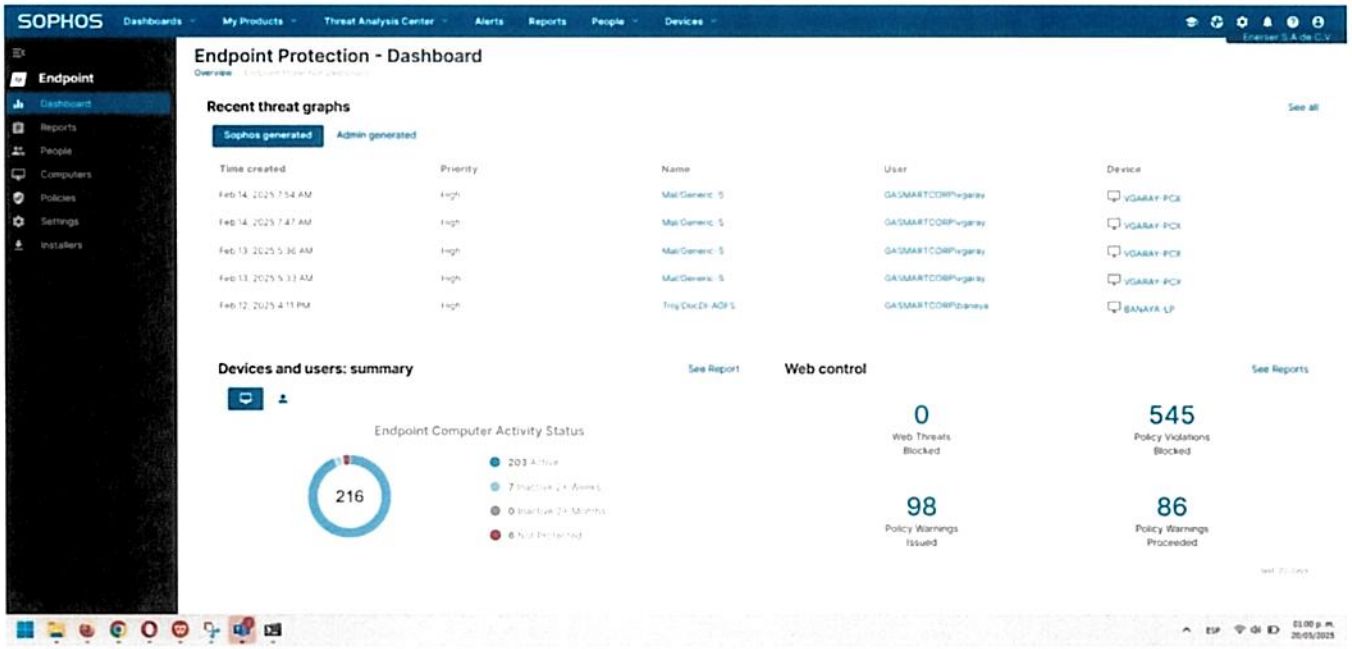
44. Protección reactiva contra codigo malicioso.
Para proteger de manera reactiva los ataques de código malicioso, se han implementado dos estrategias:

1.**Antivirus.**En esta vertiente se utiliza un antivirus basado en inteligencia artificial enfocado en comportamiento malicioso capaz especializado en ransomware y ataques día cero. En nuestro caso **Sophos Antivirus** el cual se instala en todos los equipos. Se ofrece evidencia fotográfica de la consola de administración, de la instalación en el servidor de aplicación del monedero y de un equipo cliente. La imagen muestra captura de pantalla de la consola de administración de Sophos, la cual es un servicio de nube hospedado por el fabricante del antivirus.

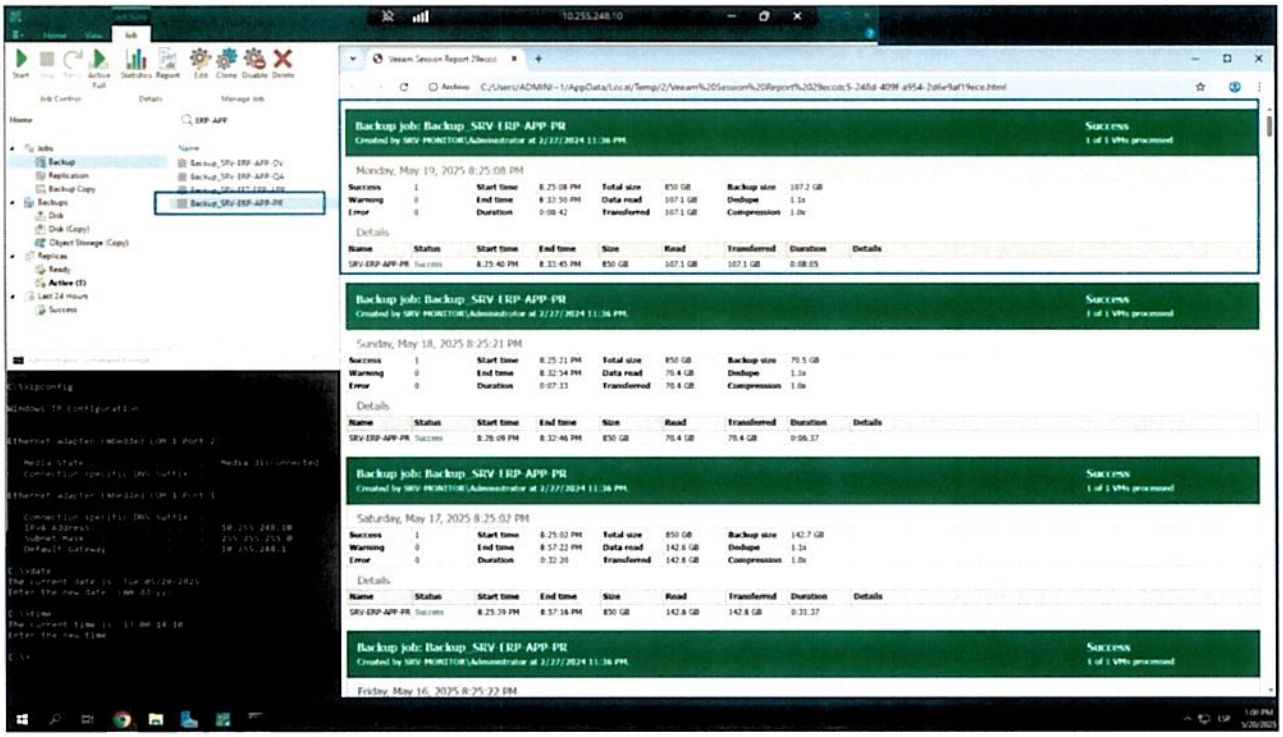


2. **Respaldos.** P ara revertir los efectos del ataque del código malicioso se utilizan los respaldos mediante Veeam.

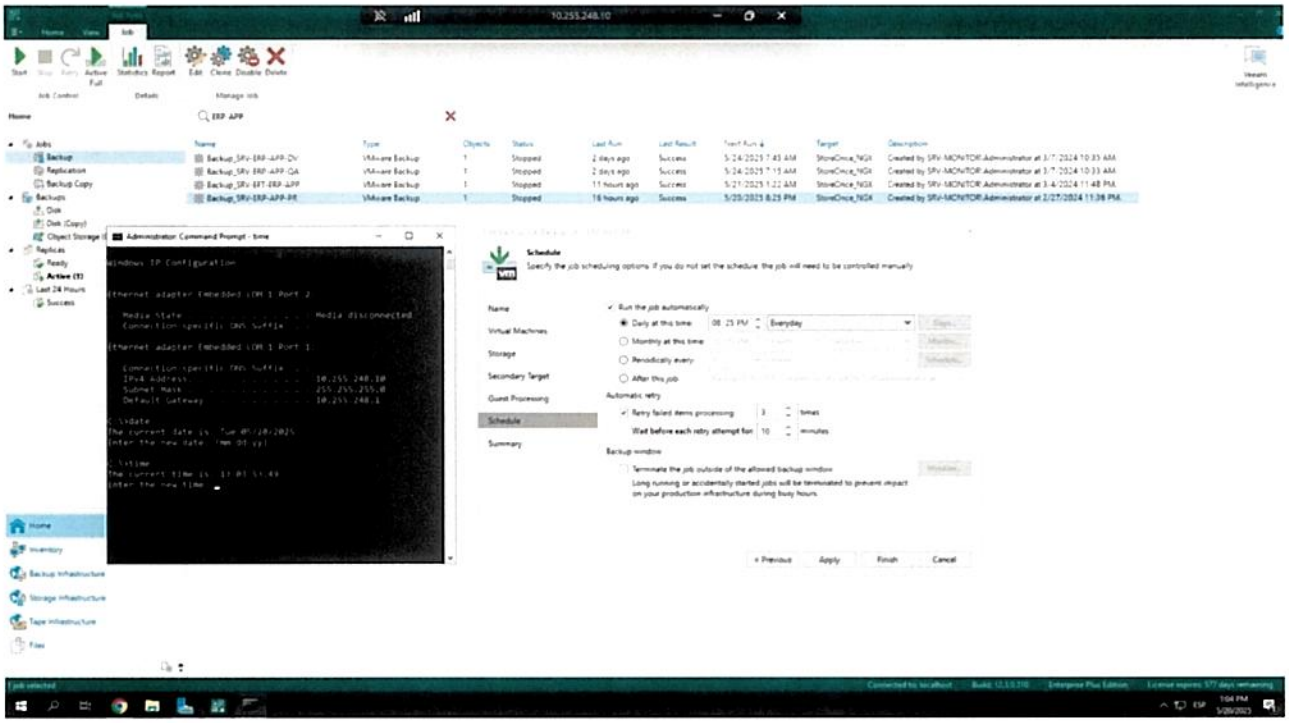
a) **Respaldos de Instantáneas en el sistema de almacenamiento.** Se realizan por el sistema de almacenamiento distribuido VeeamBackup. Estos se realizan cada 6 horas con una retención de 2 días, uno diario con retención de 2 semanas y uno semanal los días sábados con retención de 2 meses. Todos los anteriores almacenados en los discos internos de los servidores, con enfoque a una restauración muy rápida (1TB por minuto), en caso de falla.

La imagen muestra captura de pantalla donde se aprecian los respaldos mediante Veeam Backup, en este ejemplo del servidor de aplicaciones del monedero electrónico SRV-ERP-APP -PR

(Evidencia en la siguiente pagina)



La imagen muestra captura de pantalla de la consola de Veeam donde se aprecian las definiciones de las políticas de respaldo para las máquinas virtuales.



b) Respaldos des acoplados o fuera del sistema de almacenamiento. Estos se extraen fuera del almacenamiento y se almacenan de manera inmutable en dos destinos, una NAS local y en Wasabi, un servicio de almacenamiento en la nube. Estos últimos para cumplir la buena practica 3,2,1 minimizando el riesgo de un ransomware, la perdida o contaminación del repositorio principal e incluso la perdida de los sitios principal y alterno.

La imagen muestra captura de pantalla del servidor SRV-VEEAM, herramienta con la cual se realizan los respaldos desacoplados a infraestructura de externa de VMWare