ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

TEMA:

“Implementación de un sistema de ciberseguridad para minimizar ataques y vulnerabilidades del datacenter de FEMSA - Corporación GPF”

Elaborado por:
Hidalgo Olipa, Danny Alejandro

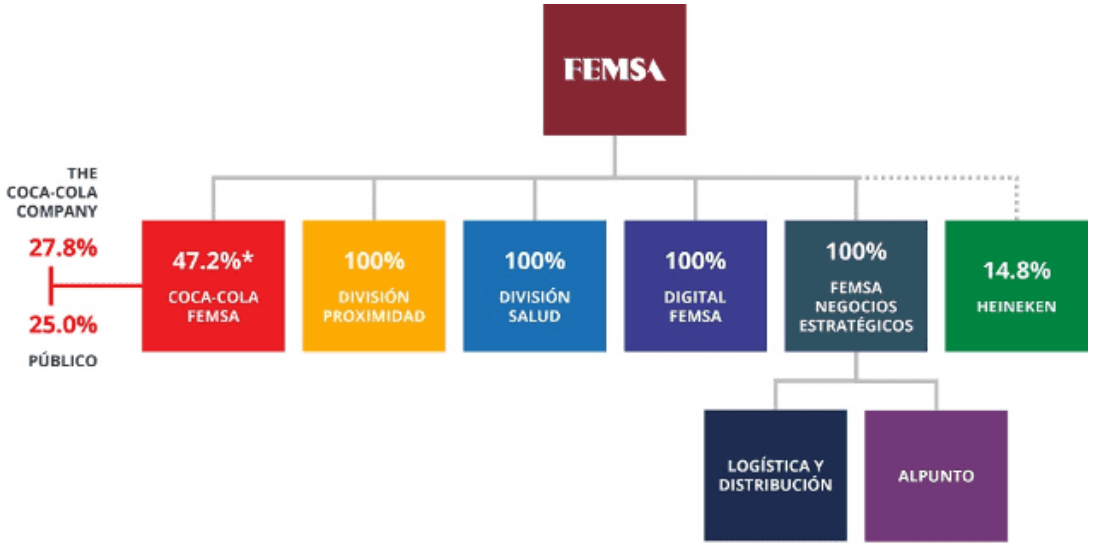
Director del Proyecto:
Ing. Sáenz Enderica, Fabian Gustavo

Sangolquí, 2023

Sumario

Introducción

Antecedentes – FEMSA y Corporación GPF



*REPRESENTA EL 56% DEL DERECHO A VOTO

Fybeca

Sana Sana Farmacias

PROVEFARMA

ABEFARM

okiDoki

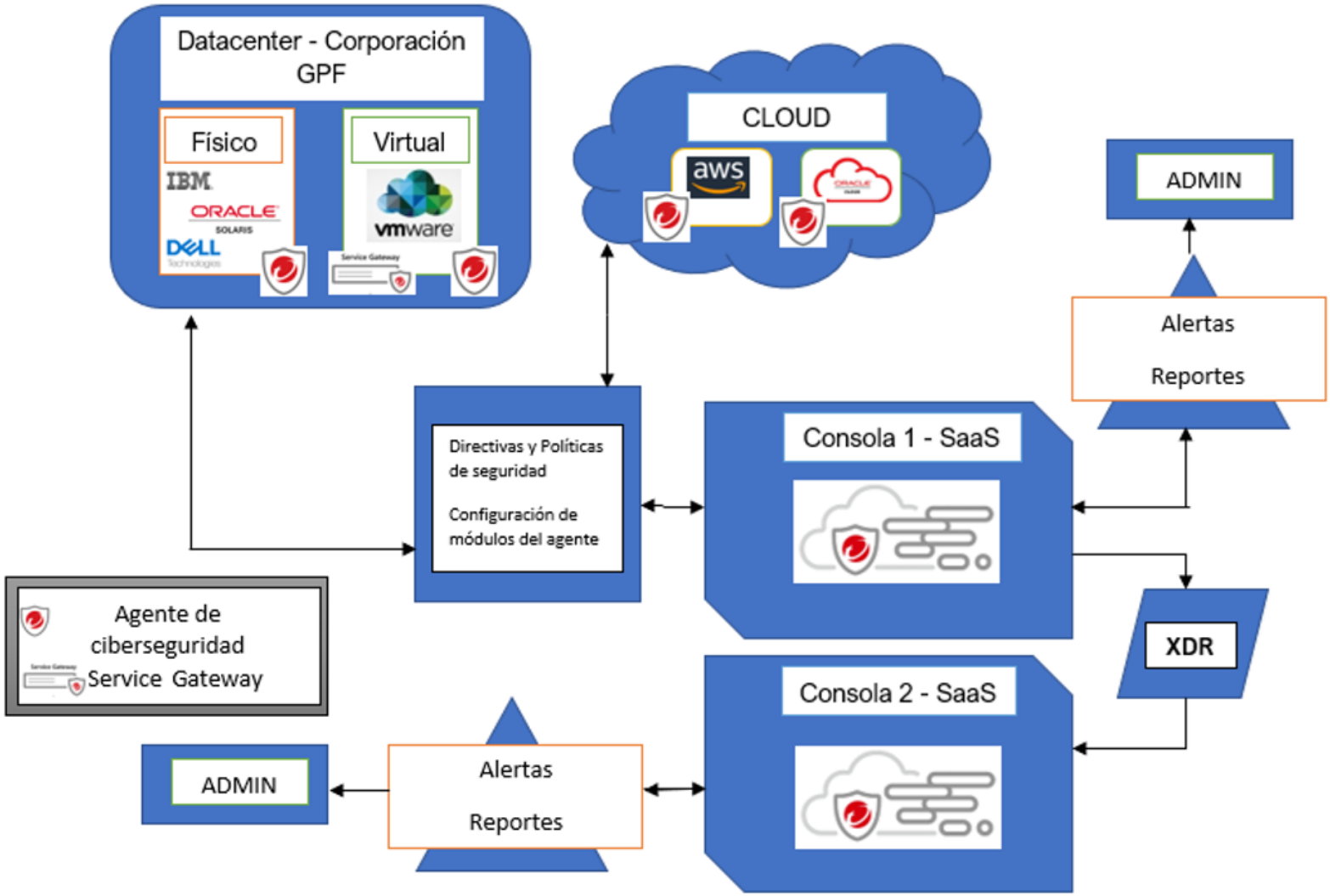
LogiHealth

Justificación

Existe una necesidad urgente enfocada en evitar los riesgos de seguridad causadas por vulnerabilidades que podrían generar la indisponibilidad de los servicios

Corporación GPF se ha planteado reforzar su estrategia de múltiples niveles de seguridad incluyendo equipos, protocolos y herramientas que permitan minimizar el impacto de un posible ataque a la organización

Alcance



Certificaciones ISO 27001, ISO 27014, ISO 27017, SOC2 y PCI DSS.

Objetivos - General

Implementar un sistema de ciberseguridad en los servidores del Data Center de la Corporación GPF definidos en entornos on premise y cloud para la protección frente a amenazas y vulnerabilidades conocidas y desconocidas.

Objetivos – Específicos

Analizar los parámetros de criticidad de los servidores para la efectiva usabilidad de las 101 licencias del agente del sistema de ciberseguridad acorde a la información proporcionada por FEMSA - Corporación GPF.

Analizar e identificar las funcionalidades de los módulos del sistema de ciberseguridad y realizar los ajustes necesarios para permitir el correcto funcionamiento de detección y respuesta extendidas (XDR).

Definir y asignar políticas de seguridad especializadas, generando un conjunto de reglas y ajustes de acuerdo con el sistema operativo y la aplicación del servidor.

Automatizar el sistema de reportes para que envíe la información precisa de los eventos que han ocurrido en cada servidor con frecuencia de 7 días.

Objetivos – Específicos

Implementar el Service Gateway mediante un paquete Open Virtualization Format (OVF) sobre VMware e integración con la consola del sistema de ciberseguridad.

Evaluar la efectividad de la solución frente a vulnerabilidades y el beneficio de la implementación de la herramienta para el negocio.

Realizar un manual de usuario para el área de infraestructura sobre el correcto uso y configuración del sistema de ciberseguridad

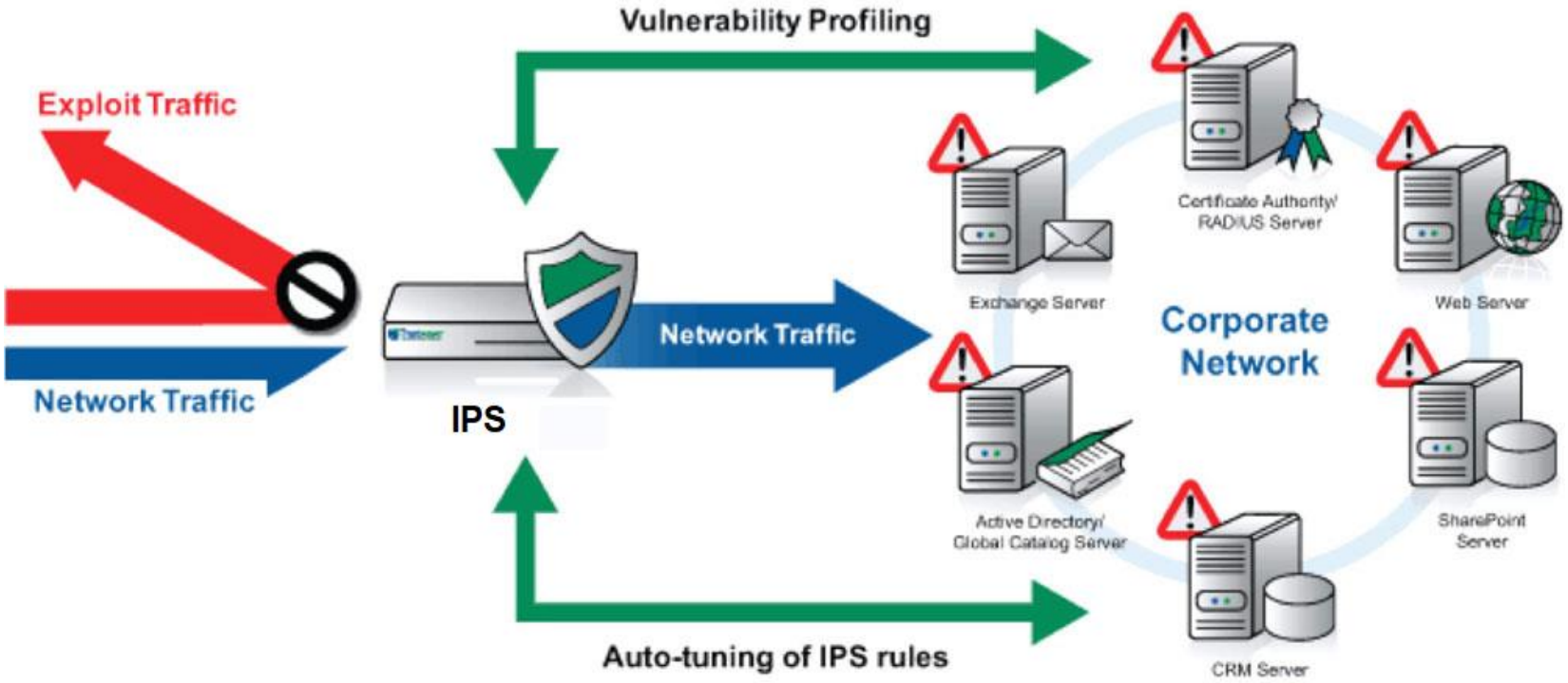
Marco conceptual

Componentes necesarios para la operación y gestión de los servicios y entornos de tecnología empresariales

Proteger la infraestructura computacional y la información contenida en los sistemas y redes de computadoras. Por lo cual se emplean protocolos, herramientas, normas, métodos, reglas, y legislaciones creadas.

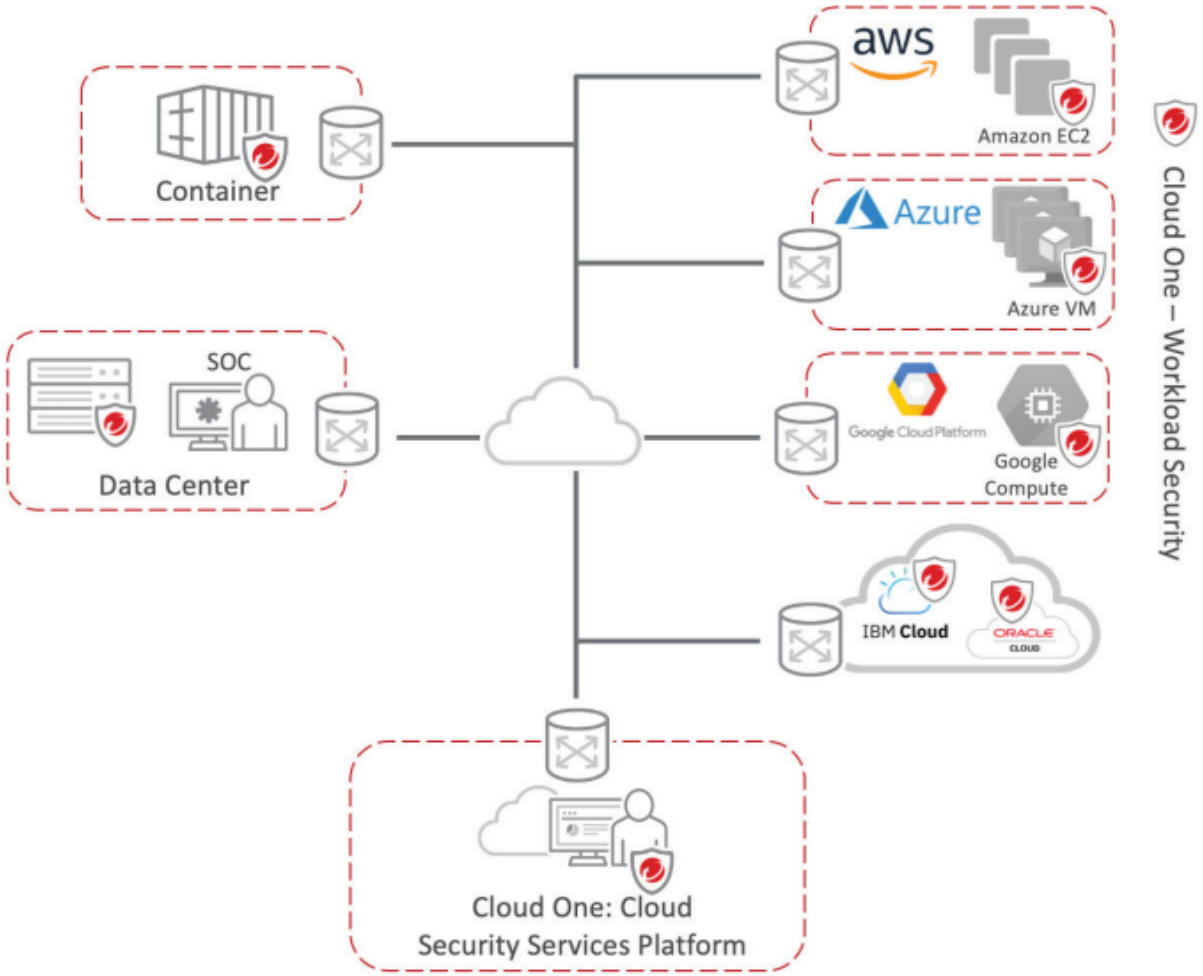
IPS – Sistema de prevención de intrusos

Tecnología que monitorea constantemente una red con el fin de identificar cualquier actividad dañina que busque aprovechar una vulnerabilidad conocida. Ayuda a las organizaciones a identificar el tráfico malicioso y bloquear de manera proactiva el ingreso de dicho tráfico a su red.



Trend Micro - Cloud One Workload Security

Ofrece una amplia gama de funciones de seguridad, como detección y prevención de intrusiones, protección contra malware, firewall de host, control de aplicaciones y seguridad de contenedores.



Posee capacidades de prevención, detección y respuesta impulsadas por inteligencia artificial, investigación e inteligencia de amenazas líderes en el mercado.

Implementación

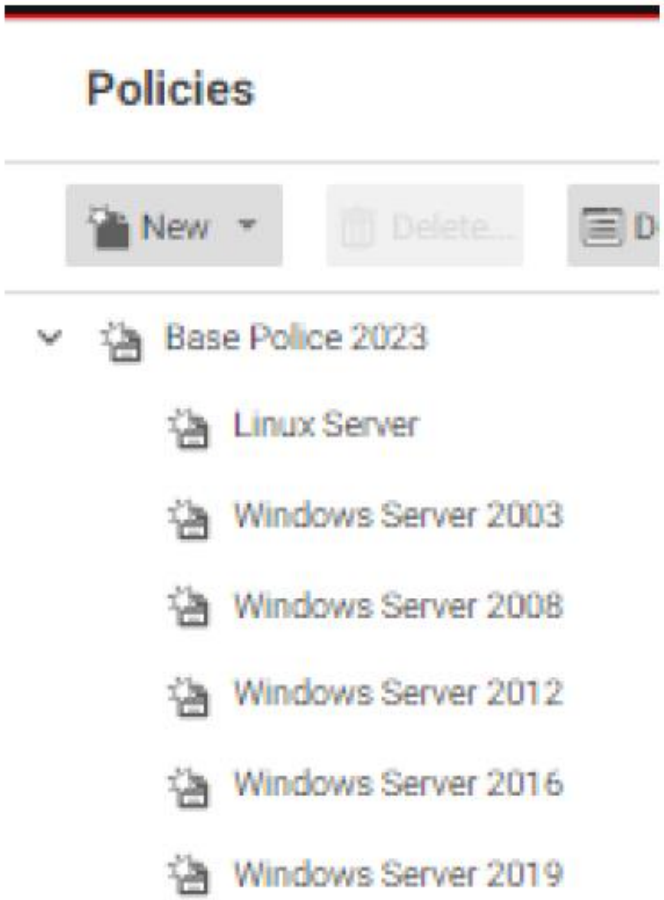
Criticidad de servidores

Sistemas Operativos	Criticidad			Total
	Alta	Baja	Media	
CentOS 6 (64 bit)	10		2	12
CentOS 7 (64 bit)	7	2	4	13
Microsoft Windows Server 2003 (32 bit)		3	1	4
Microsoft Windows Server 2008 R2 (64 bit)	1	1	1	3
Microsoft Windows Server 2012 R2 (64 bit)	3	3	7	13
Microsoft Windows Server 2016 (64 bit)	5	3	13	21
Microsoft Windows Server 2019 (64 bit)	9	7	7	23
Oracle Linux Release 6 (64 bit)			1	1
Oracle Linux Release 7 (64 bit)	3			3
Red Hat Enterprise 5 (32 bit)	2		1	3
Ubuntu Linux 20 (64 bit)		1	3	4
Total	**40**	**20**	**40**	**100**

Módulos de agentes

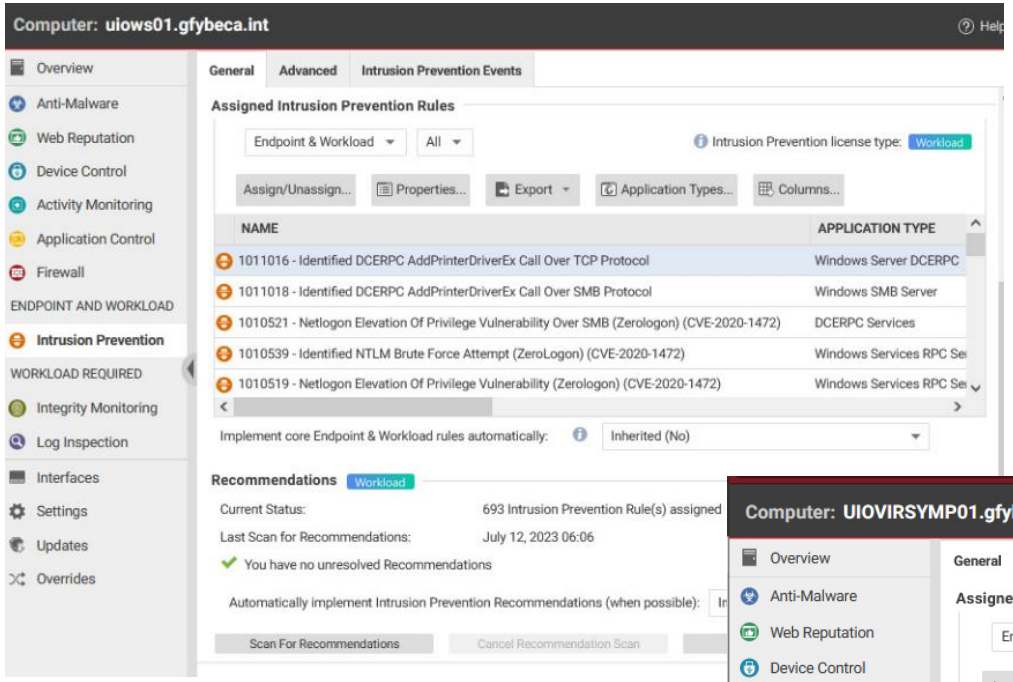
	Agent
	Managed (Online)
Anti-Malware	Off, not installed, no configuration
Web Reputation	On
Activity Monitoring	On
Device Control	Off, not installed
Application Control	Off, not installed
Firewall	Off, installed, no rules
Intrusion Prevention	**On, Prevent, 41 rules**
Integrity Monitoring	**On, Real Time, 18 rules**
Log Inspection	**Off, installed, 11 rules**
Online	Yes
Last Communication	July 19, 2023 12:49

Directivas de seguridad

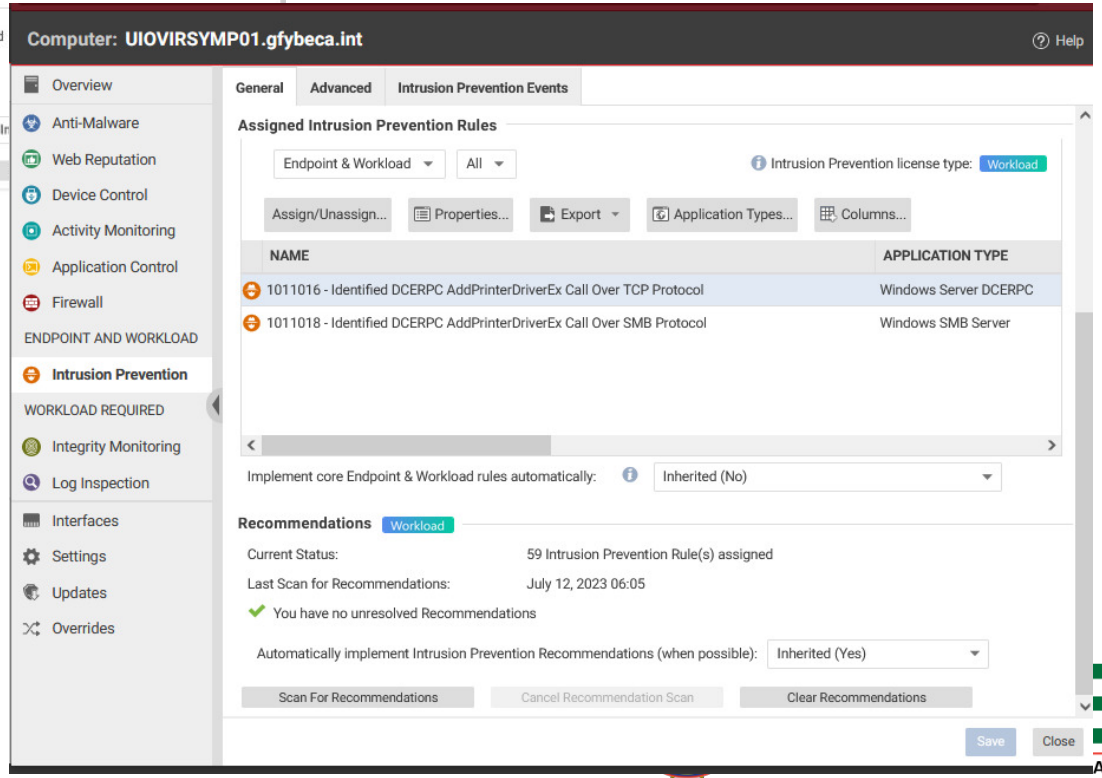


Las directivas se utilizan para almacenar reglas y opciones de configuración que pueden ser aplicadas fácilmente a múltiples equipos.

Reglas IPS

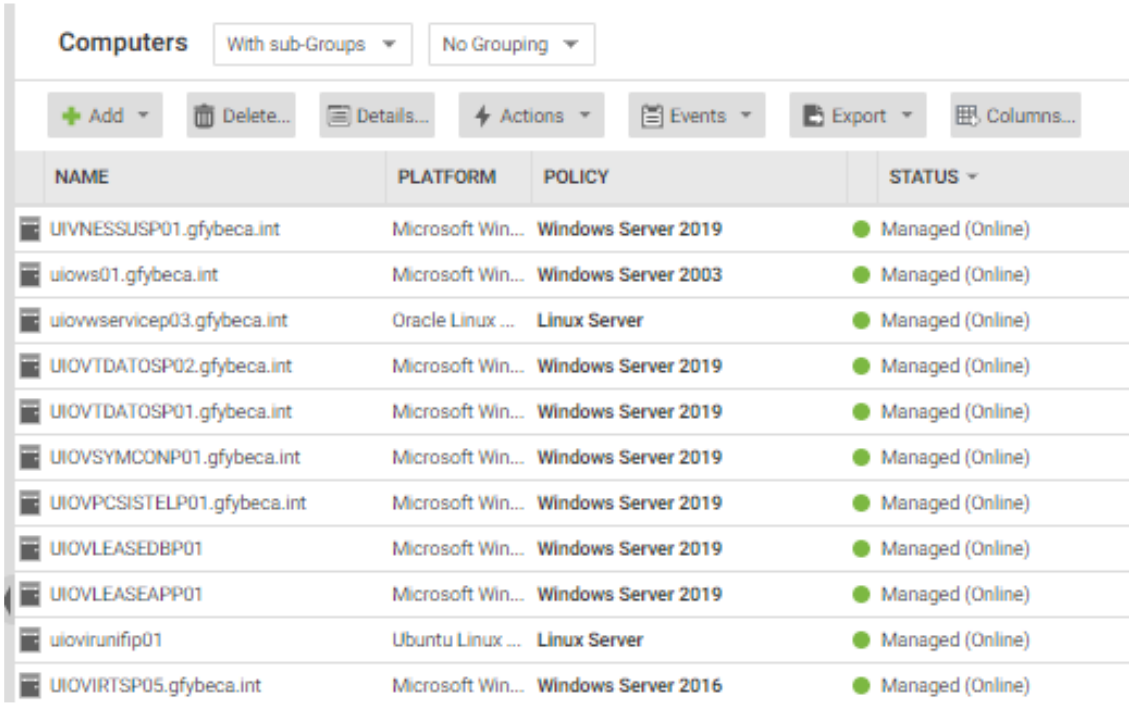


Microsoft Windows Server 2003 (32 bit)



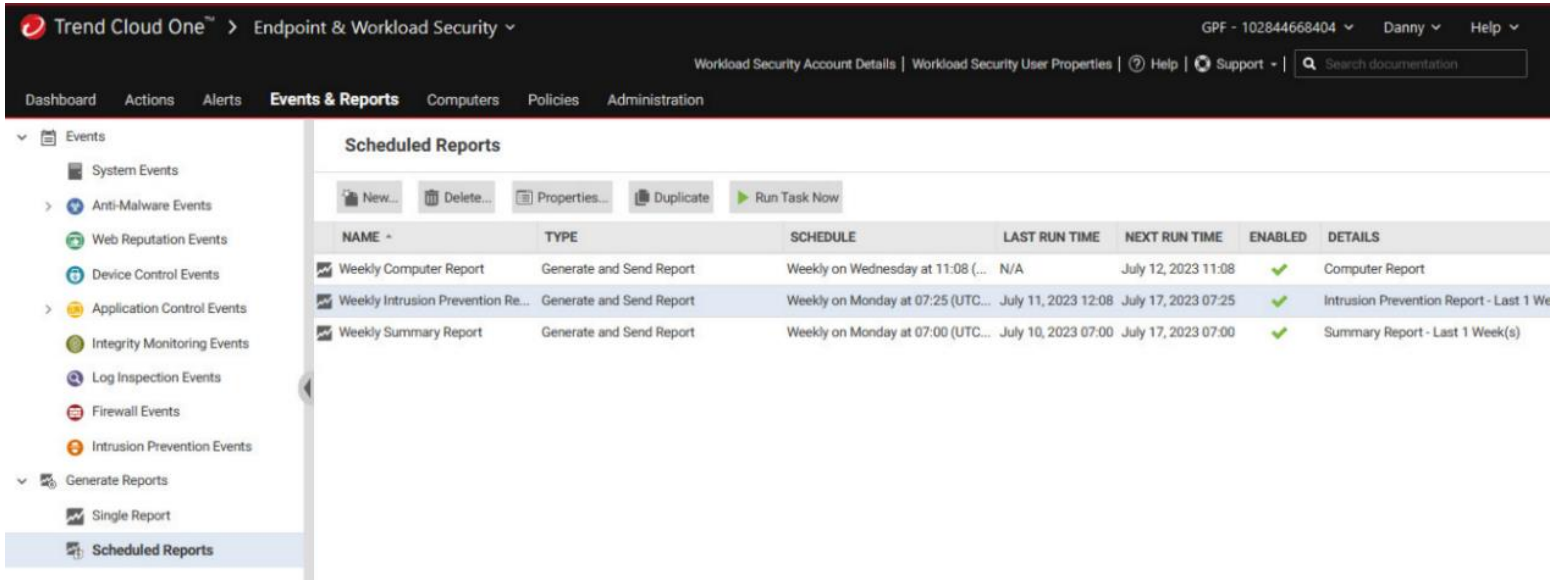
Microsoft Windows Server 2016 (64 bit)

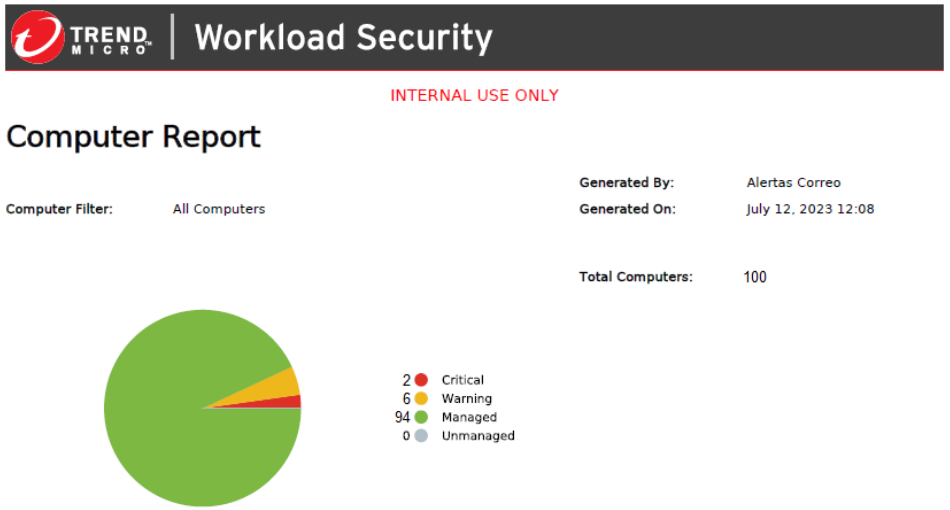
Agentes


Computers
With sub-Groups
No Grouping
Add
Delete...
Details...
Actions
Events
Export
Columns...
NAME
PLATFORM
POLICY
STATUS
UIVNESSUSP01.gfybeca.int
Microsoft Win...
Windows Server 2019
Managed (Online)
uiows01.gfybeca.int
Microsoft Win...
Windows Server 2003
Managed (Online)
uiovwservicep03.gfybeca.int
Oracle Linux ...
Linux Server
Managed (Online)
UIOVTDATOSP02.gfybeca.int
Microsoft Win...
Windows Server 2019
Managed (Online)
UIOVTDATOSP01.gfybeca.int
Microsoft Win...
Windows Server 2019
Managed (Online)
UIOVSYMCONP01.gfybeca.int
Microsoft Win...
Windows Server 2019
Managed (Online)
UIOVPCSISTELP01.gfybeca.int
Microsoft Win...
Windows Server 2019
Managed (Online)
UIOVLEASEDBP01
Microsoft Win...
Windows Server 2019
Managed (Online)
UIOVLEASEAPP01
Microsoft Win...
Windows Server 2019
Managed (Online)
uiovirunifip01
Ubuntu Linux ...
Linux Server
Managed (Online)
UIOVIRTSP05.gfybeca.int
Microsoft Win...
Windows Server 2016
Managed (Online)


Group:
Computers
Policy:
Base Police 2023 ▸ Windows Server 2003
Asset Importance:
None
Download Security Updates From:
Primary Tenant Relay Group

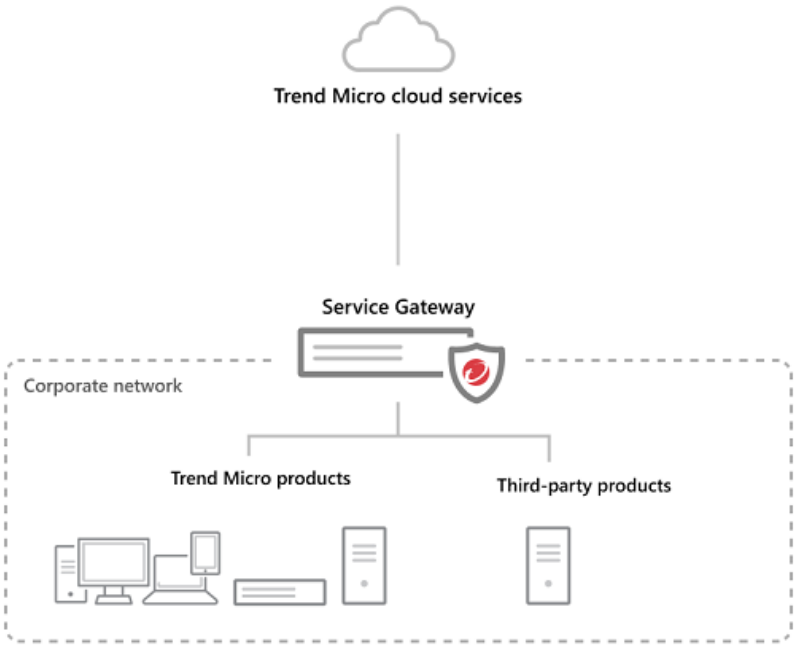
Sistema de reportes

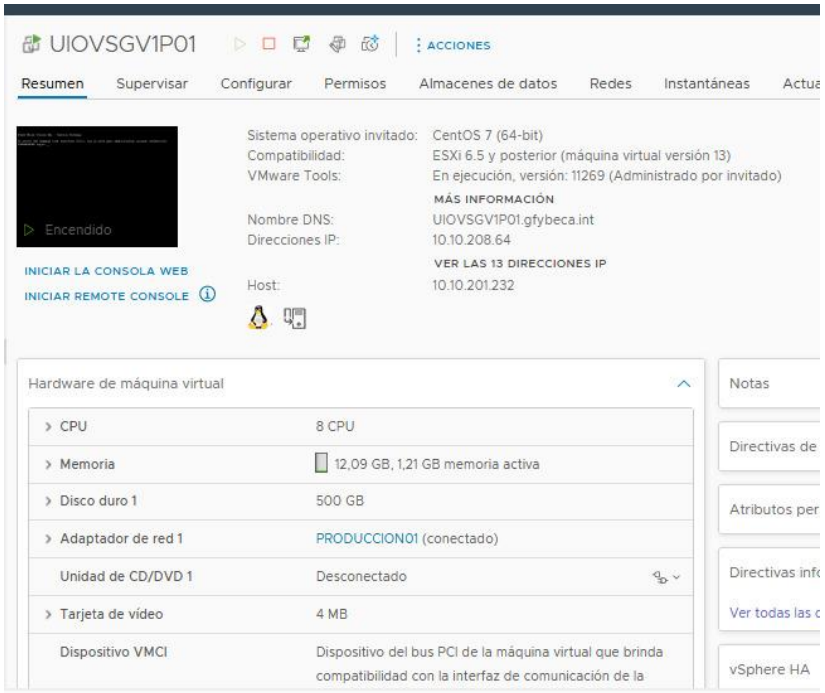




Service Gateway

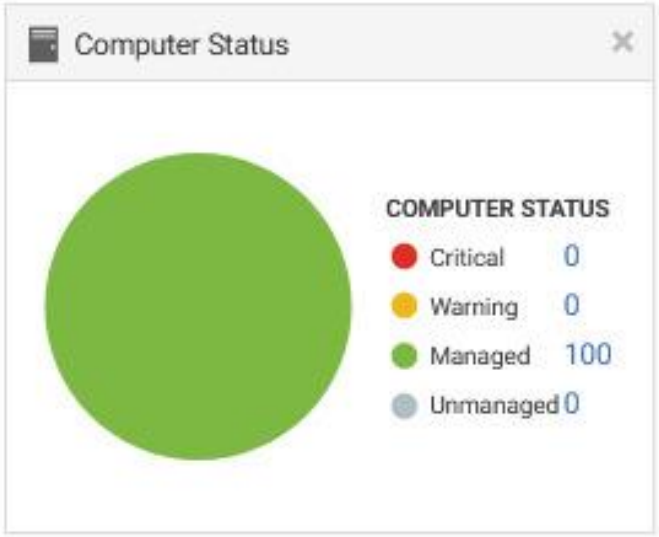
Se implementa en la red local y cumple como intermediario entre Trend Micro Vision One y otros productos instalados en la misma infraestructura.

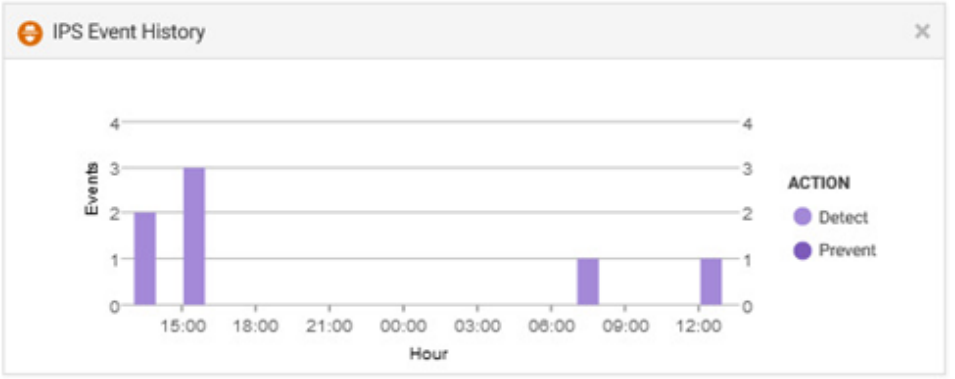


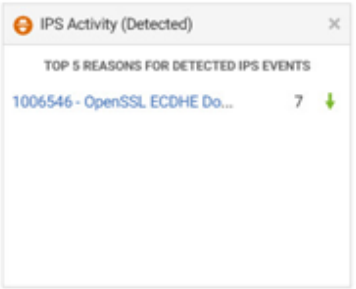


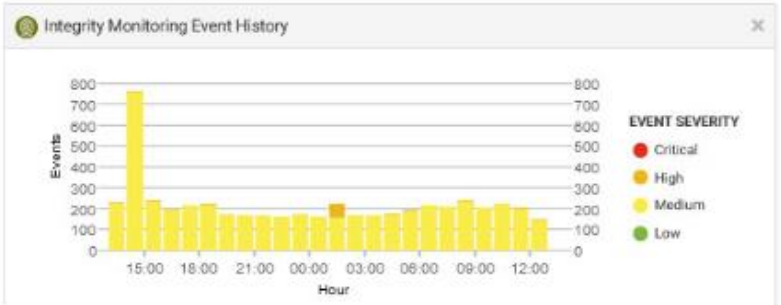
Análisis de efectividad

Dashboard General

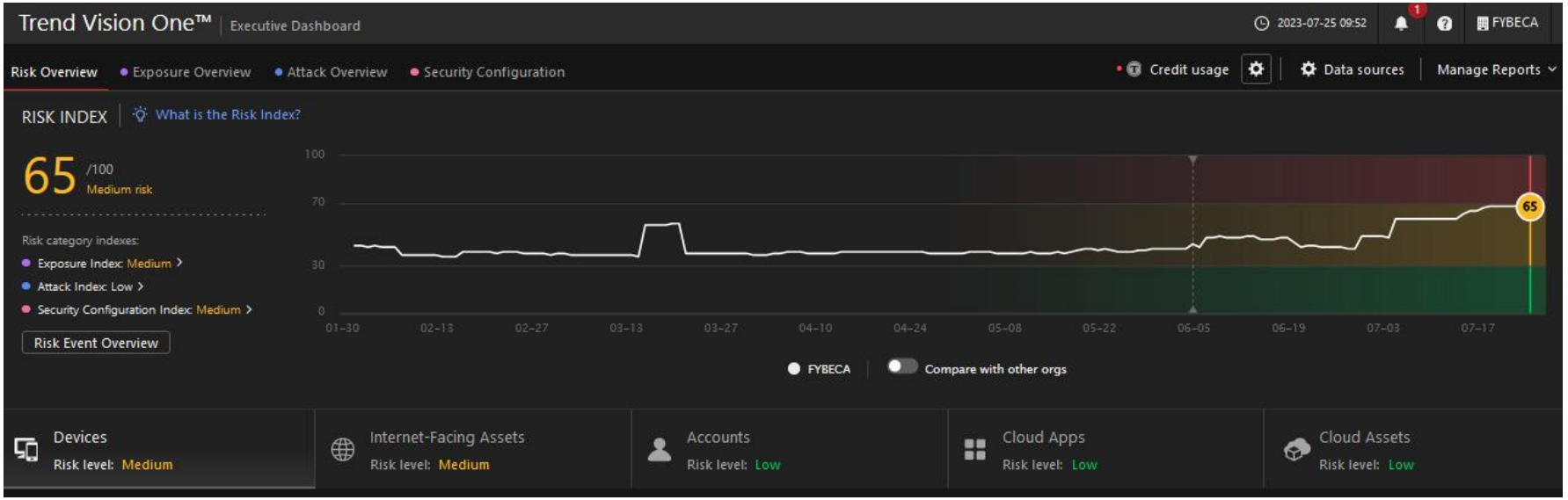


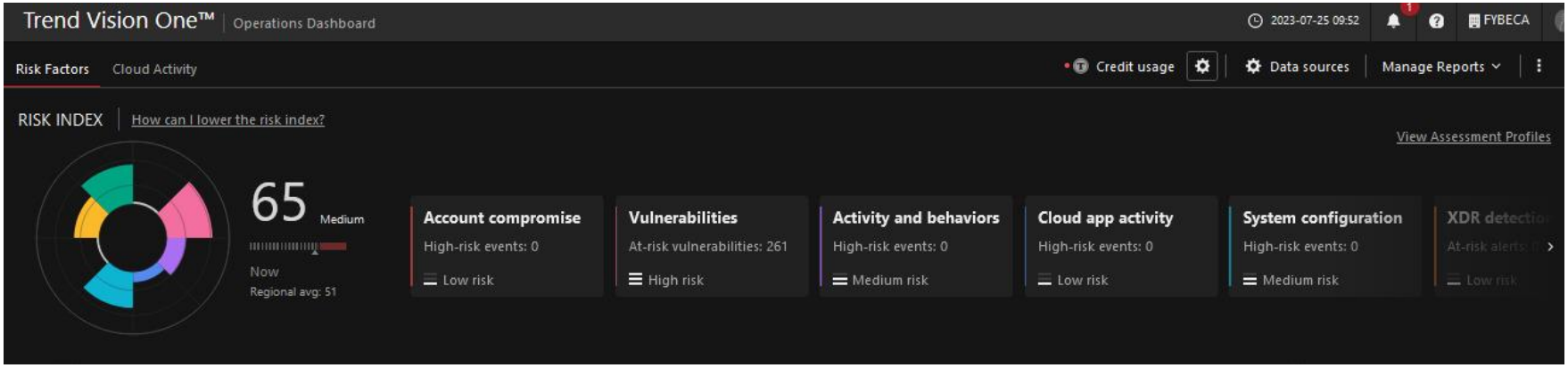




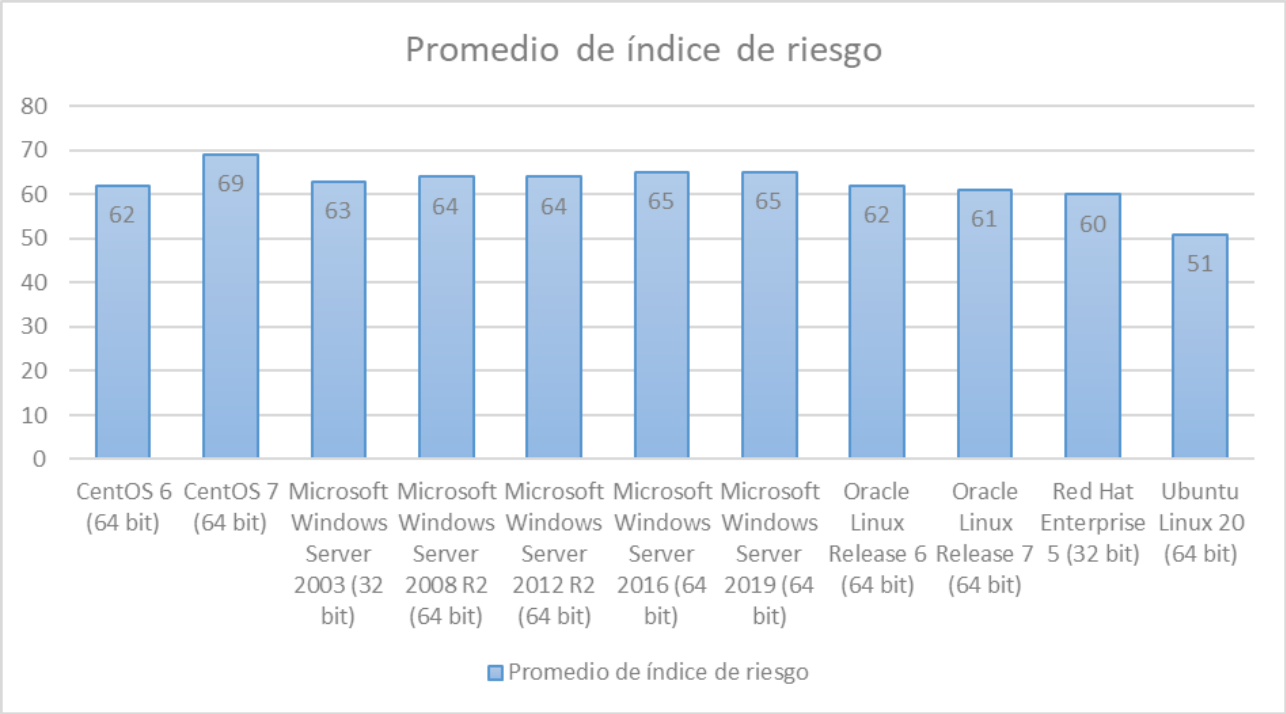


Índice de riesgo





Riesgo de Sistemas Operativos



Sistemas operativos	CVEs altamente explotables
CentOS 7	358
Microsoft Windows Server 2016	344
Microsoft Windows Server 2019	446
Total	1148

Retorno de la inversión

$$ROI = \frac{Beneficios - Costos}{Costos} \times 100\%$$

$$ROI = \frac{1\,760\,000 - 51\,134}{51\,134} \times 100\%$$

$$ROI = 33.42 \times 100\%$$

$$\boldsymbol{ROI = 3342\%}$$

Conclusiones

Conclusiones

La implementación del sistema de ciberseguridad en los servidores del Data Center de la Corporación GPF se realizó con éxito y representa una medida esencial para salvaguardar la infraestructura informática contra amenazas y vulnerabilidades conocidas y desconocidas.

Actualmente el 100% de los agentes de Deep Security instalados se comunican correctamente y reportan la información adecuada para el funcionamiento del sistema.

Para mantener un control periódico sobre el estado de los agentes de los equipos, se generan reportes programados de manera semanal.

Conclusiones

El ROI del 3342% en caso de sufrir una vulneración a su información evidencian una decisión acertada por parte de la Corporación al invertir en medidas de ciberseguridad con los servicios de Cloud One Workload Security y Vision One XDR de Trend Micro.

Los sistemas operativos que están más expuestos son Microsoft Windows Server 2019 y 2016 como la distribución de Linux CentOS 7 los cuales requieren atención por presentar 1148 vulnerabilidades altamente explotables.

¡Gracias!