



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:

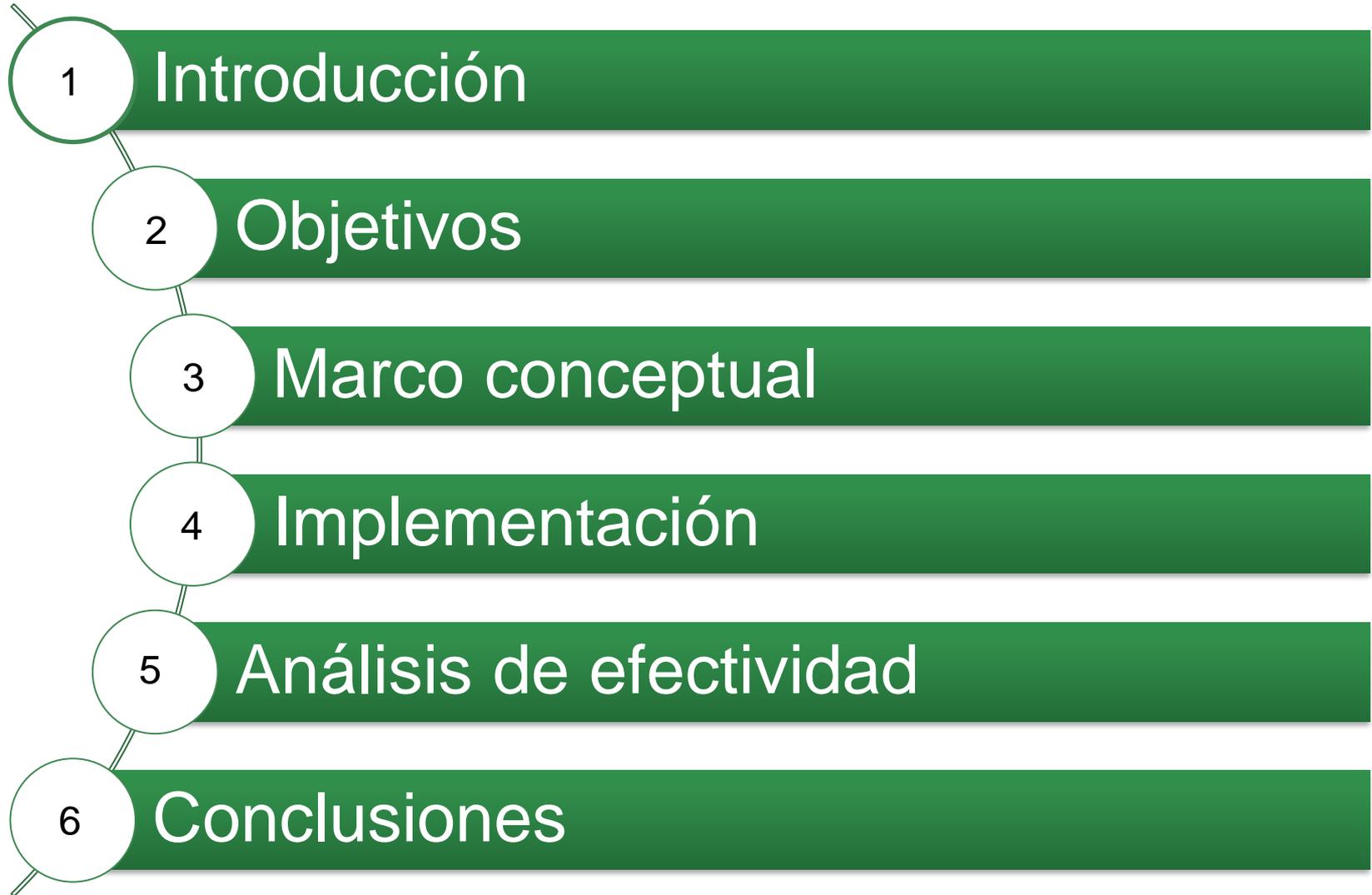
Hidalgo Olipa, Danny Alejandro

Director del Proyecto:

Ing. Sáenz Enderica, Fabian Gustavo

Sangolquí, 2023



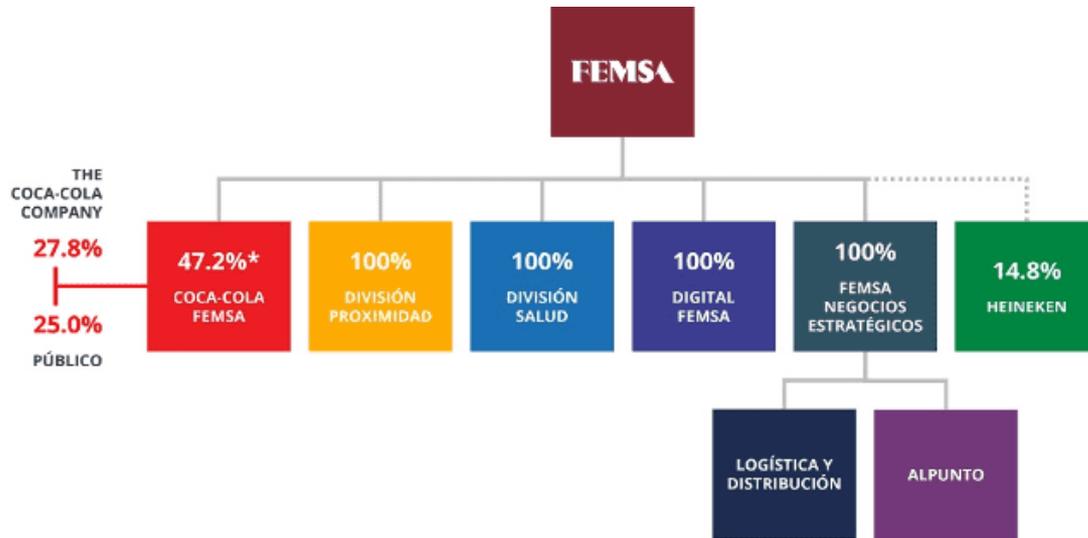


Introducción



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Antecedentes – FEMSA y Corporación GPF



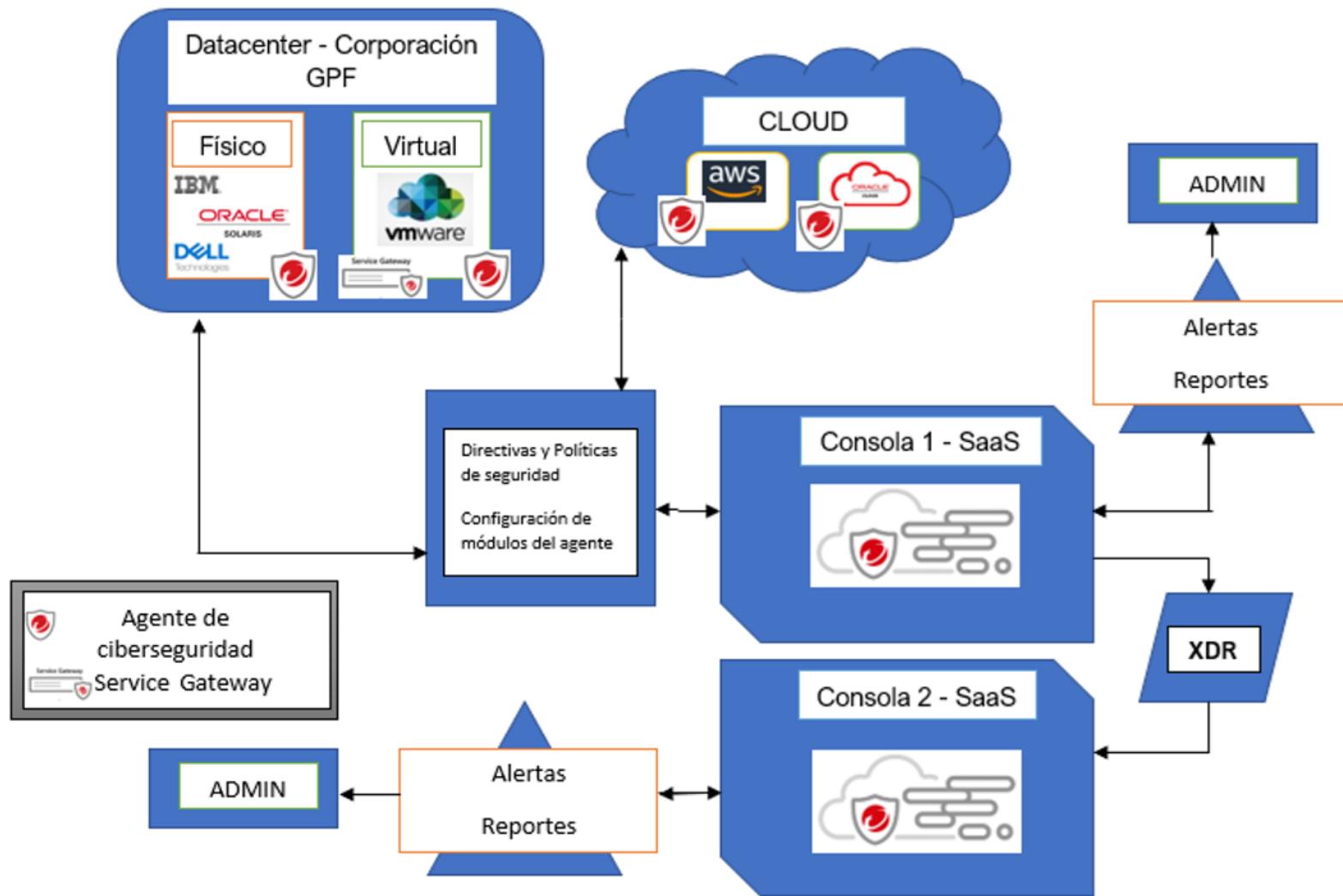
*REPRESENTA EL 56% DEL DERECHO A VOTO



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





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



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.



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.



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

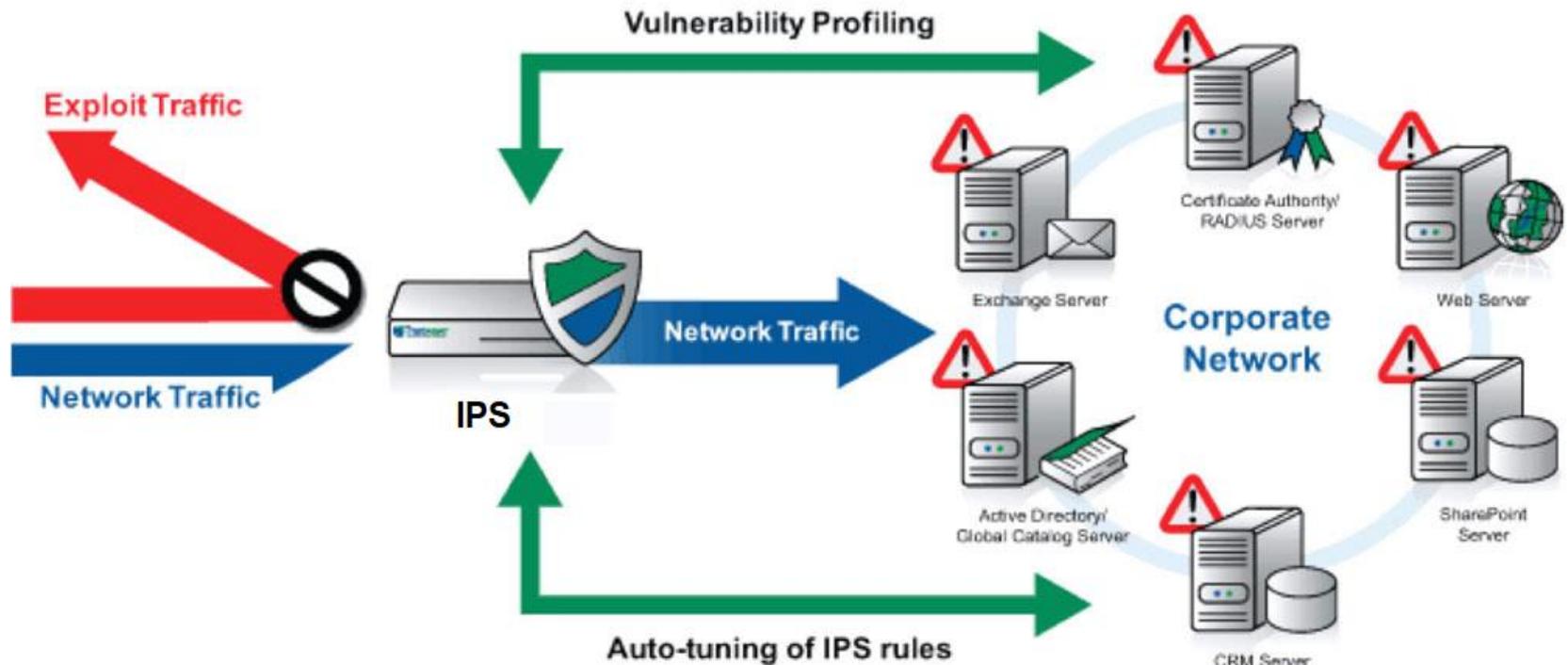


Proteger la infraestructura computacional y la información contenida en los sistemas y redes de computadoras. Por lo cual se emplean protocolos, herramientas, normas, métodos, reglas, y legislaciones creadas.



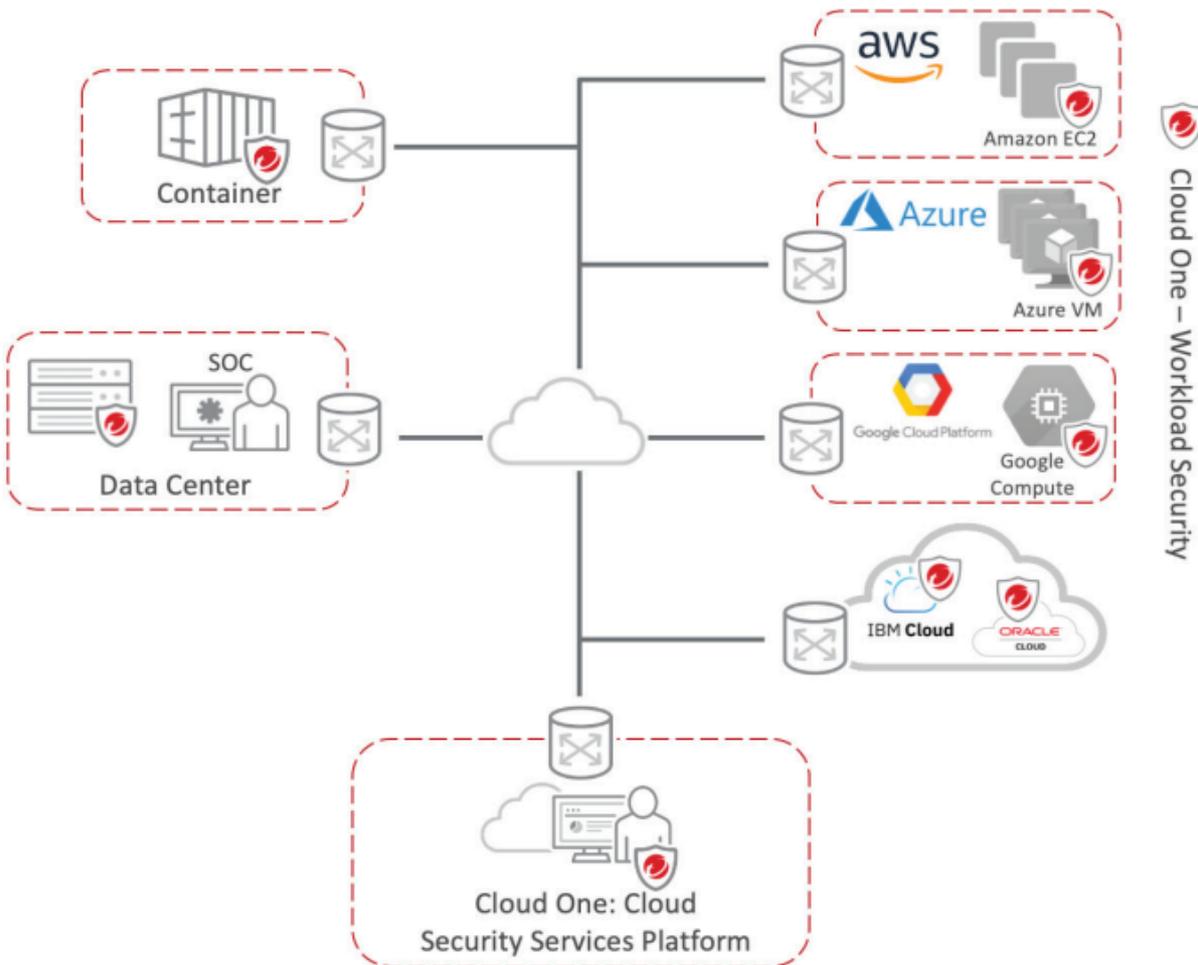
IPS – Sistema de prevención de intrusos

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.



Cloud One – Workload Security



Trend Micro - Trend Vision One

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



Implementación

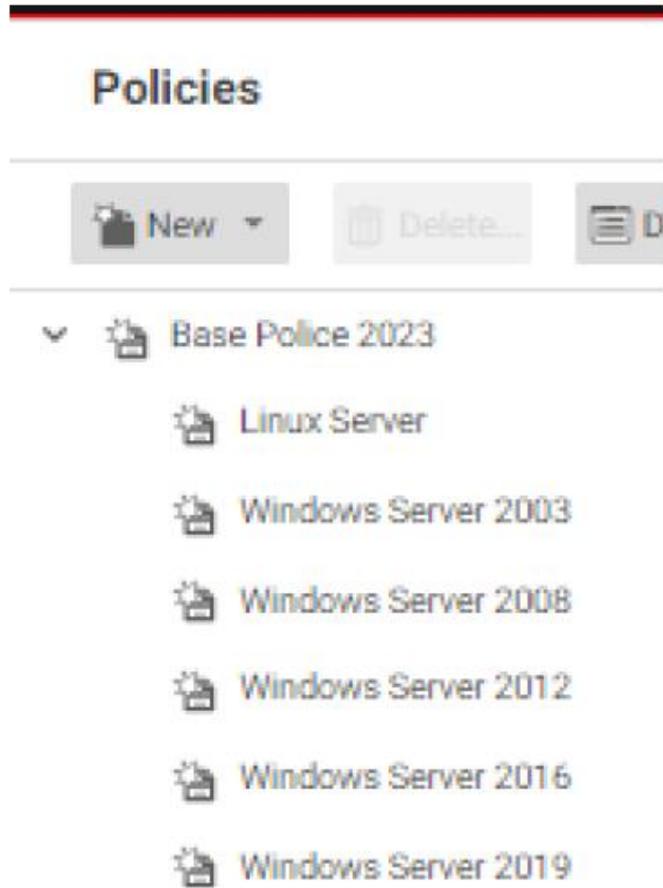


Criticidad de servidores

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



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



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

Computer: uiows01.gfybeca.int

Overview

- Anti-Malware
- Web Reputation
- Device Control
- Activity Monitoring
- Application Control
- Firewall

ENDPOINT AND WORKLOAD

Intrusion Prevention

WORKLOAD REQUIRED

- Integrity Monitoring
- Log Inspection

Interfaces

- Settings
- Updates
- Overrides

General | Advanced | Intrusion Prevention Events

Assigned Intrusion Prevention Rules

Endpoint & Workload: All | Intrusion Prevention license type: Workload

Assign/Unassign... Properties... Export... Application Types... Columns...

NAME	APPLICATION TYPE
1011016 - Identified DCERPC AddPrinterDriverEx Call Over TCP Protocol	Windows Server DCERPC
1011018 - Identified DCERPC AddPrinterDriverEx Call Over SMB Protocol	Windows SMB Server
1010521 - Netlogon Elevation Of Privilege Vulnerability Over SMB (ZeroLogon) (CVE-2020-1472)	DCERPC Services
1010539 - Identified NTLM Brute Force Attempt (ZeroLogon) (CVE-2020-1472)	Windows Services RPC Ser
1010519 - Netlogon Elevation Of Privilege Vulnerability (ZeroLogon) (CVE-2020-1472)	Windows Services RPC Ser

Implement core Endpoint & Workload rules automatically: Inherited (No)

Recommendations | Workload

Current Status: 693 Intrusion Prevention Rule(s) assigned
Last Scan for Recommendations: July 12, 2023 06:06
✓ You have no unresolved Recommendations

Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (No)

Scan For Recommendations | Cancel Recommendation Scan

Microsoft Windows Server 2003 (32 bit)

Microsoft Windows Server 2016 (64 bit)

Computer: UIOVIRSYMP01.gfybeca.int

Overview

- Anti-Malware
- Web Reputation
- Device Control
- Activity Monitoring
- Application Control
- Firewall

ENDPOINT AND WORKLOAD

Intrusion Prevention

WORKLOAD REQUIRED

- Integrity Monitoring
- Log Inspection

Interfaces

- Settings
- Updates
- Overrides

General | Advanced | Intrusion Prevention Events

Assigned Intrusion Prevention Rules

Endpoint & Workload: All | Intrusion Prevention license type: Workload

Assign/Unassign... Properties... Export... Application Types... Columns...

NAME	APPLICATION TYPE
1011016 - Identified DCERPC AddPrinterDriverEx Call Over TCP Protocol	Windows Server DCERPC
1011018 - Identified DCERPC AddPrinterDriverEx Call Over SMB Protocol	Windows SMB Server

Implement core Endpoint & Workload rules automatically: Inherited (No)

Recommendations | Workload

Current Status: 59 Intrusion Prevention Rule(s) assigned
Last Scan for Recommendations: July 12, 2023 06:05
✓ You have no unresolved Recommendations

Automatically implement Intrusion Prevention Recommendations (when possible): Inherited (Yes)

Scan For Recommendations | Cancel Recommendation Scan | Clear Recommendations

Save | Close

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)
uiowservicep03.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)
UIOVPC SISTELP01.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 ▾



Trend Cloud One™ > Endpoint & Workload Security

GPF - 102844668404 Danny Help

Workload Security Account Details | Workload Security User Properties | Help | Support | Search documentation

Dashboard Actions Alerts **Events & Reports** Computers Policies Administration

- Events
 - System Events
 - Anti-Malware Events
 - Web Reputation Events
 - Device Control Events
 - Application Control Events
 - Integrity Monitoring Events
 - Log Inspection Events
 - Firewall Events
 - Intrusion Prevention Events
- Generate Reports
 - Single Report
 - Scheduled Reports**

Scheduled Reports

New... Delete... Properties... Duplicate Run Task Now

NAME	TYPE	SCHEDULE	LAST RUN TIME	NEXT RUN TIME	ENABLED	DETAILS
Weekly Computer Report	Generate and Send Report	Weekly on Wednesday at 11:08 (...)	N/A	July 12, 2023 11:08	✓	Computer Report
Weekly Intrusion Prevention Re...	Generate and Send Report	Weekly on Monday at 07:25 (UTC...	July 11, 2023 12:08	July 17, 2023 07:25	✓	Intrusion Prevention Report - Last 1 We
Weekly Summary Report	Generate and Send Report	Weekly on Monday at 07:00 (UTC...	July 10, 2023 07:00	July 17, 2023 07:00	✓	Summary Report - Last 1 Week(s)

TREND MICRO | Workload Security

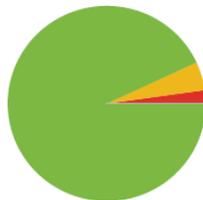
INTERNAL USE ONLY

Computer Report

Computer Filter: All Computers

Generated By: Alertas Correo
Generated On: July 12, 2023 12:08

Total Computers: 100



2 Critical
6 Warning
94 Managed
0 Unmanaged

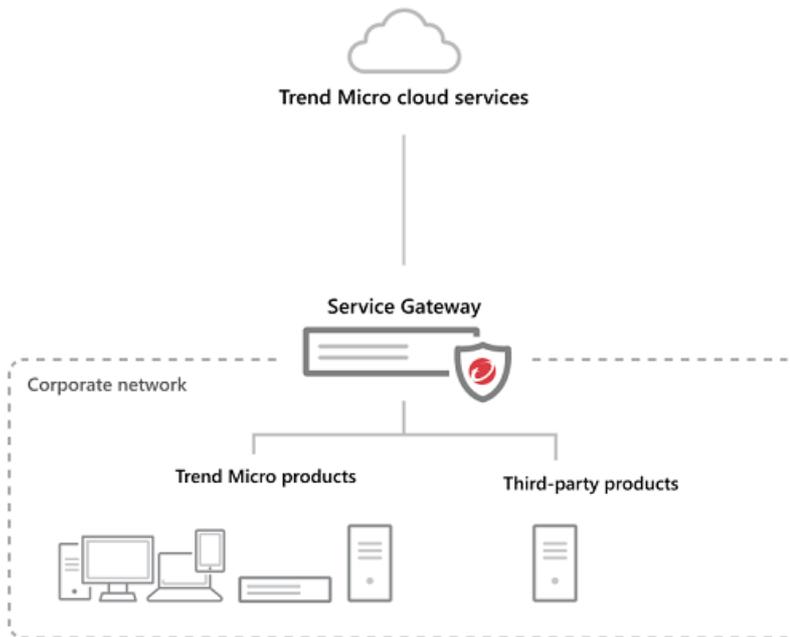
Computers By Group

Group Name	Number of Computers
Computers	100



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

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



UIOVSGV1P01

Resumen Supervisor Configurar Permisos Almacenes de datos Redes Instantáneas Actualizar

Encendido

INICIAR LA CONSOLA WEB INICIAR REMOTE CONSOLE

Sistema operativo invitado: CentOS 7 (64-bit)
Compatibilidad: ESXi 6.5 y posterior (máquina virtual versión 13)
VMware Tools: En ejecución, versión: 11269 (Administrado por invitado)

MÁS INFORMACIÓN
Nombre DNS: UIOVSGV1P01.gfybeca.int
Direcciones IP: 10.10.208.64
Host: 10.10.201.232

Hardware de máquina virtual

CPU	8 CPU
Memoria	12,09 GB, 1,21 GB memoria activa
Disco duro 1	500 GB
Adaptador de red 1	PRODUCCION01 (conectado)
Unidad de CD/DVD 1	Desconectado
Tarjeta de video	4 MB
Dispositivo VMCI	Dispositivo del bus PCI de la máquina virtual que brinda compatibilidad con la interfaz de comunicación de la

Notas

Directivas de

Atributos per

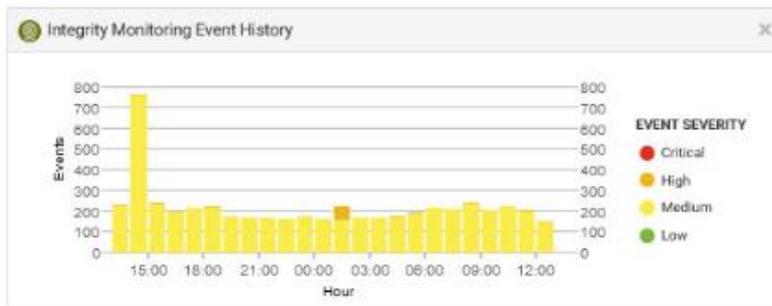
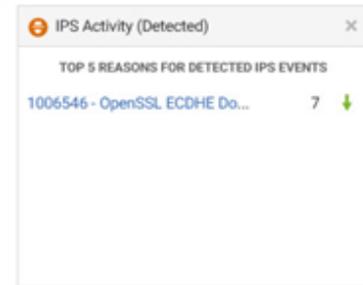
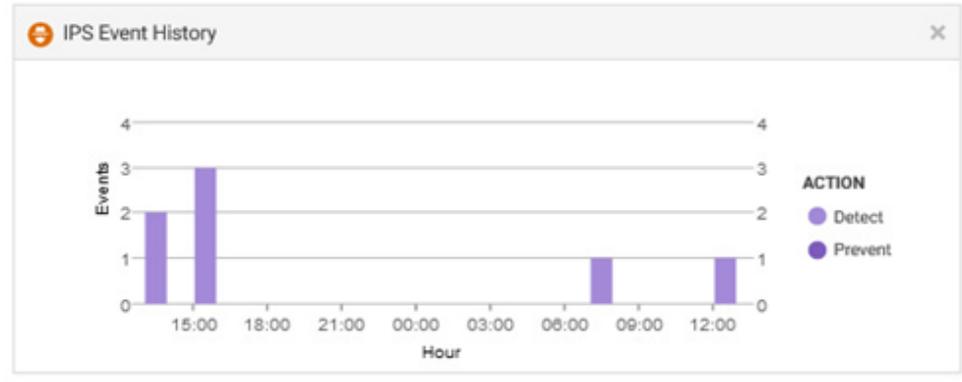
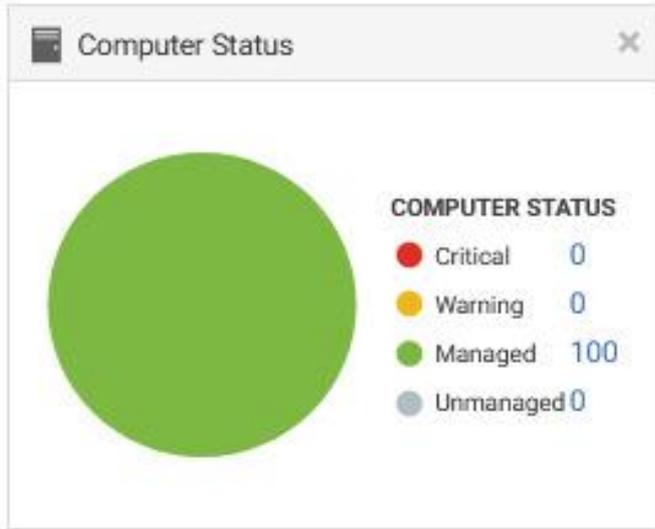
Directivas info

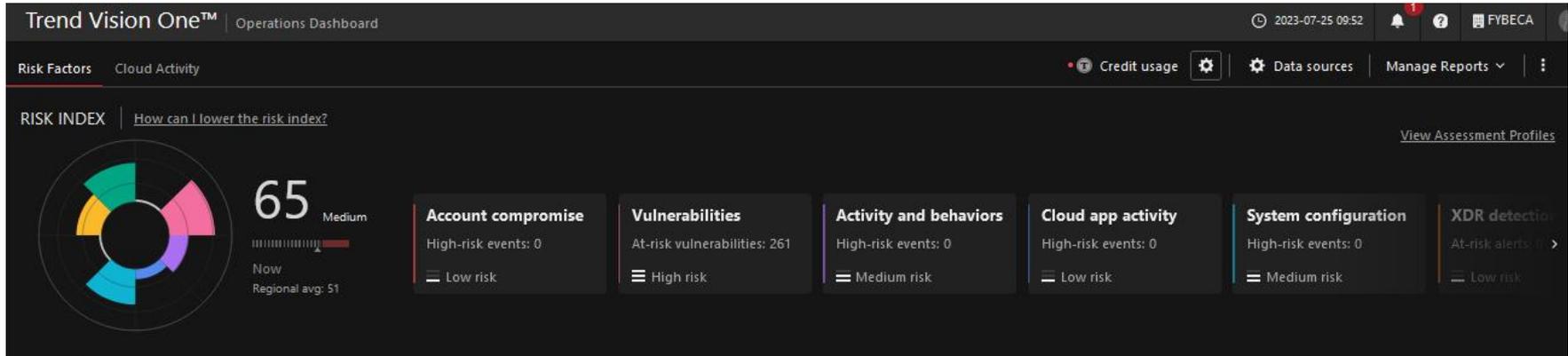
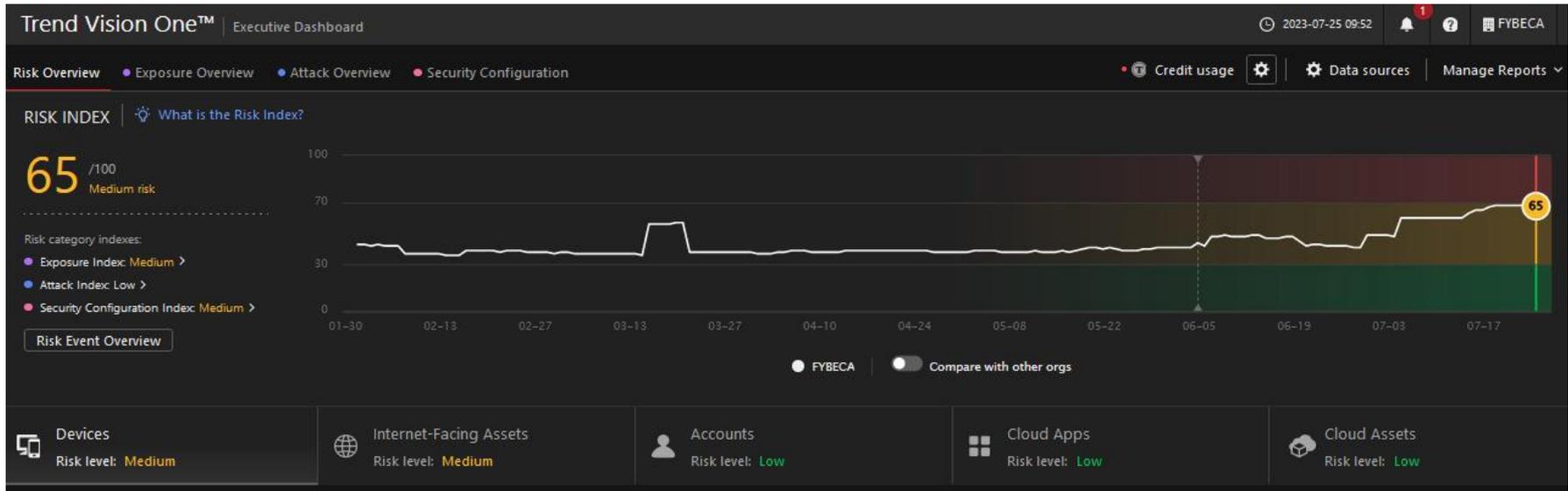
Ver todas las c

vSphere HA

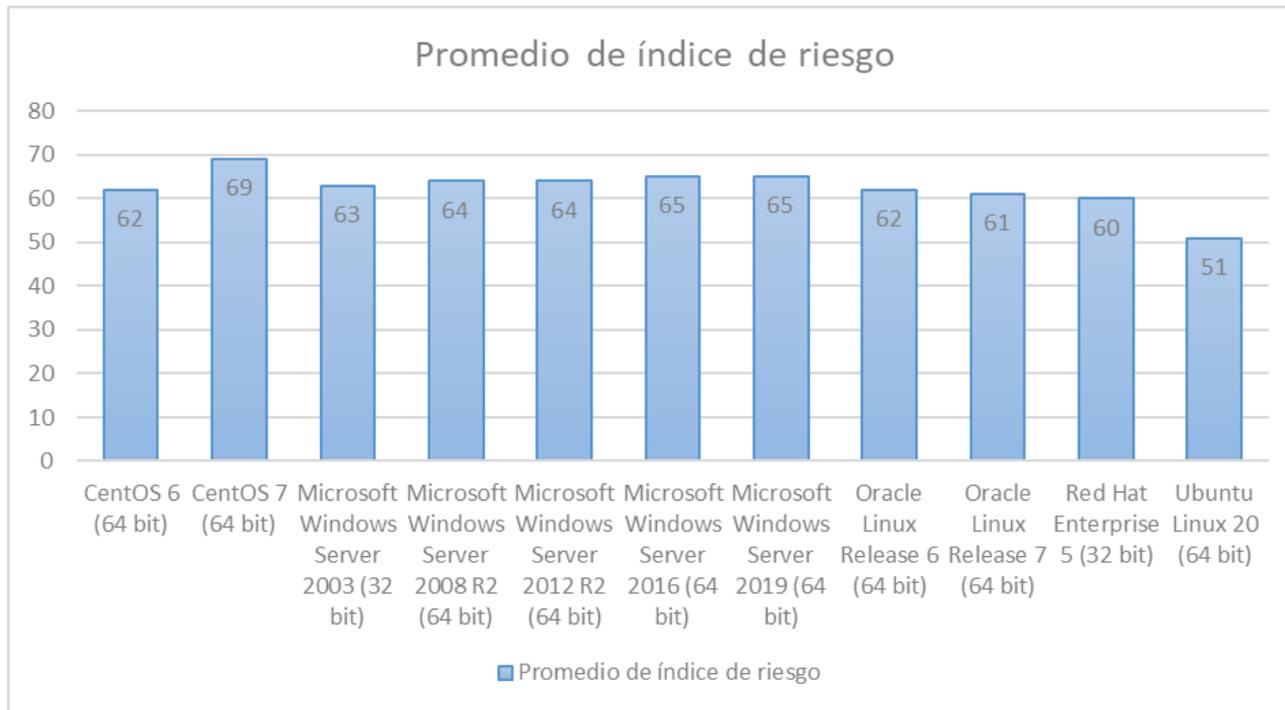
Análisis de efectividad







Riesgo de Sistemas Operativos



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



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

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

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

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



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.



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!



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA