INFORME DE GESTION DE LA PLATAFORMA DE SEGURIDAD TRELLIX EPO

Preparado para:

AERONÁUTICA CIVIL
Unidad Administrativa Especial

BOGOTÁ
2023

CONTENIDO

INTRODUCCIÓN 3
EQUIPOS GESTIONADOS 4
ESTADO ACTUAL PROTECCIÓN ANTIVIRUS MARZO 2023. 5
TRELLIX ENDPOINT SECURITY 5
VERSIONES DE PRODUCTOS TRELLIX DEL MES DE MARZO 6
Trellix Agent. 7
Endpoint Security Platform 8
Endpoint Security Threat Prevention 8
Endpoint Security Adaptive Threat Prevention 9
Endpoint Security Web Control 9
INFORMACIÓN DE ATAQUES E INFECCIONES 10
ENDPOINT SECURITY 10
Top 10 de equipos con más detecciones al corte Marzo 17 2023. 10
Top 10 de las principales amenazas detectadas durante el mes de Marzo 13
ENS: 10 principales amenazas por categoría de amenaza marzo 2023. 14
Amenazas por categoría 14
Acciones realizadas 15
INFORMACION DE ACTUALIZACIONES 17
ENS: Top 10 de las actualizaciones DAT 17
Observaciones: 18

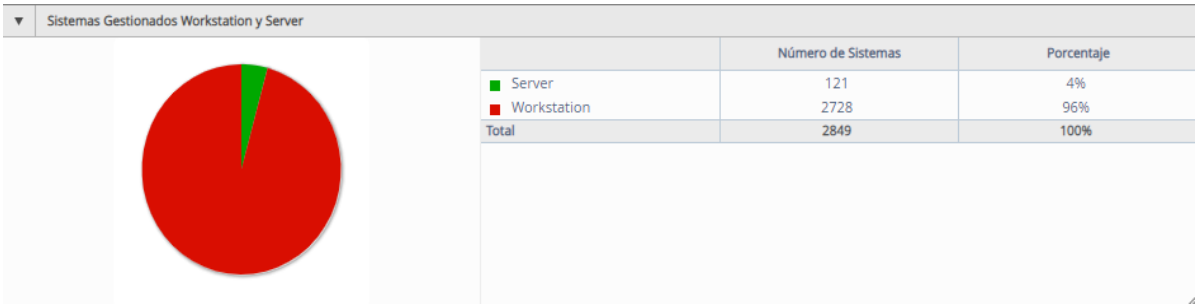
INTRODUCCIÓN

El presente informe tiene como objeto realizar una entrega de información detallada de la manera en la que actualmente opera la consola de administración Trellix ePO MVISION, la forma en la que en este momento se encuentran los productos administrados por esta, en temas relativos a estado de la protección de antivirus, estado de actualización de versiones de producto y estado de las actualizaciones de seguridad. También entregar el top 10 de los equipos que presentaron amenazas, principales amenazas detectadas, entre otros aspectos, correspondiente al mes de febrero y parte del mes de marzo de 2023.

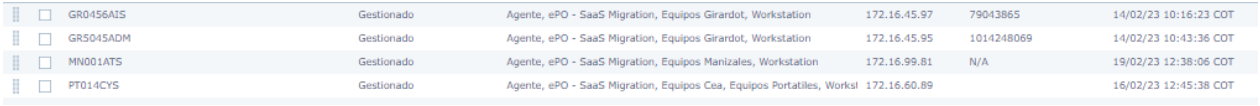
EQUIPOS GESTIONADOS

A continuación, se relaciona el número de equipos actualmente gestionados por la consola de administración Trellix MVISION ePO, número de equipos gestionados del último mes a corte de Marzo 17 de 2023.

ITEM	Marzo – 2023	
	No. Sistemas Gestionados	Porcentaje
Workstation	2728	96%
Servidores	121	4%
Total	2849	100%



A la fecha queda un reporte de 4 equipos en consola On-Premise. Algunos equipos migran automáticamente, en otros casos se tiene que hacer la actualización en sitio debido a que no se aplican las directivas y tareas de manera correcta. El número de equipos en consola On-Premise no ha sido posible migrar ya que los equipos pertenecen a distintas regionales y actualmente no tenemos una mesa de ayuda disponible para llevar a cabo esta actividad.



Se están realizando tareas de despliegue de agente en los equipos faltantes por migración para intentar restablecer comunicación y poder finalizar el proceso de subir estos equipos a MVISION. Han resultado con falla ya que son equipos que no responden a ping ni resuelven por DNS

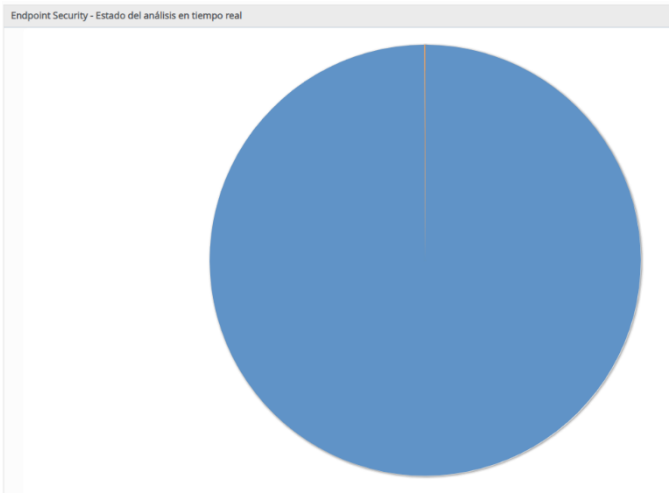
ESTADO ACTUAL PROTECCIÓN ANTIVIRUS MARZO 2023.

Es importante indicar que actualmente los equipos de cómputo de la AERONÁUTICA CIVIL (estaciones de trabajo y servidores) se encuentran netamente monitoreados por **Trellix Endpoint Security.**

TRELLIX ENDPOINT SECURITY

Estado del análisis en tiempo real.

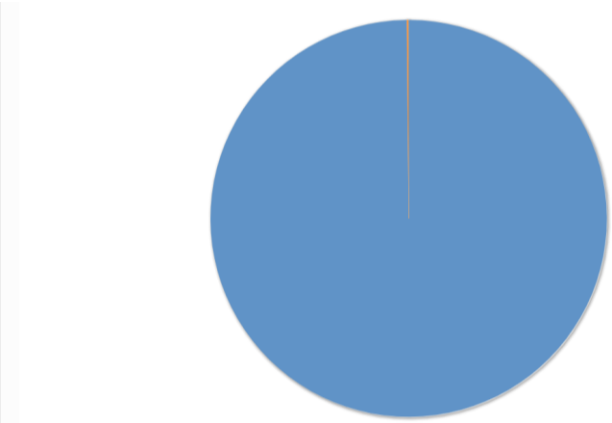
Este análisis es correspondiente al módulo de **Adaptive Threat Prevention** como detección temprana de amenazas que se puedan catalogar como amenaza en el sistema.



Análisis en tiempo real activado	Número de Sistemas de Prevenció...	Porcentaje
Verdadero	2.697	100%
Falso	2	0%
Total	2.699	100%

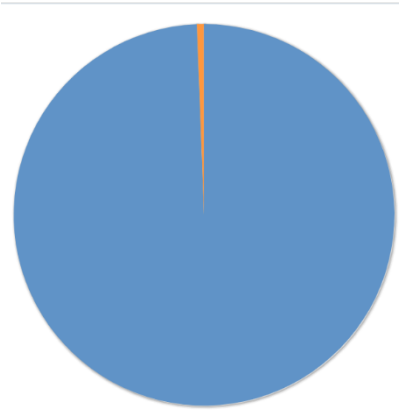
Estado de la Protección de Acceso.

Estos eventos corresponden al módulo de **Threat Prevention** en el momento de ejecución de aplicaciones que no están permitidas.



Protección de acceso a...	Número de Sistemas d...	Porcentaje
Verdadero	2.817	100%
Falso	4	0%
Total	2.821	100%

Estado de la Prevención de Exploit.



Prevención de exploit activa...	Número de Sistemas de Pre...	Porcentaje
Verdadero	2.804	99%
Falso	17	1%
Total	2.821	100%

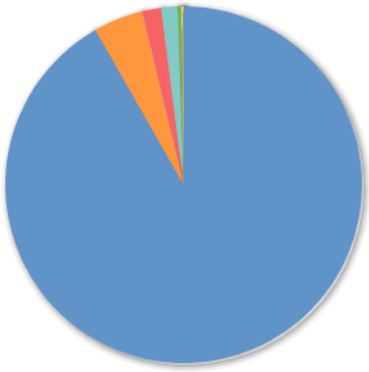
Este gráfico nos muestra el estado de explotación y minería de datos los cuales están en el módulo de **Exploit Prevention**.

VERSIONES DE PRODUCTOS TRELLIX DEL MES DE MARZO

A continuación, serán mostrados los datos relativos a las versiones de producto de los principales componentes Trellix utilizados en la AERONÁUTICA CIVIL, con el fin de dar a conocer las diferentes versiones que se encuentran instaladas en la red.

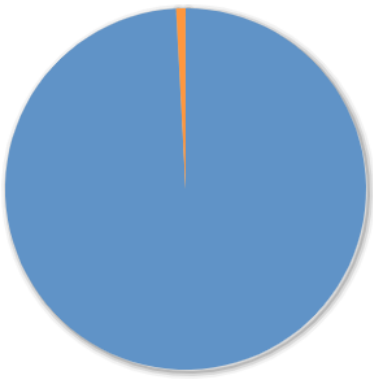
Trellix Agent.

Versiones de Mcafee agent PC



Versión de prod...	Número de Sist...	Porcentaje
5.7.8.262	2.500	92%
5.7.7.378	123	5%
5.7.6.251	47	2%
5.7.4.399	40	1%
5.7.5.504	9	0%
	5	0%
5.6.6.232	1	0%
Total	2.725	100%

Versiones de Mcafee agent Servidores



Versión de prod...	Número de Sist...	Porcentaje
5.7.8.262	120	99%
5.7.4.418	1	1%
Total	121	100%

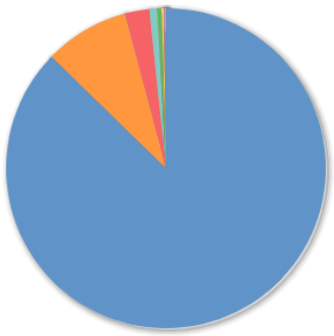
Actualmente se sigue en una tarea constante para actualizar en su totalidad y a la última versión los equipos de la AC. Es de aclarar que los nuevos equipos que sean instalados a través de la **URL** van a subir con la versión **5.7.8.262.** Esta versión incluye una mejora y resuelve varios problemas, incluidos los de seguridad. Por otro lado, los productos se han estado revisando constantemente en busca de cualquier novedad en el cambio de su versionamiento. El **92 %** de

los equipos se encuentran actualizados con las últimas dos versiones, esto a nivel de estaciones de trabajo.

Endpoint Security Platform

ENS Platform es la interfaz gráfica donde van integrados todos los módulos de ENS.

Versiones Endpoint Security Platform

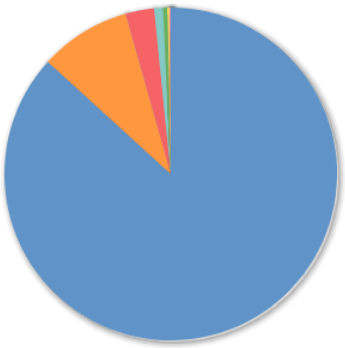


Versión de prod...	Número de Sist...	Porcentaje
10.7.0.5162	2.487	87%
10.7.0.3468	244	9%
10.7.0.3255	71	2%
	22	1%
10.7.0.3012	13	0%
10.7.0.3199	6	0%
10.7.0.3460	4	0%
10.7.0.2174	1	0%
10.7.7.107	1	0%
Total	2.849	100%

Endpoint Security Threat Prevention

ENS Threat Prevention es el módulo protección y el antivirus del sistema.

Versiones Endpoint Security Threat Prevention

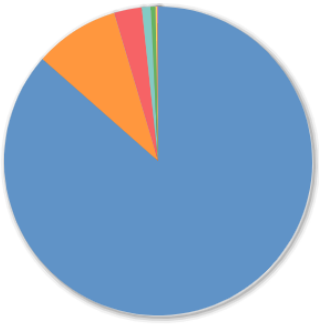


Versión de prod...	Número de Sist...	Porcentaje
10.7.0.5200	2.472	87%
10.7.0.3497	252	9%
10.7.0.3299	80	3%
	24	1%
10.7.0.3210	12	0%
10.7.0.3113	7	0%
10.7.0.2298	1	0%
10.7.7.24	1	0%
Total	2.849	100%

Endpoint Security Adaptive Threat Prevention

ENS ATP es el módulo de protección en tiempo real y detección temprana.

Versiones Endpoint Security Adaptive Threat Prevention

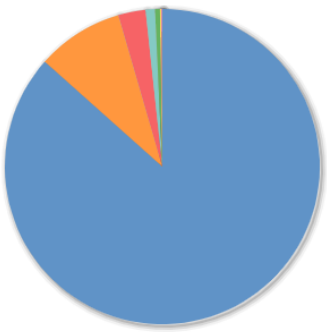


Versión de prod...	Número de Sist...	Porcentaje
10.7.0.5177	2.463	86%
10.7.0.3590	254	9%
10.7.0.3437	83	3%
	26	1%
10.7.0.3183	14	0%
10.7.0.3252	6	0%
10.7.0.2481	2	0%
Total	2.848	100%

Endpoint Security Web Control

Es el módulo de control en la navegación acá podemos ver los equipos que navegan en páginas que pueden ser potencialmente peligrosas para el sistema.

Versiones Endpoint Security Web Control



Versión de prod...	Número de Sist...	Porcentaje
10.7.0.5162	2.466	87%
10.7.0.2697	254	9%
10.7.0.2581	80	3%
	27	1%
10.7.0.2463	14	0%
10.7.0.2532	5	0%
10.7.0.1306	1	0%
10.7.0.1891	1	0%
Total	2.848	100%

Se evidencia que aproximadamente el **87 %** de los equipos ya están actualizados con las últimas dos versiones de Endpoint Security, se encuentra en ejecución un despliegue automático para que siempre ejecute el **ENS** en los equipos que no posean estos productos. En algunos equipos no fue posible realizar la actualización desde consola **ePO MVISION** debido a que el agente presenta corrupción. En otros casos si bien se han migrado los equipos no se actualizan al

versionamiento actual del agente y ENS lo que genera la creación de nuevas tareas cliente para su actualización.

Las versiones de productos que se están instalando actualmente en los nuevos equipos son:

Productos	Versión
Agente Trellix	*5.7.8.262*
Plataforma de Endpoint Security	*10.7.0.5162*
Módulo Prevención de amenazas	*10.7.0.5200*
Módulo Protección adaptable frente amenazas	*10.7.0.5177*
Módulo Control Web	*10.7.0.5162*

INFORMACIÓN DE ATAQUES E INFECCIONES

A continuación, se presenta una relación de los eventos de amenazas, detecciones y acciones realizadas por los productos **Trellix ENS Threat Prevention**, así como de los apoyos en detección realizados por el producto **ENS Adaptive Threat Protection**.

ENDPOINT SECURITY

Top 10 de equipos con más detecciones al corte marzo 17 2023.

En la tabla se muestra el top 10 de las máquinas que tuvieron más detecciones de amenazas durante el mes de diciembre, en total se detectaron **2824** amenazas.

ENS: Los 10 equipos con más detecciones mes Marzo - 2023

Nombre de sistema	Número de Eventos de amenaza
BOG120	669
BO6469DOC	662
BO0382SIN	401
MT8553STE	303
CL8486STE	250
CL7103SEI	177
CL0914CYS	124
BO004INV	91
BO7278CEA	74
LT7193ADM	73
Total	2.824

Se evidencia que las dos principales amenazas detectadas son de tipo **Autoprotección** y **Protección de acceso**, **BOG120** presentó eventos de amenaza tipo **Intrusión de host,** este tipo de amenaza se presentó al ser un server de tipo DNS externo secundario. Los intentos de vulneración que se han presentado por direcciones IP de origen malicioso han sido en su totalidad bloqueados.

ENS: Detecciones de malware por Grupo Aerocivil.

Nombre de grupo	Número de Eventos de amenaza
CEA	2.396
Piso-4	937
Cali	527
CNA	499
Portatiles	490
CGAC	430
Barranquilla	404
Leticia	392
Piso-1 y Sotano	383
Piso-2	341
Piso-3	237
Medellin	235
Pereira	140
Cartagena	88
Villavicencio	88
Guaymaral	75
Cucuta	69
Bucaramanga	63
Yopal	61
Rionegro	58
Piso-5	55
Santa Marta	45
Arauca	42
Tame	34
ARANDA	26
Barrancabermeja	26
Popayan	25
Ibague	24
Pto Asis	24
Mitu	21
BOGOTA	18
Armenia	17
San Andres	15
Quibdo	14
Tumaco	13
Pasto	12
Monteria	11

Valledupar	10
ALMACEN	8
Buenaventura	8
DORADO	7
DE ARCHIVOS	6
Mariquita	6
Neiva	6
Florencia	5
Girardot	5
Otros Aeropuertos	5
Ipiales	4
SERVIDOR MOODLE	4
Guapi	3
Corozal	2
Carepa	1
Equipos Sta. Sofia	1
Puerto Inirida	1
San Jose del Guaviare	1
Tolu	1
Total	8.419

Top 10 de las principales amenazas detectadas durante el mes de marzo

Nombre de amenaza	Número de Eventos de amenaza
autorun.inf	900
ExP:NIPS Violation	707
ATP/SuspectIf1efb0fddc15	664
Core Protection - Sanitize Trellix processes	555
W32/Gnamer	128
Prueba malware	117
W32/Victy.wormlait	69
Core Protection - Protect core McAfee files and folders	40
ATP/SuspectI50ef7c645fd5	34
Rule 10	29
Total	3.243

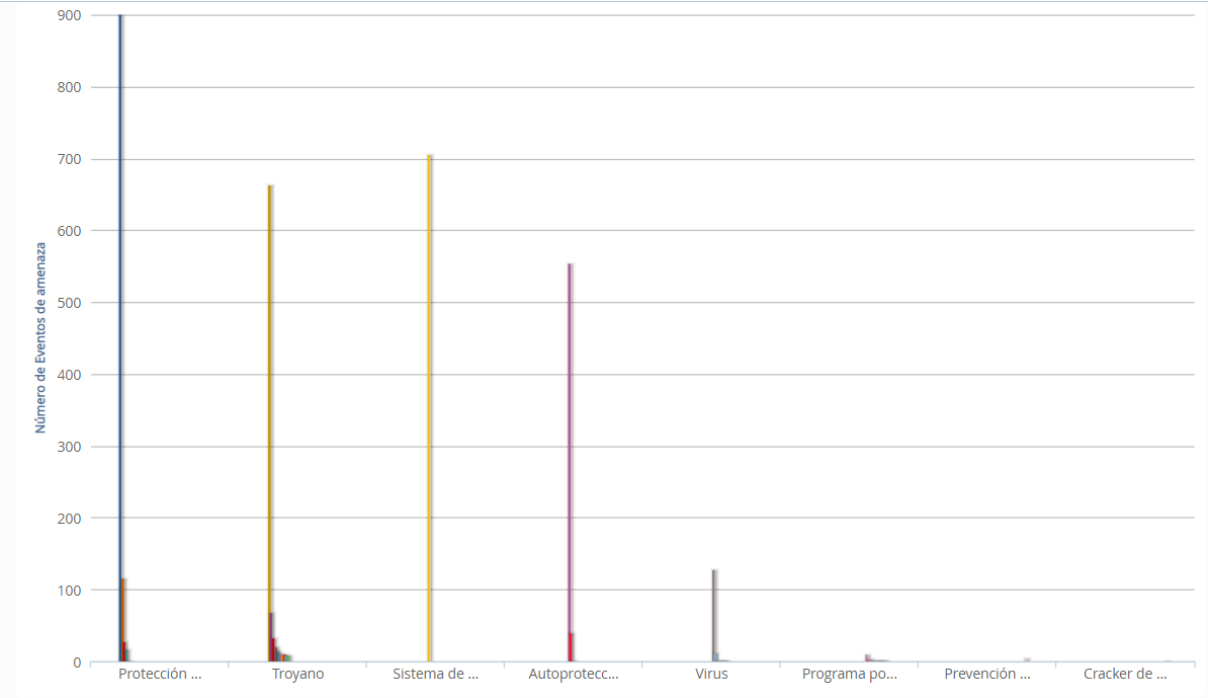
En la tabla se evidencia el top 10 de las principales amenazas registradas durante el mes de marzo, donde se evidencia que la mayoría de las amenazas presentadas se dieron principalmente por el intento de ejecución de archivos .Info en los equipos. De igual forma, para el segundo

evento de amenaza detectada es el Exp:NIPS Violation que son intentos de conexión entrantes de fuerza bruta

ENS: 10 principales amenazas por categoría de amenaza marzo 2023.

Amenazas por categoría

En el siguiente gráfico se muestra la cantidad de amenazas por categoría detectadas durante el mes de Marzo, donde se puede observar que la categoría **Protección de acceso** representa un **31.61 %** de las amenazas detectadas en la organización. Mientras que la categoría **Troyano** representa un **25.37 %** de las amenazas detectadas en el mes. Las dos categorías principales para este mes representan el **56.98 %** del total de amenazas detectadas en la entidad.

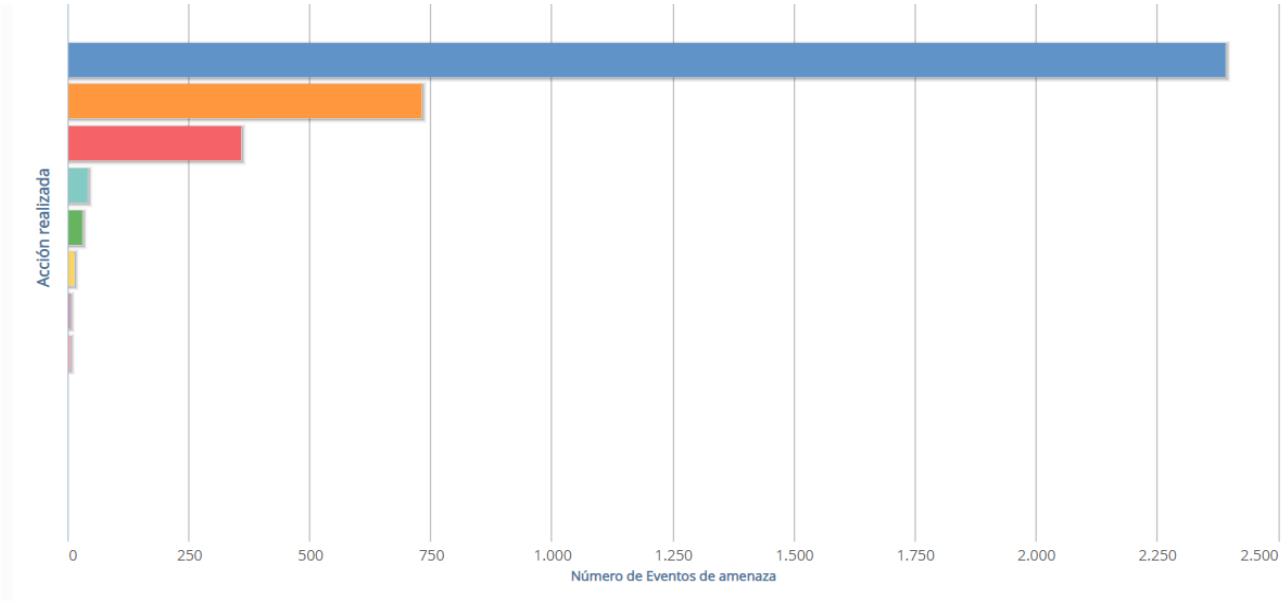


Tipo de amenaza->Nombre de amenaza	Número de Eventos de amenaza
Protección de acceso	**1.065**
autorun.inf	900
Prueba malware	117
Rule 10	29
Prevent Office Malware	18
Ejecucion Exe	1
Troyano	**855**
ATP/SuspectIf1efb0fddc15	664
W32/Victy.worm!ait	69
ATP/SuspectI50ef7c645fd5	34
ATP/SuspectI2b684979d617	21
LNK/Trojan-FQBLI2C95AB71F89E	16
GenericRXTJ-EBIBECDF3075C43	13
BAT/Agent.cy	10
VBS/Agent.gs	10
ATP/SuspectIb5cebdc81aa3	9
ATP/SuspectIcb377e2ba78e	9
Sistema de prevención de intrusiones en la red	**707**
ExP:NIPS Violation	707
Autoprotección	**596**
Core Protection - Sanitize Trellix processes	555
Core Protection - Protect core McAfee files and folders	40
Core Protection - Sanitize McAfee processes	1
Virus	**146**
W32/Gnamer	128
W32/Rontokbro.a.gen@MM	12
VBS/Autorun.worm.aajk	2
Artemis!14638217EF40	1
Autorun.gallnkI1D6064FFD701	1
VBS/Autorun.worm.aapo	1

Acciones realizadas

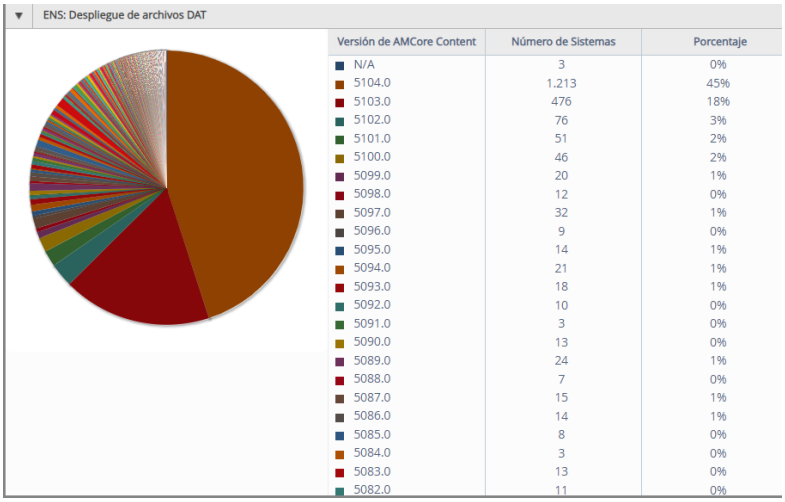
En el siguiente gráfico se muestran las acciones realizadas por el antivirus Trellix frente a las amenazas detectadas durante el mes de marzo, el **9 %** de estas amenazas fueron **eliminadas** y el **85 %** corresponde a unidades que fueron bloqueadas durante el análisis diario que el antivirus realiza en los equipos de la entidad.

Acción realizada	Número de Eventos de amenaza
Bloqueado	2.394
Protección adaptable frente a amenazas bloquearía	732
Eliminar	359
Protección adaptable frente a amenazas limpiaría	43
Permitir	30
Advertido	13
Protección adaptable frente a amenazas contendría	6
Ninguna	5
Denegar acceso	1
Total	3.583



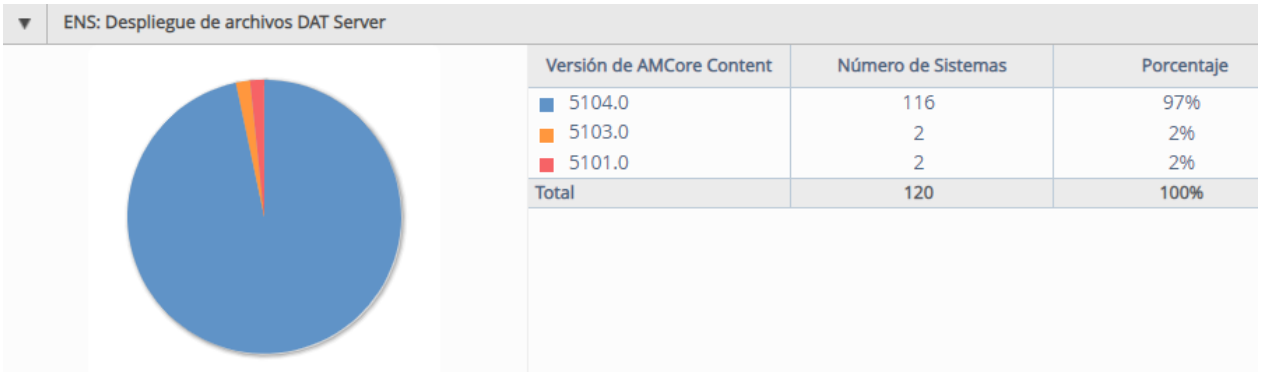
INFORMACION DE ACTUALIZACIONES

ENS: Top 10 de las actualizaciones DAT



Versión de AMCore Content	Número de Sistemas	Porcentaje
N/A	3	0%
5104.0	1.213	45%
5103.0	476	18%
5102.0	76	3%
5101.0	51	2%
5100.0	46	2%
5099.0	20	1%
5098.0	12	0%
5097.0	32	1%
5096.0	9	0%
5095.0	14	1%
5094.0	21	1%
5093.0	18	1%
5092.0	10	0%
5091.0	3	0%
5090.0	13	0%
5089.0	24	1%
5088.0	7	0%
5087.0	15	1%
5086.0	14	1%
5085.0	8	0%
5084.0	3	0%
5083.0	13	0%
5082.0	11	0%

Se han estado actualizando **1689** máquinas con una versión de firma .DAT diariamente.



Versión de AMCore Content	Número de Sistemas	Porcentaje
5104.0	116	97%
5103.0	2	2%
5101.0	2	2%
Total	120	100%

En el gráfico se muestran las versiones del archivo DAT y la cantidad de equipos con **Endpoint Security** que tiene cada versión durante el mes de marzo. Para el caso de los servers, al terminar

la jornada estos se actualizan automáticamente a la última versión de la firma que esté disponible, para el caso actual con la versión **5104**.

Observaciones:

- Aún quedan equipos pendientes por migrar de manera forzada desde consola **On-Premise**. Se ha registrado un incremento de estos equipos (**4**) ya que solo alcanzan a comunicarse una sola vez imposibilitando la migración exitosa a consola **ePO MVISION.**

- Se ha estado realizando a diario un reconocimiento de los equipos que no reportan comunicación desde hace mas de un mes es de 480 equipos actualmente

- Se notifica a la ingeniera Laura Pedraza las novedades que se han estado presentando con el renombramiento de algunos equipos a nivel central que se han visualizado desde la consola **ePO MVISION**. Se le recomienda tener especial cuidado con este tipo de novedades para evitar contratiempos tanto en el AD como en la consola de antivirus.

- El 7 de enero de 2023 se notificó a la Aeronáutica Civil que la mesa de ayuda había sido retirada, por lo cual ha ocasionado un aumento de equipos no gestionados o que no se comunican en la consola debido a la falta de validación en sitio para tener un estatus real de lo que está sucediendo actualmente en los equipos.

- Para tener una gestión efectiva y una retroalimentación adecuada de las novedades que se presenten en la consola, es fundamental contar con apoyo en sitio en diferentes equipos. Este apoyo permitirá que los especialistas puedan verificar y validar el estatus real de los equipos, así como también realizar las tareas necesarias para solucionar cualquier problema que se presente en la consola. Además, contar con el apoyo en sitio permitirá que el equipo de gestión pueda tomar decisiones más precisas y oportunas, lo que a su vez contribuirá a una gestión más eficiente y efectiva de los recursos. En definitiva, contar con un equipo que brinde apoyo en sitio es esencial para lograr una gestión exitosa y una retroalimentación constante en el manejo de los equipos.

Elaborado por:



Cesar Mauricio Sanchez Pineda
Administrador consola ePO

VoBo Jorge Enrique Torres Beltran
Supervisor Contrato 22001274 H3