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 ENERO 2023. 4
TRELLIX ENDPOINT SECURITY 4
VERSIONES DE PRODUCTOS TRELLIX DEL MES DE ENERO 6
Trellix Agent. 6
Endpoint Security Platform 7
Endpoint Security Threat Prevention 7
Endpoint Security Adaptive Threat Prevention 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 enero. 9
Top 10 de las principales amenazas detectadas durante el mes de enero. 11
ENS: 10 principales amenazas por categoría de amenaza enero 2023 11
Amenazas por categoría 11
Acciones realizadas 13
INFORMACION DE ACTUALIZACIONES 14
ENS: Top 10 de las actualizaciones DAT 14
Observaciones: 15

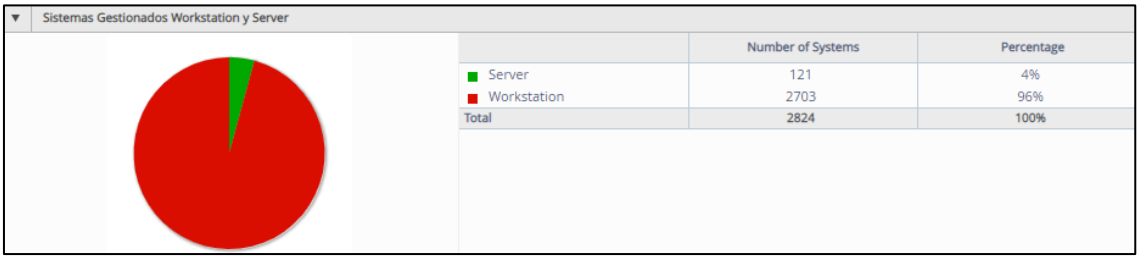
INTRODUCCIÓN

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 enero y parte del mes de febrero de 2023.

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 enero de 2023.

ITEM	Diciembre – 2022		Enero – 2023	
	No Sistemas Gestionados	Porcentaje	No Sistemas Gestionados	Porcentaje
Workstation	2667	96%	2703	96%
Servidores	121	4%	121	4%
Total	2788	100%	2824	100%



En el mes de enero y parte del mes de febrero se continuó con la 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 **48**, **49** y **50**. Es de aclarar, que aún siguen apareciendo nuevos equipos en consola local. A la fecha queda un reporte de **6 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.

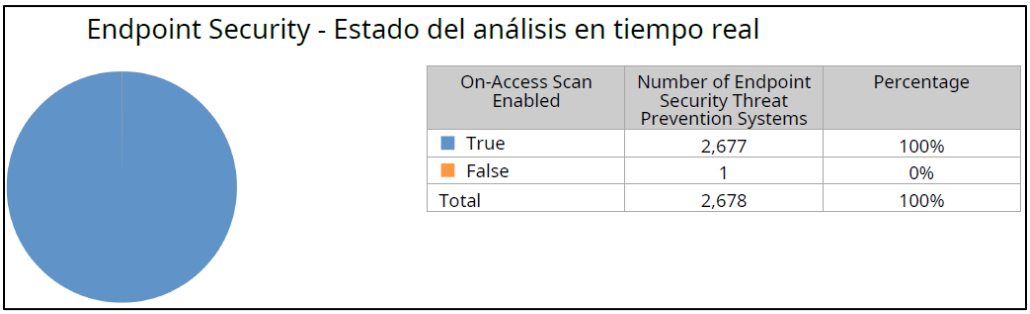
ESTADO ACTUAL PROTECCIÓN ANTIVIRUS ENERO 2023.

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.

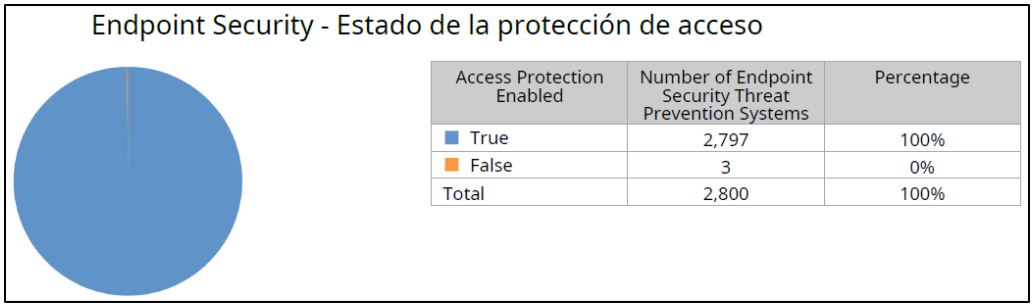
Este análisis es correspondiente al módulo de **Adaptive Threat Prevention** como detección temprana de amenazas que se puedan catalogar como amenaza en el sistema.



On-Access Scan Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,677	100%
False	1	0%
Total	2,678	100%

Estado de la Protección de Acceso.

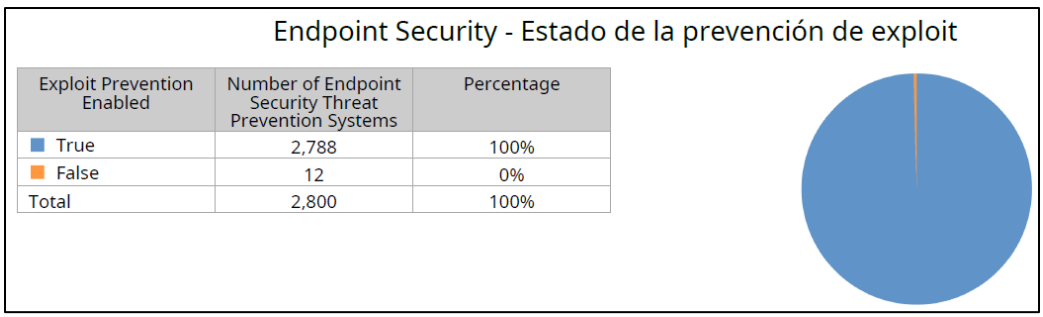
Estos eventos corresponden al módulo de **Threat Prevention** en el momento de ejecución de aplicaciones que no están permitidas.



Access Protection Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,797	100%
False	3	0%
Total	2,800	100%

Estado de la Prevención de Exploit.

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

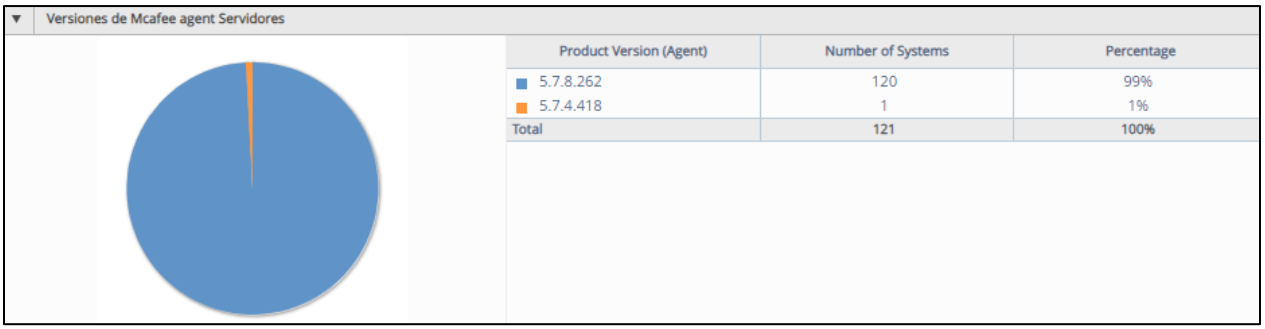


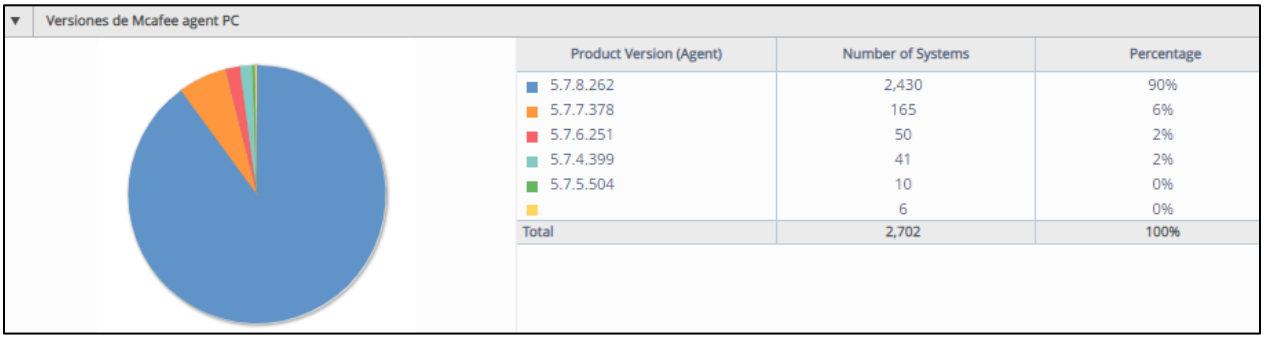
Exploit Prevention Enabled	Number of Endpoint Security Threat Prevention Systems	Percentage
True	2,788	100%
False	12	0%
Total	2,800	100%

VERSIONES DE PRODUCTOS TRELLIX DEL MES DE ENERO

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.

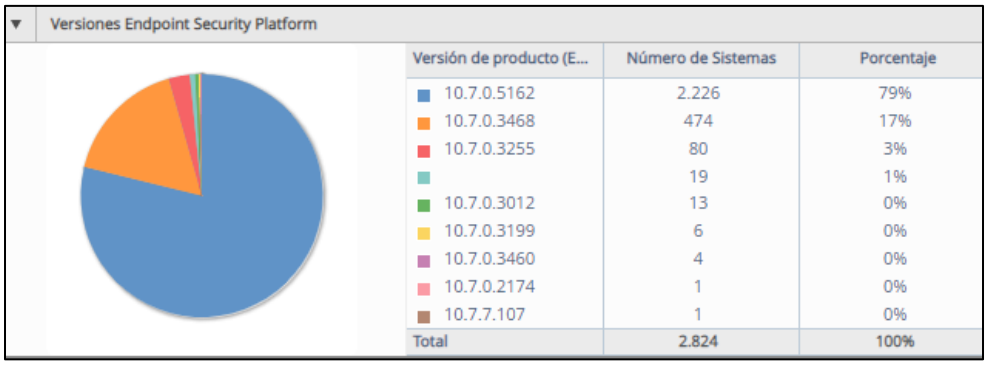




Actualmente se sigue en una tarea constante para actualizar en su totalidad y a la última versión los equipos de la AC. Es de aclarar que los nuevos equipos que sean instalados a través de la **URL** van a subir con la versión **5.7.8.262.** Esta versión incluye una mejora y resuelve varios problemas, 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 **96 %** 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.

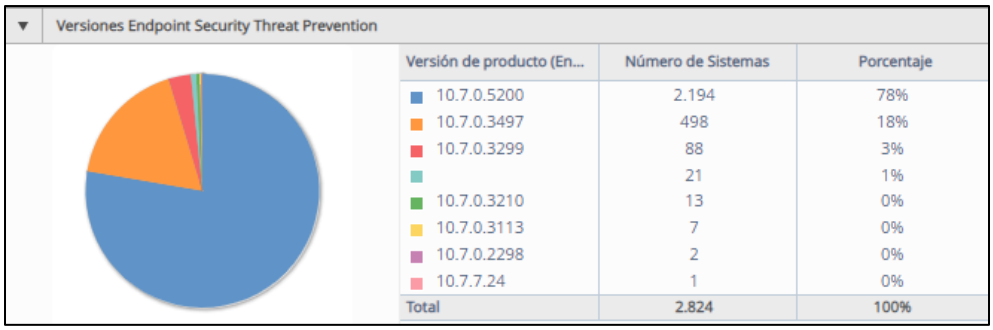


Versiones Endpoint Security Platform

Versión de producto (E...	Número de Sistemas	Porcentaje
10.7.0.5162	2.226	79%
10.7.0.3468	474	17%
10.7.0.3255	80	3%
	19	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	2.824	100%

Endpoint Security Threat Prevention

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

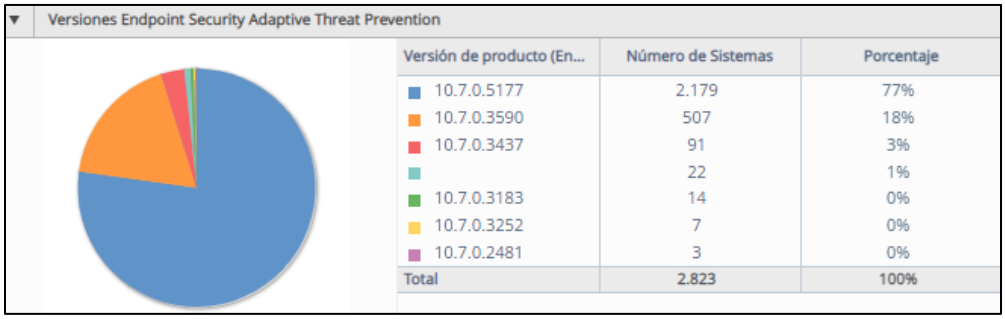


Versiones Endpoint Security Threat Prevention

Versión de producto (En...	Número de Sistemas	Porcentaje
10.7.0.5200	2.194	78%
10.7.0.3497	498	18%
10.7.0.3299	88	3%
	21	1%
10.7.0.3210	13	0%
10.7.0.3113	7	0%
10.7.0.2298	2	0%
10.7.7.24	1	0%
Total	2.824	100%

Endpoint Security Adaptive Threat Prevention

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

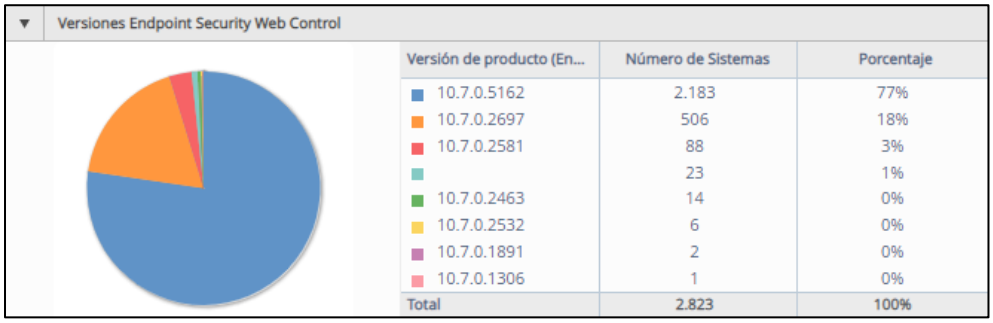


Versiones Endpoint Security Adaptive Threat Prevention

Versión de producto (En...	Número de Sistemas	Porcentaje
10.7.0.5177	2.179	77%
10.7.0.3590	507	18%
10.7.0.3437	91	3%
	22	1%
10.7.0.3183	14	0%
10.7.0.3252	7	0%
10.7.0.2481	3	0%
Total	2.823	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 (En...	Número de Sistemas	Porcentaje
10.7.0.5162	2.183	77%
10.7.0.2697	506	18%
10.7.0.2581	88	3%
	23	1%
10.7.0.2463	14	0%
10.7.0.2532	6	0%
10.7.0.1891	2	0%
10.7.0.1306	1	0%
Total	2.823	100%

Se evidencia que aproximadamente el **95,5 %** 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 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 McAfee	*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 **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 enero.

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 **1.996** amenazas.

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

Nombre de sistema	Número de Eventos de amenaza
BO0382SIN	640
BO7463ATS	512
BOG120	334
BO0167PLA	158
BO004INV	132
PE0823AIS	69
RG0930AIS	62
BO0113FIN	43
BQ0711ADM	26
LT8498ADM	20
Total	1.996

Se evidencia que las dos principales amenazas detectadas son de tipo **Autoprotección** y **Protección de acceso**, estas se presentan debido a que el equipo **BO0382SIN** ha estado intentando ejecutar el aplicativo **Bonjour**, la acción que el antivirus toma es un bloqueo al intento de ejecución. Para el caso del equipo **BO7463ATS** el requerimiento fue solucionado al aplicarse una exclusión desde la directiva **Protección de acceso**, desde la ruta **D:** y corroborarse que las funciones eran necesarias en las labores del usuario final. Por otro lado, el equipo **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.

Group Name	Number of Threat Events
CEA	995
Piso-4	912
Portatiles	472
Cali	471
CNA	468
Piso-1 y Sotano	382
Barranquilla	377
CGAC	369
Leticia	311
Piso-2	298
Medellin	235
Piso-3	157
Pereira	127
Cartagena	88
Villavicencio	78
Guaymaral	70
Cucuta	64
Yopal	61
Bucaramanga	58
Rionegro	53
Piso-5	50
Santa Marta	43
Arauca	42
Tame	34
ARANDA	26
Ibague	24
Popayan	24
Pto Asis	24
Barrancabermeja	19
Armenia	17
BOGOTA	16
San Andres	15
Quibdo	14
Pasto	12
Monteria	11
Valledupar	10
ALMACEN	8
Buenaventura	8
DORADO	7
DE ARCHIVOS	6
Mariquita	6
Neiva	6
Girardot	5
Otros Aeropuertos	5
Florencia	4
Ipiales	4
SERVIDOR MOODLE	3
Corozal	2
Guapi	2
Mitu	2
Carepa	1
Equipos Sta. Sofia	1
San Jose del Guaviare	1
Tolu	1
Total	6,499

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

En la siguiente tabla se evidencia el top 10 de las principales amenazas registradas durante el mes de enero, donde se evidencia que la mayoría de las amenazas presentadas (***Core Protection – Sanitize Trellix Processes y Prueba malware***) se dieron principalmente por el intento de ejecución del aplicativo **Bonjour** en el equipo **BO0382SIN**. De igual forma, para el segundo evento de amenaza detectado, se presentó el intento ejecución del archivo **USB.lnk** desde la partición **D:** del equipo **BO7463ATS**.

ENS: Las 10 principales amenazas detectadas mes de Enero - 2023

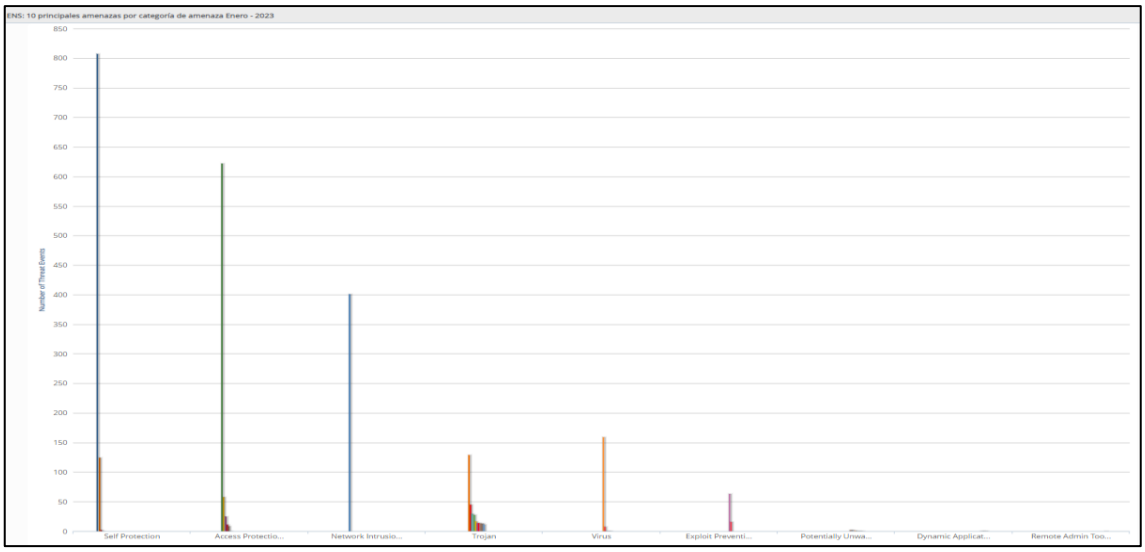
Threat Name	Number of Threat Events
Core Protection - Sanitize Trellix processes	808
Prueba malware	623
ExP:NIPS Violation	402
W32/Gnamer	160
ATP/Suspect!50ef7c645fd5	130
Core Protection - Protect core McAfee files and folders	125
Malware Behavior: Windows EFS abuse	64
autorun.inf	58
ATP/Suspect!8d7c2fd35436	46
JTI/Suspect.393221	30
Total	2,446

Por otro lado, la tercera amenaza para este mes se relaciona con ***ExP:NIPS Violation***, para esta ocasión con el intento de vulneración al servidor DNS externo secundario **BOG120.** Sobre este servidor se intentaron realizar varias vulneraciones de tipo intrusión de host que progresivamente se fueron bloqueando por el antivirus.

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

Amenazas por categoría

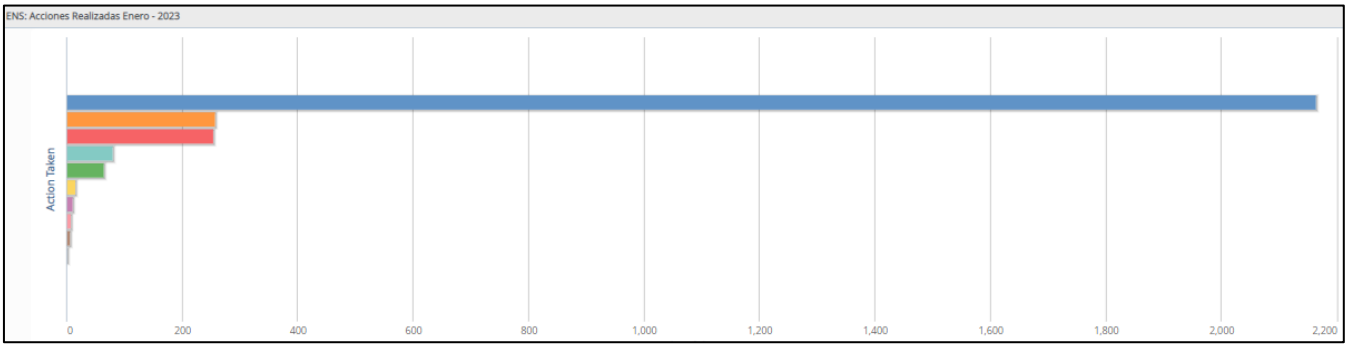
En el siguiente gráfico se muestra la cantidad de amenazas por categoría detectadas durante el mes de enero, donde se puede observar que la categoría **Autoprotección** representa un **36 %** de las amenazas detectadas en la organización. Mientras que la categoría **Protección de acceso** representa un **28 %** de las amenazas detectadas en el mes. Las dos categorías principales para este mes representan el **64 %** del total de amenazas detectadas en la entidad.



Tipo de amenaza->Nombre de amenaza	Número de eventos de amenazas
Protección personal	**937**
Core Protection - Desinfecte los procesos de Trellix	808
Core Protection: proteja los archivos y carpetas principales de McAfee	125
Core Protection - Desinfecte los procesos de McAfee	3
Autoprotección: proteger los procesos de Trellix	1
Protección de acceso	**729**
malware de prueba	623
autorun.inf	58
SkypeSetup.exe	26
regla 10	12
Prevenga el malware de Office	9
Regla 9	1
Sistema de prevención de intrusiones en la red	**402**
ExP:Violación de NIPS	402
troyano	**321**
ATP/Sospechoso!50ef7c645fd5	130
ATP/Sospechoso!8d7c2fd35436	46
JTI/Sospechoso.393221	30
ATP/Sospechoso!d05defe2c8ef	28
ATP/Sospechoso!f1efb0fddc15	17
ATP/Sospechoso!072d4d6ae385	15
ATP/¡Sospechoso!d356b8693192	15
ATP/Sospechoso! cb377e2ba78e	14
VBS/Downloader.abt	14
W32/Victy.gusano!ait	12
Virus	**171**
W32/Gnamer	160
W32/Autorun-FSV!4E964814FB35	8
VBS/Autorun.gusano.aadd!lnk	1
W32/Fujacks.o.remanentes	1
W32/Rontokbro.a.gen@MM	1
Prevención de exploits	**80**
Comportamiento de malware: abuso de Windows EFS	64
Ejecución sospechosa de extensión de archivo doble	dieciséis
Programa potencialmente no deseado	**14**
Artemisa!7BC2FF97F1B4	3
Crack-KMS	3
Artemisa!930E8B870F21	2
HTool-Keygen.c	2
Artemisa!57CC1BF06C15	1
Artemisa!F627AADB27D5	1
HackTool-AutoKMS.a	1
HTool-Crack	1
Contención dinámica de aplicaciones	**4**
ATP/Sospechoso!b3728ad271b3	1
DAC: Contenido	1
DAC: Lanzado	1
T1543.003 - Modificación de la ubicación del registro de Servicios	1
Herramienta de administración remota	**1**
RemAdm-RemoteAdmin.p	1
Total	2,659

Acciones realizadas

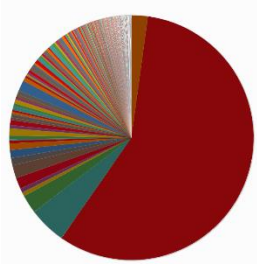
En el siguiente gráfico se muestran las acciones realizadas por el antivirus Trellix frente a las amenazas detectadas durante el mes de enero, el **9 %** de estas amenazas fueron **eliminadas** y el **85 %** corresponde a unidades que fueron bloqueadas durante el análisis diario que el antivirus realiza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



Action Taken	Number of Threat Events
Blocked	2,164
Delete	258
Adaptive Threat Protection Would Block	254
Adaptive Threat Protection Would Clean	80
Allow	64
None	15
Warned	11
Delete pending	8
Adaptive Threat Protection Would Contain	6
Continue scanning	2
Total	2,862

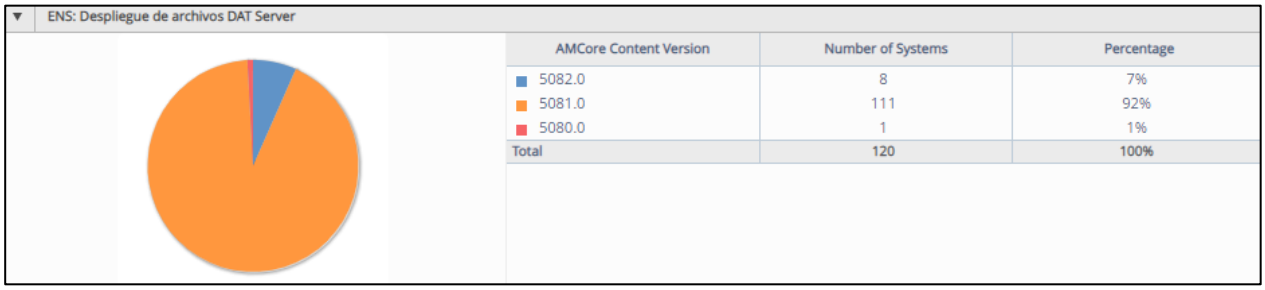
INFORMACION DE ACTUALIZACIONES

ENS: Top 10 de las actualizaciones DAT



AMCore Content Version	Number of Systems	Percentage
N/A	1	0%
5082.0	57	2%
5081.0	1,543	58%
5080.0	133	5%
5079.0	65	2%
5078.0	14	1%
5077.0	15	1%
5076.0	40	1%
5075.0	46	2%
5074.0	26	1%
5073.0	28	1%
5072.0	23	1%
5071.0	11	0%
5070.0	4	0%
5069.0	13	0%
5068.0	25	1%
4680.0	1	0%
4670.0	2	0%
4666.0	1	0%
4660.0	1	0%
0.5	2	0%
	3	0%
Total	2,682	100%

En los últimos **15 días** se han estado actualizando **2043** máquinas con una versión de firma .DAT igual o superior a la **5068**. Teniendo presente que la actualización se realiza de manera diaria. Cabe resaltar que se encuentran alrededor de **6 equipos** sin una versión de firma definida.



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 enero, igualmente se evidencia que para el caso de las Workstation el **76.2 %** de los equipos están actualizados con las **últimas 15 firmas**. 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 **5082**.

Observaciones:

- Aún quedan equipos pendientes por migrar de manera forzada desde consola **On-Premise**. Se ha registrado un incremento de estos equipos (**5**) 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 desde el **año 2022 hacia atrás**, se ha detectado que la comunicación de los equipos ha sido favorable para este año 2023 ya que hemos pasado de **410 a 285** equipos actualmente.

- Se culminó la eliminación de equipos a solicitud del ingeniero Jorge Torres, teniendo como referencia la poca información que nos estuvo brindando el contratista en su momento. Las observaciones que en la mayoría de los casos se dio fue que el equipo se encontraba en el estado **No operativo**.

- Se realizó la actualización del enlace para el ingreso de la consola **ePO MVISION** de acuerdo con el mantenimiento dado por fabricante. Dicho enlace se procedió a compartir con el ingeniero Jorge Torres para actualizar su ingreso a la plataforma.

- Se realizó a solicitud del ingeniero Jorge Torres un reporte de equipos listados conforme al orden del árbol de sistemas de la consola **ePO MVISION**. Se destacan de este listado el total de equipos, el número de equipos con la última versión instalada a nivel de agente y ENS y los equipos sin reportar desde el día 20 de enero.

- Se asiste a una primera reunión con el contratista comware para detallar la situación actual con el antivirus. Por parte de Carlos Pedroza se indica que se estuvo trabajando en la actualización de los equipos reportados el día 30 de diciembre, siendo este el último reporte que se tuvo en cuenta antes de la terminación del contrato. Se realizan las intervenciones a lugar para esclarecer el nuevo requerimiento solicitado por las directivas y el contratista.

- Se valida con ayuda del administrador de AD el estado actual del servidor **PPN**, el cual dejó de comunicar con la consola **ePO MVISION** desde el día 31 de enero. Según se informa, dicha ausencia en la comunicación se presentó por una falla eléctrica y esto generó el movimiento de equipos a otra zona.

- 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.

- A solicitud del ingeniero Nicolas Ortiz, se realiza la inscripción a boletines de ciberseguridad de las entidades Min TIC, CCIT y NIST. Lo anterior se realizó para estar atentos ante cualquier tipo de vulnerabilidad que se detecte a nivel nacional y poder tomar las medidas necesarias para estar protegidos.

Elaborado por:



Christian Ricardo Almanza Castañeda
Administrador consola ePO

VoBo Jorge Enrique Torres Beltran
Supervisor Contrato 22001274 H3