Universidad Siglo 21

Trabajo Final de Grado. Prototipado Tecnológico

Carrera: Licenciatura en Informática

SISTEMA DE TRAZABILIDAD, AUDITORIA, CONTROL Y RESGUARDO DE ACCESOS PARA SISTEMAS INDUSTRIALES OT

Autor: Carlos Daniel Vergara

Legajo: VINF10238

Paraná, Entre Ríos, junio de 2025

Índice

Índice de Tablas

Índice de Imágenes

Resumen

En la actualidad, la ciberseguridad es uno de los aspectos más importantes considerados por todas las compañías del mundo. Esto se debe a que distintos ataques de ciberseguridad han demostrado la fragilidad de sus infraestructuras tecnológicas; haciendo evidente que el eslabón más débil de la cadena es el usuario.

Las organizaciones emplean gran parte de su presupuesto en capacitación y metodologías de control para mitigar los riegos de ciberseguridad, pero aun así los casos críticos no han disminuido sino que peor, aun han aumentado.

La situación planteada estableció la necesidad de un medio que permita mantener la seguridad de la infraestructura tecnológica y que los usuarios de la misma no sean un posible factor de ataque. El presente trabajo final de grado comprende el diseño e implementación de un prototipo de aplicación web progresiva con diseño responsivo que tiene como objetivo trazar, auditar, controlar y resguardar de manera centralizada los accesos críticos de los sistemas y dispositivos industriales OT; permitiendo la seguridad y manipulación controlada de los mismos y garantizando el correcto funcionamiento del entorno industrial.

Palabras claves: aplicación, web, trazabilidad, resguardo, control.

Abstract

Currently, cybersecurity is one of the most important aspects considered by all companies worldwide. This is because several cybersecurity attacks have demonstrated the fragility of their technological infrastructures, making it even more evident that the weakest link in the chain is the user.

Organizations spend a large part of their budget on training and control methodologies to mitigate cybersecurity risks, but even so, critical cases have not decreased but, worse, have increased.

The situation presented here established the need for a means to maintain the security of the technological infrastructure and ensure that its users are not a potential attack factor. This final degree project includes the design and implementation of a progressive web application prototype with a responsive design that aims to centrally trace, audit, control, and safeguard critical access points to industrial OT systems and devices, enabling their security and controlled manipulation and ensuring the proper functioning of the industrial environment.

Keywords: application, web, traceability, safeguard, control.

Título

Sistema de Trazabilidad, Auditoria, Control y Resguardo de Acceso para Sistemas Industriales OT.

Introducción

Actualmente, la seguridad de la información, la gestión de contraseñas y accesos seguros se han convertido en aspectos críticos para las personas y organizaciones. Con el aumento constante de cuentas de acceso en línea y el crecimiento de dispositivos que pueden ser conectados a Internet, la necesidad de una solución centralizada para almacenar contraseñas y gestionar el acceso remoto se vuelve algo indispensable. Además, si esto es considerado en entornos industriales, donde los dispositivos y sistemas conservan y resguardan la seguridad de la salud y vida de los operadores mientras se mantienen la integridad de los procesos y la infraestructura, se convierte en el eje central de todo proceso industrial.

El presente proyecto aborda estas necesidades específicas mediante el desarrollo de una aplicación web diseñada para entornos industriales OT, principalmente para los accesos de nivel 1 y nivel 2 del “Modelo de Referencia Purdue” (Williams, 1993). Esta aplicación proporciona un almacenamiento seguro, centralizado y rotativo para contraseñas sensibles, permite a los usuarios acceder de forma remota a sistemas y dispositivos críticos sin necesidad de conocer las credenciales de acceso; todo a través de un dashboard según el tipo de perfil de usuario que le fue designado, que a su vez otorga solo los permisos que fueron configurados. De manera simultánea, el sistema contempla la trazabilidad para permitir en cualquier momento la auditoria de cambios, modificaciones, como así también de accesos para los perfiles de auditoría.

Antecedentes

Un estudio consultado, denominado "Comparativa de Estrategias de Ciberseguridad Nacional de Latam, realizado por El Centro de Ciberseguridad Industrial" (Industrial, Centro de Ciberseguridad, 2021, pág. 1) tuvo como objetivo revisar el estado de la situación de ciberseguridad en los ambientes públicos y privados de Latam, y como los diferentes países tratan dicho tema.

Se pudo comprobar que los ambientes en su mayoría carecían de las medidas básicas de seguridad, y en algunos casos no eran considerados dentro de las prioridades de los proyectos de Ciberseguridad.

En el caso puntual de Argentina por medio de la "Resolución 829/2019 de la Secretaria de Gobierno de Modernización, se aprobó la Estrategia Nacional de Ciberseguridad"[1], donde a través de 5 Principios Rectores y 8 objetivos, confirma la necesidad de abordar la situación actual, que debido a la cantidad de dispositivos críticos conectados a Internet genera nuevos escenarios de riesgos y amenazas que pone en riegos la disponibilidad, integridad y confidencialidad de la información como así también la afectación de la vida de las personas como la seguridad en general; todo esto como resultado de la rentabilidad que ofrece a los atacantes.

Descripción del Área Problemática

Las áreas industriales actualmente controlan la mayoría de los servicios esenciales (agua, luz, combustible, entre otros) para el desarrollo de la vida de las personas como así también de las organizaciones y países.

Caso ejemplo como el sucedido en Mayo 2021 a Colonial Pipes donde tras confirmar el ciberataque, se constato que dicha compañía era responsable del 45% de los suministros de combustibles para el este de Estados Unidos, lo que produjo el cierre de sus 8.8 km de tuberías, y aproximadamente 5 días sin suministro de combustible para aviones de pasajero, como así también vehículos terrestres.

A nivel mundial, según datos del "Foro Económico Mundial y Organizaciones de Ciberseguridad" (World Economic Forum, 2024), 9 de cada 10 organizaciones sufrieron al menos un ataque cibernético en el último año; estimando costos

[1] (Ministros, Jefatura de Gabinete de, 2019, pág. 1)

relacionados a ciberdelincuencia en aproximadamente 10,5 billones de dólares para 2025.

Esto supone un incremento del 75% con respecto al mismo periodo de 2023.

Según Kaspersky, América Latina encabeza las regiones donde se detectaron y bloquearon intentos maliciosos de diferentes tipos de malware, “El promedio de ciberataques a equipos OT en 2023 fue del 38.6%”. (Kaspersky, 2024)

La situación actual de globalización hace inevitable que empresas situadas en un lugar del mundo necesiten asistencia o control de dispositivos desde otros países lo que implica poder conectar o dar acceso a casi todos los sistemas y dispositivos. Esto a su vez proporciona un objetivo a los ciberdelincuentes, ya que, no es costoso vulnerar o bloquear estos sistemas, y el rédito económico que pueden obtener al solicitar los rescates por la información y/o accesos son extremadamente enormes.

Justificación

La creación del Sistema de Trazabilidad, Auditoría, Control y Resguardo de Acceso para Sistemas Industriales OT, fue necesaria en el ámbito de seguridad industrial principalmente, pero también aplicable a todo ámbito de seguridad tecnológico público y privado, porque los profesionales de la seguridad informática observaban la necesidad de contar con una herramienta que permita almacenar de manera segura y confiable credenciales de accesos, que permita el acceso remoto a sistemas y/o dispositivos sin la necesidad de que el usuario tenga conocimiento de las credenciales, como así también que pueda automatizarse la rotación de contraseñas de manera que se eviten accesos malintencionados ya sea a través de robos o compartición de claves. Sumando a todo esto la posibilidad de trazar y auditar todos los sucesos de acceso y uso de credenciales de manera unívoca; garantizando que todo accionar corresponde a un perfil especifico de usuario que solo tiene acceso a lo que se determinó.

La relevancia del proyecto, confirmó que al limitar el conocimiento del usuario acerca de datos críticos fortaleció el control y evitó la fuga de datos, lo que a su vez disminuyo las posibilidades de que ciberdelincuentes puedan tentar o engañar a los

usuarios y así evitar ataques que podrían ser catastróficos. Esto además evita que se creen contraseñas débiles (que no cumplen con los requisitos mínimos de cantidad/tipo de caracteres) y diccionarios de contraseñas (utilizados por los ciberdelincuentes cuando utilizan ataques de fuerza bruta).

Objetivo General del Proyecto

Diseñar y desarrollar una aplicación web progresiva, que permita trazar, auditar, controlar y resguardar de manera centralizada los accesos críticos de los sistemas y dispositivos industriales OT, donde las credenciales de acceso/control estén cifradas, con una rotación de modificación que evite usos malintencionados. Esto Aplicando perfiles de usuario para delimitar permisos y acciones.

Obteniendo como objetivo la disminución en su totalidad de ciberataques a través de accesos no autorizados.

Objetivos Específicos del Proyecto

Almacenar y modificar de manera manual y/o automatizada credenciales de acceso.

Permitir accesos remotos a dispositivos y/o sistemas OT.

Trazar y auditar todos los sucesos que se generen en el sistema.

Cifrar toda información crítica para evitar fuga de información.

Marco Teórico Referencial

Dominio del Problema

Es necesario comprender que es OT (Operational Technology – Tecnología Operativa), son todos los sistemas o dispositivos que interactúan con el ambiente físico en entornos industriales. Estos sistemas/dispositivos detectan o generan un

> cambio directo a través del control y/o monitoreo de dispositivos, procesos y eventos. Ejemplos de control sistemas industrial son: “sistemas de control de incendio, sistemas SCADA (para controlar PLC, mecanismos entre otros dispositivos)” (NIST Special Publication 800-37 Revision 2, 2018). Estos dispositivos controlan los procesos industriales, los que entre sus tareas tienen lo conocido como SAFETY que “es la expectativa de que un sistema, bajo condiciones definidas, no permitirá un estado en la vida humana, la salud, la propiedad o el medio ambiente estén en peligro” (NIST Special Publication. NIST SP 800-160v1r1, 2022).

TICs

De acuerdo con la investigación tecnológica y la documentación disponible, existe un lenguaje de programación que se destaca por sobre el resto en la utilización de la seguridad como eje principal de desarrollo, este es Python, con la utilización del framework Django.

Python fue creado por Guido van Rossum, posee licencia de código abierto. Puede ser usado en múltiple dominio de aplicaciones, como por ejemplo desarrollo web. Soporta librerías y protocolos como: HTML, XML; JSON, procesamiento de E-mail entre otros (The Python Software Foundation, 2025).

El diseño es a través de Django, que es un framework web de código abierto, escrito en Python, que respeta el patrón de diseño conocido como modelo-vista-controlador y que está enfocado en la seguridad (Django Project, 2005).

La base de datos que se utiliza es MySQL que es una base de datos relacional desarrollado bajo licencia publica general/Licencia comercial por Oracle Corporation (ORACLE Coorporation, 2025).

Con respecto a los requisitos de hardware, se simulara una estructura de servidor virtualizado con 8GB de memoria RAM y un procesador Intel i7 de 1.99GHz.

El sistema operativo para desarrollar será Windows, pero al tratarse de un sistema tipo WEB no dependerá en primera medida del mismo sino de los buscadores compatibles; los cuales en su mayoría funcionan con Windows, Linux y Mac.

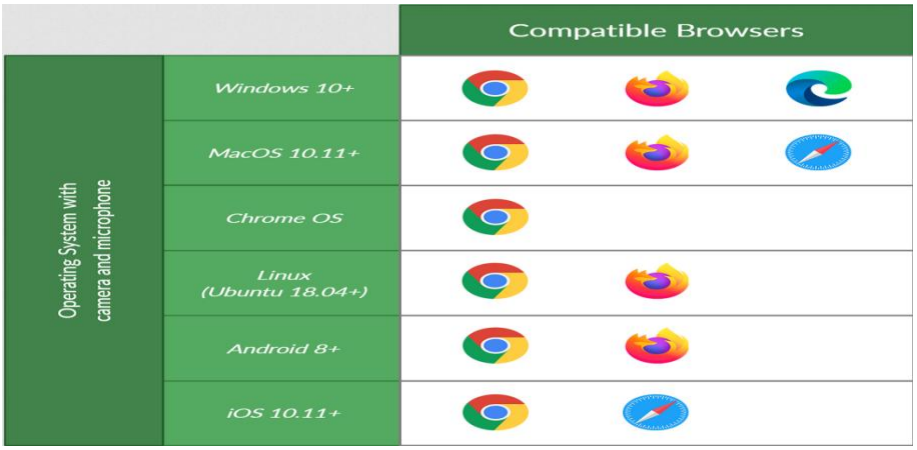


Ilustración 1 – Compatibilidad de Buscadores (Integrity Advocate, 2025)

Competencia

En el ámbito de aplicaciones web diseñadas como baúl de contraseñas y accesos remotos existen dos Rattic y CyberArk.

Rattic es una aplicación web de manejo centralizado de contraseñas, de licencia GPLv2, cuya última actualización fue en 2015 (por lo cual actualmente tiene vulnerabilidades detectadas) y que además no posee administración remota de dispositivos (Hall, 2015).

CyberArk es una empresa de seguridad de la información que ofrece baúl de contraseñas y accesos remotos en módulos separados (CyberArk Software Ltd, 2024).

Estas aplicaciones una open source y la otra de licencia paga, son los dos casos de desarrollo web, existen otras que son para entornos locales o para nubes públicas de ciertas marcas.

La aplicación Rattic cumple con las características de baúl de contraseñas y su correspondiente auditoria, sin permitir accesos a sistemas de manera automatizada.

La aplicación CyberArk contempla misma funcionalidades sin tener un dashboard de información basada en perfil del usuario.

Diseño Metodológico

El proceso para desarrollar el sistema va a seguir los lineamientos de UML, basándose en el paradigma de objetos que Object Manager Group (OMG) liberó al público. Además de ordenar todo el diseño y estructurar tan bien las etapas, el lenguaje permite que “los profesionales informáticos pueden comunicar sus ideas en un formato estándar y común, preparar planes y enfrentar nuevos desafíos” (Donald, 2003). En el desarrollo se utilizarán diferentes librerías, que van a estar presentes a lo largo de todo el proceso, en primera instancia se utilizará Python, tanto para desarrollar el Front End como el Back End.

Herramientas Metodológicas

La muestra estuvo conformada por dos empresas industriales una del sector farmacéutico y otra del sector siderúrgico, en las cuales trabaje en la segmentación de redes de conexión de niveles de automatización, y control de accesos del personal alcanzado.

Herramientas de Software

Las herramientas de desarrollo desde el punto de vista técnico fueron: Lenguaje de programación: Python, diseño a través del framework Django, motor de base de datos MySql.

Ambas herramientas fueron seleccionadas en primera medida por ser tecnologías open source, son ampliamente conocidas por su robustez al procesar grandes volúmenes de datos y además porque cumplen con todos los requisitos de seguridad planteados.

Planificación del Proyecto

En la planificación de actividades se utilizó un Diagrama de Gantt, donde se detallan las actividades a llevar a cabo para la entrega a término del proyecto; tiempo comprendido entre 17/03/2025 al 30/06/2025

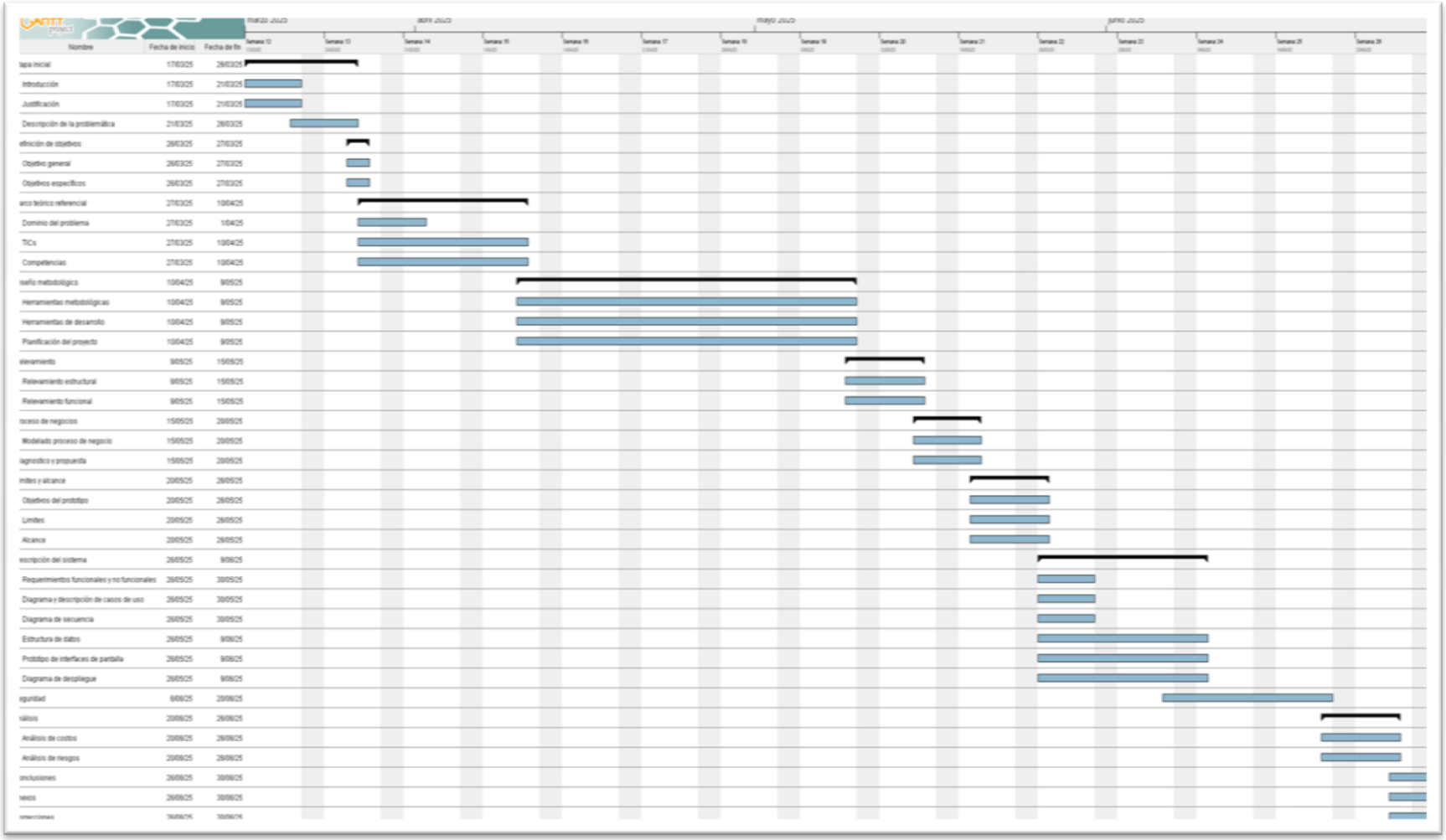


Ilustración 2: Diagrama de Gantt. Fuente: Elaboración Propia

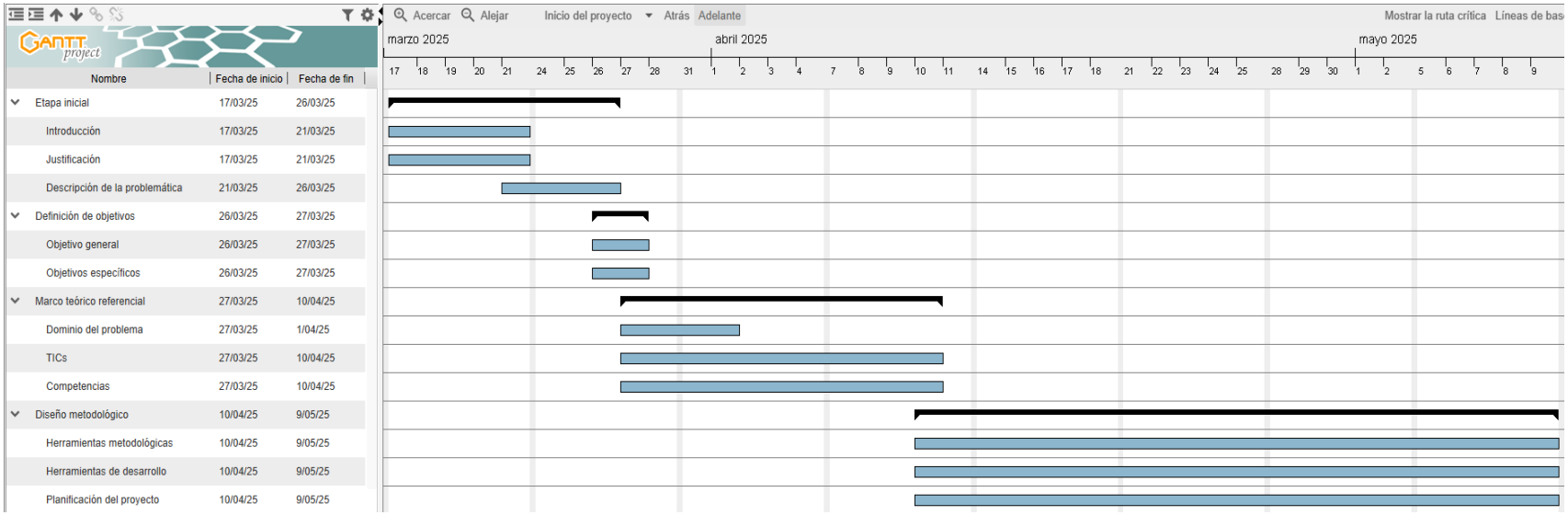


Ilustración 3: Diagrama de Gantt ampliado 1era parte. Fuente: Elaboración Propia

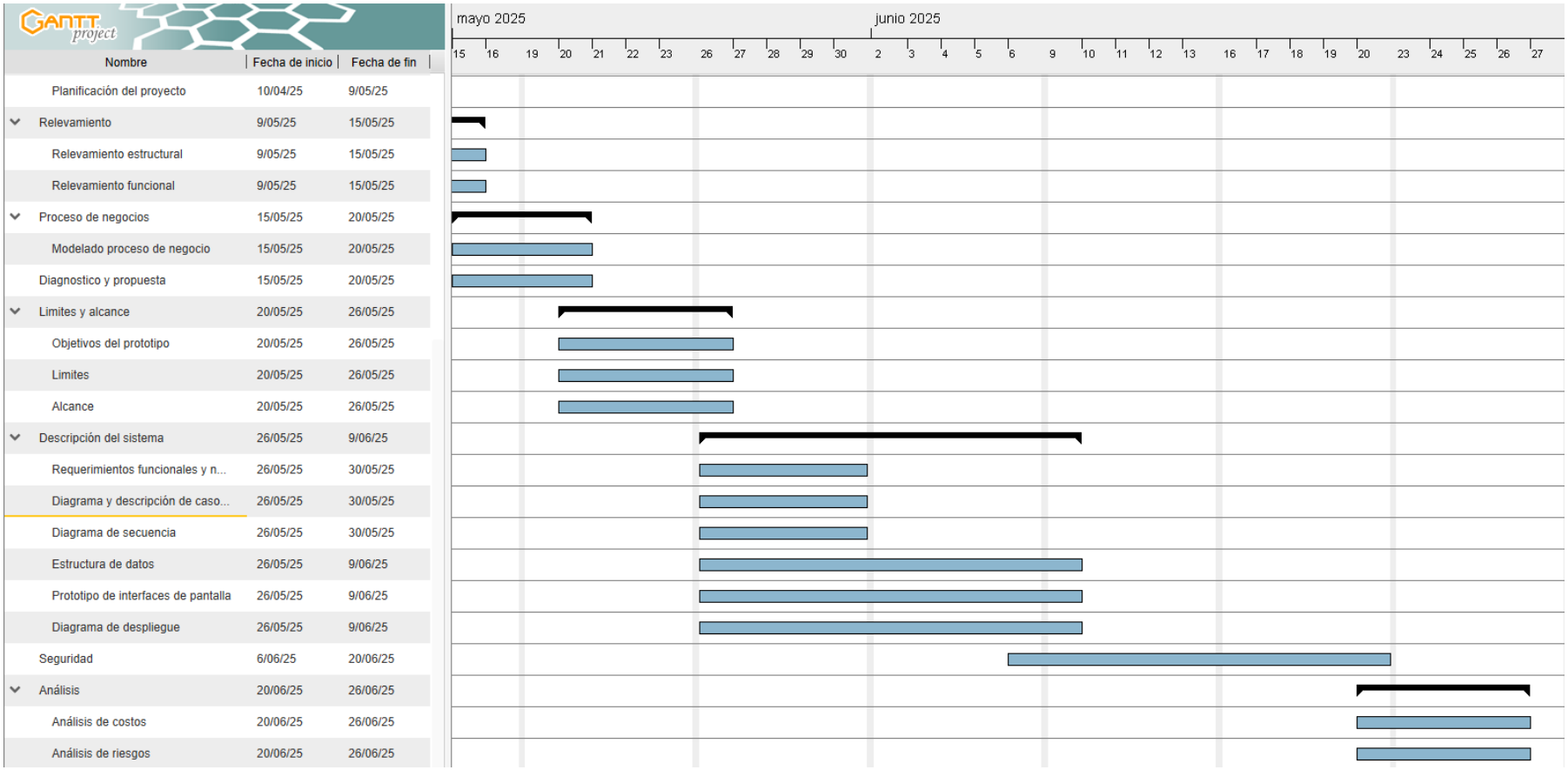
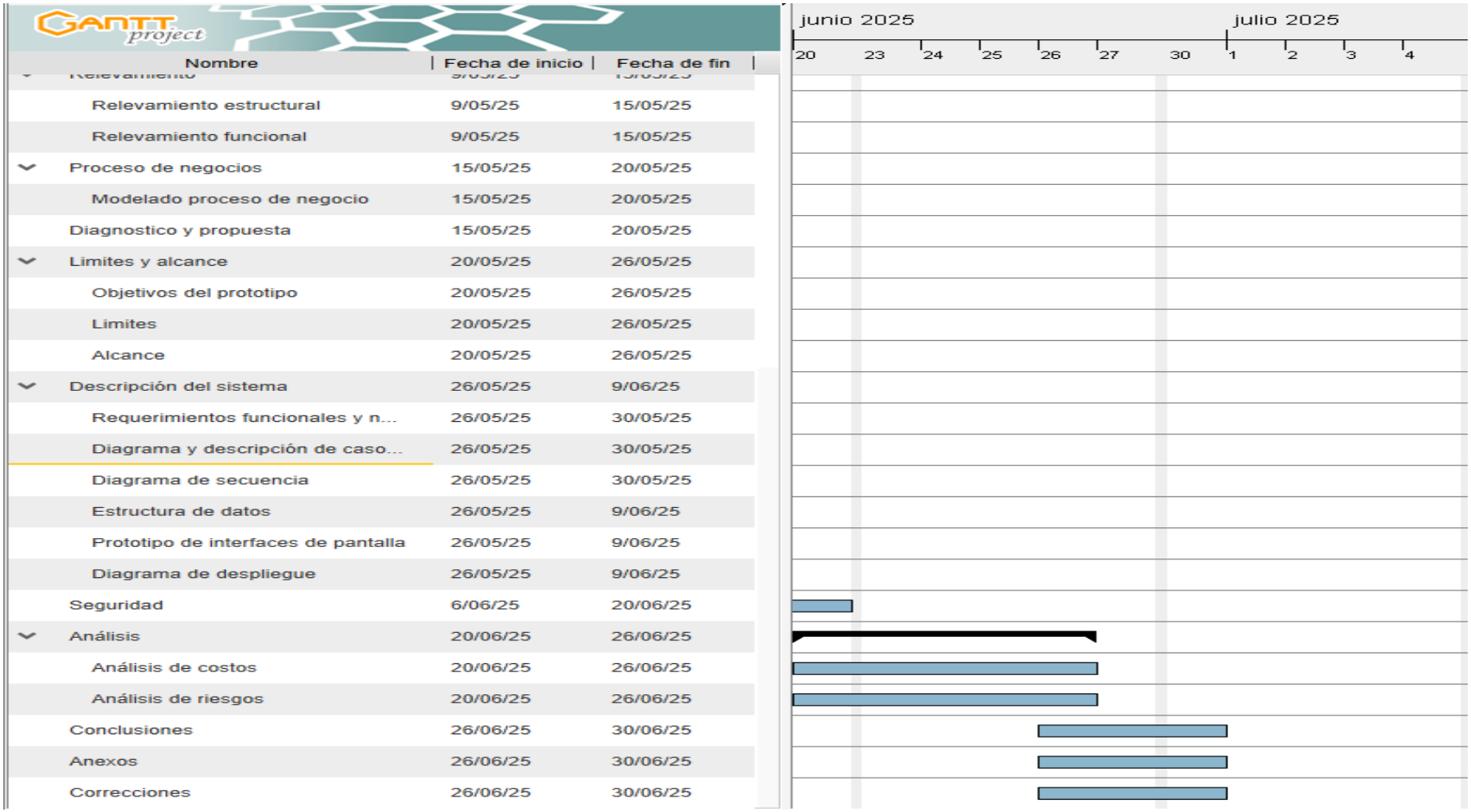


Ilustración 4: Diagrama de Gantt ampliado 2da parte. Fuente: Elaboración Propia



Nombre	Fecha de inicio	Fecha de fin
Relevamiento estructural	9/05/25	15/05/25
Relevamiento funcional	9/05/25	15/05/25
Proceso de negocios	15/05/25	20/05/25
Modelado proceso de negocio	15/05/25	20/05/25
Diagnostico y propuesta	15/05/25	20/05/25
Limites y alcance	20/05/25	26/05/25
Objetivos del prototipo	20/05/25	26/05/25
Limites	20/05/25	26/05/25
Alcance	20/05/25	26/05/25
Descripción del sistema	26/05/25	9/06/25
Requerimientos funcionales y n...	26/05/25	30/05/25
Diagrama y descripción de caso...	26/05/25	30/05/25
Diagrama de secuencia	26/05/25	30/05/25
Estructura de datos	26/05/25	9/06/25
Prototipo de interfaces de pantalla	26/05/25	9/06/25
Diagrama de despliegue	26/05/25	9/06/25
Seguridad	6/06/25	20/06/25
Análisis	20/06/25	26/06/25
Análisis de costos	20/06/25	26/06/25
Análisis de riesgos	20/06/25	26/06/25
Conclusiones	26/06/25	30/06/25
Anexos	26/06/25	30/06/25
Correcciones	26/06/25	30/06/25

Ilustración 5: Diagrama de Gantt ampliado 3da parte. Fuente: Elaboración Propia

Relevamiento

Relevamiento Estructural

Los ambientes industriales considerados en este proyecto se rigen según el "Modelo de Referencia Purdue" (Williams, 1993), considerándose la aplicación a desarrollar de NIVEL 3, que será conector con los niveles 1 y 2.

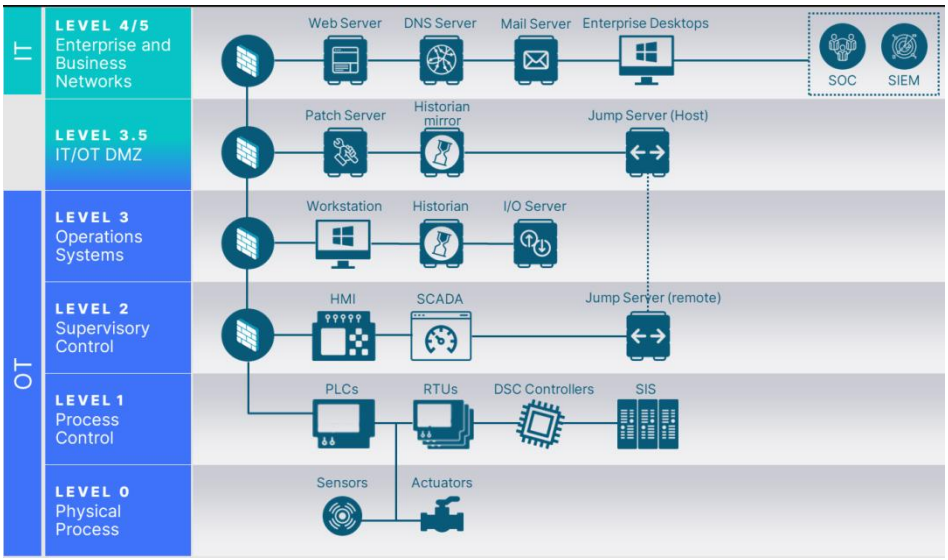


Ilustración 6: "Modelo Purdue" (Safe Breach, 2025)

Relevamiento funcional

La Gerencia Productiva es la encargada del proceso de fabricación de productos y por ende la encargada de adquirir, controlar y actualizar las tecnologías usadas. Además, es el área que autoriza la asignación de los distintos roles. Está compuesta por el gerente de producción, quien en caso de ausencia es suplantado por el subgerente de producción.

La subgerencia Productiva es la encargada del contacto directo con las áreas Operacional y Mantenimiento. Genera los informes de producción y los presenta a la Gerencia Productiva. Está compuesta por el subgerente de producción, y en caso de ausencia es suplantado por el gerente de producción.

El Área Operacional es la encargada de control, monitoreo y manipulación de los dispositivos de la línea de producción. Está compuesta por un jefe y subjefe que se reemplazan en caso de ausencia de uno de los dos, más el resto del personal.

El Área Mantenimiento es la encargada del mantenimiento preventivo, puesta a punto e implementación de los dispositivos de la línea de producción. Trabajan de manera directa y coordinada con el Área Operacional, ya que en la mayoría de los casos su trabajo es bajo demanda de esta última. Está compuesta por un jefe y subjefe que se reemplazan en caso de ausencia de uno de los dos, más el resto del personal.

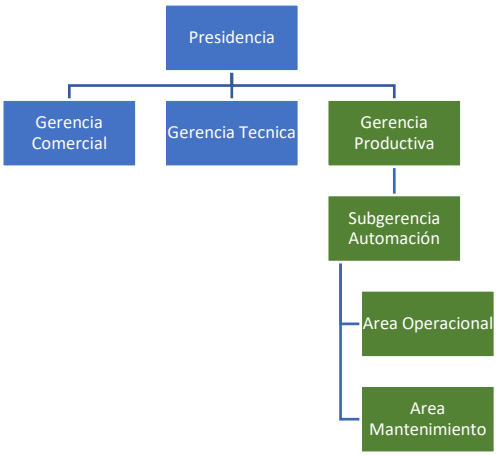


Ilustración 7: Organigrama. Fuente: Elaboración Propia

Las áreas que se encuentran pintadas de color verde son las involucradas en este proyecto.

Procesos de Negocios

Tras analizar los datos recolectados a través de técnicas como (reuniones y observación) se llega a la conclusión de que actualmente no se utiliza una estructura formal para los procesos funcionales.

Se detectan los siguientes perfiles:

Auditor: persona que verifica, controla, audita y autoriza los accesos creados y otorgados.

Administrador: persona que registra los accesos.

Operario: persona que utiliza los accesos a un sistema o dispositivo.

Tercero: persona externa a la compañía que puede utilizar los accesos a un sistema o dispositivo.

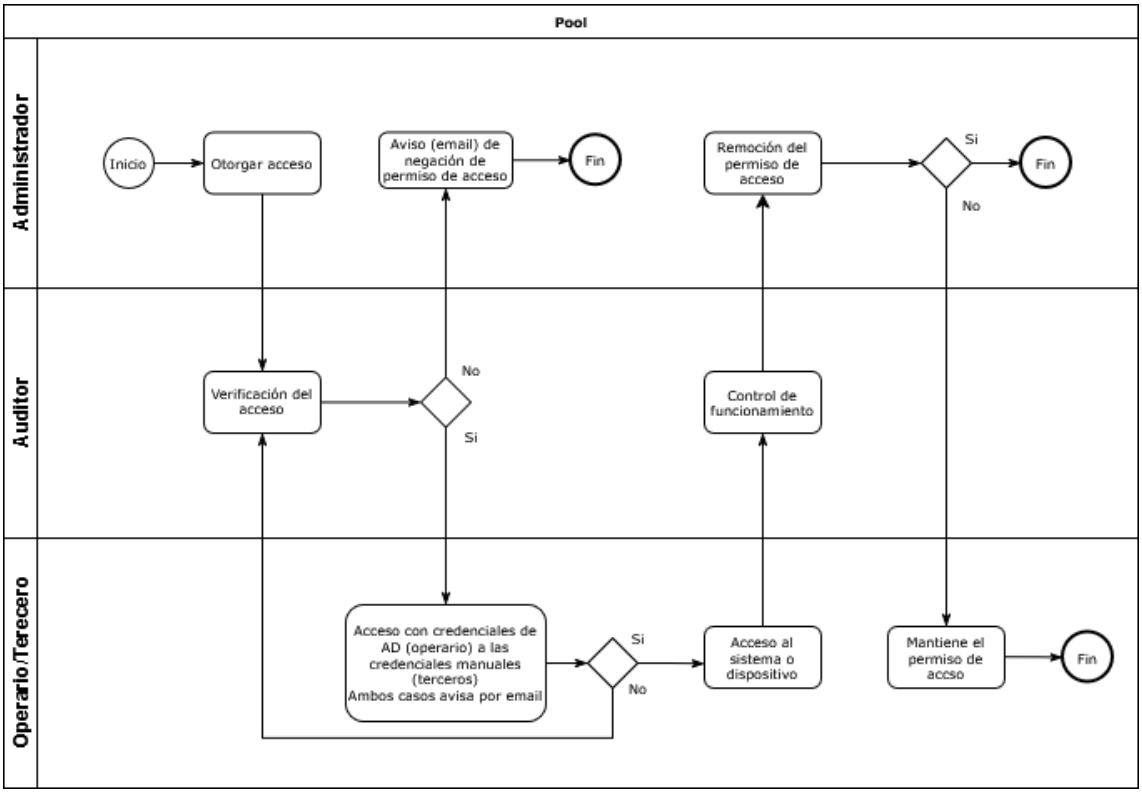


Ilustración 8: Proceso de Negocios. Fuente: Elaboración Propia

Diagnóstico y Propuesta

Nombre de proceso: Generación, control y resguardo de contraseñas de accesos

Roles: Gerencia productiva y Subgerencia automación.

Pasos: Cuando es necesario crear credenciales de acceso para sistemas no alcanzados por el servicio de Active Directory (entornos Windows) o Zentyal (entornos Linux), el operario crea las mismas anotándolas en una planilla de acceso múltiple o en una hoja de papel, o las envía por canales de comunicación inseguros.

Problema: Las credenciales creadas para accesos por fuera del sistema de acceso Active Directory o Zentyal, son conocidas por personas que no deberían, además que cuando las cambian no todos los operarios son informados lo que produce bloqueos temporales, y sumado que hay accesos de usuarios no preparados para manipular los software o peor aun que pueden generar un daño a la seguridad industrial.

Causas: La necesidad de configuración, puesta a punto o inicio de los softwares hace que los operarios utilicen estas técnicas de registro en vez de una plataforma centralizada con permisos acordes a cada rol y que sea realizado por los encargados/jefes.

Nombre de proceso: Acceso cifrado de operarios y proveedores

Roles: Área operacional y Área mantenimiento

Pasos: Hay sistemas cuya obsolescencia y/o criticidad implican que no pueden tener una rotación de credenciales como es recomendable por los procesos de seguridad industrial. Lo que implica que cuando un operario y/o un proveedor externo a la empresa (tercero) deban acceder a estos sistemas obtenga las credenciales sin ningún tipo de cifrado.

Problema: El acceso a credenciales que no tiene una rotación como lo establecen los procesos de seguridad industrial, y que además son proporcionadas sin cifrado, pone en riesgo el acceso y manipulación por personal no autorizado de los sistemas críticos del proceso industrial.

Causas: Sistemas que ya no cuentan con soporte, o que quienes lo desarrollaron no forman parte de la empresa o la obsolescencia hacen que no pueda cumplirse con la rotación necesaria y que a su vez sea conocida por múltiple personas.

Nombre de proceso: Cumplimiento de rotación de contraseñas

Roles: Gerencia productiva y Subgerencia automación.

Pasos: Según las recomendaciones de seguridad industrial, se deben modificar las contraseñas de acceso cumpliendo con requisitos de longitud y uso de caracteres. Esto generalmente lo realiza un operario que accede al sistema centralizado de credenciales (Active Directory o Zentyal) y realiza la modificación.

Problema: El acceso a los sistemas centralizados de credenciales (Active Directory o Zentyal) implica que un operario tenga credenciales con permisos altos lo que genera un riesgo si se ve comprometido su acceso, como así también es posible un error o bloqueo de acceso por incumplimiento de los requisitos de creación de contraseñas.

Causas: Debido a que los sistemas de credenciales necesitan de un usuario con permisos altos para realizar la rotación de las contraseñas, se otorga acceso a múltiples personas y se pierde el control de estos accesos.

Propuesta:

Se propone el desarrollo de un sistema que centralice las credenciales de acceso a los software que carecen de conexión con sistemas de Active Directory o Zentyal, que permita el acceso solo a las credenciales permitidas por el rol del operario a través de un dashboard; registrando todo los sucesos (visualización, modificación (de las credenciales o de los usuarios permitidos) como así también la eliminación de las mismas. Permitiendo el acceso remoto (RDP para sistemas Windows y SSH para sistemas Linux) sin la necesidad de que el operario y/o proveedor conozcan las credenciales, permitiendo el trabajo necesario; registrando todos los sucesos que se generen durante la sesión, y además realizar la rotación de claves de acceso con el cumplimiento de los requisitos, registrando todos los sucesos que se generen durante la modificación.

Objetivo, Límites y Alcances del Prototipo

Objetivo del Prototipo

Centralizar las credenciales de acceso a los software que carecen de conexión con sistemas de Active Directory o Zentyal, que permita el acceso solo a las credenciales permitidas por el rol del operario a través de un dashboard; registrando todo los sucesos (visualización, modificación de las credenciales o de los usuarios permitidos, como así también la eliminación de las mismas).

Permitir el acceso remoto (RDP para sistemas Windows y SSH para sistemas Linux) sin la necesidad de que el operario y/o proveedor conozcan las credenciales, permitiendo el trabajo necesario; registrando todos los sucesos que se generen durante la sesión.

Permitir la rotación de claves de acceso con el cumplimiento de los requisitos. A su vez registrando todos los sucesos que se generen durante la modificación.

Límites

Los limites son desde el resguardo, control y manipulación de credenciales de acceso restringidos hasta el acceso remoto con la rotación de contraseñas alcanzadas por sistemas Active Directory y Zentyal.

Alcances

- Centralizar credenciales de acceso
- Permitir accesos definidos por roles
- Acceso de información definidos por roles
- Control remoto por RDP y/o SSH
- Rotación de claves de acceso
- Control y trazabilidad de las actividades realizadas en el sistema

Descripción del Sistema

Se selecciona la metodología de lenguaje unificado de modelado (UML) para continuar con el análisis del sistema.

Requerimientos Funcionales

RF1: El sistema mostrará y permitirá el acceso a los diferentes tipos de información/sistemas a través del rol definido, visualizado desde un dashboard.

RF2: El sistema mostrara de manera cronológica los sucesos ocurridos dentro del sistema.

RF3: El sistema permitirá alta, baja y modificación de credenciales estáticas.

RF4: El sistema permitirá acceso remoto tipo RDP a entornos Windows y tipo SSH a entornos tipo Linux que tengan la configuración permitida localmente.

RF5: El sistema permitirá la rotación de claves de acceso a través de sistemas tipo Active Directory (entorno tipo Windows) o Zentyal (entornos tipo Linux)

Requerimientos No Funcionales

RNF1: Usabilidad

- Intuitivo.
- Guía de usuario.
- Alertas en caso de errores en carga de datos.

RNF2: Confiabilidad

- Mantener la integridad de la información.
- Alertas en caso de carga de información duplicada.

RNF3: Portabilidad

- Se podrá acceder desde sistemas tipo Windows y tipo Linux (con interfaz gráfica)
- Se podrán utilizar en buscadores Mozilla Firefox, Google Chrome e Edge.

Diagrama de Casos de Uso

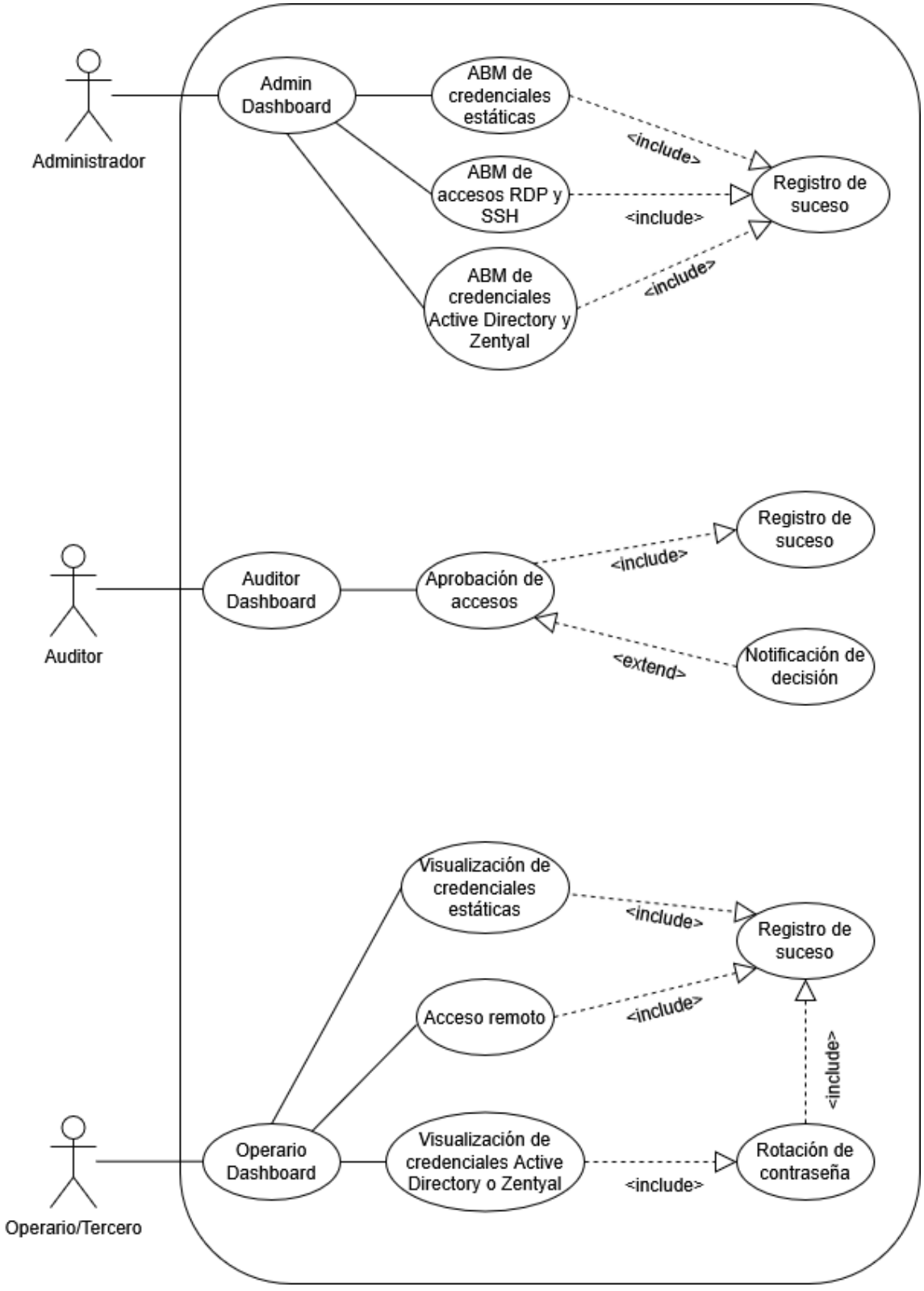


Ilustración 9: Diagrama de Casos de Uso. Fuente: Elaboración Propia

Descripción de Caso de Uso

Admin1	ABM de credenciales estáticas	
Versión	1 18/05/25	
Objetivos asociados	Acceso del rol administrador	
Precondición	El usuario con rol administrador debe haber accedido de manera exitosa al sistema.	
Secuencia Normal	Paso	Acción
	1	Seleccionar Alta, Baja o Modificación de credenciales estáticas.
	2	Completar los campos para realizar la acción de Alta, Baja o Modificación.
	3	Confirmar el cambio.
	4	Actualizar información en la base de datos.
	5	Guardar registro del suceso
Pos condición	Registro exitoso en la base datos del guardado del registro.	
Frecuencia esperada	Las veces que el rol administrador lo invoque.	
Importancia	Muy importante	
Comentarios	Sin comentarios adicionales.	

Tabla 1: Descripción de Casos de Uso Admin1. Fuente: Elaboración Propia

Admin2	ABM de accesos remotos RDP y SSH	
Versión	1 18/05/25	
Objetivos asociados	Acceso del rol administrador	
Precondición	El usuario con rol administrador debe haber accedido de manera exitosa al sistema.	
Secuencia Normal	Paso	Acción
	1	Seleccionar Alta, Baja o Modificación de accesos remotos.
	2	Completar los campos para realizar la acción de Alta, Baja o Modificación.
	3	Confirmar el cambio.

	4	Actualizar información en la base de datos.
	5	Guardar registro del suceso
Pos condición	Registro exitoso en la base datos del guardado del registro.	
Frecuencia esperada	Las veces que el rol administrador lo invoque.	
Importancia	Muy importante	
Comentarios	Sin comentarios adicionales.	

Tabla 2: Descripción de Casos de Uso Admin2. Fuente: Elaboración Propia

Admin3	ABM de credenciales Active Directory y Zentyal	
Versión	1 18/05/25	
Objetivos asociados	Acceso del rol administrador	
Precondición	El usuario con rol administrador debe haber accedido de manera exitosa al sistema.	
Secuencia Normal	Paso	Acción
	1	Seleccionar Alta, Baja o Modificación de Active Directory y Zentyal.
	2	Completar los campos para realizar la acción de Alta, Baja o Modificación.
	3	Confirmar el cambio.
	4	Actualizar información en la base de datos.
	5	Guardar registro del suceso
Pos condición	Registro exitoso en la base datos del guardado del registro.	
Frecuencia esperada	Las veces que el rol administrador lo invoque.	
Importancia	Muy importante	
Comentarios	Sin comentarios adicionales.	

Tabla 3: Descripción de Casos de Uso Admin3. Fuente: Elaboración Propia

Auditor1	Aprobación de accesos	
Versión	1 18/05/25	
Objetivos asociados	Acceso del rol auditor	
Precondición	El usuario con rol auditor debe haber accedido de manera exitosa al sistema.	
Secuencia Normal	Paso	Acción
	1	Seleccionar Aprobación de accesos
	2	Aprobar o no los accesos visualizados
	3	Confirmar el cambio.
	4	Notificar de la decisión.
	5	Actualizar información en la base de datos.
	6	Guardar registro del suceso
Pos condición	Registro exitoso en la base datos del guardado del registro.	
Frecuencia esperada	La cantidad de veces igual a los nuevos accesos cargados.	
Importancia	Muy importante	
Comentarios	Sin comentarios adicionales.	

Tabla 4: Descripción de Casos de Uso Auditor1. Fuente: Elaboración Propia

Operario1	Visualización de credenciales estáticas	
Versión	1 18/05/25	
Objetivos asociados	Acceso del rol operario	
Precondición	El usuario con rol operario debe haber accedido de manera exitosa al sistema.	
Secuencia Normal	Paso	Acción
	1	Seleccionar Visualización de credenciales estáticas.
	2	Utilizar la credencial estática seleccionada.
	3	Guardar registro del suceso.

Pos condición	Registro exitoso en la base datos del guardado del registro.
Frecuencia esperada	La cantidad de veces que el rol operario deba usar las credenciales estáticas.
Importancia	Muy importante
Comentarios	Sin comentarios adicionales.

Tabla 5: Descripción de Casos de Uso Operario1. Fuente: Elaboración Propia

Operario2	Acceso remoto	
Versión	1 18/05/25	
Objetivos asociados	Acceso del rol operario	
Precondición	El usuario con rol operario debe haber accedido de manera exitosa al sistema.	
Secuencia Normal	Paso	Acción
	1	Seleccionar Acceso Remoto
	2	Invocar el acceso del host remoto (RDP o SSH)
	3	Guardar registro del suceso.
Pos condición	Registro exitoso en la base datos del guardado del registro.	
Frecuencia esperada	La cantidad de veces que el rol operario deba usar los accesos remotos.	
Importancia	Muy importante	
Comentarios	Sin comentarios adicionales.	

Tabla 6: Descripción de Casos de Uso Operario2. Fuente: Elaboración Propia

Operario3	Visualización de credenciales de Active Directory o Zentyal	
Versión	1 18/05/25	
Objetivos asociados	Acceso del rol operario	
Precondición	El usuario con rol operario debe haber accedido de manera exitosa al sistema.	
Secuencia Normal	Paso	Acción

	1	Seleccionar Visualización de credenciales de Active Directory o Zentyal
	2	Utilizar la credencial seleccionada.
	3	Rotación de contraseña.
	4	Guardar registro del suceso.
Pos condición	Registro exitoso en la base datos del guardado del registro.	
Frecuencia esperada	La cantidad de veces que el rol operario deba usar las credenciales.	
Importancia	Muy importante	
Comentarios	Sin comentarios adicionales.	

Tabla 7: Descripción de Casos de Uso Operario3. Fuente: Elaboración Propia

Diagrama de Secuencia

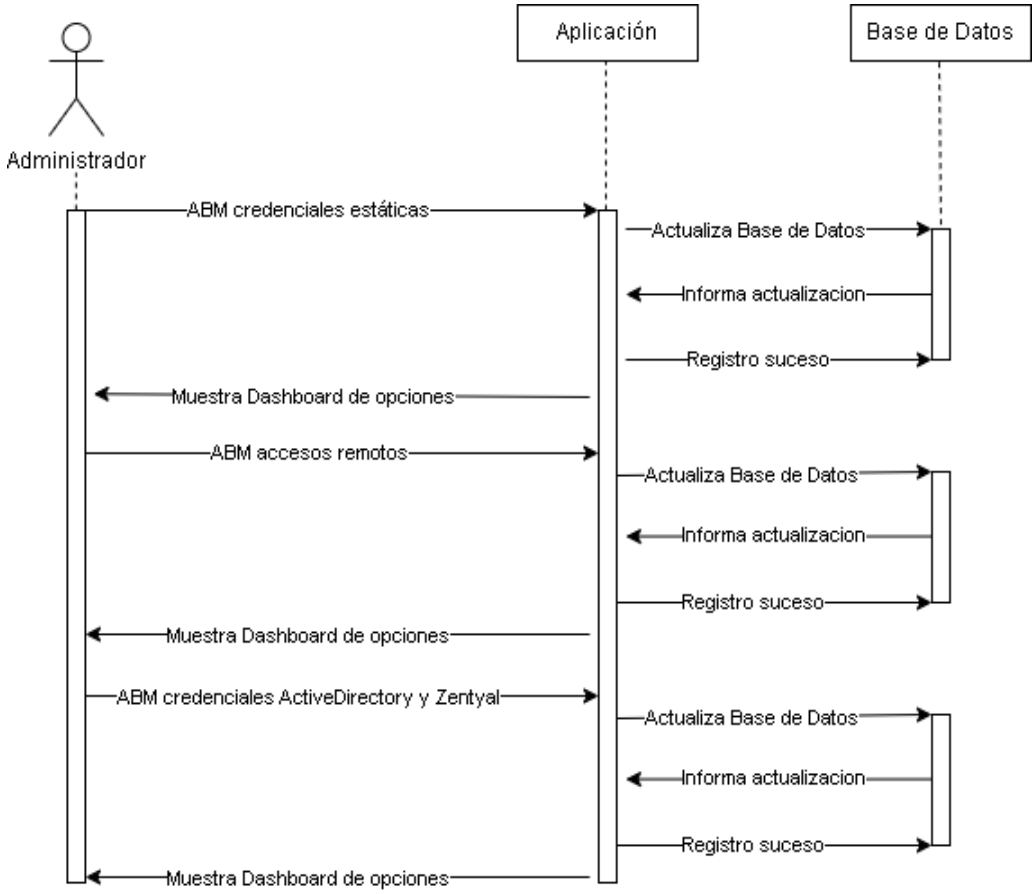


Ilustración 10: Diagrama de Secuencia administrador. Fuente: Elaboración Propia

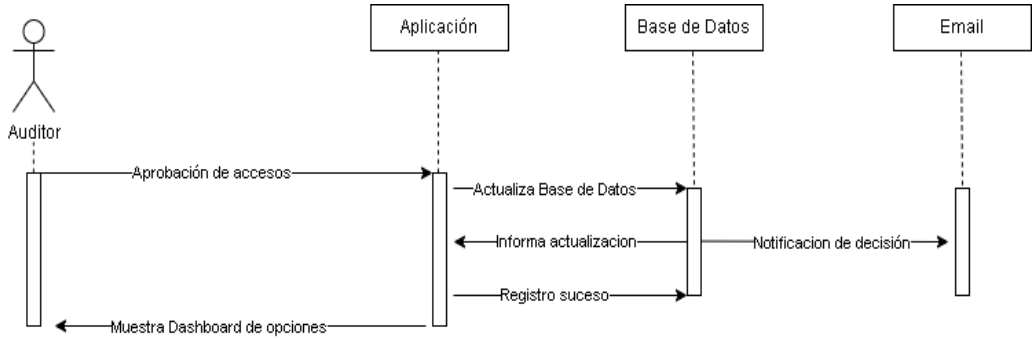


Ilustración 11: Diagrama de Secuencia auditor. Fuente: Elaboración Propia

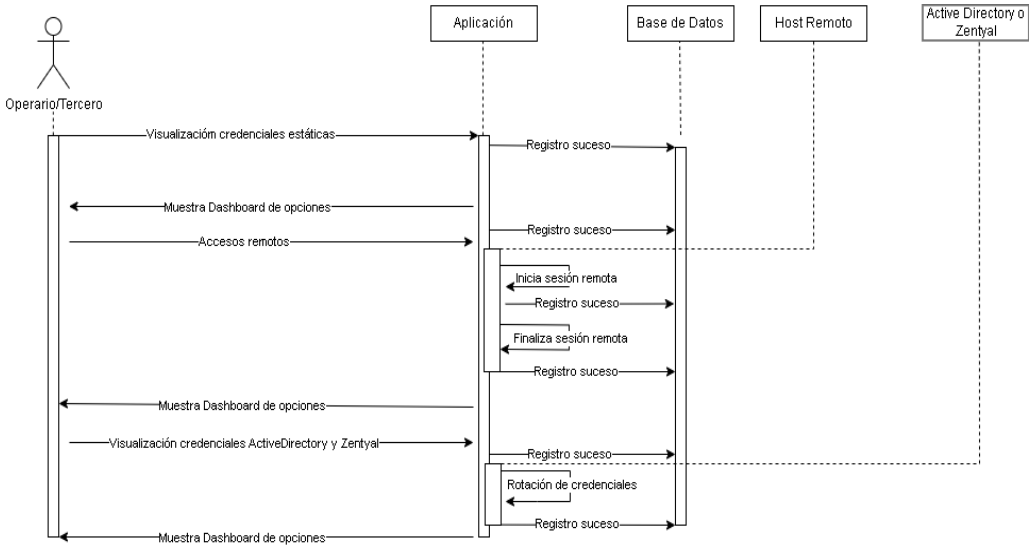


Ilustración 12: Diagrama de Secuencia operario. Fuente: Elaboración Propia

Estructura de Datos

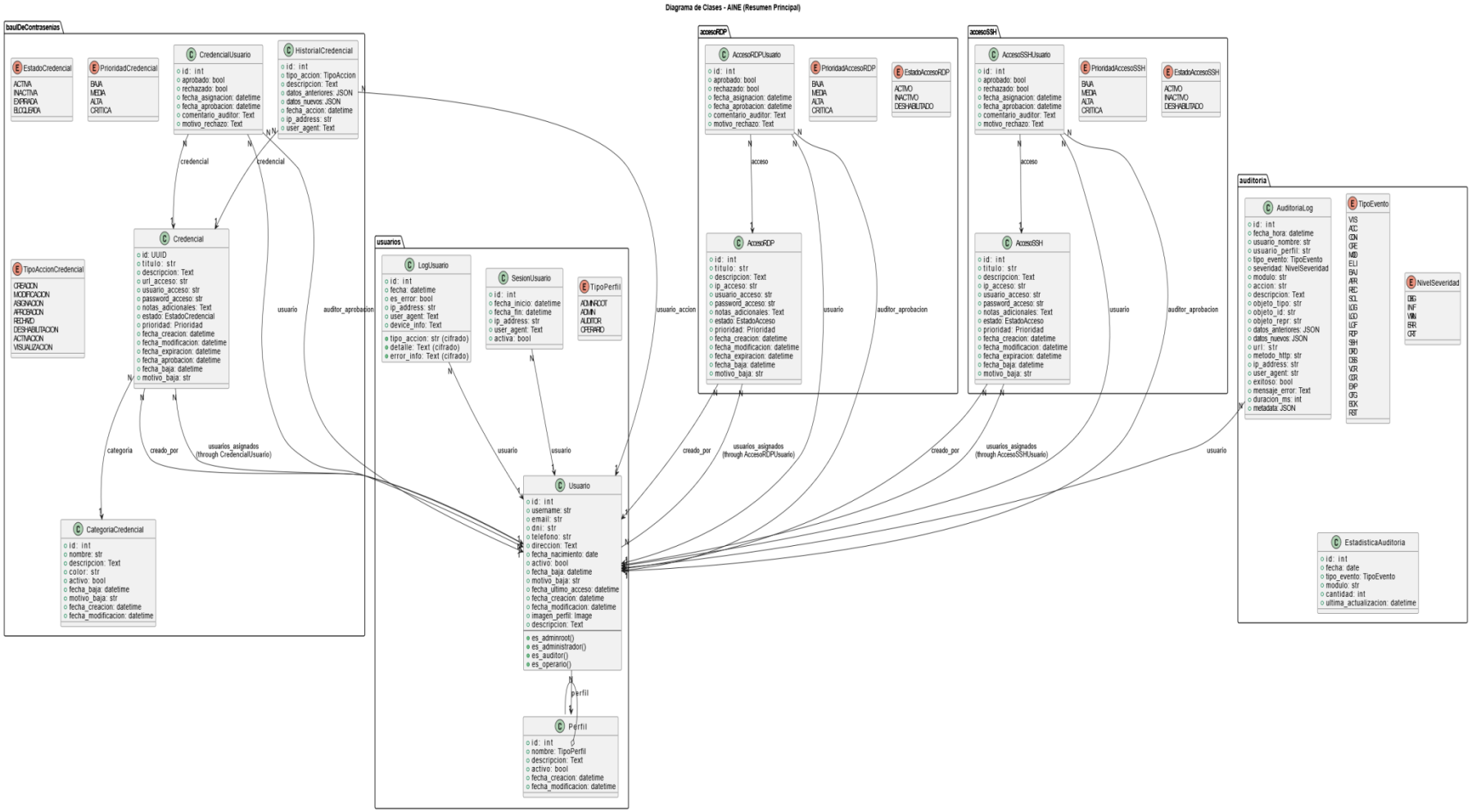


Ilustración 13: Estructura de Datos. Fuente: Elaboración Propia

Prototipos de Interfaces de Pantallas

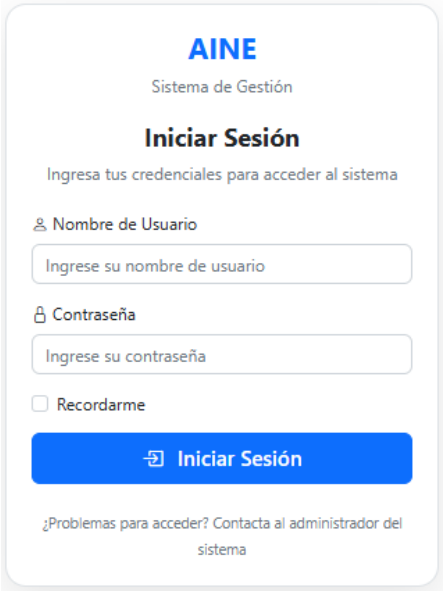


Ilustración 15: Prototipo de Interfaces de Pantalla - Login. Fuente: Elaboración Propia

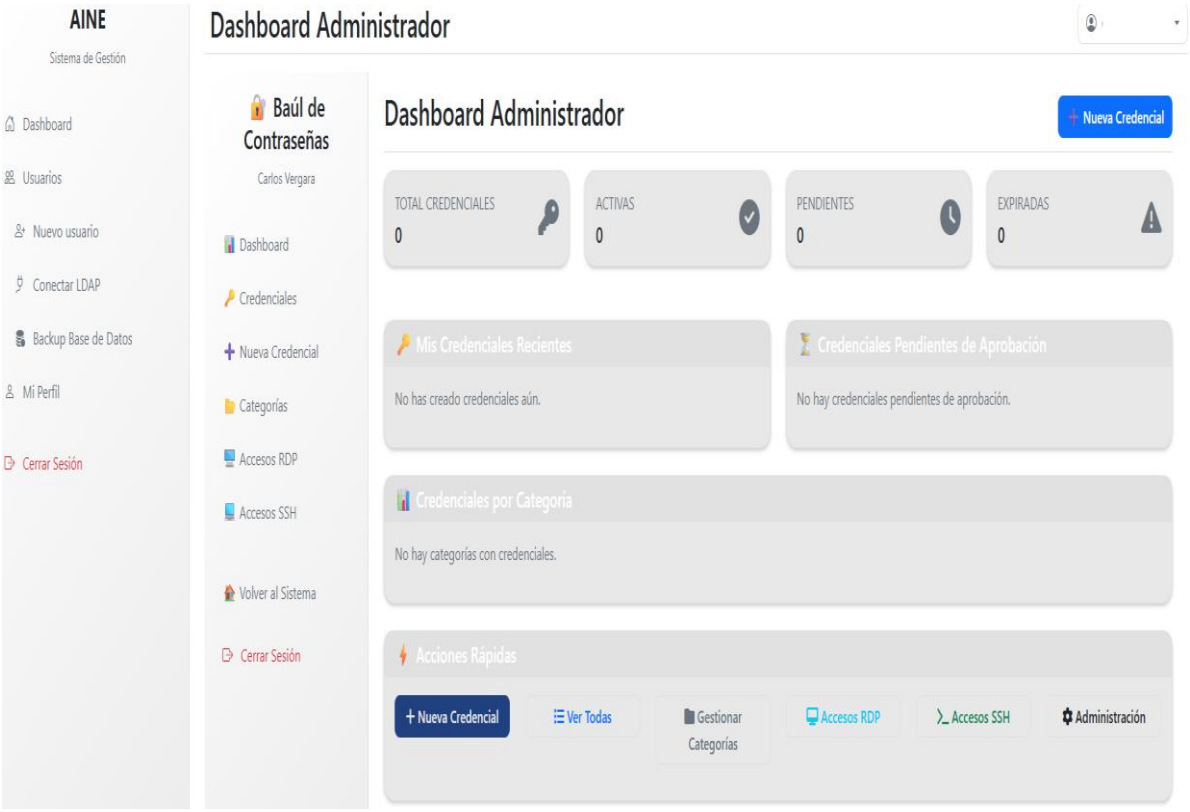


Ilustración 15: Prototipo de Interfaces de Pantalla - Administrador. Fuente: Elaboración Propia

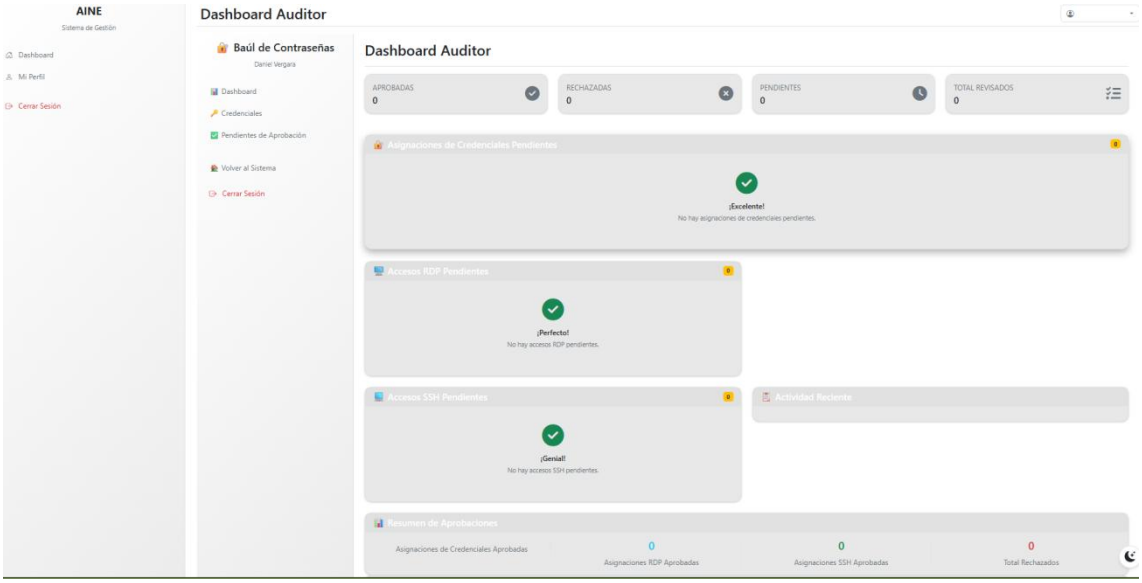


Ilustración 15: Prototipo de Interfaces de Pantalla - Auditor. Fuente: Elaboración Propia

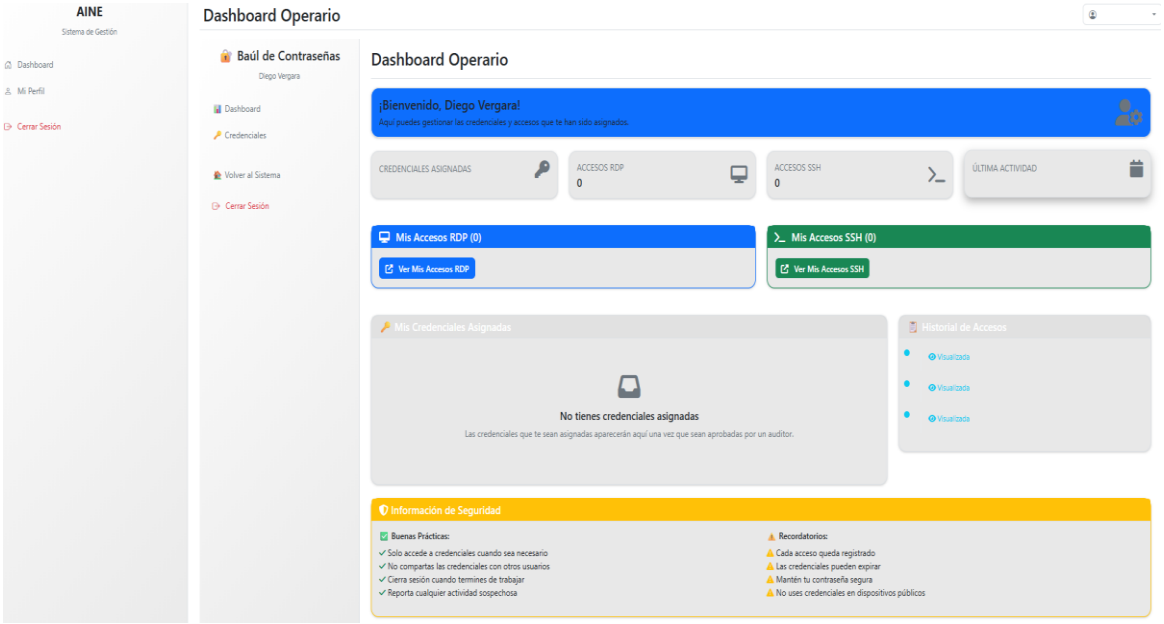


Ilustración 16: Prototipo de Interfaces de Pantalla - Operario. Fuente: Elaboración Propia

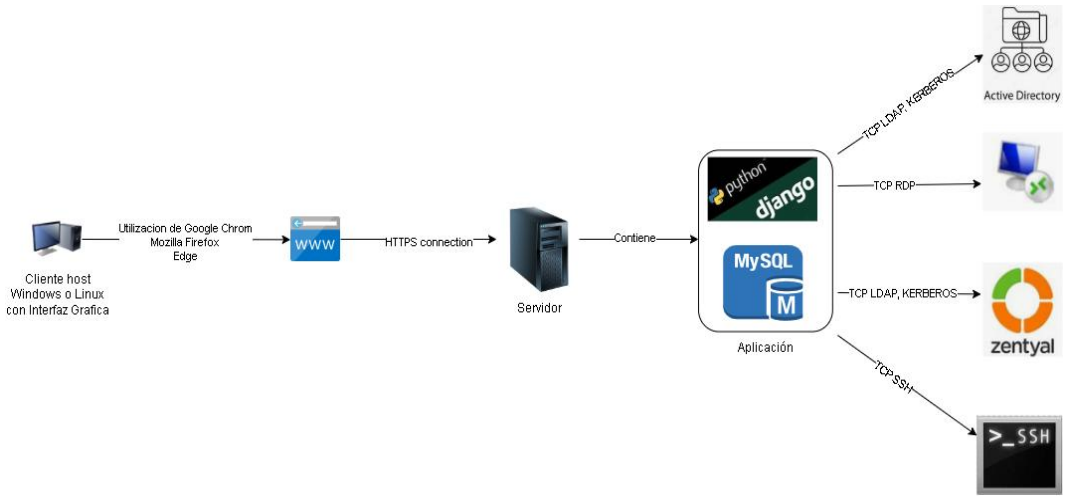


Diagrama de Despliegue

Ilustración 17: Diagrama de Despliegue. Fuente: Elaboración Propia

En el diagrama propuesto, existe un servidor que contiene el framework Django que funciona con el lenguaje de programación Python. Ambos utilizados para programar el front-end y back-end del sistema; y como motor de base de datos se utilizará MySql.

El sistema permitirá el acceso de manera remota a los entornos tipo Windows configurados para tal acceso mediante protocolo RDP, como así también permitirá el acceso de manera remota a los entornos tipo Linux configurados para tal acceso mediante protocolo SSH.

Además permitirá la comunicación con los gestores de credenciales Active Directory (entornos tipo Windows) y Zentyal (entornos tipo Linux) a través de los protocolos LDAP y KERBEROS.

Para poder ser utilizado el sistema, el usuario a través de un cliente host deberá tener un sistema operativo tipo Windows o Linux con interfaz grafica, con alguno de los siguientes buscadores webs: Google Chrome, Mozilla Firefox o Edge.

Seguridad

Los aspectos de seguridad del proyecto son:

1- El nombre de usuario como el email deben ser únicos en el sistema. Es decir, no debe haber dos usuarios con el mismo nombre de usuario o username y e-mail.

2- La contraseña debe cumplir con los siguientes requisitos:

a. No puede ser similar a datos de la cuenta de usuario (nombre, apellido, e-mail).

b. Debe contener al menos 12 caracteres.

c. Debe contener como mínimo una letra mayúscula, una letra minúscula, un número y un carácter especial.

3- La contraseña se cifra mediante el algoritmo PBKDF2 con un hash SHA256. PBKDF2 toma como entrada una contraseña, un salt, un número entero que define cuántas "iteraciones" de la función hash se realizarán y un número entero que describe la longitud de clave deseada para la salida. (https://www.ssltrust.com.au/blog/pbkdf2-password-key-derivation, 2021).

4. Existen 3 perfiles bien diferenciados:

a. Administrado: tiene acceso a realizar:

* Altas/bajas/modificaciones de credenciales estáticas.

* Altas/bajas/modificaciones de accesos RDP y SSH.

* Altas/bajas/modificaciones de credenciales Active Directory y Zentyal.

b. Auditor: tiene acceso a realizar:

* Aprobaciones de las altas realizadas por el administrador, con su respectiva notificación de decisión.

* Auditar todos los sucesos de la aplicación.

c. Operario: tiene acceso a realizar:

* Uso de credenciales estáticas permitidas.

* Uso de accesos RDP y SSH permitidas.

* Uso de credenciales Active Directory y Zentyal permitidas.

5. Si la aplicación es utilizada en un entorno cloud público se puede configurar certificados SSL para cifrar el tráfico en entre el navegador cliente y el servidor, SSL es una tecnología estandarizada que permite cifrar el tráfico de datos entre un navegador web y un sitio web (o entre dos servidores web), protegiendo así la conexión. Haciendo inaccesible la información si fuese interceptada. (https://www.digicert.com/es/what-is-ssl-tls-and-https, 2025)

Política de respaldo de la información

El respaldo de la información es de suma importancia para la recuperación de los sistemas luego de una falla a nivel de hardware o software.

El código fuente de la aplicación será almacenado en cuatro puntos distintos; dos de ellos estarán en nubes públicas destinadas a repositorios de código: GitLab y Github; los otros dos puntos son nubes privadas destinadas a contener en texto plano la estructura completa del código: Google Drive y Mega.

En relación a la información alojada en la base de datos, el sistema contara con una función bajo demanda, que permitirá realizar una copia cifrada; que podrá ser almacenada local o externamente.

Análisis de Costos

Para representar los costos asociados al sistema se presenta un análisis en base a los costos de desarrollo con personal capacitado y equipamiento necesario para su implementación.

A continuación, se detallan los costos relacionados al desarrollo de la aplicación con todos sus componentes.

Los valores de referencia de honorarios mensuales han sido tomados desde la página web del Consejo Profesional de Ciencias Informáticas de la Provincia de Córdoba el día 08/06/2025. (https://cpcipc.org.ar/honorarios-recomendados/, 2025)

Rol	Honorarios Profesionales ($)	Meses	Subtotal ($)
Analista Funcional Junior	1.534.504,25	0.5	767.252,13
Diseño de Páginas Web	1.786.211,22	1	1.786.211,22
Desarrollador Full Stack Developer	2.554.023,97	2	5.108.047,94
Arquitectura de Infraestructura	2.282.360,59	1	2.282.360,59
Tester	1.984.672,85	0.5	992.336,43
		Total Costo de Desarrollo $	10.936.208,31

Tabla 8: Análisis de Costos de Desarrollo. Fuente: Elaboración Propia

Los valores de referencia de costo de hardware han sido tomados desde la página web de Lenovo. (https://www.lenovo.com/ar/es/notebooks/, 2025)

Recurso Hardware/Software	Costo por Unidad ($)	Cantidad	Subtotal ($)
ThinkPad X13 Yoga 4ta Gen (Intel) – Black. SO:Windows 11 Pro.	2.149.998,00	4	8.599.992,00
		Total Costo de Hardware $	8.599.992,00

Tabla 9: Análisis de Costos de Hardware. Fuente: Elaboración Propia

A modo de resumen, se detallan los costos totales del desarrollo.

Concepto	Descripción	Subtotal ($)
Costo de Desarrollo	Costo total para el desarrollo del sistema	10.936.208,31
Costo de Hardware/Software	Costo total del Hardware/Software necesario para el desarrollo	8.599.992,00
	Total Costos $	19.536.200,31

Tabla 10: Análisis de Costos. Fuente: Elaboración Propia

Análisis de Riesgos

A continuación se especifican los riesgos identificados en el proyecto con la probabilidad de ocurrencia.

Identificación de los riesgos

ID	Tipo	Riesgo	Probabilidad	Impacto
1	Proyecto	No conseguir personal idóneo para desarrollar en el proyecto.	Baja	Medio
2	Proyecto	No cumplir con el desarrollo en tiempo y forma.	Media	Alto
3	Proyecto	Abandono del personal afectado al desarrollo.	Media	Alto
4	Proyecto	Incumplimiento de los estándares de funcionamiento por parte de la aplicación.	Media	Medio
5	Proyecto	Cambios de costos por inestabilidad económica (inflación)	Alta	Alto
6	Proyecto	Vulneración del sistema	Baja	Alto
7	Proyecto	Cambios en los protocolos de comunicación.	Baja	Alto

Tabla 11: Identificación de Riesgos. Fuente: Elaboración Propia

En la siguiente tabla se evalúan las causas de los distintos riesgos previamente identificados.

ID	RIESGO	CAUSA
1	No conseguir personal idóneo para desarrollar en el proyecto.	Personal altamente calificado en diferentes tecnologías que es muy demandado en el ambiente laboral.
2	No cumplir con el desarrollo en tiempo y forma.	Demoras o retrasos en etapas del proyecto debido a situaciones externas y/o propias del desarrollo.
3	Abandono del personal afectado al desarrollo.	Personal muy calificado que obtiene mejores propuestas laborales.
4	Incumplimiento de los estándares de funcionamiento por parte de la aplicación.	Fallas en el diseño y desarrollo de la aplicación.
5	Cambios de costos por inestabilidad económica (inflación)	Cambios económicos del país que alteran los costos previamente evaluados.
6	Vulneración del sistema	Vulnerabilidades halladas en funciones o bibliotecas utilizadas.
7	Cambios en los protocolos de comunicación.	Modificación de protocolos de conexión por los fabricantes de hardware.

Tabla 12: Identificación de Riesgos. Fuente: Elaboración Propia

Análisis cualitativo del riesgo

				Impacto				
				Muy Bajo	Bajo	Medio	Alto	Muy Alto
				1	2	3	4	5
Probabilidad	Muy Alta	90%	0,9	0,9	1,8	2,7	3,6	4,5
	Alta	70%	0,7	0,7	1,4	2,1	2,8	3,5
	Media	50%	0,5	0,5	1	1,5	2	2,5
	Baja	30%	0,3	0,3	0,6	0,9	1,2	1,5
	Muy Baja	10%	0,1	0,1	0,2	0,3	0,4	0,5

Tabla 13: Análisis Cualitativo del Riesgo. Fuente: Elaboración Propia

Análisis cuantitativo del riesgo

Para determinar cuáles son los riesgos más peligrosos para el proyecto, se asignaran valores de probabilidad de ocurrencia e impacto a cada uno.

ID	Riesgo	Probabilidad de Ocurrencia	Impacto
1	No conseguir personal idóneo para desarrollar en el proyecto.	30%	3
2	No cumplir con el desarrollo en tiempo y forma.	50%	4
3	Abandono del personal afectado al desarrollo.	50%	4
4	Incumplimiento de los estándares de funcionamiento por parte de la aplicación.	50%	3
5	Cambios de costos por inestabilidad económica (inflación)	70%	4
6	Vulneración del sistema	30%	4
7	Cambios en los protocolos de comunicación.	30%	4

Tabla 14: Análisis Cuantitativo del Riesgo (Ocurrencia – Impacto). Fuente: Elaboración Propia

A continuación se verificará el grado de exposición al riego, que se obtiene de multiplicar el impacto por el porcentaje de probabilidad, luego se ordenan los datos de mayor a menor según grado de exposición.

Riesgo	Probabilidad	Impacto	Grado de Exposición	Porcentaje	Porcentaje Acumulado
Cambios de costos por inestabilidad económica (inflación)	70%	4	2.8	24.14%	24.14%
No cumplir con el desarrollo en tiempo y forma.	50%	4	2	17.24%	41.38%
Abandono del personal afectado al desarrollo.	50%	4	2	17.24%	58.62%
Incumplimiento de los estándares de funcionamiento por parte de la aplicación.	50%	3	1.5	12.93%	71.55%
Vulneración del sistema	30%	4	1.2	10.34%	81.90%
Cambios en los protocolos de comunicación.	30%	4	1.2	10.34%	92.24%
No conseguir personal idóneo para desarrollar en el proyecto.	30%	3	0.9	7.76%	100.00%

Tabla 14: Análisis Cuantitativo del Riesgo (Ocurrencia – Impacto). Fuente: Elaboración Propia

Mediante un diagrama de Pareto se puede verificar de manera gráfica que riesgos afectan de manera significativa el desarrollo de la aplicación en función de su importancia.

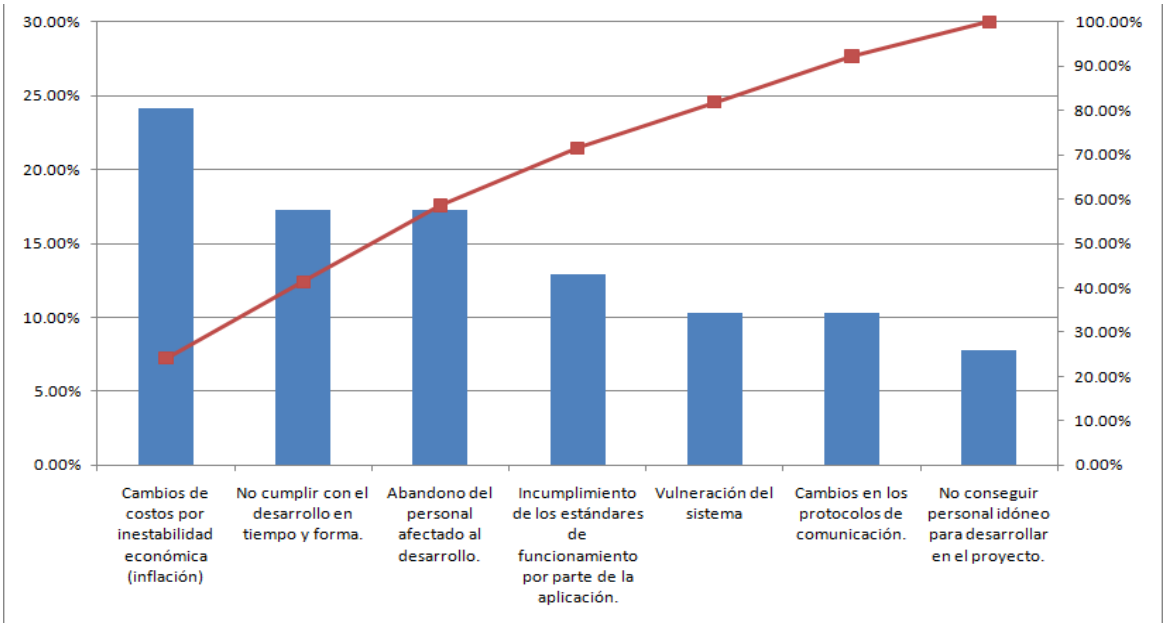


Ilustración 18: Diagrama de Pareto. Fuente: Elaboración Propia

El diagrama permite identificar los 4 principales riesgos que comprenden el 71,55% de posibles problemas en el desarrollo. Por esto se debe enfocar los esfuerzos para evitarlos o minimizarlos al máximo.

Plan de contingencia

El plan de contingencia permitirá afrontar de la mejor manera los principales riesgos asociados al proyecto.

Riesgo	Plan de Contingencia
Cambios de costos por inestabilidad económica (inflación)	Determinar clausulas de actualización de costo en relación a la inflación local.
No cumplir con el desarrollo en tiempo y forma.	Establecer un seguimiento diario de los avances en relación a las situaciones externas y/o internas.

Abandono del personal afectado al desarrollo.	Contar con una actualización de remuneración del personal y además documentación minuciosa del proyecto.
Incumplimiento de los estándares de funcionamiento por parte de la aplicación.	Implementar controles rigurosos que cotejen el desarrollo con los estándares actuales.

Tabla 15: Plan de Contingencia. Fuente: Elaboración Propia

Conclusiones

Se ha llevado a cabo un proyecto que tuvo como objetivo diseñar y desarrollar una aplicación web progresiva, que permita trazar, auditar, controlar y resguardar de manera centralizada los accesos críticos de los sistemas y dispositivos industriales OT, donde las credenciales de acceso/control estén cifradas, con una rotación de modificación que evite usos malintencionados. Logrando la disminución en su totalidad de ciberataques a través de accesos no autorizados.

Ser conscientes de que en la actualidad la infraestructura cibernética como su seguridad son pilares fundamentales de la continuidad de negocio de cualquier compañía, y que el trabajo como diseñadores de estas soluciones debe ser altamente confiable, motivó que este proyecto, logre generar mayor seguridad a entornos industriales, que por su función presentan niveles de criticidad altísimos, y que a su vez mediante una manipulación mal intencionada puede poner en riesgo la vida de muchas personas y demás seres vivos como así también del ambiente que lo rodea.

El conocimiento adquirido a lo largo de la carrera, permitió visualizar una necesidad que debía ser abordada; y además ofreció una solución acorde manteniendo los estándares globales de desarrollo seguro.

Es un desafío constante mantener la integridad de los sistemas con los estándares establecidos, esto implica que el conocimiento en el desarrollo de nuevas tecnologías se mantenga día a día en continua actualización de los saberes, lo cual ha sido logrado con la universidad y que continuará en el tiempo.

Profesionalmente este proyecto permitió comprender de manera más profunda aspectos que pueden pasar desapercibidos o que no son notados en la implementación final de los sistemas, y que sin los cuales no podrían existir o que harían fracasar cualquier tipo de desarrollo.

Finalmente, todo este aprendizaje otorgó herramientas que a pesar de estar pensadas para entornos de desarrollo, pueden ser utilizadas en otros tipos de proyectos donde el orden y control de procedimientos garantizan un correcto abordaje de situaciones, mejorando así el desempeño profesional.

Demo

Para la demostración del Prototipado Tecnológico se anexa un enlace a Google Drive, donde se encuentran la estructura de directorios con los archivos del código fuente, y un video ejemplo que corrobora el funcionamiento de la herramienta.

Link:
https://drive.google.com/drive/folders/1mgC1duKTaVYI5xbQSjCnJkRX0Vya9MXU?usp=drive_link

Referencias

CyberArk Software Ltd. (2024). *cyberark.com*. Recuperado el 27 de abril de 2025, de https://www.cyberark.com/

CyberArk Software Ltd. (2024). *cyberark.com*. Obtenido de https://www.cyberark.com/

Django Project. (2005). *djangoproject.com*. Recuperado el 27 de abril de 2025, de https://www.djangoproject.com

Django Project. (2005). *djangoproject.com*. Obtenido de https://www.djangoproject.com

Donald, B. (15 de junio de 2003). *developer.ibm.com*. Recuperado el 27 de abril de 2025, de developer.ibm.com/articles/an

Hall, D. (13 de mayo de 2015). *github.com/tildaslash/RatticWeb*. Recuperado el 27 de abril de 2025, de https://github.com/tildaslash/RatticWeb

https://cpcipc.org.ar/honorarios-recomendados/. (08 de junio de 2025). Recuperado el 08 de junio de 2025, de https://cpcipc.org.ar/honorarios-recomendados/.

https://www.digicert.com/es/what-is-ssl-tls-and-https. (08 de junio de 2025). Recuperado el 08 de junio de 2025, de https://www.digicert.com/es/what-is-ssl-tls-and-https.

https://www.lenovo.com/ar/es/notebooks/. (08 de junio de 2025). Obtenido de https://www.lenovo.com/ar/es/notebooks/.

https://www.lenovo.com/ar/es/notebooks/. (08 de junio de 2025). Recuperado el 08 de junio de 2025, de https://www.lenovo.com/ar/es/notebooks/.

https://www.ssltrust.com.au/blog/pbkdf2-password-key-derivation. (06 de enero de 2021). Recuperado el junio de 2025, de https://www.ssltrust.com.au/blog/pbkdf2-password-key-derivation.

https://www.ssltrust.com.au/blog/pbkdf2-password-key-derivation. (22 de junio de 2021). Recuperado el 2025 de junio de 2025, de https://www.ssltrust.com.au/blog/pbkdf2-password-key-derivation.

Industrial, Centro de Ciberseguridad. (2021). *www.cci-es.org*. Recuperado el 27 de abril de 2025, de https://www.cci-es.org/

Integrity Advocate. (2025). *integrityadvocate.com*. Recuperado el 27 de abril de 2025, de integrityadvocate.com/support/

Kaspersky. (23 de mayo de 2024). *https://latam.kaspersky.com*. Recuperado el 27 de abril de 2025, de https://latam.kaspersky.com: https://latam.kaspersky.com/about/press-releases/el-promedio-de-ciberataques-a-equipos-ot-en-2023-fue-del-386?srsltid=AfmBOopoS1vxAxyIfO_48yU4tlYL31qBFe-Vl1vDoW3OOAPwRFOJvEkt

Ministros, Jefatura de Gabinete de. (28 de mayo de 2019). *argentina.gob.ar*. Obtenido de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-829-2019-323594

NIST Special Publication 800-37 Revision 2. (01 de Diciembre de 2018). *nvlpubs.nist.gov*. Recuperado el 27 de abril de 2025, de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST Special Publication 800-37 Revision 2. (Diciembre de 2018). *nvlpubs.nist.gov*. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST Special Publication. NIST SP 800-160v1r1. (01 de noviembre de 2022). *nvlpubs.nist.gov*. Recuperado el 27 de abril de 2025, de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

NIST Special Publication. NIST SP 800-160v1r1. (noviembre de 2022). *nvlpubs.nist.gov*. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

ORACLE Coorporation. (2024). *mysql.com*. Obtenido de https://www.mysql.com/why-mysql/

ORACLE Coorporation. (2025). *mysql.com*. Recuperado el 27 de abril de 2025, de https://www.mysql.com/why-mysql/

rattic.org. (2015). *RatticWeb*. Obtenido de https://github.com/tildaslash/RatticWeb

Safe Breach. (27 de abril de 2025). *www.safebreach.com*. Recuperado el 27 de abril de 2025, de www.safebreach.com/blog/bringing-it-and-ot-security-together-bas-purdue/

The Python Software Foundation. (2024). *python.org*. Obtenido de www.python.org/about/apps/

The Python Software Foundation. (2025). *python.org*. Recuperado el 27 de abril de 2025, de www.python.org/about/apps/

Williams, T. (1993). *The Purdue Enterprise Reference Architecture.* IFAC 12th Triennisl World Congress.

World Economic Forum. (10 de Enero de 2024). *www.weforum.org*. Recuperado el 27 de Abril de 2025, de www.weforum.org/publications/global-risks-report-2024/digest/