FECHA:	09/04/2025
ACTIVIDAD:	Garantizar las soluciones antivirus para sus servidores físicos, virtuales y computadores
PROCESO VINCULADO:	MIPG Evidencias conjunto de datos abiertos.
RESPONSABLE:	Equipo de sistemas
OBJETIVO	garantizar la implementación, configuración y mantenimiento efectivo de soluciones antivirus en los servidores físicos, virtuales y computadores del hospital mental
Dimensión:	Gestión con Valores para Resultados
Política:	Seguridad Digital

CONTENIDO DEL INFORME

Detalla las estrategias y consideraciones fundamentales para garantizar la implementación, configuración y mantenimiento efectivo de soluciones antivirus en los servidores físicos, virtuales y computadores del hospital mental, con el objetivo primordial de proteger la información sensible de los pacientes y asegurar la continuidad operativa de los sistemas críticos para la prestación de servicios médicos.

1. Introducción

La protección de los sistemas informáticos en un hospital mental es una tarea de vital importancia. No solo se trata de salvaguardar equipos, sino de asegurar la confidencialidad de la información sensible de los pacientes, la integridad de los datos clínicos y la disponibilidad ininterrumpida de los servicios esenciales para la atención de la salud mental. En este contexto, la implementación y el mantenimiento adecuado de soluciones antivirus en todos los servidores físicos, entornos virtuales y computadores de la institución se convierte en una línea de defensa fundamental contra las crecientes y sofisticadas amenazas cibernéticas. Este informe profundiza en las estrategias clave, las consideraciones específicas y las mejores prácticas necesarias para garantizar que las soluciones antivirus operen de manera efectiva, proporcionando una capa de seguridad sólida que contribuya a la protección integral de la infraestructura tecnológica y, en última instancia, al bienestar de quienes confían en los servicios del hospital mental.

1. **Objetivos específicos:**

- Implementar una solución antivirus empresarial centralizada Seleccionar y desplegar una plataforma antivirus robusta que permita la gestión, configuración y monitorización de la protección en todos los servidores físicos, virtuales y computadores desde una consola centralizada.

- Configurar la protección en tiempo real en todos los endpoints Asegurar que la funcionalidad de escaneo y bloqueo de amenazas en tiempo real esté activa y correctamente configurada en cada servidor y computador conectado a la red del hospital.

- Establecer políticas de análisis programados regulares: Definir y programar análisis completos y rápidos de forma periódica en todos los sistemas, optimizando los horarios para minimizar el impacto en el rendimiento durante las horas de mayor actividad.

- Gestionar las actualizaciones de firmas y software de forma automática: Configurar la solución antivirus para que reciba e instale automáticamente las últimas definiciones de virus y actualizaciones del software, garantizando la protección contra las amenazas más recientes.

- Definir y gestionar las exclusiones de forma controlada: Identificar y configurar las exclusiones necesarias (ej. archivos de bases de datos específicas) de manera justificada y documentada, minimizando los riesgos de seguridad al tiempo que se asegura la funcionalidad de los sistemas críticos.

- Establecer un protocolo de gestión de cuarentena: Definir un proceso claro para la gestión de archivos y amenazas detectadas y puestas en cuarentena, incluyendo su análisis, posible restauración y eliminación segura.

1. **Metodología**

se articula en cinco fases interconectadas y secuenciales, diseñadas para asegurar la implementación, configuración, operación y mejora continua de las soluciones antivirus en los servidores físicos, virtuales y computadores del hospital mental. Este enfoque iterativo permitirá una adaptación constante a las cambiantes amenazas y a las necesidades específicas del entorno hospitalario.

1.1 Evaluación y planificación

- Comprender el entorno tecnológico de la E.S.E, identificar los riesgos específicos y definir los requisitos detallados para el antivirus.
- Evaluar las amenazas cibernéticas relevantes para el hospital mental (HMRS) generar un análisis especifico de riesgos.
- Establecer criterios claros para la selección de la solución de antivirus considerando la cobertura multiplataforma.
- Revisión de las regulaciones de protección de datos de salud, otras normativas relevantes para asegurar el cumplimiento en la implementación de la solución antivirus.
- Desarrollo de un plan detallado que incluya cronograma, responsables, recursos necesarios, estrategias de despliegue y comunicación.

1.2 Implementación y Configuración

- Desplegar la solución antivirus de manera eficiente y configurar sus parámetros para una protección robusta y adaptada al entorno del hospital.
- Despliegue del agente antivirus en todos los endpoints utilizando la consola de administración centralizada, asegurando una instalación uniforme y eficiente.
- Definición y aplicación de políticas de seguridad antivirus específicas para diferentes grupos de usuarios o tipos de sistemas, considerando sus roles y riesgos asociados.

- Configuración de análisis completos y rápidos con horarios optimizados para minimizar el impacto en el rendimiento durante las horas de atención.

1.3 Operación y mantenimiento

- Asegurar el funcionamiento continuo y efectivo de la solución antivirus, manteniéndola actualizada y respondiendo proactivamente a posibles incidentes.
- Supervisión constante del estado de protección de todos los endpoints a través de la consola de administración.
- Verificación y aseguramiento de la correcta recepción e instalación automática de las actualizaciones de firmas y software.
- Análisis periódico de los registros de eventos del antivirus para identificar patrones sospechosos o posibles incidentes.
- Implementación de un protocolo claro para la recepción, análisis y respuesta a las alertas generadas por el sistema antivirus.

1.4 Pruebas de Efectividad

- Verificar la capacidad de la solución antivirus para detectar y responder a las amenazas de manera efectiva.
- Realización de pruebas controladas utilizando malware seguro o herramientas de simulación de ataques para evaluar la capacidad de detección y bloqueo de la solución antivirus.
- Evaluación de la precisión de la solución antivirus, identificando y ajustando las configuraciones para minimizar los falsos positivos (alertas incorrectas) y garantizar la detección de amenazas reales (falsos negativos).
- Evaluación periódica de la infraestructura para identificar posibles vulnerabilidades que podrían ser explotadas a pesar de la protección antivirus.

1.5 Optimización

- Adaptar la estrategia antivirus a las nuevas amenazas, a los cambios en la infraestructura del hospital y a las lecciones aprendidas.
- Evaluación anual de la estrategia antivirus, considerando las nuevas amenazas, las mejores prácticas de la industria y las necesidades cambiantes del hospital.
- Realización de programas de formación y concienciación periódicos para el personal sobre las nuevas amenazas, las mejores prácticas de seguridad y el uso correcto del antivirus.
- Investigación y evaluación de nuevas funcionalidades o soluciones antivirus que puedan mejorar la protección del hospital.

2. Resultados.

Se espera una protección antivirus integral y activa en todos los sistemas del hospital, con actualizaciones automáticas, análisis regulares y alertas tempranas ante amenazas. La gestión eficaz de las amenazas detectadas y la comprobada efectividad de la solución, junto con un personal informado y una estrategia adaptable, conducirán a una reducción significativa de los incidentes de seguridad

- **Protección Integral Activa:** El 100% de los servidores físicos, virtuales y computadores del hospital cuentan con protección antivirus en tiempo real y activa.
- **Actualizaciones Automáticas:** Las firmas de virus y el software antivirus se actualizan automáticamente en todos los sistemas, garantizando la protección contra las últimas amenazas.
- **Análisis Periódicos Completos:** Se realizan análisis programados regulares en todos los sistemas sin impactar significativamente el rendimiento operativo.
- **Efectividad Comprobada:** Las pruebas periódicas demuestran la capacidad de la solución antivirus para detectar y bloquear amenazas conocidas.
- **Personal Informado:** El personal del hospital comprende la importancia del antivirus y las prácticas seguras de uso.

3. Conclusión

garantizar soluciones efectivas en el hospital mental es crucial para proteger la información sensible de los pacientes y la continuidad de los servicios. Esto requiere una estrategia integral que abarque la implementación centralizada, la configuración óptima, el mantenimiento continuo, las pruebas periódicas y la concienciación del personal. Un enfoque proactivo y adaptable, con una gestión centralizada y la automatización de tareas clave, es fundamental para mitigar las amenazas cibernéticas y asegurar un entorno digital seguro que respalde la calidad de la atención y la confianza de los pacientes.