Categoria	Riesgo identificado	Descripcion	Probabilidad	Impacto	Nivel de riesgo	Color	Plan de Mitigacion
Deliberados	Ataques cibernéticos.	Hackers podrian intentar vulnerar la red del sistema de	Alta.	Alta.	Crítico.		medidas de seguridad como cifrado de datos.
	Acceso no autorizado.	Usuarios no autorizados podrían manipular sensores o datos confidenciales dél sistema.	Media.	Alta.	Alto.		Establecer sistemas de autenticación robustos y controles de acceso estrictos.
	Sabotaje interno.	Un empleado podría modificar o dañar el sistema intencionadamente.	Baja.	Alta.	Medio.		Realizar auditorias internas regulares y supervisión de actividades sospechosasa
Accidentales	Fallos en el hardware.	Un fallo en los sensores o servidores podria interrumpir el	Media.	Alta.	Alto.		Mantener un inventario de hardware de repuesto y de estrés periodicas.

	Configuración errónea del sistema	Cambios en la configuracion podrían generar datos erróneos o mal funcionamiento	Alta.	Media.	Alto.		Implementar procedimientos claros para cambios y configuraciones, ademas de pruebas previas en entornos controlados.
	Pérdida de energía	Un corte de energía podria desconectar servidores y sensores.	Media.	Alta.	Alto.		Instalar sistemas de respaldo de energía, como UPS o generadores.
Ambientales	Fenomenos naturales (inundaciones, terremotos, etc.)	Eventos climaticos extremos o desastres naturales podrían dañar la infraestructura del sistema.	Baja.	Alta.	Medio.		Construir sistemas en ubicaciones seguras y mantener planes de contingencia para recuperarse ante desastres.
	Interferencias electromagnéticas.	Equipos cercanos podrían generar ruido electormagnético que afecte la	Baja.	Media.	Bajo.		Utilizar cables y equipos con blindaje electromagnético adecuado.
	Fluctuaciones en las condiciones climáticas.	temperatura o humedad podrían afectar la sensibilidad de los sensores.	Media.	Media.	Medio.		Implemetar sistemas de protección ambiental para los sensores.

Sobre el proyecto	Retrasos en el desarrollo del software.	Problemas técnicos o falta de recursos podrían retrasan la entrega del proyecto.	Media.	Alta.	Alto.		Realizar un cronograma detallado con márgenes de tiempo y priorizar tareas claves.
	Falta de capacitación del personal.	Usuarios finales podrían no entender cómo usar el sistema, cusando errores o frustración.	Alta.	Media.	Alto.		Proporcionar manuales claros y realizar capacitaciones regulares para el personal.
	Dependencia excesiva de un proveedor o tecnología única.	Si el proveedor de sensores o servidores deja de operar, el proyecto podría colapsar.	Media.	Alta.	Alto.		Diversificar proveedores y utilizar tecnologías estándar.
	Baja adopción del sistema por parte de los usuarios.	Los usuarios podrían resistirse a usar el sistema por desconfianza o falta de interés.	Media.	Media.	Medio.		Realizar campañas de sensibilización, enfocadas en los beneficios del sistema.
Improbables	Fallos catastróficos simultáneos en todos los sensores.	Es altamente improbale que todos los sensores fallen al mismo tiempo.	Muy baja.	Alta.	Bajo.		Diseñar el sistema con redundancia y múltiples nodos de monitoreo.

	Sabotaje externo masivo	Coordinación masiva para destruir infraestructura fisica o digital.	Muy baja.	Muy alta.	Bajo.		Diseñar ubicaciones seguras para infraestructura fisica y contar con protocolos de respuesta rápida en caso de emergencias.

Leyenda de colores	
	Riesgos críticos (requieren
	Riesgos altos (importantes, necesitan planes de acción efectivos).
	moderados (deben monitorearse y mitigarse con planes preventivos).
	(pueden ocurrir, pero tienen un impacto limitado;