INFORME DE GESTION DE LA PLATAFORMA DE SEGURIDAD TRELLIX EPO

Preparado para:

AERONÁUTICA CIVIL
Unidad Administrativa Especial

BOGOTÁ
2022

CONTENIDO

INTRODUCCIÓN 3
EQUIPOS GESTIONADOS 4
ESTADO ACTUAL PROTECCIÓN ANTIVIRUS SEPTIEMBRE 2022. 4
MCAFEE ENDPOINT SECURITY 5
VERSIONES DE PRODUCTOS MCAFEE DEL MES DE SEPTIEMBRE 6
McAfee Agent 6
Endpoint Security Platform 6
Endpoint Security Threat Prevention 7
Endpoint Security Adaptive Threat Protección 7
Endpoint Security Web Control 8
INFORMACIÓN DE ATAQUES E INFECCIONES 9
ENDPOINT SECURITY 9
Top 10 de equipos con más detecciones durante el mes de septiembre 9
Top 10 de las principales amenazas detectadas durante el mes de septiembre 11
ENS: 10 principales amenazas por categoría de amenaza septiembre 2022 11
Amenazas por categoría 11
Acciones realizadas 12
INFORMACION DE ACTUALIZACIONES 14
ENS: Top 10 de las actualizaciones DAT 14
Observaciones 14

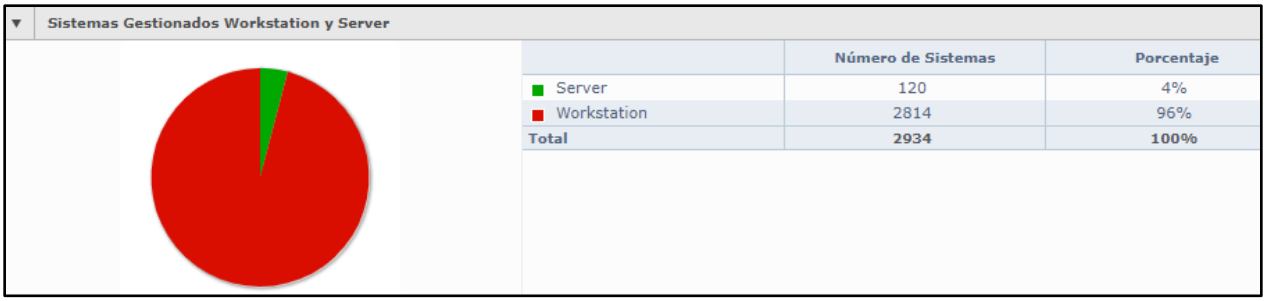
INTRODUCCIÓN

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, correspondiente al mes de septiembre de 2022.

EQUIPOS GESTIONADOS

A continuación, se relaciona el número de equipos actualmente gestionados por la consola de administración Trellix ePO, en donde se realiza una comparativa del número de equipos gestionados del mes de septiembre de 2022.

ITEM	Julio - 2022		Septiembre - 2022	
	No Sistemas Gestionados	Porcentaje	No Sistemas Gestionados	Porcentaje
Workstation	2727	96%	2814	96%
Servidores	120	4%	120	4%
Total	2847	100%	2934	100%



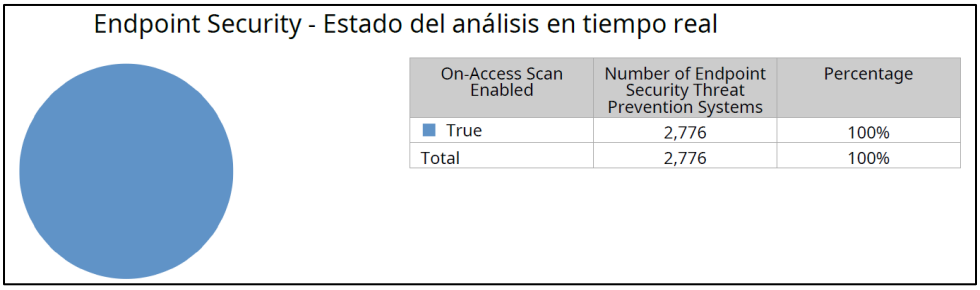
En el mes de septiembre se continuó con migración de equipos a consola en la nube. Se realizo depuración con base en la revisión de equipos que presentaban una versión de firma desactualizada, más concretamente equipos con versión 47 y 48. Es de aclarar, que aún siguen apareciendo nuevos equipos en consola local. A la fecha queda un reporte de 13 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.

ESTADO ACTUAL PROTECCIÓN ANTIVIRUS SEPTIEMBRE 2022.

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

TRELLIX ENDPOINT SECURITY

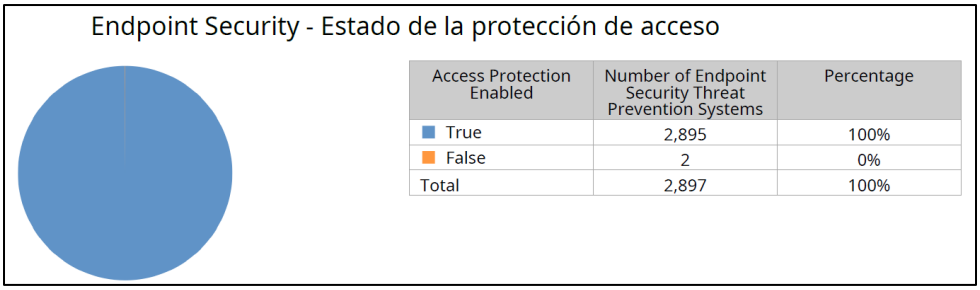
Estado del análisis en tiempo real.



On-Access Scan Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,776	100%
Total	2,776	100%

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

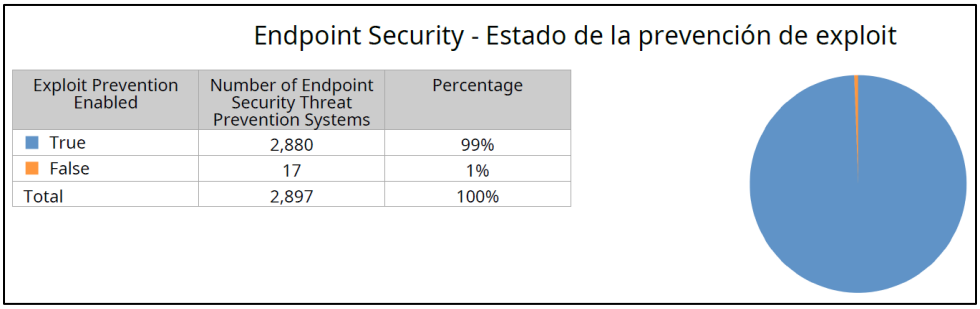
Estado de la Protección de Acceso.



Access Protection Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,895	100%
False	2	0%
Total	2,897	100%

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

Estado de la Prevención de Exploit.



Exploit Prevention Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,880	99%
False	17	1%
Total	2,897	100%

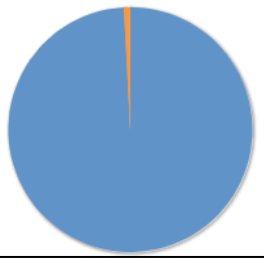
Este gráfico nos muestra el estado de explotación y minería de datos los cuales están en el módulo de **Exploit Prevention**.

VERSIONES DE PRODUCTOS TRELLIX DEL MES DE SEPTIEMBRE

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.

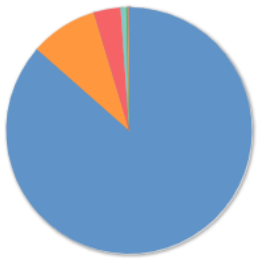
Trellix Agent.

Versiones de Mcafee agent Servidores



Versión de producto (Agent)	Número de Sistemas	Porcentaje
5.7.7.378	119	99%
5.7.4.418	1	1%
Total	120	100%

Versiones de Mcafee agent PC



Versión de producto (Agent)	Número de Sistemas	Porcentaje
5.7.7.378	2.432	86%
5.7.6.251	249	9%
5.7.4.399	100	4%
5.7.5.504	20	1%
	6	0%
5.6.6.232	3	0%
5.6.3.157	2	0%
Total	2.812	100%

Desde el mes de Julio, se generó una nueva versión del agente **5.7.7.378**, 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 **5.7.7.378.** 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.

Endpoint Security Platform

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

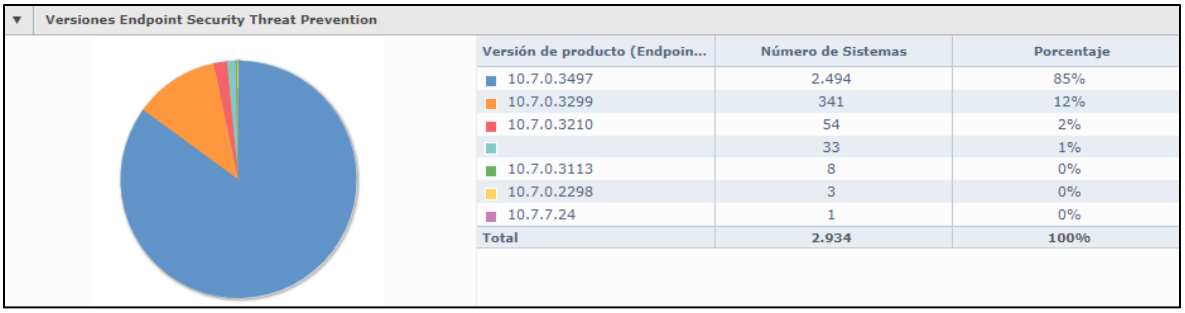


Versiones Endpoint Security Platform

Versión de producto (Endpoin...	Número de Sistemas	Porcentaje
10.7.0.3468	2.471	84%
10.7.0.3255	322	11%
10.7.0.3460	45	2%
10.7.0.3012	37	1%
	33	1%
10.7.0.3199	22	1%
10.7.0.2174	3	0%
10.7.7.107	1	0%
Total	**2.934**	**100%**

Endpoint Security Threat Prevention

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

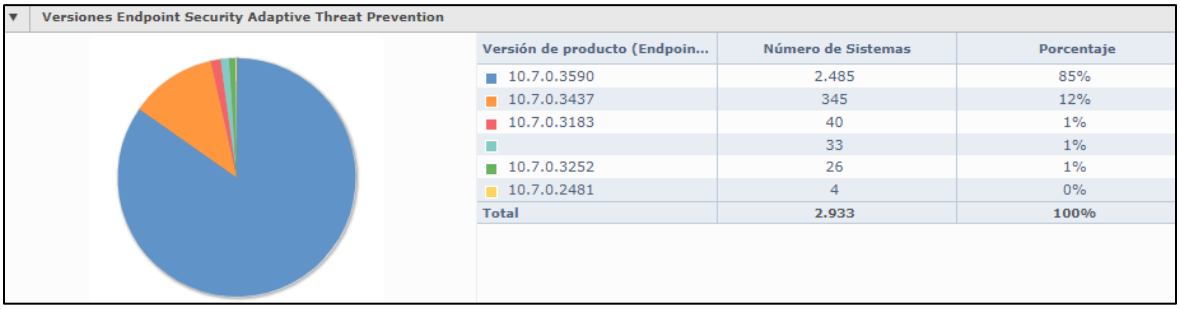


Versiones Endpoint Security Threat Prevention

Versión de producto (Endpoin...	Número de Sistemas	Porcentaje
10.7.0.3497	2.494	85%
10.7.0.3299	341	12%
10.7.0.3210	54	2%
	33	1%
10.7.0.3113	8	0%
10.7.0.2298	3	0%
10.7.7.24	1	0%
Total	**2.934**	**100%**

Endpoint Security Adaptive Threat Prevention

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

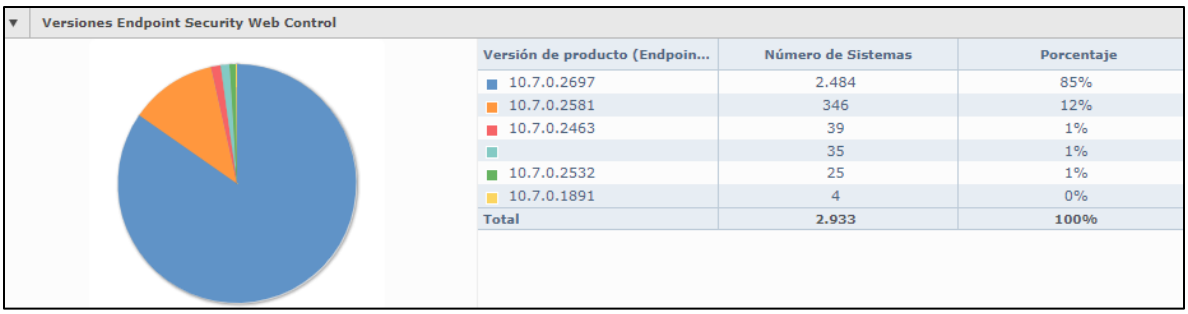


Versiones Endpoint Security Adaptive Threat Prevention

Versión de producto (Endpoin...	Número de Sistemas	Porcentaje
10.7.0.3590	2.485	85%
10.7.0.3437	345	12%
10.7.0.3183	40	1%
	33	1%
10.7.0.3252	26	1%
10.7.0.2481	4	0%
Total	**2.933**	**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.



Versión de producto (Endpoin...	Número de Sistemas	Porcentaje
10.7.0.2697	2.484	85%
10.7.0.2581	346	12%
10.7.0.2463	39	1%
	35	1%
10.7.0.2532	25	1%
10.7.0.1891	4	0%
Total	2.933	100%

Se evidencia que aproximadamente el **96,5%** 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, por lo cual se realizaron una serie de correos para la apertura de casos a la **linea3000** para que realicen la correcta instalación en sitio, por esta razón se evidencian sistemas sin versionamiento de los productos, debido a la corrupción que presentan actualmente en el agente y los equipos que aún están en proceso de migración desde la consola local.

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

Productos	Versión
Agente McAfee	*5.7.7.378*
Plataforma de Endpoint Security	*10.7.0.3468*
Módulo Prevención de amenazas	*10.7.0.3497*
Módulo Protección adaptable frente amenazas	*10.7.0.3590*
Módulo Control Web	*10.7.0.2697*

INFORMACIÓN DE ATAQUES E INFECCIONES

A continuación, se presenta una relación de los eventos de amenazas, detecciones y acciones realizadas por los productos **McAfee 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 durante el mes de septiembre.

En la tabla se muestra el top 10 de las máquinas que tuvieron más detecciones de amenazas durante el mes de septiembre, en total se detectaron **3.764** amenazas.

ENS: Los 10 equipos con más detecciones mes Septiembre - 2022

Nombre de sistema	Número de Eventos de amenaza
BOG130	1.526
BO0991CEA	598
PP6170ADM	420
BO004SAR	323
BO0162CEA	307
BO7083SST	233
BOG120	122
BO7463ATS	104
EJ0566AD	68
BO001SLB	63
Total	**3.764**

Se evidencia que la principal amenaza detectada fue por el tipo **Prevención de exploits**, estas se presentan debido a que el equipo **BOG130** cuenta con una administración por parte del contratista **K2 Ingeniería S.A.S.** y desde la cuenta **Adminambienta**l se generan diferentes ejecutables automáticos de manera paralela, de tal forma que en conjunto se crean funcionalidades para la revisión de los datos de ruido y procesamiento diario del aeropuerto como objeto de contrato con la entidad. Es por esta razón que se realizan una serie de exclusiones en el server. Por otro lado, el equipo **BO0991CEA** presenta eventos de amenaza tipo **Autoprotección,** se realiza un caso a L3000 para la eliminación del aplicativo **Autorun.inf** desde la carpeta OneDrive del usuario final.

ENS: Detecciones de malware por Grupo Aerocivil.

Nombre de grupo	Número de Eventos de amenaza
Portatiles	310
Piso-1 y Sotano	257
CEA	238
CNA	175
Cali	158
Leticia	146
Piso-4	141
Piso-2	106
CGAC	102
Medellin	93
Rionegro	87
Piso-3	50
Barranquilla	45
Cartagena	41
Villavicencio	36
Santa Marta	30
Tame	25
Cucuta	23
Piso-5	22
Pto Asis	17
Guaymaral	16
Pereira	15
Yopal	15
Ibague	14
Barrancabermeja	10
Popayan	10
Arauca	6
Pasto	6
Bucaramanga	5
Neiva	5
DE ARCHIVOS	4
Monteria	4
Armenia	3
BOGOTA	3
San Andres	3
DORADO	2
Quibdo	2
Carepa	1
Equipos Sta. Sofia	1
Guapi	1
Linea 3000	1
Mitu	1
San Jose del Guaviare	1
Total	**2.231**

Top 10 de las principales amenazas detectadas durante el mes de septiembre.

En la siguiente tabla se evidencia el top 10 de las principales amenazas registradas durante el mes de septiembre, donde se evidencia que la mayoría de las amenazas presentadas (***Suspicious Double File Extension Execution y Autorun.inf***) se dieron principalmente por la ejecución del aplicativo **ATechScheduler** en el server **BOG130** y la comprobación del virus **Autorun.inf** en varias rutas relacionadas a una serie de usuarios. Este último se ha bloqueado satisfactoriamente.

ENS: Las 10 principales amenazas detectadas mes de Septiembre - 2022

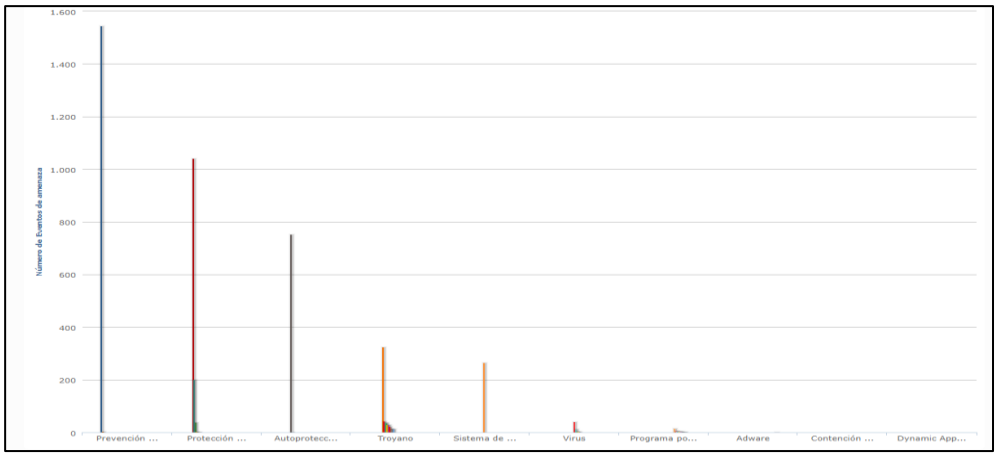
Nombre de amenaza	Número de Eventos de amenaza
Suspicious Double File Extension Execution	1.545
autorun.inf	1.041
Core Protection - Sanitize McAfee processes	752
ATP/Suspect!f1efb0fddc15	325
ExP:NIPS Violation	265
Prueba malware	201
ATP/Suspect!50ef7c645fd5	44
W32/Gnamer	42
Artemis!040CD888E971	40
Rule 10	38
Total	**4.293**

Por otro lado, la tercera amenaza para este mes se relaciona con **Core Protection - Sanitize McAfee processes**, para esta ocasión con la ejecución del aplicativo **Bonjour** en varios equipos. El equipo más recurrente fue el **PP6170ADM** al cual se le realizó escalamiento a **linea3000**.

ENS: 10 principales amenazas por categoría de amenaza septiembre 2022.

Amenazas por categoría

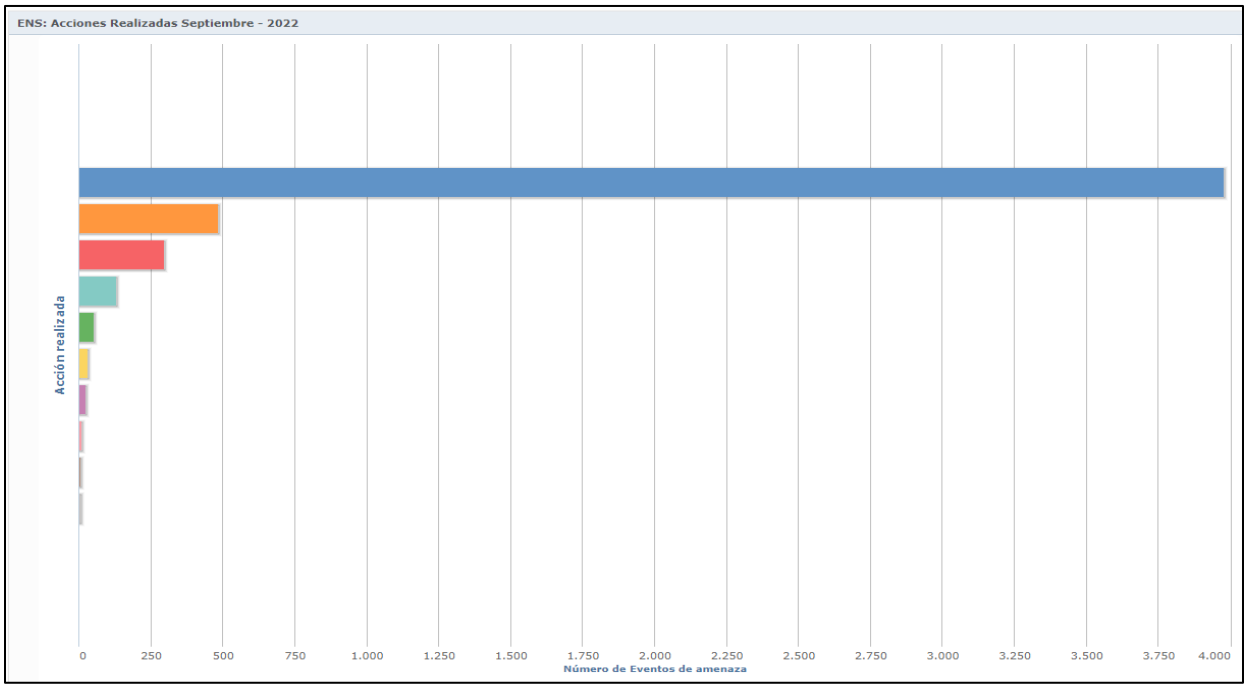
En el siguiente gráfico se muestra la cantidad de amenazas por categoría detectadas durante el mes de septiembre, donde se puede observar que la categoría **Prevención de exploits** representa un **34.4 %** de las amenazas detectadas en la organización. Mientras que la categoría **Protección de acceso** representa un **28.5 %** de las amenazas detectadas en el mes.



Tipo de amenaza->Nombre de amenaza	Número de Eventos de amenaza
Prevención de exploits	**1.549**
Suspicious Double File Extension Execution	1.545
Malware Behavior: Windows EFS abuse	4
Protección de acceso	**1.290**
autorun.inf	1.041
Prueba malware	201
Rule 10	38
SkypeSetup.exe	4
Rule 9	3
Remotely creating autorun files	2
1.bat	1
Autoprotección	**755**
Core Protection - Sanitize McAfee processes	752
Autoprotección: Protección de los procesos de McAfee	3
Troyano	**573**
ATP/Suspect!f1efb0fddc15	325
ATP/Suspect!50ef7c645fd5	44
Artemis!040CD888E971	40
ATP/Suspect!8d7c2fd35436	37
ATP/Suspect!cb377e2ba78e	30
Generic Trojan.ep	30
LNK/Trojan-FQBL!D25E15DABE24	23
JTI/Suspect.393221	16
ATP/Suspect!d05defe2c8ef	14
JS/Bondat.a!lnk	14
Sistema de prevención de intrusiones en la red	**265**
ExP:NIPS Violation	265
Virus	**72**
W32/Gnamer	42
W32/Autorun-FSV!4E964814FB35	13
VBS/Autorun.worm.aajk	5
W32/Rontokbro.a.gen@MM	5
Artemis!14638217EF40	3
VBS/Autorun.worm.aait	1
W32/Autorun.worm.aajv	1
W32/IRCBot.gen.b!lnk	1
W32/Ramnit.a!htm.e	1
Programa potencialmente no deseado	**51**
Crack-KMS	15
FilePatcher	7
Artemis!DDFA6D83D395	5
Artemis!E1F132D2FF44	4
HackTool-AutoKMS	4
PUP-XME-GQ	4
Artemis!881406640426	3
HackTool-AutoKMS.b	3
HTool-PassView	3
PUP-XCX-TF	3
Adware	**2**
Adware-SaveNow.v	2
Contención de aplicación dinámica	**2**
DAC:Contained	1
DAC:Released	1
Dynamic Application Containment	**1**
JTI/Trusted.196612!32ed3bed1adc	1
Total	**4.560**

Acciones realizadas

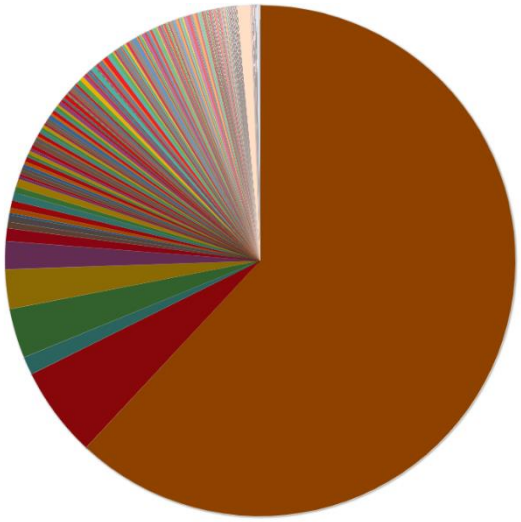
En el siguiente gráfico se muestra las acciones realizadas por el antivirus McAfee frente a las amenazas detectadas durante el mes de julio, el **2.6 %** de estas amenazas fueron eliminadas y el **79.2 %** corresponde a unidades que serían bloqueadas durante el análisis.



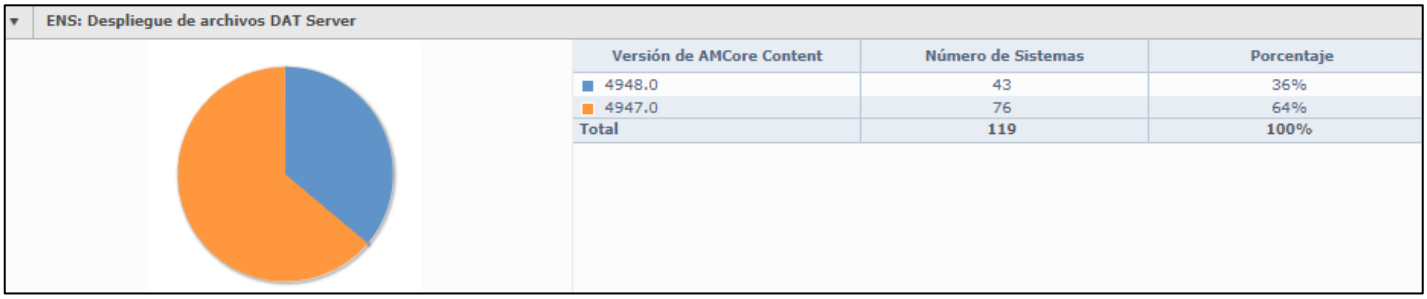
Acción realizada	Número de Eventos de amenaza
Bloqueado	3.979
Protección adaptable frente a amenazas bloquearía	486
Eliminación pendiente	296
Eliminar	132
Protección adaptable frente a amenazas limpiaría	52
Advertido	31
Permitir	24
Continuar con el análisis	10
Protección adaptable frente a amenazas contendría	6
Not Applicable	6
Total	**5.022**

INFORMACION DE ACTUALIZACIONES

ENS: Top 10 de las actualizaciones DAT



Versión de AMCore Content	Número de Sistemas	Porcentaje
4948.0	1.734	62%
4947.0	158	6%
4946.0	32	1%
4945.0	88	3%
4944.0	70	3%
4943.0	49	2%
4942.0	23	1%
4941.0	11	0%
4940.0	12	0%
4939.0	4	0%
4938.0	9	0%
4937.0	13	0%
4936.0	14	1%
4935.0	11	0%
4934.0	14	1%
4933.0	5	0%
4932.0	4	0%
4931.0	7	0%
4930.0	6	0%
4929.0	5	0%
4928.0	6	0%
4927.0	8	0%
4926.0	2	0%
4925.0	4	0%
4924.0	6	0%
4923.0	5	0%
4922.0	6	0%
4921.0	9	0%
4920.0	5	0%
4918.0	1	0%
4917.0	3	0%
4916.0	6	0%
4915.0	6	0%
4914.0	5	0%
4913.0	5	0%
4912.0	2	0%
4911.0	2	0%
4910.0	5	0%
4909.0	5	0%
4908.0	7	0%
4907.0	4	0%
4906.0	6	0%
4903.0	4	0%
4902.0	5	0%
4901.0	4	0%
4900.0	7	0%
4899.0	4	0%
4898.0	1	0%
4897.0	1	0%
4896.0	2	0%
4895.0	1	0%
4894.0	6	0%
4892.0	1	0%
4891.0	1	0%
4890.0	1	0%
4889.0	3	0%
4888.0	2	0%
4887.0	7	0%
4886.0	4	0%
4885.0	3	0%
4884.0	1	0%
4883.0	3	0%
4882.0	1	0%
4881.0	8	0%
4880.0	8	0%
4879.0	5	0%
4754.0	4	0%
4753.0	1	0%
4752.0	1	0%
4748.0	1	0%
4745.0	1	0%
4742.0	3	0%
4741.0	3	0%
4739.0	2	0%
4734.0	1	0%
4733.0	3	0%
4732.0	1	0%
4731.0	2	0%
4730.0	1	0%
4726.0	1	0%
4723.0	2	0%
4713.0	1	0%
4712.0	1	0%
4710.0	1	0%
4709.0	1	0%
4707.0	1	0%
4706.0	1	0%
4702.0	1	0%
4698.0	1	0%
4697.0	1	0%
4696.0	1	0%
4695.0	1	0%
4692.0	1	0%
4691.0	1	0%
4686.0	1	0%
4683.0	24	1%
4682.0	2	0%
4680.0	1	0%
4678.0	1	0%
4674.0	1	0%
4670.0	2	0%
4668.0	1	0%
4666.0	1	0%
4660.0	1	0%
0.5	5	0%
	2	0%
Total	2.796	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 septiembre, igualmente se evidencia que el **68 %** de los equipos están actualizados con las últimas dos firmas.

Observaciones:

- En la **ePO On-premise** aún quedan equipos que no fue posible migrarlos a consola MVISION debido a que no tenían comunicación reciente o tienen algún inconveniente con los productos, se ha enviado listado semanalmente a las coordinadoras de L3000 para que visualicen la cantidad de equipos que quedan en la consola antigua y realicen plan de acción para subirlos a la nube. A la fecha se ha estado realizando un proceso constante para migrar automáticamente a la consola **ePO MVISION** los equipos que aparezcan progresivamente. Es de aclarar que no todos los equipos suben y es necesario intervenirlos en sitio o de manera remota con autorización del usuario final.

- Por correo electrónico y teams se ha dado respuesta a los técnicos en sitio, indicándoles si los equipos han reportado correctamente en consola **ePO MVISION** o si por el contrario falta por actualizar alguno de los módulos de ENS, firma o agente. No obstante, se ha venido presentando un decremento en las notificaciones para revisión de equipos por correo electrónico este mes.

- Se retoma la generación de un reporte semanal del antivirus, desde este reporte se pueden evidenciar los casos que semanalmente se atienden por parte del administrador, como son las solicitudes de los técnicos de L3000 para validar el estado del antivirus en los Endpoint, el número total de equipos que no responden hasta el mes de Julio en consola **ePO MVISION** y el total de equipos en consola **ePO On-Premise**.

- Se han estado configurando una serie de tareas cliente con el fin de poder desinstalar en 27 equipos el módulo FW. Estos despliegues están configurados para actualizar el versionamiento del módulo y luego proceder a desinstalarlo apenas se efectúe una comunicación con el agente.

- Se encuentran este mes equipos con hostname duplicado en la consola **ePO MVISION**. Se proceden a eliminar con el fin de tener un conteo y monitoreo de equipos verídicos.

Elaborado por:



Jorge Enrique Torres Beltran

Firmado digitalmente por Jorge Enrique Torres Beltran
Nombre de reconocimiento (DN): cn=Jorge Enrique Torres Beltran, o, ou, email=jorge.torres@Aerocivil.gov.co, c=<n
Fecha: 2022.10.18 15:04:23 -05'00'

Christian Ricardo Almanza Castañeda
Administrador consola ePO

VoBo Jorge Enrique Torres Beltran
Supervisor Contrato 22001274 H3