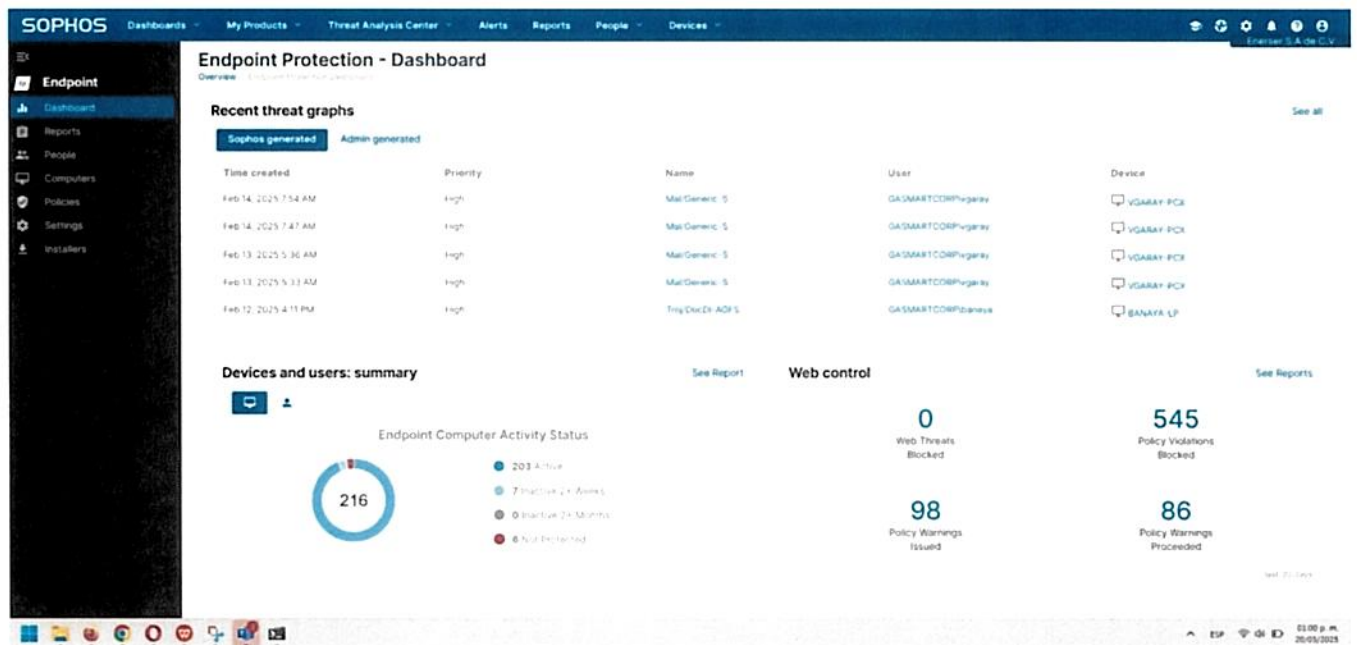


44. Protección reactiva contra código malicioso.

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.** Para 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)

[Handwritten signature]

The screenshot displays the Veeam Backup & Replication console. On the left, the 'Jobs' tree shows a backup job for 'Backup_Srv ERP APP PR'. The main pane shows the job's history with three successful runs. Each run includes a summary table and a detailed table of statistics.

Backup job: Backup_Srv ERP APP PR
Created by SRV-MONITOR\Administrator at 2/27/2024 11:36 PM

Monday, May 19, 2025 8:25:08 PM

Success	1	Start time	8:25:08 PM	Total size	850 GB	Backup size	187.2 GB
Warning	0	End time	8:32:39 PM	Data read	187.1 GB	Dedup	1.1x
Error	0	Duration	0:08:42	Transferred	187.1 GB	Compression	1.0x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRV-ERP-APP-PR	Success	8:25:40 PM	8:32:45 PM	850 GB	187.1 GB	187.1 GB	0:08:05	

Backup job: Backup_Srv ERP APP PR
Created by SRV-MONITOR\Administrator at 2/27/2024 11:36 PM

Sunday, May 18, 2025 8:25:21 PM

Success	1	Start time	8:25:21 PM	Total size	850 GB	Backup size	70.5 GB
Warning	0	End time	8:32:54 PM	Data read	70.4 GB	Dedup	1.1x
Error	0	Duration	0:07:33	Transferred	70.4 GB	Compression	1.0x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRV-ERP-APP-PR	Success	8:26:09 PM	8:32:46 PM	850 GB	70.4 GB	70.4 GB	0:06:37	

Backup job: Backup_Srv ERP APP PR
Created by SRV-MONITOR\Administrator at 2/27/2024 11:36 PM

Saturday, May 17, 2025 8:25:02 PM

Success	1	Start time	8:25:02 PM	Total size	850 GB	Backup size	142.7 GB
Warning	0	End time	8:57:22 PM	Data read	142.6 GB	Dedup	1.1x
Error	0	Duration	0:32:20	Transferred	142.6 GB	Compression	1.0x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
SRV-ERP-APP-PR	Success	8:25:39 PM	8:57:16 PM	850 GB	142.6 GB	142.6 GB	0:31:37	

Backup job: Backup_Srv ERP APP PR
Created by SRV-MONITOR\Administrator at 2/27/2024 11:36 PM

Friday, May 16, 2025 8:25:22 PM

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.

The screenshot shows the 'Schedule' tab for a backup job. It displays a table of backup jobs and their status. The 'Schedule' section on the right allows configuring the job's execution frequency and automatic retry options.

Name	Type	Objects	Status	Last Run	Last Result	Last Run 4	Target	Description
Backup_Srv ERP APP PR	VMware Backup	1	Stopped	2 days ago	Success	5/14/2025 7:43 AM	StoreOnce_NG4	Created by SRV-MONITOR\Administrator at 3/7/2024 10:33 AM
Backup_Srv ERP APP QA	VMware Backup	1	Stopped	2 days ago	Success	5/14/2025 7:15 AM	StoreOnce_NG4	Created by SRV-MONITOR\Administrator at 3/7/2024 10:33 AM
Backup_Srv ERP APP PR	VMware Backup	1	Stopped	11 hours ago	Success	5/21/2025 1:22 AM	StoreOnce_NG4	Created by SRV-MONITOR\Administrator at 3/4/2024 11:48 PM
Backup_Srv ERP APP PR	VMware Backup	1	Stopped	16 hours ago	Success	5/25/2025 8:25 PM	StoreOnce_NG4	Created by SRV-MONITOR\Administrator at 2/27/2024 11:36 PM

Schedule
Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Name ☒ Run the job automatically

Virtual Machines ☒ Daily at this time 08:25 PM ☐ Monday at this time ☐ Periodically every ☐ After this job

Storage ☐ StoreOnce_NG4 ☐ StoreOnce_NG4 ☐ StoreOnce_NG4

Secondary Target ☐ StoreOnce_NG4 ☐ StoreOnce_NG4 ☐ StoreOnce_NG4

Guest Processing ☒ Run before items processing ☐ Wait before each retry attempt for 10 minutes

Automatic retry ☒ Retry failed items processing ☐ Wait before each retry attempt for 10 minutes

Summary ☐ Terminate the job outside of the allowed backup window. Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

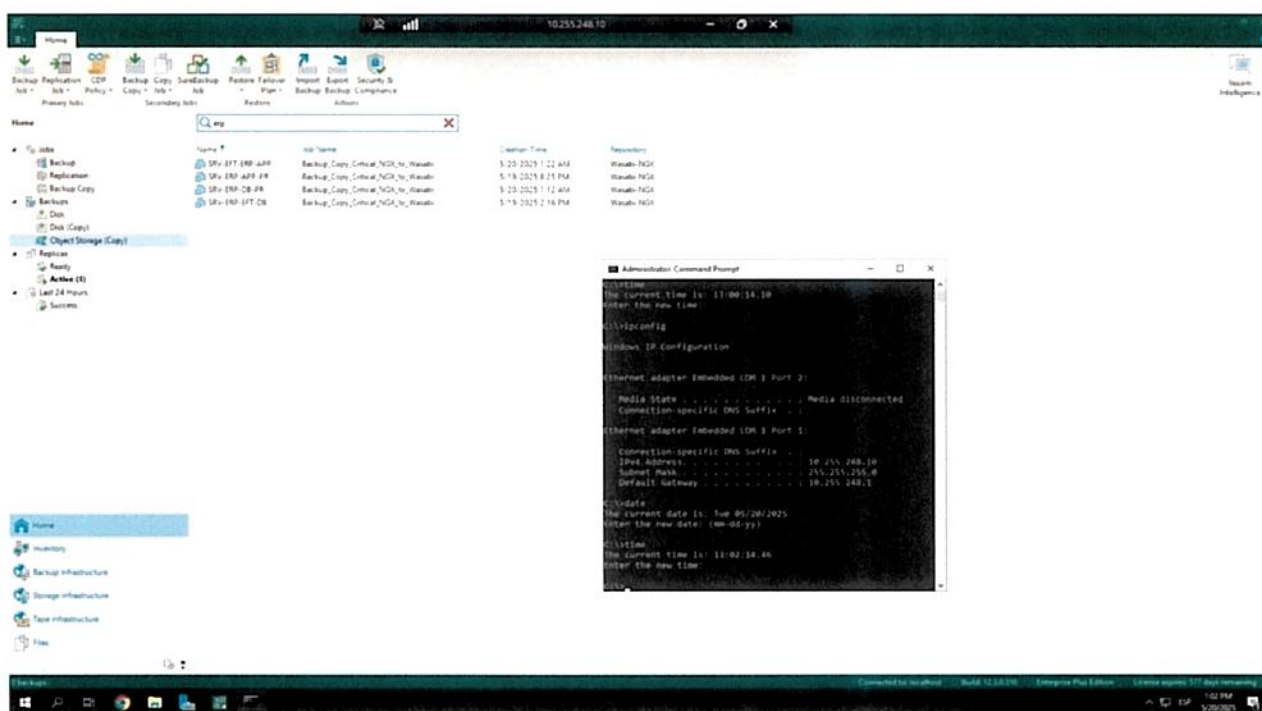
Backup window ☐ Terminate the job outside of the allowed backup window. Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Buttons: Previous Apply Finish Cancel

Handwritten signature

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



[Handwritten signature]