



ESCUELA SUPERIOR
DE GUERRA

"General Rafael Reyes Prieto"

Colombia

Integrantes

Laura Gutierrez
Carolina Salinas
Fabián Gómez

Cohorte XIX maestría 2025 2

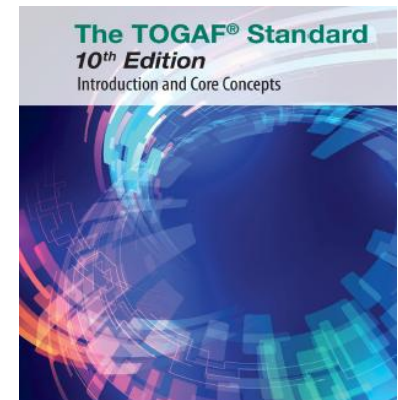
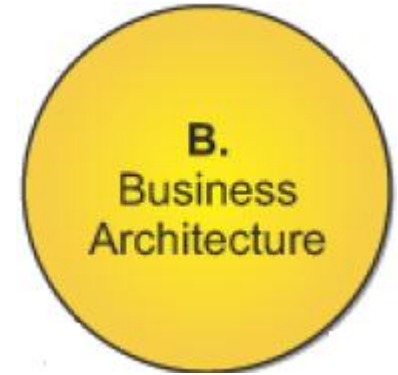
Septiembre 2025

La Fase B: Arquitectura de Negocio

Establecer una visión integral del negocio de la Electrificadora Andina, detallando la **estructura organizativa** (Dirección General, Operaciones, Comercial, TI, Seguridad), los **procesos de negocio críticos** (distribución de energía, facturación, gestión de clientes, mantenimiento y proveedores), los **objetivos estratégicos** (continuidad del servicio, resiliencia, protección de datos y cumplimiento normativo) y las **relaciones entre áreas TI-OT** que soportan la operación.



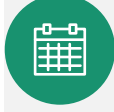

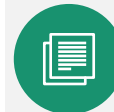
Objetivo principal de la Fase B

- Definir la arquitectura de negocio candidata
- Alinear la arquitectura con la estrategia
- Considerar el valor de negocio
- Identificar los elementos clave del negocio



Actividades FASE B

B.
Business
Architecture

	Desarrollo de la arquitectura de línea de base	Levantamiento del estado actual de procesos de distribución, comercialización y atención al cliente.	Documentar la infraestructura de TI actual (SCADA, medidores manuales, call center).	Identificar brechas en continuidad del servicio y tiempos de respuesta	Analizar fortalezas y debilidades del modelo operativo actual.
	Desarrollo de la arquitectura de negocio de destino	Diseñar procesos de mantenimiento predictivo y monitoreo remoto mediante IoT y Smart Grids.	Definir un modelo omnicanal de atención al cliente (app móvil, chatbot, web).	Planear integración de energía renovable y generación distribuida.	Diseñar un ERP centralizado para gestión administrativa y financiera.
	Considerar el valor del negocio	Evaluar costo-beneficio de implementar medidores inteligentes frente a pérdidas técnicas.	Cuantificar el impacto económico de la reducción de fraudes energéticos	Estimar ahorros operativos derivados de la digitalización de procesos internos.	Medir la mejora en satisfacción de clientes por servicios digitales.
	Identificar factores de éxito	Capacitación técnica del personal en nuevas tecnologías (IoT, ciberseguridad, analítica).	Compromiso directivo para liderar la transformación digital	Colaboración con proveedores estratégicos de tecnología.	Implementación de un programa de gestión del cambio para empleados y clientes.
	Considerar las restricciones	Cumplir con la normativa CREG en calidad del servicio y con ISO 27001 para gestión de seguridad de la información.	El presupuesto para proyectos de ciberseguridad es limitado; se debe justificar con análisis costo-beneficio.	No se pueden detener las operaciones críticas (24/7). Cualquier cambio debe hacerse en ventanas de mantenimiento muy controladas.	Coexistencia de sistemas antiguos SCADA con nuevas soluciones digitales, lo que obliga a crear una arquitectura híbrida.

Resultados de B | Arquitectura del negocio

B. Business Architecture

02

Procesos clave de negocio digitalizados:
facturación automatizada, autoservicio en línea, gestión de reclamos y soporte remoto.



04

Operación crítica: red SCADA fortalecida con monitoreo de ciberseguridad en tiempo real.



01

Modelo organizacional:
integración entre áreas de negocio, TI y OT bajo una gobernanza común de seguridad y operación.



03

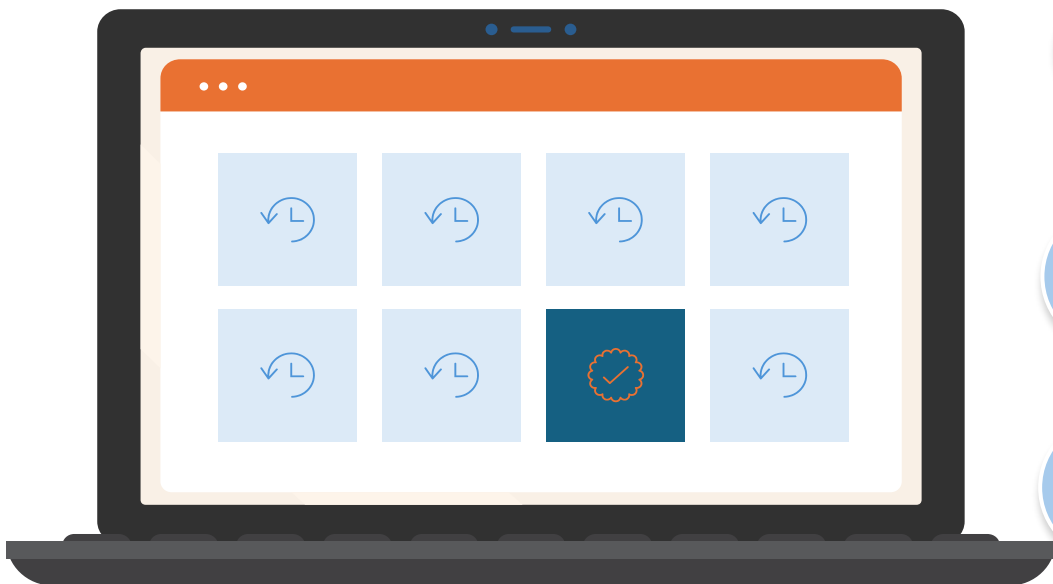
Servicios nuevos:
plataforma digital para que los clientes consulten consumos, reporten fallas y generen pagos electrónicos seguros.



Resultado: un negocio **más ágil, resiliente y alineado con las metas estratégicas** de confiabilidad y continuidad energética.

Definición de las necesidades de negocio

Se identifican claramente las prioridades que deben ser cubiertas



1

Mayor **resiliencia operativa** ante ciberataques y desastres naturales

2

Mejor experiencia del cliente: autoservicio digital, tiempos de respuesta más cortos y comunicación directa de fallas.

3

Cumplimiento regulatorio: reportes automáticos de calidad del servicio exigidos por la CREG.

4

Optimización de costos: reducción de pérdidas técnicas y no técnicas mediante analítica de datos y sistemas inteligentes.

5

Gestión del talento: capacitación de personal en nuevas tecnologías de seguridad industrial y digitalización.

Un entendimiento compartido

Se logra alinear a todos los interesados en torno a la arquitectura:

- La **Gerencia General** entiende que invertir en ciberseguridad y digitalización no es un gasto, sino una protección al negocio.
- El área **operativa** (ingenieros eléctricos) y el área **TI** reconocen la importancia de trabajar juntos en la seguridad de sistemas SCADA.
- Los **proveedores tecnológicos** y aliados estratégicos comparten un modelo de integración para garantizar la interoperabilidad.
- Los **clientes y entes reguladores** perciben transparencia y mejora en la calidad del servicio.



¿Cómo se modelan los procesos de negocio?

Tiene como objetivo representar cómo la organización ejecuta sus operaciones, qué actores intervienen y cómo se alinean los procesos con las metas estratégicas.

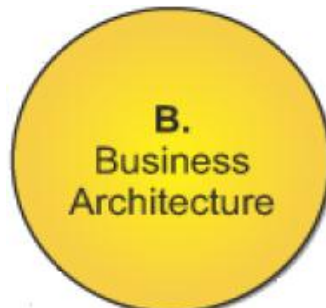
- Mapas jerárquicos para la visión integral de áreas.
- Catálogos de procesos con responsables, objetivos y KPI.
- Diagramas BPMN para detallar flujos críticos como facturación o gestión de fallas.
- Diagramas ArchiMate para conectar procesos con TI-OT, aplicaciones y datos.
- Matrices Actor-Función para clarificar responsabilidades.

¿Cómo se identifican los requisitos de seguridad a nivel de negocio?

Los requisitos de seguridad a nivel de negocio se identifican como parte del diseño de la **Arquitectura de Negocio (Fase B)** y luego se refinan en la **Arquitectura de Sistemas de Información y Tecnología (Fases C y D)**.

Los requisitos de seguridad a nivel de negocio se identifican a partir de:

- Estrategia (continuidad, resiliencia, cumplimiento).
- Procesos críticos (distribución, facturación, clientes, mantenimiento).
- Riesgos y amenazas.
- Dimensiones de seguridad (CIA, continuidad, trazabilidad).
- Documentación en catálogos y matrices TOGAF.







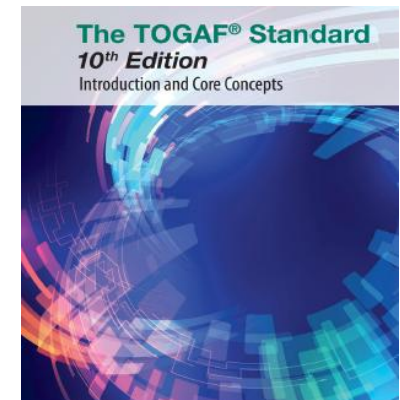
La Fase C: Desarrollar la Arquitectura de la Información

Se centra en el desarrollo de las arquitecturas de sistemas de información objetivo, es decir, la arquitectura de datos y la arquitectura de aplicaciones, identificando los componentes de la hoja de ruta de arquitectura basándose en las diferencias con la arquitectura de línea base. Esta fase es crucial para definir el estado futuro de las arquitecturas de datos y aplicaciones, y su interacción con el resto de dominios, asegurando que la arquitectura de negocio se mantenga coherente y alineada con las necesidades del negocio.



Objetivo principal de la Fase C

-  Desarrollar la Arquitectura de Datos
-  Desarrollar la Arquitectura de Aplicaciones
-  Identificar la Hoja de Ruta
-  Asegurar la Coherencia con la Arquitectura de Negocio



Fase C



ARQUITECTURA DE LOS SISTEMAS DE INFORMACIÓN



Arquitectura de datos

Objetivo: Definir el modelo de datos objetivo que permita soportar los procesos críticos de negocio y la integración con aplicaciones.

- Diseñar un **modelo lógico y físico de datos** que integre información de clientes, facturación, consumo energético, activos de red y SCADA.
- Implementar un **Data Lake híbrido** (nube + on-premise) para analítica avanzada, predicción de consumo y detección de pérdidas técnicas/no técnicas.
- Definir políticas de **seguridad de datos**: clasificación (confidencial, sensible, público), cifrado en tránsito y reposo, y control de accesos basado en roles (RBAC).
- Establecer **gobernanza de datos** (data quality, master data management, trazabilidad).

Arquitectura de aplicaciones

Objetivo: Definir el conjunto de aplicaciones que soportarán los procesos de negocio y garantizarán interoperabilidad, seguridad y escalabilidad.

- Identificar aplicaciones críticas: **SCADA, ERP, CRM, facturación, portal de clientes, sistema de cuadrillas**.
- Diseñar una **arquitectura orientada a servicios (SOA)** o **microservicios** para facilitar integración y evolución.
- Definir flujos de datos seguros entre aplicaciones:
 - SCADA ↔ ERP (estado de la red para gestión de activos).
 - ERP ↔ CRM (datos de clientes y facturación).
 - CRM ↔ Portal web/móvil (autogestión de clientes).
- Integrar la **seguridad en el SDLC (Software development life cycle)**: revisiones de código seguro, pruebas de penetración en aplicaciones, DevSecOps con CI/CD (integración y entrega continua).

Asegurar la coherencia

Objetivo: Validar que las arquitecturas de datos y aplicaciones soporten los objetivos estratégicos definidos en la Fase B (arquitectura de negocio).

- Mejorar confiabilidad del servicio eléctrico → **Soporte TI/OT**: SCADA integrado con monitoreo predictivo.
- Optimizar la atención al cliente → **Soporte TI**: CRM y portal en línea con autoservicio.
- Incrementar ciberresiliencia → **Soporte TI/Seguridad**: integración SIEM con logs de aplicaciones y datos críticos.
- Validar que cada aplicación y modelo de datos tenga un **alineamiento directo** con los procesos clave de negocio (facturación, atención, operación de red).



Hoja de ruta

La hoja de ruta priorizará en el corto plazo la integración ERP-CRM y la modernización del portal de clientes, mientras que en el mediano plazo se implementará el Data Lake y el SOC (centro de ciberseguridad).



Situación actual: aplicaciones aisladas, poca automatización y flujos de datos fragmentados



Migrar el CRM a plataforma cloud segura.



Integrar SCADA con ERP mediante bus de servicios.



Implementar Data Lake para analítica avanzada.



Desplegar DevSecOps para aplicaciones nuevas.

Situación **objetivo:**
integración en tiempo real, automatización de procesos, nube híbrida para escalabilidad.

Actividades clave en la Fase C



Resultados de la Fase C

**Modelos de
arquitectura de datos y
aplicaciones objetivo**

**Componentes de la
hoja de ruta**

**Consideraciones de
desarrollo**

Actividades FASE C



Selección de Referencias

- Adoptar marcos como **ISO/IEC 27001** para la gestión segura de la información, además de **Smart Grid Interoperability Standards** para aplicaciones relacionadas con la red eléctrica inteligente.



Definición de Vistas

- **Funcional:** procesos de atención al cliente y gestión de reclamos.
- **Datos:** consumo eléctrico y facturación.
- **Seguridad:** cifrado de datos de clientes y autenticación en portales web.



Identificación de Deficiencias

- Duplicidad de bases de datos para clientes.
- Baja integración entre el sistema comercial y el sistema de mantenimiento de red.
- Riesgos de fuga de información por aplicaciones obsoletas.



Considerar Interacciones

La implementación de una aplicación de **medidores inteligentes** impacta en:

- **Negocio:** mejora la facturación en tiempo real.
- **Datos:** requiere nuevos modelos de almacenamiento masivo (Big Data).
- **Tecnología:** demanda infraestructura de IoT y redes seguras.

Resultados Fase C



1. Modelos de arquitectura de datos y aplicaciones objetivo

- Modelo de datos centralizado en un **Data Lake corporativo** para consolidar información de consumo, facturación, fraudes eléctricos y mantenimiento.
- Implementación de un **modelo de aplicaciones** con módulos integrados: SCADA seguro, ERP para gestión administrativa, CRM para atención al cliente y plataforma IoT para Smart Grids (redes eléctricas inteligentes).
- Flujos de datos definidos entre sistemas críticos (generación, distribución, clientes) asegurando **integridad, disponibilidad y trazabilidad**.



2. Componentes de la hoja de ruta

- Implementación de **medidores inteligentes** con transmisión segura de datos en tiempo real.
- Migración progresiva a **infraestructura híbrida (nube + on-premise)**.
- Despliegue de una **plataforma de ciberseguridad** con SIEM, monitoreo de amenazas y firewalls de próxima generación.
- Desarrollo de **aplicación móvil** para clientes con funciones de autogestión (consultar consumo, reportar fallas, pagos en línea).
- Capacitación en **DevSecOps** para el personal de TI.



3. Consideraciones de desarrollo

- Enfoque **DevSecOps** para garantizar que la seguridad esté integrada en todo el ciclo de vida de desarrollo de software (SDLC).
- Estrategia **Build vs. Buy**: desarrollo interno de aplicaciones críticas (facturación y atención al cliente), pero adquisición de soluciones robustas para SCADA, SIEM y gestión de identidades.
- Plan de adopción gradual con pilotos en zonas urbanas antes de desplegar en áreas rurales.
- Políticas de **gestión del cambio** para asegurar aceptación de empleados y usuarios finales.

¿Arquitecturas de datos y aplicaciones?

- Base de datos centralizada de clientes, contratos y consumos.
- Integración de datos de medidores inteligentes (IoT).
- Almacén de datos (Data Warehouse) para analítica y predicción de demanda.

¿Cómo se diseñan modelos de datos seguros y se integra la seguridad en el ciclo de vida de desarrollo de software?

Modelos de datos seguros

1. Clasificación de datos: Crítico (OT/SCADA), Confidencial (PII, pagos), Interno, Público.

2. Electrificadora Andina:

1. Portal de clientes: tokenización y masking.
2. Medidores inteligentes: TLS + segmentación OT.
3. SCADA: control de acceso con PAM (Gestión de accesos privilegiados) + auditoría.

Seguridad en el SDLC (DevSecOps)

1. Requerimientos: incluir seguridad y regulaciones desde el inicio.

2. Diseño: validación de arquitecturas.

3. Desarrollo: secure coding, análisis de dependencias, sin secretos en código.

4. CI/CD: SAST, SCA, DAST, escaneo de infraestructura y contenedores.

5. Operación: monitoreo con SIEM, gestión de vulnerabilidades y respuesta a incidentes.

La Fase D: Arquitectura de Tecnología

Se enfoca en desarrollar la Arquitectura Tecnológica de destino, definiendo el hardware, software y las tecnologías de comunicación necesarias para soportar las arquitecturas lógicas de datos y aplicaciones. Su objetivo es crear el modelo de infraestructura que permita la transformación digital, asegurando que sea escalable, segura y cumpla con los objetivos de la empresa, y para ello se utilizan los resultados de fases previas como las arquitecturas de datos y aplicaciones.



¿Qué es la Arquitectura Tecnológica?

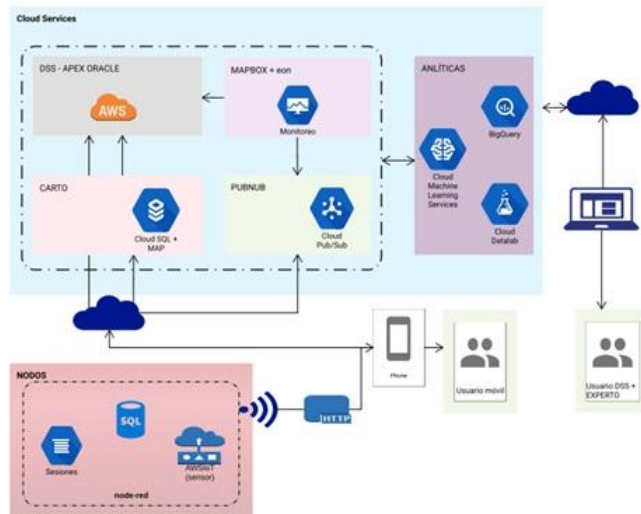
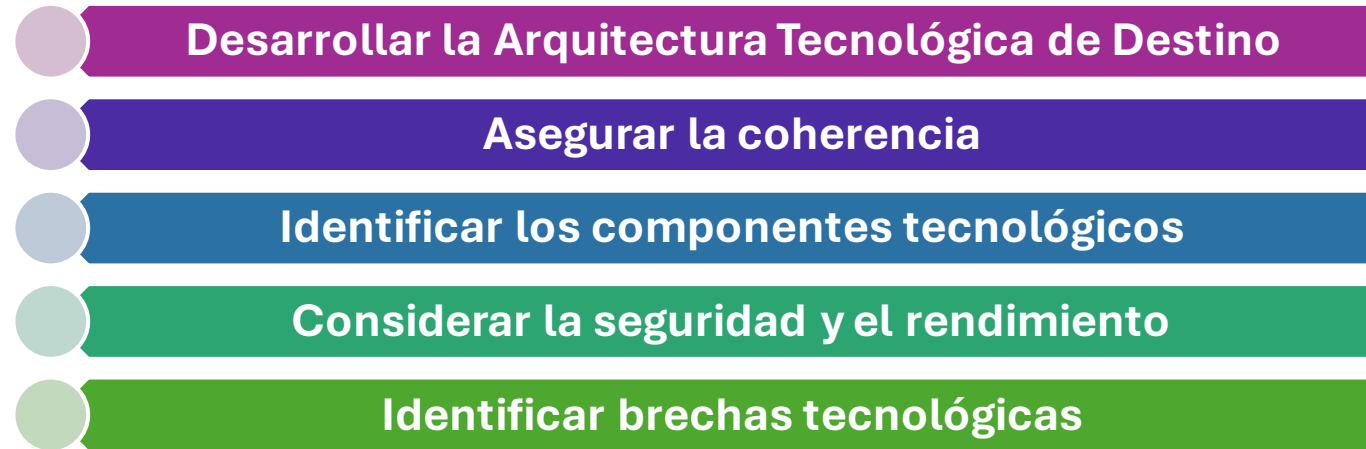


Figura 9. Arquitectura de referencia

- Es una descripción de su cartera de infraestructura completa que le indica cuándo comprar infraestructura y cuándo usar esta infraestructura.
- Nos dice dónde poner los límites entre los sistemas.
- Nos dice cómo abordará su ciclo de vida.



Objetivo principal de la Fase D



Beneficios

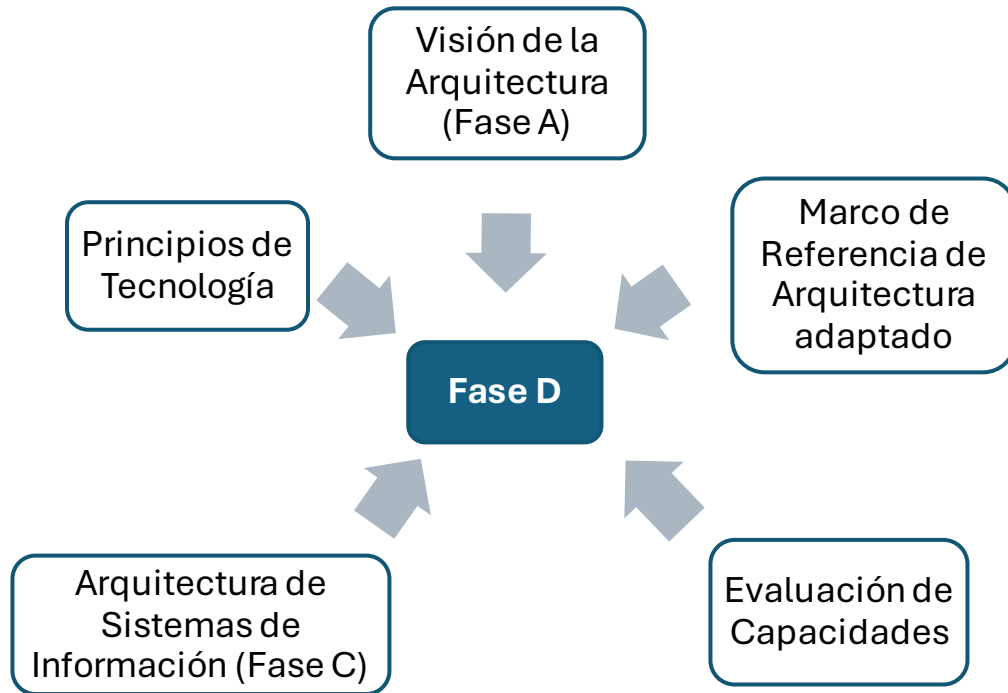
Asegura que la infraestructura tecnológica esté alineada con el negocio

Reduce riesgos de incompatibilidad tecnológica

Facilita la transición hacia entornos modernos (cloud, edge, IoT, ciberseguridad).

Define estándares que mejoran la gobernanza de TI.

Entradas



Estas entradas trabajan en conjunto para desarrollar el diseño de la infraestructura de TI necesaria para cumplir con los requisitos de negocio y los objetivos de la visión de la arquitectura.

Salidas

<input type="checkbox"/>	Principios de Tecnología
<input type="checkbox"/>	Arquitectura Tecnológica de Destino
<input type="checkbox"/>	Análisis de Brechas Tecnológicas
<input type="checkbox"/>	Requerimientos de Arquitectura Tecnológica
<input type="checkbox"/>	Declaración o Estatuto de Trabajo de Arquitectura
<input type="checkbox"/>	Repositorio de Arquitectura
<input type="checkbox"/>	Vista de Arquitectura Tecnológica

Estas salidas muestran la infraestructura necesaria para soportar las arquitecturas de negocio y de sistemas de información de la organización.

¿Cómo se seleccionan las tecnologías de seguridad?

Revisar los requisitos de seguridad

Aplicar principios de arquitectura de seguridad

Seleccionar modelos de referencia y building blocks

Evaluar y comparar tecnologías candidatas

Definir estándares y políticas tecnológicas

Documentar en la Arquitectura Tecnológica

¿Cómo se diseña la infraestructura técnica que soporte los controles de ciberseguridad?

Identificación de controles de seguridad requeridos

Mapeo de controles a componentes técnicos

Diseño de la arquitectura tecnológica con capas de seguridad

Definición de estándares y políticas técnicas

Integración en diagramas de arquitectura (outputs de la fase D)

¿Pongamos en práctica lo tratado!

Kahoot!