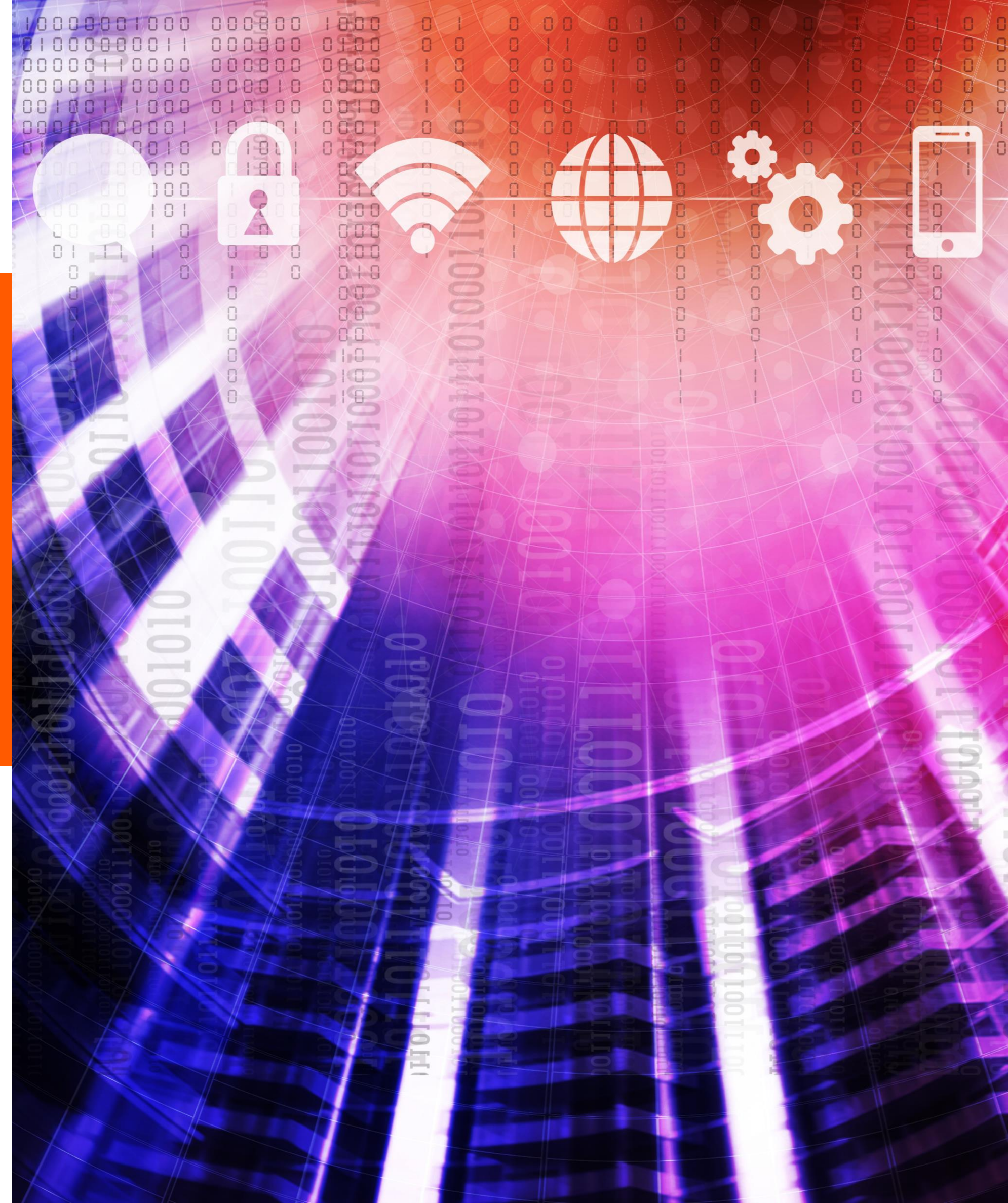


CÓMO ASEGURAR LA CIBERSEGURIDAD

LA IMPORTANCIA DE LA CERTIFICACIÓN Y DE LA
CORRECTA DEFINICIÓN DE REQUISITOS DE

● Marta Castro
● 27 septiembre 2022



Índice

01 Introducción. Contexto	3
02 Problemáticas del Sector	7
03 Soluciones ante las necesidades del sector	8
04 Metodología	9

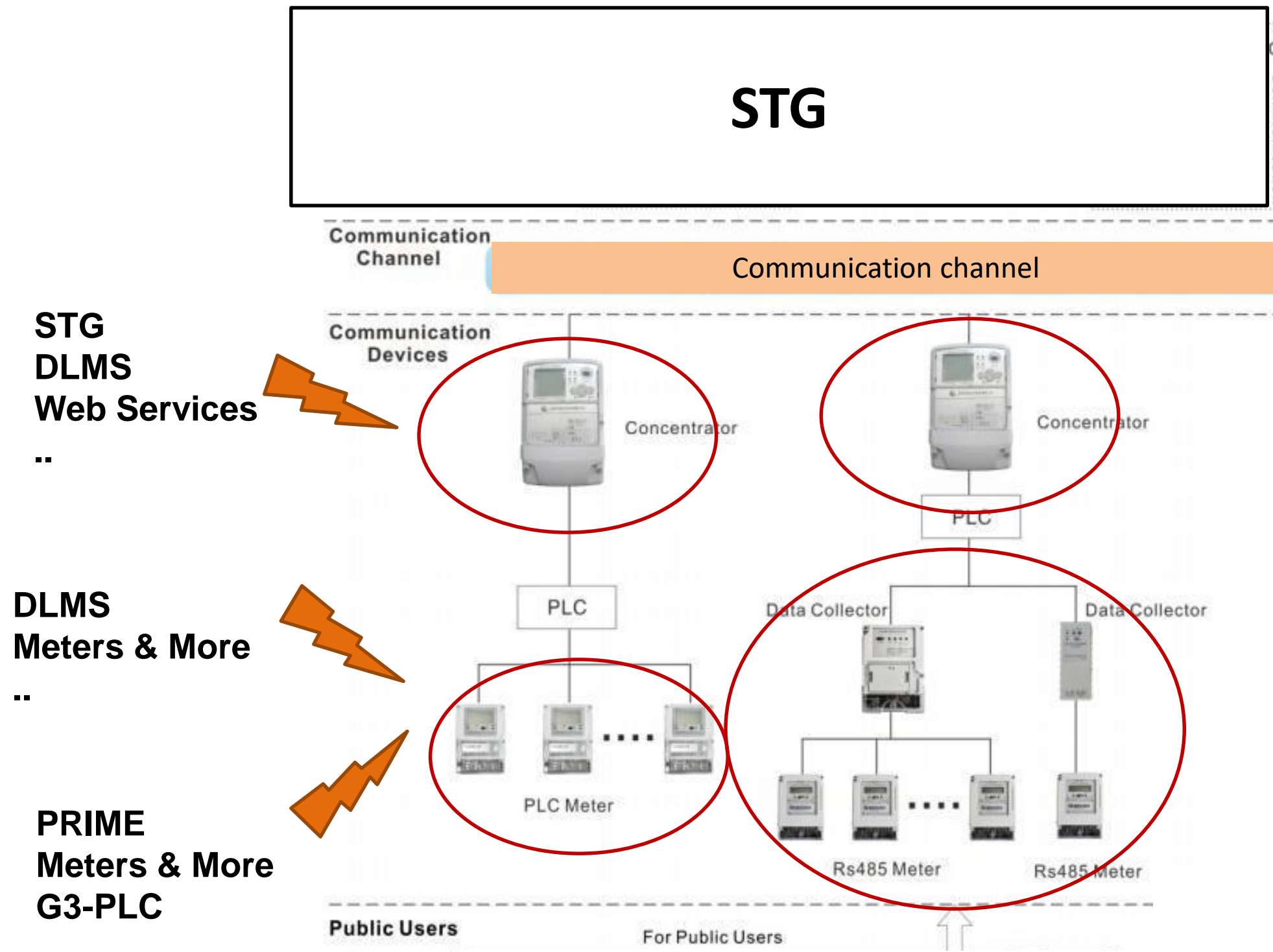
CONTEXTO

En los últimos años, se ha pasado de una red eléctrica tradicional donde apenas existían comunicaciones, siendo necesaria la presencia física de personal técnico para el mantenimiento, análisis de fallos, lectura de eventos y alarmas o lectura de consumos para tarificar



A una red eléctrica y un sistema AMI inteligente donde las comunicaciones, los datos y la tecnología, posibilitan la gestión centralizada y reducen el factor humano en tareas de menor valor añadido.

CONTEXTO



- El aumento de la inteligencia en la red provoca que esté más expuesta a ciberataques
- Riesgos de vulnerabilidad de nuevas tecnologías
- Incremento de puntos de acceso a equipos
- Incremento de la consciencia y el interés del ciudadano por mantener su privacidad
- Mayores exigencias regulatorias

CONTEXTO



- ✓ Diferentes versiones de un mismo fabricante
- ✓ Multifabricante
- ✓ Multiprotocolo
- ✓ Diferente interpretación de la norma, especificaciones, requisitos de cliente..
- ✓ Diferente versión de configuraciones
- ✓ Necesidades de adaptaciones o ajustes, cambio de FW
- ✓ Diferencias en el criterio o metodología de ensayos

CONTEXTO

Particularidades del sector eléctrico:

- Necesidad de mantenimiento de servicio en activo, a pesar de encontrarse en situaciones de ataque.
- Elevada exigencia a los equipos en lo que respecta a tiempos de respuesta.
- Dispersión geográfica y de equipos.



PROBLEMÁTICA DEL SECTOR

Regulatorios

- Falta de estandarización. No existe una normativa clara
- Requisitos genéricos
- Requisitos impuestos por un tercero → cómo adecuarlos a cada empresa

Capacitación del personal

- Desconocimiento de la integración OT (Tecnologías de Operación) – IT (Tecnologías de Información)
- Las soluciones del mundo IT no siempre son aplicable (Disponibilidad vs. Confidencialidad, Tiempos de respuesta mucho más exigentes y Dispersión geográfica y de equipos)
- Falta de personal experto en OT y IT
- Evolución hacia el mundo cloud

Mantenimiento Despliegue

- Cómo incluir ciberseguridad en redes ya desplegadas. ¿Qué hacer con los sistemas desplegados?
- Cómo gestionar todo el ciclo de vida de los activos. Acortar el ciclo de vida de los activos
- Actualizaciones continuas
- Gestión de riesgos. Gestión de parches

SOLUCIONES A LAS PROBLEMÁTICA DEL SECTOR

Regulatorios

- elaborar un **análisis de vulnerabilidades** del sistema y del equipo.
- estudio de los diferentes protocolos, estándares, normativas, requisitos genéricos y requisitos particulares con el objetivo de elaborar una **especificación particular que recoja todos los requisitos adaptados a las necesidades del cliente**

Capacitación del personal

- La **formación del personal** tanto en los aspectos regulatorios como en la especificación particular que resuma los requisitos particulares del cliente es clave para asegurar que todas las personas de la empresa son conscientes de la importancia y necesidad de la ciberseguridad.

Mantenimiento Despliegue

- elaborar y definir unos procedimientos de ensayos que recojan de forma detallada los pasos a realizar para comprobar y verificar cada uno de los requisitos de la especificación dando lugar a la certificación del producto.
- Plantear el despliegue cómo parte de una **metodología global**, en la se defina y acompañe al cliente desde la idea hasta el correcto despliegue de las soluciones en campo

METODOLOGÍA

TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación

REQUISITOS

1

Definir requisitos de usuario

PROCEDIMIENTOS DE ENSAYO

2

Definición de procedimientos de ensayos de acuerdo a la normativa + especificaciones + requisitos de cliente. Casos de Uso

PLATAFORMAS DE ENSAYO

3

Desarrollo de plataformas de ensayo automatizadas

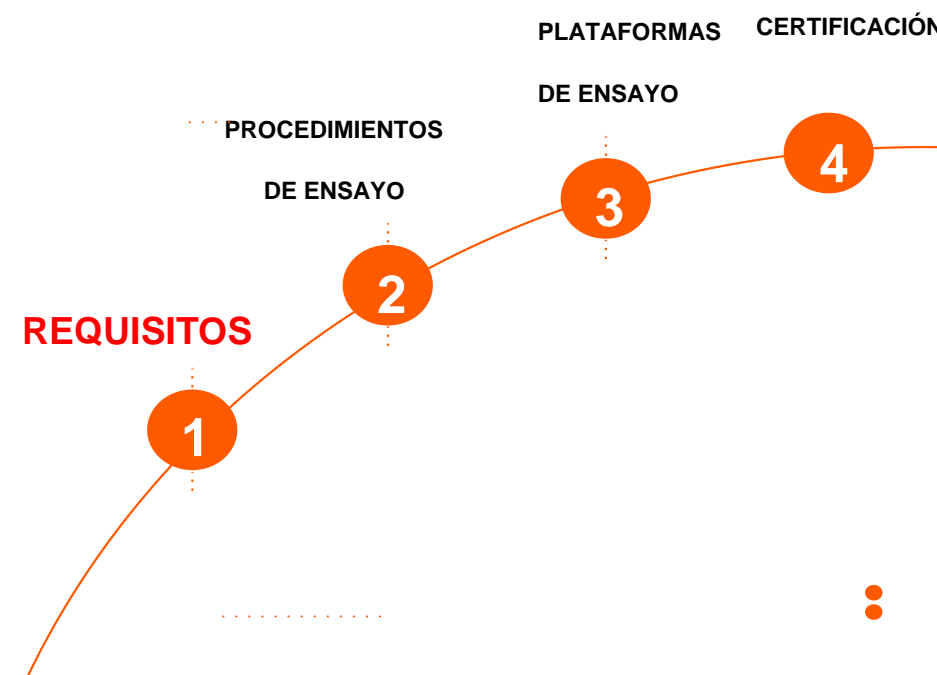
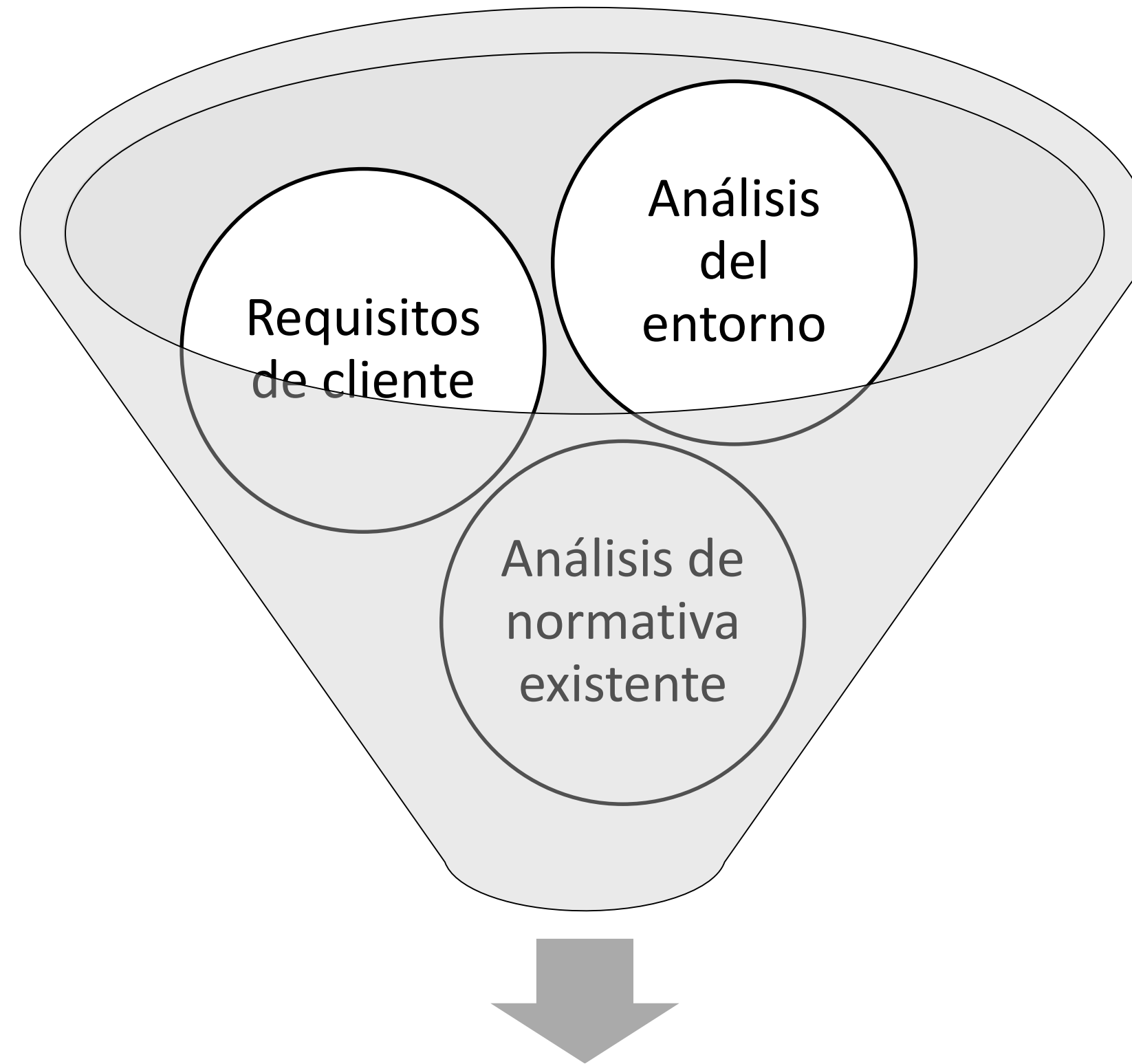
CERTIFICACIÓN

4

Ayudar al CLIENTE a asegurar el cumplimiento con la normativa y a asegurar la **INTEROPERABILIDAD** y **CIBERSEGURIDAD** en campo.

METODOLOGÍA - REQUISITOS

TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación



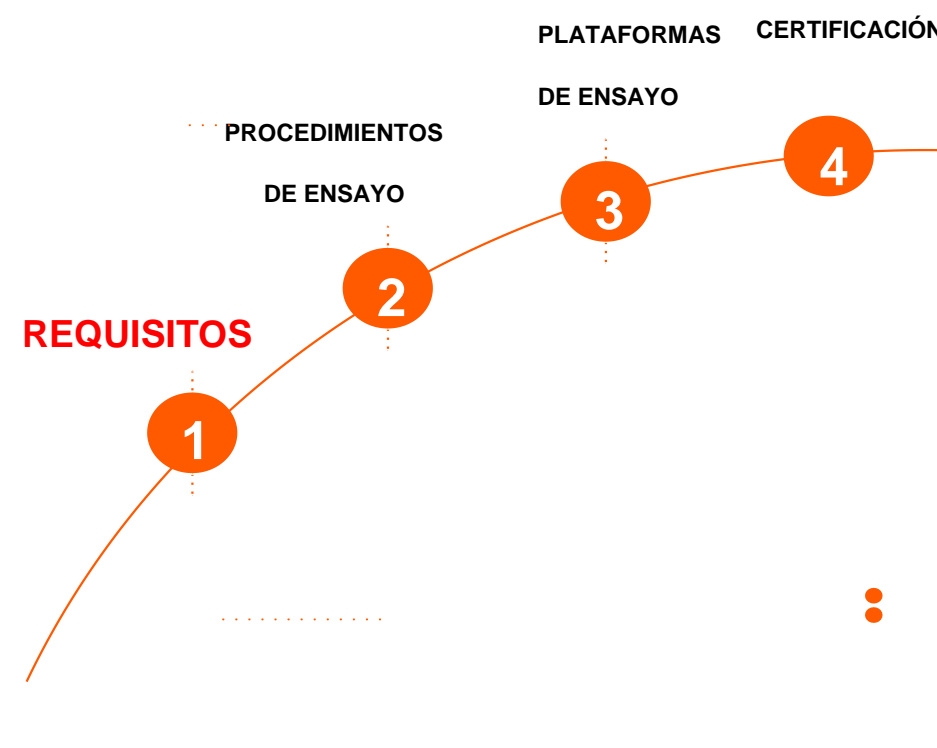
•**OBJETIVO: definir los requisitos aplicables a su sistema o equipo**

METODOLOGÍA - REQUISITOS

TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación

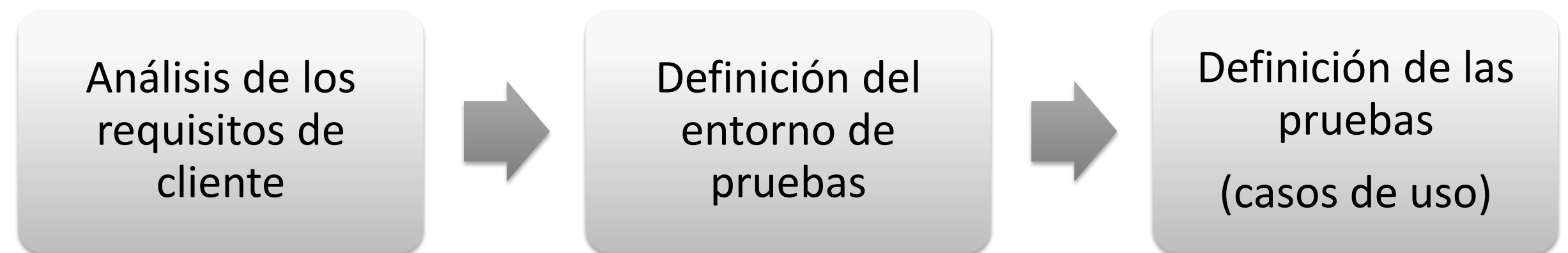
Los **requisitos clave de ciberseguridad en los sistemas AMI** se basan en:

- El **control de acceso basado en roles**: es necesario definir la información a la que van a tener acceso los diferentes roles y con qué nivel de permisos. Es decir, hay que detallar la lista de objetos y sus derechos de acceso.
- La **encriptación** para garantizar la **confidencialidad**.
- La **autenticación** para verificar el **origen y la integridad** de los mensajes.
- La gestión de las claves de ciberseguridad.
- Registros de eventos de seguridad.
- Medidas y registros ante fraudes y ataques de ciberseguridad.

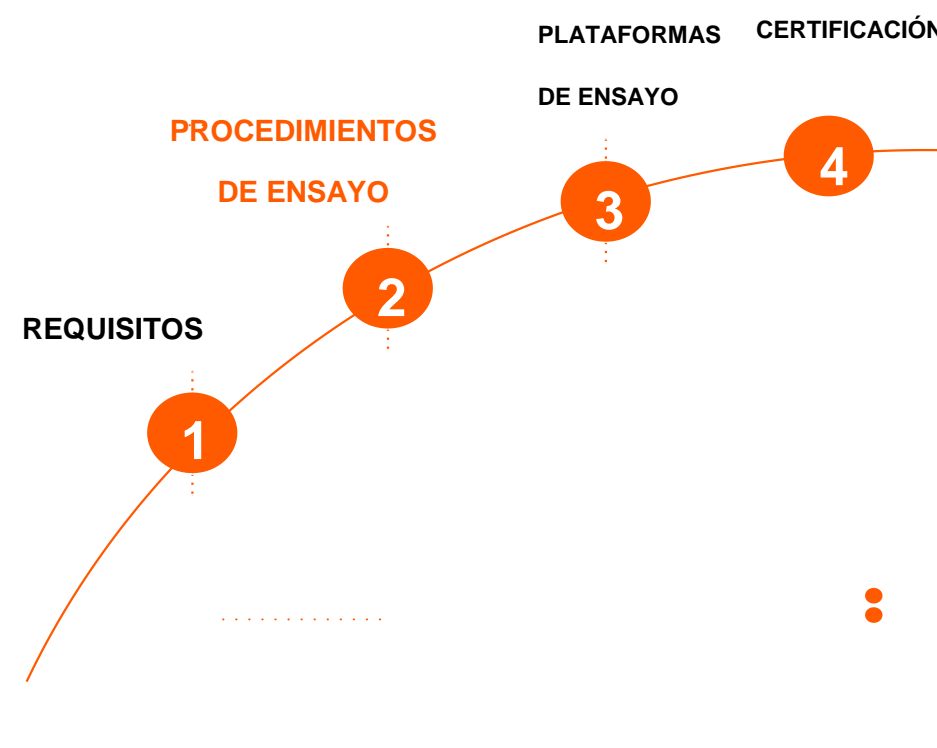


METODOLOGÍA – PROCEDIMIENTOS DE ENSAYO

TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación



- Asegurar el cumplimiento de los requisitos del cliente
- Asegurar que todos los laboratorios ensayan y aplican las pruebas siguiendo el mismo procedimiento
- Definir un entorno de pruebas y equipamiento de ensayos común a todos los laboratorios



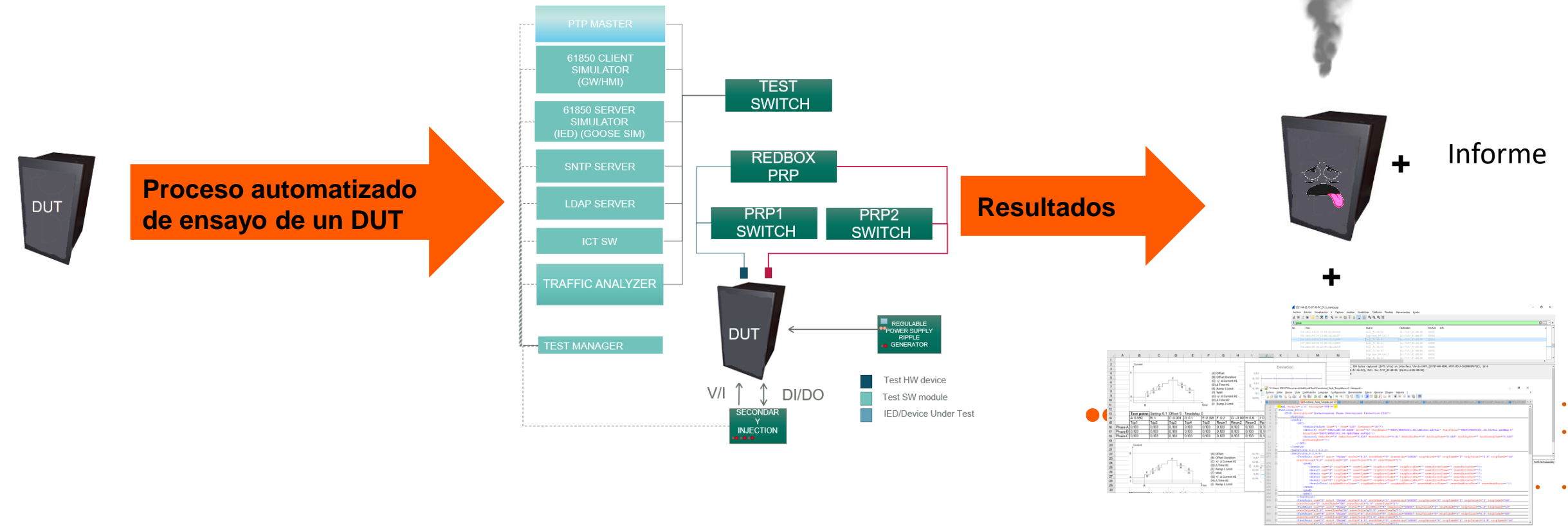
METODOLOGÍA - HERRAMIENTAS

TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación

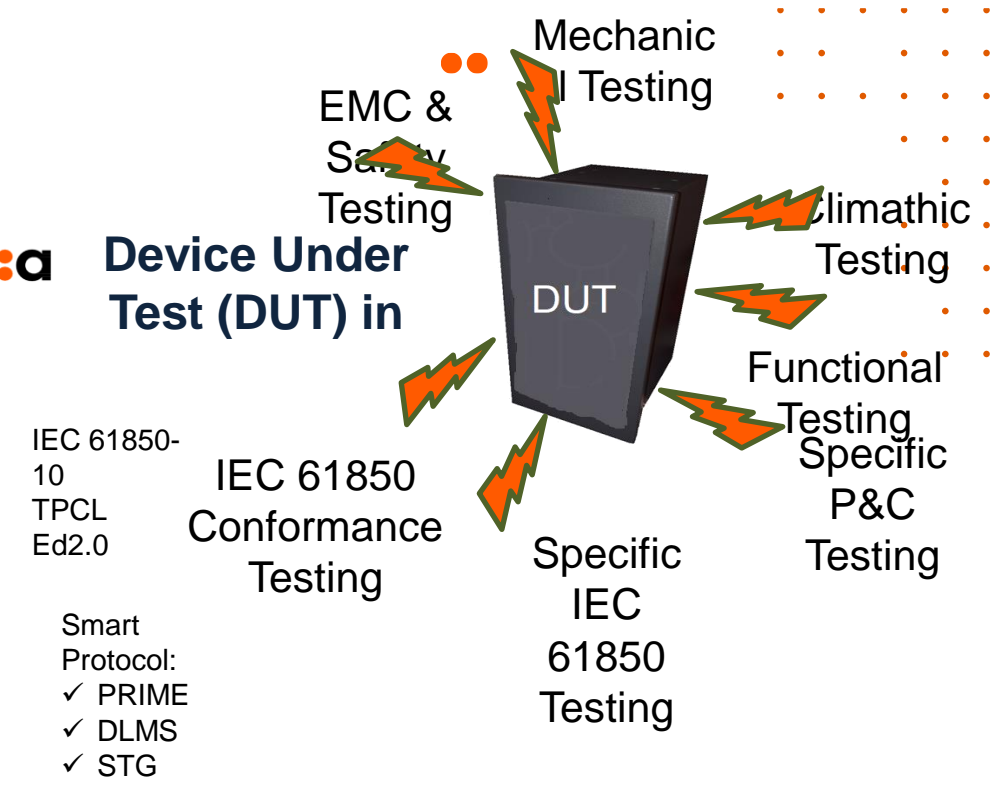
Certificación Manual



Certificación Automatizada

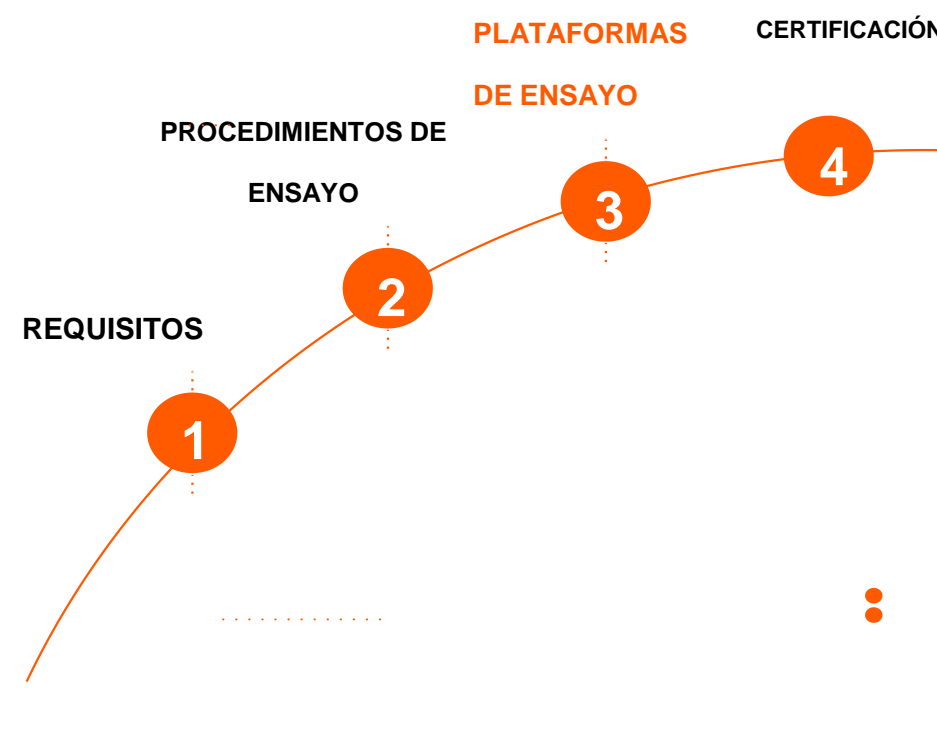


Device Under Test (DUT) in



METODOLOGÍA - HERRAMIENTAS

TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación



¿¿Qué nos aporta una herramienta de ensayos??

Mejora el proceso de certificación

Repetitividad de ensayos.
Independencia del técnico de ensayos

Automatización de ensayos.
Evidencias

Ensayos en paralelo y por la noche

Beneficios

Fabricantes para aceleración de su desarrollo

○ Clientes finales para validaciones internas

○ Otros laboratorios

METODOLOGÍA – HERRAMIENTAS - EJEMPLOS

TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación

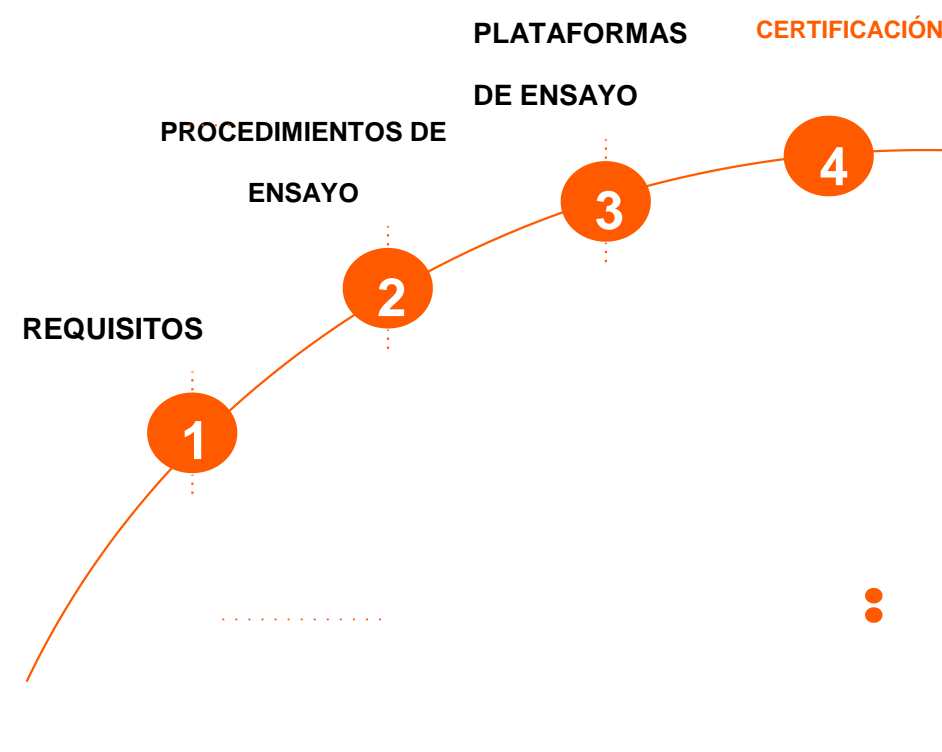


- ✓ Herramienta Conformance Testing Tool Protocolos:
 - ✓ IEC 61850
 - ✓ PRIME 1.3.6
 - ✓ PRIME 1.4
 - ✓ DLMS
- ✓ Herramienta Ensayos FUNCIONALES
 - ✓ Herramienta ensayos IED
 - ✓ Herramienta ensayos GTW
 - ✓ Herramienta ensayos HMI
 - ✓ Herramienta ensayos Smart Meters
 - ✓ Herramienta ensayos Concentradores de datos
- ✓ Herramienta ensayos Protección y Control
- ✓ Herramienta Ciberseguridad



METODOLOGÍA – CERTIFICACIÓN

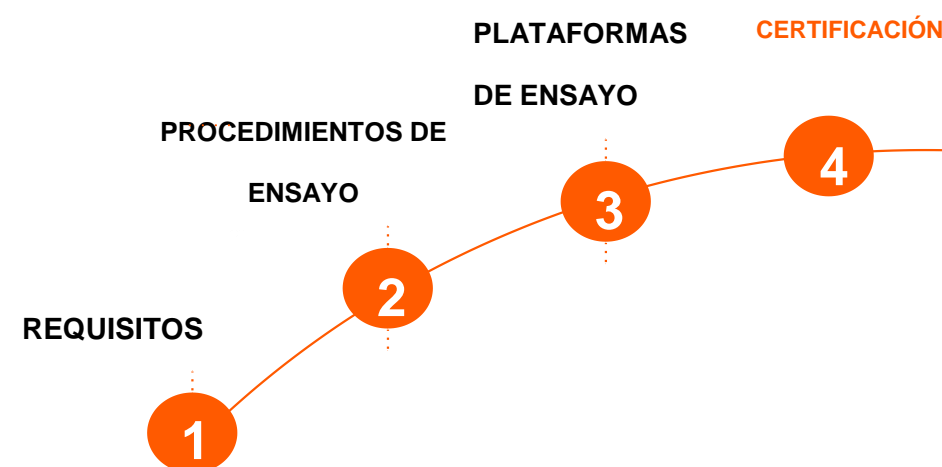
TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación



- Certificación tipo → Equipo con **versión SW y HW específica.**
- Cualquier cambio de FW se debe certificar de nuevo.
- Importante definir unos ensayos mínimos que aseguren la calidad y la funcionalidad del equipo.

METODOLOGÍA – CERTIFICACIÓN

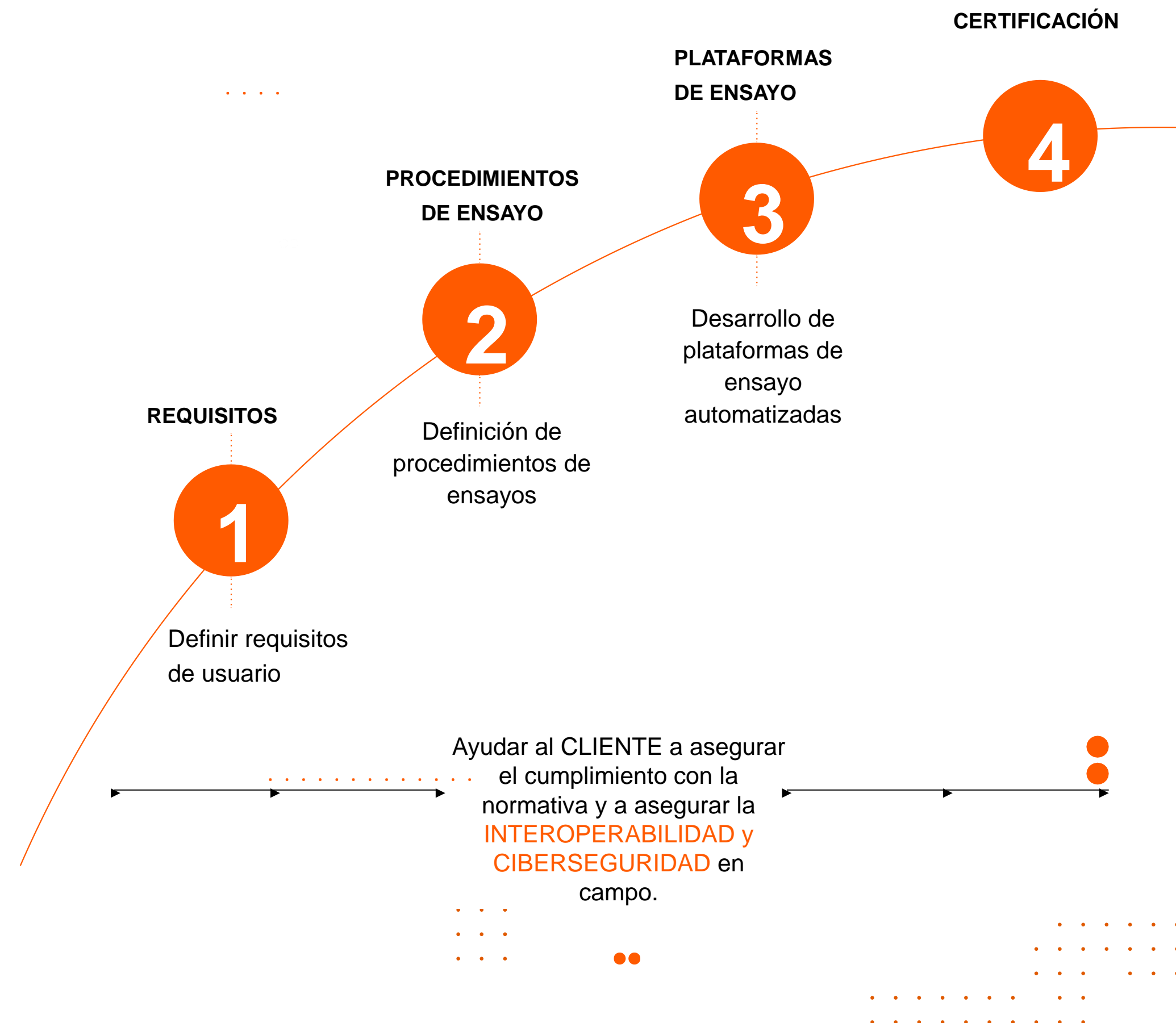
TECNALIA ayuda al cliente en todo el proceso desde la definición de requisitos hasta la certificación



CONCLUSIONES

Importancia de la metodología para:

- ✓ Abordar un despliegue ordenado
- ✓ Reducir las ambigüedades
- ✓ Cumplimiento de normativa y requisitos cliente
- ✓ Asegurar la Interoperabilidad
- ✓ Asegurar la ciberseguridad



Marta Castro
Directora de Digital Lab Services

marta.castro@tecnalia.com
667178914



tecnalia.com

tecnalia

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

