Requerimientos Funcionales de Software

RF-01	**Realizar diagnóstico de ciber-riesgo**	
Objetivos asociados	Realizar diagnóstico de ciber riesgo sobre la infraestructura tecnológica de red	
Requisitos asociados	Obtener patrones de ataques viables. Obtener patrones de riesgo	
Descripción	El componente deberá realizar el diagnóstico de ciber-riesgos sobre la infraestructura de red	
Precondición	Ninguna.	
Secuencia Normal	**Paso**	**Acción**
	1	Diagnosticador solicita información sobre ataques viables
	2	Generador de ataques viables entrega información a Diagnosticador
	3	Diagnosticador solicita información sobre patrones de riesgo
	4	Gestor de patrones de riesgo entrega información solicitada a Diagnosticador
	5	Diagnosticador realiza diagnóstico de ciber-riesgos en infraestructura en base a información recopilada
Postcondición	Ninguna	
Excepciones	**Paso**	**Acción**
	1	De no existir ataques viables, diagnosticador informará la situación
Rendimiento	**Paso**	**Cota de tiempo**
		10 segundos
Frecuencia esperada	1 veces/día	
Comentarios		

RF-02	**Obtener patrones de ataques viables**	
Objetivos asociados	Determinar patrones de ataques viables sobre infraestructura de red, en base al diagnóstico de vulnerabilidades.	
Requisitos asociados	Realizar diagnóstico de vulnerabilidades	
Descripción	El componente deberá determinar los patrones de ataque viables en base a una infraestructura de red.	
Precondición	Poseer base de datos con patrones de ataques viables existentes y sus vulnerabilidades asociadas.	
Secuencia Normal	**Paso**	**Acción**
	1	Generador de ataques viables realiza diagnóstico de vulnerabilidades
	2	Generador de ataques viables consulta información de patrones a base de datos.
	3	Generador de ataques viables determina la relación o dualidad entre patrones de ataques y vulnerabilidades.
	4	Generador de ataques viables determina patrones de ataques viables en la infraestructura de red
Postcondición	Generador de ataques viables entrega información a diagnosticador	
Excepciones	**Paso**	**Acción**
	4	De no existir ataques viables, generador de ataques viables informará a diagnosticador.
Rendimiento	**Paso**	**Cota de tiempo**
		10 segundo
Frecuencia esperada	1 veces/día	
Comentarios		

RF-03	**Obtener patrones de riesgo**	
Objetivos asociados	Determinar los riesgos asociados a la información obtenida sobre infraestructura	
Requisitos asociados	Ninguno.	
Descripción	El componente gestor de patrones de ataque deberá determinar los riesgos asociados a la información de infraestructura otorgada.	
Precondición	Debe existir información de infraestructura otorgada.	
Secuencia Normal	**Paso**	**Acción**
	1	Gestor de patrones de riesgo solicitará datos de infraestructura a componente cliente.
	2	Componente cliente entregará información de infraestructura asociada.
	3	Gestor de patrones de riesgo determinará los patrones de riesgo, asociados a la información de la infraestructura.
Postcondición	Gestor de patrones de riesgo entregará información a diagnosticador	
Excepciones	**Paso**	**Acción**
	2	De no existir datos de infraestructura asociados, gestor de patrones de riesgo notificará a diagnosticador.
	3	De no existir patrones de riesgo asociados, notificará a diagnosticador.
Rendimiento	**Paso**	**Cota de tiempo**
		5 segundo
Frecuencia esperada	1 veces/día	
Comentarios		

RF-04	**Realizar diagnóstico de vulnerabilidades**	
Objetivos asociados	Realizar y entregar información acerca del diagnóstico de vulnerabilidades	
Requisitos asociados	Ninguno.	
Descripción	El componente generador de ataques viables deberá realizar el análisis de infraestructura de red mediante herramientas conocidas y validadas a fin de determinar vulnerabilidades existentes.	
Precondición	Ninguna.	
Secuencia Normal	**Paso**	**Acción**
	1	El generador de ataques viables realizará un análisis de disponibilidad del protocolo ICMP, mediante comando ping
	2	El generador de ataques viables determinará si la infraestructura presenta vulnerabilidades asociadas al protocolo ICMP (posibilidad de ping)
	3	El generador de ataques viables realizará análisis de puertos abiertos mediante herramienta nmap.
	4	El generador de ataques viables detectará vulnerabilidades asociadas a los puertos abiertos encontrados.
Postcondición	Se utilizará diagnóstico de vulnerabilidades para obtener patrones de ataque viables.	
Excepciones	**Paso**	**Acción**
	1	En caso de no tener conexión a internet, se notificará al diagnosticador.
	3	En caso de no tener conexión a internet, se notificará al diagnosticador.
Rendimiento	**Paso**	**Cota de tiempo**
		100 segundo
Frecuencia esperada	1 veces/día	
Comentarios		

RF-05	**Proponer solución de seguridad sobre infraestructura de red**	
Objetivos asociados	Proponer una solución de seguridad, frente a los riesgos asociados a la infraestructura de red analizada.	
Requisitos asociados	Realizar diagnóstico de ciber-riesgo.	
Descripción	El sistema pronosticador, propondrá a través de una interfaz de usuario, una solución de seguridad frente al análisis y resultados obtenidos.	
Precondición	Diagnóstico de ciber-riesgo realizado.	
Secuencia Normal	**Paso**	**Acción**
	1	Mediante interfaz de usuario se iniciará proceso de generación de propuesta de mejora de infraestructura
	2	El componente “propuesta infraestructura” solicitará al diagnosticador el diagnóstico de ciber-riesgos.
	3	El diagnosticador entregará al componente “propuesta infraestructura” la información sobre el diagnóstico realizado.
	2	El componente “propuesta infraestructura” analizará la información obtenida del diagnóstico de ciber-riesgos.
	3	El componente “propuesta infraestructura” realizará una propuesta de mejora de infraestructura, basándose en las vulnerabilidades de red y patrones de ataque detectados.
	4	Se mostrará mediante interfaz de usuario la propuesta realizada.
Postcondición	Ninguna	
Excepciones	**Paso**	**Acción**
	2	En caso de no existir diagnóstico de ciber-riesgo, se notificará mediante interfaz de usuario.
Rendimiento	**Paso**	**Cota de tiempo**
		20 segundo
Frecuencia esperada	1 veces/mes	
Comentarios	ninguno	

Requerimientos no funcionales

1. El sistema será desarrollado para las plataformas Windows o Linux.
2. La interfaz de usuario será implementada como sistema de escritorio.
3. El sistema deberá mantener los datos protegidos del acceso no autorizado
4. El sistema debe contar con manual de usuario estructurado.
5. El sistema solo debe funcionar conectado a internet.