Despliegue y configuración
Panda AntiRansomware 360
(Adaptive Defense 360) v3.20.00

ÍNDICE

1. OBJETIVO

1. El objeto de esta guía es detallar los procedimientos necesarios para desplegar el producto de seguridad Adaptive Defense 360 en su versión 3.20.00 y establecer las configuraciones básicas para conseguir una protección efectiva de los puestos de trabajo y servidores.

2. ALCANCE

2. Esta guía se dirige al Administrador de la seguridad del sistema encargado del despliegue de software en los Sistemas de Tecnologías de la Información y Comunicaciones de las Organizaciones, así como al personal encargado de establecer la configuración de seguridad de puestos de usuario y servidores.

3. DESPLIEGUE

3. El proceso de instalación de Adaptive Defense 360 3.20.00 comprende una serie de pasos, algunos opcionales, que dependen del estado de la red en el momento del despliegue y del número de equipos a proteger. Para desarrollar un despliegue con garantías de éxito es necesario elaborar una planificación que comprenda los puntos mostrados a continuación:

    a) Crea cuentas de administración en la consola web para el despliegue.

    b) Haz un inventario de los equipos desprotegidos.

    c) Comprueba que se cumplen los requisitos mínimos de la plataforma destino.

    d) Establece la ventana de servicio para el despliegue.

    e) Crea las configuraciones de red necesarias.

    f) Revisa el acceso a los recursos de Panda Security 360 en la nube.

    g) Revisa la configuración de seguridad por defecto.

    h) Determina el tipo de despliegue (remoto, local, herramientas de terceros o imagen).

    i) Ejecuta un despliegue escalonado.

    j) Completa el despliegue.

    k) Realiza las comprobaciones finales.

3.1. Crea cuentas de administración en la consola web para el despliegue

4. Dependiendo del número de Administradores de la seguridad del sistema en la Organización y de sus tareas asignadas, se recomienda limitar el acceso de los recursos de la consola web al mínimo imprescindible.

5. Todas las acciones que el Administrador ejecuta en la consola web quedan registradas. Para poder hacer un seguimiento de cada uno de los

Administradores asignados al despliegue y a la protección de la seguridad informática de la Organización se recomienda crear cuentas de administración independientes.

6. Para crear una cuenta de administrador con permisos para desplegar Adaptive Defense 360 sigue los pasos mostrados a continuación:

    a) Haz clic en el menú superior **Configuración**, menú lateral **Usuarios.**

    b) En la pestaña **Roles** haz clic en el botón **Añadir.**

    c) Introduce un **Nombre** y una **Descripción** indicando que se tratará de una cuenta temporal para el despliegue inicial.

    d) Selecciona el grupo **Todos** del árbol de grupos.

    e) Selecciona los permisos **Añadir, descubrir y eliminar equipos**, **Modificar configuración de red** (proxys y caché), **Reiniciar equipos**, **Asignar licencias**, **Configurar seguridad para estaciones y servidores**, **Configurar seguridad para dispositivos Android**, **Modificar ajustes por equipo** (actualizaciones, contraseñas, etc.) y desactiva el resto de permisos.

3.2. Haz un inventario de los equipos desprotegidos

7. Dependiendo del tipo de dispositivo a proteger y de si hay equipos ya instalados con Adaptive Defense 360, el inventario se puede efectuar de varias maneras:

    a) **Inventario manual o mediante herramientas de terceros**: se aplica para todos los dispositivos MacOS, Linux y Android y también para equipos Windows si no existe previamente ningún puesto de usuario o servidor con Adaptive Defense 360 instalado en el segmento de red.

    b) **Descubrimiento automático**: descubre puestos de usuario y servidores Windows que no tengan Adaptive Defense 360 3.20.00 instalado. Consulta el punto 3.3 para más información.

8. Una vez efectuado el inventario de dispositivos a proteger, comprueba el número de licencias libres contratadas en el menú superior **Estado**, menú lateral **Licencias**, barra **Sin asignar**. Si el número de equipos a proteger es mayor que el número de licencias sin asignar, ponte en contacto con tu comercial asignado para adquirir las licencias necesarias.

Figura 1: ventana de licencias

3.3. Descubre automáticamente los equipos sin proteger

9. Para descubrir los equipos Windows conectados a la red que no tienen Adaptive Defense 360 instalado se requiere:

    a) Como mínimo un equipo Windows con Adaptive Defense 360 instalado en cada segmento de red donde se quiera ejecutar un descubrimiento automático.

    b) Asignar al equipo Windows el rol de Descubridor.

    c) Cumplir con los requisitos de descubrimiento mostrados más adelante.

Asignación del rol descubridor

10. Para asignar el rol de descubridor a un equipo Windows de la red sigue los pasos siguientes:

    a) Haz clic en el menú superior **Configuración**, menú **lateral Configuración de red**, pestaña **Descubrimiento**, botón **Añadir equipo descubridor**.

    b) Selecciona de la lista el equipo a asignar el rol de descubridor. Se recomienda seleccionar equipos con recursos hardware suficientes y que estén en funcionamiento el mayor número de horas del día posibles.

Figura 2: añadir un equipo descubridor

Configuración del rol descubridor

11. A continuación, configura la tarea de descubrimiento que lanzará el equipo descubridor:

    a) Haz clic en el enlace **Configurar**.

    b) **Ejecutar automáticamente**: haz clic en el desplegable para establecer si la tarea de búsqueda se ejecutará de forma puntual (**No**) o programada (**Todos los días**). Si eliges **Todos los días**, selecciona en el desplegable la hora a la que se lanzará la tarea y la casilla de verificación **Hora local** del dispositivo, y si la hora se refiere a la configurada en el puesto de trabajo a desplegar o al servidor Adaptive Defense 360.

    c) **Buscar en toda la red**: busca todos los equipos que pertenecen al segmento de red donde reside el equipo descubridor.

    d) **Buscar solo en los siguientes rangos de direcciones IP**: limita el ámbito de búsqueda a los rangos de IPs introducidos. Establece un rango mediante dos direcciones IP separadas por un guion. Introduce varios rangos de IP separándolos con comas. La búsqueda queda restringida a la subred a la que pertenece el equipo descubridor.

    e) **Buscar solo equipos de los siguientes dominios**: selecciona aquellos equipos encontrados dentro de la subred a la que pertenece el equipo descubridor, y que estén integrados en los dominios Windows indicados.

Requisitos de descubrimiento

12. Para que un equipo pueda ser descubierto se tienen que cumplir los requisitos mostrados a continuación:

    a) Se descubrirán los equipos Windows, Linux y MacOS de la Organización que no tengan previamente instalado Adaptive Defense 360.

    b) El equipo con rol de descubridor tiene que ser siempre un equipo Windows.

    c) Un equipo descubridor solo pude descubrir equipos dentro de la subred o subredes a las que pertenece.

3.4. Comprueba que se cumplen los requisitos mínimos de la plataforma destino

13. Comprueba que se cumplen los requisitos hardware y de sistema operativo mínimos en los equipos a instalar Adaptive Defense 360.

Requisitos Windows

a) **Estaciones de trabajo**: Windows XP SP3 (solo 32 bits), Windows Vista, Windows 7, Windows 8 y Windows 10.

b) **Servidores**: Windows 2003 SP2, Windows 2008, Windows Small Business Server 2011 y superiores, Windows Server 2012 R2, Windows Server 2016, Windows Server Core 2008 y superiores.

c) **Servidores Exchange**: 2003 al 2016.

d) **Procesador**: Pentium 1 Ghz.

e) **Memoria RAM**: 1 Gbyte.

f) **Espacio para la instalación**: 650 Mbytes.

Requisitos Linux

a) **Sistemas operativos 64 bits**: Ubuntu 14.04 LTS y superiores, Fedora 23 y superiores.

b) **Kernel soportado**: hasta la versión 4.10 64 bits.

c) **Puertos**: se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

d) **Procesador**: Pentium 1 Ghz

e) **Memoria RAM**: 1.5 Gbytes

f) **Espacio para la instalación**: 100 Mbytes.

Requisitos MacOS

a) **Sistemas operativos**: macOS 10.10 Yosemite y superiores.

b) **Puertos**: se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

c) **Procesador**: Intel Core 2 Duo

d) **Memoria RAM**: 2 Gbyte

e) **Espacio para la instalación**: 400 Mbytes.

Requisitos Android

a) **Sistemas operativos**: Android 4.0 y superiores.

b) **Espacio para la instalación**: 10 Mbytes (dependiendo del modelo de dispositivo se requerirá espacio adicional).

14. Verifica que no existen incompatibilidades de software y hardware con Adaptive Defense 360. En caso de duda contacta con el Technical Account Manager asignado.

Compatibilidad con productos de seguridad de terceros fabricantes

15. Aunque Adaptive Defense 360 es compatible con productos antivirus de terceros, por defecto desinstala automáticamente la solución existente para no penalizar el rendimiento del equipo. Consulta la URL https://www.pandasecurity.com/spain/support/card?id=50021 para obtener un

listado con todos los productos que Adaptive Defense 360 desinstala de forma automática.

16. Para desplegar Adaptive Defense 360 y no desinstalar el antivirus existente consulta el punto 25 para crear una configuración de seguridad adicional y haz clic en **Desinstalar automáticamente protecciones de otros fabricantes** dentro de la sección **General**, **Desinstalar otros productos de seguridad de la configuración creada**.

3.5. Establece la ventana de servicio para el despliegue

17. Dependiendo del método de despliegue y del software de seguridad instalado previamente en los equipos, puede ser necesaria la programación de una ventana de servicio fuera de la jornada laboral. En condiciones normales la instalación de Adaptive Defense 360 no requiere el reinicio de la máquina, si bien se produce un corte en las comunicaciones de 4 segundos de duración aproximada, que puede afectar a los programas que no gestionan adecuadamente las conexiones de red ya establecidas.

18. En el caso de que el equipo tenga instalado otro producto de seguridad, tanto de Panda Security como de terceros, es posible que se requiera un reinicio para completar la instalación. Consulta la Tabla 1 para comprobar si será necesario un reinicio para completar la instalación de Adaptive Defense 360.

Producto anterior	Versión de Adaptive Defense 360	Básica
Ninguno	Trial o comercial	**NO**
Endpoint Protection Legacy, Endpoint Protection Plus Legacy, Adaptive Defense 360 Legacy, Adaptive Defense Legacy, Panda Fusion Legacy	Comercial	**PROBABLE** (solo si requiere actualización de la protección)
Antivirus de terceros	Trial	**NO** (por defecto los dos productos conviven)
Antivirus de terceros	Comercial	**POSIBLE** (puede requerir reinicio para completar la desinstalación del producto de terceros)
Sistemas Citrix	Trial o comercial	**POSIBLE** (en versiones anteriores)

Tabla 1: listado de productos y requisitos de reinicio para completar la instalación

3.6. Crea las configuraciones de proxy e idioma necesarias

19. Adaptive Defense 360 conecta con la nube de Panda Security para proteger los equipos de la Organización, para comunicar el estado de la protección, y para recibir las configuraciones del Administrador de la seguridad del sistema introducidas en la consola de administración. Por defecto, Adaptive Defense 360 utiliza la puerta de enlace configurada en cada equipo, pero si el puesto de usuario o servidor no tiene conexión directa a Internet, será necesario generar tantas Configuraciones de proxy e idioma en la consola de administración como salidas distintas a través de proxy se utilicen en la Organización.

3.6.1 Configuración de proxy e idioma para conexión directa

20. No es necesario crear una Configuración de proxy e idioma para los equipos con conexión directa a Internet. La Configuración por defecto permite el acceso de Adaptive Defense 360 sin intermediarios a Internet.

3.6.2 Configuración de proxy e idioma para proxy corporativo

21. Crea una configuración de proxy e idioma por cada proxy corporativo utilizado en la organización:

    a) Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma**, botón **Añadir**.

    b) Indica el **Nombre** y la **Descripción** de la configuración de red creada.

    c) Deja sin especificar **Destinatarios No se ha asignado a ningún equipo**.

    d) Haz clic en la sección **Proxy** en el selector **Proxy corporativo.**

    e) Introduce la **dirección IP**, **puerto** y la información de las **credenciales** necesarias.

    f) Haz clic en el botón **Guardar.**

3.6.3 Conexión a través de un equipo con Adaptive Defense 360 instalado (proxy Adaptive Defense 360)

22. Para asignar el rol de proxy a un equipo con Adaptive Defense 360 instalado:

    a) Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma**, botón **Añadir.**

    b) Haz clic en la sección **Proxy** en el selector **Proxy de Panda Security 360** y en el link **Seleccionar equipo**.

c) En la ventana **Seleccionar proxy** haz clic en el link **Añadir nuevo proxy**. Se mostrará un listado de equipos con Adaptive Defense 360 ya instalado. Selecciona el equipo que hará las veces de proxy.

Requisitos para equipos con rol de proxy

a) El rol de proxy Panda Adaptive Defense 360 solo se puede asignar a equipos con el sistema operativo Windows.

b) Se requiere un equipo con hardware suficiente para manejar todas las conexiones de sus equipos vecinos.

c) Se recomienda un equipo de tipo servidor ya que es recomendable que esté en funcionamiento las 24 horas del día.

d) Es necesario que el equipo que hace la función de proxy tenga conexión a Internet, bien directa, bien indirecta a través de un proxy corporativo.

23. Crea una **Configuración de proxy e idioma** por cada proxy Panda Adaptive Defense 360 designado:

a) Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma**, botón **Añadir.**

b) Indica el **Nombre** y la **Descripción** de la configuración de red creada.

c) Haz clic en la sección **Proxy**, selector **Proxy de Panda Security 360** y en el link **Seleccionar equipo.**

d) En la ventana **Seleccionar proxy** haz clic en el equipo que se utilizará como proxy.

e) Haz clic en el botón **Guardar**.

3.7. Revisa el acceso a los recursos de Panda Security en la nube

24. Para el correcto funcionamiento de Adaptive Defense 360 es necesario que las URL mostradas a continuación sean accesibles desde los equipos protegidos de la red.

URLs

a) - https://*.pandasecurity.com

b) - http://*.pandasecurity.com

c) - https://*.windows.net

d) - https://pandasecurity.logtrust.com

e) - http://*.pandasoftware.com Tráfico de entrada y salida (Antispam y filtrado URL)

f) - http://*.pand.ctmail.com

g) - http://download.ctmail.com

Puertos

a) - Port 80 (HTTP, websocket)

b) - Port 443 (HTTPS)

3.8. Revisa la configuración de seguridad por defecto

25. La configuración de seguridad por defecto asignada al grupo Todos del árbol de equipos aplica un nivel de protección medio – alto compatible con la mayor parte de los puestos de usuario de las Organizaciones. Aun así, es posible que pueda presentar dificultades en algunas configuraciones de red muy específicas o en servidores. Haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, **Configuración por defecto** para revisar la configuración. En el caso de que algún parámetro no sea adecuado para tu red sigue los pasos mostrados a continuación para generar una nueva configuración de seguridad y asignarla a los equipos desplegados.

    a) Haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, icono  de la **Configuración por defecto** para crear una copia de la configuración modificable.

    b) Indica el nombre de la configuración y haz clic en el link **Destinatarios No se ha asignado a ningún equipo**. Haz clic en el icono  de la sección **Grupos de equipos** y selecciona el grupo **Todos**.

    c) Haz clic en el link **Atrás** y despliega las distintas secciones de la configuración de seguridad para modificar las opciones oportunas. Cuando termines haz clic en el botón **Guardar**.

    d) Abre nuevamente la configuración creada y haz clic en destinatarios. Asigna el grupo **Todos**.

3.9. Despliega de forma escalonada

26. Para minimizar problemas que afecten a los usuarios de los puestos de trabajo, organiza un despliegue por fases:

    a) Divide el parque de equipos en varios grupos, dependiendo del total de puestos a instalar. Contacta con el TAM asignado para recoger sugerencias acerca de la mejor manera de agrupar los equipos en cada Organización.

    b) En el primer grupo selecciona aquellos equipos más representativos de cada gama de hardware o software utilizado en la Organización. Incluye en el cada grupo un único equipo por gama.

    c) Despliega Adaptive Defense 360 y deja transcurrir un periodo de tiempo de uno o varios días para ver si se produce alguna incidencia.

d) Una vez trascurrido el tiempo previsto repite los puntos b y c ampliando el número de equipos por grupo y minimizando el periodo de tiempo entre despliegue y despliegue.

3.10. Selecciona el tipo de despliegue (remoto, local, herramientas de terceros, imagen base)

27. Dependiendo del tipo de equipo a instalar y de las herramientas implantadas en la Organización, podrás desplegar Adaptive Defense 360 de forma local o remota.
28. Independientemente del tipo de despliegue elegido, sigue la guía general de cuatro pasos indicada a continuación:
    a) Selecciona del tipo de plataforma a desplegar (Windows, Linux, macOS, Linux o Android).
    b) Asocia al paquete de instalación a un grupo del Árbol de equipos. Para simplificar el despliegue inicial, todos los equipos se integrarán en el grupo Todos.
    c) Asocia al paquete de instalación una Configuración de proxy e idioma creada en el punto 3.6 en el caso de que los equipos de la red no tengan salida directa a Internet y requieran de un proxy corporativo o un equipo con Adaptive Defense 360 instalado.
    d) Si la infraestructura de red de la Organización requiere el uso de distintos proxys según la subred a la que pertenece el equipo a desplegar, será necesario crear varios paquetes de instalación con la Configuración de proxy e idioma apropiada.

3.10.1 Como instalar Adaptive Defense 360 de forma local

a) Este procedimiento es compatible con los equipos Windows, Linux, macOS y Android.
b) Este procedimiento se aplica a los equipos Windows cuando no es posible su descubrimiento por no cumplirse los requisitos del punto 12.
c) Haz clic en el menú superior **Equipos**, botón **Añadir equipos**
d) Selecciona el sistema operativo de la ventana emergente: Windows, macOS, Linux, Android.

Figura 3: ventana de selección de plataforma a instalar

e) **Para equipos Windows, Linux y macOS**

   a. Selecciona el grupo donde será ubicado el equipo (**Todos**) y la Configuración de proxy e idioma creada previamente.

   b. Si el equipo tiene salida directa a internet asigna **Configuración por defecto** para la opción **Selecciona el proxy e idioma para los equipos.**

   c. Si el equipo tiene salida a internet mediante proxy corporativo asigna la Configuración de proxy e idioma apropiada creada en el punto 3.6 para la opción **Selecciona el proxy e idioma para los equipos.**

   d. Si el equipo tiene salida a internet a través de otro equipo con Adaptive Defense 360 con el rol de proxy, asigna la Configuración de proxy e idioma apropiada creada en el punto 3.6 para la opción **Selecciona el proxy e idioma para los equipos.**

f) **Para dispositivos Android**

   a. Selecciona el grupo donde será ubicado el equipo (**Todos**) y escanea el código QR mostrado en la ventana emergente con la cámara del propio teléfono móvil o tablet.

   b. Los dispositivos Android no soportan la comunicación a través de proxy.

g) Haz clic en el botón **Descargar instalador** para obtener el paquete de instalación o **Enviar URL por mail** para abrir la aplicación de correo electrónico y componer un mensaje con la URL de descarga. Este mensaje deberá de ser enviado a los usuarios de los equipos a proteger.

3.10.2 Como instalar Adaptive Defense 360 de forma remota

29. Para instalar Adaptive Defense 360 de forma remota sin utilizar herramientas de distribución de software de terceros es necesario cumplir con los siguientes requisitos:

    a) Existe un equipo instalado y con el rol de descubridor asignado dentro de la misma subred donde se desplegará Adaptive Defense 360.

    b) El equipo descubridor efectuó un descubrimiento de los equipos en el segmento de red y permanece encendido y con conexión a la red durante todo el proceso de despliegue.

    c) Acceso administrativo al recurso Admin$ en la maquina a desplegar.

    d) Credenciales de administrador del dominio o del administrador local real y administración remota activada.

30. Para instalar Adaptive Defense 360 de forma remota sin utilizar herramientas de distribución de software de terceros sigue los pasos mostrados a continuación:

    a) Haz clic en el menú superior **Estado** y en la zona **Mis listados,** link **Añadir.**

    b) Selecciona el listado **Equipos administrados no descubiertos** y haz clic en el botón **Añadir**. Se mostrará una ventana con todos los equipos de la red que no tienen Adaptive Defense 360 instalado.

    c) Con las casillas de selección marca los equipos a instalar y haz clic en la barra superior **Instalar agente de Panda**.

    d) En la ventana emergente Selecciona el grupo donde será ubicado el equipo (**Todos**), y selecciona la Configuración de proxy e idioma creada en el punto 3.6.

    e) Haz clic en el botón **Instalar**. Transcurridos ## minutos la instalación se habrá completado.

3.10.3 Como instalar Adaptive Defense 360 de forma remota con herramientas de terceros

31. La consola Adaptive Defense 360 genera un paquete de instalación .msi compatible con las herramientas de despliegue centralizado, como por ejemplo Directorio Activo de Microsoft, Microsoft Systems Management Server (SMS), IBM Tivoli etc. Consulta el apartado 3.10.1 para generar y descargar el paquete de instalación Adaptive Defense 360.

3.10.4 Como instalar Adaptive Defense 360 mediante maquetas / imágenes “gold”

32. En redes de tamaño mediano o grande y compuestas por dispositivos homogéneos, se recomienda generar una “maqueta” o imagen “gold”, “master”

o imagen “plataforma” que contiene el sistema operativo ya actualizado junto a todos los programas necesarios para que el usuario pueda desempeñar sus tareas. Esta maqueta se volcará en todos los equipos de la red, acelerando el proceso de instalación.

33. La instalación del software Adaptive Defense 360 en cualquier equipo lleva asociada la asignación automática de un identificador único que es utilizado por Panda Security para referenciarlo en la consola de administración. Si se genera una imagen base con el software Adaptive Defense 360 ya instalado y se vuelca en otros equipos, todos los puestos que reciban esa imagen heredarán el mismo identificador, de forma que la consola mostrará un único equipo.

34. Para evitar esta situación es necesaria la utilización de un programa que borre el identificador generado al instalar el software en el equipo. Este programa se llama **reintegra.zip.** Consulta la url https://www.pandasecurity.com/usa-es/support/card?id=500201 en la web de soporte de Panda Security para descargar el software y obtener instrucciones precisas dependiendo del tipo de entorno virtual.

3.11. Consulta el resultado de la instalación

35. Para consultar el resultado de la instalación sigue los pasos mostrados a continuación:

    a) Haz clic en el menú superior **Estado.**

    b) El widget **Estado de la protección** mostrará los equipos instalados y los que tienen algún tipo de error. Si los equipos con el rol descubridor han detectado puestos sin proteger, éstos se mostrarán en la parte inferior del widget.

Figura 4: widget con el estado del despligue

4. Diseño del árbol de equipos

36. Una vez completado el despliegue inicial, todos los puestos de usuario y servidores estarán integrados en el grupo Todos. Para facilitar la asignación de configuraciones de seguridad es necesario organizar los puestos de trabajo y servidores en diferentes grupos. La herramienta implementada en Adaptive Defense 360 es el **Árbol de equipos**, accesible desde el menú superior **Equipos** haciendo clic en el icono .

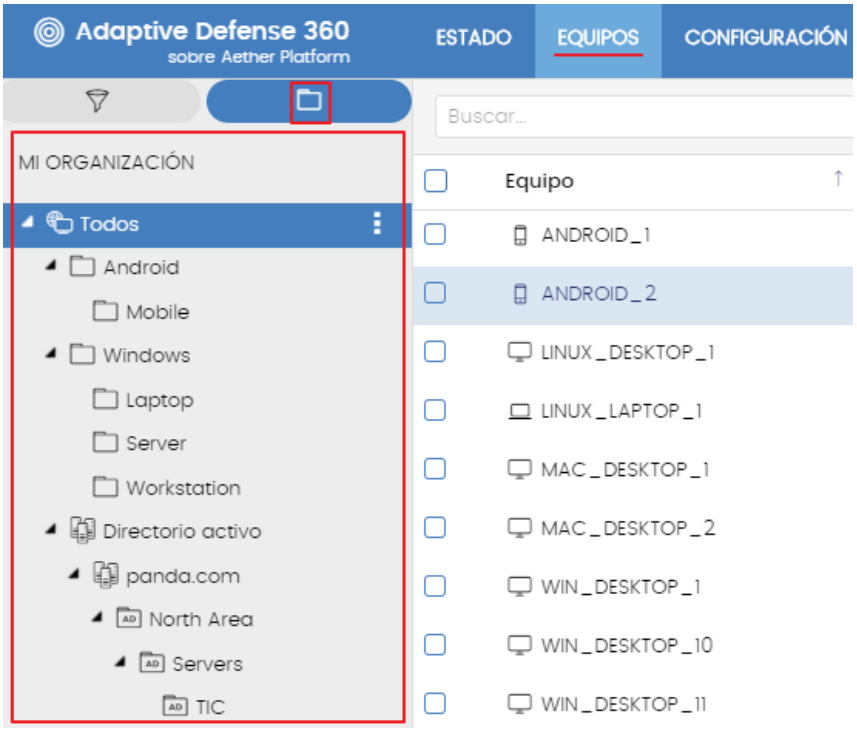

Figura 5: vista general del Árbol de equipos

4.1. Criterios de diseño para el árbol de equipos

37. Se distinguen cinco criterios de diseño para el Árbol de equipos. La elección de unos u otros depende de factores como el tamaño de la Organización, los objetivos de seguridad establecidos o la facilidad de gestión requerida. Estos criterios no son excluyentes y dentro de una Organización se pueden aplicar todos o ninguno de ellos:

    a) **Criterios de rango / responsabilidad**: crea grupos que coincidan con las necesidades de seguridad según el grado de responsabilidad de los usuarios en la Organización. Cada grupo estará compuesto por equipos manejados por usuarios con necesidades de protección similares. Por ejemplo “grupo directivos”o “grupo de programadores”. Este enfoque se recomienda para potenciar la protección de los equipos.

    b) **Criterios de topología de red**: crea grupos que coincidan con la estructura interna de la red de la Organización. Cada grupo estará compuesto por los puestos de usuario y servidores que pertenecen a una misma subred. Por ejemplo “grupo delegación Sevilla” o “grupo planta 3”. Este enfoque se recomienda para favorecer la gestión de las comunicaciones de Adaptive Defense 360 en caso de que cada subred requiera una configuración de comunicación particular con Internet.

    c) **Criterios organizativos**: crea grupos que coincidan con la estructura organizativa de la empresa. Cada grupo estará compuesto por los equipos que pertenecen a un mismo departamento. Por ejemplo “grupo Diseño”

o “grupo Contabilidad”. Se recomienda cuando cada departamento está formado por perfiles de trabajadores homogéneos con las mismas necesidades de seguridad.

d) **Criterios de función o rol del equipo**: crea grupos que contengan equipos que desempeñen funciones similares en la Organización. Por ejemplo “grupo servidores de correo” o “grupo servidores de impresión”.

e) **Criterios de Directorio Activo:** el administrador de Adaptive Defense 360 delega en el Directorio activo de la Organización la agrupación de los puestos de usuario y servidores.

f) **Sin criterio de diseño:** en redes de tamaño menor de 10 equipos es usual integrar los puestos de trabajo en el grupo raíz Todos del Árbol de equipos. De esta forma todos o la mayor parte de los equipos reciben el mismo tratamiento en cuanto a seguridad y conectividad con la red.

4.2. Grupos de directorio activo y grupos nativos

38. El Árbol de equipos se divide en dos secciones: la formada por los grupos nativos de Adaptive Defense 360 (1) y por los grupos de Directorio activo (2).

39. El objetivo de la sección de Directorio activo del Árbol de equipos es facilitar la gestión del Administrador de la seguridad del sistema, replicando la estructura ya configurada en el Directorio activo de la Organización dentro de la consola Adaptive Defense 360. De esta forma el administrador dispondrá de un entorno de gestión familiar desde el primer momento.

40. Al generar el paquete de instalación de Adaptive Defense 360, la consola de administración ofrece la posibilidad de integrar los puestos de trabajo en la zona del Árbol de equipos dedicada al directorio activo, eligiendo la opción **Añadir los equipos en su ruta de Active Directory**. La zona de Directorio activo en el Árbol de equipos se genera por sí misma conforme los puestos de usuario y servidores van recibiendo el paquete de instalación. Al finalizar el proceso de despliegue, la estructura de grupos y unidades organizativas existentes en la Organización quedará replicada en la consola de administración de Adaptive Defense 360, siempre y cuando haya al menos un puesto de trabajo o servidor instalado en cada grupo.

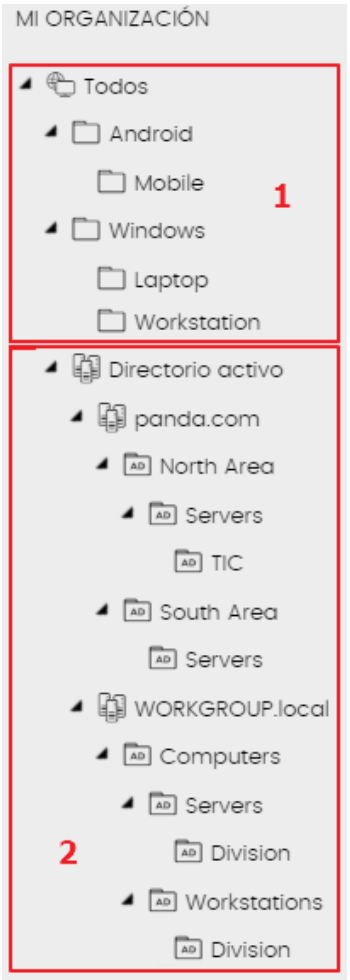

Figura 6: zona de grupos nativos (1) y grupos de Directorio Activo (2)

41. La gestión de los grupos de Directorio activo dentro del árbol de equipos se delega en el propio Directorio activo de la Organización: para mover un equipo de un grupo de Directorio activo a otro es necesario moverlo en el Directorio activo de la Organización. Al cabo de unos minutos la información se replicará en la consola de administración y el equipo aparecerá en el nuevo grupo.

4.3. Asignación de configuraciones de seguridad

42. De forma general, la seguridad de los puestos de usuario y servidores se establece asignando configuraciones de seguridad previamente creadas a los grupos del Árbol de equipos. Este enfoque facilita la gestión de la protección de los equipos, ya que todos los miembros de un mismo grupo son tratados de igual manera desde el punto de vista de la seguridad.

43. Si un equipo se aparta de los requisitos de seguridad establecidos para su grupo, mueve el equipo a otro grupo que tenga asociada una configuración adecuada. Si no existe ningún grupo que encaje con las necesidades del equipo, asígnale una configuración de seguridad individual.

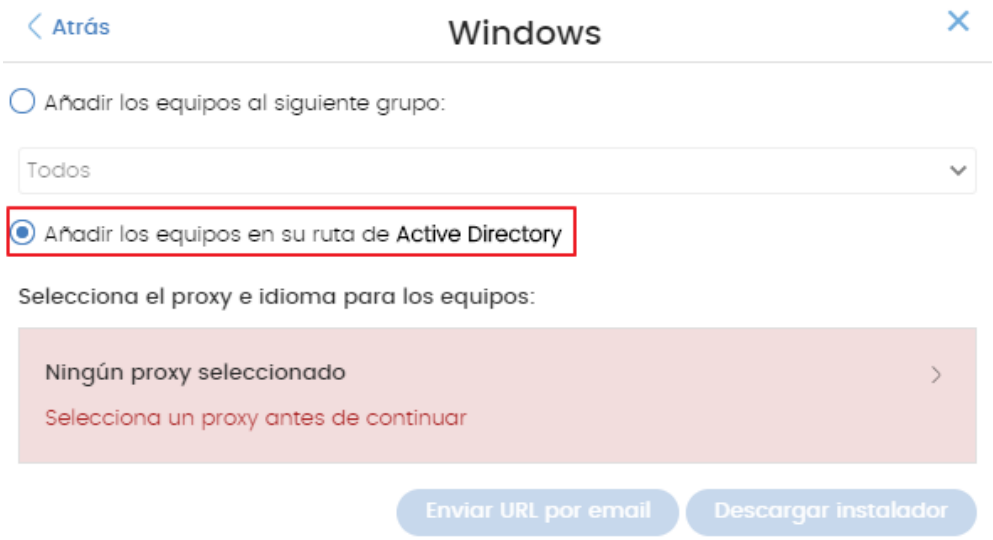

Figura 7: configuración del paquete de instalación para integrar los puestos de usuario y servidores en grupos de directorio activo dentro del árbol de equipos

4.4. Grupos de equipos y herencia de configuraciones

44. La configuración de seguridad asignada a un grupo de equipos es heredada por todos los grupos que cuelgan de él. Esta funcionalidad facilita la asignación de configuraciones si tener que especificarlas de forma individual por cada grupo.

45. La herencia de configuraciones se puede romper en cualquier nivel del Árbol de equipos reasignando de forma manual una configuración nueva a un grupo de nivel inferior dentro del Árbol de equipos. La configuración heredada quedará anulada por la nueva configuración asignada, y los subgrupos podrán heredar si así lo deseas esta nueva configuración.

5. Configuraciones de seguridad

46. El Responsable de Seguridad preparará diferentes configuraciones según las necesidades de los usuarios y de los requisitos marcados por la Política de Seguridad TIC de las Organizaciones. A continuación, se indican los parámetros clave de una configuración de seguridad y en qué casos están recomendados según la categoría de la Organización. Consulta la tabla consolidada del capítulo 10 con las recomendaciones para las tres categorías de sistemas definidos en el Anexo I del Real Decreto 3/2010 del 8 de enero.

5.1. Protección avanzada: Audit, Hardening, Lock

47. La protección avanzada clasifica todos los procesos que se ejecutan en los puestos de usuario y servidores como goodware o malware gracias a algoritmos de machine learning alojados en la nube de Panda Security. Por esta razón, es

capaz de detectar amenazas de tipo APT (Advanced Persistent Threaths) Managed attacks y amenazas desconocidas o especialmente complejas.

5.1.1 Configuración recomendada

48. A continuación, se muestra la configuración recomendada del módulo Protección avanzada para las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Sección Protección avanzada (Windows) – Comportamiento				
Protección avanzada	Habilita la protección avanzada.	Aplica	Aplica	Aplica
Modo Audit	Solo audita, no bloquea el malware avanzado.	Op.	Op.	Op.
Modo Hardening	Bloquea el malware conocido y los procesos desconocidos de fuentes no seguras.	Aplica	Aplica	Aplica
Modo Lock	Bloquea el malware y todos los procesos desconocidos.	N.A	Op.	Aplica

5.1.2 Acceso a la configuración de protección avanzada

49. Para visualizar o modificar la configuración de protección avanzada haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Protección avanzada (Windows)**.

50. Haz clic el botón **Protección avanzada** para activar la funcionalidad y selecciona del desplegable **Modo de funcionamiento** uno de los tres modos de protección (**Audit**, **Hardening** o **Lock)**.

5.1.3 Funcionamiento de la protección avanzada

51. La protección avanzada monitoriza todos los procesos y los clasifica en goodware o malware. Sin embargo, el administrador puede establecer la estrategia de bloqueo mediante el tipo de protección a implementar (Audit, Hardening, Lock):

    a) **Audit**: no ejecuta ninguna acción de bloqueo, independiente de la clasificación obtenida. Las clasificaciones se muestran en el panel de control de Adaptive Defense 360. Usa esta opción en el despliegue inicial si hay serias dudas de que Adaptive Defense 360 no clasifique correctamente los programas utilizados en la Organización, o si los

usuarios están usando programas de tipo PUP que serán bloqueados al ser considerados como malware.

b) **Hardening**: bloquea la ejecución del malware y de aquellos programas sin clasificar que vengan de fuentes no seguras, como Internet o dispositivos USB. El bloqueo de estos programas es temporal hasta que el sistema dicte una clasificación, momento en que se liberará el bloqueo si se trataba de goodware. Para minimizar las molestias al usuario, los programas sin clasificar por el sistema y que estaban almacenados en el puesto del usuario o servidor en el momento de la instalación de Adaptive Defense 360 no son bloqueados. Una vez terminada la clasificación, todos los programas catalogados como malware serán bloqueados. Se recomienda utilizar esta configuración para todos los equipos de la red que no tengan requisitos extraordinarios de seguridad.

c) **Lock**: bloquea la ejecución del malware y de todos los programas sin clasificar temporalmente hasta que el sistema dicte una clasificación con garantías, momento en que se liberará el bloqueo si se trata de goodware. Utiliza esta configuración en los equipos que requieren una máxima protección sin importar las molestias que ocasione al usuario. En esta configuración únicamente se permite la ejecución de los programas conocidos como goodware.

5.1.4 Preparación de la protección avanzada

52. Es posible que en el funcionamiento diario de un equipo protegido con Adaptive Defense 360 aparezca un pequeño porcentaje de programas desconocidos que tengan que ser clasificados. Dependiendo de la configuración avanzada, estos programas serán bloqueados hasta que los algoritmos de clasificación emitan un resultado (goodware o malware), con lo que los usuarios no podrán utilizar estos programas de forma temporal.

53. Si el departamento de IT controla la instalación de programas en los equipos de la red y quiere minimizar el impacto del software desconocido en el trabajo de los usuarios, pero a su vez no se quiere hacer concesiones a la seguridad permitiendo temporalmente la ejecución de programas sin clasificar, es recomendable preparar de antemano la ejecución del software nuevo antes de su instalación y uso masivo.

54. El procedimiento de preparación se puede dividir en cuatro pasos, mostrados a continuación.

a) **Configuración de un PC de pruebas**: el objetivo es determinar si el software a utilizar es ya conocido como goodware, malware o es desconocido para Adaptive Defense 360. Para ello utiliza el PC de un usuario de la red, o prepara un equipo dedicado a este objetivo. Asígnale inicialmente una configuración de seguridad avanzada Hardening.

b) **Instalación del software**: instala el software en el equipo de pruebas y ejecútalo de forma normal. Si Adaptive Defense 360 encuentra algún módulo o programa desconocido lo bloqueará mostrando una ventana emergente en el equipo. Además, se añadirá un nuevo elemento en el panel **Programas actualmente bloqueados en clasificación**. Internamente, Adaptive Defense 360 registrará los eventos generados por el uso del programa y enviará los binarios a la nube para poder estudiarlos. Si no se han presentado bloqueos en el modo Hardening, cambia la configuración a modo Lock y vuelve a ejecutar el programa recién instalado. En el caso de que aparezcan nuevos bloqueos el panel **Programas actualmente bloqueados en clasificación** los reflejará.

c) **Reclasificación de programas bloqueados**: en el momento en que Adaptive Defense 360 emita una clasificación de los programas bloqueados se enviará una notificación por correo al administrador. Se indicará si la clasificación es goodware, o su bloqueo definitivo por considerarse una amenaza. Cuando todos los procesos hayan sido reclasificados como goodware, el software instalado será apto para su ejecución en el parque informático.

d) **Envío del programa directamente a la nube de Panda Security**: Adaptive Defense 360 está configurado para no impactar en el rendimiento de la red en caso de tener que enviar ficheros a la nube de Panda Security. Si quieres acelerar su envío ponte el contacto con el departamento de soporte de Panda Security.

5.2. Protección avanzada: anti-exploit

55. Los puestos de usuario pueden contener procesos vulnerables: programas con fallos de diseño que, aunque siendo legítimos, no interpretan correctamente ciertas secuencias de datos que reciben del exterior. Al recibir estos patrones, se produce un mal funcionamiento interno del proceso, que deriva en una inyección de fragmentos de código en las regiones de memoria gestionadas por éste. Los programas así afectados reciben el nombre de “procesos comprometidos”. La inyección de código provoca que estos procesos ejecuten acciones para las que no fueron programados, generalmente peligrosas y que comprometen la seguridad del equipo. La protección anti-exploit de Adaptive Defense 360 detecta y bloquea estas inyecciones de código malicioso.

5.2.1 Configuración anti-exploit recomendada

56. A continuación, se muestra la configuración recomendada del módulo Protección Anti-exploit para las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Sección Protección avanzada (Windows) – Anti-exploit				
Auditar	Solo audita, no bloquea el intento de explotación.	Aplica	Op.	Op.
Bloquear	Bloquea los intentos de explotación.	Op.	Aplica	Aplica
Informar	Muestra un mensaje al usuario con cada intento de explotación.	Op.	Op.	Op.
Pedir permiso	El cierre del proceso afectado requiere el permiso del usuario.	Op.	Op.	Op.

5.2.2 Acceso a la configuración de protección anti-exploit

57. Para visualizar o modificar la configuración de protección anti-exploit haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Protección avanzada (Windows)**.

58. Haz clic en el botón **Protección avanzada** y en **Anti-Exploit** para activar la funcionalidad. Selecciona del desplegable **Modo de funcionamiento** uno de los dos modos de protección (**Auditar**, **Bloquear**) y a las opciones de notificación (**Informar**, **Pedir permiso**).

5.2.3 Funcionamiento de la protección anti-exploit

59. Adaptive Defense 360 bloquea los exploits mediante dos cursos de acción diferentes, dependiendo del tipo de ataque detectado:

    a) **Bloqueo del exploit**: se detecta la inyección de código en el proceso vulnerable cuando todavía no se ha completado. El proceso no llega a comprometerse y el riesgo del equipo es nulo.

    b) **Detección del exploit**: Adaptive Defense 360 detecta la inyección de código en el proceso vulnerable cuando ya se ha producido. Debido a que el proceso vulnerable ya contiene el código malicioso, es imperativo cerrarlo antes de que ejecute acciones que puedan poner en peligro la seguridad del equipo.

5.2.4 Configuración de la protección anti-exploit

a) **Auditar**: se notifica en la consola Web la detección del exploit, pero no se toman acciones contra él ni se informa al usuario del equipo. La notificación también puede producirse vía correo electrónico según la configuración de las alertas, a través de la opción **Detecciones de exploits**

accesible desde el menú superior **Configuración**, menú lateral **Mis alertas**.

b) **Bloquear**: bloquea los ataques de tipo exploit. Puede requerir el cierre del proceso afectado por el exploit.

c) **Informar del bloqueo al usuario del equipo**: el usuario recibe una notificación, pero el proceso comprometido se cierra de forma automática si es necesario.

d) **Pedir permiso al usuario**: el usuario recibe una petición de autorización para el cierre del proceso comprometido por el exploit, en caso de ser necesario. Esta opción resulta útil para que el usuario pueda salvar la información crítica antes producirse el cierre del proceso. Si se requiere el reinicio del equipo se pedirá confirmación al usuario, independientemente de la configuración **Pedir permiso al usuario**.

5.3. Protección antivirus permanente

60. La protección antivirus permanente es el módulo de seguridad tradicional que cubre los vectores de infección más utilizados por los hackers. Este módulo se alimenta tanto del archivo de identificadores publicado por Panda Security para su descarga en local, como del acceso en tiempo real a la Inteligencia Colectiva.

61. Adaptive Defense 360 implementa varios motores de detección que permiten analizar el comportamiento de los procesos de forma local. De esta manera se detectan scripts maliciosos, virus de macro y las últimas técnicas de ejecución de malware sin fichero (los llamados FileLess Malware). Como complemento se incorporan además los tradicionales motores heurísticos y de detección de ficheros maliciosos por características estáticas.

5.3.1 Configuración antivirus recomendada

62. A continuación, se muestra la configuración recomendada del módulo Protección antivirus permanente para las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Sección Antivirus				
Antivirus de archivos	Detecta amenazas en el sistema de ficheros.	Aplica	Aplica	Aplica
Antivirus de correo	Detecta amenazas en los mensajes de correo en las aplicaciones de mensajería instaladas.	Op.	Op.	Op.
Antivirus para navegación web	Detecta amenazas descargadas mediante el navegador web.	Aplica	Aplica	Aplica

Detectar virus		Aplica	Aplica	Aplica
Detectar herramientas de hacking y PUPs		Aplica	Aplica	Aplica
Bloquear acciones maliciosas		Aplica	Aplica	Aplica
Detectar phishing		Aplica	Aplica	Aplica
Analizar comprimidos en mensajes de correo	Descomprime los ficheros adjuntos en mensajes de correo. Requiere un extra de proceso.	Op.	Op.	Op.
Analizar comprimidos en disco (No recomendado)	Descomprime los archivos encontrados en el sistema de ficheros. Requiere un extra de proceso.	N.A	Op.	Aplica
Analizar todos los archivos independientemente de su extensión cuando son creados o modificados (No recomendado)	Analiza todos los ficheros encontrados sin importar el tipo. Requiere un extra de proceso.	N.A	Op.	Aplica

5.3.2 Acceso a la configuración de la protección antivirus

63. Para visualizar o modificar la configuración de protección antivirus en puestos de trabajo Windows, Linux y macOS haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Antivirus**.

64. Para visualizar o modificar la configuración de protección antivirus en dispositivos móviles Android haz clic en el menú superior **Configuración**, menú lateral **Dispositivos Android**, selecciona una configuración de la lista y haz clic en la sección **Antivirus**.

5.3.3 Recomendaciones de la protección antivirus

65. A continuación, se enumeran recomendaciones generales para configurar la protección antivirus permanente dependiendo del software instalado en los puestos de usuario y servidores y de la potencia de proceso instalada:

    a) Activa siempre **Antivirus de archivos** para analizar y desinfectar o eliminar las amenazas encontradas en el sistema de ficheros del equipo.

    b) Si los usuarios utilizan programas de mensajería instalados en el puesto de trabajo, activa siempre **Antivirus de correo** para analizar los ficheros

adjuntos en los mensajes recibidos y **Analizar los ficheros adjuntos comprimidos en los mensajes de texto**.

c) Si los usuarios utilizan navegadores web activa siempre **Antivirus para navegación web** para analizar los ficheros descargados con estas herramientas.

d) Activa siempre todos los tipos de amenazas a detectar: **Virus**, **Herramientas de hacking y PUPs**, **Acciones maliciosas** y **Phishing**.

e) No se recomienda seleccionar **Analizar comprimidos en disco** por su alto consumo de CPU y memoria. Solo está justificado en entornos con requisitos de seguridad muy alta.

f) No se recomienda seleccionar **Analizar todos los archivos independientemente de su extensión cuando son creados o modificados**. Solo está justificado en entornos con requisitos de seguridad muy alta.

5.4. Protección Firewall

66. Adaptive Defense 360 implementa tres herramientas para filtrar el tráfico de red que reciben o envían los equipos Windows de las Organizaciones:

a) **Protección mediante reglas de sistema**: son las reglas que describen características de las comunicaciones establecidas por el equipo (puertos, IPs, protocolos etc). Permite o deniega los flujos de datos que coincidan con las reglas configuradas.

b) **Protección de programas**: establece un conjunto de reglas que permiten o deniegan la comunicación a determinados programas instalados en el puesto de usuario o servidor.

c) **Sistema de detección de intrusos**: detecta y rechaza patrones de tráfico de red malformado que afectan a la seguridad o al rendimiento del equipo protegido.

5.4.1 Configuración Firewall recomendada

67. A continuación, se muestra la configuración recomendada del módulo Firewall para las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Sección Firewall (equipos Windows)				
La configuración firewall la establece	El usuario del puesto configura las opciones de filtrado del cortafuegos.	Op.	N.A	N.A

el usuario de cada equipo (activado)				
La configuración firewall la establece el usuario de cada equipo (desactivado)	El Administrador establece la configuración del cortafuegos para los puestos de usuario y servidores.	Op.	Aplica	Aplica
Red pública	Añade reglas en el extra en el puesto de trabajo cuando la red a la que se conectan no es segura.	Op.	Op.	Op.
Red de confianza	Relaja las reglas añadidas de forma automática en el puesto de trabajo cuando la red a la que se conectan es segura.	Op.	Op.	Op.
Reglas de programa permitir	Permite por defecto la comunicación de todos los programas instalados en el equipo.	Aplica	Op.	N.A
Reglas de programa denegar	Deniega por defecto la comunicación de todos los programas instalados en el equipo.	Op.	Op.	Aplica
Activar las reglas de Panda	Agrega reglas básicas de protección de programas.	Op.	Aplica	Aplica
Reglas de conexión Activar las reglas de Panda	Agrega reglas básicas de sistema.	Op.	Aplica	Aplica
Bloquear intrusiones (configuración por defecto)	Rechaza ciertos tipos de tráfico mal formado o sospechoso.	Aplica	Op.	N.A
Bloquear intrusiones (configuración todo seleccionado)	Rechaza todos los tipos soportados de tráfico mal formado o sospechoso.	N.A	Op.	Aplica

5.4.2 Acceso a la configuración de Firewall

68. Para visualizar o modificar la configuración de protección Firewall haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Firewall**.

5.4.3 Funcionamiento de la protección Firewall

Modos de funcionamiento

69. La protección firewall tiene dos modos de funcionamiento, accesibles mediante el control **La configuración firewall la establece el usuario de cada equipo**:

a) **Activado** (firewall en modo usuario o auto administrado): el usuario podrá configurar desde la consola local el firewall de su equipo. Este modo delega la gestión de la seguridad en el propio usuario. No se recomienda en redes con requisitos de seguridad medio o altos.

b) **Desactivado** (firewall en modo administrador): el administrador configura el cortafuegos de los equipos a través de perfiles de configuración. Recomendado para una máxima protección.

Tipos de red

70. Los equipos de usuario portátiles pueden conectarse a redes con un grado de seguridad muy diverso. Para ajustar el comportamiento por defecto del cortafuegos, el Administrador deberá de seleccionar el tipo de red al que se conectan usualmente los equipos del perfil configurado. La variación del comportamiento del software Adaptive Defense 360 según la red seleccionada se refleja en la consola en el número de reglas añadidas de forma automática. Estas reglas se pueden ver en **Reglas de programa** y **Reglas de conexión** como **Reglas de Panda**.

    a) **Red pública**: cibercafés, aeropuertos, etc. Limita el nivel de visibilidad de los equipos protegidos y la compartición de archivos, recursos y directorios.

    b) **Red de confianza**: oficinas, domicilios etc. El equipo es visible para el resto de usuarios de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

5.4.4 Configuración de la protección firewall

Reglas de programa

71. Para establecer los programas que podrán comunicarse con la red y los que tendrán bloqueado el envío y recepción de datos sigue los pasos mostrados a continuación, en el orden indicado:

    a) Establece la acción por defecto.

        a. **Permitir**: recomendada para organizaciones con requisitos de seguridad medios. Establece una estrategia permisiva que acepta por defecto las conexiones de todos los programas cuyo comportamiento no haya sido definido explícitamente. Este es el modo configurado por defecto y considerado el más básico.

        b. **Denegar**: recomendada para organizaciones con requisitos de seguridad altos. Establece una estrategia restrictiva que deniega por defecto las conexiones de los programas cuyo comportamiento no haya sido definido explícitamente. Este es el modo avanzado de funcionamiento ya que requiere añadir reglas con todos los programas que los usuarios utilizan de forma habitual; de otro modo las comunicaciones de esos programas serán denegadas.

b) **Activar reglas de Panda**: activa las reglas generadas automáticamente por Panda Security para el tipo de red definido.

c) Añade reglas para definir el comportamiento específico de una aplicación

Regla de conexión

72. Estas reglas aplican filtrado de tráfico basado en las cabeceras TCP/IP de la comunicación. Afectan a todo el puesto de usuario o servidor, independientemente del proceso en cuestión, y son prioritarias con respecto a las reglas configuradas anteriormente para la conexión de los programas a la red.

73. Sigue los pasos mostrados a continuación, en el orden indicado:

    a) Establece la acción por defecto del cortafuegos, situada en **Reglas para programas**.

        a. **Permitir**: recomendada para organizaciones con requisitos de seguridad medios. Establece una estrategia permisiva que acepta por defecto las conexiones cuyo comportamiento no ha sido definido. Este es el modo básico de configuración: todas las conexiones no descritas mediante reglas serán automáticamente aceptadas.

        b. **Denegar**: recomendada para organizaciones con requisitos de seguridad altos. Establece una estrategia restrictiva que deniega por defecto las conexiones cuyo comportamiento no ha sido definido mediante reglas en el paso anterior. Este es el modo avanzado de funcionamiento: todas las conexiones no descritas mediante reglas serán automáticamente denegadas.

    b) **Activar reglas de Panda**: activa las reglas generadas automáticamente por Panda Security para el tipo de red definido anteriormente.

    c) Añade reglas que describan conexiones de forma específica junto a una acción asociada.

5.4.5 Configuración de la protección contra intrusiones

74. El módulo IDS detecta y rechaza tráfico mal formado y especialmente preparado para impactar negativamente en el rendimiento o la seguridad del equipo a proteger. Adaptive Defense 360 identifica 15 tipos de patrones genéricos que pueden ser activados o desactivados haciendo clic en la casilla apropiada. A continuación, se detallan los tipos de tráfico mal formado soportados y una explicación de cada uno de ellos:

    a) **IP explicit path**: rechaza los paquetes IP que tengan la opción de “explicit route”. Son paquetes IP que no se encaminan en función de su dirección IP de destino, en su lugar la información de encaminamiento es fijada de ante mano.

b) **Land Attack**: comprueba intentos de denegación de servicio mediante bucles infinitos de pila TCP/IP al detectar paquetes con direcciones origen y destino iguales.

c) **SYN flood**: lanza inicios de conexión TCP de forma masiva para obligar al equipo a comprometer recursos para cada una de esas conexiones. Se establece un límite máximo de conexiones TCP abiertas para evitar una sobrecarga del equipo atacado.

d) **TCP Port Scan**: detecta si un equipo intenta conectarse a varios puertos del equipo protegido en un tiempo determinado. Se filtran tanto las peticiones de apertura de puerto como las respuestas al equipo sospechoso, para que el origen del tráfico de escaneo no obtenga información del estado de los puertos

e) **TCP Flags Check**: detecta paquetes TCP con combinaciones de flags inválidas. Actúa como complemento a las defensas de “Port Scanning” al detener ataques de este tipo como "SYN & FIN" y "NULL FLAGS" y los de “OS identification” ya que muchas de estas pruebas se basan en respuestas a paquetes TCP inválidos.

f) **Header lengths**

   a. **IP**: rechaza los paquetes entrantes con un tamaño de cabecera IP que se salga de los límites establecidos.

   b. **TCP**: rechaza los paquetes entrantes con un tamaño de cabecera TCP que se salga de los límites establecidos.

   c. **Fragmentation control**: comprueba el estado de los fragmentos de un paquete a reensamblar, protegiendo al equipo de ataques por consumo excesivo de memoria en ausencia de fragmentos, redireccionado de ICMP disfrazado de UDP y scanning de máquina disponible.

g) **UDP Flood**: rechaza los paquetes UDP que llegan a un determinado puerto si exceden en cantidad a un número determinado en un periodo determinado.

h) **UDP Port Scan**: protege contra escaneo de puertos UDP.

i) **Smart WINS**: rechaza las respuestas WINS que no se corresponden con peticiones que el equipo haya solicitado.

j) **Smart DNS**: rechaza las respuestas DNS que no se corresponden con peticiones que el equipo haya solicitado.

k) **Smart DHCP**: rechaza las respuestas DHCP que no se corresponden con peticiones que el equipo haya solicitado.

l) **ICMP Attack**:

a. **SmallPMTU**: detecta valores inválidos en el tamaño del paquete utilizados para generar una denegación de servicio o ralentizar el tráfico saliente.

b. **SMURF**: detecta el envió de grandes cantidades de tráfico ICMP (echo request) a la dirección de broadcast de la red con la dirección de origen cambiada (spoofing) a la dirección de la víctima. La mayoría de los equipos de la red responderán a la víctima, multiplicando el tráfico por cada equipo de la subred.

c. **Drop unsolicited ICMP replies**: rechaza todas las respuestas ICMP no solicitadas o que hayan expirado por el timeout establecido.

m) **ICMP Filter echo request**: rechaza las peticiones de Echo request.

n) **Smart ARP**: rechaza las respuestas ARP que no se corresponden con peticiones que el equipo protegido ha solicitado, para evitar escenarios de tipo ARP cache poison.

o) **OS Detection**: falsea datos en las respuestas al remitente para engañar a los detectores de sistemas operativos y así evitar posteriores ataques dirigidos.

5.5. Control de dispositivos

75. Los dispositivos de uso común como llaves USB, unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles son una vía de infección para los equipos de las Organizaciones. El módulo Control de dispositivos permite definir el comportamiento del equipo protegido al conectar u operar con un dispositivo extraíble o de almacenamiento masivo.

5.5.1 Configuración Control de dispositivos recomendada

76. A continuación, se muestra la configuración recomendada del módulo Control de dispositivos para las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Sección Control de dispositivos (equipos Windows)				
Unidades de almacenamiento extraíbles		Aplica	Aplica	Aplica
Unidades de CD/DVD		Op.	Op.	Aplica
Dispositivos Bluetooth		Op.	Aplica	Aplica
Dispositivos móviles		Aplica	Aplica	Aplica

Dispositivos de captura de imágenes		Op.	Aplica	Aplica
Módems		Aplica	Aplica	Aplica

5.5.2 Acceso a la configuración de Control de dispositivos

77. Para visualizar o modificar la configuración de protección Control de dispositivos haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Control de dispositivos**.

5.5.3 Política de control de dispositivos

78. Establece limitaciones en el acceso a los dispositivos según los recursos que el usuario demande de su puesto de trabajo y el grado de seguridad requerido por la Organización:

    a) **Unidades de almacenamiento extraíbles**: los discos duros externos pueden contener malware procedente de otros equipos no controlados. Los dispositivos utilizados para el traspaso de información entre varios usuarios o entre equipos sin administrar y administrados son especialmente peligrosos.

    b) **Dispositivos móviles**: los dispositivos móviles contienen unidades de almacenamiento similares a las del punto anterior. Además, estos dispositivos pueden ser de carácter personal y por lo tanto no administrado por la Organización.

    c) **Dispositivos de captura de imágenes**: muchas amenazas en circulación recogen información activando la webcam instalada en el equipo de usuario o en el portátil.

    d) **Módems**: permiten al usuario sortear la protección perimetral de la Organización, estableciendo un canal de comunicación directo a Internet.

    e) **Unidades de CD/DVD:** permiten introducir información en los puestos de usuario y servidores de fuentes externas no controladas.

    f) **Dispositivos Bluetooth**: los dispositivos Wifi o módems inalámbricos pueden ser utilizados por los usuarios para sortear la protección perimetral de la Organización, estableciendo un canal de comunicación directo a Internet.

5.5.4 Configuración del Control de dispositivos

79. El módulo **Control de dispositivos** de Adaptive Defense 360 establece limitaciones en el uso de grupos de periféricos. Selecciona el dispositivo o dispositivos que deseas autorizar y asigna un nivel de utilización:

a) Haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona la configuración de seguridad de la lista, haz clic en la sección **Control de dispositivos (Windows)** y **Activar control de dispositivos**.

b) Selecciona el nivel de acceso permitido a cada grupo de dispositivos: **bloquear**, **permitir**, **permitir lectura**, **permitir lectura y escritura**.

5.5.5 Configuración de los dispositivos permitidos

80. La configuración de dispositivos permitidos establece excepciones sobre equipos y positivos concretos. Para establecer una excepción haz clic en el icono ⊕, selecciona de la lista los dispositivos asociados a los equipos que quieres permitir y haz clic en el botón **Añadir**.

5.6. Control de acceso a páginas web

81. Restringe el acceso a recursos web para evitar la visita a sitios que contienen malware o phishing. Además, optimiza del ancho de banda de la red y la productividad, impidiendo que los usuarios dediquen tiempo a actividades sin relevancia para la Organización.

5.6.1 Configuración de Control de acceso a páginas web recomendada

82. A continuación, se muestra la configuración recomendada del módulo Acceso a páginas web para las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Sección Control de acceso a páginas web				
Siempre activo	Restringe el acceso web todo el día.	Op.	Aplica	Aplica
Activar solo durante las siguientes horas	Establece restricciones en determinadas franjas horarias.	Op.	N.A.	N.A.
Denegar el acceso a páginas de las siguientes categorías	Bloquea el acceso a páginas web que pertenecen a las categorías temáticas seleccionadas.	Aplica	Aplica	Aplica
Denegar el acceso a páginas cuya categoría sea desconocida	Bloquea el acceso a páginas web sin categoría temática asociada.	N.A.	Op.	Aplica
Permitir siempre el acceso a las siguientes	Lista blanca de páginas web.	Op.	Op.	Op.

direcciones y dominios				
Denegar el acceso a las siguientes direcciones y dominios	Lista negra de páginas web	Op.	Op.	Op.

5.6.2 Acceso a la configuración de Control de acceso a páginas web

83. Para visualizar o modificar la configuración de Control de acceso a páginas web haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Control de acceso a páginas web**.

5.6.3 Configuración del acceso a páginas web

84. Configura las limitaciones a recursos web según las necesidades de los usuarios y la Política de Seguridad TIC implantada en la Organización:

    a) Selecciona **Siempre activo** para establecer el control de forma permanente o **Activar solo durante las siguientes horas**. Selecciona en el calendario los días de la semana y las franjas horarios en las que Control de acceso a páginas web estará activado (por ejemplo, las franjas horarias que coincidan con la jornada laboral). Se recomienda **Siempre activo.**

    b) Haz clic en las casillas de selección las categorías de sitios web que los usuarios verán impedido el acceso.

    c) Para evitar el acceso a sitios web poco seguros que no están clasificados en la base de datos de Adaptive Defense 360 haz clic en el selector **Denegar el acceso a páginas cuya categoría sea desconocida**. Se recomienda en sistemas que requieren un nivel de seguridad alto.

    d) Añade las urls y dominios de acceso libre a **Permitir siempre el acceso a las siguientes direcciones y dominios**. Por defecto se incorporan los recursos web de Microsoft necesarios para actualizar los puestos de usuario y servidores

    e) Añade las urls y dominios cuyo acceso queda prohibido a **Denegar el acceso a las siguientes direcciones y dominios**. Estas urls siempre se denegarán independientemente de su pertenencia o no a una categoría denegada.

5.7. Antivirus para servidor Exchange

85. Adaptive Defense 360 es capaz de analizar los servidores Exchange en busca de virus, herramientas de hacking y programas potencialmente no deseados, con destino los buzones de los usuarios de la Organización.

86. La protección antivirus para servidores Exchange es aplicable a las versiones 2003, 2007, 2010, 2013 y 2016 y su funcionamiento varía dependiendo del rol del servidor de correo y de la versión.

Modo de análisis	Antivirus para servidor Exchange
Buzón	2003, 2007, 2010
Transporte	2003, 2007, 2010, 2013, 2016

Protección de buzones

87. Aplica a los servidores Exchange 2003, 2007 y 2010 con el rol de Mailbox, y permite analizar las carpetas / buzones en segundo plano o cuando el mensaje es recibido y almacenado en la carpeta del usuario. Admite la manipulación de los diferentes elementos del cuerpo del mensaje analizado, lo que permite sustituir los elementos peligrosos encontrados por otros seguros, introducir únicamente los elementos peligrosos en cuarentena etc.

Protección de transporte

88. Aplica a los servidores Exchange 2003, 2007, 2010, 2013 y 2016 con el rol de Acceso de clientes, Edge Transport y Hub, y permite analizar el tráfico que es atravesado por el servidor Microsoft Exchange.

5.7.1 Configuración Antivirus para servidor Exchange recomendada

89. A continuación, se muestra la configuración recomendada del módulo Antivirus para servidor Exchange para las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Antivirus para servidores Exchange				
Activar protección de buzones	Analiza los buzones cuando el mensaje es recibido y almacenado en la carpeta del usuario.	Aplica	Aplica	Aplica
Activar protección de transporte	Analiza todo el tráfico que pasa por el servidor Exchange	N.A	Op.	Aplica
Exclusiones para mejorar el rendimiento	Excluye del análisis ciertas carpetas de la instalación de Microsoft Exchange para mejorar el rendimiento	Aplica	Aplica	Aplica
Detectar virus		Aplica	Aplica	Aplica
Detectar herramientas de hacking y PUPs		Aplica	Aplica	Aplica

Activar análisis inteligente de buzones	Analiza los buzones en segundo plano aprovechando los tiempos de menor carga. No se analizan los mensajes ya examinados a no ser que se haya publicado un nuevo archivo de identificadores.	Aplica	Aplica	Aplica

5.7.2 Acceso a la configuración de la protección antivirus para servidores Exchange

90. Para visualizar o modificar la configuración de protección antivirus para servidores Exchange en servidores Windows haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Antivirus para servidores Exchange**.

5.8. Anti-spam para servidores Exchange

91. Adaptive Defense 360 implementa una protección anti-spam para servidores Exchange que optimiza el tiempo de trabajo de los usuarios y aumenta la seguridad de los equipos de la red.
92. La protección antivirus para servidores Exchange es aplicable a las versiones 2003, 2007, 2010, 2013 y 2016 en modo transporte.

5.8.1 Configuración Anti-spam para servidores Exchange recomendada

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Anti-spam para servidores Exchange				
Detectar spam	Activa el módulo anti-spam	Aplica	Aplica	Aplica
Acción a realizar	**Dejar pasar el mensaje**: añade la etiqueta "Spam" al asunto de los mensajes. **Mover el mensaje a**...: reenvía el correo a la dirección indicada con la etiqueta Spam en el asunto. **Borrar el mensaje.** **Marcar con SCL** (Spam Confidence Level): añade una cabecera SCL con un valor entre 0 y 9 (0: no es spam - 9 si es spam) para su tratamiento posterior.	Aplica	Aplica	Aplica

Direcciones y dominios permitidos	Lista blanca de direcciones y dominios.	Op.	Op.	Op.
Direcciones y dominios de spam	Lista negra de direcciones y dominios.	Op.	Op.	Op.

5.8.2 Acceso a la configuración de la protección anti-spam Exchange

93. Para visualizar o modificar la configuración de protección anti-spam en servidores Windows Exchange haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Anti-spam para servidores Exchange**.

5.9. Filtrado de contenidos para servidores Exchange

94. Permite filtrar los mensajes de correo electrónico en servidores Windows Exchange según extensión la de los archivos adjuntos incluidos en ellos.

5.9.1 Configuración de Filtrado de contenidos para servidores Exchange recomendada

95. A continuación, se muestra la configuración recomendada del módulo Filtrado de contenidos para servidores Exchange para las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores - Anti-spam para servidores Exchange				
Acción a realizar	**Mover el mensaje a**..: reenvía el correo a la dirección indicada. **Borrar el mensaje.**	Aplica	Aplica	Aplica
Considerar archivos adjuntos peligrosos	Ejecuta la acción sobre los mensajes que tengan archivos adjuntos con las extensiones indicadas.	Aplica	Aplica	Aplica
Considerar archivos adjuntos peligrosos todos los que tienen doble extensión, excepto…	Ejecuta la acción sobre todos los mensajes con adjuntos de doble extensión, excepto los indicados.	Aplica	Aplica	Aplica

5.9.2 Acceso a la configuración de la protección anti-spam Exchange

96. Para visualizar o modificar la configuración de protección anti-spam en servidores Windows Exchange haz clic en el menú superior **Configuración**, menú

lateral **Estaciones y servidores**, selecciona una configuración de la lista y haz clic en la sección **Anti-spam para servidores Exchange**.

6. Configuración de las actualizaciones

97. Adaptive Defense 360 es un servicio cloud gestionado, por esta razón las Organizaciones no necesitan implantar procedimientos que actualicen las infraestructuras de back-end que soportan los servicios de protección; sin embargo, sí es necesaria la actualización del software instalado en los equipos de la Organización.

98. Los elementos instalados en el puesto del usuario son tres:

    a) Agente de comunicaciones Panda.

    b) Motor de la protección Adaptive Defense 360.

    c) Archivo de identificadores / fichero de firmas para la protección antivirus tradicional.

99. El método de actualización de cada componente y plataforma varía en función de la tabla mostrada a continuación:

Modulo	Plataforma			
	Windows	**macOS**	**Linux**	**Android**
Agente Panda	Bajo demanda			
Protección Adaptive Defense 360	Configurable	Configurable	Configurable	No
Archivo de identificadores	Habilitar / Deshabilitar	Habilitar / Deshabilitar	Habilitar / Deshabilitar	No

    a) **Bajo demanda**: una vez que esté disponible, el Administrador puede iniciar la actualización cuando desee, pudiendo de esta forma retrasarla hasta el momento que considere oportuno.

    b) **Configurable**: el Administrador puede definir ventanas de actualización recurrentes y en el futuro mediante la consola, siendo posible además desactivar la actualización.

    c) **Habilitar / Deshabilitar**: el administrador puede desactivar la actualización. Si la actualización está activada, ésta se producirá automáticamente cuando esté disponible.

    d) **No**: el administrador no puede influir en el proceso de actualización. Las actualizaciones se efectuarán cuando estén disponibles y no es posible deshabilitarlas ni posponerlas.

6.1. Configuración de equipos cache

100. Adaptive Defense 360 permite asignar el rol de cache a uno o más puestos de la red. Estos equipos descargan y almacenan de forma automática todos los ficheros necesarios para que otros puestos con Adaptive Defense 360 instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección, sin necesidad de acceder a Internet. De esta manera, se produce un ahorro de ancho de banda.

Asignación del rol cache

101. Para asignar el rol de caché a un equipo Windows de la red sigue los pasos siguientes:

a) Haz clic en el menú superior **Configuración**, menú **lateral Configuración de red**, pestaña **Caché**, botón **Añadir equipo caché.**

b) Selecciona de la lista el equipo a asignar el rol de caché. Se recomienda seleccionar equipos con recursos hardware suficientes y que estén en funcionamiento el mayor número de horas del día posible.

Requisitos de cache

a) Solo los equipos Windows de la Organización que tengan Adaptive Defense 360 instalado pueden tener el rol caché asignado.

b) Los equipos Windows, macOS y Linux que estén en la misma subred que el equipo cache podrán beneficiarse de las actualizaciones centralizadas.

6.2. Actualización del agente de comunicaciones Panda

102. Es el componente software instalado en los puestos de usuario y servidores que hace de puente entre el módulo de protección y la nube de Panda Security. El agente Panda gestiona las comunicaciones, eventos y configuraciones de seguridad implementadas por el Administrador desde la consola de administración.

103. El agente de comunicaciones se actualiza de forma automática y sin intervención del Administrador de la Organización, previa notificación y acuerdo sobre la fecha y hora.

104. Para comprobar la versión del agente publicado por Panda Security haz clic en el icono  del menú superior y en el menú **Acerca de**. Se mostrará una ventana con la información del agente publicado.

6.3. Actualización del motor de la protección Adaptive Defense 360

105. Es el módulo encargado de proteger el puesto del usuario o servidor. Se sirve del agente de comunicaciones para recibir las configuraciones, y le entrega estadísticas y datos de las detecciones y elementos analizados.

6.3.1 Configuración de actualización de la protección recomendada

106. A continuación, se muestra la configuración recomendada para la actualización de la protección en las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Ajustes por equipo – Sección Actualizaciones				
Actualizar automáticamente Panda Adaptive Defense 360 en los equipos	Actualiza el motor de protección cuando se detecte una nueva versión publicada en los servidores de Panda Security.	Aplica	Op.	Op.
Rango de horas		Op.	Op.	Op.
Rango de fechas		Op.	Op.	Op.
Reiniciar	Reinicia el puesto de usuario o servidor de forma automática para completar la actualización.	Op.	Op.	Op.

6.3.2 Acceso a la configuración de Actualizaciones del motor de la protección

107. Para visualizar o modificar la configuración de la actualización del motor de protección Adaptive Defense 360 sigue los pasos mostrados a continuación:

a) Haz clic en el menú superior **Configuración,** panel de la izquierda **Ajustes por equipo** y selecciona una configuración.

b) En la sección **Actualizaciones** activa **Actualizar automáticamente Panda Adaptive Defense 360 en los equipos.**

c) Configura cuando se actualizará el motor de protección:

   a. Selecciona la franja horaria o **A cualquier hora.**

   b. Selecciona la fecha de actualización.

d) Configura si el equipo se reiniciará automáticamente una vez aplicada la actualización.

6.4. Actualización del archivo de identificadores / fichero de firmas para la protección antivirus tradicional

108. El fichero de firmas contiene los patrones que el antivirus utiliza para detectar las amenazas.

6.4.1 Configuración de la actualización del fichero de firmas recomendada

109. A continuación, se muestra la configuración recomendada para la actualización del fichero de firmas en las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores / Dispositivos Android – Sección General				
Actualizaciones automáticas de conocimiento	La actualización se produce de forma automática cuando se detecte un nuevo fichero de firmas publicado.	Aplica	Aplica	Aplica
Realizar un análisis en segundo plano cada vez que se actualice el conocimiento	Analiza el sistema de ficheros con el nuevo archivo de identificadores.	Op.	Aplica	Aplica
Actualizar sólo a través de Wi-Fi	Minimiza el consumo de datos destinado a las actualizaciones de dispositivos Android.	Op.	Op.	Op.

6.4.2 Acceso a la configuración de la actualización del fichero de firmas

110. Para visualizar o modificar la configuración de la actualización del motor de protección Adaptive Defense 360 en equipos Windows, Linux y macOS sigue los pasos mostrados a continuación:

a) Haz clic en el menú superior **Configuración**, panel de la izquierda **Estaciones y servidores** y selecciona una configuración o crea una nueva.

b) En la sección **General**, **Actualizaciones** activa **Actualizaciones automáticas de conocimiento**

c) Activa **Realizar un análisis en segundo plano cada vez que se actualice el conocimiento**

111. Para visualizar o modificar la configuración de la actualización del motor de protección Adaptive Defense 360 en dispositivos Android sigue los pasos mostrados a continuación:

a) Haz clic en el menú superior **Configuración**, panel de la izquierda **Dispositivos Android** y selecciona una configuración o crea una nueva.

b) En la sección Actualizaciones haz clic en **Actualizar sólo a través de Wi-Fi.**

c) Si has modificado una configuración previamente asignada, los cambios se despegarán en el momento.

d) Si has creado una nueva configuración, asígnala a los grupos de equipos pertinentes en el árbol de equipos.

7. Seguridad del agente

112. Adaptive Defense 360 incorpora características que impiden la modificación de la configuración o el cierre del producto para desactivar sus funciones de protección.

7.1. Configuración recomendada de la seguridad del agente

113. A continuación, se muestra la configuración recomendada para la seguridad del agente en las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Ajustes por equipo– Sección Seguridad frente a manipulaciones no deseadas de las protecciones				
Solicitar contraseña para desinstalar la protección desde los equipos	Adaptive Defense 360 solo se podrá desinstalar si el usuario tiene la contraseña de administración.	Aplica	Aplica	Aplica
Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos	Permite que el usuario pueda activar o desactivar las protecciones.	Op.	Op.	Op.
Activar protección anti-tamper	Evita la descarga o cierre no autorizados de los procesos de protección.	Aplica	Aplica	Aplica
Contraseña para poder realizar tareas de administración avanzada desde los equipos	Acceso a la consola local del producto para ejecutar tareas de configuración.	Aplica	Aplica	Aplica

7.2. Acceso a la configuración de Seguridad frente a manipulaciones no deseadas de las protecciones

114. Para visualizar o modificar la configuración de la seguridad frente a manipulaciones no deseadas de las protecciones haz clic en el menú superior **Configuración**, menú lateral **Ajustes por equipo**, selecciona una configuración de

la lista y en la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**, activa las opciones deseadas.

8. Uso de la red y privacidad

115. Adaptive Defense 360 puede incluir información adicional sobre las acciones que ejecuta el malware o los programas desconocidos en el equipo del usuario. Esta información se mostrará posteriormente en los informes y en las herramientas de análisis forense. A continuación, se indica la información recogida:

a) Nombre del fichero accedido por el malware o programa desconocido

b) Ruta en el puesto del usuario donde se encontró.

c) Cuenta iniciada en el puesto de usuario en el momento de registrarse la actividad sospechosa.

116. Los ficheros ejecutables encontrados en el equipo del usuario y que sean desconocidos para la plataforma Adaptive Defense 360 serán enviados a la nube de Panda Security para su análisis. Esta funcionalidad está configurada de manera que el impacto en el rendimiento sea desapercibido.

8.1. Configuración recomendada del uso de la red y la privacidad

117. A continuación, se muestra la configuración recomendada para el uso de la red y la privacidad en las tres categorías de sistemas reconocidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**
Estaciones y servidores– Sección Protección avanzada, Privacidad y Uso de red				
Recoger y mostrar en la consola el nombre y ruta completa	Las acciones de los procesos monitorizados que involucran accesos al sistema de ficheros se envían con la ruta y nombre completo del fichero.	Op.	Op.	Op.
Recoger y mostrar en la consola el usuario que tiene la sesión iniciada	Las acciones de los procesos monitorizados se envían con el nombre de la cuenta / usuario que lo ejecutó.	Op.	Op.	Op.
Número máximo de MB	Máximo número de megabytes transferidos por hora y puesto de trabajo para enviar programas desconocidos para su clasificación.	Op.	Op.	Op.

8.2. Acceso a la configuración del uso de la red y de la privacidad

118. Para visualizar o modificar la configuración del envío de información privada y el uso que hace Adaptive Defense 360 de la red de la Organización haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, selecciona una configuración de la lista y en la sección **Protección avanzada (Equipos Windows)** indica las opciones siguientes:

a) En la sección **Privacidad** indica con los selectores si se enviará información privada de los ficheros accedidos por el malware o por procesos desconocidos

b) En la sección **Uso de la red** indica el máximo número de megabytes por equipo utilizados para enviar archivos desconocidos pendientes de clasificar.

8.2.1 Funcionamiento del uso de la red y de la privacidad

119. Si no deseas que esta información sea enviada a la nube de Panda Security, desactiva la casilla apropiada en la pestaña **Privacidad**. Adicionalmente, Adaptive Defense 360 puede mostrar la información de la cuenta de usuario que estaba logeada en el equipo donde se detectó la amenaza. Si no deseas que esta información sea enviada a la nube de Panda Security desactiva la casilla apropiada en la pestaña **Privacidad.**

120. Un fichero desconocido se envía una sola vez para todos los clientes que usan Adaptive Defense 360. Además, se han implementado mecanismos de gestión del ancho de banda con el objetivo de minimizar el impacto en la red del cliente. Para configurar el número máximo de megas que un agente podrá enviar en una hora introducir el valor y hacer clic en Ok. Para establecer transferencias ilimitadas dejar el valor a 0.

9. Configuración de acceso a Adaptive Defense 360

121. Adaptive Defense 360 implementa mecanismos AAA (Authentication, Authorization and Accounting, Autenticación, Autorización y Registro) para conceder acceso a la consola limitado y condicionado a las credenciales suministradas por el Administrador de la seguridad del sistema.

9.1. Autenticación

122. La fase de autenticación abarca los procesos que validan las credenciales suministradas y permiten el acceso a la consola de Adaptive Defense 360. Se implementan dos modos de autenticación:

a) Autenticación básica.

b) Autenticación de dos factores (2FA).

9.1.1 Autenticación básica

123. Para crear una cuenta de acceso a la consola de administración con autenticación básica es necesario utilizar una cuenta con el permiso **Gestionar usuarios y roles** activado en su rol asignado. Sigue los pasos mostrados a continuación:

a) Haz clic en el menú superior **Configuración**, menú lateral **Usuarios**, botón **Añadir.**

b) Introduce el mail de acceso y el rol de la cuenta.

c) Haz clic en el botón **Guardar**. El sistema enviará un correo a la cuenta para generar la contraseña de acceso.

9.1.2 Autenticación de dos factores (2FA)

124. La autenticación de dos factores (2FA, Two Factor Authentication) requiere el uso de un dispositivo adicional para validar el acceso del administrador a la consola web.

Requisitos 2FA

125. Se requiere un dispositivo móvil o tablet y el programa Google Authenticator o equivalente instalado

Figura 8: Google Authenticator

Activación de 2FA

a) Inicia la sesión en la consola de administración con la cuenta que quieres activar 2FA.

b) En el menú superior haz clic en el icono  y selecciona **Configurar mi perfil** en el menú.

c) En el menú lateral haz clic en **Inicio de sesión** y en el link **Activar Verificación en dos pasos**. Se mostrará una ventana emergente con un código QR.

d) Abre Google Authenticator en tu dispositivo móvil y enfoca la cámara sobre el código QR mostrado. Cuando la aplicación lo reconozca generará un código, cópialo en la ventana de la consola y haz clic en **Verificar**.

Acceso a la consola de administración mediante 2FA

a) Introduce el nombre de usuario y contraseña de la cuenta.

b) Ejecuta Google Authenticator e introduce el código generado. Los códigos tienen una validez de 30 segundos, trascurridos los cuales el código expirará y se generará un nuevo código.

9.2. Autorización

126. Adaptive Defense 360 implementa un sistema de permisos agrupados en roles que configuran el nivel de acceso del administrador a las diferentes herramientas de la consola de administración. Además, permite establecer un ámbito o alcance formado por grupos de equipos que serán gestionables por el administrador.

9.2.1 Criterios para la creación de roles

127. El número de roles creados depende del tamaño de la Organización y del departamento IT encargado de gestionar la seguridad de la red. A continuación, se muestran los criterios para la creación de roles:

a) **Según el cometido del técnico**: Organizaciones de tamaño medio y grande tienen grupos de técnicos especializados en el despliegue de aplicaciones, monitorización, análisis forense, configuración de la seguridad etc.

b) **Según la estructura organizativa de la empresa**: grupos de administradores pueden estar asignados a departamentos concretos o a oficinas y delegaciones. Fuera de ese ámbito el administrador no tendrá posibilidad de gestionar la seguridad de los equipos de la organización.

c) **Según el cometido de los equipos**: grupos de administradores pueden estar dedicados a gestionar la seguridad de servidores de ficheros, portátiles en itinerancia, dispositivos móviles como smartphones o tables, servidores de correo etc.

9.2.2 Acceso a la configuración de roles

128. Para crear o modificar un rol sigue los pasos mostrados a continuación:

a) Haz clic en el menú superior **Configuración**, menú lateral **Usuarios**, pestaña **Roles.**

b) Haz clic en el botón **Añadir** para crear un nuevo rol o en un rol previamente creado para editarlo.

c) Introduce el nombre y descripción.

d) Configura el ámbito de acceso del rol en función de los criterios de creación de roles definidos en la Organización. Para ello selecciona los grupos de equipos que serán accesibles al rol.

e) Activa o desactiva los permisos asignados al rol.

f) Haz clic en el botón **Guardar**.

9.3. Registro

129. Adaptive Defense audita toda la actividad de los Administradores desarrollada en la consola de administración.

9.3.1 Acceso a la actividad del Administrador

130. Para mostrar la actividad del Administrador en la consola web sigue los pasos mostrados a continuación:

a) Haz clic en el menú superior **Configuración**, menú lateral **Usuarios**, pestaña **Actividad.**

b) Selecciona el tipo de información a mostrar en el listado: **Acciones** o **Sesiones**.

c) Define el intervalo a mostrar y la cuenta que ejecutó las acciones en el desplegable **Filtros**.

10. CRITERIOS DE CONFIGURACION DE ADAPTIVE DEFENSE 360

131. Para cumplir con las necesidades de seguridad de las Organizaciones se presenta una matriz de funcionalidades asignadas a las tres categorías de los sistemas definidas en el Anexo I del Real Decreto 3/2010 del 8 de enero.

		Categoría		
Funcionalidad	**Descripción**	**Básica**	**Media**	**Alta**

Estaciones y servidores - Sección Protección avanzada (Windows) – Comportamiento				
Protección avanzada	Habilita la protección avanzada.	Aplica	Aplica	Aplica
Modo Audit	Solo audita, no bloquea el malware avanzado.	Op.	Op.	Op.
Modo Hardening	Bloquea el malware conocido y los procesos desconocidos de fuentes no seguras.	Aplica	Aplica	Aplica
Modo Lock	Bloquea el malware y todos los procesos desconocidos.	N.A	Op.	Aplica
Estaciones y servidores - Sección Protección avanzada (Windows) – Anti-exploit				
Auditar	Solo audita, no bloquea el intento de explotación.	Aplica	Op.	Op.
Bloquear	Bloquea los intentos de explotación.	Op.	Aplica	Aplica
Informar	Muestra un mensaje al usuario con cada intento de explotación.	Op.	Op.	Op.
Pedir permiso	El cierre del proceso afectado requiere el permiso del usuario.	Op.	Op.	Op.
Estaciones y servidores - Sección Antivirus				
Antivirus de archivos	Detecta amenazas en el sistema de ficheros.	Aplica	Aplica	Aplica
Antivirus de correo	Detecta amenazas en los mensajes de correo en las aplicaciones de mensajería instaladas.	Op.	Op.	Op.
Antivirus para navegación web	Detecta amenazas descargadas mediante el navegador web.	Aplica	Aplica	Aplica
Detectar virus		Aplica	Aplica	Aplica
Detectar herramientas de hacking y PUPs		Aplica	Aplica	Aplica
Bloquear acciones maliciosas		Aplica	Aplica	Aplica
Detectar phishing		Aplica	Aplica	Aplica
Analizar comprimidos en mensajes de correo	Descomprime los ficheros adjuntos en mensajes de correo. Requiere un extra de proceso.	Op.	Op.	Op.
Analizar comprimidos en disco (No recomendado)	Descomprime los archivos encontrados en el sistema de ficheros. Requiere un extra de proceso.	N.A	Op.	Aplica

Analizar todos los archivos independientemente de su extensión cuando son creados o modificados (No recomendado)	Analiza todos los ficheros encontrados sin importar el tipo. Requiere un extra de proceso.	N.A	Op.	Aplica
Estaciones y servidores - Sección Firewall (equipos Windows)				
La configuración firewall la establece el usuario de cada equipo (activado)	El usuario del puesto configura las opciones de filtrado del cortafuegos.	Op.	N.A	N.A
La configuración firewall la establece el usuario de cada equipo (desactivado)	El Administrador establece la configuración del cortafuegos para los puestos de usuario y servidores.	Op.	Aplica	Aplica
Red pública	Añade reglas en el extra en el puesto de trabajo cuando la red a la que se conectan no es segura.	Op.	Op.	Op.
Red de confianza	Relaja las reglas añadidas de forma automática en el puesto de trabajo cuando la red a la que se conectan es segura.	Op.	Op.	Op.
Reglas de programa permitir	Permite por defecto la comunicación de todos los programas instalados en el equipo.	Aplica	Op.	N.A
Reglas de programa denegar	Deniega por defecto la comunicación de todos los programas instalados en el equipo.	Op.	Op.	Aplica
Activar las reglas de Panda	Agrega reglas básicas de protección de programas.	Op.	Aplica	Aplica
Reglas de conexión Activar las reglas de Panda	Agrega reglas básicas de sistema.	Op.	Aplica	Aplica
Bloquear intrusiones (configuración por defecto)	Rechaza ciertos tipos de tráfico mal formado o sospechoso.	Aplica	Op.	N.A
Bloquear intrusiones (configuración todo seleccionado)	Rechaza todos los tipos soportados de tráfico mal formado o sospechoso.	N.A	Op.	Aplica
Estaciones y servidores - Sección Control de dispositivos (equipos Windows)				

Unidades de almacenamiento extraíbles		Aplica	Aplica	Aplica
Unidades de CD/DVD		Op.	Op.	Aplica
Dispositivos Bluetooth		Op.	Aplica	Aplica
Dispositivos móviles		Aplica	Aplica	Aplica
Dispositivos de captura de imágenes		Op.	Aplica	Aplica
Módems		Aplica	Aplica	Aplica
Estaciones y servidores - Sección Control de acceso a páginas web				
Siempre activo	Restringe el acceso web todo el día.	Op.	Aplica	Aplica
Activar solo durante las siguientes horas	Establece restricciones en determinadas franjas horarias.	Op.	N.A.	N.A.
Denegar el acceso a páginas de las siguientes categorías	Bloquea el acceso a páginas web que pertenecen a las categorías temáticas seleccionadas.	Aplica	Aplica	Aplica
Denegar el acceso a páginas cuya categoría sea desconocida	Bloquea el acceso a páginas web sin categoría temática asociada.	N.A.	Op.	Aplica
Permitir siempre el acceso a las siguientes direcciones y dominios	Lista blanca de páginas web.	Op.	Op.	Op.
Denegar el acceso a las siguientes direcciones y dominios	Lista negra de páginas web	Op.	Op.	Op.
Estaciones y servidores - Antivirus para servidores Exchange				
Activar protección de buzones	Analiza los buzones cuando el mensaje es recibido y almacenado en la carpeta del usuario.	Aplica	Aplica	Aplica
Activar protección de transporte	Analiza todo el tráfico que pasa por el servidor Exchange	N.A	Op.	Aplica
Exclusiones para mejorar el rendimiento	Excluye del análisis ciertas carpetas de la instalación de Microsoft Exchange para mejorar el rendimiento	Aplica	Aplica	Aplica
Detectar virus		Aplica	Aplica	Aplica

Detectar herramientas de hacking y PUPs		Aplica	Aplica	Aplica
Activar análisis inteligente de buzones	Analiza los buzones en segundo plano aprovechando los tiempos de menor carga. No se analizan los mensajes ya examinados a no ser que se haya publicado un nuevo archivo de identificadores.	Aplica	Aplica	Aplica
Estaciones y servidores - Anti-spam para servidores Exchange				
Detectar spam	Activa el módulo anti-spam	Aplica	Aplica	Aplica
Acción a realizar	**Dejar pasar el mensaje**: añade la etiqueta "Spam" al asunto de los mensajes. **Mover el mensaje a**...: reenvía el correo a la dirección indicada con la etiqueta Spam en el asunto. **Borrar el mensaje.** **Marcar con SCL** (Spam Confidence Level): añade una cabecera SCL con un valor entre 0 y 9 (0: no es spam - 9 si es spam) para su tratamiento posterior.	Aplica	Aplica	Aplica
Direcciones y dominios permitidos	Lista blanca de direcciones y dominios.	Op.	Op.	Op.
Direcciones y dominios de spam	Lista negra de direcciones y dominios.	Op.	Op.	Op.
Estaciones y servidores - Anti-spam para servidores Exchange				
Acción a realizar	**Mover el mensaje a**..: reenvía el correo a la dirección indicada. **Borrar el mensaje.**	Aplica	Aplica	Aplica
Considerar archivos adjuntos peligrosos	Ejecuta la acción sobre los mensajes que tengan archivos adjuntos con las extensiones indicadas.	Aplica	Aplica	Aplica
Considerar archivos adjuntos peligrosos todos los que tienen doble extensión, excepto…	Ejecuta la acción sobre todos los mensajes con adjuntos de doble extensión, excepto los indicados.	Aplica	Aplica	Aplica
Ajustes por equipo – Sección Actualizaciones				
Actualizar automáticamente Panda Adaptive	Actualiza el motor de protección cuando se detecte una nueva	Aplica	Op.	Op.

Defense 360 en los equipos	versión publicada en los servidores de Panda Security.			
Rango de horas		Op.	Op.	Op.
Rango de fechas		Op.	Op.	Op.
Reiniciar	Reinicia el puesto de usuario o servidor de forma automática para completar la actualización.	Op.	Op.	Op.
Estaciones y servidores / Dispositivos Android – Sección General				
Actualizaciones automáticas de conocimiento	La actualización se produce de forma automática cuando se detecte un nuevo fichero de firmas publicado.	Aplica	Aplica	Aplica
Realizar un análisis en segundo plano cada vez que se actualice el conocimiento	Analiza el sistema de ficheros con el nuevo archivo de identificadores.	Op.	Aplica	Aplica
Actualizar sólo a través de Wi-Fi	Minimiza el consumo de datos destinado a las actualizaciones de dispositivos Android.	Op.	Op.	Op.
Ajustes por equipo– Sección Seguridad frente a manipulaciones no deseadas de las protecciones				
Solicitar contraseña para desinstalar la protección desde los equipos	Adaptive Defense 360 solo se podrá desinstalar si el usuario tiene la contraseña de administración.	Aplica	Aplica	Aplica
Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos	Permite que el usuario pueda activar o desactivar las protecciones.	Op.	Op.	Op.
Activar protección anti-tamper	Evita la descarga o cierre no autorizados de los procesos de protección.	Aplica	Aplica	Aplica
Contraseña para poder realizar tareas de administración avanzada desde los equipos	Acceso a la consola local del producto para ejecutar tareas de configuración.	Aplica	Aplica	Aplica
Estaciones y servidores– Sección Protección avanzada, Privacidad y Uso de red				
Recoger y mostrar en la consola el	Las acciones de los procesos monitorizados que involucran accesos al sistema de ficheros se	Op.	Op.	Op.

nombre y ruta completa	envían con la ruta y nombre completo del fichero.			
Recoger y mostrar en la consola el usuario que tiene la sesión iniciada	Las acciones de los procesos monitorizados se envían con el nombre de la cuenta / usuario que lo ejecutó.	Op.	Op.	Op.
Número máximo de MB	Máximo número de megabytes transferidos por hora y puesto de trabajo para enviar programas desconocidos para su clasificación.	Op.	Op.	Op.