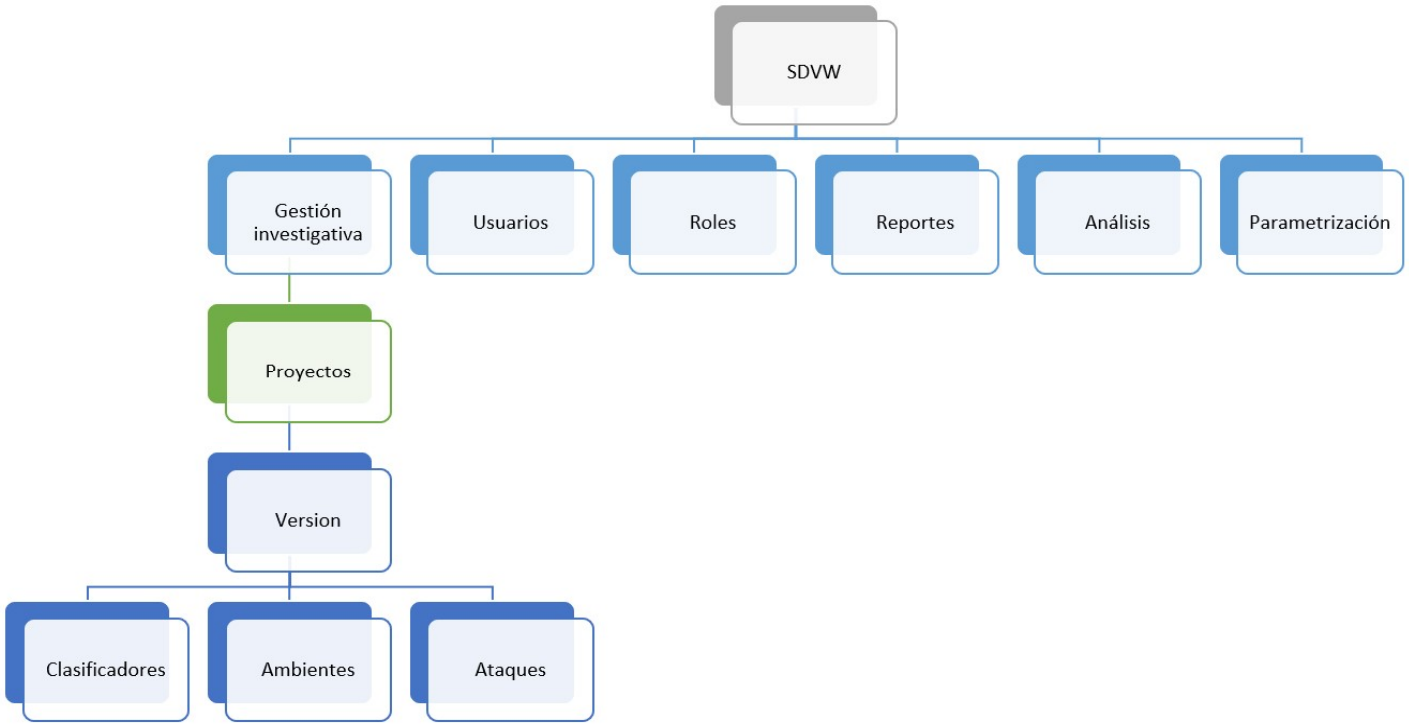

Requerimientos:

R1. El sistema debe permitir crear un usuario con: nombre, correo, contraseña, rol, estado.
R2. El sistema debe permitir modificar el nombre de un usuario.
R3. El sistema debe permitir modificar un rol a un usuario.
R4. El sistema debe permitir modificar la contraseña de un usuario.
R5. El sistema debe permitir cambiar el estado de un usuario.
R6. El sistema debe permitir limpiar una contraseña mediante un correo.
R7. El sistema debe permitir crear un proyecto con: nombre, fecha de creación, autor, estado y tipo de estudio.
R8. El sistema debe permitir gestionar versiones de cada proyecto.
R9. El sistema debe permitir adicionar colaboradores a un proyecto.
R10. El sistema debe permitir remover colaboradores a un proyecto.
R11. El sistema debe permitir modificar el estado del proyecto

R12. El sistema debe permitir modificar el tipo de algoritmo de clasificación
R13. El sistema debe permitir modificar el tipo de entrenamiento del algoritmo
R14. El sistema debe permitir modificar el DataSet de entrenamiento
R15. El sistema debe permitir añadir vulnerabilidades al ambiente controlado
R16. El sistema debe permitir remover vulnerabilidades al ambiente controlado
R17. El sistema debe permitir volver a un estado inicial de un ambiente controlado
R18. El sistema debe permitir realizar ataques a un ambiente controlado
R19. El sistema debe permitir configurar los ataques al ambiente controlado tipo de vulnerabilidades y frecuencia de los ataques.
R20. El sistema debe generar reportes comparativos con los cambios realizados en los proyectos: indicadores estadísticos para la evaluación de estos (aciertos, falsos positivos, falsos negativos).
R21. El sistema debe generar reportes de los ataques que se hayan realizado a la aplicación.
R22. El sistema debe generar reportes de funcionamiento del sistema de detección
R23. El sistema debe permitir crear, modificar y eliminar roles.
R24. El sistema debe tener la capacidad de analizar una captura de tráfico web proporcionada por el usuario, para determinar si pertenece a un ataque, y si lo es, a qué tipo.
R25. El sistema debe poder modificar sus parámetros.

Itearación 1

Requerimiento	Subsistema					
	Gestión investigativa Proyectos Versión	Usuarios	Roles	Reportes	Análisis	Parametrización
R1		X				
R2		X				
R3		X				
R4		X				
R5		X				
R6		X				
R7	X					
R8	X					
R9		X				
R10		X				

R11	X					
R12	X					
R13	X					
R14	X					
R15	X					
R16	X					
R17	X					
R18	X					
R19	X					
R20				X		
R21				X		
R22				X		
R23			X			
R24					X	
R25						X

Proyectos/Versión :

R7.PRY1 El sistema debe permitir crear un proyecto con: nombre, fecha de creación, autor, estado y tipo de estudio.
R8.VER1 El sistema debe permitir gestionar versiones de cada proyecto.
R11.PRY1 El sistema debe permitir modificar el estado del proyecto.
R12.PRY1 El sistema debe permitir modificar el tipo de algoritmo de clasificación.
R13.PRY1 El sistema debe permitir modificar el tipo de entrenamiento del algoritmo .
R14.PRY1 El sistema debe permitir modificar el DataSet de entrenamiento.
R15.PRY1 El sistema debe permitir añadir vulnerabilidades al ambiente controlado.
R16PRY1. El sistema debe permitir remover vulnerabilidades al ambiente controlado.
R17.PRY1 El sistema debe permitir volver a un estado inicial de un ambiente controlado.
R18.PRY1 El sistema debe permitir realizar ataques a un ambiente controlado.
R19.PRY1 El sistema debe permitir configurar los ataques al ambiente controlado tipo de vulnerabilidades y frecuencia de los ataques.

Usuarios:

R1.USU1 El sistema debe permitir crear un usuario con: nombre, correo, contraseña, rol, estado.
R2.USU1 El sistema debe permitir modificar el nombre de un usuario.
R3.USU1 El sistema debe permitir modificar un rol a un usuario.
R4.USU1 El sistema debe permitir modificar la contraseña de un usuario.

R5.USU1 El sistema debe permitir cambiar el estado de un usuario.
R6.USU1 El sistema debe permitir limpiar una contraseña mediante un correo.
R9.USU1 El sistema debe permitir adicionar colaboradores a un proyecto.
R10.USU1 El sistema debe permitir remover colaboradores a un proyecto.

Roles:
R23.ROL1 El sistema debe permitir crear, modificar y eliminar roles.

Reportes:
R20.REP1 El sistema debe generar reportes comparativos con los cambios realizados en los proyectos: indicadores estadísticos para la evaluación de estos (aciertos, falsos positivos, falsos negativos).
R21.REP1 El sistema debe generar reportes de los ataques que se hayan realizado a la aplicación.
R22.REP1 El sistema debe generar reportes de funcionamiento del sistema de detección.

Análisis
R24.ANL1 El sistema debe tener la capacidad de analizar una captura de tráfico web proporcionada por el usuario, para determinar si pertenece a un ataque, y si lo es, a qué tipo.

Parametrización:
R25.PARAM1 El sistema debe poder modificar sus parámetros.

Itearación 2

Requerimiento	Subsistema							
	Gestión investigativa			Usuarios	Roles	Reportes	Análisis	arametrizació
	Proyectos							
	Versión							
	Clasificadores	Ambientes	Ataques					
R12	X							
R13	X							
R14	X							

R15		X						
R16		X						
R17		X						
R18			X					
R19			X					

Clasificadores:

R12.PRY1.CLAS1 El sistema debe permitir modificar el tipo de algoritmo de clasificación.

R13.PRY1.CLAS1 El sistema debe permitir modificar el tipo de entrenamiento del algoritmo de clasificación seleccionado.

R14.PRY1.CLAS1 El sistema debe permitir modificar el DataSet de entrenamiento que usará el clasificador.

Ambientes:

R15.PRY1.AMB1 El sistema debe permitir añadir vulnerabilidades al ambiente controlado.

R16PRY1.AMB1 El sistema debe permitir remover vulnerabilidades al ambiente controlado.

R17.PRY1.AMB1 El sistema debe permitir volver a un estado inicial de un ambiente controlado.

Ataques:

R18.PRY1.ATQ1 El sistema debe permitir realizar ataques a un ambiente controlado.

R19.PRY1.ATQ1 El sistema debe permitir configurar los ataques al ambiente controlado tipo de vulnerabilidades y frecuencia de los ataques.