INFORME DE LA GESTIÓN DEL ANTIVIRUS

ESE – CARMEN EMILIA OSPINA – NEIVA

KAVANTIC S.A.S.

Manizales, Mayo de 2023

Carrera 24 N° 22-02 Of. 603 Edificio Plaza Cent
Tel. 6 8847890 Manizales – Colombia
informacion@kavantic.co

www.kavantic.co

Señores

ESE CARMEN EMILIA OSPINA – NEIVA

Nos permitimos enviar informe de gestión de la consola de antivirus ESET

El software de seguridad de Antivirus de ESET basa su protección a través de múltiples capas de protección de seguridad, las cuales trabajan de forma automática con el fin de detectar, bloquear, eliminar el malware y proteger a los usuarios de las ciberamenazas.

Kavantic SAS, cuenta con un excelente recurso humano, capacitado para dar solución a todas las inquietudes relacionadas con la seguridad de la información, y dar respuesta oportuna a los incidentes que se presenten en su entorno empresarial.

Esperamos que la información aquí consignada cumpla con todas sus expectativas.

Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co

CONTENIDO

Consola de Administración.....3
MÓDULO ANTIVIRUS
Detecciones.....4
Detecciones en los últimos 30 días.....5
Resumen diario de casos de detección en los últimos 30 días – Firewall.....6
Principales detecciones en los últimos 30 días – Antivirus.....6
MÓDULO FIREWALL
Detecciones en los últimos 30 días.....7
Resumen diario de casos de detección en los últimos 30 días – Firewall.....7
Principales detecciones en los últimos 30 días – Antivirus.....7
ESET LiveGrid®.....8
RECOMENDACIONES
Generales.....9
Listado de equipos por actualizar antivirus.....9

Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co

www.kavantic.co

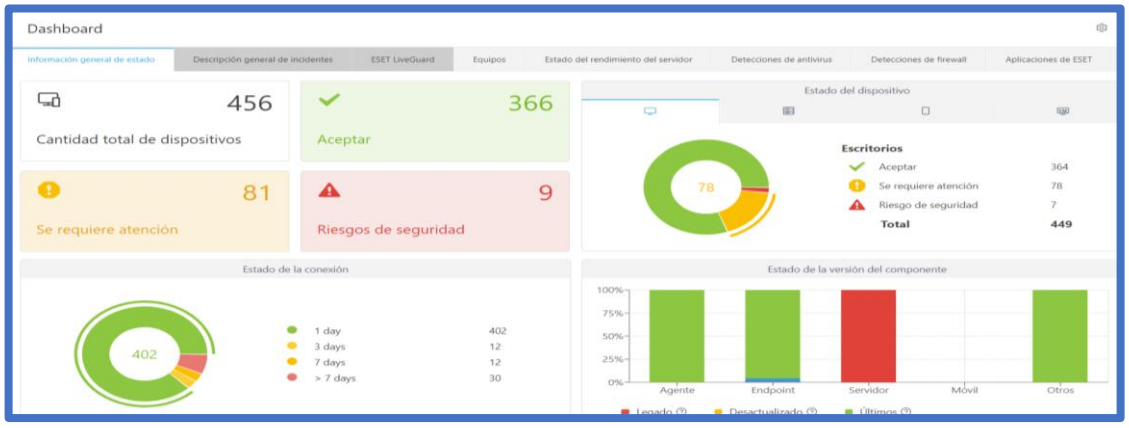
Consola de Administración

ESET PROTECT

Administra los productos de ESET en estaciones de trabajo, servidores y dispositivos móviles en un entorno de red desde una ubicación central, administrando tareas, políticas, con el fin de supervisar el estado del sistema y responder rápidamente a problemas o amenazas que se produzcan en computadores remotos.

Actualmente la ESE CARMEN EMILIA OSPINA, cuenta con el producto ESET PROTECT Advanced On-Premise, licenciado para 500 nodos, con fecha de vencimiento de licencia el 15/11/2023. El servidor dispuesto para administración de los equipos es ON - PREMISE, donde actualmente se encuentran administrados 456**/500** dispositivos.

DASH BOARD



El Dash Board, indique que:

- 366 equipos se encentran “sin problemas”.
- 81 equipos, pendientes de actualizaciones de Windows o reinicio.
- 9 equipos con riegos de seguridad, entre ellos dos servidores, a los cuales es urgente aplicarlos las actualizaciones del producto. Están en versión 7, y ya está liberada la versión 10.0.120. Haga clic aquí, para ver el listado.

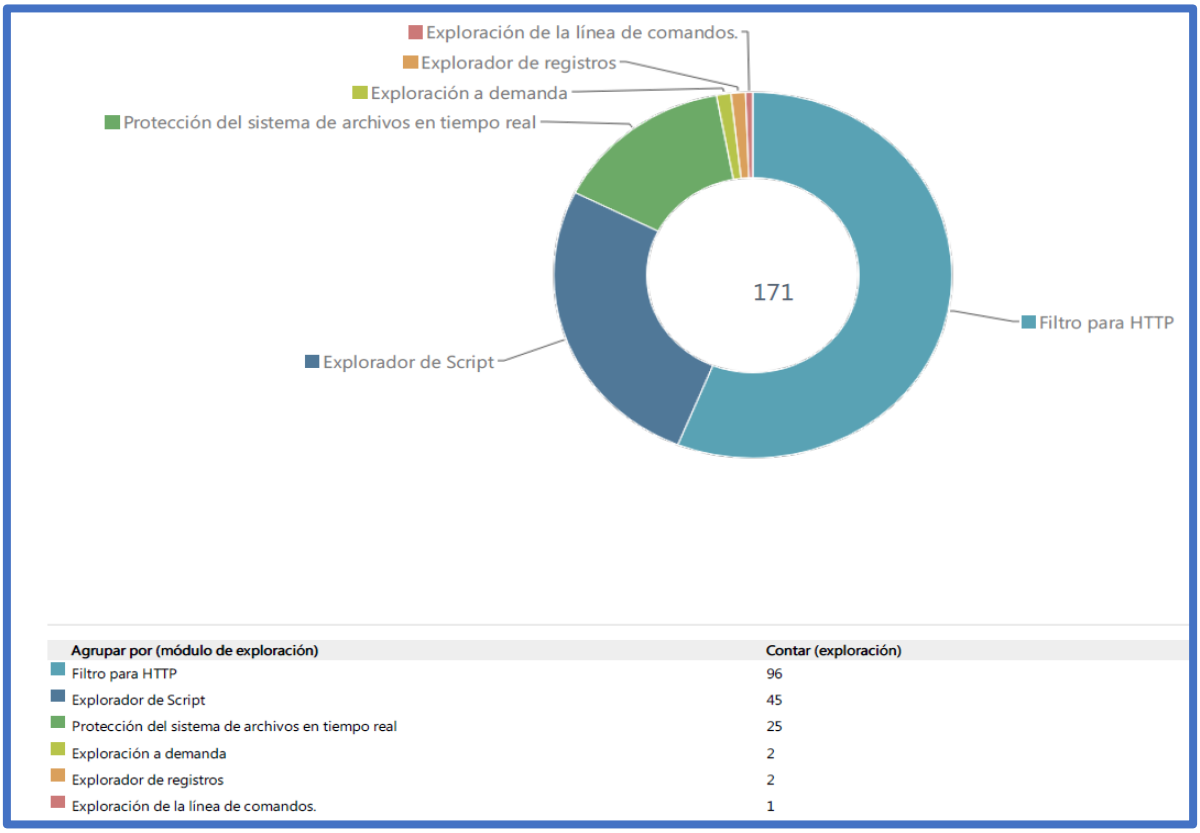
Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co
www.kavantic.co

MÓDULO ANTIVIRUS

Detecciones

Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.). ESET detecta una amplia gama de programas maliciosos existentes, así como software malicioso ubicado en archivos empaquetados.

Los sistemas de protección y detección en el módulo de exploración de ESET, neutralizó 171 detecciones. Se puede apreciar en el siguiente gráfico, que 96, y 45, de estas detecciones, se neutralizaron por el Filtro para HTTP, y el Explorador de Script, respectivamente.

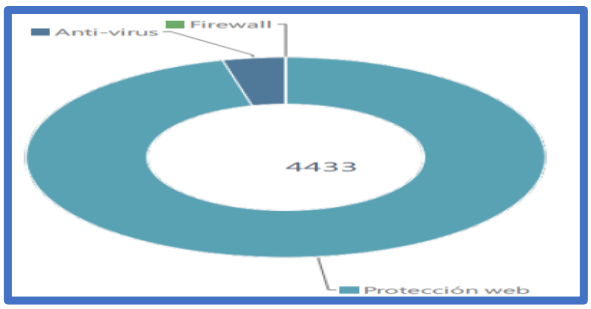


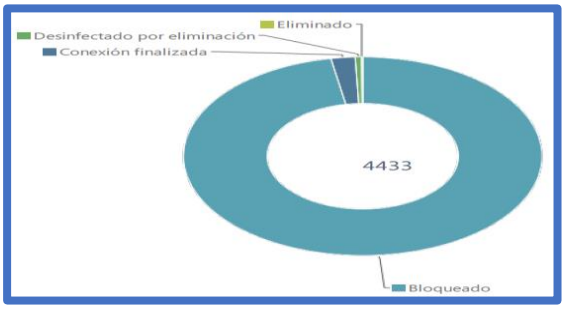
Agrupar por (módulo de exploración)	Contar (exploración)
Filtro para HTTP	96
Explorador de Script	45
Protección del sistema de archivos en tiempo real	25
Exploración a demanda	2
Explorador de registros	2
Exploración de la línea de comandos.	1

Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co

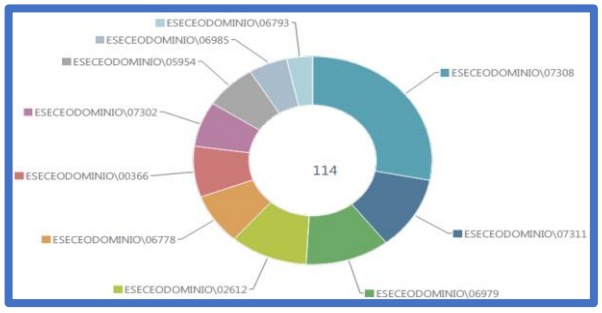
Detecciones en los últimos 30 días

En este periodo, puede observar detecciones de virus y archivos maliciosos, donde la solución de seguridad ESET EndPoint Security utilizó el nivel de desinfección balanceado para desinfectar, bloquear, mover a Cuarentena o finalizar la conexión de estas amenazas. Se exponen algunas detecciones a continuación.

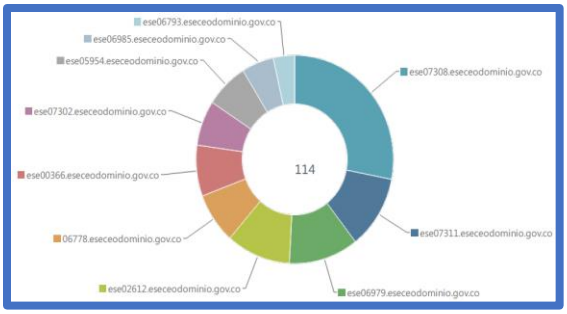




Principales usuarios con casos de detección



Principales equipos con casos de detección

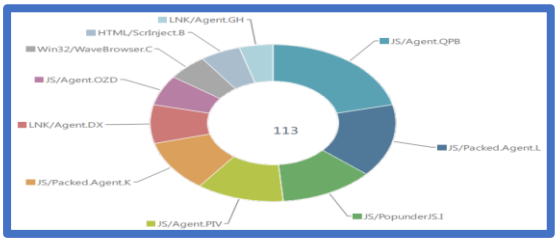


Se puede verificar que, el Sistema de Protección Web está realizando correctamente la detección y posterior bloqueo de amenazas, Para este período, fueron 4260/4433. Todas infecciones, fueron bloqueadas correctamente y de forma instantánea.

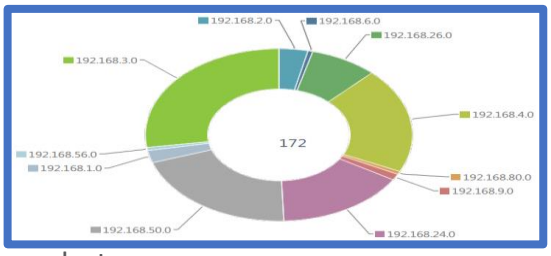
Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co

Principales detecciones en los últimos 30 días

Detecciones por nombre



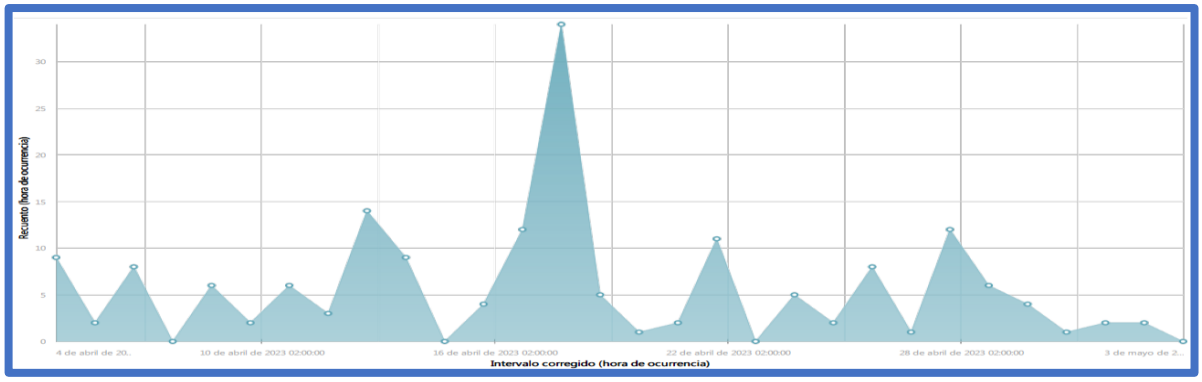
Detecciones por IPV4



Entre las infecciones detectadas y neutralizadas, se destacan:

- **S/PopunderJS.I:** PUA. Corresponde a una detección de una PUA, que está relacionado con la aplicación PopUnder. Si bien no se trata de algo necesariamente malicioso, es un complemento que puede resultar "molesto" para la experiencia del usuario
- **JS/Agent.PIV:** Troyano. Realiza actividades suelen incluir el establecimiento de conexiones de acceso remoto, la captura de entradas del teclado, la recopilación de información del sistema, la descarga/carga de archivos, la colocación de otro malware en el sistema infectado, la realización de ataques de denegación de servicio (DoS) y la ejecución/terminación de procesos.
- **HTML/ScrInject.B:** Troyano. Tiene la capacidad de gestionar conexiones de acceso remoto, realizar denegación de servicio (DoS) o DoS distribuido (DDoS), capturar entradas de teclado, eliminar archivos u objetos o finalizar procesos.

Resumen diario de casos de detección en los últimos 30 días



Analizado el gráfico, se puede apreciar que el 20 de abril de 2023, fue la fecha con más ocurrencias (40), seguido del 13 y 29 de abril, con 14 ocurrencias por día.

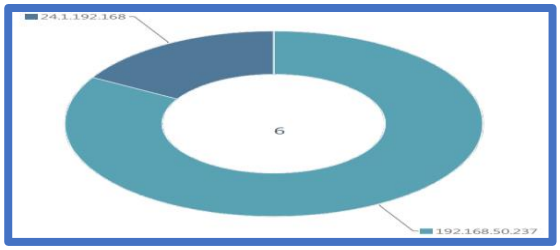
Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co
www.kavantic.co

MÓDULO FIREWALL

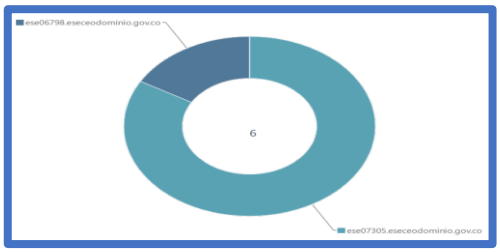
Principales Detecciones bloqueadas en los últimos 30 días

En este periodo, puede observar detecciones de Firewall donde la solución de seguridad ESET finalizó y bloqueó la conexión de estas amenazas. Se exponen algunas detecciones a continuación.

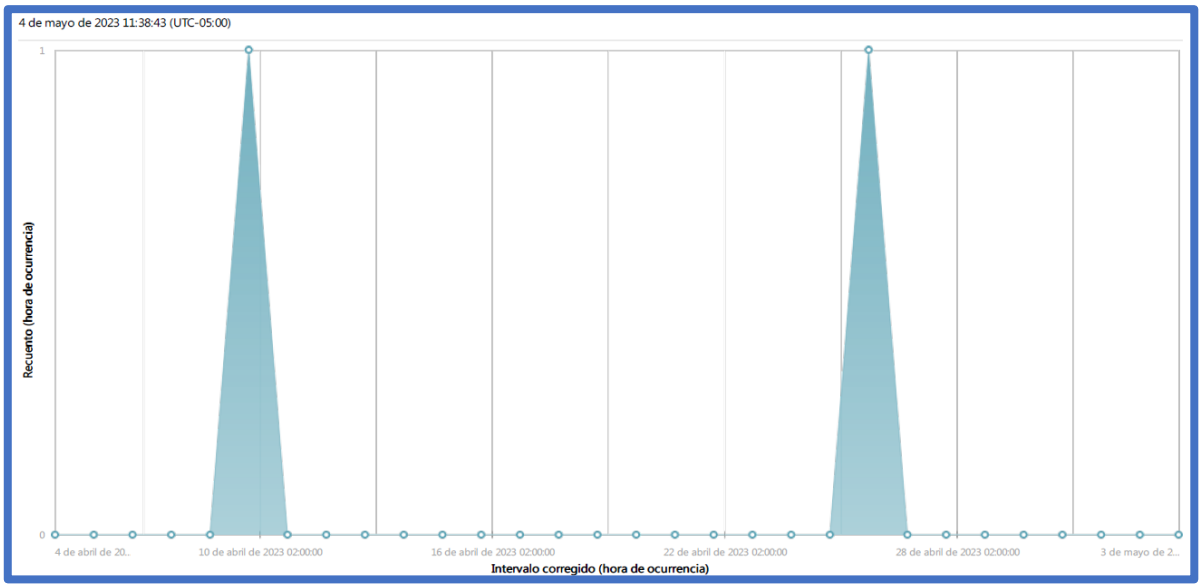
Principales destinos con casos de Firewall



Principales equipos con casos de Firewall



Resumen diario de casos de detección en los últimos 30 días



Analizado los gráficos, se puede apreciar ataques por “fuerza bruta” y “botnet” (2 eventos en el mes).

El sistema Firewall de ESET, bloqueó dichos intentos de conexión y ataques.

Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co

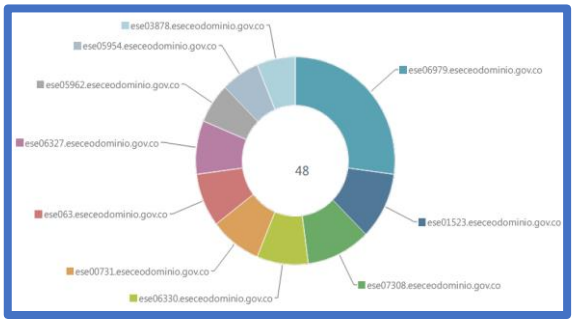
www.kavantic.co

ESET LiveGrid®

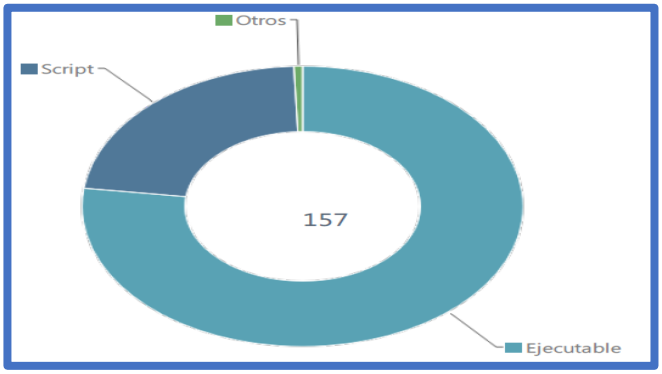
ESET LiveGrid® es un sistema de prevención que reúne información acerca de las amenazas detectadas en los equipos de los usuarios de ESET alrededor del mundo. La base de datos de ESET LiveGrid® contiene información de reputación acerca de amenazas potenciales. Cuando se encuentra activado, ESET LiveGrid® puede detectar y bloquear las amenazas introducidas más recientemente. Esto hace a ESET LiveGrid® una herramienta particularmente efectiva para defenderse ante las amenazas que emergen velozmente a diario, como nuevos tipos de ransomware (por ejemplo, Cryptolocker, Crypto wall, etc.).

Principales usuarios con más envíos

Principales equipos con más envíos



Archivos enviados a ESET LiveGuard y ESET LiveGrid®



Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co

RECOMENDACIONES

Generales:

Actualizaciones Windows: Efectuar la instalación de las respectivas actualizaciones automáticas del Sistema Operativo, con el fin de no generar huecos de seguridad.

Reinicio de equipos: Realizar el reinicio de computadores que han sido actualizado con las nuevas versiones de Antivirus, con el fin de completar la instalación del mismo.

Actualizaciones Antivirus para Servidores: Por seguridad, se debe realizar la instalación de forma manual del antivirus actualizado para los servidores, y realizar el reinicio de los mismos. De esta forma, se evitará ingreso de virus al estar actualizados tanto bases de datos como la herramienta de seguridad

Versión actual para servidores: **10.0.12010.0 (A partir de Windows Server 2012).**

Versión actual para Endpoint: **10.0.2045.0 (Windows 10 & 11),**

9.1.2063.0 (Windows 7, 8 & 8.1).

Nombre del equipo	Estado de los módulos	Direcciones IP	Nombre del sistema operativo	Producto de seguridad	Versión
ser-apli.eseceodominio.gov.co	No actualizado	192.168.1.25	Microsoft Windows Server 2016 Standard	ESET File Security	7.0.12016.0
ese00593.eseceodominio.gov.co	No actualizado	192.168.24.20	Microsoft Windows 10 Pro N	ESET Endpoint Security	10.0.2045.0
ese02428.eseceodominio.gov.co	No actualizado	192.168.30.17	Microsoft Windows 10 Pro	ESET Endpoint Security	10.0.2034.0
vfile.eseceodominio.gov.co	No actualizado	192.168.1.42	Microsoft Windows Server 2016 Standard	ESET File Security	7.0.12016.0
ese00333.eseceodominio.gov.co	No actualizado	192.168.24.59	Microsoft Windows 10 Pro N	ESET Endpoint Security	10.0.2034.0
ese03636.eseceodominio.gov.co	No actualizado	192.168.13.5	Microsoft Windows 10 Pro N	ESET Endpoint Security	10.0.2034.0
ese00116.eseceodominio.gov.co	No actualizado	192.168.50.134	Microsoft Windows 10 Pro	ESET Endpoint Security	10.0.2034.0
ese05491.eseceodominio.gov.co	No actualizado	192.168.12.16	Microsoft Windows 10 Pro	ESET Endpoint Security	10.0.2034.0
ese02514.eseceodominio.gov.co	No actualizado	192.168.30.18	Microsoft Windows 10 Pro	ESET Endpoint Security	10.0.2034.0

Carrera 24 N° 22-02 Of. 603
Ed. Plaza Centro, Manizales – Colombia
Tel. 6068847890 - Mail: informacion@kavantic.co
www.kavantic.co