Requerimientos Funcionales de Software

RF-01	**Consulta patrones de ataques viables**	
Objetivos asociados	Gestionar los patrones de ataques viables	
Requisitos asociados	Información sobre patrones de ataque existentes	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el encargado de seguridad lo considere oportuno	
Precondición	ninguna	
Secuencia Normal	**Paso**	**Acción**
	1	El encargado de seguridad solicita al sistema información acerca de los patrones de ataque viables en la empresa.
	2	El sistema analiza la infraestructura y muestra la información asociada a los patrones de ataque viables: nombre, nivel de riesgo asociado, impacto, vulnerabilidad, datos técnicos.
	3	El sistema almacena información recopilada para acciones futuras.
	4	Si el encargado de seguridad desea enviar información al correo o imprimir como PDF, el sistema realiza la acción solicitada.
Postcondición	Ninguna	
Excepciones	**Paso**	**Acción**
	4	Si el encargado de seguridad solicita cancelar la operación, el sistema cancela la operación, a continuación este caso de uso termina
	2	En caso de no presentar patrones de ataques viables, el sistema informa al usuario, a continuación este caso de uso termina.
Rendimiento	**Paso**	**Cota de tiempo**
	4	5 segundo
Frecuencia esperada	1 veces/día	
Comentarios	El formato de visualización de los datos está pendiente de definición	

RF-02	**Propuesta plan de mejora de Infraestructura**	
Objetivos asociados	Ejecutar plan de mejora sobre las vulnerabilidades asociadas	
Requisitos asociados	Información sobre patrones de ataque existentes	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el encargado de seguridad lo considere oportuno	
Precondición	Se han consultado los patrones de ataque viables	
Secuencia Normal	**Paso**	**Acción**
	1	El encargado de seguridad solicita al sistema propuesta de mejora de infraestructura basada en análisis de patrones viables
	2	El sistema elabora y permite visualización de propuesta de mejora de infraestructura asociada.
	3	El encargado de seguridad puede solicitar realizar modificaciones en el plan de mejora propuesto
	4	El sistema permite al encargado de seguridad modificar el plan propuesto en base a su criterio.
	5	El encargado de seguridad puede solicitar el envío del plan generado vía correo electrónico o imprimir en formato PDF
	6	El sistema guarda los datos del plan propuesto y modificado, luego realiza la acción solicitada.
Postcondición	Ninguna	
Excepciones	**Paso**	**Acción**
	5	Si el encargado de seguridad solicita cancelar la operación, el sistema cancela la operación, a continuación este caso de uso termina
	2	En caso de no identificar posibles mejoras en la infraestructura, el sistema informa al usuario, a continuación este caso de uso termina.
Rendimiento	**Paso**	**Cota de tiempo**
	4	5 segundo
Frecuencia esperada	1 veces/día	
Comentarios	El formato de visualización de los datos está pendiente de definición	

RF-03	**Calcula variación de probabilidad de ataques**	
Objetivos asociados	Comprobar la mejora obtenida en base al plan propuesto	
Requisitos asociados	Plan de mejora generado.	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el encargado de seguridad lo considere oportuno	
Precondición	Se ha generado e implementado un plan de mejora	
Secuencia Normal	**Paso**	**Acción**
	1	El encargado de seguridad solicita al sistema cuantificar la mejora obtenida tras la implementación del plan (reducción de % de riesgo).
	2	El sistema cuantifica la diferencia del riesgo sobre la infraestructura, antes y después de la implementación del plan y muestra la información al encargado de seguridad.
	3	El encargado de seguridad puede solicitar al sistema información detallada de ataques y la mejora en cuestión.
	4	El sistema muestra la información solicitada al encargado de seguridad
	5	El encargado de seguridad puede solicitar el envío de la información obtenida, vía correo electrónico, o imprimir en formato PDF
	6	El sistema guarda la información, luego realiza la acción solicitada.
Postcondición	Ninguna	
Excepciones	**Paso**	**Acción**
	5	Si el encargado de seguridad solicita cancelar la operación, el sistema cancela la operación, a continuación este caso de uso termina
Rendimiento	**Paso**	**Cota de tiempo**
	4	5 segundo
Frecuencia esperada	3 veces/día	
Comentarios	El formato de la cuantificación está pendiente de definición.	

RF-03	**Compara ciber-ataques viables**	
Objetivos asociados	Obtener información acerca de cuáles ciber-ataques son más críticos y generan mayor impacto negativo sobre la infraestructura, en caso de ser ejecutados.	
Requisitos asociados	Información sobre ciber-ataques viables.	
Descripción	El sistema deberá comportarse tal como se describe en el siguiente caso de uso cuando el encargado de seguridad lo considere oportuno	
Precondición	Se han consultado los patrones de ataque viables	
Secuencia Normal	**Paso**	**Acción**
	1	El encargado de seguridad solicita al sistema comparar dos ciber-ataques viables, a fin de manejarlos en orden de riesgo, impacto y criticidad.
	2	El sistema muestra la información solicitada al encargado de seguridad: Nombre, % de probabilidad, criticidad, impacto sobre la infraestructura, riesgos asociados, prioridad.
	3	El encargado de seguridad puede solicitar acceder al historial de un ciber-ataque particular y ver cómo ha variado su probabilidad de ser ejecutado en el tiempo.
	4	El sistema muestra la información solicitada al encargado de seguridad
Postcondición	Ninguna	
Excepciones	**Paso**	**Acción**
	3	Si el encargado de seguridad solicita cancelar la operación, el sistema cancela la operación, a continuación este caso de uso termina
	4	En caso de no presentar historial del ciber-ataque particular, el sistema informa al usuario, a continuación este caso de uso termina.
Rendimiento	**Paso**	**Cota de tiempo**
	4	5 segundo
Frecuencia esperada	20 veces/día	
Comentarios	El formato de la cuantificación está pendiente de definición.	

RF-05	**Obtener información de patrones existentes**	
Objetivos asociados	Obtener información de patrones de ataque existentes para pronosticar riesgos en una infraestructura determinada.	
Requisitos asociados	ninguna	
Descripción	El sistema deberá mantener actualizada la información acerca de patrones de ataques existente.	
Precondición	ninguna	
Secuencia Normal	**Paso**	**Acción**
	1	El sistema solicitará información actualizada de patrones de ciber-ataques existentes. conectará con repositorios, a fin de actualizar información de patrones de ciber ataques.
	2	El sistema recepciona información entregada por repositorios y la almacena, a fin de mantener actualizado el registro de ciber-ataques existentes.
Postcondición	Ninguna	
Excepciones	**Paso**	**Acción**
	1	En caso de no presentar conexión a internet, el sistema se mantendrá intentando hasta conseguirlo, posteriormente notificará al encargado vía correo electrónico. A continuación este caso de uso termina.
Rendimiento	**Paso**	**Cota de tiempo**
	4	10 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.