

ADQUIRIR HERRAMIENTAS DE SOFTWARE QUE FACILITE Y SOPORTE EL ANÁLISIS DE VULNERABILIDADES EN LOS SISTEMAS Y PROCESOS INSTITUCIONALES, SIN INCLUIR LA PRESTACIÓN DIRECTA DEL SERVICIO DE ANÁLISIS NI CONSULTORÍA																						
N°	Clase	Fuente	Etapas	Tipo	Descripción(Que puede pasar y cómo puede ocurrir)	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración del Riesgo	Categoría	¿A quien se le asigna?	Tratamiento /Controles a ser Implementados	Impacto después del tratamiento				Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y Revisión		
													Probabilidad	Impacto	Valoración del Riesgo	Categoría				¿Afecta la ejecución del control?	¿Cómo se realiza el monitoreo?	Periodicidad ¿ Cuando?
	Específico	Externo	Ejecución	Tecnológico	La herramienta presenta incompatibilidades técnicas con la infraestructura institucional por diferencias en arquitectura, protocolos o capacidades de integración, generando fallas en su despliegue o funcionamiento parcial.	Retrasos en la puesta en operación y limitación en la ejecución de análisis sobre activos críticos, afectando el cumplimiento del objeto contractual.	4	5	9	Riesgo Extremo	Contratista	Validación de compatibilidad técnica previa, pruebas de integración, certificación de interoperabilidad y aceptación técnica por parte del supervisor.	2	4	6	Riesgo Alto	Si	Contratista	Acta de inicio del contrato	Acta de recibo a satisfacción de la implementación	Validación de pruebas de integración y actas de aceptación técnica.	Semanal
2	General	Interno	Planeación	Tecnológico	El inventario de activos institucionales no se encuentra completamente identificado o actualizado, generando omisiones en la cobertura del análisis de vulnerabilidades.	Cobertura parcial del análisis de seguridad y posibles vulnerabilidades no identificadas en activos no incluidos.	3	5	8	Riesgo Extremo	Entidad	Validación y depuración del inventario de activos previo al inicio del contrato y articulación con el contratista para su inclusión en la herramienta.	2	4	6	Riesgo Alto	Si	Entidad	Etapas precontractual	Entrega oficial del inventario validado al contratista	Verificación del inventario frente a reportes de cobertura.	Mensual
3	Específico	Externo	Ejecución	Tecnológico	La configuración inicial de la herramienta es inadecuada, generando resultados erróneos en la identificación o priorización de vulnerabilidades.	Falsos positivos o negativos y decisiones técnicas basadas en información no confiable.	4	5	9	Riesgo Extremo	Contratista	Parametrización conforme a estándares (CVSS), validación técnica y aprobación de línea base por la supervisión.	2	4	6	Riesgo Alto	Si	Contratista	Fase de configuración inicial	Aprobación del informe de línea base	Revisión técnica de resultados y validación funcional.	Mensual
4	Específico	Externo	Ejecución	Operacional	Se presentan retrasos en la instalación o puesta en operación por incumplimiento del cronograma del contratista.	Afectación del plazo contractual y retraso en la ejecución del análisis de vulnerabilidades.	3	5	8	Riesgo Extremo	Contratista	Seguimiento a cronograma, control de hitos y aplicación de cláusulas de incumplimiento.	2	4	6	Riesgo Alto	Si	Contratista	Acta de inicio	Cumplimiento de hitos contractuales	Seguimiento a cronograma y reportes de avance.	Semanal
5	Específico	Externo	Ejecución	Tecnológico	La herramienta no logra integrarse con sistemas institucionales debido a limitaciones técnicas del proveedor.	Pérdida de interoperabilidad y disminución de la eficiencia del ecosistema de seguridad.	4	4	8	Riesgo Extremo	Contratista	Pruebas de integración, validación de APIs y cumplimiento de estándares de interoperabilidad.	2	3	5	Riesgo Medio	Si	Contratista	Inicio fase de integración	Validación de integraciones	Pruebas funcionales y revisión de logs.	Mensual
6	Específico	Externo	Ejecución	Tecnológico	El proveedor no realiza actualizaciones oportunas de la base de datos de vulnerabilidades.	Desactualización del sistema y aumento del riesgo de incidentes.	3	5	8	Riesgo Extremo	Contratista	Control de versiones, validación de actualizaciones y cumplimiento de soporte.	2	4	6	Riesgo Alto	Si	Contratista	Inicio operación	Verificación continua durante ejecución	Revisión de versiones y reportes.	Mensual
7	Específico	Externo	Ejecución	Tecnológico	La herramienta no cumple con los niveles de servicio establecidos (SLA).	Interrupciones en la operación y afectación de continuidad.	3	5	8	Riesgo Extremo	Contratista	Monitoreo de SLA, penalidades y control de disponibilidad.	2	4	6	Riesgo Alto	Si	Contratista	Inicio operación	Seguimiento de SLA	Monitoreo de disponibilidad.	Mensual
8	Específico	Externo	Ejecución	Seguridad	Se presenta fuga de información o accesos no autorizados por deficiencias en controles de seguridad de la herramienta.	Compromiso de la seguridad de la información institucional.	3	5	8	Riesgo Extremo	Contratista	Implementación de controles de acceso, cifrado y auditoría.	2	4	6	Riesgo Alto	Si	Contratista	Configuración de seguridad	Auditoría aprobada	Revisión de logs y auditorías.	Mensual
9	General	Interno	Ejecución	Operacional	El personal institucional no apropia la herramienta por deficiencias en gestión interna del conocimiento.	Uso ineficiente de la solución y dependencia operativa.	3	4	7	Riesgo Alto	Entidad	Gestión interna del conocimiento y validación de apropiación funcional.	2	3	5	Riesgo Medio	Si	Entidad	Inicio transferencia de conocimiento	Validación de uso autónomo	Evaluación de uso y desempeño.	Mensual
10	Específico	Externo	Ejecución	Contractual	El licenciamiento entregado presenta restricciones que limitan el uso de la herramienta.	Incumplimiento del objeto contractual y limitación funcional.	3	5	8	Riesgo Extremo	Contratista	Validación contractual del licenciamiento y certificación del fabricante.	2	4	6	Riesgo Alto	Si	Contratista	Revisión del licenciamiento	Validación funcional completa	Pruebas de funcionalidades.	Mensual