



CUESTIONARIO

Seguridad de la Información

1. ¿Qué mecanismos de control de acceso se encuentran implementados para asegurar que solo usuarios autorizados puedan acceder a la información sensible y a las funcionalidades críticas del sistema?
2. ¿Cuál es el procedimiento establecido para la gestión del ciclo de vida de las contraseñas, incluyendo la definición de políticas de complejidad, rotación periódica y almacenamiento seguro mediante técnicas de cifrado robustas?

Infraestructura Tecnológica

3. ¿La infraestructura tecnológica del sistema es escalable y flexible para adaptarse a futuras necesidades y crecimientos en la demanda de recursos?
4. ¿Se cuenta con planes y procedimientos de respaldo y recuperación ante desastres para garantizar la disponibilidad y la integridad de los datos en caso de fallos o incidentes?

Desarrollo y Mantenimiento

5. ¿Se actualiza regularmente el sistema de captura de incidencias para incorporar nuevas funcionalidades o corregir errores reportados por el personal veterinario?
6. ¿El software pasa por procesos de prueba automatizados y manuales para asegurar su correcto funcionamiento? De ser así, ¿qué tipos de pruebas se aplican?

Procedimientos y Control Interno

7. ¿Hay lineamientos definidos para el personal veterinario sobre cómo registrar correctamente una incidencia en el sistema?



8. ¿Se realiza una revisión periódica de los registros de incidencias para verificar su precisión y completitud?

Evaluación General

9. ¿La interfaz de usuario es intuitiva y fácil de usar?
10. ¿Se ha establecido un plan de mantenimiento y actualización del sistema para garantizar su continuidad y relevancia a largo plazo?

TABLA DE PUNTOS

TABLA DE PUNTOS	
SI	
NO	
NO APLICA	
TOTAL	



MATRIZ DE RIESGOS

MATRIZ DE RIESGOS					
No.	RIESGO	DESCRIPCIÓN	PROBABILIDAD (bajo- Medio- Alto)	IMPACTO (Bajo- Alto- Crítico)	CONTROL EXISTENTE
1	Vulnerabilidades de seguridad	Falta de mecanismos de seguridad adecuados para proteger el sistema y los datos			
2	Errores de código	Errores en el código del software que pueden causar fallos o comportamientos inesperados			
3	Problemas de escalabilidad	El sistema no puede manejar crecientes demandas de usuarios y datos			
4	Falta de documentación	Falta de documentación adecuada sobre el sistema, su funcionamiento y mantenimiento			
5	Problemas de compatibilidad	El sistema no es compatible con otros sistemas o plataformas			
6	Riesgos de privacidad	El sistema no protege adecuadamente la privacidad de los usuarios y sus datos			
7	Falta de pruebas y validación	Falta de pruebas y validación adecuadas para garantizar la calidad y funcionalidad del software			
8	Problemas de recuperación ante desastres	El sistema no tiene planes de contingencia y recuperación ante desastres adecuados			



CRONOGRAMA DE ACTIVIDADES			
	FECHA	ACTIVIDAD	AUDITOR
	04/05/2025	Cuestionario	Miguel
	05/05/2025	Logo de la empresa	Daniel
	05/05/2025	Cuestionario	Daniel- Ana
	06/05/2025	Matriz de Riesgos	Daniel-Miguel
	07/05/2025	Matriz de Riesgos	Diana-Ana
	08/05/2025	Carta Formal	Diana
	09/05/2025	Carta Formal	Ana