PROYECTO INFORMÁTICA 2026

Bachillerato Técnico Profesional

Soporte Técnico Informático

INSTITUTO TECNOLÓGICO SUPERIOR

ARIAS - BALPARDA

ANEP | UTU | DIRECCIÓN GENERAL DE EDUCACIÓN TÉCNICO PROFESIONAL

its tu futuro

Tramo 8 | Grado 3°

BTP Soporte y Mantenimiento informático 3ºDQ

Instituto Tecnológico Superior

“Arias - Balparda”

2026

Índice

1. Fundamentación del proyecto

1.1 Presentación general

El Proyecto de Laboratorio de Informática Inteligente y Alta Disponibilidad, en adelante **PLIIAD**, es una propuesta técnica, operativa y sostenible orientada a la reestructuración integral de las tecnologías de la información y a la automatización de la infraestructura educativa. Este proyecto busca resolver una necesidad crítica: establecer un marco de trabajo integrado y estandarizado para la implementación de un laboratorio de informática que sea plenamente operativo, inteligente y seguro. Su propósito es evitar que las salas tecnológicas operen de forma aislada, transformándose en entornos que automaticen el control de sus recursos y garanticen la trazabilidad absoluta en la gestión de los servicios informáticos.

El proyecto parte de una realidad actual diagnosticada en la institución educativa, la cual presenta una infraestructura tecnológica fragmentada e ineficiente. Actualmente, el laboratorio de informática carece de un sistema centralizado para la gestión de incidentes técnicos (Help Desk), lo que provoca notorias demoras en el soporte al usuario y una preocupante falta de trazabilidad en las reparaciones lógicas y físicas. A nivel de entorno físico, la sala no cuenta con controles automatizados, lo que deriva en un gasto energético innecesario por concepto de luces y equipamiento encendidos sin uso, además de riesgos críticos para la integridad del hardware debido a la total falta de monitoreo térmico en los racks y de seguridad en el acceso físico a la dependencia. Asimismo, la ausencia de un protocolo de validación sistemático impide asegurar que el software desplegado sea estable o que el hardware reciclado haya sido debidamente sanitizado antes de su puesta en producción.

El PLIIAD propone un abordaje práctico e interdisciplinario liderado por el equipo de estudiantes, quienes actúan bajo la dinámica de una consultora de TI. La intervención no se limita únicamente a realizar una instalación convencional de equipos, sino que abarca el diseño, la implementación y la validación de un Laboratorio de Informática 4.0. Esta solución integra una infraestructura de red estable y resistente a fallas o intentos de acceso no autorizado; una arquitectura de servidores robusta armada sobre virtualización y administración automatizada por scripts; una capa de domótica basada en STEM+ con la placa micro:bit para la eficiencia energética; y un proceso formal de Testing y Aseguramiento de la Calidad (QA). De esta forma, el proyecto no solo optimiza el rendimiento y la seguridad

del laboratorio del centro educativo, sino que establece un modelo de gestión de alta disponibilidad, seguro y eficiente bajo normas internacionales.

1.2 Necesidad tecnológica y social

En el escenario contemporáneo, la convergencia entre la disponibilidad de los servicios informáticos, la seguridad de la información y la optimización de los recursos físicos es fundamental para el desarrollo de cualquier organización. Las instituciones de enseñanza, los entornos corporativos y los organismos públicos se ven orillados a migrar hacia infraestructuras centralizadas y de alta disponibilidad para sostener sus flujos operacionales diarios. Sin embargo, los procesos de actualización técnica suelen implementarse de forma aislada y reactiva (a medida que ocurre un problema, se plantea una solución, en lugar de aplicar medidas de prevención), priorizando la resolución inmediata de fallas superficiales mientras se descuida la integración sistémica, el monitoreo proactivo y el control eficiente del entorno.

Este enfoque desarticulado se traduce en deficiencias operacionales concretas dentro del ámbito institucional:

- Expone a la organización a tiempos de inactividad prolongados debido a la ausencia de un canal centralizado de incidencias (Help Desk), lo que anula la trazabilidad de los soportes técnicos y fragmenta la gestión del mantenimiento.
- Provoca un consumo eléctrico desmedido y económicamente insostenible al mantener luminarias y estaciones de trabajo encendidas durante horarios no operativos por falta de automatización.
- Somete a los componentes activos alojados en los racks (servidores, switches, routers) a fallas catastróficas por sobrecalentamiento, debido a la inexistencia de sistemas de control térmico.
- Debilita el resguardo del equipo informático al carecer de un control de acceso físico automatizado y seguro a las salas técnicas del centro.
- Impide garantizar la estabilidad de las aplicaciones desplegadas y la integridad de los datos, al no contar con protocolos rigurosos de validación de software ni de sanitización forense para discos duros reciclados.

Mediante la estructuración de este modelo, el proyecto busca estandarizar y democratizar las metodologías de despliegue de centros de cómputos inteligentes. Su propósito es proporcionar un marco de trabajo técnico y metodológico que sea perfectamente replicable en otros laboratorios de la red de UTU, instituciones educativas públicas, así como en pequeñas y medianas empresas (pymes) que requieran modernizar su infraestructura crítica con un presupuesto optimizado.

La solución diseñada por la consultora trasciende la instalación convencional de software o el montaje físico de terminales. El proyecto propone una intervención integral sobre el espacio físico y lógico desde una perspectiva general, donde la automatización domótica, el aislamiento de servicios, la seguridad perimetral y la auditoría sistemática cooperan para construir un entorno tecnológico resistente, seguro y energéticamente responsable.

1.3 Problema a resolver

El problema principal que aborda este proyecto es la falta de un marco de trabajo integrado y estandarizado para la implementación, gestión y aseguramiento de un laboratorio de informática que funcione de manera plenamente operativa, inteligente y segura.

Actualmente, ante la ausencia de una metodología centralizada, la gestión tecnológica e infraestructural de la sala se enfrenta a situaciones críticas como las siguientes:

- Para reportar o solucionar un problema técnico, los usuarios y el personal no disponen de un sistema centralizado de gestión de incidentes (Help Desk), lo que genera demoras severas en la asistencia técnica y una total falta de trazabilidad en el historial de reparaciones físicas y lógicas.
- Para regular el entorno de la sala, no se cuenta con automatizaciones ni sensores, lo que deriva en un gasto energético innecesario e ininterrumpido al mantenerse luminarias y terminales encendidas fuera de los horarios de clase.
- Para proteger la integridad física de la infraestructura central, los racks de comunicaciones carecen de sistemas de telemetría que alerten sobre variaciones térmicas imprevistas, quedando vulnerables a fallas catastróficas por sobrecalentamiento.
- Para asegurar el patrimonio tecnológico del laboratorio, la dependencia carece de

mecanismos controlados que restrinjan el acceso físico de personal no autorizado a las áreas críticas del centro.

- Para desplegar nuevas soluciones lógicas o reutilizar hardware recuperado, no se aplican protocolos de validación sistemáticos que certifiquen la estabilidad del software instalado o garanticen la sanitización forense y segura de los datos remanentes en los soportes de almacenamiento.

La persistencia de estas problemáticas degrada la continuidad de los servicios digitales del instituto, debilita los niveles de ciberseguridad, incrementa sustancialmente los costos operativos y dificulta un flujo de trabajo profesionalizado. Por consiguiente, el PLIIAD se constituye como una solución integral que automatiza el espacio físico mediante un entorno físico y virtual, robustece la infraestructura de servidores a través de herramientas de virtualización y aplica procesos de testing sistemáticos para certificar la fiabilidad del laboratorio bajo estándares internacionales

1.4 Justificación del proyecto

El proyecto se justifica desde cuatro dimensiones principales:

Dimensión Tecnológica: Permite reforzar y aplicar de forma práctica destrezas avanzadas de informática, abarcando desde la segmentación de redes lógicas (VLANs) y el análisis de estabilidad ante ataques en entornos controlados, hasta la contenerización de servicios mediante Docker, el endurecimiento de accesos SSH y la destrucción forense de datos bajo el estándar internacional NIST SP 800-88. Esto desplaza las configuraciones tradicionales hacia una arquitectura moderna de infraestructura digital

Dimensión Educativa: Funciona como el escenario de convergencia e integración curricular definitiva para las asignaturas técnicas del trayecto: UTULAB, Laboratorio STEM+, Taller de Soporte Técnico, Instalación y Configuración de Sistemas Operativos, y Laboratorio de Testing (QA), en perfecta comunicación con la asignatura de profundización (Laboratorio de Sistemas Operativos). Este enfoque sumerge a los estudiantes en un entorno que emula las dinámicas reales de una consultora de TI, desarrollando competencias críticas alineadas a las demandas actuales de la Industria 4.0

Dimensión Organizativa: Introduce una transformación en la gobernanza operativa de los recursos técnicos del instituto, sustituyendo las metodologías reactivas por un sistema

centralizado de gestión de incidentes (Help Desk) que garantiza la trazabilidad del soporte. Asimismo, optimiza la resiliencia física de la sala al incorporar telemetría térmica en los racks para prevenir fallas de hardware y reduce los costos económicos del centro mediante la automatización inteligente del consumo eléctrico.

Dimensión Social: Aporta valor directo a la comunidad educativa al resguardar la privacidad de la información institucional y proteger el patrimonio físico del laboratorio a través de un control de acceso automatizado y seguro. De igual modo, promueve la responsabilidad ética y el compromiso ambiental entre los usuarios, demostrando que la alta disponibilidad y la ciberseguridad pueden coexistir con el uso inteligente de la energía y la sostenibilidad tecnológica

2. Objetivos del proyecto

2.1 Objetivo general

Diseñar, implementar y validar un Laboratorio de Informática Inteligente y de Alta Disponibilidad (PLIIAD) mediante la simulación de una consultora de TI, integrando una infraestructura de red estable y segura, una arquitectura de servidores virtualizada y automatizada, y un entorno físico-virtual domótico orientado a la eficiencia energética, garantizando la fiabilidad de todo el ecosistema tecnológico bajo estrictos estándares internacionales de calidad y testing.

2.2 Objetivos específicos

El proyecto deberá cumplir con los siguientes objetivos específicos:

- Diseñar y estructurar la topología física y lógica de la red del laboratorio, implementando una segmentación estricta mediante subredes o VLAN para aislar el tráfico administrativo, de estudiantes, de servidores y de dispositivos IoT .
- Evaluar la estabilidad y la respuesta defensiva de la infraestructura de red mediante mediciones matemáticas de latencia, pérdida de paquetes y disponibilidad, en conjunto con simulaciones controladas de amenazas perimetrales (escaneo de puertos e intentos de acceso no autorizados)

- Desplegar una arquitectura de servidores corporativos robusta utilizando virtualización y el software de gestión de incidentes (hay soluciones ya realizadas en el mercado, como GLPI, osTicket, Zammad, entre otras, que pueden ser autoalojadas).
- Automatizar las tareas del Centro de Cómputos y la continuidad del negocio, mediante el desarrollo de scripts avanzados en bash para la gestión de usuarios y la ejecución de políticas de respaldos (backups) remotos.
- Transformar el espacio físico del laboratorio en un entorno domótico, mediante la placa programable micro:bit y una red de sensores/actuadores orientados a la climatización inteligente, el ahorro energético y el control de acceso restringido
- Construir el prototipo de automatización física bajo criterios de sostenibilidad, utilizando componentes mecánicos y estructuras recuperadas del desguace técnico de hardware en desuso .
- Diseñar y ejecutar un Plan de Pruebas funcionales de software (Testing de caja negra), para validar rigurosamente la interfaz, la base de datos y los flujos críticos del sistema de Help Desk instalado.
- Asegurar la destrucción confidencial de la información institucional, aplicando protocolos de borrado seguro y sanitización forense en discos duros reciclados bajo las directrices del estándar internacional NIST SP 800-88
- Consolidar las evidencias y la gobernanza del proyecto, mediante la creación de registros de auditoría (QA Logs), tableros de control estadísticos (QA Dashboard) y la emisión de reportes técnicos individuales de aceptación para la puesta en producción de los equipos
- Elaborar la documentación técnica y los manuales de procedimiento, integrando planos de red, bitácoras de intervención, diagramas de bloques y memorias descriptivas que aseguren la escalabilidad de todo el ecosistema tecnológico implementado

3. Público objetivo

El PLIIAD estará orientado a los siguientes tipos de usuarios u organizaciones:

- El propio centro (ITS) se verá directamente beneficiado al contar con un aula informatizada de alto rendimiento, un canal formal para canalizar sus reportes de

fallas y un entorno automatizado que cuide los activos informáticos

- Técnicos o encargados de la sala que requerirán interfaces de consola simplificadas y scripts automatizados para la administración diaria de los usuarios y las copias de seguridad sin necesidad de realizar tareas manuales complejas
- Alumnos y docentes de diversas asignaturas que utilizarán las terminales del laboratorio y requerirán un entorno de red estable, conectividad de baja latencia y un sistema de gestión accesible para notificar cualquier desperfecto en sus sesiones de trabajo
- Autoridades que necesiten auditar de forma transparente el rendimiento de la infraestructura, controlar el gasto energético de la sala, verificar la seguridad física de los accesos y contar con reportes de calidad que avalen el estado del equipamiento
- Organizaciones externas que busquen un modelo de infraestructura y metodológico de referencia, económico y eficiente, para replicar soluciones de virtualización, domótica y testing en sus propias instalaciones

El proyecto deberá diseñarse considerando que el abanico de usuarios finales presentará diferentes niveles de alfabetización digital y técnica. Por esta razón, el sistema de interfaces del Help Desk debe ser intuitivo y de fácil navegación, los paneles de control automatizados para los operadores deben incluir menús interactivos claros por consola, y las señalizaciones físicas e indicadores visuales de la automatización domótica en la sala deben ser autoexplicativos, garantizando que cualquier usuario comprenda las alertas de temperatura o las restricciones de acceso sin requerir conocimientos especializados

4. Alcance del proyecto

El proyecto se centrará en el diseño, la implementación, el monitoreo y la validación de la infraestructura de red, la arquitectura de servidores y la automatización física del espacio asignado, bajo un marco formal de aseguramiento de la calidad. El desarrollo técnico de la consultora abarca las siguientes áreas operacionales y componentes mínimos como protocolo de acción:

- **Infraestructura, Conectividad y Ciberseguridad Perimetral:**
    - Diseño lógico y físico de la topología de red, incluyendo servidores, estaciones de trabajo, dispositivos IoT, sistema Help Desk y accesos remotos seguros.

- Segmentación estricta de la red del laboratorio mediante VLANs o subredes para separar de manera aislada las zonas Administrativa, de Estudiantes, de Servidores e IoT
- Configuración avanzada de los dispositivos activos de red (switches, routers) y de los servicios de infraestructura esenciales (DHCP, DNS y Gateway)
- Análisis de estabilidad y carga de la red mediante pruebas de conectividad
- Ejecución de simulaciones controladas de amenazas (escaneo de puertos, contraseñas débiles e intentos de acceso SSH no autorizado) e implementación de la respuesta defensiva del sistema a través de reglas de firewall, endurecimiento de contraseñas y auditoría profunda de logs

- **Arquitectura de Servidores, Virtualización y Automatización Lógica:**
  - Justificación técnica de la selección de sistemas operativos tanto para el servidor corporativo como para las estaciones de trabajo, definiendo detalladamente los roles de usuario, niveles de acceso y privilegios
  - Gestión avanzada de almacenamiento en servidores y clientes, aplicando conceptos estructurados de particionamiento de disco y selección de sistemas de archivos adecuados
  - Despliegue y configuración de la plataforma de contenedores Docker para soportar, aislar y ejecutar de forma eficiente las imágenes y microservicios asociados al software de Help Desk
  - Desarrollo de un menú interactivo avanzado en bash para el operador del centro de cómputos, automatizando mediante tareas el alta, baja, consulta y modificación de usuarios y servicios.
  - Programación de scripts automatizados en bash para la ejecución de políticas de respaldos (backups) periódicos que realicen el empaquetado y transferencia remota de datos críticos hacia un almacenamiento seguro.
- **Entornos físicos, Domótica y Sostenibilidad:**
  - Diseño y desarrollo de una interfaz físico-virtual basada en la placa programable micro:bit para automatizar la climatización, el ahorro energético y el control de acceso a la sala
  - Programación de la lógica de control del sistema domótico implementando el uso de variables, control de flujo y funciones en el código fuente (bloques o scripts).
  - Integración de componentes electrónicos y sensores (temperatura, movimiento

o presencia) combinados con actuadores para dar respuesta automática a los estímulos del medio

- Construcción de un prototipo físico operativo y ensamblado que represente la automatización de la sala, priorizando el uso de materiales recuperados del desguace técnico y componentes mecánicos de hardware en desuso

5. Tecnologías a utilizar

- **Componentes Pasivos:** Cableado estructurado de par trenzado (Categorías 5e o 6), conectores RJ-45, canalizaciones plásticas, perfiles de distribución y racks de comunicaciones para el alojamiento centralizado del equipamiento.
- **Herramientas de Análisis y Simulación:** Comandos nativos de diagnóstico por consola, analizadores de protocolos de red para el monitoreo de tráfico y software de modelado de topologías (como Cisco Packet Tracer).
- **Unidades de procesamiento:** Placas de desarrollo programables micro:bit.
- **Plataformas de Gestión de Servicios:** Soluciones de código abierto auto alojadas (Self-Hosted) para la gestión de incidentes (como GLPI o osTicket), utilizadas para la validación de flujos de trabajo en pruebas de caja negra.
- **Seguridad y Sanitización:** Herramientas de software para el borrado seguro y destrucción lógica de datos (como DBAN, Rufus o comandos dd en entornos Linux) aplicadas a discos duros y unidades de almacenamiento.

6. Documentación obligatoria

El proyecto deberá entregar un cuerpo documental estructurado, claro y suficiente que permita comprender, ejecutar, mantener y auditar tanto las intervenciones de infraestructura lógica y física como los procesos de automatización y aseguramiento de la calidad en el laboratorio.

6.1 Documentación funcional y de relevamiento

Deberá incluir:

- Descripción detallada del diagnóstico inicial y las vulnerabilidades detectadas en el laboratorio actual.
- Objetivos generales, específicos y alcances delimitados
- Estructura orgánica del equipo, detallando los roles profesionales de cada integrante y las responsabilidades asumidas.
- Marco conceptual del Laboratorio 4.0 y justificación socio-tecnológica del entorno.
- Estudio de viabilidad comercial, legal (Ley N.º 18.331 de Protección de Datos Personales) y constitución formal bajo la figura jurídica correspondiente.
- Modelado de los flujos de atención y procesos de escalabilidad ante la apertura y cierre de incidentes en la plataforma de servicios.

6.2 Documentación Técnica de Infraestructura y Sistemas

Deberá incluir:

- Planos de la arquitectura general de la red, especificando las topologías físicas y lógicas implementadas.
- Esquema de direccionamiento IP y matriz de segmentación por subredes o VLANs (Administrativa, Estudiantes, Servidores e IoT).
- Manual técnico de instalación paso a paso del sistema operativo del servidor, con su correspondiente esquema de particionado de discos.
- Código fuente documentado de los scripts avanzados en bash desarrollados para la automatización de tareas de usuarios y la ejecución de respaldos remotos.
- Diagramas de bloques lógicos, esquemas de conexión electrónica y código fuente (en bloques o scripts) desarrollado para la placa micro:bit.
- Memoria descriptiva de los materiales reciclados y componentes mecánicos integrados en el prototipo físico domótico.

6.3 Documentación de Aseguramiento de la Calidad (QA) y Ciberseguridad

Deberá incluir:

- Plan de Pruebas formal de caja negra diseñado para evaluar las funciones críticas de la interfaz web y bases de datos del Help Desk.
- Historial técnico unificado (QA Logs) que registre la ejecución de los casos de prueba, identificación de defectos ("No Conformidades") y sus respectivos re-testeos.
- Listas de verificación técnicas estructuradas en formato binario (cumple / no cumple) aplicadas a la certificación del hardware y estaciones de trabajo.
- Métricas matemáticas del análisis de estabilidad de red (latencia, pérdida de paquetes y disponibilidad) e informes de pruebas de carga por concurrencia.
- Reportes de auditoría perimetral que documenten la respuesta defensiva del firewall y el análisis de logs ante las simulaciones de ataques controlados.
- Certificados e informes técnicos de sanitización digital y destrucción confidencial de datos bajo el estándar **NIST SP 800-88**.
- Tablero estadístico (QA Dashboard) y Reportes de Aceptación individuales firmados por la consultora para habilitar la puesta en producción del laboratorio.

6.4 Manual de procedimientos y usuario

Deberá explicar detalladamente al operador y al usuario cómo:

- Acceder, navegar e interactuar correctamente con la plataforma de Help Desk para la apertura, seguimiento y cierre de tickets de incidentes.
- Ejecutar e interactuar con el menú modular por consola en bash para la gestión automatizada de usuarios en el servidor.
- Iniciar y restaurar las copias de seguridad de los datos institucionales a partir de los scripts automatizados.
- Interpretar los indicadores visuales, alertas térmicas y códigos de error del sistema domótico en la sala.
- Operar de forma segura los actuadores y los mecanismos de control de acceso físico del laboratorio inteligente.
- Seguir las directrices de mantenimiento preventivo, ergonomía del aula y normativas de seguridad eléctrica de la infraestructura tecnológica.

7. Exclusiones del sistema

Para evitar ambigüedades técnicas y delimitar con precisión el campo de acción de la consultora de TI, se establece de manera estricta que el **PLIIAD** no incluirá los siguientes componentes, servicios ni desarrollos:

- No se programará una aplicación web ni un sistema propio para la gestión de incidentes o inventario; el alcance técnico en esta área se limita exclusivamente al despliegue, parametrización y aseguramiento de la calidad de plataformas de código abierto existentes (Self-Hosted) como GLPI u osTicket.
- Las soluciones de control ambiental y de acceso de la unidad no pretenden una instalación comercial o cableado eléctrico de alta potencia para todo el centro educativo. Las intervenciones se limitan a un prototipo funcional a escala basado en la placa micro:bit.
- Queda fuera del alcance la programación de software para dispositivos móviles destinados a controlar los sensores o interactuar con la mesa de ayuda.
- El mantenimiento del equipamiento se enfoca en el diagnóstico, limpieza, optimización y descarte seguro; no se realizarán tareas de microsoldadura electrónica avanzada, sustitución de capacitores en placas base ni otra actividad similar.
- El manejo de materiales se limita de forma exclusiva a la economía circular local (recuperación de piezas mecánicas en desuso y la sanitización forense de discos reciclados).
- El diseño e implementación de la red física del laboratorio se concentra estrictamente en la conectividad por cableado estructurado de cobre (categorías 5e o 6) y enlaces inalámbricos internos, excluyendo fusiones de fibra o tendidos troncales WAN.

8. Requerimientos de funcionamiento empresarial

La ejecución de este proyecto se articulará bajo la simulación de una empresa de Servicios de Integración Tecnológica, constituida formalmente con el propósito de dar respuesta a las demandas infraestructurales, de automatización y de aseguramiento de la calidad del centro educativo.

Como parte de la propuesta corporativa, la consultora presentará un análisis detallado y recomendaciones específicas para el despliegue del equipamiento de red, servidores y sistemas domóticos, estructurando su funcionamiento en base a los siguientes parámetros esenciales:

- **Costos y Presupuestación:** Elaboración de un presupuesto comercial desglosado que contemple los costos de hardware activo y pasivo, licenciamiento de código abierto, componentes electrónicos, herramientas de campo y la estimación de horas de servicio técnico, optimizando la inversión mediante soluciones rentables como la virtualización.
- **Claridad Expositiva y Planificación:** Presentación estructurada de la propuesta técnica y comercial a través de un cronograma de hitos, detallando con precisión las fases de relevamiento, el aprovisionamiento de servidores, las ventanas de pruebas (testing) y la puesta en producción del laboratorio sin interrumpir las actividades académicas.
- **Documentación Presentada:** Entrega formal de una carpeta técnica de ingeniería que consolide las políticas de respaldo, guías de sistemas, planos de infraestructura, registros de auditoría (QA Logs) y manuales operativos.
- **Amigabilidad y Usabilidad del Sistema:** Diseño centrado en el usuario final. Esto implica una interfaz limpia e intuitiva para el sistema de Help Desk autoalojado, menús interactivos por consola en bash autoexplicativos para los operadores, indicadores visuales claros en el prototipo domótico y un etiquetado inequívoco del rack y cableado de la sala.
- **Utilización de Herramientas Gráficas:** Inclusión de diagramas de arquitectura lógica y física de red, esquemas de circuitos electrónicos para la placa micro:bit,

diagramas de flujo para los procesos de bash

- **Seguridad y Confidencialidad de Datos Sensibles:** Con el fin de blindar la responsabilidad legal de la institución y garantizar el cumplimiento de la Ley N.º 18.331 de Protección de Datos Personales en Uruguay, la consultora aplicará protocolos obligatorios de seguridad lógica.

9. Requerimientos distinguidos por asignatura

Estos requerimientos definen los componentes a entregar en cada una de las instancias. Los contenidos de las instancias son sumativos (en la segunda entrega se presentan los requerimientos corregidos de la primera completos y los nuevos de la segunda y en la tercera entrega se presentan los requerimientos corregidos de primera y segunda entrega completos en conjunto con la tercera entrega)

9.1 Componente TP

UTULAB

Entrega 1

Cada equipo deberá presentar los siguientes puntos:

- Nombre y logo de la empresa de TI (el equipo de alumnos), explicando de forma sencilla por qué eligieron ese diseño y qué rol va a cumplir cada integrante en el proyecto.
- Explicación de los problemas reales del salón: Detallar por qué es necesario arreglar la red, por qué hace falta instalar un sistema de tickets (Help Desk) para reportar fallas y para qué sirve automatizar el laboratorio.
- La meta principal del proyecto: Redactar el objetivo general y hacer una lista con los pasos o tareas principales que van a seguir para cumplir con los tiempos de entrega.

Entrega 2

Cada equipo deberá expandir el documento central incorporando:

- Leyes y normas obligatorias. Mencionar brevemente la ley uruguaya de protección de datos (para asegurar que cuidamos la información de la UTU) y la norma que explica cómo borrar discos duros de forma segura sin dejar rastro de datos viejos.
- Diagnóstico inicial del laboratorio. Una lista detallada de cómo encontraron el salón antes de trabajar (cuántas computadoras hay, el estado de los cables de red y qué materiales necesitan conseguir o reparar).

Entrega 3

Cada equipo deberá entregar el documento impreso definitivo que incluya:

- Resumen Ejecutivo de una sola página que explique de forma rápida y directa cuál era el problema del salón, qué herramientas instalaron y cómo quedó funcionando todo al final.
- Calendario y presupuesto final de los días que les llevó trabajar y una planilla con los costos simples de los materiales usados (cables, conectores, herramientas) demostrando que se ahorró dinero usando software gratuito.
- Matriz FODA del Proyecto. Un cuadro sencillo con las Fortalezas, Oportunidades, Debilidades y Amenazas que tuvo el equipo durante el año.
- Conclusiones y Reflexiones. Qué aprendió el grupo, qué cosas funcionaron bien y qué dificultades tuvieron que resolver para que el sistema de tickets y la red queden estables.
- Anexos y Fotos. Lista de las páginas web o libros consultados, fotos del proceso y capturas de pantalla del sistema de tickets ya instalado.

STEM+

Entrega 1

Cada equipo deberá presentar:

- Investigación sobre un problema específico del salón. Elegir un problema de la sala para resolver con tecnología (por ejemplo: el sobrecalentamiento de los servidores en el rack, el gasto innecesario de luz cuando el salón está vacío, o la falta de seguridad en la puerta de acceso).
- Diseño de la solución con la placa micro:bit. Explicar cómo la placa va a solucionar ese problema (por ejemplo: un extractor que se prende solo si sube la temperatura, luces inteligentes que se activan con movimiento, o una alarma con sensor de presencia para cuidar el rack).
- Diagramas y materiales reciclados. Dibujos sencillos de cómo se conectará todo y una lista de los materiales en desuso que planean rescatar para armar la maqueta (como ventiladores viejos de computadoras, luces LED de gabinetes rotos o plásticos).

Entrega 2

Cada equipo deberá presentar:

- Mostrar cómo están armando la maqueta o el tablero protector utilizando los plásticos, metales o partes de gabinetes viejos que recuperaron (fotos y capturas).
- Código fuente para la micro:bit: Entregar el programa desarrollado (en bloques de MakeCode o scripts de texto). El código debe ser sencillo pero ordenado

- Lista de componentes y primeras pruebas. Descripción de los sensores (temperatura, movimiento) y actuadores (motores, relés, alarmas) que conectaron, junto con una bitácora corta que anote los primeros intentos de prueba y los errores que tuvieron que corregir.

Entrega 3

Cada equipo deberá entregar:

- Prototipo definitivo. Presentar la maqueta o dispositivo electrónico-mecánico 100% armado y funcionando en tiempo real.
- Documento breve que explique cómo trabaja el hardware junto con el software, detallando los circuitos y la utilidad real que tiene para el cuidado del laboratorio.
- Registro en fotos y videos. Un archivo de fotos y un video corto (video de youtube) que demuestre claramente al sistema funcionando (por ejemplo: mostrando cómo al acercar calor al sensor, el ventilador de la micro:bit se enciende automáticamente).

Taller de soporte técnico

Entrega 1

Cada equipo deberá presentar:

- Diagrama de Red Completo con planos de la topología física y lógica de la sala, identificando switches, routers, gateways y los puntos críticos de conectividad.
- Segmentación de Red (VLANs/Subredes) con tabla de direccionamiento IP detallando la separación obligatoria de las 4 redes: Administrativa, Estudiantes, Servidores e IoT.
- Configuración de Servicios Esenciales. Capturas de pantalla o guías cortas de la configuración de los servicios básicos: DHCP, DNS, Switch y Router.

Entrega 2

Cada equipo deberá presentar:

- Informe de Estabilidad de Red. Resultados con métricas reales utilizando comandos como ping y traceroute para medir latencia, disponibilidad y pérdida de paquetes.
- Pruebas de Carga en el sistema Help Desk: Registro de cómo se comporta el sistema de tickets (GLPI/osTicket) cuando se simulan varios usuarios conectados a la vez, anotando si hubo caídas o demoras.

- Implementación de Monitoreo. Configuración de herramientas sencillas para detectar dispositivos conectados, controlar el consumo de ancho de banda y activar alertas si se cae algún servicio esencial.

Entrega 3

Cada equipo deberá presentar:

- Informe de las pruebas de seguridad controladas que hicieron dentro del aula (escaneo de puertos, pruebas de contraseñas débiles e intentos fallidos de conexión SSH no autorizada al servidor).
- Evidencias claras de cómo el firewall bloqueó los accesos indebidos y capturas de pantalla de los logs del sistema donde se registran esos intentos fallidos.
- Detalle de las reglas de seguridad aplicadas (fortalecimiento de contraseñas, corrección de permisos de usuarios) y consejos finales para mantener la red segura.

Instalación y configuración de sistemas operativos

Entrega 1

Cada equipo deberá presentar:

- Justificar de forma sencilla por qué eligieron cierta distribución de Linux para el servidor (ej. Ubuntu Server, Debian) y qué sistema operativo usarán las computadoras de los alumnos.
- Definición de roles y privilegios. Un cuadro que detalle los niveles de acceso (quién es Administrador, quién es Operador y qué permisos básicos tienen los Estudiantes en el laboratorio).
- Manual de Instalación y Almacenamiento. Guía paso a paso para instalar el sistema operativo del servidor desde cero. Debe incluir los requisitos de hardware y cómo se van a dividir los discos (particiones primarias/lógicas y la elección del sistema de archivos, como ext4).

Entrega 2

Cada equipo deberá presentar:

- Puesta a Punto y Seguridad Inicial. Evidencias de las actualizaciones del sistema, configuración de la red (IP fija, DNS) y activación del firewall local con políticas de contraseñas seguras.

- Menú Interactivo en bash. Código fuente y capturas de un script ejecutable en bash. Este menú debe permitir al operador del centro realizar específicamente: Altas, Bajas y Modificaciones de usuarios del sistema.
- Acceso Remoto Seguro por SSH. Configuración del servicio SSH para administrar el servidor a distancia.
- Documentar cómo aplicaron el borrado seguro de datos en caso de reutilizar discos duros viejos, asegurando que la información anterior se destruyó por completo antes de instalar el sistema.

Entrega 3

Cada equipo deberá presentar:

- Despliegue de la aplicación. Instalación del software Help Desk en el servidor, listo para recibir tickets.
- Política de Backups Automatizada. Un script en bash programado para ejecutarse solo (crontab). Debe empaquetar los datos críticos del Help Desk y simular o realizar la transferencia hacia un almacenamiento seguro (segunda máquina virtual).
- Un reporte que registre los errores de arranque o incompatibilidades de hardware que surgieron durante el proyecto y cómo los solucionaron.

Laboratorio de testing

Entrega 1

Cada equipo de trabajo deberá presentar:

- Plan de Pruebas del Help Desk (Caja Negra). Diseñar un cuadro simple con los casos de prueba para verificar las funciones básicas del sistema de tickets (ej. comprobar que un usuario pueda abrir un ticket, que se le pueda asignar a un técnico y que se pueda cerrar el incidente sin errores).
- Listas de Verificación de Hardware (Checklists Binarios). Crear planillas para revisar el armado físico de las computadoras y el servidor. Debe incluir puntos básicos de orden del rack, seguridad eléctrica (cables ordenados, puesta a tierra) y ergonomía del salón (altura de mesas, sillas).
- Plan de Borrado Seguro (NIST SP 800-88). Explicar brevemente qué herramienta o comando van a usar para hacer la limpieza completa de los discos reciclados y cómo van a verificar que los datos anteriores se eliminaron.

Entrega 2

Cada equipo de trabajo deberá presentar:

- Evidencias (capturas de pantalla) de que la interfaz web del Help Desk y su base de datos funcionan bien y no pierden información al guardar un ticket.
- Certificación de Conectividad de Red. Registrar las pruebas físicas hechas a los cables de red de la sala para asegurar que están bien armados, no pierden datos y cumplen con la categoría correspondiente (5e o 6).
- Lista con todos los errores o fallas encontrados durante las pruebas (tanto en el software de tickets como en el hardware de las PC) y anotar si se pudieron solucionar o si el problema persiste.
- Capturas de pantalla o reportes del programa utilizado que demuestren que el borrado seguro de los discos duros se realizó con éxito.

Entrega 3

Cada equipo de trabajo deberá presentar:

- QA Logs (Registro de Auditoría). El historial técnico unificado donde se anoten todas las pruebas que se hicieron durante el año, incluyendo los re-testeos de los equipos o configuraciones que habían fallado al principio y luego se arreglaron.
- QA Dashboard (Tablero de Control). Un informe estadístico muy sencillo con gráficos o porcentajes clave del proyecto (ej. porcentaje de discos borrados con éxito, cuántas PC pasaron la prueba inicial a la primera, y la velocidad o rendimiento final de la red).
- Hojas de aprobación individuales firmadas por el equipo de testing que declaren formalmente qué computadoras y servicios del salón superaron el control de calidad y quedan listos para usarse de forma oficial.

9.2 Componente AP

Laboratorio de Sistemas Operativos

Entrega 1

Cada equipo de trabajo deberá presentar :

- Configuración de la plataforma de virtualización elegida (puede ser VirtualBox o el hipervisor que prefieran) lista para alojar los servidores virtuales del proyecto.
- Un script de consola con un menú interactivo para revisar el estado básico de la máquina (espacio libre en disco, memoria RAM usada y procesos activos).

- Activación de un firewall nativo fácil de administrar (como ufw o firewalld), aplicando reglas básicas para cerrar todos los puertos que no se usen y permitir solo las conexiones del laboratorio.

Entrega 2

Cada equipo deberá presentar y defender ante el docente:

- Puesta en marcha de una máquina virtual Linux (ej. Ubuntu Server o Debian) corriendo dentro del entorno virtual.
- Instalación básica de un servidor web con base de datos (Apache y MariaDB) para dejar el entorno preparado para guardar datos locales e inventarios.
- Configuración de la interfaz de red del servidor virtual utilizando una IP fija (estática), asegurando que mantenga siempre la misma dirección y puerta de enlace dentro del salón.
- Un script en bash que copie los archivos de registro (logs) del sistema, filtre los mensajes de error más importantes y los guarde ordenados en una carpeta de respaldo dentro del sistema.

Entrega 3

Cada equipo deberá entregar:

- Menú script de panel final en bash para el administrador. Este menú debe unificar los scripts del año: poder prender/apagar servicios, ver el estado de la red, revisar los logs en tiempo real y activar o desactivar el firewall desde opciones numeradas.
- Mostrar el archivo de texto generado automáticamente por su propio menú en bash, que registre con fecha y hora qué opciones usó cada integrante del grupo para hacer mantenimiento.
- Configuración de una segunda máquina virtual o un directorio secundario en red que actúe como respaldo automatizado, programado para recibir copias de la base de datos por si el servidor principal llega a fallar.

10. Cronograma

Se establecen las siguientes fechas clave para las entregas parciales y la defensa final:

- **Primera entrega (digital):** Lunes 10 de agosto.
- **Segunda entrega (digital):** Lunes 14 de septiembre.
- **Entrega final (impresa):** Lunes 26 de octubre.

- **Defensas:** 3, 4, 5 y 6 de noviembre.
  Se publican en tiempo y forma con horarios.

11. Conformación de grupos

- Los Grupos deberán estar conformados por:
  - Alumnos de un mismo tercer año.
  - Un mínimo de 3 (tres) y un máximo de 4 (cuatro) alumnos.
- La conformación del Grupo, deberá:
  - Ser dirigida al docente de Tutoría de proyecto UTULab y entregar copia impresa a coordinación (coordinación de Informática), de acuerdo con las normas de documentación vigentes.
  - Deberá ser presentada antes del 21 de Julio de 2026
  - En dicha nota, deberá figurar la siguiente información mínima (tendrá un estándar de presentación publicado en la página web en la sección **INFORMÁTICA**):
    - Nombre del tercer año al cual pertenece el grupo.
    - Nombre de fantasía asignado al grupo, debiendo ser un nombre con posibilidades comerciales y que contenga un significado que los alumnos puedan explicar llegado el caso.
    - Para cada uno de los alumnos, deberá aparecer:
      - Nombre completo y foto.
      - Número de cédula de identidad.
      - Teléfono particular, si lo tuviera.
      - Teléfono celular, si lo tuviera.
      - Dirección de email.
      - No se aceptará ninguna nota que no identifique plenamente al alumno, es decir, que no contenga nombre y apellido del alumno.
    - Tener un representante, entre sus integrantes, el cual deberá ser explicitado.
- **NO SE PODRÁN REALIZAR CAMBIOS EN LOS INTEGRANTES DE LOS GRUPOS DE PROYECTOS LUEGO DE LA SEGUNDA ENTREGA.**

12. Defensa y entrega final

- En ésta fecha cada uno de los grupos de cada tercer año deberá “vender” al plantel docente el proyecto que han realizado.
- Junto con la “venta” deberá entregarse material impreso que justifique la misma.

13. ¿Cómo debo entregar mis entregas digitales?

Se deberán entregar, **DOS PENDRIVE ***, debidamente identificados, en un **SOBRE DE PAPEL** con:

- Nombre fantasía del grupo de proyecto
- Grupo en que se cursa.

Dentro de cada **PENDRIVE**, deberá haber una carpeta por **MATERIA**, correctamente identificadas con:

- Nombre de la materia
- Nombre del docente

Dentro de cada carpeta de cada **MATERIA**:

- Documento de entrega de la materia (formato PDF y que respete el estándar de documentación publicado)
- Aplicación funcionando si corresponde.
- Cualquier archivo o imagen adicional

Recuerde que toda la documentación debe cumplir con la estandarización brindada por la escuela. La misma se encuentra en nuestra **PÁGINA WEB** en la sección de **INFORMÁTICA**.

Finalizada la corrección los **PENDRIVE** se devuelven para que puedan ser reutilizados.

* El segundo **PENDRIVE** será una copia del primero, **ES LA COPIA DE RESPALDO**.

14. ¿Cómo debo entregar, la ENTREGA IMPRESA?

Se deberá entregar una carpeta impresa **POR CADA MATERIA** debidamente identificada. Los documentos impresos deberán cumplir con los estándares de documentación de la escuela, que se encuentran publicados en la página web del instituto. Se deberá llevar dos copias del **estándar de entrega de documentos** (una para la institución y otra para el grupo)

Notas **IMPORTANTES**:

Para este Proyecto regirá la integración de “Grupos” vigente para la primera entrega, con las modificaciones que hayan sido realizadas y autorizadas desde ese momento. Se recuerda que el grupo de Proyecto será indivisible a no ser que sea comunicada a la coordinación la disolución del mismo y los ajustes que ello signifique en otros grupos. De todas maneras, es de destacar que:

- Dicha disolución no tendrá efecto hasta tanto no sea aprobada
- Todo lo realizado, en materia de proyecto, hasta ese momento, es propiedad intelectual de todos los integrantes, es decir, pertenece a todos los integrantes del grupo, por igual.