

Risk Source	Probability			Impact			Result	Impact Areas			Response Plan	Status
	Low	Medium	High	Low	Medium	High		Cost	Schedule	Performance		
1 <b>Ataque cibernetico al sistema de control</b> Karyme V		5				9	45	×	×	×	Para mitigar un posible ataque cibernetico al sistema de control, se deben aplicar medidas de ciberseguridad como firewalls, antivirus, segmentación de redes, autenticación robusta y actualizaciones periódicas. Además, es clave contar con un plan de respuesta a incidentes y capacitar al personal en buenas prácticas de seguridad.	Open
2 <b>Retrasos en la implementacion</b> Karyme V		4				8	32	×	×	×	Para mitigar los retrasos en la implementación, es importante planificar con tiempos realistas, asignar recursos adecuados, hacer seguimiento constante al avance y anticipar posibles riesgos con planes de contingencia para resolver obstáculos rápidamente.	Open
3 <b>Desaguste entre el inventario fisico y el sistema</b> Karyme V		4				8	32	×	×		Para mitigar el desajuste entre el inventario físico y el sistema, es clave implementar controles periódicos de auditoría y conciliación, capacitar al personal en registros precisos, automatizar el ingreso y salida de inventario cuando sea posible,	Open
4 <b>Ausensia de plan de respuesta ante incidentes</b> Karyme V		5			6		30	×	×	×	Para mitigar la ausencia de un plan de respuesta ante incidentes, es fundamental desarrollar e implementar un protocolo claro que incluya la detección, análisis, contención, recuperación y notificación de incidentes. Este plan debe ser probado regularmente y conocido por todo el personal involucrado.	Open

5	<b>Incumplimiento de ley de protección de datos</b> Karyme V	3					9	27	×	×	×	Para mitigar el incumplimiento de la Ley de Protección de Datos, se debe implementar políticas claras de privacidad, asegurar el consentimiento informado de los usuarios, aplicar medidas técnicas como cifrado y control de accesos, y capacitar al personal en el manejo adecuado de datos personales conforme a la normativa vigente.	Open
6	<b>Falta de capacitación de personal</b> Karyme V		4			6		24	×	×	×	Para mitigar la falta de capacitación del personal, se debe implementar un plan de formación continua que incluya entrenamientos técnicos, manuales de usuario y sesiones prácticas, asegurando que el equipo cuente con las competencias necesarias para operar y mantener el sistema eficientemente.	Open
7	<b>Resistencia al cambio de proceso</b> Karyme V		4			6		24		×	×	Para mitigar la resistencia al cambio de proceso, es clave comunicar claramente los beneficios del cambio, involucrar al personal desde etapas tempranas, ofrecer capacitaciones adecuadas y acompañamiento durante la transición, fomentando así una actitud positiva y participativa hacia la nueva forma de trabajo.	Open
8	<b>Fallo de los módulos durante la marcha blanca</b> Karyme V		4			6		24	×	×	×	Para mitigar el fallo de módulos durante la marcha blanca, se debe realizar pruebas exhaustivas en ambientes controlados antes del lanzamiento, contar con un plan de contingencia para resolver problemas rápidamente, y mantener un monitoreo constante durante esta fase para detectar y corregir fallos de forma ágil.	Open
9	<b>Contraseñas administrativas débiles</b> Karyme V		6			4		24	×	×		Para mitigar el uso de contraseñas administrativas débiles, se deben establecer políticas de seguridad que exijan contraseñas complejas y únicas, implementar autenticación multifactor, y realizar capacitaciones periódicas para concienciar al personal sobre la	Open

												importancia de una buena gestión de contraseñas.	
10	<b>capacitacion insuficiente del personal</b> Karyme V		4			5		20	×	×	×	<p>Para mitigar la capacitación insuficiente del personal, es importante diseñar un programa de formación completo y continuo, que incluya materiales actualizados, sesiones prácticas y evaluaciones periódicas, garantizando que el equipo adquiera y mantenga las habilidades necesarias para operar eficazmente.</p>	Open
11	<b>Mal registro de auditoria</b> Karyme V	3				6		18	×	×	×	<p>Para mitigar el mal registro de auditoría, es importante implementar sistemas automáticos de registro con controles de integridad, definir qué eventos deben auditarse, capacitar al personal en la correcta generación y revisión de registros, y realizar auditorías periódicas para asegurar que los registros sean completos y confiables.</p>	Open
12	<b>Mal registro de auditoria</b> Karyme V	3				6		18	×	×	×	<p>Para mitigar el mal registro de auditoría, es importante implementar sistemas automáticos de registro con controles de integridad, definir qué eventos deben auditarse, capacitar al personal en la correcta generación y revisión de registros, y realizar auditorías periódicas para asegurar que los registros sean completos y confiables.</p>	Open
13	<b>Sobre costos de compra de equipo y licencias</b> Karyme V	2					8	16	×	×	×	<p>Para mitigar los sobrecostos en la compra de equipos y licencias, se debe realizar una planificación financiera detallada, comparar múltiples proveedores, priorizar soluciones escalables o de código abierto cuando sea posible, y evaluar bien las necesidades reales del sistema antes de realizar adquisiciones.</p>	Open
14	<b>Fallas tecnologicas</b> Karyme V	2				6		12	×	×		<p>Para mitigar las fallas tecnológicas, es fundamental realizar mantenimientos preventivos periódicos, contar con sistemas de respaldo y</p>	Open

												recuperación, monitorear el rendimiento constantemente, y capacitar al personal para la detección temprana y solución rápida de problemas técnico	
15	<b>Tiempo de respuestas tardío</b> Karyme V		5		2			10	×	×		Para mitigar el tiempo de respuesta tardío, se deben optimizar las consultas y procesos del sistema, mejorar la infraestructura de red y servidor, y aplicar técnicas de caché. Además, es clave monitorear continuamente el rendimiento para detectar cuellos de botella y aplicar mejoras proactivas.	Open
16	<b>Alcance del proyecto mal definido</b> Karyme V	1					9	9	×	×	×	Para mitigar un alcance del proyecto mal definido, es clave establecer objetivos claros y específicos desde el inicio, involucrar a todas las partes interesadas en la definición de requerimientos, y documentar detalladamente el alcance para evitar confusiones o cambios inesperados durante el desarrollo.	Open
17	<b>Incompatibilidad con módulos del sistema</b> Karyme V	1				6		6	×	×	×	Para mitigar la incompatibilidad con módulos del sistema, se debe realizar una evaluación previa de compatibilidad antes de integrar nuevos módulos, utilizando entornos de prueba controlados. Además, se recomienda mantener actualizada la documentación técnica, implementar versiones estables y establecer un plan de retroceso en caso de fallos, asegurando una integración gradual y monitoreada.	Open
18	<b>Asignación incorrecta de permisos</b> Karyme V	1				5		5		×	×	Para mitigar la asignación incorrecta de permisos, se debe establecer una política clara de roles y accesos basada en el principio de mínimo privilegio, realizar revisiones periódicas de permisos, y capacitar al personal encargado para asegurar que solo los usuarios autorizados tengan acceso a funciones y datos según su responsabilidad.	Open

19	Redundancia en el servidor de acceso Karyme V	1			3			3	×	×	×	Para mitigar la redundancia en el servidor de acceso, se debe implementar un sistema de balanceo de carga y servidores en alta disponibilidad (HA), que distribuyan el tráfico y aseguren la continuidad del servicio en caso de fallas, minimizando puntos únicos de fallo y garantizando la disponibilidad del sistema.	Open
----	--	---	--	--	---	--	--	---	---	---	---	---	------

	Risk	Date Created	Created By	Date Updated	Updated By
1	Ataque cibernetico al sistema de control	09/30/2025 17:38	Karyme V	09/30/2025 17:48	Karyme V
2	Retrasos en la implementacion	09/30/2025 17:47	Karyme V	09/30/2025 17:47	Karyme V
3	Desaguste entre el inventario fisico y el sistema	09/30/2025 17:50	Karyme V	09/30/2025 17:50	Karyme V
4	Ausensia de plan de respuesta ante incidentes	09/30/2025 17:40	Karyme V	09/30/2025 17:40	Karyme V
5	Incumplimineto de ley de proteccion de datos	09/30/2025 17:37	Karyme V	09/30/2025 17:37	Karyme V
6	Falta de capacitacion de personal	09/30/2025 17:33	Karyme V	09/30/2025 17:33	Karyme V
7	Resistencia al cambio de proceso	09/30/2025 17:34	Karyme V	09/30/2025 17:34	Karyme V
8	Fallo de los modulos durante la marcha blanca	09/30/2025 17:41	Karyme V	09/30/2025 17:41	Karyme V
9	Contraseñas administratibas debiles	09/30/2025 17:43	Karyme V	09/30/2025 17:44	Karyme V
10	capacitacion insuficiente del personal	09/30/2025 17:42	Karyme V	09/30/2025 17:42	Karyme V
11	Mal registro de auditoria	09/30/2025 17:52	Karyme V	09/30/2025 17:52	Karyme V
12	Mal registro de auditoria	09/30/2025 17:52	Karyme V	09/30/2025 17:52	Karyme V
13	Sobre costos de compra de equipo y licencias	09/30/2025 17:36	Karyme V	09/30/2025 17:48	Karyme V
14	Fallas tecnologicas	09/30/2025 17:49	Karyme V	09/30/2025 17:49	Karyme V
15	Tiempo de respuestas tardio	09/30/2025 17:32	Karyme V	09/30/2025 17:32	Karyme V
16	Alcence del proyecto mal definido	09/30/2025 17:47	Karyme V	09/30/2025 17:47	Karyme V
17	Incompatibilidad con modulos del sistema	09/30/2025 17:29	Karyme V	09/30/2025 17:29	Karyme V
18	Asignacion incorrecta de permisos	09/30/2025 17:51	Karyme V	09/30/2025 17:51	Karyme V
19	Redundancia en el servidor de acceso	09/30/2025 17:31	Karyme V	09/30/2025 17:31	Karyme V

