ZIUR
INDUSTRIAL CYBER SECURITY
CENTER-GIPUZKOA

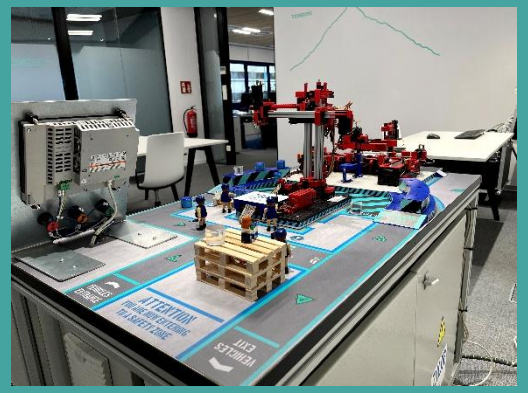
Laboratorio de CiberSeguridad Industrial

DONOSTIA
SAN SEBASTIÁN

Gipuzkoako
Foru Aldundia
Diputación Foral
de Gipuzkoa

AGENDA

- ¿Porqué un Laboratorio de CiberSeguridad Industrial?
- Diseño del Laboratorio ICS
- Casos de USO del Laboratorio ICS
- Opciones de USO del Laboratorio ICS



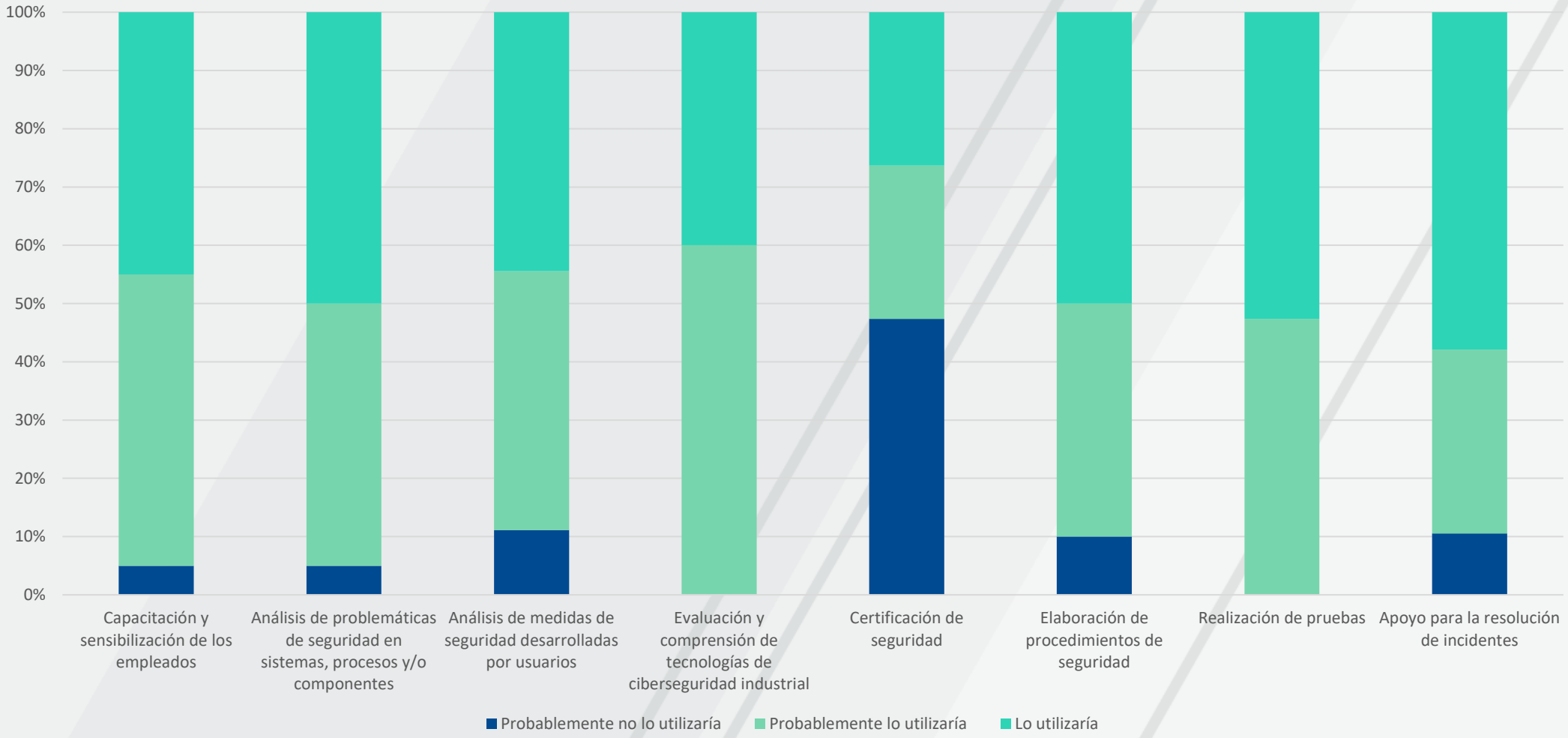
Laboratorio de CiberSeguridad Industrial

Laboratorio ICS

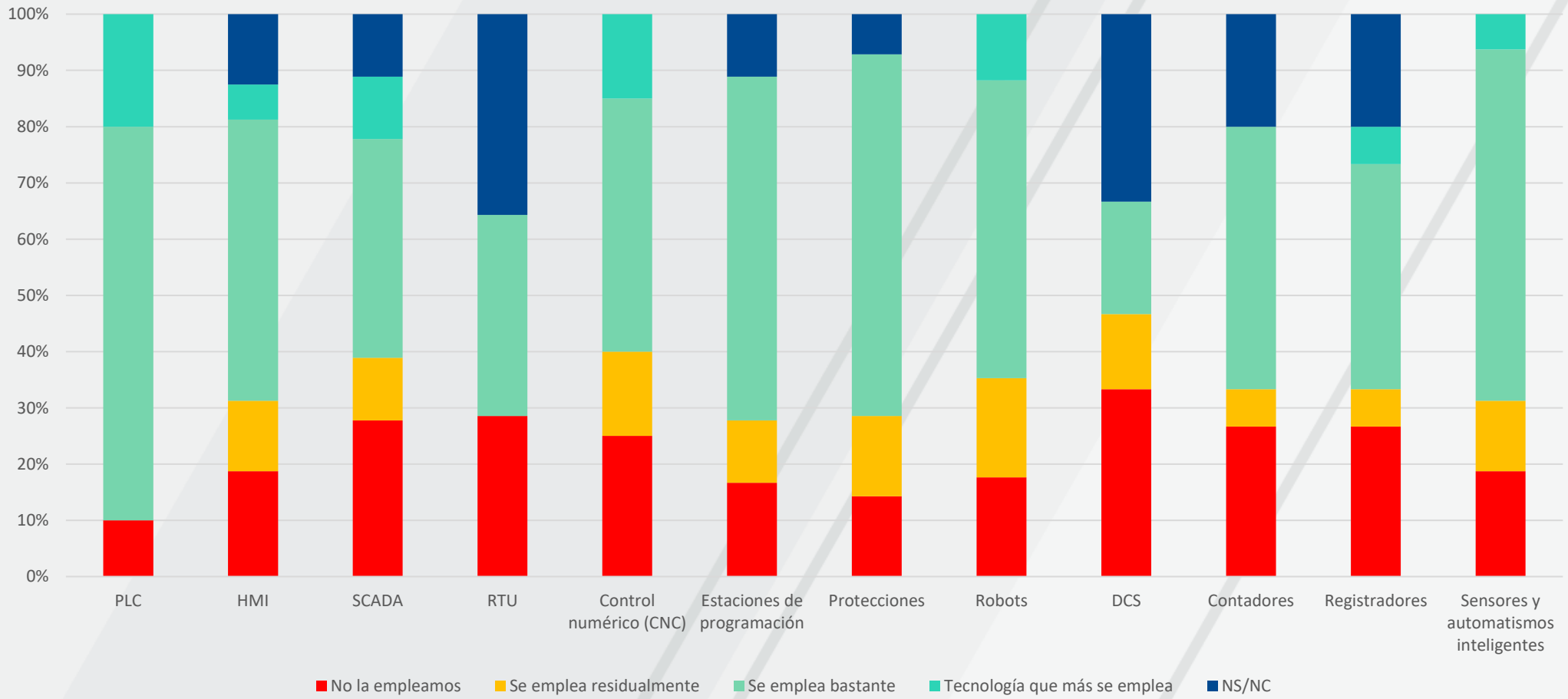
¿PORQUÉ UN LABORATORIO DE CIBERSGURIDAD INDUSTRIAL EN GIPUZKOA?

EMPRESAS: AYUDAS DE INTERÉS

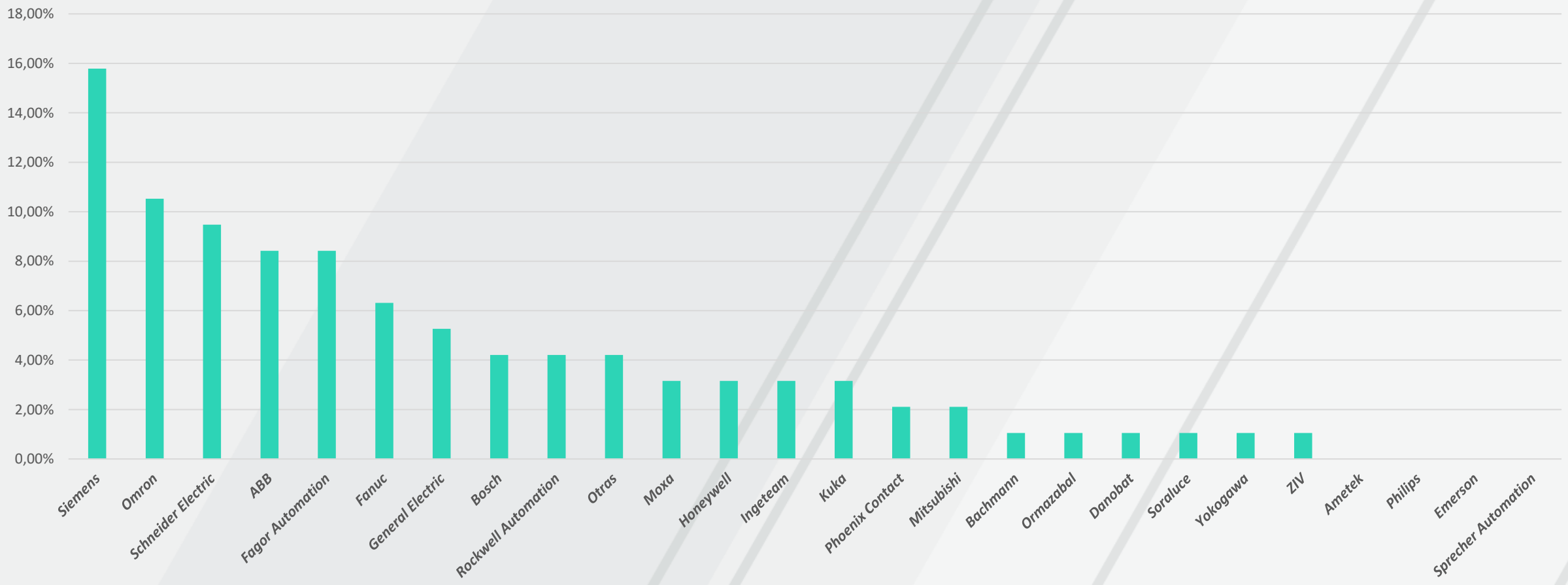
El SECTOR INDUSTRIAL constituye una de las actividades más relevantes de Euskadi, ya que aporta cerca del 25% de su PIB y emplea a 40.000 personas.



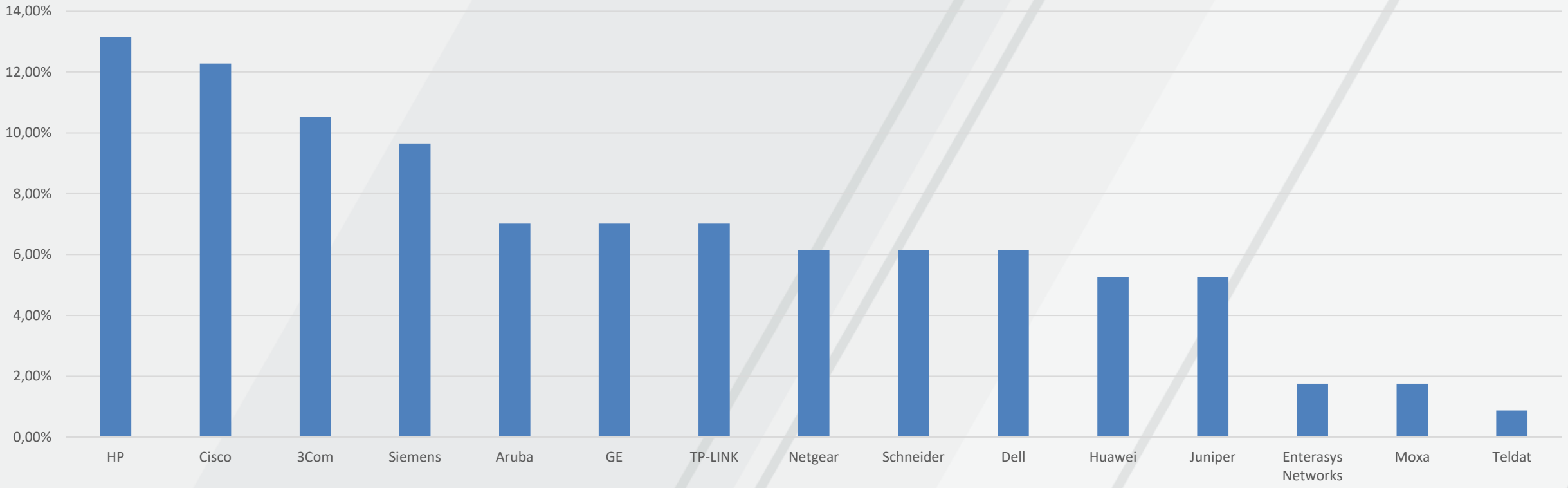
TECNOLOGIAS DE AUTOMATIZACION Y CONTROL



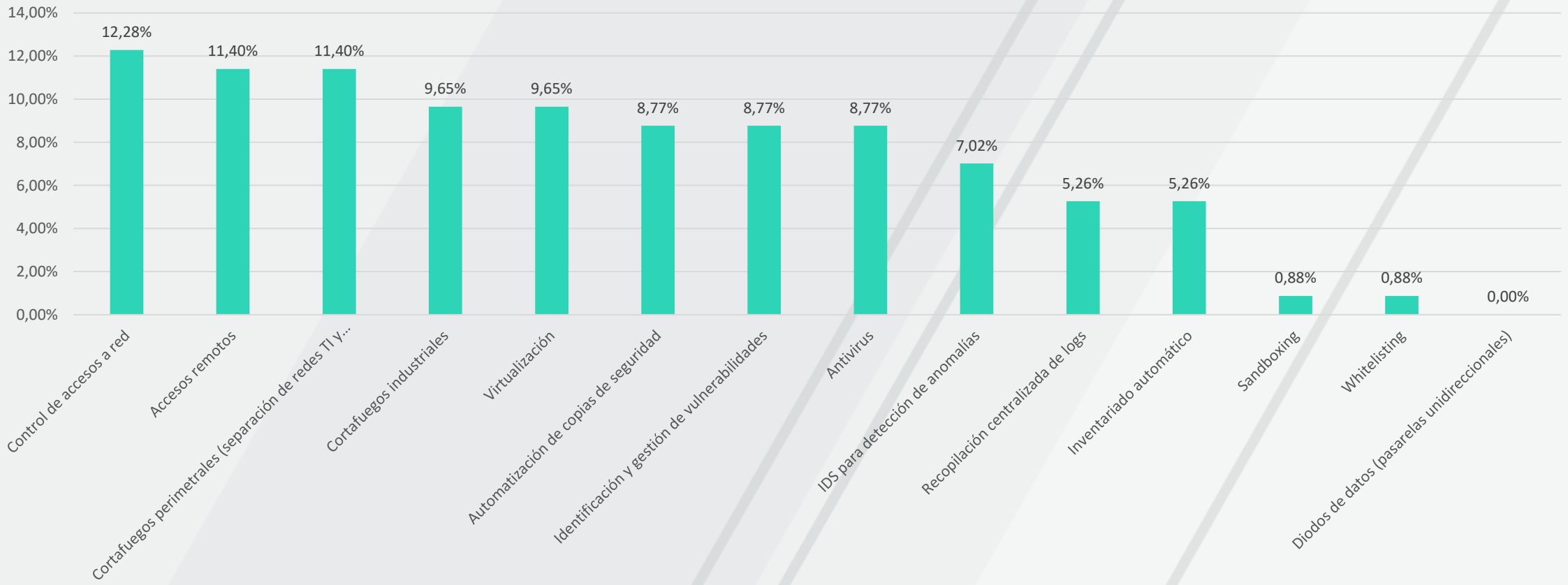
FABRICANTES DE AUTOMATIZACION Y CONTROL



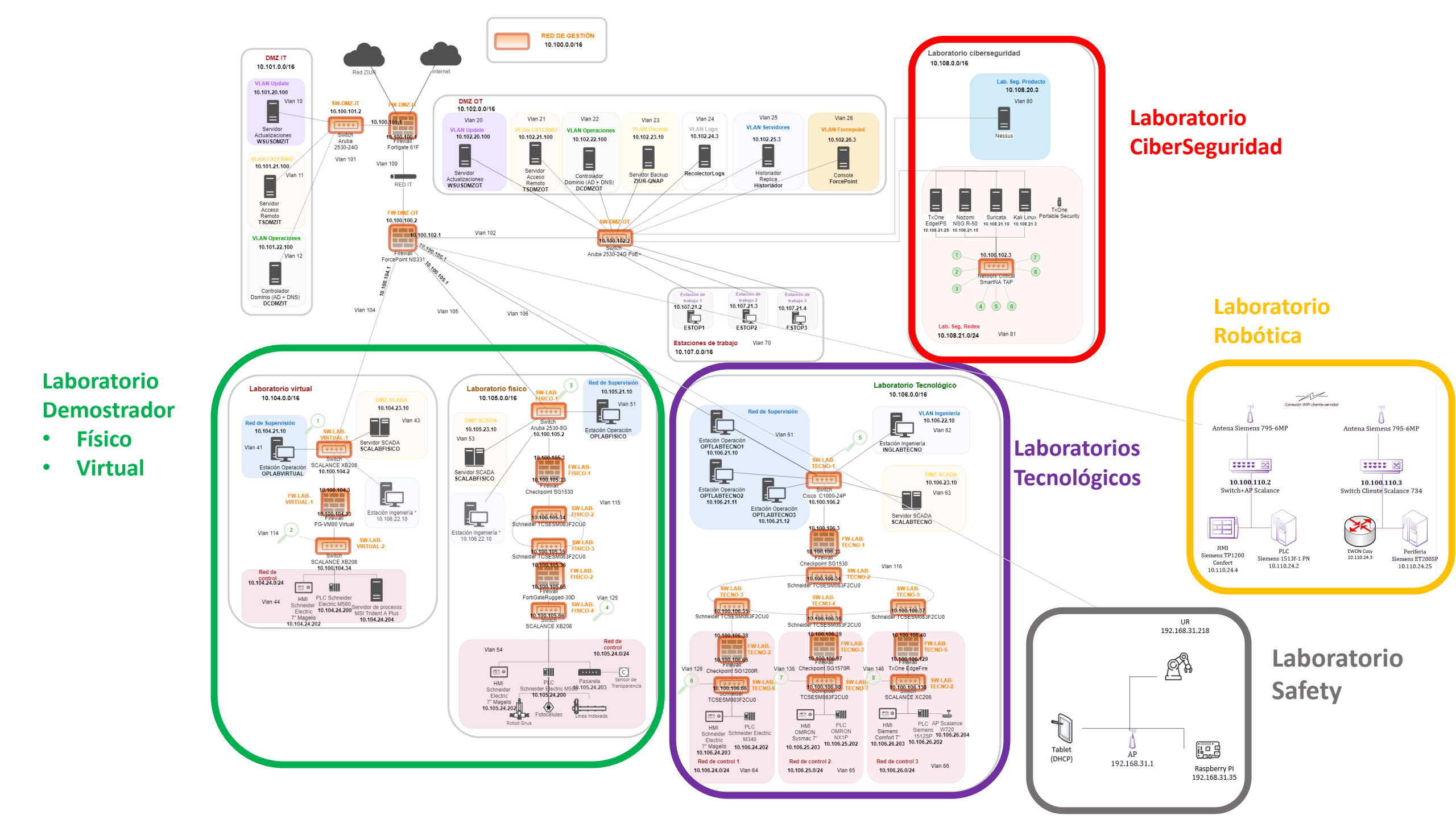
FABRICANTES ELECTRONICA DE RED



TECNOLOGIAS DE CIBERSEGURIDAD INDUSTRIAL DE INTERÉS



DISEÑO DEL LABORATORIO


Laboratorio Demostrador
• Físico
• Virtual
Laboratorio CiberSeguridad
Laboratorio Robótica
Laboratorios Tecnológicos
Laboratorio Safety
RED DE GESTIÓN
10.100.0.0/16
DMZ IT
10.101.0.0/16
DMZ OT
10.102.0.0/16
Laboratorio ciberseguridad
10.108.0.0/16
Laboratorio virtual
10.104.0.0/16
Laboratorio fisico
10.105.0.0/16
Laboratorio Tecnológico
10.106.0.0/16
Estaciones de trabajo
10.107.0.0/16
UR
192.168.31.218
AP
192.168.31.1
Tablet
(DHCP)
Raspberry PI
192.168.31.35

Elementos Comunes del Laboratorio

DMZ - IT

- Elementos típicos de un entorno corporativo
- Servidor de actualizaciones sistemas de gestión e IT
- Acceso remoto
- Controlador de Dominio
- AV Panda Adaptive Defense 360

DMZ - OT

- Servidor de actualizaciones sistemas OT
- Acceso remoto
- Controlador de Dominio
- Servidor Backup
- Recolector Logs
- Historiador réplica
- Servidor Backup y Control de Versiones Industrial VDOG
- Servidor MES
- Solución industrial data Analytics
- Network Access Control ARUBA
- Soluciones Acceso Remoto: TeamViewer, AnyDesk

Elementos de Red Comunes del Laboratorio

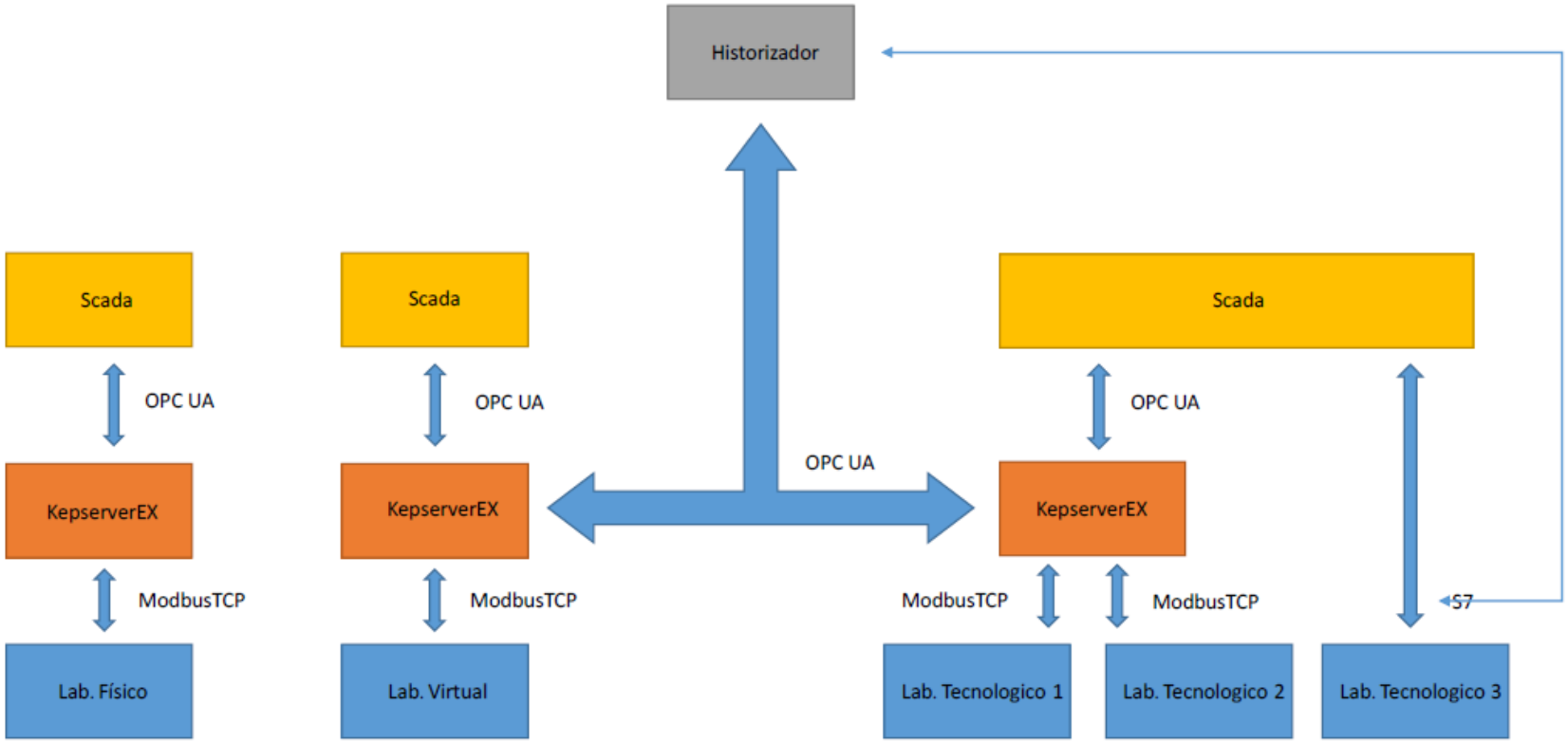
IT

- Firewalls Fortigate
- Switch Aruba 2530- 24G
- Host DELL R740:
  - Controlador de dominio IT
  - Terminal Server IT
  - Servidor de actualizaciones IT

OT

- Firewall Palo Alto
- 2 x Switch Aruba 2530- 24G PoE+
- Host DELL R740:
  - Controlador de dominio OT
  - Terminal Server OT
  - Servidor de actualizaciones OT

Componentes Comunes del Laboratorio – Protocolos Industriales



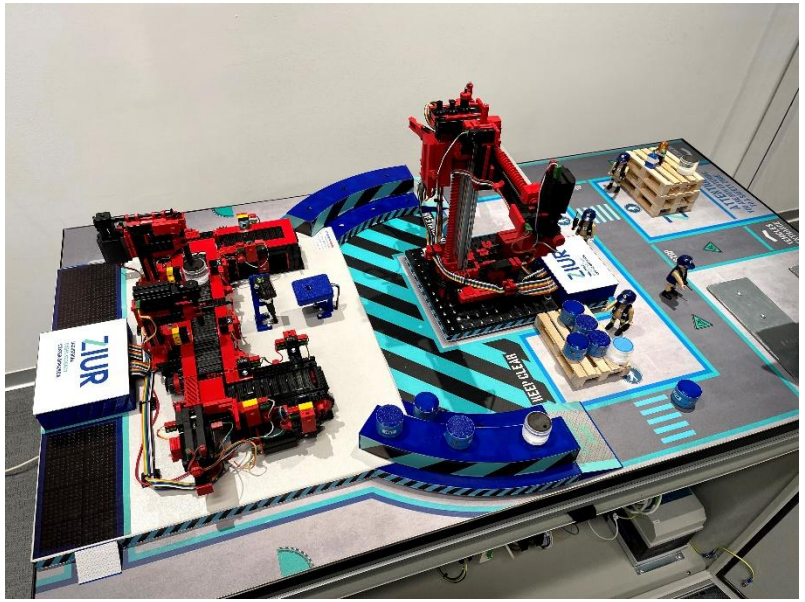
<u>OTRAS POSIBILIDADES</u>:

- El S7-1500 (Tecnológico 3) puede ejercer de servidor OPC UA (requiere licencia)
- El HMI de Siemens (Tecnológico 3) puede ejercer de servidor OPC UA
- WinCC Scada puede ser configurado como OPC UA para conexión con el Historizador
- El Historizador puede conectar al PLC de Omron (Tecnológico 2) mediante FINS

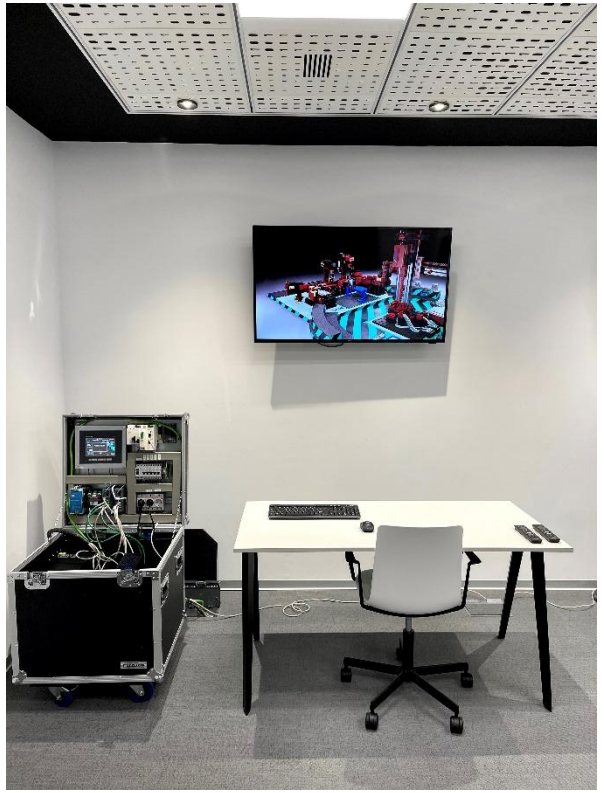
Laboratorio Demostrador

- ✓ Tiene como objetivo mostrar los diferentes elementos de un entorno industrial y los impactos que pueden causar incidentes de ciberseguridad

- ✓ Compuesto por:
  - Laboratorio físico
  - Laboratorio virtual – Fines formativos

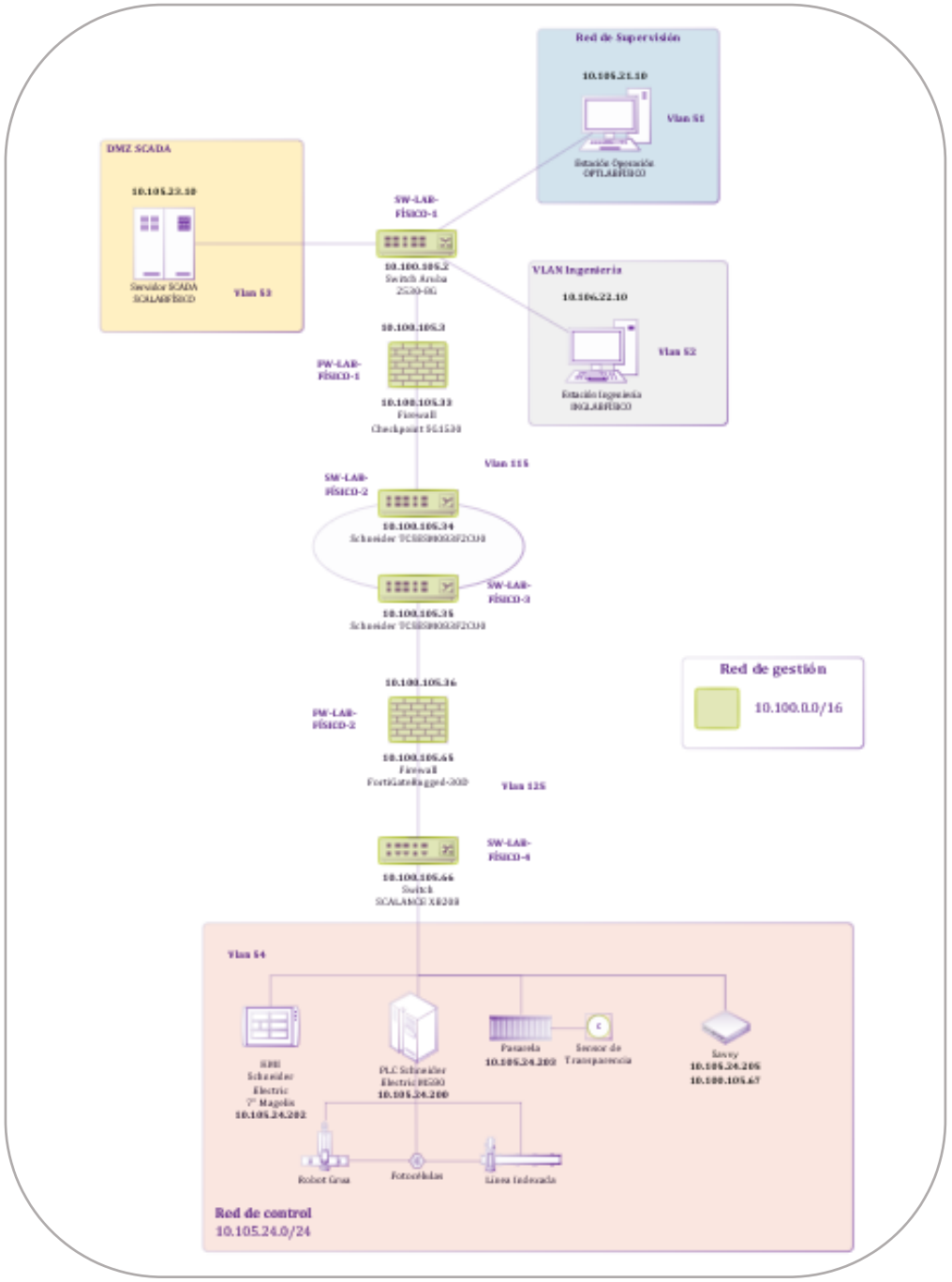


DMZ SCADA
- Estación ingeniería
- Historiador
- Servidor SCADA



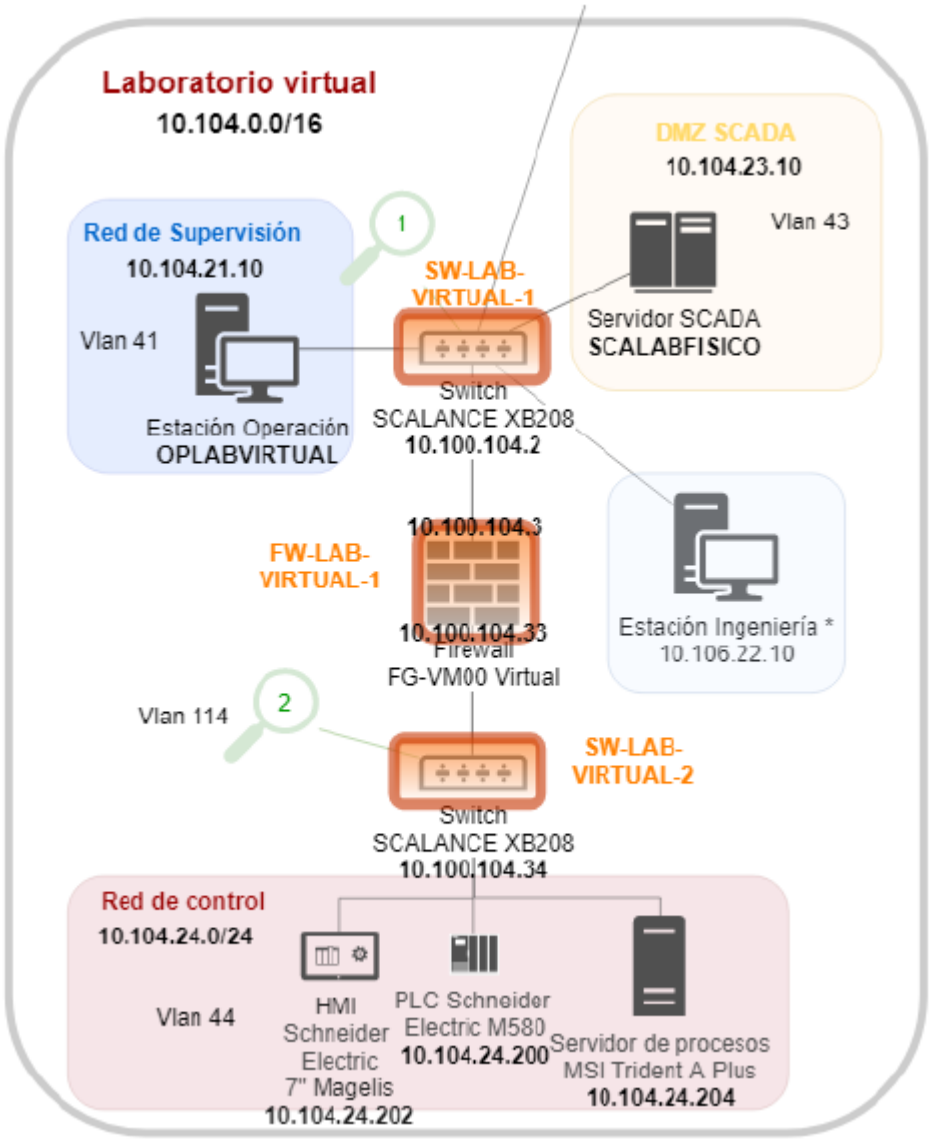
Componentes del Laboratorio demostrador Físico

- Switch Aruba 2530-8G
- Firewall Checkpoint SG1530
- 3 x Switch Schneider TCSEM083F2CU0
- Switch Siemens Scalance XB208
- Firewall FortiGateRugged 30D
- Solución industrial data Analytics SAVVY
- HPE ML30 Gen 10
  - Estación de operación
  - Servidor SCADA
  - Estación de Ingeniería



Componentes del Laboratorio Demostrador Virtual

- 2 x Switch Siemens Scalance XB208
- Host HPE ML30 Gen 10
  - Estación de operación
  - Servidor SCADA
  - Estación de Ingeniería
  - Firewall Virtual Fortinet FG-VM100 Virtual



Laboratorio Tecnológico

- ✓ Tiene como objetivo recoger los dispositivos más utilizados en el entorno industrial guipuzcoano para poder utilizarse en cualquier prueba

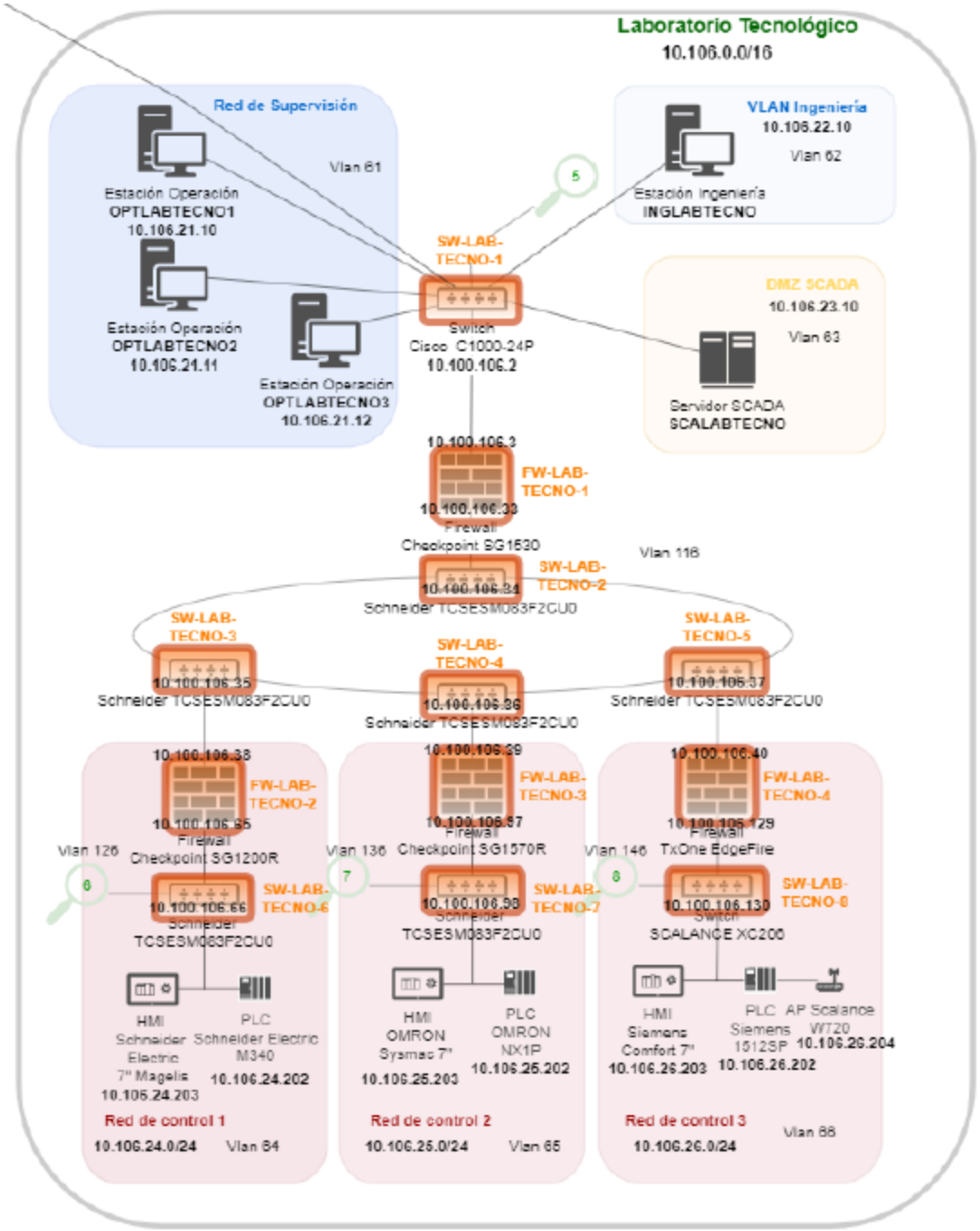
- ✓ Compuesto por tres módulos o circuitos que pueden ser usados de forma independiente o combinados

Módulos:
- FW industrial
- Switch
- PLC
- HMI

DMZ SCADA (común)
- Switch
- Servidor I/O
- Historiador
- Servidor SCADA

Componentes de los Laboratorios Tecnológicos

- Switches
  - Cisco C1000-24P
  - Siemens Scalance XC206
  - 6 x Schneider TCSEM083F2CU0
- AP Siemens Scalance W720
- Firewalls
  - 3 x Checkpoint SG1530, SG1200R, SG1570R
  - TxOne EdgeFire
  - Siemens
- PLCs
  - Schneider M340
  - Omron NX1P2
  - Siemens S7-1500
- HMIs
  - Schneider GTO
  - Omron NA
  - Siemens TP700 Comfort
- Host Servidor DELL 740
  - Estaciones de operación
  - Estación de ingeniería común para todos los laboratorios
  - Servidor SCADA



Laboratorio de CiberSeguridad

Tiene como objetivo:

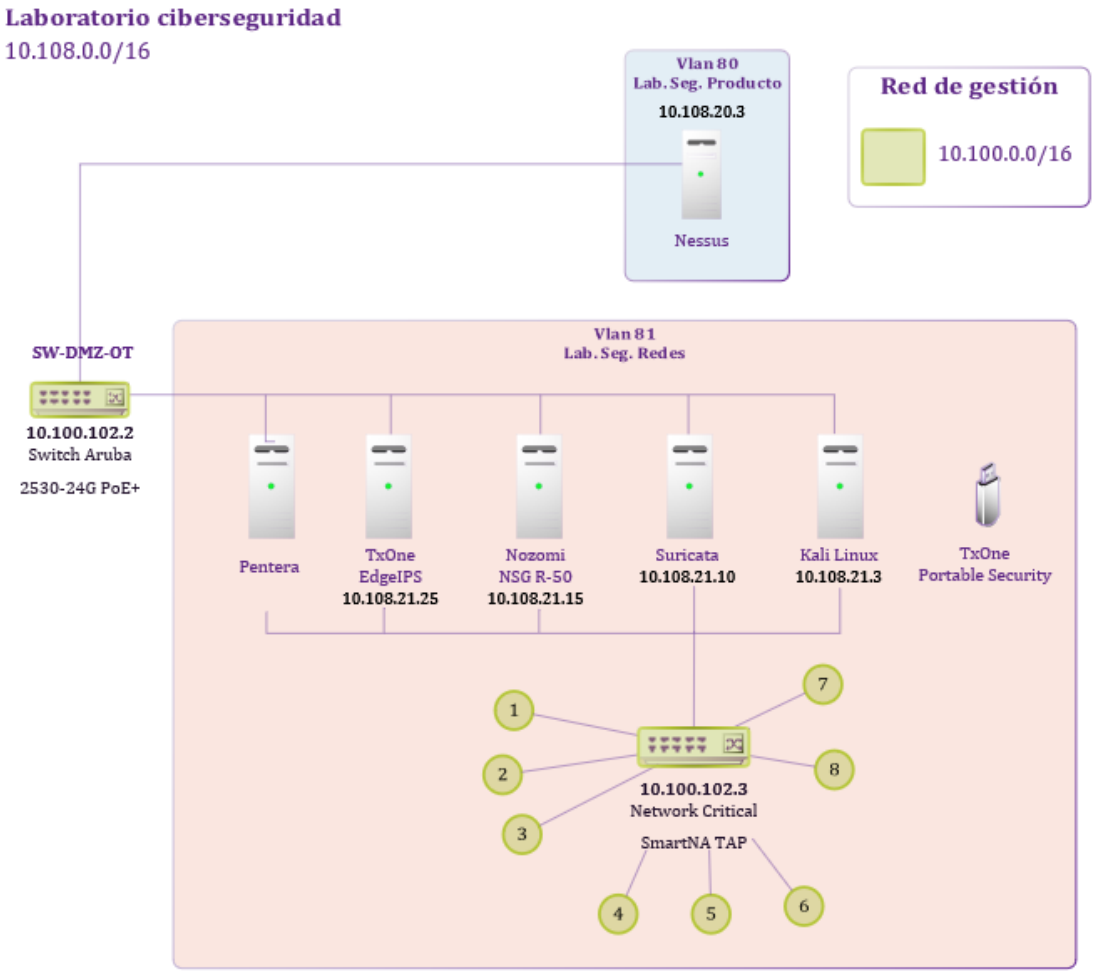
- ✓ Analizar los niveles de ciberseguridad de entornos o productos industriales
- ✓ Recrear incidentes de ciberseguridad para estudiarlos
- ✓ Análisis forense de malware OT
- ✓ Probar nuevas tecnologías de ciberseguridad OT

Compuesto por:

- Switch
- SmartTAP
- Sondas
- Snort
- TxOne EdgeIPS
- Escáner de vulnerabilidades
- Herramienta de Pentesting automatizada
- Herramienta Network Access Control
- Herramientas de ciberseguridad

Componentes del Laboratorio De Ciberseguridad

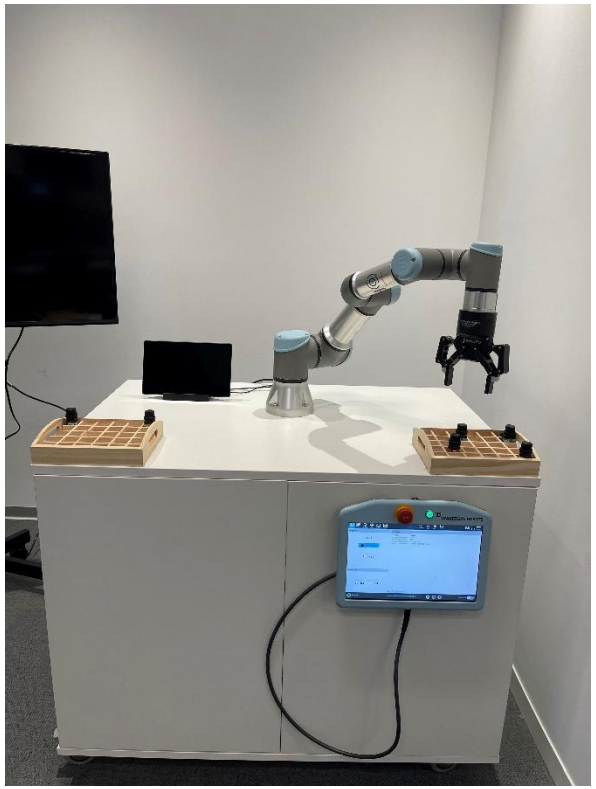
- Sonda TxOne EdgeIPS
- Sonda Nozomi NSG R-50
- IDS Open Source Suricata
- Agregador/TAP NPB Networks Critical
- Dispositvo TxOne Portable Security
- Herramienta de Pentesting PENTERA
- Herramienta Network Access Control ARUBA
- Tablero simulación ciberincidente industrial KIPS (KASPERSKY)
- Host Servidor DELL 740
  - Distribución Kali Linux con diversas herramientas
  - Escaner Nessus



Laboratorio Robótica

Tiene como objetivo:

- ✓ Analizar las arquitecturas de seguridad en entornos robóticos
- ✓ Recrear incidentes de ciberseguridad, en entornos robóticos, para estudiarlos
- ✓ Analizar soluciones de seguridad específicas para entornos robóticos
- ✓ Probar nuevas tecnologías de ciberseguridad OT

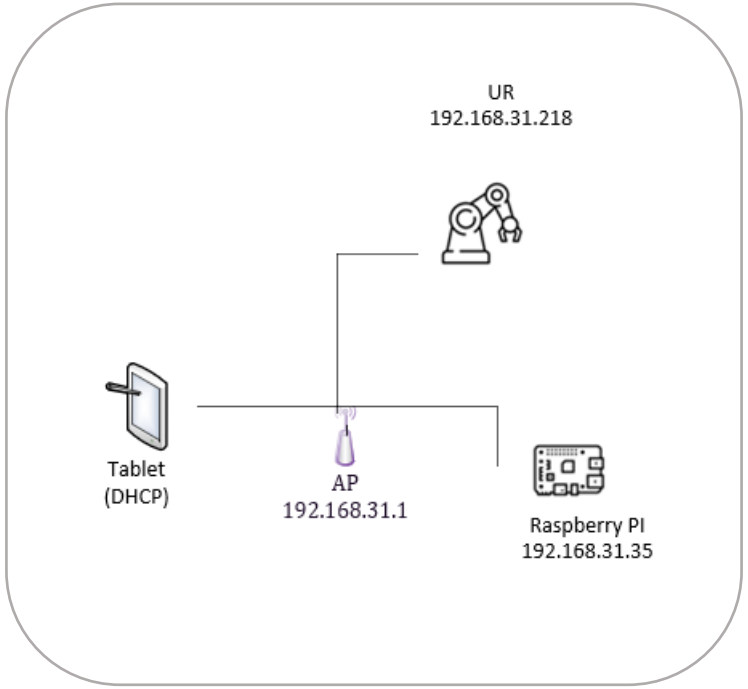


Compuesto por:

- Brazo Robótico
- Gripper
- Tableta
- Pantalla
- Raspberry PI
- Punto de Acceso
- Herramientas de ciberseguridad

Componentes del Laboratorio De Robótica

- Brazo Robótico UR
- Gripper genérico
- Tableta
- Raspberry PI
- Punto de Acceso



Laboratorio Safety

Tiene como objetivo:

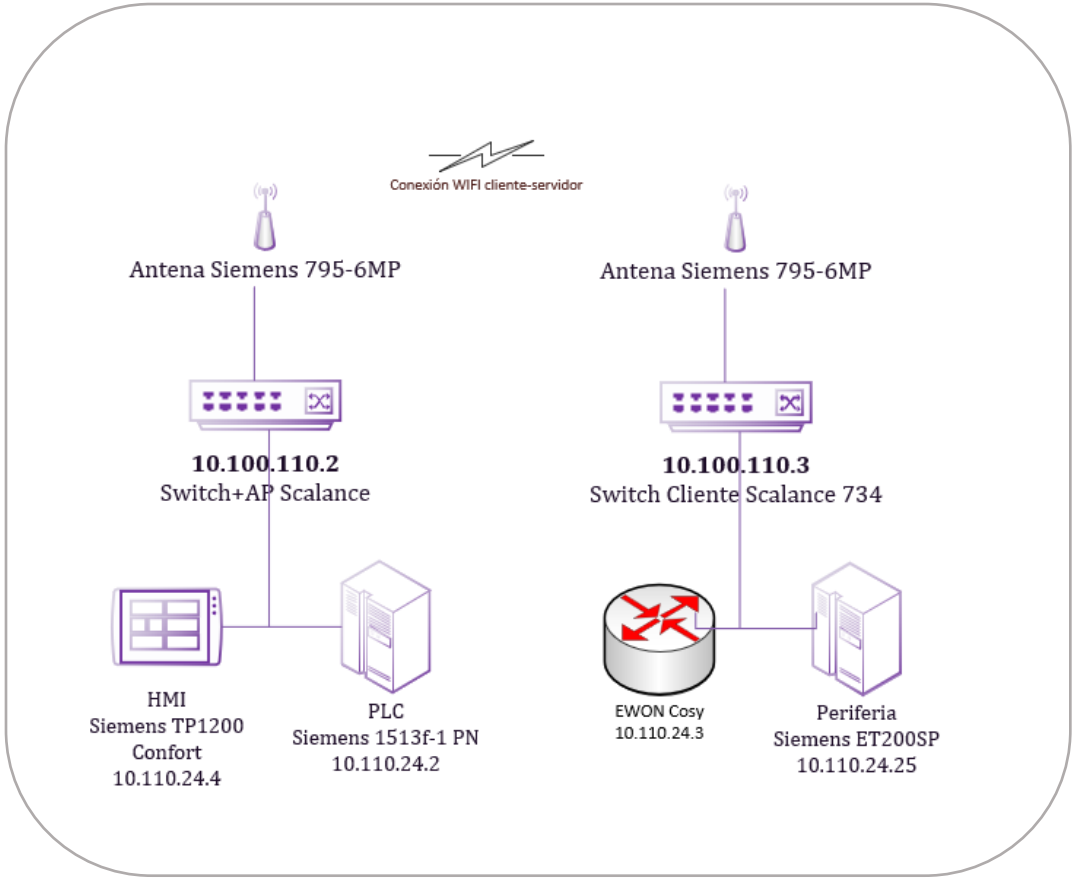
- ✓ Analizar las recomendaciones de seguridad en entornos Safety
- ✓ Analizar diferentes diseños de arquitecturas seguras en entornos Safety
- ✓ Recrear y analizar incidentes de ciberseguridad, típicos de este tipo de entornos
- ✓ Probar nuevas tecnologías de ciberseguridad OT

Compuesto por:

- Switches
- Puntos de Acceso
- Barrera de seguridad
- PLC
- HMI
- Sistema MES

Componentes del Laboratorio De Safety

- Switch Scalance
- Switch Scalance 734
- ANTENA Siemens
- ANTENA Siemens
- PLC Siemens
- HMI Siemens
- Router wan EWON
- Periferia Siemens
- Sistema MES



Sala Privada

Casos de USO GENERALES

Laboratorio ICS

Casos de uso 1

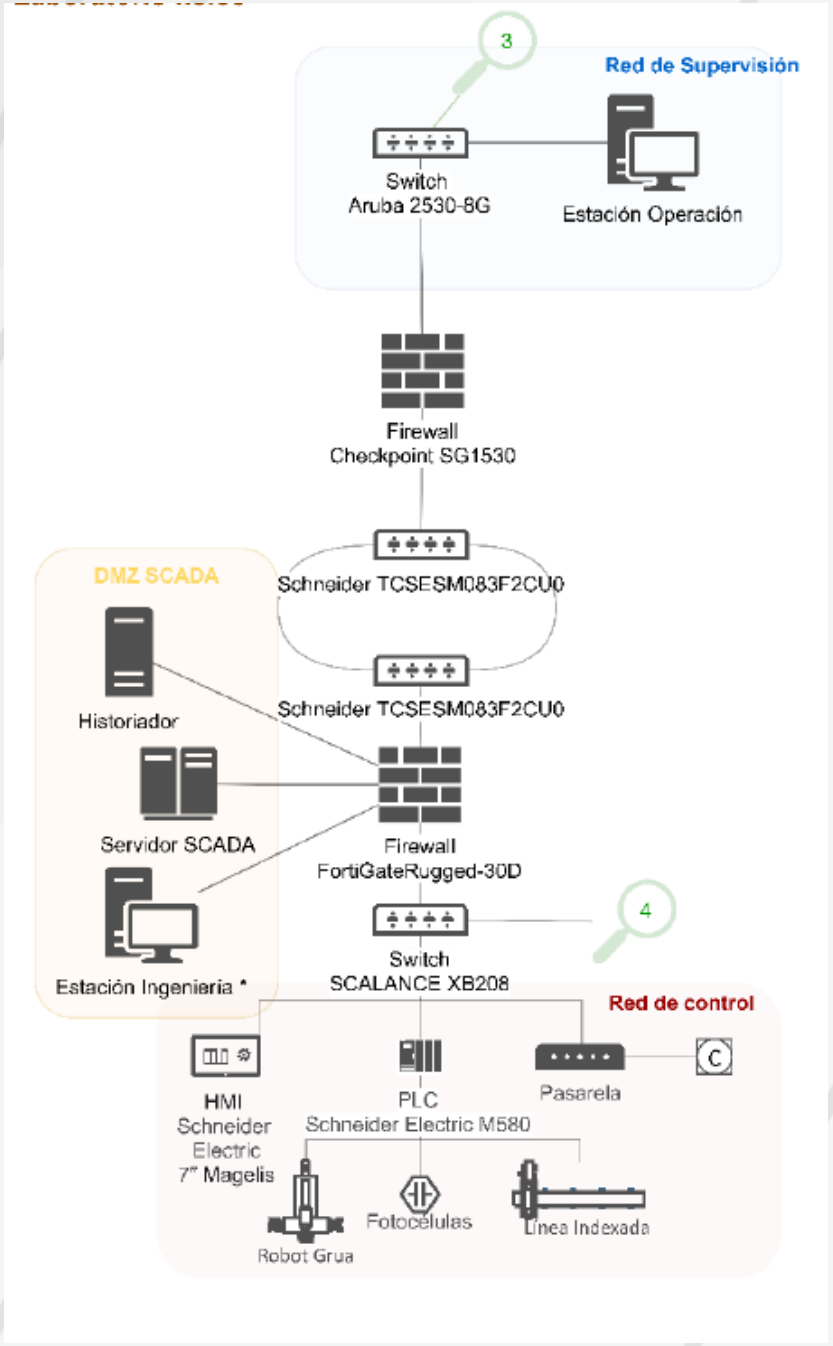
- Estudiar diferentes estrategias de defensa de los entornos industriales mediante la modificación de arquitecturas de red, bastionado, parcheo de equipos, segregación y segmentación de redes mediante firewalls, reglas de monitorización de redes industriales, etc.
- Evaluar dispositivos industriales en busca de fallas de ciberseguridad – Test de CIBERSEGURIDAD
- Realizar pruebas sobre entornos realistas con los componentes y fabricantes más utilizados en la industria guipuzcoana.
- Facilitar la formación y concienciación sobre la ciberseguridad, tanto en el ámbito industrial como en el corporativo.
- Prueba y aplicación de políticas de ciberseguridad, procedimientos y/o instrucciones técnicas, como el bastionado de equipos.
- Prueba de desarrollos propios de usuarios del laboratorio de ZIUR en las condiciones de un entorno de producción controlado.
- Realización de pruebas de hacking ético y pentesting sobre equipamiento industrial y soluciones de automatización.
- Simulación de incidentes de ciberseguridad para el estudio de cómo afectan a los entornos industriales y desarrollo de medidas complementarias para detectar y mitigar los incidentes.
- Eventos, formación, POCs

Laboratorio Demostrador Físico

Casos de uso

- ✓ Reproducir los elementos más característicos de la industria guipuzcoana, incluyendo los componentes de los sistemas de control. Gracias a las dimensiones del entorno, y las características de montaje, ZIUR dispondrá de un entorno versátil y portable que podrá usar en eventos y conferencias.

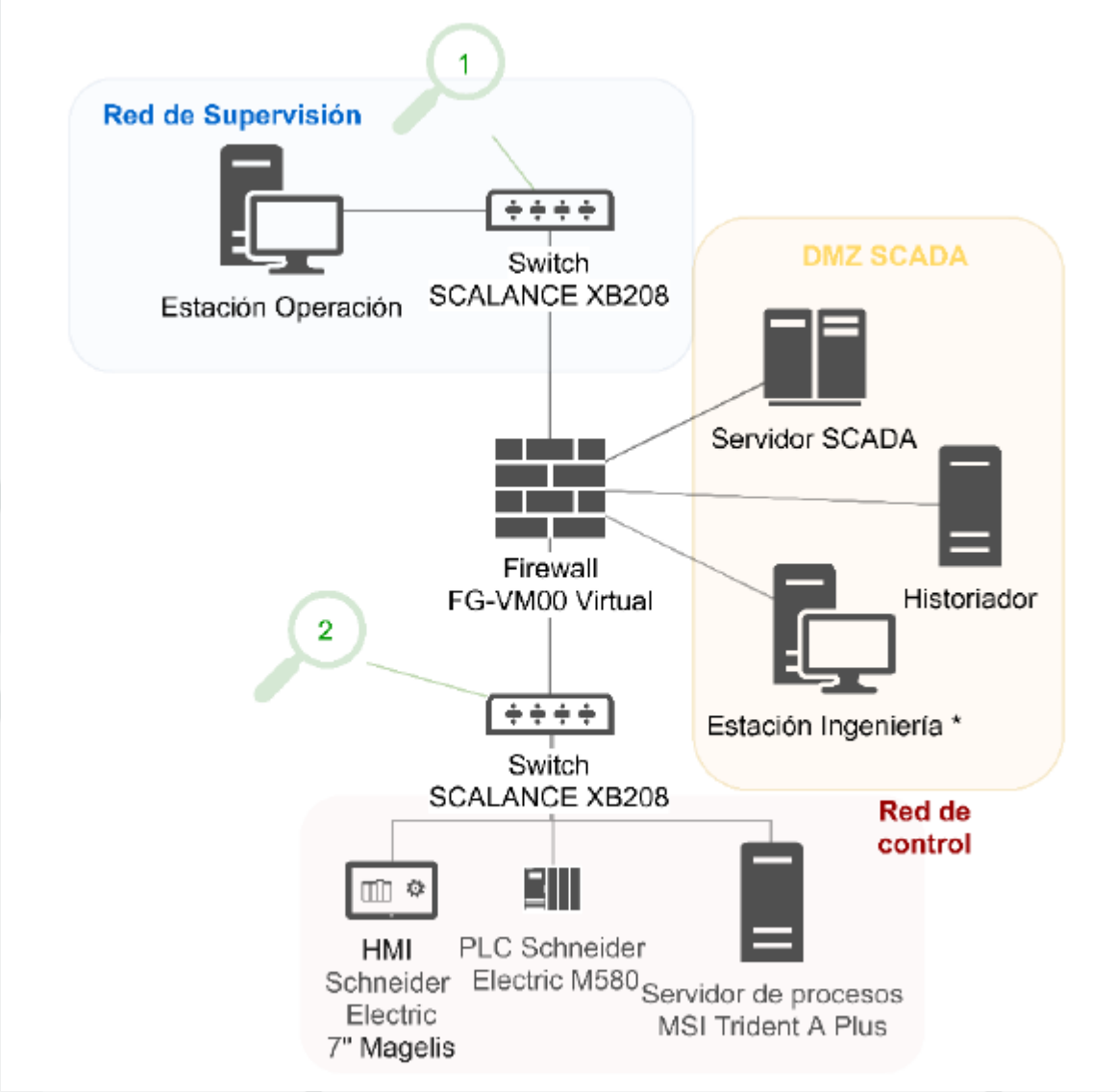
- ✓ Por otro lado, las redes de supervisión y control del laboratorio se están monitorizadas por el LABORATORIO DE CIBERSEGURIDAD, de modo que el entorno podrá ser utilizado para realizar simulaciones de incidentes de ciberseguridad y ver cómo afectan a los procesos industriales para poder definir estrategias de defensa ante ataques cibernéticos. La generación de un entorno que recree los componentes de una industria real, permite establecer e investigar sobre metodologías y políticas de ciberseguridad de los equipos utilizados para la operación y supervisión del proceso o electrónica de red, como el bastionado de equipos.



Laboratorio Demostrador Virtual

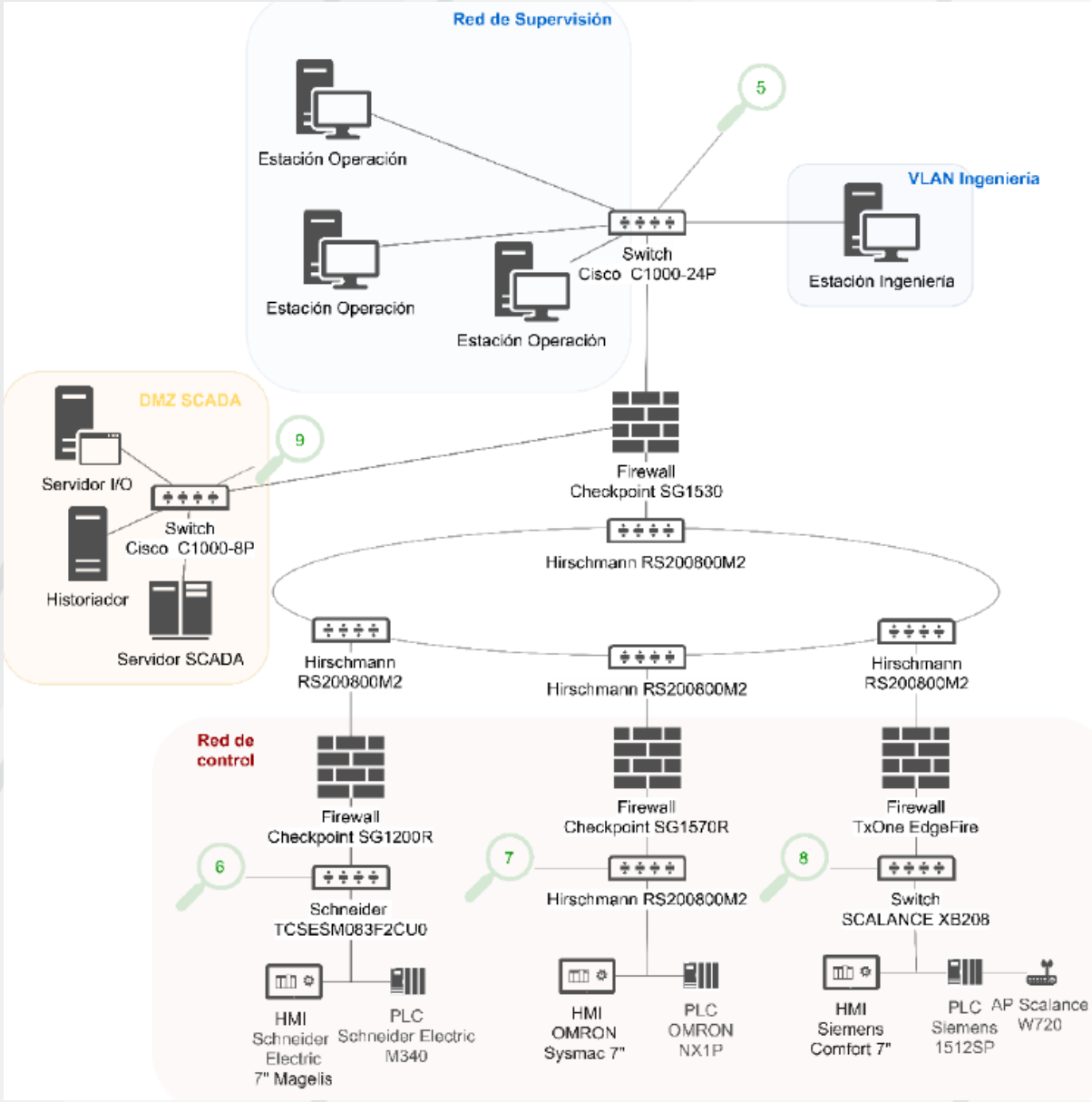
Casos de uso

- ✓ Entorno transportable sobre el que realizar sesiones de formación en ciberseguridad industrial fuera de sus laboratorios.
- ✓ El laboratorio permite realizar pruebas de intrusión sobre los sistemas de control industrial y simular incidentes de ciberseguridad para comprobar la afectación sobre los procesos.
- ✓ Pruebas sobre los dispositivos encargados de segmentar las redes y sobre la configuración de los equipos para comprobar las consecuencias reales de la materialización de una amenaza bajo un entorno que no se encuentra debidamente configurado.



Laboratorio Tecnológico
Casos de Uso

- ✓ Laboratorio modular para probar diferentes escenarios y configuraciones para comprobar como afectarían cuando un ataque cibernético se produce
- ✓ Diferentes fabricantes, permite evaluar nuevas medidas y funcionalidades de seguridad que se hayan desarrollado para la industria, permitirá realizar comparaciones técnicas sobre equipamiento y propuestas de fabricantes a nivel de ciberseguridad y evaluarlos
- ✓ Analizar diferentes arquitecturas y estrategias de defensa para cada uno de los entornos (configuración de firewalls, segmentaciones de red, parcheo de sistemas, etc.)
- ✓ Pruebas de carga y test de estrés sobre elementos de la red y equipamiento industrial, así como permitir el análisis o evaluación de las soluciones crecientes para la digitalización de los sistemas de control asociados a la INDUSTRIA 4.0



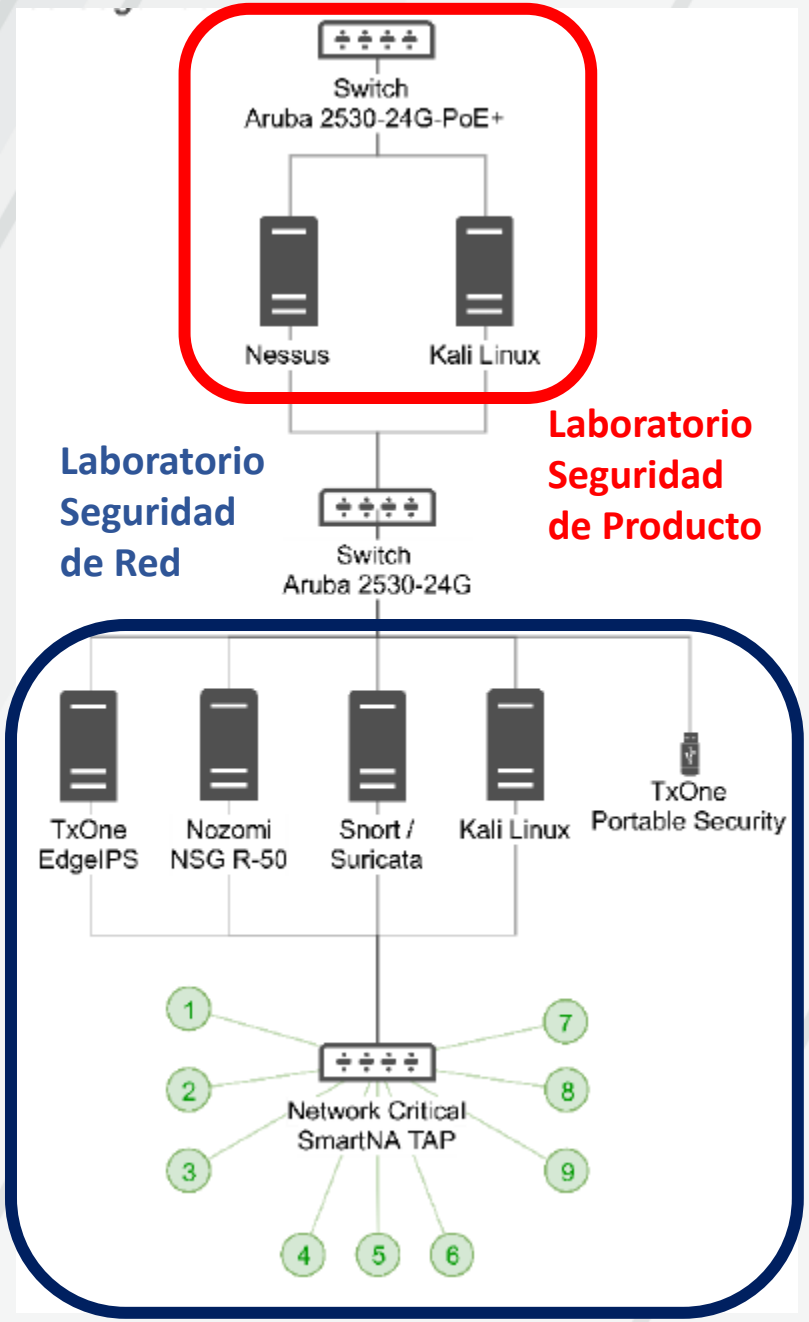
Laboratorio de CiberSeguridad

Casos de Uso

Se integran todas las herramientas necesarias para realizar evaluaciones de pentesting y hacking ético sobre dispositivos industriales y nuevas arquitecturas de red.

La integración de este laboratorio permitirá:

- Evaluación de funcionalidades y medidas de ciberseguridad desarrolladas en dispositivos industriales
- Realizar comparaciones de ciberseguridad sobre equipamiento industrial que proporcionen una misma solución técnica.
- Desarrollar estrategias de defensa para los entornos industriales a partir del análisis de amenazas conocidas.
- Probar nuevas soluciones de ciberseguridad adaptadas a los entornos industriales
- Identificación de malas prácticas de seguridad como uso de protocolos de comunicación inseguros, segmentación de red inadecuada o mala configuración de equipos.
- Detección de malware en equipamiento industrial
- Búsqueda de vulnerabilidades de software sobre equipamiento industrial y electrónica de red.



Opciones de uso del Laboratorio

Laboratorio ICS

¿ Eres una Empresa Industrial Gipuzkoana?

¿Cómo puedes usar el Laboratorio?

ENTORNO SEGURO

- Testear la Ciberseguridad de tus productos y tus desarrollos
- Conocer Nuevas Tecnologías
- POCs
- Formación Interna
- Comparar Tecnologías de CiberSeguridad de 3os

¿ Eres un Fabricante Industrial?

¿Cómo puedes usar el Laboratorio?

SHOWROOM

- Enseñar a clientes nuevos productos, desarrollos
- Entorno Real y controlado
- Demostrar Productos
- Validar Integraciones en entorno OT

¿ Eres un Fabricante de CiberSeguridad?

¿Cómo puedes usar el Laboratorio?

PRUEBAS DE CONCEPTO

- Enseñar a clientes nuevos productos, desarrollos
- Entorno Real y controlado
- Demostrar integración segura de tus Productos en OT
- Integración con otros fabricantes

¿ Eres un Integrador?

¿Cómo puedes usar el Laboratorio?

LABORATORIO PROPIO

- Enseñar a clientes nuevos productos, desarrollos
- Entorno Real y controlado
- Demostrar tus capacidades
- Demostración Portfolio Completo – Integraciones entre productos
- Formación Interna
- POCs

¿ Eres un Centro de Formación o Universidad?

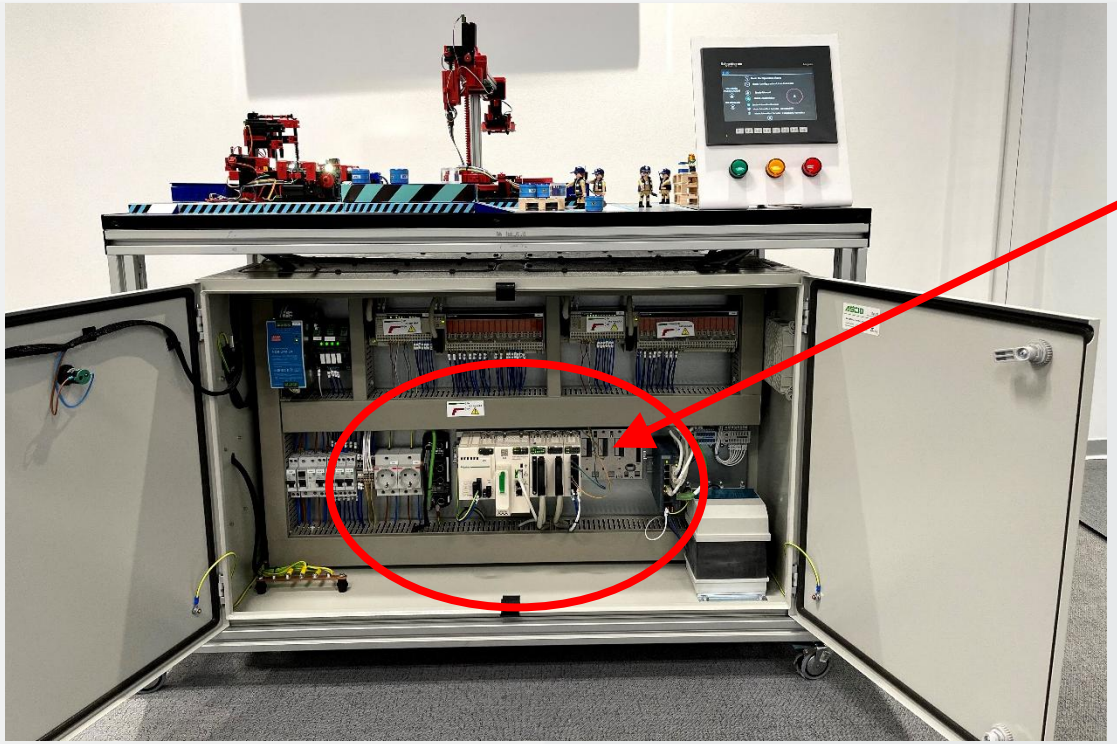
¿Cómo puedes usar el Laboratorio?

LABORATORIO PARA PRACTICAS

- Formación en diferentes tecnologías de automatización
- Formación en diferentes fabricante industriales
- Formación en tecnologías de ciberseguridad
- Posibilidad de modificar el entorno y configuración de los dispositivos para prácticas

Simulación de un ataque ICS

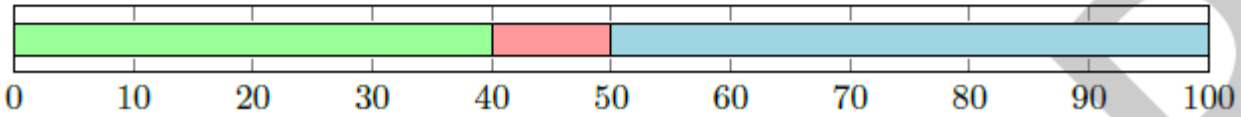
Laboratorio ICS



Vulnerability	Severity
Wind River VxWorks CVE-2008-2476	High
Wind River VxWorks CVE-2010-2966	High
Wind River VxWorks CVE-2010-2967	High
Wind River VxWorks CVE-2010-2968	High
Wind River VxWorks CVE-2015-7599	High
Wind River VxWorks CVE-2020-11440	Medium

OWASP TOP 10 INTERNET OF THINGS 2018

Published by	OWASP - The Open Web Application Security Project Foundation
Published on	2018-10-14
Rules violated	1
Manual checks required	5



Tableros KIPS - KASPERSKY

KIPS muestra lo siguiente:

- La función que juega la ciberseguridad en la continuidad y rentabilidad del negocio.
- Los desafíos y amenazas emergentes que enfrentan las empresas.
- Los errores típicos que cometen las empresas al construir su ciberseguridad.
- Cómo la cooperación entre los equipos comerciales y de seguridad permite mantener las operaciones estables y una protección sostenida contra las ciberamenazas.

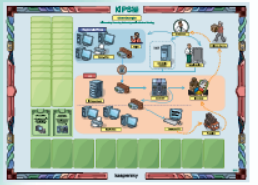
Según la situación, los equipos son responsables de la seguridad de TI de la empresa en esa industria. Su tarea es garantizar el funcionamiento normal y sin interrupciones de la empresa, mantener las relaciones con clientes y proveedores, y encontrar y neutralizar las ciberamenazas.

Cuando la empresa sufre un ciberataque, los participantes experimentan el impacto que tiene en la producción y los ingresos, y aprenden a adoptar distintas estrategias y soluciones de negocios e IT para minimizar los efectos negativos y seguir obteniendo dinero.

El GANADOR es el equipo que termine la partida con más ingresos, después de haber encontrado y analizado todas las trampas del sistema de ciberseguridad y haber respondido adecuadamente.

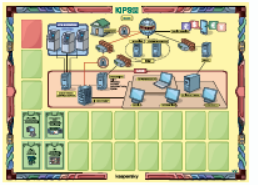
Situaciones de KIPS para empresas de todos los sectores verticales

Sociedad



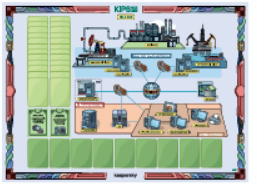
Protege la empresa frente a **ransomware, APT, errores de seguridad de automatización.**

Banco



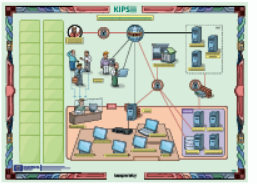
Protege las instituciones financieras contra **APT emergentes de alto nivel, como Tyukpin, Carbanak.**

Petróleo y gas



Examina el impacto de diversas amenazas, desde **la desfiguración del sitio web hasta un ransomware real y una sofisticada APT.**

Administraciones públicas locales



Protege los servidores web públicos frente a ataques y exploits.

Central eléctrica

Protege los sistemas de control industrial y las infraestructuras críticas de ciberataques del tipo Stuxnet.

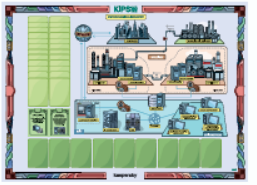
Planta de tratamiento de agua

Protege la infraestructura de TI de una planta de purificación de agua y garantice la estabilidad de dos líneas de producción.

Holding de petróleo

Garantiza la ciberseguridad para proteger los ingresos de una empresa petrolera y de energía internacional con oficinas en todo el mundo.

Industria petroquímica



Garantiza el funcionamiento normal de la nueva sucursal de una gran compañía petroquímica que se centra en la producción de etileno.

Table 4.2 – *Continued from previous page*

CVE-ID	Description	Severity	Vulnerable version(s)
CVE-2010-2967 Published on 2010-08-05	The loginDefaultEncrypt algorithm in loginLib in Wind River VxWorks before 6.9 does not properly support a large set of distinct possible passwords, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session. *According to the vulnerability's CVSSv2 rating, the vulnerability can be exploited remotely.*	High	6.4
CVE-2010-2968 Published on 2010-08-05	The FTP daemon in Wind River VxWorks does not close the TCP connection after a number of failed login attempts, which makes it easier for remote attackers to obtain access via a brute-force attack. *According to the vulnerability's CVSSv2 rating, the vulnerability can be exploited remotely.*	High	6.4
CVE-2015-7599 Published on 2017-02-07	Integer overflow in the _authenticate function in svc_auth.c in Wind River VxWorks 5.5 through 6.9.4.1, when the Remote Procedure Call (RPC) protocol is enabled, allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a username and password. *According to the vulnerability's CVSSv2 rating, the vulnerability can be exploited remotely.*	High	6.4
CVE-2020-11440 Published on 2020-07-23	httpRpmFs in WebCLI in Wind River VxWorks 5.5 through 7 SR0640 has no check for an escape from the web root. *According to the vulnerability's CVSSv2 rating, the vulnerability can be exploited remotely.*	Medium	6.4

CVE-ID	Description	Severity	Vulnerable version(s)
CVE-2008-2476 Published on 2008-10-03	The IPv6 Neighbor Discovery Protocol (NDP) implementation in (1) FreeBSD 6.3 through 7.1, (2) OpenBSD 4.2 and 4.3, (3) NetBSD, (4) Force10 FTOS before E7.7.1.1, (5) Juniper JUNOS, and (6) Wind River VxWorks 5.x through 6.4 does not validate the origin of Neighbor Discovery messages, which allows remote attackers to cause a denial of service (loss of connectivity) or read private network traffic via a spoofed message that modifies the Forward Information Base (FIB). *According to the vulnerability's CVSSv2 rating, the vulnerability can be exploited remotely.*	High	6.4
CVE-2010-2966 Published on 2010-08-05	The INCLUDE_SECURITY functionality in Wind River VxWorks 6.x, 5.x, and earlier uses the LOGIN_USER_NAME and LOGIN_USER_PASSWORD (aka LOGIN_PASSWORD) parameters to create hardcoded credentials, which makes it easier for remote attackers to obtain access via a (1) telnet, (2) rlogin, or (3) FTP session. *According to the vulnerability's CVSSv2 rating, the vulnerability can be exploited remotely.*	High	6.4

ZIUR
INDUSTRIAL CYBER SECURITY
CENTER-GIPUZKOA

Eskerrik asko