad y procedimientos de gestión relacionados para proteger la información a través de todos los métodos de conectividad
Propósito Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información	3. Gestionar la seguridad de endpoint	Garantizar que los dispositivos de punto final (Endpoint, término en inglés) (p. ej., ordenador portátil, ordenador de sobremesa, servidor y otros dispositivos móviles o de red o software) tengan una seguridad a un nivel igual o superior al de los requisitos de seguridad definidos para la información procesada, almacenada o transmitida.
	4. Gestionar la identidad del usuario y el acceso lógico	Asegurarse de que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requisitos del negocio. Coordinarse con las unidades del negocio que gestionan sus propios derechos de acceso en los procesos de negocio
Metas de alineamiento • Gestión de riesgo relacionado con I&T • Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad	5. Gestionar el acceso físico a los activos de I&T.	Definir e implantar procedimientos (incluyendo procedimientos de emergencia) para otorgar, limitar y revocar el acceso a las instalaciones, edificios y áreas, de acuerdo con las necesidades del negocio. El acceso a las instalaciones, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Este requisito aplica a todas las personas que accedan a las instalaciones, incluyendo personal interno, personal temporal, socios y clientes, proveedores, visitantes y cualquier otro tercero.

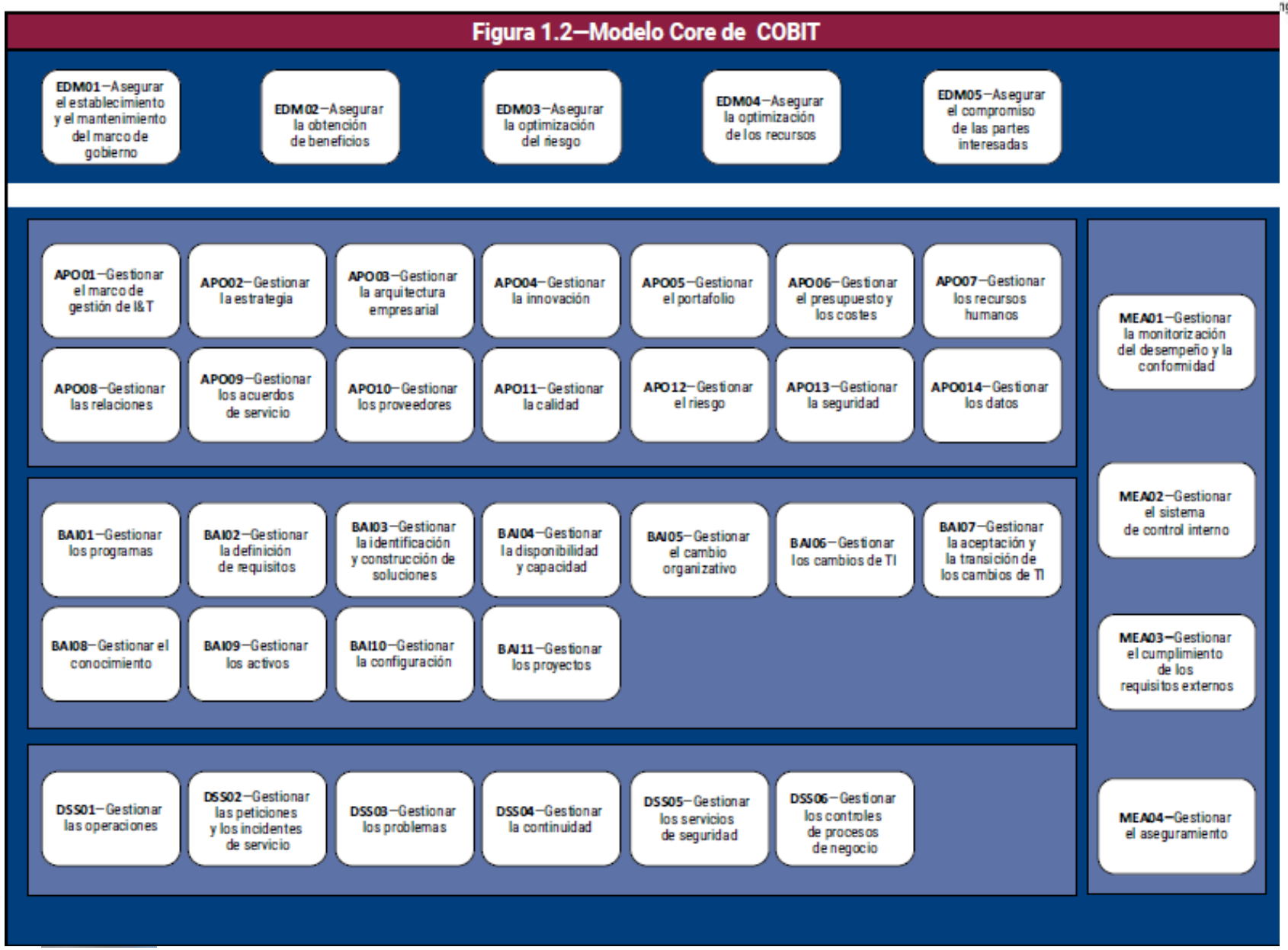
94

Controles generales : Seguridad de la Información

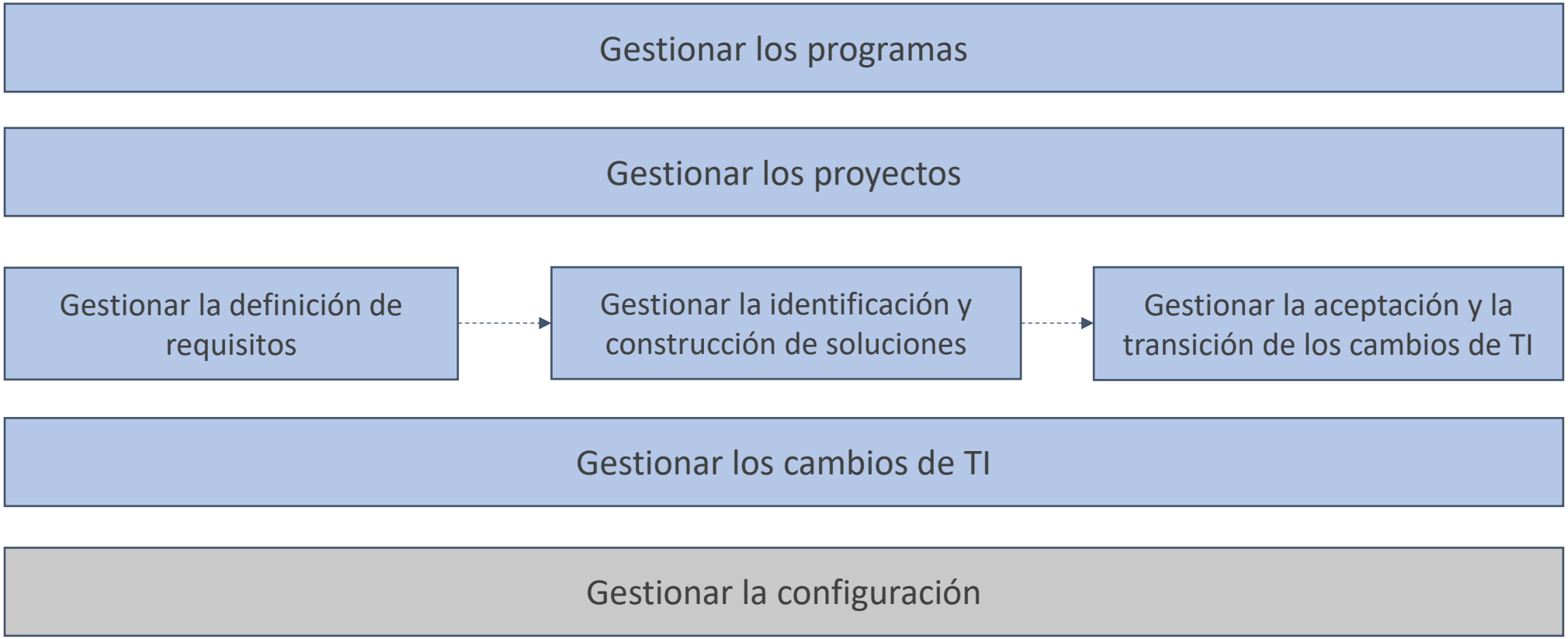
CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los servicios de seguridad **Descripción** Proteger la información de la empresa para mantener el nivel de riesgo de la seguridad de la información aceptable para la empresa, conforme con la política de seguridad. Establecer y mantener roles y privilegios de acceso de seguridad de la información. Realizar una monitorización de la seguridad. **Propósito** Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad de la información **Metas de alineamiento** • Gestión de riesgo relacionado con I&T • Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad	6. Gestionar documentos sensibles y dispositivos de salida 7. Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad	Establecer protecciones físicas apropiadas, prácticas contables y gestión de inventario relativa a activos sensibles de I&T, como formas especiales, instrumentos negociables, impresoras para fines especiales o tokens de seguridad Mediante el uso de un portafolio de herramientas y tecnologías (p.ej. herramientas de detección de intrusión), gestionar las vulnerabilidades y monitorizar la infraestructura para detectar accesos no autorizados. Asegurar que las herramientas, tecnologías y detección de seguridad están integradas en la monitorización general de eventos y la gestión de incidentes

Controles generales : Seguridad de la Información

Seguridad de la Información



Controles generales : Construcción



Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los programas **Descripción** Gestionar todos los programas del portafolio de inversión, de conformidad con la estrategia de la empresa y de forma coordinada, según un enfoque de gestión de programas estándar. Iniciar, planificar, controlar y ejecutar programas, y monitorizar el valor esperado del programa	1. Mantener un enfoque estándar en la gestión de programas	Mantener un enfoque estándar para la gestión de programas que permita la revisión del gobierno y la gestión, la toma de decisiones y las actividades de gestión de la entrega. Estas actividades deben centrarse de consistentemente en el valor y los objetivos de la empresa (es decir, los requisitos, riesgo, costes, calendario y objetivos de calidad).
Propósito Obtener el valor de negocio deseado y reducir el riesgo de retrasos, costes y erosión de valor inesperados. Para ello, mejorar las comunicaciones y la participación del negocio y usuarios finales, garantizar el valor y la calidad de los entregables del programa y realizar un seguimiento de los proyectos dentro de los programas, y maximizar la contribución del programa al portafolio de inversiones	2. Iniciar un programa.	Iniciar un programa para confirmar los beneficios esperados y obtener autorización para proceder. Esto incluye acordar el patrocinio, confirmar el mandato del programa mediante la aprobación del caso de negocio conceptual, asignar un equipo de dirección o un comité , cuyas tareas sean elaborar un resumen del programa, revisar y actualizar el caso de negocio, desarrollar un plan de consecución de beneficios y obtener la aprobación de los patrocinadores antes de proceder
	3. Gestionar el compromiso de las partes interesadas	Gestionar el compromiso de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna para todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas
Metas de alineamiento • Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T • Ejecución de programas dentro de plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad	4. Desarrollar y mantener el plan del programa.	Formular un programa para sentar las bases iniciales. Posicionarlo para la ejecución exitosa mediante la formalización del alcance del trabajo y la identificación de los entregables que satisfarán las metas y producirán valor. Mantener y actualizar el plan del programa y el caso de negocio durante todo el ciclo de vida económico completo del mismo, para asegurar su alineación con los objetivos estratégicos, reflejar el estado actual y el conocimiento adquirido hasta la fecha

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los programas		
Descripción Gestionar todos los programas del portafolio de inversión, de conformidad con la estrategia de la empresa y de forma coordinada, según un enfoque de gestión de programas estándar. Iniciar, planificar, controlar y ejecutar programas, y monitorizar el valor esperado del programa	5. Lanzar y ejecutar el programa	Poner en marcha el programa para adquirir y dirigir los recursos necesarios y así lograr las metas y beneficios del programa tal y como está definido en el plan. De acuerdo con los criterios de revisión de cambios de fase (stage-gate) o publicación, prepararse para la iteración de cambio de fase o revisiones de la publicación a fin de informar sobre el avance y tener el caso para financiar hasta la siguiente revisión de cambio de fase o publicación
Propósito Obtener el valor de negocio deseado y reducir el riesgo de retrasos, costes y erosión de valor inesperados. Para ello, mejorar las comunicaciones y la participación del negocio y usuarios finales, garantizar el valor y la calidad de los entregables del programa y realizar un seguimiento de los proyectos dentro de los programas, y maximizar la contribución del programa al portafolio de inversiones	6. Monitorizar, controlar y reportar sobre los resultados del programa	Monitorizar y controlar el rendimiento en comparación con el plan durante todo el ciclo de vida económico de la inversión, cubriendo la entrega de soluciones a nivel del programa y el valor/resultado a nivel de la empresa. Reportar el rendimiento al comité de dirección del programa y a los patrocinadores
	7. Gestionar la calidad del programa.	Preparar y ejecutar un plan de gestión de la calidad, procesos y prácticas, alineado con el sistema de gestión de calidad (SGC). Describe el enfoque de calidad hacia el programa y cómo se implementará. Todas las partes afectadas deberían revisar y aceptar formalmente el plan e incorporarlo al plan de programa integrado
Metas de alineamiento • Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T • Ejecución de programas dentro de plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad	8. Gestionar el riesgo del programa	Eliminar o minimizar el riesgo específico asociado a los programas mediante un proceso sistemático de planificación, identificación, análisis, respuesta, monitorización y control de las áreas o eventos que, potencialmente, pueden ocasionar un cambio no deseado. Definir y registrar cualquier riesgo al que se enfrenta la gestión del programa
	9. Cerrar un programa	Retirar el programa del portafolio de inversiones activas cuando exista el acuerdo de que se ha alcanzado el valor deseado o cuando esté claro que no se alcanzará dentro de los criterios de valor establecidos para el programa

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los proyectos **Descripción** Gestionar todos los proyectos que se inician en la empresa, alineados con la estrategia de la empresa y de forma coordinada, con base en una estrategia de gestión de proyectos estándar. Iniciar, planificar, controlar y ejecutar proyectos, y concluir con una revisión post-implementación **Propósito** Lograr los resultados definidos en el proyecto y reducir el riesgo de retrasos inesperados, costes y erosión del valor mediante la mejora de las comunicaciones y la participación del negocio y de los usuarios finales. Garantizar el valor y la calidad de los entregables del proyecto y maximizar su contribución a los programas definidos y al portafolio de inversiones **Metas de alineamiento** • Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T • Agilidad para convertir los requisitos del negocio en soluciones operativas • Ejecución de programas dentro del plazo, sin exceder el presupuesto y que cumplan con los requisitos y estándares de calidad	1. Mantener un enfoque estándar en la gestión de proyectos	Mantener una estrategia estándar para la gestión de proyectos que permita la revisión del gobierno y gestión, la toma de decisiones y las actividades de gestión de entrega. Estas actividades deberían centrarse consistentemente en el valor y los objetivos del negocio (es decir, los requisitos, riesgo, costes, calendario y objetivos de calidad).
	2. Establecer e iniciar un proyecto.	Definir y documentar la naturaleza y alcance del proyecto con el objetivo de confirmar y desarrollar un entendimiento común del alcance del proyecto entre las partes interesadas. Los patrocinadores del proyecto deben aprobar formalmente la definición
	3. Gestionar la participación de las partes interesadas	Gestionar la participación de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna que llegue a todas las partes interesadas relevantes. Esto incluye planificar, identificar e involucrar a las partes interesadas y gestionar sus expectativas
	4. Desarrollar y mantener el plan del proyecto	Establecer y mantener un plan de proyecto formal, integrado y aprobado (que cubra los recursos del negocio y de TI) para guiar la ejecución y el control del proyecto durante su ciclo de vida. El alcance de los proyectos debe definirse claramente y vincularse al desarrollo o mejora de las capacidades del negocio
	5. Gestionar la calidad del proyecto	Preparar y ejecutar un plan de gestión de la calidad, procesos y prácticas, alineadas con el sistema de gestión de calidad (SGC). Describir el enfoque de calidad del proyecto y cómo se implementará. El plan debería evaluarse y aceptarse formalmente por todas las partes afectadas e incorporarse al plan integrado del proyecto

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los proyectos **Descripción** Gestionar todos los proyectos que se inician en la empresa, alineados con la estrategia de la empresa y de forma coordinada, con base en una estrategia de gestión de proyectos estándar. Iniciar, planificar, controlar y ejecutar proyectos, y concluir con una revisión post-implementación **Propósito** Lograr los resultados definidos en el proyecto y reducir el riesgo de retrasos inesperados, costes y erosión del valor mediante la mejora de las comunicaciones y la participación del negocio y de los usuarios finales. Garantizar el valor y la calidad de los entregables del proyecto y maximizar su contribución a los programas definidos y al portafolio de inversiones **Metas de alineamiento** • Beneficios obtenidos del portafolio de inversiones y servicios relacionados con I&T • Agilidad para convertir los requisitos del negocio en soluciones operativas • Ejecución de programas dentro del plazo, sin exceder el presupuesto y que cumplan con los requisitos y estándares de calidad	6. Gestionar el riesgo del proyecto	Eliminar o minimizar el riesgo específico asociado a los proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, monitorización y control de las áreas o eventos que, potencialmente, pueden ocasionar un cambio no deseado. Definir y registrar cualquier riesgo al que se enfrenta la gestión del proyecto
	7. Supervisar y controlar los proyectos	Medir el rendimiento del proyecto en comparación con los criterios clave, como son el calendario, la calidad, los costes y el riesgo. Identificar cualquier desviación de los objetivos esperados. Evaluar el impacto de las desviaciones en el proyecto y en el programa general e informar los resultados a las partes interesadas
	8. Gestionar los recursos del proyecto y los paquetes de trabajo	Gestionar los paquetes de trabajos asociados al proyecto mediante el establecimiento de requisitos formales para autorizarlos y aceptarlos y, asignar y coordinar los recursos de negocio y de TI apropiados
	9. Cerrar un proyecto o iteración	Al final de cada proyecto, liberación o iteración, requerir a las partes interesadas del proyecto para que determinen si el mismo ha dado los resultados previstos en cuanto a las capacidades y ha contribuido como se esperaba a los beneficios del programa. Identificar y comunicar las actividades pendientes necesarias para lograr los resultados planeados del proyecto y/o los beneficios del programa. Identificar y documentar las lecciones aprendidas para futuros proyectos, liberaciones iteraciones y programas

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la definición de requisitos **Descripción** Identificar las soluciones y analizar los requisitos antes de su adquisición o construcción para asegurarse de que se ajustan a los requisitos estratégicos de la empresa cubriendo los procesos , aplicaciones, información/datos, infraestructura y servicios del negocio Coordinar la revisión de opciones viables con las partes interesadas afectadas, incluidos costes y beneficios relativos, análisis de riesgos y aprobación de los requisitos y soluciones propuestas **Propósito** Crear soluciones óptimas que satisfagan las necesidades de la empresa mientras que se minimiza el riesgo **Metas de alineamiento** • Prestación de servicios I&T alineados con los requisitos del negocio • Agilidad para convertir los requisitos del negocio en soluciones operativas • Ejecución de programas dentro del plazo, sin exceder el presupuesto y cumpliendo con los requisitos y estándares de calidad	1. Definir y mantener los requisitos funcionales y técnicos del negocio	Con base en el caso de negocio, identificar, priorizar, especificar y acordar los requisitos de información , funcionales, técnicos y de control del negocio que cubran el alcance/comprensión de todas las iniciativas necesarias para lograr los resultados esperados de la solución empresarial propuesta habilitada por la I&T.
	2. Realizar un estudio de factibilidad y formular soluciones alternativas	Realizar un estudio de factibilidad de las posibles soluciones alternativas, evaluar su viabilidad y seleccionar la opción preferida. Si es apropiado, implementar la opción seleccionada como un piloto para determinar posibles mejoras
	3. Gestionar el riesgo de los requisitos	Identificar, documentar, priorizar y mitigar el riesgo funcional, técnico y de procesamiento de la información asociado con los requisitos empresariales, las hipótesis y la solución propuesta
	4. Obtener la aprobación de requisitos y soluciones	Coordinar la retroalimentación de las partes interesadas afectadas En etapas clave predeterminadas, obtener la aprobación y autorización del patrocinador del negocio o del dueño del producto para los requisitos funcionales y técnicos, estudios de factibilidad, análisis de riesgos y soluciones recomendadas

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la identificación y construcción de soluciones **Descripción** Establecer y mantener productos y servicios identificados (tecnología, procesos de negocio y flujos de trabajo) alineados con los requisitos de la empresa que cubran el diseño, desarrollo, adquisición/subcontratación y la asociación con proveedores. Gestionar la configuración, preparación de pruebas, pruebas, gestión de requisitos y mantenimiento de procesos de negocio, aplicaciones, información/datos, infraestructura y servicios **Propósito** Garantizar una prestación ágil y escalable de productos y servicios digitales. Establecer soluciones oportunas y rentables (tecnología, procesos de negocio y flujos de trabajo) capaces de apoyar los objetivos estratégicos y operativos de la empresa. **Metas de alineamiento** • Prestación de servicios de I&T en línea con los requisitos del negocio • Agilidad para convertir los requisitos del negocio en soluciones operativas • Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad	1. Diseño de soluciones de alto nivel	Desarrollar y documentar diseños de alto nivel para la solución en términos de tecnología, procesos de negocio y flujos de trabajo. Usar técnicas de desarrollo por fases o Agile rápido acordadas y apropiadas. Asegurar la alineación con la estrategia de I&T y la arquitectura empresarial. Volver a evaluar y actualizar los diseños cuando se presenten problemas significativos durante las fases de diseño detallado o construcción, o según evolucione la solución. Aplicar un enfoque centrado en el usuario; asegurarse de que las partes interesadas participan activamente en el diseño y la aprobación de cada versión
	2. Diseñar componentes detallados para la solución	Desarrollar, documentar y elaborar diseños detallados de forma progresiva. Usar técnicas de desarrollo Agile por fases o rápido acordadas y apropiadas, abordando todos los componentes (procesos de negocio y controles automatizados y manuales relacionados, aplicaciones soportadas por I&T, servicios de infraestructura y productos de tecnología, así como a los socios/ proveedores). Asegurarse de que el diseño detallado incluya acuerdos de nivel de servicio (SLA) internos y externos, así como acuerdos de nivel operativo (OLA).
	3. Desarrollar los componentes de la solución	Desarrollar progresivamente los componentes de la solución en un entorno independiente, de acuerdo con los diseños detallados siguiendo estándares y requisitos de desarrollo y documentación, de aseguramiento de la calidad (QA) y de aprobación. Asegurarse de que se abordan todos los requisitos de control en los procesos de negocio, las aplicaciones y los servicios de infraestructura soportadas por I&T, servicios y productos de tecnología, y los servicios de socios/proveedores

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la identificación y construcción de soluciones **Descripción** Establecer y mantener productos y servicios identificados (tecnología, procesos de negocio y flujos de trabajo) alineados con los requisitos de la empresa que cubran el diseño, desarrollo, adquisición/subcontratación y la asociación con proveedores. Gestionar la configuración, preparación de pruebas, pruebas, gestión de requisitos y mantenimiento de procesos de negocio, aplicaciones, información/datos, infraestructura y servicios **Propósito** Garantizar una prestación ágil y escalable de productos y servicios digitales. Establecer soluciones oportunas y rentables (tecnología, procesos de negocio y flujos de trabajo) capaces de apoyar los objetivos estratégicos y operativos de la empresa. **Metas de alineamiento** • Prestación de servicios de I&T en línea con los requisitos del negocio • Agilidad para convertir los requisitos del negocio en soluciones operativas • Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad	4. Adquirir los componentes de la solución	Adquirir los componentes de la solución basados en el plan de adquisiciones, de acuerdo con los requisitos y diseños detallados, los principios y estándares de arquitectura, y los procedimientos generales de adquisición y contratos de la compañía, requisitos de QA y estándares de aprobación. Asegurarse de que el proveedor identifica y aborda todos los requisitos legales y contractuales
	5. Construir soluciones	Instalar y configurar soluciones e integrarlas con las actividades del proceso de negocio. Durante la configuración e integración del hardware y el software de infraestructura, implementar medidas de control, seguridad, privacidad y auditabilidad para proteger los recursos y asegurar la disponibilidad y la integridad de los datos. Actualizar el catálogo de productos o servicios para reflejar las nuevas soluciones
	6. Realizar el aseguramiento de calidad (QA).	Desarrollar, aprovisionar y ejecutar un plan de aseguramiento de la calidad (QA) que esté alineado con el sistema de gestión de la calidad (QMS) para obtener la calidad especificada en la definición de los requisitos y en las políticas y procedimientos de calidad de la empresa
	7. Preparar las pruebas de la solución	Establecer un plan de pruebas y los entornos/ambientes necesarios para probar los componentes individuales e integrados de la solución. Incluir los procesos de negocio y los servicios de soporte, aplicaciones e infraestructura.
	8. Ejecutar las pruebas de la solución	Durante el desarrollo, ejecutar pruebas continuamente (incluidas pruebas de control), de acuerdo con el plan de pruebas definido y las prácticas de desarrollo en el entorno apropiado. Incluir a los dueños de los procesos de negocio y a los usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores y problemas que se identificaron durante las pruebas

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la identificación y construcción de soluciones **Descripción** Establecer y mantener productos y servicios identificados (tecnología, procesos de negocio y flujos de trabajo) alineados con los requisitos de la empresa que cubran el diseño, desarrollo, adquisición/subcontratación y la asociación con proveedores. Gestionar la configuración, preparación de pruebas, pruebas, gestión de requisitos y mantenimiento de procesos de negocio, aplicaciones, información/datos, infraestructura y servicios **Propósito** Garantizar una prestación ágil y escalable de productos y servicios digitales. Establecer soluciones oportunas y rentables (tecnología, procesos de negocio y flujos de trabajo) capaces de apoyar los objetivos estratégicos y operativos de la empresa. **Metas de alineamiento** • Prestación de servicios de I&T en línea con los requisitos del negocio • Agilidad para convertir los requisitos del negocio en soluciones operativas • Ejecución de programas dentro del plazo, sin exceder el presupuesto, y que cumplan con los requisitos y estándares de calidad	9. Gestionar los cambios a los requisitos	Hacer seguimiento al estado de requisitos individuales (incluidos todos los requisitos rechazados) durante el ciclo de vida del proyecto. Gestionar la aprobación de cambios a los requisitos
	10. Mantener las soluciones	Desarrollar y ejecutar un plan para mantener los componentes de la solución y la infraestructura. Incluir revisiones periódicas frente a las necesidades del negocio y los requisitos operativos
	11. Definir productos y servicios de TI y mantener el portafolio de servicios	Definir y acordar opciones nuevas o modificadas de productos o servicios de TI y del nivel de servicio. Documentar las definiciones de productos y servicios nuevas o modificadas y las opciones de nivel de servicio que se actualizarán en el portafolio de productos y servicios.
	12. Diseñar soluciones conforme a la metodología de desarrollo definida.	Diseñar, desarrollar e implementar soluciones con la metodología de desarrollo adecuada (es decir, en cascada, Agile o bimodal I&T), conforme a la estrategia y requisitos globales.

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la aceptación y la transición de los cambios de TI		
Descripción Aceptar formalmente y hacer operativas las nuevas soluciones. Incluir la planificación de la implementación, conversión de sistemas y datos, pruebas de aceptación, comunicación, preparación de la puesta en producción, paso a producción de nuevos o modificados procesos de negocio y servicios de I&T, soporte temprano de la producción y revisión posterior a la implementación	1. Establecer un plan de implementación	Establecer un plan de implementación que cubra la conversión de sistemas y datos, criterios de pruebas de aceptación, comunicación, formación, preparación de puestas en producción, paso a producción, soporte temprano en producción, plan de fallback/backup y revisión posterior a la implementación. Obtener la aprobación de las partes interesadas
	2. Planificar la conversión de procesos de negocio, sistemas y datos	Prepararse para la migración de los procesos de negocio, datos de servicios e infraestructura de I&T como parte de los métodos de desarrollo de la empresa. Incluir pistas de auditoría y un plan de recuperación si la migración falla
Propósito Implementar soluciones de forma segura y conforme a las expectativas y resultados acordados	3. Plan de pruebas de aceptación	Establecer un plan de pruebas basado en estándares de toda la empresa que defina roles, responsabilidades y criterios de entrada y salida. Asegurarse de que las partes interesadas aprueben el plan
Metas de alineamiento • Agilidad para convertir los requisitos del negocio en soluciones operativas	4. Establecer un entorno de pruebas	Definir y establecer un entorno de pruebas seguro y representativo del proceso de negocio planificado y del entorno de operaciones de TI, en cuanto a rendimiento, capacidad, seguridad, controles internos, prácticas operativas, calidad de los datos, requisitos de privacidad y cargas de trabajo

Controles generales : Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la aceptación y la transición de los cambios de TI **Descripción** Aceptar formalmente y hacer operativas las nuevas soluciones. Incluir la planificación de la implementación, conversión de sistemas y datos, pruebas de aceptación, comunicación, preparación de la puesta en producción, paso a producción de nuevos o modificados procesos de negocio y servicios de I&T, soporte temprano de la producción y revisión posterior a la implementación	5. Realizar pruebas de aceptación	Probar los cambios de forma independiente de acuerdo con el plan de pruebas definido antes de la migración al entorno operativo en producción
Propósito Implementar soluciones de forma segura y conforme a las expectativas y resultados acordados	6. Promover a producción y gestionar las liberaciones (releases)	Promover la solución aceptada al negocio y a las operaciones. Cuando sea apropiado, ejecutar la solución como una implementación piloto o en paralelo con la solución antigua durante un período definido y comparar el comportamiento y los resultados. Si se producen problemas significativos, volver al entorno original usando el plan de fallback/backup. Gestionar las liberaciones de los componentes de la solución
Metas de alineamiento • Agilidad para convertir los requisitos del negocio en soluciones operativas	7. Proporcionar soporte oportuno en producción	Proporcionar, durante un periodo de tiempo acordado, soporte oportuno a los usuarios y a las operaciones de I&T para resolver problemas y ayudar a estabilizar la nueva solución
	8. Realizar una revisión post-implementación.	Realizar una revisión post-implementación para confirmar los resultados, identificar las lecciones aprendidas y desarrollar un plan de acción. Evaluar el rendimiento y los resultados reales del servicio nuevo o modificado, en comparación con el rendimiento y resultados previstos por el usuario o cliente

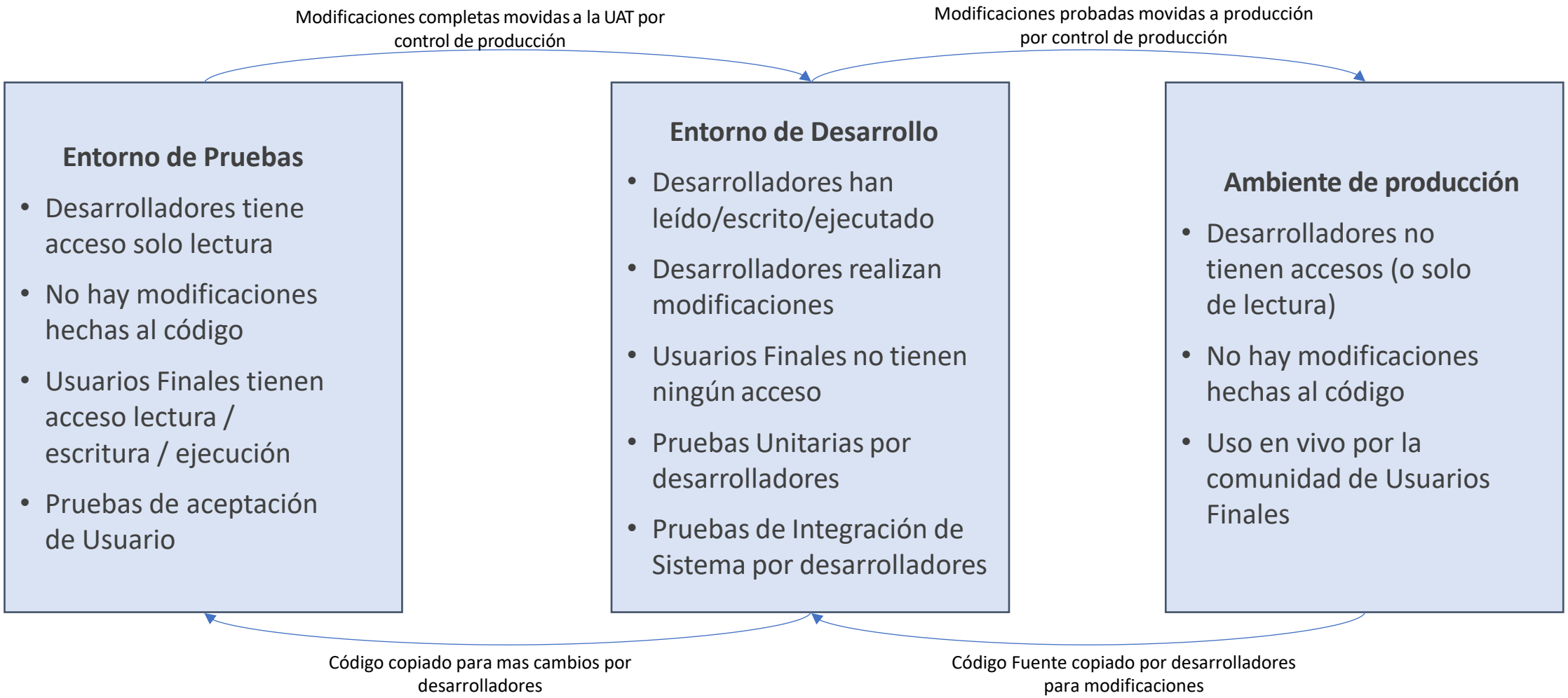
Separación de funciones

	Desarrollo	Producción	Pruebas
Usuario Final	Sin acceso	Leer / escribir / ejecutar	Leer / escribir / ejecutar
Desarrollador de Aplicaciones	Leer / escribir / ejecutar	Leer	Leer
Control de Producción / bibliotecario	Varía	Escribir	Escribir

Controles generales: Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los cambios de TI **Descripción** Gestionar todos los cambios de una manera controlada, incluidos los cambios estándar y los mantenimientos de emergencia en relación con los procesos de negocio, las aplicaciones y la infraestructura. Esto incluye estándares y procedimientos de cambio, evaluación del impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación **Propósito** Facilitar una ejecución de cambios rápida y confiable para el negocio. Mitigar el riesgo de afectar negativamente la estabilidad o integridad del entorno que se ha modificado **Metas de alineamiento** • Agilidad para convertir los requisitos del negocio en soluciones operativas	1. Evaluar, priorizar y autorizar solicitudes de cambio.	Evaluar todas las solicitudes de cambio para determinar el impacto en los procesos de negocio y servicios de I&T; y evaluar si el cambio afectará negativamente al entorno operativo e introducirá riesgos inaceptables. Asegurarse de que los cambios se registran, priorizan, clasifican, evalúan, autorizan, planifican y programan
	2. Gestionar cambios de emergencia	Gestionar cuidadosamente los cambios de emergencia para minimizar futuros incidentes. Asegurar que el cambio de emergencia está controlado y se realiza de forma segura. Verificar que los cambios de emergencia se evalúan adecuadamente y se autorizan después del cambio
	3. Hacer seguimiento e informar sobre cambios de estado	Mantener un sistema de seguimiento e informes para documentar los cambios rechazados y comunicar el estado de los cambios aprobados, en proceso y finalizados. Asegurarse de que los cambios aprobados se implementan según lo previsto.
	4. Cerrar y documentar los cambios	Siempre que se implementen cambios, actualizar la solución, la documentación del usuario y los procedimientos afectados por el cambio

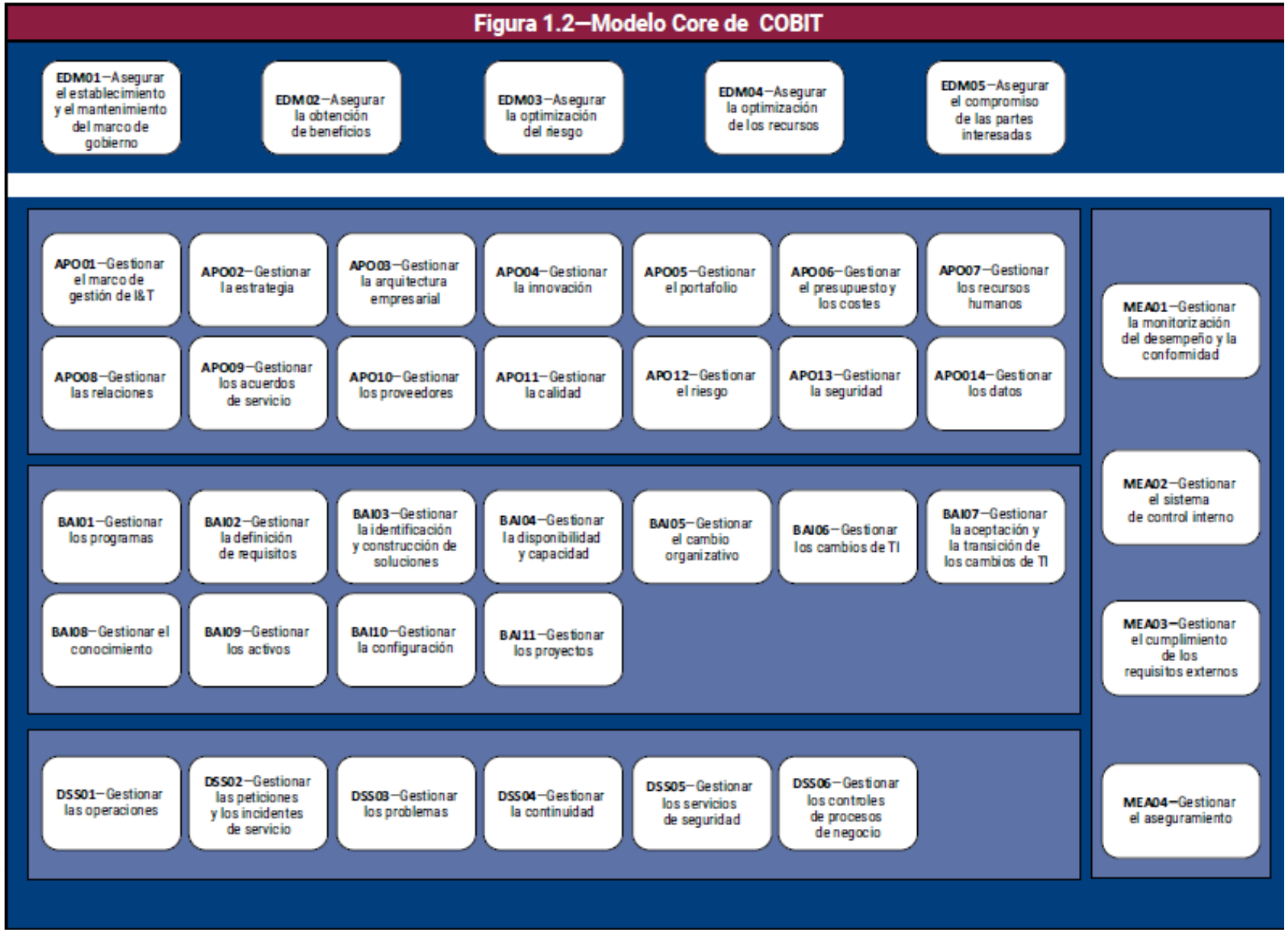
Proceso de control de cambios



Controles generales: Construcción

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la configuración **Descripción** Definir y mantener descripciones y relaciones entre recursos claves y las capacidades necesarias para ofrecer servicios habilitados por I&T. Incluir la recopilación de información sobre la configuración, estableciendo líneas de referencia, verificando y auditando esta información, y actualizando el repositorio de configuración	1. Establecer y mantener un modelo de configuración	Establecer y mantener un modelo lógico de servicios, activos, infraestructura, y registro de los elementos de configuración (CI), incluyendo las relaciones entre estos. Incluir los CIs que se consideran necesarios para gestionar los servicios eficazmente y, proporcionar una única descripción confiable de los activos en un servicio.
	2. Establecer y mantener un repositorio de configuración y una línea de referencia.	Establecer y mantener un repositorio de gestión de la configuración y crear líneas de referencias de configuración controladas
Propósito Proporcionar información suficiente sobre los activos de servicio para facilitar que el servicio se gestione de forma eficiente. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio	3. Mantener y controlar los elementos de configuración	Mantener un repositorio actualizado de los elementos de configuración (CIs) incluyendo cualquier cambio en la configuración
	4. Generar informes de estado y de la configuración	Definir y generar informes de la configuración sobre los cambios de estado en los elementos de la configuración
Metas de alineamiento • Seguridad de la información, infraestructura de procesamiento, aplicaciones y, privacidad	5. Verificar y revisar la integridad del repositorio de configuración	Revisar periódicamente el repositorio de configuración y verificar su integridad y precisión en comparación con la meta deseada

Controles generales: Operaciones



Controles generales: Operaciones

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar las operaciones **Descripción** Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar los servicios de I&T, internos y externalizados. Incluir la ejecución de procedimientos de operación estándar predefinidos y las actividades de supervisión requeridas	1. Ejecutar procedimientos operativos	Mantener y ejecutar procedimientos y tareas operativas de manera confiable y consistente
	2. Gestionar servicios tercerizados de I&T.	Gestionar la operación de los servicios tercerizados de I&T para mantener la protección de la información empresarial y la confiabilidad de la provisión del servicio
Propósito Proporcionar los resultados de los productos y servicios operativos de I&T según lo planeado	3. Monitorizar la infraestructura de I&T.	Monitorizar la infraestructura de I&T y eventos relacionados. Almacenar suficiente información cronológica en los logs de operación que permita la reconstrucción y revisión de las secuencias temporales de las operaciones y otras actividades asociadas o que apoyan las operaciones
	4. Gestionar el medioambiente	Mantener medidas de protección contra los factores medioambientales. Instalar equipos y dispositivos especializados para monitorizar y controlar el ambiente
Metas de alineamiento • Prestación de servicios de I&T conforme a los requisitos del negocio	5. Gestionar las instalaciones	Gestionar las instalaciones, incluidos los equipos de suministro eléctrico y comunicaciones, alineados con las leyes y reglamentos existentes, los requisitos técnicos y del negocio, las especificaciones del proveedor, y las directrices de salud y seguridad

Procesamiento de datos

Procesamiento por lotes (batch)	Procesamiento en línea
• Se caracteriza por múltiples actualizaciones a los datos de la empresa, procesados a la vez, generalmente durante la noche. La finalización exitosa del proceso de la noche es fundamental para el inicio de la jornada de los procesos de negocio.	• Se caracteriza por las actualizaciones de los datos de la empresa transacción por transacción, por regla general, inmediatamente o en "tiempo real." La constante disponibilidad del ambiente es fundamental para los procesos de negocio que soporta.

Ambos tienen riesgos y controles únicos; de haber escasos controles, podría afectar la disponibilidad de los sistemas y la integridad de la información

Controles generales: Operaciones

CONCEPTOS GENERALES		PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar las peticiones y los incidentes de servicio	**Descripción** Proporcionar una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todos los tipos de incidentes. Restaurar el servicio normal, registrar y completar las solicitudes de usuario; y registrar, investigar, diagnosticar, escalar y resolver los incidentes	1. Definir esquemas de clasificación para incidentes y peticiones de servicio	Definir esquemas de clasificación y modelos de incidentes y de peticiones de servicio
		2. Registrar, clasificar y priorizar las peticiones e incidentes	Identificar, registrar y clasificar las peticiones de servicio y los incidentes, y asignarles una prioridad de acuerdo con la criticidad para el negocio y los acuerdos de servicio
		3. Verificar, aprobar y resolver peticiones de servicio	Seleccionar los procedimientos apropiados para peticiones y verificar que las solicitudes de servicio cumplan con los criterios de solicitud definidos. Obtener aprobación, si se requiere, y satisfacer las solicitudes
		4. Investigar, diagnosticar y asignar incidentes	Identificar y registrar los síntomas de los incidentes, determinar las causas posibles y asignarlos para su resolución
		5. Resolver y recuperarse de los incidentes	Documentar, aplicar y probar las soluciones definitivas o temporales (workarounds) identificados. Realizar acciones de recuperación para restaurar el servicio relacionado con I&T.
		6. Cerrar las peticiones de servicio y los incidentes	Verificar la solución satisfactoria del incidente y/o el cumplimiento de la petición y su cierre
		7. Hacer seguimiento al estado y producir informes	Hacer seguimiento, analizar e informar regularmente sobre los incidentes y el cumplimiento de las solicitudes. Examinar tendencias para proporcionar información para la mejora continua
	Propósito Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidencias de los usuarios. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio. Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes		
	Metas de alineamiento • Prestación de servicios de I&T en línea con los requisitos del negocio		

Controles generales: Operaciones

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los problemas **Descripción** Identificar y clasificar los problemas y su causa raíz. Ofrecer una solución oportuna para evitar incidentes recurrentes. Ofrecer recomendaciones de mejoras	1. Identificar y clasificar los problemas	Definir e implementar criterios y procedimientos para identificar e informar sobre los problemas. Incluir la clasificación, categorización y priorización del problema
Propósito Aumentar la disponibilidad, mejorar los niveles de servicio, reducir los costes y atender mejor las necesidades del cliente y lograr su satisfacción mediante una reducción del número de problemas operativos, e identificar las causas raíz como parte de la resolución de problemas	2. Investigar y diagnosticar problemas.	Investigar y diagnosticar problemas con la ayuda de expertos en la materia para evaluar y analizar su causa raíz.
	3. Presentar los errores conocidos	Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los errores conocidos, documentar las soluciones temporales apropiadas e identificar las soluciones potenciales
Metas de alineamiento • Prestación de servicios de I&T conforme a los requisitos del negocio	4. Resolver y cerrar los problemas.	Identificar e iniciar soluciones sostenibles dirigidas a la causa raíz del problema. Presentar solicitudes de cambio a través del proceso de gestión de cambio establecido, si es necesario, para resolver los errores. Asegurarse de que el personal afectado conoce las medidas adoptadas y los planes desarrollados para evitar que ocurran incidentes en el futuro
	5. Realizar una gestión proactiva de los problemas	Recopilar y analizar los datos operacionales (especialmente los registros del incidente y los cambios) para identificar las tendencias que están emergiendo que puedan indicar problemas. Guardar los registros de problemas para permitir su evaluación

Controles generales: Operaciones

CONCEPTOS GENERALES		PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar la continuidad	**Descripción** Establecer y mantener un plan que permita a las organizaciones empresariales y a TI responder a los incidentes y adaptarse rápidamente a las interrupciones. Esto permitirá la operación continua de los procesos críticos de negocio y de los servicios de I&T necesarios, y mantener la disponibilidad de recursos, activos e información en un nivel aceptable para la empresa	1. Definir la política de continuidad del negocio, sus objetivos y alcance	Definir la política y alcance de la continuidad del negocio, alineado con los objetivos de la empresa y de las partes interesadas, para mejorar la resiliencia del negocio
	Propósito Adaptarse rápidamente, continuar con las operaciones del negocio y mantener la disponibilidad de los recursos y la información a un nivel aceptable para la empresa en caso de una interrupción significativa (p.ej., amenazas, oportunidades, demandas).	2. Mantener la resiliencia del negocio	Evaluar las opciones de resiliencia del negocio y elegir una estrategia viable y rentable para asegurar la continuidad, la recuperación ante un desastre y la respuesta ante incidentes de la empresa ante un desastre u otro incidente o interrupción mayor
		3. Desarrollar e implementar una respuesta de continuidad del negocio.	Desarrollar un plan de continuidad del negocio (BCP) y un plan de recuperación de desastres (DRP) basados en la estrategia. Documentar todos los procedimientos necesarios para que la empresa continúe con sus actividades críticas en caso de incidente
	Metas de alineamiento • Prestación de servicios de I&T conforme a los requisitos de negocio • Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad	4. Realizar ejercicios, probar y revisar el plan de continuidad del negocio (BCP) y el plan de respuesta ante desastres (DRP).	Probar la continuidad de forma periódica para ver el comportamiento de los planes contra resultados predeterminados, mantener la resiliencia del negocio y permitir que se desarrollen soluciones innovadoras
		5. Revisar, mantener y mejorar los planes de continuidad	Conducir una revisión periódica de la capacidad de continuidad para asegurar su idoneidad, lo adecuado y su efectividad. Gestionar los cambios a los planes de acuerdo con el proceso de control de cambios para asegurar que los planes de continuidad se mantienen actualizados y reflejan continuamente los requisitos actuales del negocio.

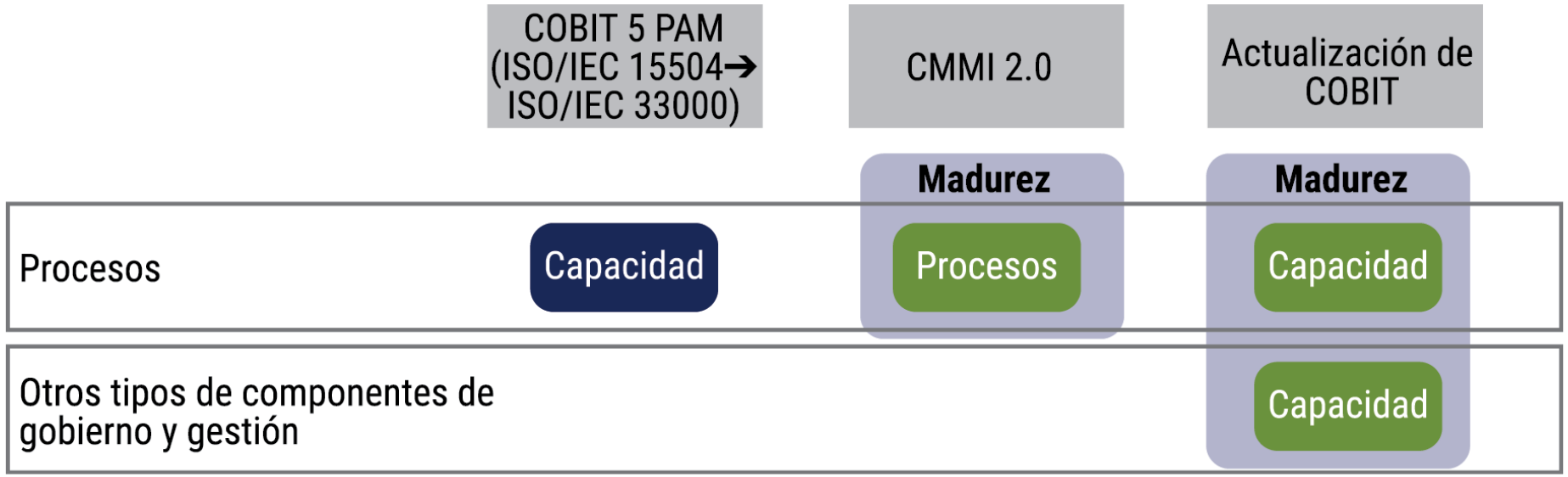
Controles generales: Operaciones

CONCEPTOS GENERALES	PRÁCTICAS	DESCRIPCIÓN DE LAS PRÁCTICAS
Gestionar los proveedores **Descripción** Gestionar los productos y servicios relacionados con I&T proporcionados por todo tipo de proveedores para que satisfagan los requisitos de la empresa. Esto incluye la búsqueda y selección de proveedores, gestión de relaciones, gestión de contratos y revisión y monitorización del rendimiento de proveedores y el ecosistema de proveedores (incluida la cadena ascendente de suministro) para que sea efectiva y cumpla con la legislación **Propósito** Optimizar las capacidades de I&T disponibles para apoyar la estrategia y la hoja de ruta de I&T, minimizar el riesgo asociado con proveedores que no rinden o cumplen con los requisitos y asegurar precios competitivos **Metas de alineamiento** • Prestación de servicios de I&T conforme a los requisitos del negocio	1. Identificar y evaluar los contratos y las relaciones con los proveedores.	Buscar e identificar continuamente proveedores y clasificarlos en tipo, importancia y criticidad. Establecer criterios de evaluación del proveedor y de los contratos. Evaluar el portafolio general de proveedores y contratos vigentes y alternativos
	2. Seleccionar proveedores	Seleccionar proveedores externos de acuerdo con una práctica justa y formal para garantizar la mejor selección basado en los requisitos especificados. Los requisitos deben optimizarse con la participación de los proveedores externos potenciales
	3. Gestionar los contratos y las relaciones con los proveedores.	Formalizar y gestionar la relación con el proveedor para cada uno de los proveedores. Gestionar, mantener y monitorizar los contratos y la prestación de servicios. Asegurar que los contratos nuevos o modificados cumplan con los estándares de la empresa y con los requisitos legales y regulatorios. Tratar las disputas contractuales
	4. Gestionar los riesgos de los proveedores	Identificar y gestionar el riesgo relacionado con los proveedores para proporcionar continuamente una prestación de servicios segura, eficiente y eficaz. Esto también incluye a los subcontratistas o proveedores de nivel superior que son relevantes para la prestación del servicio del proveedor directo
	5. Supervisar el rendimiento y el cumplimiento del proveedor	Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y la ejecución del valor del contrato. Abordar los problemas identificados

CAPÍTULO 4: Proceso de Evaluación y Documentación

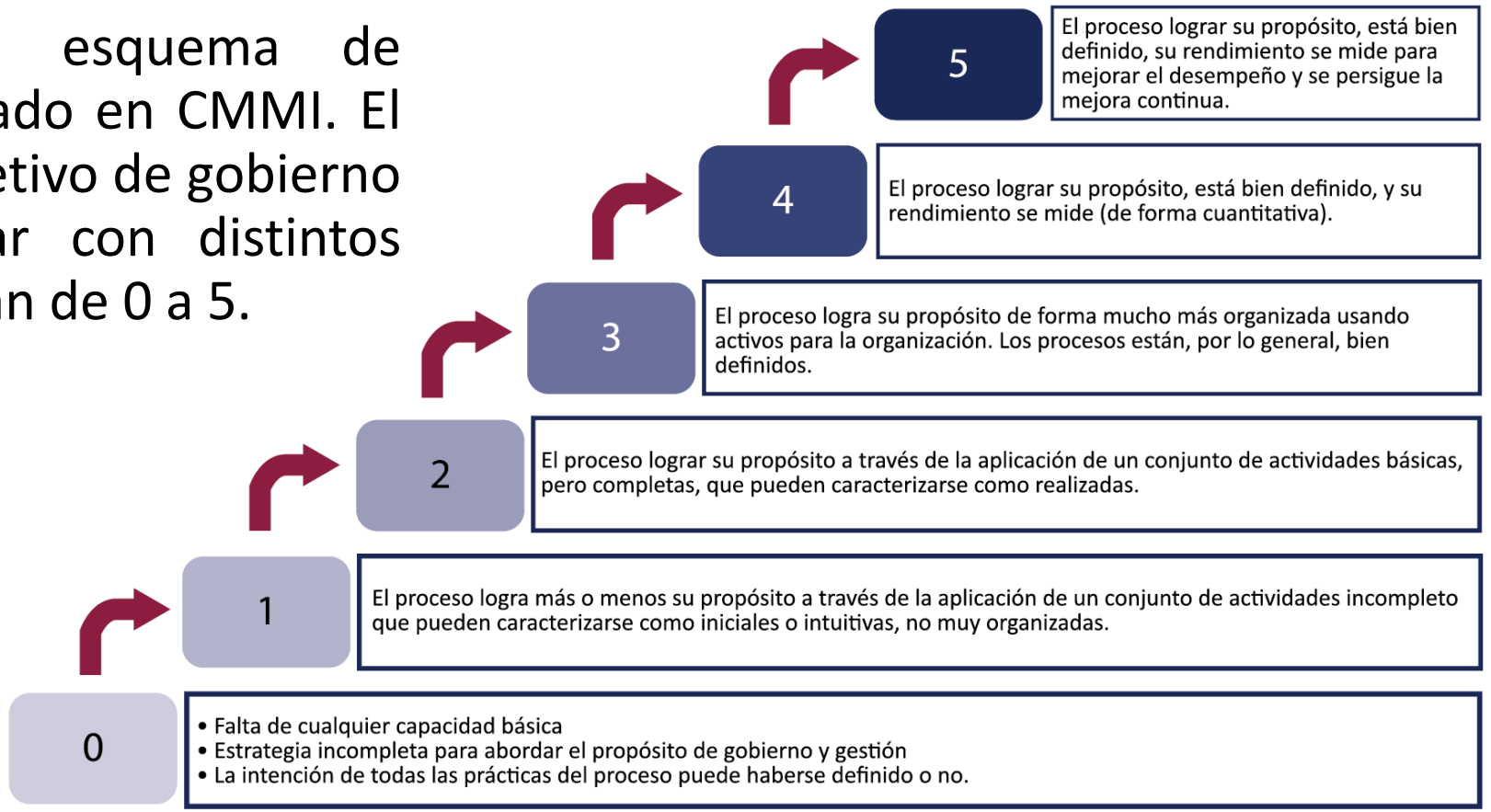
Visión general de la gestión del desempeño de COBIT

Figura 6.1—Niveles de capacidad



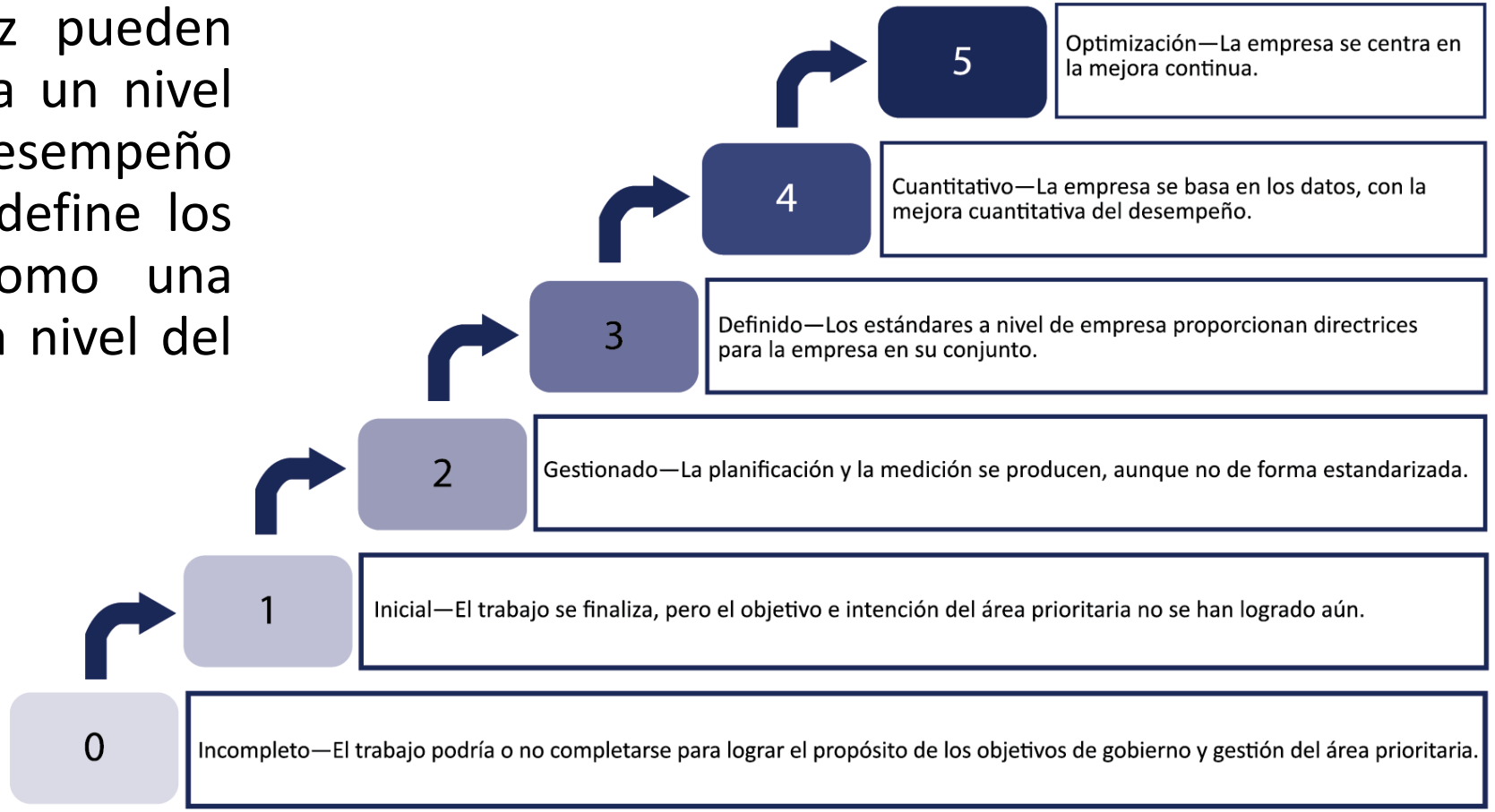
Niveles de capacidad del proceso

- COBIT 2019 admite un esquema de capacidad de procesos basado en CMMI. El proceso dentro de cada objetivo de gobierno y gestión puede funcionar con distintos niveles de capacidad, que van de 0 a 5.



Niveles de madurez del área prioritaria

- Los niveles de madurez pueden usarse cuando se precisa un nivel más alto para el desempeño expresado. COBIT 2019 define los niveles de madurez como una medida de desempeño a nivel del área prioritaria.



Fases del Proceso de Evaluación de Controles

- **1. Planificación:** Definir el Alcance (qué sistemas/procesos se evalúan), Objetivos (qué se busca) y Criterio (contra qué norma).
- **2. Ejecución (Trabajo de Campo):** Recolección de evidencia y pruebas.
- **3. Reporte (Informe):** Documentar y comunicar los hallazgos.
- **4. Seguimiento**: Verificar que los hallazgos se hayan corregido.

Metodología: Evaluación de Diseño (ToD) vs. Operativa (ToE)

1. Evaluación de Diseño (ToD - Test of Design):

¿El control está bien diseñado para mitigar el riesgo? ¿Es adecuado?

Ejemplo: Revisar que la política de passwords exija 12 caracteres (Buen diseño).

2. Evaluación de Efectividad Operativa (ToE - Test of Effectiveness):

¿El control funciona en la práctica consistentemente?

Ejemplo: Probar 30 usuarios al azar para ver si realmente sus passwords tienen 12 caracteres (Prueba de operación).

El Walkthrough (Prueba de Recorrido) para ToD

- Es la técnica principal para probar el Diseño (ToD).
- Seguir una transacción de inicio a fin para confirmar que el control existe y funciona como se documentó.
- **Ejemplo**: Seguir el proceso de "creación de un nuevo usuario" desde la solicitud de RRHH hasta la asignación de permisos en el sistema.

Técnicas para Obtención de Evidencia: Inspección, Entrevista, Re-ejecución

1. Inspección: Revisión de documentos, políticas, logs o configuraciones (ej. "Muéstreme la configuración del firewall").

2. Entrevista: Preguntar al personal cómo realiza el proceso (ej. "¿Cómo aprueba usted un cambio?").

3. Observación: Ver al personal realizar el proceso.

4. Reejecución (Re-performance): El evaluador vuelve a ejecutar el control (ej. "El evaluador recalcula el reporte de ventas").

Herramientas: Cuestionarios CCI, Muestreo y CAATs

- **CCI (Cuestionario de Control Interno):** Checklist de preguntas (Sí/No/N.A.) basado en el criterio (ej. ISO 27002).
- **Muestreo**: Técnica para seleccionar un subconjunto (muestra) para la prueba de Efectividad Operativa (ToE).
- **CAATs (Técnicas de Auditoría Asistidas por Computadora):** Uso de software (ej. Excel, ACL, Python) para analizar grandes volúmenes de datos (ej. analizar 1 millón de logs).

Documentación de la Evaluación: La Regla de los Papeles de Trabajo (PT)

- **Definición:** Los PT son la evidencia del evaluador. Contienen las pruebas, capturas de pantalla, logs y conclusiones.

- **Regla de Oro:** Un Papel de Trabajo debe ser autosuficiente. Un colega debe poder entender qué se hizo, qué se encontró y por qué se concluyó eso, solo leyendo el PT.

Estructura del Informe de Hallazgos: El Modelo de las 4 C's

- Un Hallazgo es una debilidad de control que debe ser reportada.
- Para que un hallazgo sea profesional, debe contener 4 elementos (las 4 C's):
- Condición, Criterio, Causa y Conclusión/Recomendación.

Condición, Criterio, Causa y Recomendación (4 C's Detalladas)

1. Condición: Lo que es (El problema).
Ej: "Se detectó que 5 ex-empleados aún tienen cuentas activas en el sistema."

2. Criterio: Lo que debería ser (La norma o política).
Ej: "La política interna 5.1 de RRHH exige la baja de cuentas el mismo día de la desvinculación."

3. Causa: Por qué pasó (La raíz del problema).
Ej: "Falta de un proceso de notificación formal entre RRHH y TI."

4. Recomendación: La solución (sugerencia de mejora).
Ej: "Implementar un ticket automático de baja de usuario generado por RRHH."

Seguimiento de Hallazgos y Matriz de Plan de Acción

- El trabajo no termina con el informe.
- Matriz de Plan de Acción (Seguimiento): Documento donde la gerencia auditada se compromete a una fecha de remediación para cada hallazgo.
- El evaluador debe realizar un seguimiento (ej. 6 meses después) para verificar que las correcciones se implementaron.

JUAN CARLOS LÓPEZ
jclopez@exacta.com.ec
DIRECTOR GENERAL
+ 593 99 9506 1566
www.exactaconsulting.com.ec
Ec.linkedin.com/in/jclopezexacta/