

1. OBJETIVO

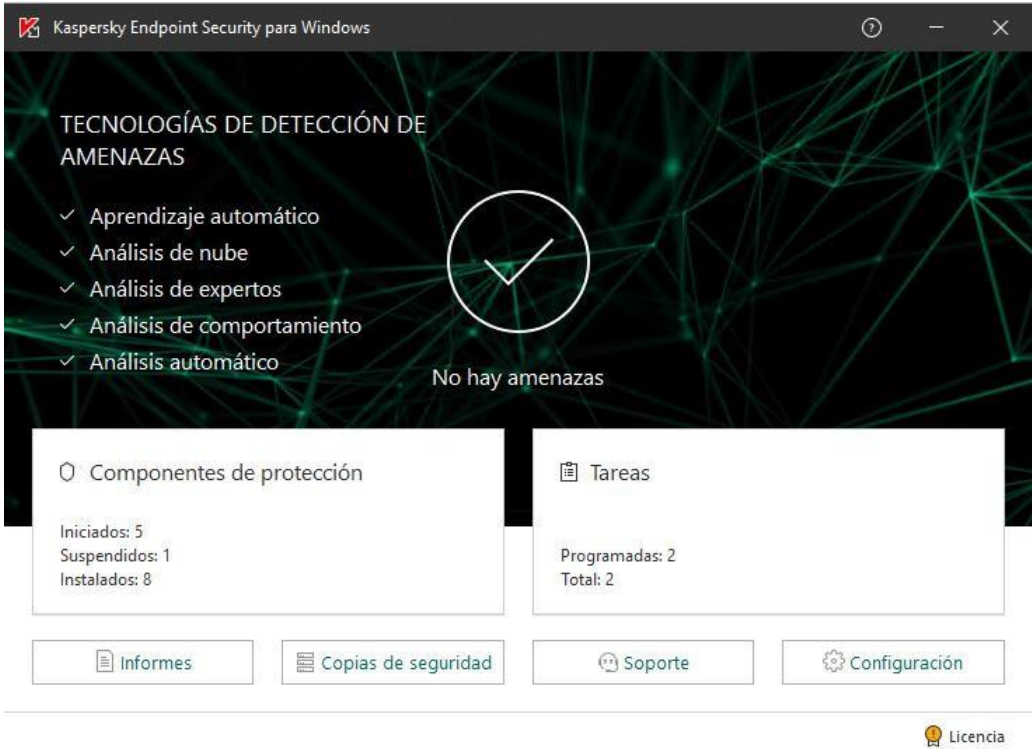
Establecer las actividades para prevenir la presencia de software o código malicioso, sobre los servicios brindados por la infraestructura tecnológica en el proceso gestión tecnológica necesaria, mitigando y/o eliminando cuando sean detectados, aprovechando al máximo los componentes que sobre la plataforma de antivirus existen.

2. ALCANCE

Inicia desde las actividades establecidas por medio del antivirus para tratar la presencia de software o código malicioso, hasta la mitigación de los diferentes riesgos. Este procedimiento aplica para las diferentes plataformas de cómputo, y debe ser aplicado por el área de tecnología, adicionalmente contempla las fuentes informativas de los proveedores para su instalación y mantenimiento.

3. DEFINICIONES

-Se tiene instalado en el servidor donde se manejan las maquinas virtuales el siguiente antivirus llamado Kaspersky antivirus suite.



-Se cuenta con un firewall perimetral llamado Fortinet 100 E



FortiGate 100E ofrece capacidades de firewall de próxima generación para empresas medianas y grandes, con la flexibilidad de implementarse en el campus o sucursal empresarial. Protegerse contra las amenazas cibernéticas Procesador de seguridad de alto rendimiento, eficacia de seguridad y visibilidad profunda.

Seguridad

- Identifica miles de aplicaciones dentro del tráfico de red para inspección profunda y aplicación de políticas granulares
 - Protege contra malware, exploits y sitios web maliciosos en tráfico encriptado y no encriptado
 - Prevenir y detectar ataques conocidos y desconocidos utilizando inteligencia de amenazas continua de los laboratorios FortiGuard con IA servicios de seguridad

Rendimiento

- Ofrece el mejor rendimiento de protección contra amenazas de la industria y latencia ultrabaja utilizando un procesador de seguridad incorporado (SPU) tecnología
- Proporciona rendimiento y protección líderes en la industria para SSL tráfico encriptado

Certificación

- Mejor eficacia de seguridad probada y validada independientemente y rendimiento
- Recibió certificaciones de terceros incomparables de NSS Labs, ICSA, Virus Bulletin y AV Comparatives

Redes

- Las mejores capacidades SD-WAN de Breed para habilitar la aplicación Dirección usando el control de ruta WAN para una alta calidad de experiencia
- Ofrece capacidades de red avanzadas, de alto rendimiento, y capacidades escalables de IPsec VPN para consolidar redes y seguridad

Administración

- Incluye una consola de administración que es efectiva, fácil de usar, y proporciona automatización y visibilidad integrales de la red.
- Proporciona integración Zero Touch con Single de Security Fabric

Panel de gestión de vidrio

- La lista de verificación de cumplimiento predefinida analiza la implementación y destaca las mejores prácticas para mejorar la postura de seguridad general

Security Fabric

- Permite que los productos de Fortinet y los socios de Fabric-ready proporcionen visibilidad más amplia, detección integrada de extremo a extremo, amenaza intercambio de inteligencia y remediación automatizada
- Crea automáticamente visualizaciones de topología de red que descubra dispositivos IoT y proporcione visibilidad completa de Fortinet y productos asociados Fabric-ready

FIN.

	MECANISMOS DE PROTECCIÓN CONTRA VIRUS INFORMÁTICOS.	Clasificación: 2
		Versión: 3.0
		Fecha de Actualización: 29-Feb-2024

CONTROL DE CAMBIOS		
VERSIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA ACTUALIZACIÓN
1.0	Emisión inicial	19-Abr-2023
2.0	Se agregan responsables documentales	31-Jul-2023
3.0	Se agregan responsables documentales	29-JFeb-2024

Elaborado por: Director administrativo y director de T. I	Revisado por: Director administrativo y auditor interno	Aprobado por: Presidente
Fecha: 29/02/2024	Fecha: 29/02/2024	Fecha: 29/02/2024