Guía de Seguridad de las TIC
CCN-STIC 1213

Procedimiento de empleo seguro
Adaptive Defense 360

Marzo 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.03.28 10:50:30 +02'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-111-8

ÍNDICE

1. INTRODUCCIÓN 5
2. OBJETO Y ALCANCE 6
3. ORGANIZACIÓN DEL DOCUMENTO 7
4. FASE PREVIA A LA INSTALACIÓN 8
4.1 ENTREGA SEGURA DEL PRODUCTO 8
4.2 ENTORNO DE INSTALACIÓN SEGURO 9
4.3 REGISTRO Y LICENCIAS 9
4.4 CONSIDERACIONES PREVIAS 10
4.4.1 COMPROBAR QUE SE CUMPLEN LOS REQUISITOS MÍNIMOS DE LA PLATAFORMA DE DESTINO 10
4.4.2 COMPROBAR QUE SE CUMPLEN LOS REQUISITOS DE ACCESO A LA CONSOLA DE ADMINISTRACION 12
4.4.3 COMPROBAR EL ACCESO A LAS URLS DEL SERVICIO 12
4.4.4 COMPATIBILIDAD CON PRODUCTOS DE SEGURIDAD DE TERCEROS FABRICANTES 12
4.4.5 ESTABLECER UNA VENTANA DE SERVICIO PARA EL DESPLIEGUE INICIAL DEL PRODUCTO 13
4.4.6 CREACIÓN DE LAS CONFIGURACIONES DE RED NECESARIAS 13
4.4.7 CONFIGURAR EL ACCESO POR CONEXIÓN DIRECTA 13
5. FASE DE DESPLIEGUE DEL PRODUCTO 17
5.1 ELABORAR UN INVENTARIO DE EQUIPOS DESPROTEGIDOS 17
5.1.1 DESCUBRIMIENTO AUTOMÁTICO DE EQUIPOS SIN PROTEGER 18
5.2 REVISAR EL ACCESO EXITOSO A LOS RECURSOS DE ADAPTIVE DEFENSE 360 EN LA NUBE 20
5.3 CREACIÓN DE LA ESTRUCTURA NECESARIA DEL ÁRBOL DE EQUIPOS 20
5.3.1 CRITERIOS DE DISEÑO PARA EL ÁRBOL DE EQUIPOS 21
5.3.2 GRUPOS NATIVOS 22
5.3.3 GRUPOS IP 22
5.3.4 GRUPOS DE DIRECTORIO ACTIVO Y GRUPOS NATIVOS/IP 23
5.3.5 GRUPOS Y ASIGNACIÓN DE CONFIGURACIONES DE SEGURIDAD 24
5.4 REVISIÓN DE LA CONFIGURACIÓN DE SEGURIDAD POR DEFECTO 24
5.5 DESPLIEGUE DE FORMA ESCALONADA 24
6. FASE DE INSTALACIÓN 26
6.1 INSTALAR ADAPTIVE DEFENSE 360 DE FORMA LOCAL 26
6.2 INSTALAR ADAPTIVE DEFENSE 360 DE FORMA REMOTA 28
6.3 INSTALAR ADAPTIVE DEFENSE 360 DE FORMA REMOTA CON HERRAMIENTAS DE TERCEROS 28
6.4 INSTALAR ADAPTIVE DEFENSE 360 MEDIANTE MAQUETAS/IMÁGENES “GOLD” .29
6.5 INSTALAR ADAPTIVE DEFENSE 360 EN UN ENTORNO VDI PERSISTENTE O EN UN EQUIPO FÍSICO 29
6.6 INSTALAR ADAPTIVE DEFENSE 360 EN UN ENTORNO VDI NO PERSISTENTE 30
6.7 COMPROBAR EL RESULTADO DE LA INSTALACIÓN 32

7. FASE DE CONFIGURACIÓN 33
7.1 CATEGORÍAS Y ASIGNACIÓN DE CONFIGURACIONES 33
7.1.1 GRUPOS DE EQUIPOS Y HERENCIA DE CONFIGURACIONES 33
7.2 CONFIGURACIONES DE SEGURIDAD 34
7.2.1 PROTECCIÓN AVANZADA: *AUDIT, HARDENING, LOCK* 34
7.2.2 PROTECCIÓN AVANZADA: ANTI-*EXPLOIT* 36
7.2.3 PROTECCIÓN ANTIVIRUS PERMANENTE 38
7.2.4 PROTECCIÓN FIREWALL 40
7.2.5 PROTECCIÓN ANTIRROBO 46
7.2.6 CONTROL DE ACCESO A PÁGINAS WEB 49
7.2.7 ANTIVIRUS PARA SERVIDOR EXCHANGE 51
7.2.8 ANTI-SPAM PARA SERVIDORES EXCHANGE 53
7.2.9 FILTRADO DE CONTENIDOS PARA SERVIDORES EXCHANGE 54
7.2.10 CONFIGURACIÓN DE BLOQUEO PARA APLICACIONES 54
7.3 AUTENTICACIÓN 56
7.3.1 AUTENTICACIÓN BÁSICA 56
7.3.2 AUTENTICACIÓN DE DOS FACTORES (2FA) 56
7.4 ADMINISTRACIÓN DEL PRODUCTO 58
7.4.1 CREACIÓN DE CUENTAS DE ADMINISTRACIÓN 58
7.4.2 CREACIÓN Y CONFIGURACIÓN DE ROLES 59
7.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 60
7.6 GESTIÓN DE CERTIFICADOS 61
7.7 SERVIDORES DE AUTENTICACIÓN 61
7.8 SINCRONIZACIÓN 61
7.9 ACTUALIZACIONES 62
7.9.1 CONFIGURACIÓN DE EQUIPOS CACHE 63
7.9.2 ACTUALIZACIÓN DEL AGENTE DE COMUNICACIONES 64
7.9.3 ACTUALIZACIÓN DEL MOTOR DE PROTECCIÓN ADAPTIVE DEFENSE 360 64
7.9.4 ACTUALIZACIÓN DEL ARCHIVO DE IDENTIFICADORES/FICHERO DE FIRMAS PARA LA PROTECCIÓN ANTIVIRUS TRADICIONAL 65
7.9.5 ACTUALIZACIÓN DE LA CONSOLA DE ADMINISTRACIÓN 66
7.10 ALTA DISPONIBILIDAD 67
7.11 REGISTRO Y AUDITORÍA 67
7.11.1 ACCESO A LA ACTIVIDAD DEL ADMINISTRADOR 68
7.11.2 ACCESO A LOS EVENTOS DEL SISTEMA 68
7.12 BACKUP 68
7.12.1 BACKUP DE FICHEROS BORRADOS POR PANDA DATA CONTROL 68
7.12.2 RESTAURACIÓN DE FICHEROS PREVIAMENTE BORRADOS POR EL ADMINISTRADOR 69
7.12.3 GESTIÓN DE LA ZONA DE BACKUP/CUARENTENA 69
7.12.4 RESTAURACIÓN DE ELEMENTOS EN CUARENTENA 70
7.13 SEGURIDAD DEL AGENTE 70
7.13.1 ACCESO A LA CONFIGURACIÓN DE SEGURIDAD FRENTE A MANIPULACIONES NO DESEADAS DE LAS PROTECCIONES 70
7.13.2 CONFIGURACIÓN RECOMENDADA DE LA SEGURIDAD DEL AGENTE 71

7.14 USO DE LA RED Y PRIVACIDAD 72
7.14.1 ACCESO A LA CONFIGURACIÓN DEL USO DE LA RED Y DE LA PRIVACIDAD 74
7.14.2 CONFIGURACIÓN RECOMENDADA DEL USO DE LA RED Y LA PRIVACIDAD 74
7.14.3 FUNCIONAMIENTO DEL USO DE LA RED Y LA PRIVACIDAD 75
7.15 CRITERIOS DE CONFIGURACIÓN DE ADAPTIVE DEFENSE 360 75
8. FASE DE OPERACIÓN 83
9. REFERENCIAS 84

1. INTRODUCCIÓN

1. **Adaptive Defense 360** es una solución de seguridad para puestos de usuario y servidores, formada por diferentes tecnologías que ofrecen un servicio gestionado de protección contra el malware, sin necesidad de instalar, gestionar o mantener recursos hardware adicionales en la infraestructura de la organización.
2. Adaptive Defense 360 es un servicio multiplataforma alojado en la nube, compatible con Windows, macOS, Linux, Android, y con entornos virtuales y VDI.
3. Supervisa y clasifica todos los procesos ejecutados en los equipos, en base a su comportamiento y naturaleza.

2. OBJETO Y ALCANCE

4. El propósito de este documento es detallar los procedimientos necesarios para desplegar el producto **Adaptive Defense 360 en su versión 3.71.00**, así como para establecer las configuraciones básicas para conseguir una configuración segura y una protección efectiva de los puestos de trabajo y servidores.
5. Se recomienda consultar el apartado 4.4.1 de este documento para obtener un listado de las plataformas compatibles con Adaptive Defense 360 3.71.00.

3. ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento se estructura en los apartados descritos a continuación:

   a) **Apartado 4.** En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

   b) **Apartado 5.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue del producto.

   c) **Apartado 6.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

   d) **Apartado 7.** En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   e) **Apartado 8.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. El instalador de Adaptive Defense 360 está firmado con un certificado digital que permite garantizar su autenticidad e integridad. El usuario puede comparar la información del certificado con la mostrada a continuación. Por su parte, el instalador despliega el agente de Adaptive Defense 360 en el equipo del usuario, que se encarga a su vez de descargar y autenticar de forma automática el resto de módulos necesarios (protección, *plugins*, etc) mediante su hash SHA-256.

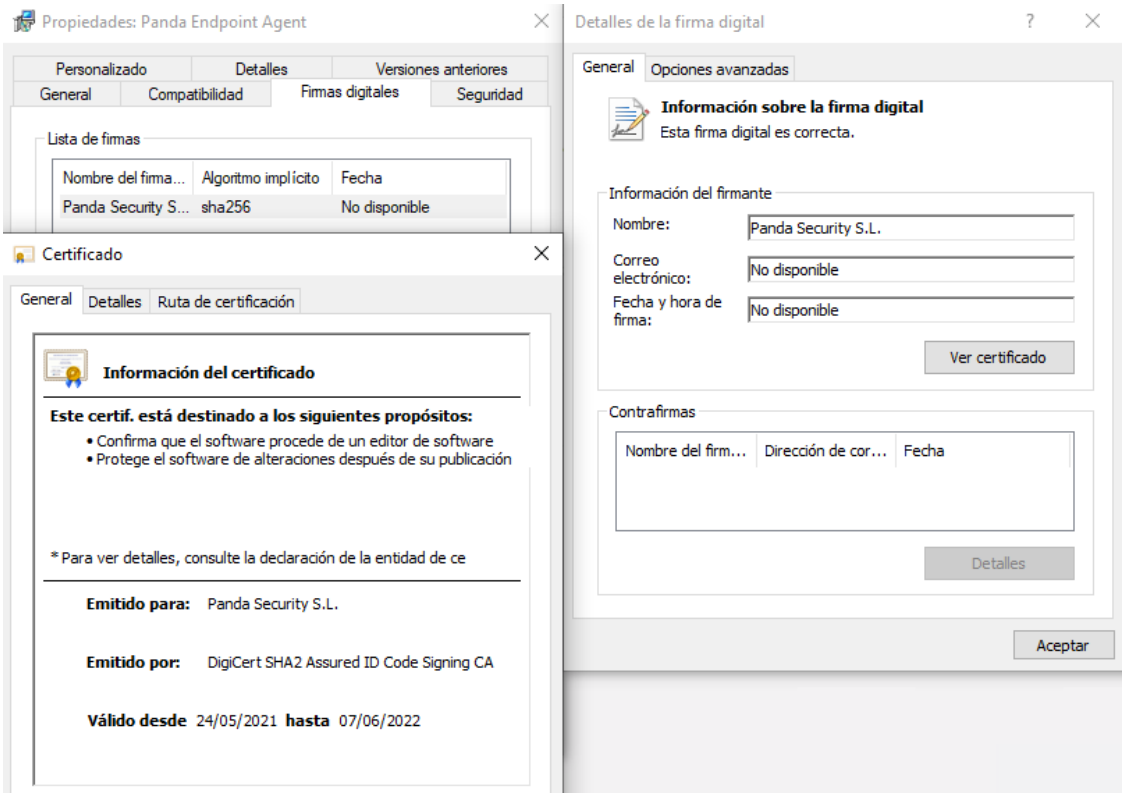

Figura 1: Detalles de la firma digital del instalador

8. A continuación, se enumeran los pasos a seguir para obtener la huella digital de un producto firmado:

   a) Haz clic con el botón derecho del ratón sobre el instalador y elige **Propiedades** en el menú de contexto.

   b) En la ventana **Propiedades** haz clic en la pestaña **Firmas digitales**.

   c) Elige en **Lista de firmas** Panda Security S.L. y haz clic en el botón **Detalles**. Se mostrará la ventana **Detalles de la firma digital**.

   d) En la ventana **Detalles de la firma digital**, selecciona la pestaña **General** y haz clic en el botón **Ver certificado**. Se abrirá la ventana **Certificado**.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. Adaptive Defense 360 no requiere servidores de control, bases de datos u otras soluciones *hardware* o *software* para proteger los equipos de la infraestructura IT del cliente. La consola de gestión se aloja en la nube y el administrador de la red se conecta a ella a través de un navegador web mediante una conexión segura.

4.3 REGISTRO Y LICENCIAS

10. Tras llevar a cabo una estimación del número de dispositivos a proteger, es necesario comprobar el número de licencias libres contratadas en el menú superior **Estado**, menú lateral **Licencias**, barra **Sin asignar**. En caso de que el número de equipos a proteger sea mayor que el número de licencias sin asignar deberán adquirirse las licencias necesarias.

Figura 2: Ventana de licencias

11. Una licencia de Adaptive Defense 360 solo puede ser asignada a un único equipo en un momento concreto, ya sea una estación de trabajo, dispositivo móvil o servidor.
12. La asignación de licencia a un equipo puede llevarse a cabo de forma automática o de forma manual.
13. En caso de emplear la asignación automática, al instalar el *software* en un equipo de la red, y siempre que existan licencias sin utilizar, el sistema asignará de forma automática una licencia libre.
14. En caso de emplear la asignación manual, se seguirán los pasos que se indican a continuación:
    a) En el menú **Equipos**, localizar el dispositivo al que le será asignada la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
    b) Hacer clic en el equipo seleccionado, para mostrar la ventana de detalles.
    c) En la pestaña **Detalles > Licencias**, se mostrará el estado **Sin licencias**. Tras hacer clic en el icono **"+"** se asignará de forma automática una licencia libre.
15. Asimismo, el proceso de liberación de licencias puede llevarse a cabo tanto de forma automática como de forma manual.

16. En caso de llevarse a cabo de forma automática, al desinstalar el *software* de un equipo de la red, el sistema recuperará de forma automática una licencia, y la devolverá al grupo de licencias sin usar.
17. Para liberar de forma manual una licencia de Adaptive Defense 360 de un equipo de la red, se seguirán los pasos que se indican a continuación:
    a) En el menú **Equipos**, localizar el dispositivo cuya licencia se desea liberar mediante el árbol de carpetas, el árbol de filtros, o la herramienta de búsqueda.
    b) Hacer clic en el equipo para mostrar su información.
    c) En la pestaña **Detalles > Licencias** se mostrará el estado del equipo. Tras hacer clic en el icono **"+"**, se liberará la licencia, y se devolverla al grupo de licencias sin utilizar.
18. Para visualizar los detalles asociados a las licencias contratadas, se hará clic en el menú superior **Estado**, y a continuación en el menú lateral **Licencias**. Se mostrará una ventana con dos gráficas: **Licencias contratadas** y **Caducidad de licencias**.
19. Para más información sobre el proceso de gestión y manejo de licencias, se recomienda consultar el Capítulo 7: Licencias, de la Guía de Administración del producto **[REF4]**.

4.4 CONSIDERACIONES PREVIAS

20. El proceso de despliegue e instalación de Adaptive Defense 360 3.71.00 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 UNA SERIE DE PUNTOS**:

4.4.1 COMPROBAR QUE SE CUMPLEN LOS REQUISITOS MÍNIMOS DE LA PLATAFORMA DE DESTINO

21. Comprobar que no existen incompatibilidades de software y hardware con Adaptive Defense 360. En caso de duda, contactar con el *Technical Account Manager* (TAM) asignado.
22. Comprobar que se cumplen los requisitos *hardware* y de Sistema Operativo mínimos en los equipos a instalar Adaptive Defense 360.

4.4.1.1 REQUISITOS WINDOWS[1]

a) **Estaciones de trabajo**: Windows 8 y Windows 10.

[1] A fecha de publicación de la presente guía, el fabricante declara que la herramienta se ejecuta sobre otras versiones del sistema operativo, no obstante, solamente se han incluido aquellas versiones con soporte, dado que son las únicas recomendadas. Este listado está sujeto a modificaciones en caso de que dichas versiones del sistema

b) **Servidores**: Windows Server 2012 R2, Windows Server 2016 y 2019.

c) Servidores Exchange: 2003 al 2019.

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

e) Memoria RAM: 1 Gbyte.

f) Espacio para la instalación: 650 Mbytes.

4.4.1.2 REQUISITOS LINUX

a) **Sistemas operativos 64 bits**: Ubuntu 18.04 LTS y superiores, Fedora 34 y superiores, Debian 10.0 y superiores, CentOS 7.0 y superiores, Red Hat Enterprise Linux RHEL 7.0 y superiores, LinuxMint 19 o superiores.

b) **Kernel soportado**: desde la versión 3.12 hasta la versión 5.00 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.

4.4.1.3 REQUISITOS MACOS

a) **Sistemas operativos**: macOS 10.15 Catalina 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.

4.4.1.4 REQUISITOS ANDROID

a) **Sistemas operativos**: Android 9.X y superiores.

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

operativo lleguen al fin de su ciclo de vida. Este comentario es igualmente aplicable a los requisitos de LINUX, MacOS y Android.

4.4.2 COMPROBAR QUE SE CUMPLEN LOS REQUISITOS DE ACCESO A LA CONSOLA DE ADMINISTRACION

23. La consola de administración es compatible con la última versión de los navegadores mostrados a continuación:
    a) Chrome.
    b) Internet Explorer.
    c) Microsoft Edge.
    d) Firefox.
    e) Opera.

4.4.3 COMPROBAR EL ACCESO A LAS URLS DEL SERVICIO

24. Para el correcto funcionamiento de Adaptive Defense 360 es necesario que los equipos protegidos de la red puedan acceder a las URLs mostradas a continuación:
    a) https://.pandasecurity.com*
    b) http://.pandasecurity.com*
    c) https://.windows.net*
    d) http://.globalsign.com*
    e) http://.digicert.com*
    f) http://.pand.ctmail.com*
    g) http://download.ctmail.com
    h) https://pandasecurity.devo.com
25. Para el correcto funcionamiento de Adaptive Defense 360 es necesario que los equipos protegidos de la red puedan acceder a los puertos mostrados a continuación:
    a) Puerto 80 (HTTPs)
    b) Puerto 443 (HTTPs)

4.4.4 COMPATIBILIDAD CON PRODUCTOS DE SEGURIDAD DE TERCEROS FABRICANTES

26. 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. Se recomienda consultar la URL https://www.pandasecurity.com/spain/support/card?id=50021 **[REF1]** para obtener un listado con todos los productos que Adaptive Defense 360 desinstala de forma automática.

4.4.5 ESTABLECER UNA VENTANA DE SERVICIO PARA EL DESPLIEGUE INICIAL DEL PRODUCTO

27. 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 del equipo, aunque se produce un corte en las comunicaciones de 4 segundos de duración aproximada. Este corte puede afectar al funcionamiento de los programas que no gestionan adecuadamente las conexiones de red ya establecidas.

4.4.6 CREACIÓN DE LAS CONFIGURACIONES DE RED NECESARIAS

28. Adaptive Defense 360 se conecta con la nube 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 web. 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 red en la consola web como salidas distintas a través de proxy se utilicen en la Organización.

4.4.7 CONFIGURAR EL ACCESO POR CONEXIÓN DIRECTA

29. No es necesario crear una configuración de red para los equipos con conexión directa a Internet. La configuración por defecto permite el acceso de EDPR sin intermediarios a Internet.

4.4.7.1 CONFIGURAR EL ACCESO POR PROXY CORPORATIVO

30. Para crear una configuración de red por cada proxy corporativo utilizado en la Organización deberán seguirse los pasos que se indican a continuación:

    a) Hacer clic en el menú superior **Configuración**, menú lateral **Configuración de red**, botón **Añadir**.

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

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

    d) En la sección **Proxy,** hacer clic en el botón ⊕.

    e) Se mostrará el desplegable en el que seleccionar **Proxy corporativo.**

    f) Introducir la **dirección IP**, **puerto** y la información de las **credenciales** necesarias.

    g) Hacer clic en el botón **Añadir.**

    h) Seleccionar el proxy añadido y hacer clic en los iconos ↑ ↓ para establecer el orden en el que los equipos intentarán conectarse al mismo. Si un equipo intenta acceder a Internet a través de un proxy y éste no se encuentra en

funcionamiento, avanzará en la lista al siguiente proxy, hasta encontrar uno operativo.

i) Hacer clic en el botón de **Guardar** para finalizar la configuración.

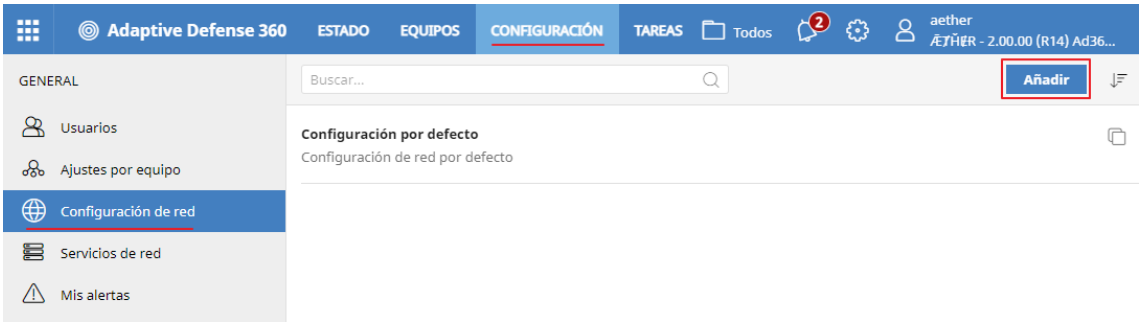

Figura 3: Menú Configuración > Configuración de red

4.4.7.2 CONEXIÓN A TRAVÉS DE UN EQUIPO CON ADAPTIVE DEFENSE 360 INSTALADO (PROXY PANDA)

31. Para asignar el rol de proxy a un equipo con Adaptive Defense 360 instalado deberán seguirse los pasos que se indican a continuación:

    a) Hacer clic en el menú superior **Configuración**, menú lateral **Servicios de red**, pestaña **Proxy de Panda**. Se mostrará un listado de los equipos que tienen el rol de proxy Panda asignado.

    b) Hacer clic en el botón **Añadir servidor proxy de Panda.** Se mostrará la ventana **Añadir proxy de Panda** con un listado de los equipos con el producto ya instalado.

    c) Utilizar la caja de búsqueda superior para localizar equipos concretos.

    d) Hacer clic en un equipo para asignarle el rol de proxy Panda. El equipo se agregará al listado de equipos con el rol proxy Panda asignado.

Figura 4: Configuración proxy Panda

4.4.7.2.1 REQUISITOS PARA EQUIPOS CON ROL DE PROXY

a) El rol de proxy Panda 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, ya sea directa o indirecta a través de un proxy corporativo.

32. Para crear una configuración de red por cada proxy Panda designado deberán seguirse los pasos que se indican a continuación:

a) Hacer clic en el menú superior **Configuración**, menú lateral **Configuración de red**, botón **Añadir.**

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

c) Hacer clic en la sección **Proxy**, con el botón ⊕ para abrir la ventana **Añadir proxy**.

d) Seleccionar la opción Proxy de Adaptive Defense 360 y hacer clic en **Seleccionar equipo**.

e) En la ventana **Seleccionar servidor proxy** hacer clic en el equipo que se utilizará como proxy.

f) Hacer clic en el botón **Guardar** y después en **Añadir**.

5. FASE DE DESPLIEGUE DEL PRODUCTO

33. El proceso de despliegue e instalación de Adaptive Defense 360 3.71.00 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. Estos pasos son:

    a) Creación de cuentas de administración para el despliegue.

    b) Realización de un inventario de los equipos desprotegidos localizados en la infraestructura de red.

    c) Creación de la estructura del árbol de equipos que alojará a los dispositivos desplegados y determina cómo se integrarán una vez que Adaptive Defense 360 esté instalado.

        - En el nodo **Todos** del árbol de equipos para moverlos de forma manual una vez haya terminado el despliegue.
        - En su grupo correspondiente según la dirección IP del equipo.
        - En el grupo del Directorio Activo al que pertenece el equipo.

    d) Asignación de configuraciones a los grupos del árbol de equipos. En el Apartado 7 FASE DE CONFIGURACIÓN se describen los diferentes procedimientos de configuración de los componentes de este producto.

    e) Revisión del acceso exitoso a los recursos de Adaptive Defense 360 en la nube.

    f) Revisión de la configuración de seguridad por defecto.

    g) Realización de comprobaciones finales.

5.1 ELABORAR UN INVENTARIO DE EQUIPOS DESPROTEGIDOS

34. 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. Una solución de ejemplo para realizar un descubrimiento e inventario de la red es **Panda Systems Management [REF12]**.

    b) **Descubrimiento automático**: descubre puestos de usuario y servidores Windows que no tengan Adaptive Defense 360 3.71.00 instalado.

35. Una vez efectuado el inventario de dispositivos a proteger, es necesario comprobar 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, será necesario adquirir las licencias necesarias.

Figura 5: Ventana de licencias

5.1.1 DESCUBRIMIENTO AUTOMÁTICO DE EQUIPOS SIN PROTEGER

36. 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 **Descubridor**.

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

5.1.1.1 REQUISITOS DE DESCUBRIMIENTO

37. 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 Descubridor deberá ser siempre un equipo Windows.

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

5.1.1.2 ASIGNAR EL ROL DESCUBRIDOR

38. Para asignar el rol Descubridor a un equipo Windows de la red, se seguirán los pasos siguientes:

    a) Hacer clic en el menú superior Configuración, panel lateral Servicios de red, pestaña Descubrimiento, botón Añadir equipo descubridor.

    b) Seleccionar de la lista el equipo al que se asignará el rol Descubridor. Se recomienda seleccionar equipos con recursos hardware suficientes y que estén en funcionamiento el mayor número de horas del día posibles.

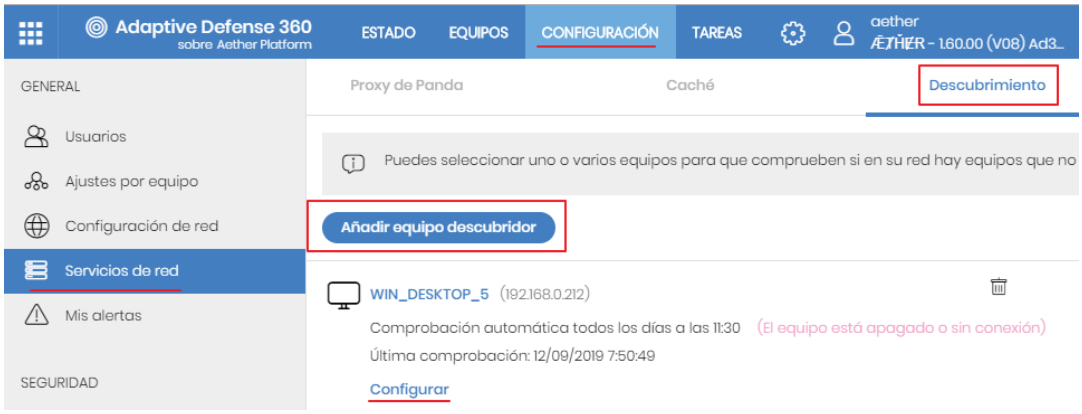

Figura 6: Añadir un equipo descubridor

5.1.1.3 CONFIGURAR EL ROL DE DESCUBRIDOR

39. A continuación, se configurará la tarea de descubrimiento que lanzará el equipo descubridor:

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

    b) **Ejecutar automáticamente**: hacer clic en el desplegable para establecer si la tarea de búsqueda se ejecutará de forma puntual (**No**) o programada (**Todos los días**). Si se selecciona **Todos los días**, es necesario seleccionar también en el desplegable la hora a la que se lanzará la tarea, así como la casilla de verificación **Hora local del dispositivo** 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**: buscar todos los equipos que pertenecen al segmento de red donde reside el equipo descubridor.

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

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

40. Para más información, se recomienda consultar el apartado “Descubrir equipos”, de la Guía de Administración del producto [REF4].

5.2 REVISAR EL ACCESO EXITOSO A LOS RECURSOS DE ADAPTIVE DEFENSE 360 EN LA NUBE

41. 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. Consultar el apartado 4.4.3 de este documento para ver el listado de las mencionadas URLs.

5.3 CREACIÓN DE LA ESTRUCTURA NECESARIA DEL ÁRBOL DE EQUIPOS

42. Para facilitar la asignación de configuraciones de seguridad, es necesario organizar los puestos de trabajo y servidores en diferentes grupos. Para esta tarea, Adaptive Defense 360 utiliza el **árbol de equipos**, accesible desde el menú superior **Equipos,** haciendo clic en el icono . Dependiendo del tipo de despliegue elegido, los puestos de usuario y servidores se integran en el grupo **Todos** del árbol de equipos o se mueven de forma automática a un grupo u otro dependiendo de ciertas reglas definidas por el Administrador. Este enfoque ahorra tiempo de gestión y simplifica las tareas del Administrador.

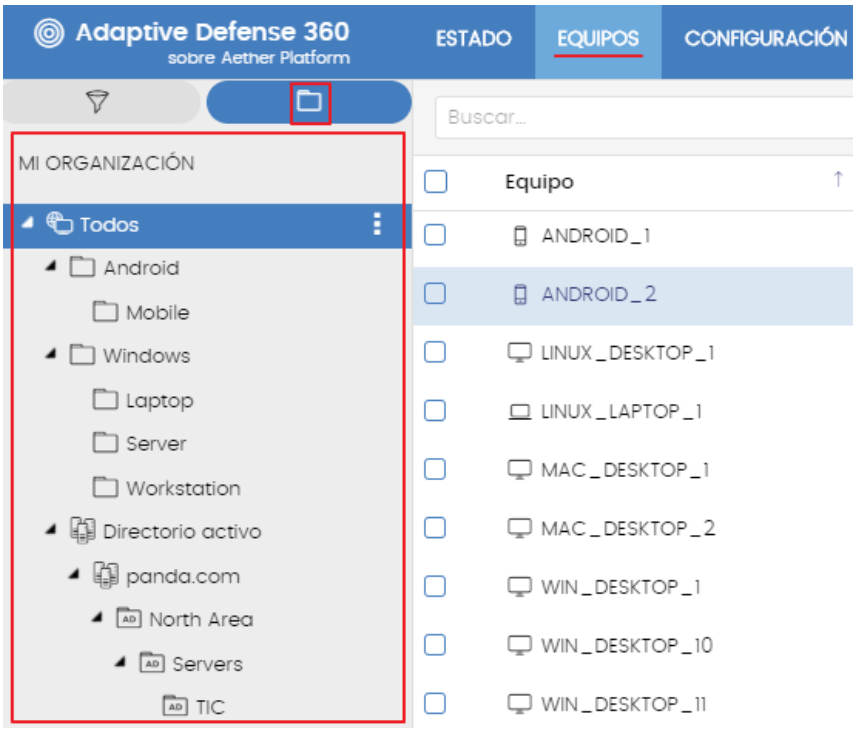

Figura 7: Vista general del árbol de equipos

43. La razón principal para mantener un árbol de equipos correctamente organizado es la de facilitar la asignación de configuraciones a los equipos con Adaptive Defense 360instalado: cada grupo del árbol de equipos tiene asignada una configuración que se aplica a todos los dispositivos que lo forman. De este modo, mover equipos de un grupo a otro permite cambiar de forma rápida la configuración aplicada, así como agrupar dispositivos de forma ágil para evitar la asignación individual de configuraciones.

44. Dependiendo de la forma en la que se asignan equipos a los grupos existentes, Adaptive Defense 360 implementa tres tipos distintos de grupos:

45. **Grupos nativos**: son los grupos estándar de Adaptive Defense 360 que soportan todas las operaciones (movimiento, renombrado, borrado etc.) Pueden contener otros grupos nativos y equipos.

46. **Grupos IP**: son grupos nativos que tienen asociado un rango de direcciones IP. Al integrar un nuevo equipo, Adaptive Defense 360consultará su IP y lo moverá de forma automática al grupo IP apropiado.

47. **Grupos Active Directory**: replican la estructura del Active Directory instalado en la empresa, y por esta razón tienen limitadas algunas operaciones. Pueden contener otros grupos de Active Directory y equipos.

5.3.1 CRITERIOS DE DISEÑO PARA EL ÁRBOL DE EQUIPOS

48. 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**: crear 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. El tipo de grupo que mejor encaja en este criterio es el grupo nativo.

    b) **Criterios de topología de red**: crear 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. El tipo de grupo que mejor encaja en este criterio es el grupo IP.

    c) **Criterios organizativos**: crear 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. El tipo de grupo que mejor encaja en este criterio es el grupo nativo o el grupo IP.

    d) **Criterios de función o rol del equipo**: crear grupos que contengan equipos que desempeñen funciones similares en la Organización. Por ejemplo, “grupo

servidores de correo" o "grupo servidores de impresión". El tipo de grupo que mejor encaja en este criterio es el grupo nativo.

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. El tipo de grupo que mejor encaja en este criterio es el grupo Active Directory.

f) **Sin criterio de diseño:** en redes de tamaño menor de 10 equipos, es habitual 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. El tipo de grupo que mejor encaja en este criterio es el grupo nativo.

5.3.2 GRUPOS NATIVOS

49. Los grupos nativos pueden utilizarse para gestionar el árbol de carpetas de forma manual. Para crear, modificar o borrar un grupo, hacer clic en el icono ⋮ de la rama del grupo donde se desee operar y elegir en el menú desplegable la operación.

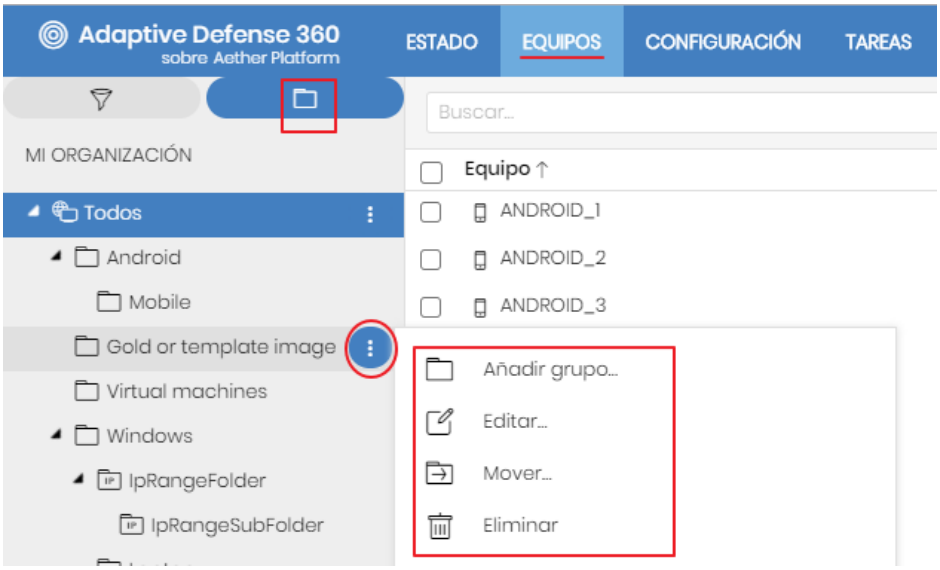

Figura 8: Acceso a las herramientas de gestión de grupos nativos

50. Crear, mover, borrar y renombrar grupos nativos son tareas que se realizarán en la zona superior del árbol de equipos (1 en la Figura 9). La zona inferior está reservada para los grupos de Active Directory. Estos grupos no se pueden modificar de forma directa.

5.3.3 GRUPOS IP

51. Los grupos IP son grupos nativos que tienen asociado un rango de IPs. Esta característica permite a Adaptive Defense 360 mover los equipos recién integrados en la plataforma al grupo apropiado, dependiendo de la dirección IP del dispositivo instalado.

52. Para crear un grupo IP deberán seguirse los pasos mostrados a continuación:

    a) Consultar el punto 49 para crear un grupo nativo.

    b) En la ventana Añadir grupo hacer clic en el enlace **Añadir reglas de asignación automática por IPs**.

    c) Escribir en la caja de texto los rangos de IPs asignados al grupo, utilizando el carácter "-" para separar el límite superior del inferior, o indica direcciones IP individuales separadas por el carácter ",".

5.3.4 GRUPOS DE DIRECTORIO ACTIVO Y GRUPOS NATIVOS/IP

53. El árbol de equipos se divide en dos secciones: la formada por los grupos nativos y grupos IP de Adaptive Defense 360 (1 en la Figura 10) y por los grupos de Directorio activo (2 en la Figura 11).

54. 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.

55. 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 web y el equipo aparecerá en el nuevo grupo.

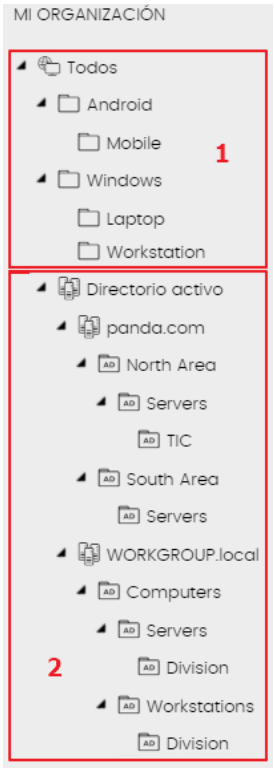

Figura 12: Zona de grupos nativos(1) y grupos de Directorio Activo (2)

5.3.5 GRUPOS Y ASIGNACIÓN DE CONFIGURACIONES DE SEGURIDAD

56. 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 sean tratados de igual manera desde el punto de vista de la seguridad.

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

5.4 REVISIÓN DE LA CONFIGURACIÓN DE SEGURIDAD POR DEFECTO

58. 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. Se puede revisar la configuración haciendo clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores > Configuración por defecto**. En el caso de que algún parámetro no sea adecuado para la red, se generará una nueva configuración de seguridad y se asignará a los equipos desplegados, para lo que se seguirán los pasos mostrados a continuación:

    a) Hacer 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) Indicar el nombre de la configuración y hacer clic en el link **Destinatarios No se ha asignado a ningún equipo**. Hacer clic en el icono de la sección **Grupos de equipos** y seleccionar el grupo **Todos**.

    c) Hacer clic en el link **Atrás** y desplegar las distintas secciones de la configuración de seguridad para modificar las opciones oportunas. Hacer clic en el botón **Guardar** para finalizar.

    d) Abrir nuevamente la configuración creada y hacer clic en **destinatarios**. Asignar el grupo **Todos**.

5.5 DESPLIEGUE DE FORMA ESCALONADA

59. Para minimizar problemas que afecten a los usuarios de los puestos de trabajo, es recomendable organizar un despliegue por fases, para lo cual deberán seguirse los siguientes pasos:

    a) Dividir el parque de equipos en varios grupos, dependiendo del total de puestos a instalar. Contactar con el TAM (*Technical Account Manager*) asignado para

recoger sugerencias acerca de la mejor manera de agrupar los equipos en cada Organización.

b) En el primer grupo, es recomendable seleccionar aquellos equipos más representativos de cada gama de hardware o software utilizado en la Organización. Incluir en cada grupo un único equipo por gama.

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

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

6. FASE DE INSTALACIÓN

60. Es posible desplegar Adaptive Defense 360 de forma local o remota dependiendo del tipo de equipo a instalar y de las herramientas implantadas en la Organización.

61. Independientemente del tipo de despliegue elegido, deberán seguirse los siguientes pasos:

    a) Seleccionar del tipo de plataforma a desplegar (Windows, Linux, MacOS, Linux o Android).

    b) Determina el tipo de integración en el árbol de equipos que se llevará a cabo.

    c) Asocia al paquete de instalación una configuración de red de las creadas en el punto 4.4.6 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. 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 red apropiada.

6.1 INSTALAR ADAPTIVE DEFENSE 360 DE FORMA LOCAL

62. Para acceder a la ventana de instalación se seguirán los pasos mostrados a continuación:

    a) Hacer clic en el menú superior **Equipos**, botón **Añadir equipos.**

    a) Seleccionar el Sistema Operativo de la ventana emergente: Windows, MacOS, Linux, Android.

Figura 13: Ventana de selección de plataforma a instalar

63. El procedimiento manual se aplica a equipos Windows, Linux y MacOS y obliga a seleccionar la forma de integración en el árbol de equipos:

    a) **Añadir los equipos al siguiente grupo (Todos)**: los equipos se asignarán al grupo **Todos** para que una vez instalado Adaptive Defense 360 el Administrador pueda realizar la asignación a su gusto.

b) **Añadir los equipos en su ruta de Active Directory**: la asignación del grupo es automática en función del grupo del Active Directory al que pertenezca el equipo.

c) **Seleccionar el grupo en función de la IP del equipo**: la asignación del grupo será automática en función de la IP del equipo.

Figura 14: Ventana de selección de integración

d) En el apartado **Selecciona el proxy e idioma para los equipos** indicar la configuración de red apropiada: si el equipo tiene salida directa a Internet, asignar **Configuración por defecto**. Si el equipo tiene salida a Internet mediante proxy corporativo o proxy Adaptive Defense 360, asignar la configuración de red apropiada.

64. Para dispositivos Android el procedimiento manual es ligeramente diferente:

a) Seleccionar el grupo donde será ubicado el equipo (**Todos**) y escanear el código QR mostrado en la ventana emergente con la cámara del propio teléfono móvil o *tablet*. **Los dispositivos Android no soportan la comunicación a través de proxy**.

b) Hacer 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.

6.2 INSTALAR ADAPTIVE DEFENSE 360 DE FORMA REMOTA

65. 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) Disponer de un equipo instalado y con el rol Descubridor asignado dentro de la misma subred donde se desplegará Adaptive Defense 360.

    b) El equipo descubridor ha efectuado 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) Deberá disponerse de acceso administrativo al recurso Admin$ (recurso que se usa durante la administración remota de un equipo) en la maquina a desplegar.

    d) Deberá disponerse de credenciales de administrador del dominio o del administrador local real, y la administración remota deberá estar activada.

66. Para instalar Adaptive Defense 360 de forma remota sin utilizar herramientas de distribución de software de terceros, deberán seguirse los pasos mostrados a continuación:

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

    b) Seleccionar el listado **Equipos no administrados descubiertos** y hacer 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 Adaptive Defense 360. Para determinar el tipo de integración del dispositivo en el árbol de equipos consultar el punto 48.

    d) Hacer clic en el botón **Instalar**. Transcurridos unos minutos, la instalación se habrá completado.

6.3 INSTALAR ADAPTIVE DEFENSE 360 DE FORMA REMOTA CON HERRAMIENTAS DE TERCEROS

67. 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. Para generar y descargar el paquete de instalación de Adaptive Defense 360, consultar el párrafo 61. Utilizar una línea de comandos similar a la mostrada a continuación:

```
Msiexec /i "PandaAetherAgent.msi"
    GROUPPATH="Madrid\Contabilidad"
    PRX_SERVER="ProxyCorporative" PRX_PORT="3128"
    PRX_USER="admin" PRX_PASS="panda"
```

GROUPPATH="grupo1\grupo2": ruta dentro del árbol de equipos donde se integrará el equipo. Si no se indica este parámetro o el grupo no existe, el equipo se integrará en el nodo raíz **Todos**.

PRX_SERVER: dirección IP o nombre del servidor proxy corporativo.

PRX_PORT: puerto del servidor proxy corporativo.

PRX_USER: usuario del servidor proxy corporativo.

PRX_PASS: contraseña del servidor proxy corporativo

6.4 INSTALAR ADAPTIVE DEFENSE 360 MEDIANTE MAQUETAS/IMÁGENES "GOLD"

68. Para acceder a la ventana de instalación deberán seguirse los pasos mostrados a continuación: 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.

69. La instalación del software Adaptive Defense 360 en cualquier equipo lleva asociada la asignación automática de un identificador único, que es utilizado para referenciarlo en la consola web. Si se genera una imagen base con el software 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.

70. 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 Panda Aether tool [REF7]. Es posible descargar el software y obtener instrucciones precisas según el tipo de entorno virtual desde la URL https://www.pandasecurity.com/spain/support/card?id=710050 **[REF2]** en la Web de soporte de Panda Security.

6.5 INSTALAR ADAPTIVE DEFENSE 360 EN UN ENTORNO VDI PERSISTENTE O EN UN EQUIPO FÍSICO

71. En entornos VDI persistentes o en hardware físico, los equipos conservan la información que han almacenado en el disco duro entre reinicios, y por esta razón el proceso de creación de imagen *gold* solo requiere de una única configuración de actualización para Adaptive Defense 360.

72. Una vez instalado el Sistema Operativo actualizado, e instalados todos los programas que los usuarios necesitarán, deberán seguirse los pasos mostrados a continuación:

a) Instalar el software cliente en el equipo según los pasos mostrados en el párrafo 62.

b) Comprobar que el equipo tiene conexión a Internet, y asignarle una configuración con la actualización de la protección y el conocimiento de Adaptive Defense 360 activadas. Consultar los párrafos 183 y 187.

c) Ejecutar la herramienta **Panda Aether tool** y hacer clic en el botón ***Start cache scan*** para analizar el equipo y precargar la cache de *goodware* de Adaptive Defense 360.

d) Hacer clic en el botón ***Unregister device*** para borrar el identificador del equipo. Es necesario asegurarse de que la casilla de selección ***Is a gold image*** NO está marcada.

e) Apagar el equipo y generar la imagen con el software de administración de entornos virtuales que utilices.

6.6 INSTALAR ADAPTIVE DEFENSE 360 EN UN ENTORNO VDI NO PERSISTENTE

73. En un entorno VDI no persistente son necesarias dos configuraciones de actualización de Adaptive Defense 360: una para actualizar la imagen *gold* en el momento de su preparación y mantenimiento, y otra para desactivar las actualizaciones en su ejecución, ya que no tiene sentido consumir ancho de banda para actualizar el software si el sistema de almacenamiento del equipo se va a revertir a su estado original en cada reinicio.

74. **Preparación de la imagen *gold***. Una vez instalado el Sistema Operativo actualizado y todos los programas que los usuarios necesitarán, sigue los pasos mostrados a continuación:

    a) Instalar el software cliente Adaptive Defense 360 según los pasos mostrados en el párrafo 59.

    b) Comprobar que el equipo tiene conexión a Internet y asignarle una configuración con la actualización de la protección y el conocimiento de Adaptive Defense 360 activadas. Consultar los párrafos 183 y 187.

    c) Ejecutar la herramienta **Panda Aether tool** y hacer clic en el botón ***Start cache scan*** para analizar el equipo y precargar la cache de *goodware* de Adaptive Defense 360.

    d) Hacer clic en el botón *Unregister device* para borrar el identificador del equipo y asegurarse de que la casilla de selección *Is a gold image* SÍ está marcada.

    e) Asignar al equipo una configuración que deshabilite la actualización de la protección y del conocimiento de Adaptive Defense 360. Consultar los párrafos 183 y 187.

f) Deshabilitar el servicio Panda Endpoint Agent desde el panel de servicios de Windows para que no arranque automáticamente al usar esta imagen *gold* en las instancias virtuales.

g) Apagar el equipo para generar la imagen con el software de administración de entornos virtuales que se utilicen.

h) En el menú superior Configuración, panel lateral Entornos VDI define el máximo número de equipos que estarán activos simultáneamente. Esto permitirá una gestión automática de las licencias que consumen estos equipos.

75. **Ejecutar el entorno VDI no persistente**: para que Adaptive Defense 360 se ejecute con normalidad, es necesario cambiar el tipo de inicio del servicio del agente, que previamente hemos deshabilitado en la imagen *gold*. Para ello, deberán seguirse los pasos mostrados a continuación:

a) Utilizar las herramientas de administración de GPO en un equipo físico conectado al dominio, y crear una GPO para cambiar el tipo de inicio del servicio Panda Endpoint Agent. Para conocer más detalles, se recomienda consultar la URL https://www.microsoft.com/es-ES/download/details.aspx?id=21895 **[REF3].**

b) Dentro de la configuración de GPO, navegar a la siguiente ruta: **Computer Configuration > Policies > Windows Settings > Security Settings > System Services > Panda Endpoint Agent**.

c) Cambiar la configuración del servicio a automática, para que se modifique en el siguiente arranque y así pueda integrarse con la consola.

76. **Mantener la imagen gold para entornos VDI no persistentes:** dado que los equipos VDI tienen asignada una configuración de actualización deshabilitada, es necesario actualizar la imagen gold de forma manual como mínimo una vez al mes para que reciba la última versión de la protección y del fichero de firmas. Para ello, es necesario acceder al equipo que tiene instalada la imagen gold y seguir los pasos mostrados a continuación:

a) Habilitar el servicio **Panda Endpoint Agent**.

b) Comprobar que el equipo tiene conexión a Internet y asignarle una configuración con la actualización de la protección y el conocimiento de Adaptive Defense 360activada. Consultar párrafos 183 y 187.

c) Ejecutar la herramienta **Panda Aether tool** y hacer clic en el botón **Start cache scan** para analizar el equipo y precargar la cache de goodware de Adaptive Defense 360.

d) Hacer clic en el botón **Unregister device** para borrar el identificador del equipo y asegurarse de que la casilla de selección **Is a gold image** SÍ está marcada.

e) Asignar al equipo una configuración que deshabilite la actualización de la protección y del conocimiento de Adaptive Defense 360. Consultar los párrafos 183 y 187.

f) Deshabilitar el servicio **Panda Endpoint Agent** para que no arranque automáticamente al usar esta imagen *gold* en las instancias virtuales.

g) Apagar el equipo para generar la imagen con el software de administración de entornos virtuales utilizados.

h) Sustituir en el entorno VDI la imagen anterior por la nueva obtenida.

i) Repetir este proceso de mantenimiento al menos una vez al mes.

6.7 COMPROBAR EL RESULTADO DE LA INSTALACIÓN

77. Para comprobar el resultado de la instalación, es necesario seguir los pasos mostrados a continuación:

a) Hacer 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 15: Widget con el estado del despliegue

78. Para más información acerca de la fase de instalación del producto, se recomienda consultar la **Guía de Buenas Prácticas para la Puesta en Marcha de Panda Adaptive Defense 360 sobre Aether [REF13]**.

7. FASE DE CONFIGURACIÓN

7.1 CATEGORÍAS Y ASIGNACIÓN DE CONFIGURACIONES

79. Las configuraciones ofrecen al Administrador un modo rápido de establecer los parámetros de seguridad, productividad y conectividad gestionados por Adaptive Defense 360 en los equipos que administran. Se soportan las siguientes categorías de configuraciones:

    a) **Ajustes por equipo**: definen el intervalo de actualizaciones del software en los equipos, la contraseña de instalación y la protección anti-*tamper*. Consultar los párrafos 185, 189 y 208.

    b) **Proxy e idioma**: definen el idioma del agente instalado en el equipo de usuario y establecen los parámetros necesarios para poder conectar con Internet.

    c) **Estaciones y servidores**: definen la configuración de seguridad de los equipos de la red Windows, MacOS y Linux, tanto de los puestos de trabajo como servidores. Consultar el párrafo 83.

    d) **Dispositivos Android**: define la configuración de seguridad y antirrobo de dispositivos Android (*tablets* y *smartphones*). Consultar el párrafo 117.

80. Para asignar una configuración a un grupo en el árbol de carpetas, deberán seguirse los pasos mostrados a continuación:

    a) Hacer clic en el menú superior **Equipos** y en el icono ⋮ del grupo al que se desee asignar la configuración.

    b) Hacer clic en el apartado **Configuraciones** del menú desplegado. Se mostrarán las categorías de configuraciones disponibles.

    c) Hacer clic en la categoría de configuración a asignar: se mostrarán las configuraciones disponibles de la categoría elegida. Elegir la configuración y ésta quedará asignada al grupo, de forma que todos sus miembros la reciban de forma inmediata.

7.1.1 GRUPOS DE EQUIPOS Y HERENCIA DE CONFIGURACIONES

81. 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 sin tener que especificarlas de forma individual por cada grupo.

82. 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 se desea esta nueva configuración.

7.2 CONFIGURACIONES DE SEGURIDAD

83. 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. En el apartado 7.15 CRITERIOS DE CONFIGURACIÓN DE ADAPTIVE DEFENSE 360 se puede consultar la tabla consolidada con las recomendaciones para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

7.2.1 PROTECCIÓN AVANZADA: *AUDIT, HARDENING, LOCK*

84. 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. Por esta razón, es capaz de detectar amenazas de tipo APT (*Advanced Persistent Threaths*) *Managed attacks* y amenazas desconocidas o especialmente complejas.

7.2.1.1 ACCESO A LA CONFIGURACIÓN DE PROTECCIÓN AVANZADA

85. Para visualizar o modificar la configuración de protección avanzada, hacer clic en el menú superior **Configuración**. En el menú lateral **Estaciones y servidores**, seleccionar una configuración de la lista y hacer clic en la sección **Protección avanzada**.

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

7.2.1.2 CONFIGURACIÓN RECOMENDADA

87. A continuación, se muestra la configuración recomendada del módulo **Protección avanzada** para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		BÁSICA	MEDIA	ALTA
Estaciones y servidores - Sección Protección avanzada - Modo de funcionamiento (Sólo 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

7.2.1.3 FUNCIONAMIENTO DE LA PROTECCIÓN AVANZADA

88. 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, independientemente de la clasificación obtenida. Las clasificaciones se muestran en el panel de control de Adaptive Defense 360. Se recomienda usas 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*. Se recomienda utilizar 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*.

7.2.1.4 PREPARACIÓN DE LA PROTECCIÓN AVANZADA

89. 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), por lo que los usuarios no podrán utilizar estos programas de forma temporal.

90. Adaptive Defense 360 requiere de cierta cantidad de tiempo para clasificar el software desconocido como *goodware* o malware. Durante este tiempo, se bloqueará la ejecución del software desconocido en el equipo del usuario,

impactando negativamente en su productividad. Para minimizar el tiempo de bloqueo, es recomendable preparar de antemano la ejecución del software nuevo antes de su instalación y uso masivo.

91. 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, se recomienda utilizar el PC de un usuario de la red o preparar un equipo dedicado a este objetivo. A este equipo se le asignará inicialmente una configuración de seguridad avanzada *Hardening*.

    b) **Instalación del software**: se instalará el software en el equipo de pruebas y se ejecutará 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, se registrarán 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*, deberá cambiarse la configuración a modo *Lock* y se volverá 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 se bloqueará definitivamente 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 Adaptive Defense 360**: Adaptive Defense 360 está configurado para no impactar en el rendimiento de la red en caso de tener que enviar ficheros a la nube. Se podrá contactar con el departamento de soporte para acelerar su envío.

7.2.2 PROTECCIÓN AVANZADA: ANTI-*EXPLOIT*

92. Los puestos de usuario pueden contener procesos vulnerables: programas con fallos de diseño que, aun 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.

7.2.2.1 ACCESO A LA CONFIGURACIÓN DE PROTECCIÓN ANTI-*EXPLOIT*

93. Para visualizar o modificar la configuración de protección anti-*exploit*, se hará clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, se seleccionará una configuración de la lista y se hará clic en la sección **Protección avanzada**.

94. Para activar la funcionalidad, hacer clic en el botón **Protección avanzada** y en **Anti-*Exploit***. Se seleccionará del desplegable **Modo de funcionamiento** uno de los dos modos de protección (**Auditar**, **Bloquear**) y las opciones de notificación (**Informar**, **Pedir permiso**).

7.2.2.2 CONFIGURACIÓN ANTI-EXPLOIT RECOMENDADA

95. A continuación, se muestra la configuración recomendada del módulo Protección Anti-*exploit* para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		BÁSICA	MEDIA	ALTA
Estaciones y servidores - Sección Protección avanzada– 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.

7.2.2.3 FUNCIONAMIENTO DE LA PROTECCIÓN ANTI-*EXPLOIT*

96. 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. No implica pérdida de información por parte del proceso afectado.

    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.

7.2.2.4 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.

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**.

7.2.3 PROTECCIÓN ANTIVIRUS PERMANENTE

97. 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 (una plataforma de conocimiento en la nube que aumenta exponencialmente la capacidad de detección). Esta plataforma consta de servidores que clasifican y procesan de forma automática toda la información que la comunidad de usuarios proporciona sobre las detecciones que se han producido en sus equipos. La protección Adaptive Defense 360 instalada en los equipos consulta a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección sin afectar negativamente al consumo de recursos.

98. 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.

7.2.3.1 ACCESO A LA CONFIGURACIÓN DE LA PROTECCIÓN ANTIVIRUS

99. Para visualizar o modificar la configuración de protección antivirus en puestos de trabajo Windows, Linux y MacOS, hacer clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, seleccionar una configuración de la lista y hacer clic en la sección **Antivirus**.

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

7.2.3.2 CONFIGURACIÓN ANTIVIRUS RECOMENDADA

101. A continuación, se muestra la configuración recomendada del módulo **Protección antivirus permanente** para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		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 y luego los analiza. Requiere un extra de recursos de procesamiento.	Op.	Op.	Op.
Analizar comprimidos en disco (No recomendado)	Descomprime y analiza los archivos encontrados en el sistema de ficheros. Requiere un extra de recursos de procesamiento.	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 recursos de procesamiento.	N.A	Op.	Aplica

7.2.3.3 RECOMENDACIONES DE LA PROTECCIÓN ANTIVIRUS

102. 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) Activar 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, activar 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, activar siempre **Antivirus para navegación web** para analizar los ficheros descargados con estas herramientas.

    d) Activar 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.

7.2.4 PROTECCIÓN FIREWALL

103. 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.

7.2.4.1 ACCESO A LA CONFIGURACIÓN DE FIREWALL

104. Para visualizar o modificar la configuración de protección Firewall, hacer clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, seleccionar una configuración de la lista y hacer clic en la sección **Firewall (equipos Windows)**.

7.2.4.2 CONFIGURACIÓN FIREWALL RECOMENDADA

105. A continuación, se muestra la configuración recomendada del módulo Firewall para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		BÁSICA	MEDIA	ALTA
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 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 Adaptive Defense 360	Agrega reglas básicas de protección de programas.	Op.	Aplica	Aplica
Reglas de conexión Activar las reglas de Adaptive Defense 360	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

7.2.4.3 FUNCIONAMIENTO DE LA PROTECCIÓN FIREWALL

7.2.4.3.1 MODOS DE FUNCIONAMIENTO

106. La protección firewall tiene dos modos de funcionamiento, activando o desactivando en la consola la opción "**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 medios 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.

7.2.4.3.2 TIPOS DE RED

107. 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 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 Adaptive Defense 360.

    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 los usuarios de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

    c) **Detectar automáticamente:** El tipo de red (red pública o red de confianza) se selecciona de forma automática en función de una serie de criterios definidos por el Administrador que el equipo protegido debe cumplir. Hacer clic en el enlace **Configurar reglas** para determinar cuándo un equipo está conectado a una red de confianza.

7.2.4.3.3 DETECTAR AUTOMÁTICAMENTE EL TIPO DE RED AL QUE SE CONECTA EL EQUIPO

108. Adaptive Defense 360 permite añadir uno o más criterios que el equipo protegido por el cortafuegos deberá cumplir para seleccionar de forma automática la configuración **Red de confianza**. Si ninguna de estas condiciones se cumple, el tipo de red establecido en la interfaz de red será **Red pública**.

109. Un criterio es una regla que determina si una interfaz de red del equipo se considera que está conectado a una red de confianza. Esta asociación se realiza mediante la

resolución de un dominio definido previamente en un servidor DNS interno de la empresa: si el equipo es capaz de conectar con el servidor DNS de la empresa y resolver el dominio configurado, querrá decir que está conectado a la red de la empresa y, por lo tanto, el cortafuegos puede asumir que el equipo se encuentra en una red de confianza. A continuación, se muestra un ejemplo de configuración completo:

NOTA: En este ejemplo se utilizará "miempresa.com" como la zona principal del cliente que quiere que sus equipos detecten de forma automática si están conectados a la red corporativa.

a) Añadir el registro de tipo A "*criteriocortafuegos*" en la zona "miempresa.com" del servidor DNS interno de la red, sin especificar dirección IP ya que no tendrá ninguna utilidad.

b) Según esta configuración, "criteriocortafuegos.miempresa.com" será el dominio que Adaptive Defense 360 intentará resolver para comprobar que se encuentra dentro de la red corporativa.

c) Reiniciar el servidor DNS para cargar la nueva configuración si fuera necesario, y comprobar que "criteriocortafuegos.miempresa.com" se resuelve correctamente desde todos los segmentos de la red interna con las herramientas **nslookup [REF8]**, **dig [REF 9]** o **host [REF10]**.

d) En la consola, hacer clic en el enlace **Configurar reglas** para determinar cuándo un equipo está conectado a una red de confianza. Se mostrará una ventana con los siguientes campos a completar:

- **Nombre del criterio**: indica un nombre descriptivo de la regla a configurar. Por ejemplo, "micriterioDNS".
- **Servidor DNS**: indica la dirección IP del servidor DNS de la red interna de la empresa que recibirá la petición de resolución.
- **Dominio**: indica la petición que el equipo enviará al servidor DNS para su resolución. Introduce "criteriocortafuegos.miempresa.com".

e) Hacer clic en el botón **Aceptar**, en el botón **Guardar** y nuevamente en el botón **Guardar**.

f) Una vez configurado y aplicado el criterio, el equipo intentará resolver el dominio "criteriocortafuegos.miempresa.com" en el servidor DNS especificado cada vez que se produzca un evento en la interfaz de red (conexión/desconexión, cambio de IP etc.). Si la resolución DNS es correcta, se asignará a la interfaz de red que se utilizó la configuración asignada a la red de confianza.

7.2.4.4 CONFIGURACIÓN DE LA PROTECCIÓN FIREWALL

7.2.4.4.1 REGLAS DE PROGRAMA

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

    a) Establecer la acción por defecto.

        - **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.
        - **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 Adaptive Defense 360**: activa las reglas generadas automáticamente para el tipo de red definido.

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

7.2.4.4.2 REGLAS DE CONEXIÓN

111. 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.

112. Se deberán seguir los pasos mostrados a continuación, en el orden indicado:

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

        - **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.
        - **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 Adaptive Defense 360**: activa las reglas generadas automáticamente para el tipo de red definido anteriormente.

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

7.2.4.5 CONFIGURACIÓN DE LA PROTECCIÓN CONTRA INTRUSIONES

113. 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 antemano.

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*:

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

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

7.2.5 PROTECCIÓN ANTIRROBO

114. La configuración de antirrobo permite enviar acciones a los dispositivos móviles para evitar la filtración de los datos que contienen o favorecer su localización en caso de pérdida o robo del terminal.

7.2.5.1 ACCESO A LA CONFIGURACIÓN DE LA PROTECCIÓN ANTIRROBO

115. Para visualizar o modificar la configuración de la protección antirrobo en dispositivos móviles Android, hacer clic en el menú superior **Configuración**, menú lateral **Dispositivos Android,** seleccionar una configuración de la lista y hacer clic en la sección **Antirrobo**.

116. Hacer clic el botón **Protección antirrobo** para activar la funcionalidad.

7.2.5.2 CONFIGURACIÓN DE LA PROTECCIÓN ANTIRROBO

117. A continuación, se muestra la configuración recomendada del módulo Bloqueo de programas para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		BÁSICA	MEDIA	ALTA
Dispositivos Android – Sección Antirrobo				
Protección antirrobo		Op.	Aplica	Aplica
Informar de la localización del dispositivo	El dispositivo envía sus coordenadas GPS a los servidores de Panda Security para poder geolocalizarlo.	Op.	Op.	Aplica
Sacar foto al tercer intento de desbloqueo y enviarla por email	Si el usuario del dispositivo falla tres veces consecutivas al desbloquearlo, se tomará una fotografía y se enviará por correo electrónico a las direcciones de correo separadas por coma introducidas en la caja de texto habilitada a tal efecto.	Op.	Aplica	Aplica
Permitir al usuario activar el modo privado	El usuario puede impedir la toma de fotografías y el registro de las coordenadas GPS del dispositivo y posterior envío al servidor de Panda Security, aunque el Administrador haya establecido esta configuración.	Op.	Aplica	N.A

7.2.5.3 CONTROL DE DISPOSITIVOS

118. 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.

7.2.5.4 ACCESO A LA CONFIGURACIÓN DE CONTROL DE DISPOSITIVOS

119. Para visualizar o modificar la configuración de protección Control de dispositivos, hacer clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, seleccionar una configuración de la lista y hacer clic en la sección **Control de dispositivos (Equipos Windows)**.

7.2.5.5 CONFIGURACIÓN CONTROL DE DISPOSITIVOS RECOMENDADA

120. A continuación, se muestra la configuración recomendada del módulo **Control de dispositivos** para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría 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

7.2.5.6 POLÍTICA DE CONTROL DE DISPOSITIVOS

121. 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.

7.2.5.7 CONFIGURACIÓN DEL CONTROL DE DISPOSITIVOS

122. El módulo **Control de dispositivos** de Adaptive Defense 360 establece limitaciones en el uso de grupos de periféricos. Para ello, deberá seleccionase el dispositivo o dispositivos que se desea autorizar y asignar un nivel de utilización de la siguiente manera:

a) Hacer clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, seleccionar la configuración de seguridad de la lista, hacer clic en la sección **Control de dispositivos (Equipos Windows)** y **Activar control de dispositivos**.

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

7.2.5.8 CONFIGURACIÓN DE LOS DISPOSITIVOS PERMITIDOS

123. 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**.

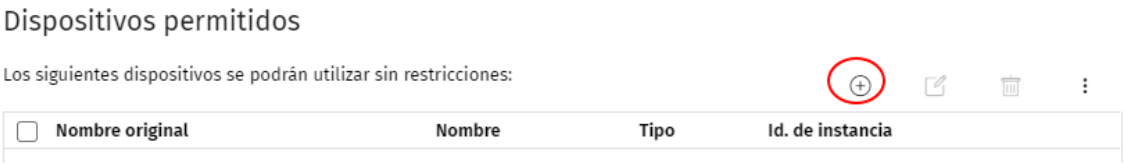

Figura 16: Añadir dispositivos permitidos

7.2.6 CONTROL DE ACCESO A PÁGINAS WEB

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

7.2.6.1 ACCESO A LA CONFIGURACIÓN DE CONTROL DE ACCESO A PÁGINAS WEB

125. 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**.

7.2.6.2 CONFIGURACIÓN DE CONTROL DE ACCESO A PÁGINAS WEB RECOMENDADA

126. A continuación, se muestra la configuración recomendada del módulo Acceso a páginas web para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría 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 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.

7.2.6.3 CONFIGURACIÓN DEL ACCESO A PÁGINAS WEB

127. 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 de las categorías de sitios web a las 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.

7.2.7 ANTIVIRUS PARA SERVIDOR EXCHANGE

128. 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.

129. 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.[2]

Modo de análisis	Antivirus para servidor Exchange
Buzón	2003, 2007, 2010
Transporte	2003, 2007, 2010, 2013, 2016, 2019

7.2.7.1 PROTECCIÓN DE BUZONES

130. 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.

7.2.7.2 PROTECCIÓN DE TRANSPORTE

131. Aplica a los servidores Exchange 2003, 2007, 2010, 2013, 2016 y 2019 con el rol de Acceso de clientes, *Edge Transport* y *Hub*, y permite analizar el tráfico que es atravesado por el servidor Microsoft Exchange.[3]

[2] Las versiones 2003, 2007 y 2010 de Windows Exchange se encuentran, a fecha de publicación de la presente guía, fuera de soporte de seguridad, por lo que no se recomienda su utilización.

[3] Las versiones 2003, 2007 y 2010 de Windows Exchange se encuentran, a fecha de publicación de la presente guía, fuera de soporte de seguridad, por lo que no se recomienda su utilización.

7.2.7.3 ACCESO A LA CONFIGURACIÓN DE LA PROTECCIÓN ANTIVIRUS PARA SERVIDORES EXCHANGE

132. 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**.

7.2.7.4 CONFIGURACIÓN ANTIVIRUS PARA SERVIDOR EXCHANGE RECOMENDADA

133. A continuación, se muestra la configuración recomendada del módulo Antivirus para servidor Exchange para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		BÁSICA	MEDIA	ALTA
Estaciones y servidores - Antivirus para servidores Exchange				
Activar protección de buzones	Analiza los mensajes de correo cuando se reciben y almacenan en la carpeta asignada al usuario. Al activar esta opción se muestra un mensaje en la consola para confirmar las exclusiones que se aplicarán en el análisis de los adjuntos para mejorar el rendimiento del equipo	Aplica	Aplica	Aplica
Activar protección de transporte	Analiza todo el tráfico que pasa por el servidor Exchange	N.A	Op.	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
Restauración de mensajes con virus y otras amenazas (nuevo)	Configura el servidor SMTP que reenviará los mensajes restaurados desde la consola web.	Op.	Op.	Op.

El servidor requiere autenticación (nuevo)	Haz clic en el botón de activación si el servidor SMTP no es "open relay".	Op.	Op.	Op.

7.2.8 ANTI-SPAM PARA SERVIDORES EXCHANGE

134. 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.

135. La protección antivirus para servidores Exchange es aplicable a las versiones 2003, 2007, 2010, 2013, 2016 y 2019 en modo transporte.[4]

7.2.8.1 ACCESO A LA CONFIGURACIÓN DE LA PROTECCIÓN ANTI-SPAM EXCHANGE

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

7.2.8.2 CONFIGURACIÓN ANTI-SPAM PARA SERVIDORES EXCHANGE RECOMENDADA

Funcionalidad	Descripción	Categoría		
		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.

[4] Las versiones 2003, 2007 y 2010 de Windows Exchange se encuentran, a fecha de publicación de la presente guía, fuera de soporte de seguridad, por lo que no se recomienda su utilización.

7.2.9 FILTRADO DE CONTENIDOS PARA SERVIDORES EXCHANGE

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

7.2.9.1 ACCESO A LA CONFIGURACIÓN DE FILTRADO DE CONTENIDOS PARA SERVIDORES EXCHANGE

138. Para visualizar o modificar la configuración de filtrado de contenidos en servidores Windows Exchange, hacer clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, seleccionar una configuración de la lista y hacer clic en la sección **Filtrado de contenidos para servidores Exchange**.

7.2.9.2 CONFIGURACIÓN DE FILTRADO DE CONTENIDOS PARA SERVIDORES EXCHANGE RECOMENDADA

139. A continuación, se muestra la configuración recomendada del módulo Filtrado de contenidos para servidores Exchange para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		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

7.2.10 CONFIGURACIÓN DE BLOQUEO PARA APLICACIONES

140. Para incrementar la seguridad de base en los equipos Windows de la red, se recomienda que el Administrador prohíba completamente la ejecución de los programas que considere peligrosos o no compatibles con la actividad desarrollada en la empresa.

7.2.10.1 ACCESO A LA CONFIGURACIÓN DEL BLOQUEO DE PROGRAMAS

141. Para visualizar o modificar la configuración de bloqueo de programas en puestos de trabajo Windows, hacer clic en el menú superior **Configuración**, menú lateral **Bloqueo de programas** y seleccionar una configuración de la lista.

142. Hacer clic en el botón **Activar bloqueo de aplicaciones** para activar la funcionalidad.

7.2.10.2 CONFIGURACIÓN DE BLOQUEO DE PROGRAMAS RECOMENDADA

143. A continuación, se muestra la configuración recomendada del módulo Bloqueo de programas para las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		Básica	Media	Alta
Bloqueo de programas				
Activar bloqueo de aplicaciones		Op.	Aplica	Aplica
Introduce los nombres de los programas que quieres bloquear:	Nombres de los ficheros a los que Adaptive Defense 360 impedirá su ejecución. En esta caja de texto acepta listas de nombres de ficheros copiadas / pegadas y separados por retorno de carro. No se admiten comodines para evitar configuraciones demasiado amplias que comprometan el buen funcionamiento del equipo.	Op.	Aplica	Aplica
Introduce los códigos MD5 de los programas que quieres bloquear:	MD5 de los ficheros a los que Adaptive Defense 360 impedirá su ejecución. En esta caja de texto acepta listas de MD5s copiadas / pegadas y separados por retorno de carro.	Op.	Aplica	Aplica
Informar a los usuarios de los equipos de los bloqueos	Muestra una ventana desplegable al usuario del equipo indicando el motivo por el cual la ejecución del programa se encuentra bloqueada.	Op.	Aplica	Op.

7.2.10.3 RECOMENDACIONES DEL BLOQUEO DE PROGRAMAS

144. Las causas que pueden llevar a un Administrador a prohibir la ejecución de un determinado programa pueden ser variadas:

a) Programas que por su forma de ejecución consumen mucho ancho de banda o establecen un número de conexiones desproporcionadamente alto, poniendo en peligro el rendimiento de la conectividad de la empresa si son ejecutados por muchos usuarios concurrentes.

b) Programas que permiten acceder a contenidos susceptibles de contener amenazas de seguridad o a contenidos protegidos por licencias que la empresa no posee.

c) Programas que permiten acceder a contenidos no relacionados con la actividad de la empresa y que pueden afectar al rendimiento de los usuarios.

145. No deberán bloquearse programas del Sistema Operativo o componentes que sean necesarios para poder ejecutar correctamente los programas de usuario. Adaptive Defense 360 no bloqueará ninguno de sus programas o módulos para garantizar el correcto funcionamiento de la solución de seguridad instalada.

7.3 AUTENTICACIÓN

146. 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.

147. 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).

7.3.1 AUTENTICACIÓN BÁSICA

148. Para crear una cuenta de acceso a la consola web 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) Hacer clic en el menú superior **Configuración**, menú lateral **Usuarios**, botón **Añadir.**

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

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

7.3.2 AUTENTICACIÓN DE DOS FACTORES (2FA)

149. 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.

7.3.2.1 REQUISITOS DE 2FA

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

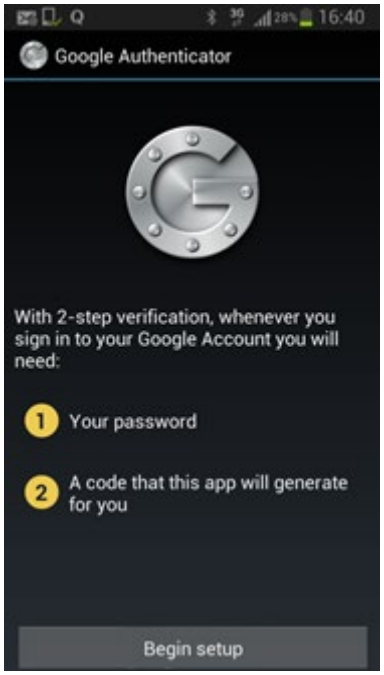

Figura 17: Google Authenticator

7.3.2.2 ACTIVACIÓN DE 2FA

a) Inicia la sesión en la consola web con la cuenta en la 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**.

151. Para más información sobre cómo llevar a cabo el proceso de activación de la Autenticación de doble factor, se recomienda consultar el siguiente enlace: https://www.pandasecurity.com/es/support/card?id=700088 **[REF14]**

7.3.2.3 ACCESO A LA CONSOLA WEB 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.

7.3.2.4 FORZAR LA ACTIVACIÓN DE 2FA A TODOS LOS USUARIOS DE LA CONSOLA

152. Para forzar la activación de 2FA a todos los usuarios de la consola es necesario que la cuenta de usuario que forzará la activación tenga permisos de "Gestionar usuarios y roles", y que además tenga visibilidad completa sobre el parque de usuarios.

a) En el menú superior **Configuración**, hacer clic en la pestaña **Seguridad**.

b) Activar la opción **Exigir tener activada la verificación en dos pasos para acceder a esta cuenta**.

c) Si la cuenta de usuario que activa la funcionalidad 2FA para todos los usuarios de la consola no tiene activada la verificación en dos pasos para su propia cuenta, se mostrará una ventana de aviso que le permitirá acceder a la **Cuenta Adaptive Defense 360** para activarlo.

7.4 ADMINISTRACIÓN DEL PRODUCTO

7.4.1 CREACIÓN DE CUENTAS DE ADMINISTRACIÓN

153. Creación de cuentas de administración a través de la consola web:

a) 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.

b) 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.

7.4.1.1 CREACIÓN DE UNA CUENTA DE ADMINISTRACIÓN PARA EL DESPLIEGUE INICIAL DE ADAPTIVE DEFENSE 360

154. A continuación, se enumeran los pasos a seguir para llevar a cabo la creación de una cuenta de administración con permisos para hacer un despliegue de Adaptive Defense 360:

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

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

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

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

e) Seleccionar los permisos Añadir, descubrir y eliminar equipos, Modificar configuración de red (proxys y caché), Configurar ajustes por equipo (actualizaciones, contraseñas, etc.), Reiniciar y reparar equipos, Asignar licencias, Configurar seguridad para estaciones y servidores, Configurar seguridad para dispositivos Android, Utilizar la protección antirrobo para

dispositivos Android (localizar, borrar, bloquear, etc.), Configurar bloqueo de programas y desactiva el resto de los permisos.

155. 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 web. Además, permite establecer un ámbito o alcance formado por grupos de equipos que serán gestionables por el Administrador.

7.4.2 CREACIÓN Y CONFIGURACIÓN DE ROLES

156. Un rol es una configuración específica de permisos de acceso a la consola, que se aplica a una o más cuentas de usuario. De esta forma, un administrador concreto está autorizado a ver o modificar determinados recursos de la consola, dependiendo del rol asignado a la cuenta de usuario con la que accedió a Adaptive Defense 360.

157. A continuación, se muestra la estructura de un rol:

a) **Nombre del rol:** designado en el momento de la creación del rol.

b) **Grupos sobre los que tiene permisos:** restringe el acceso a determinados equipos de la red. Para configurar esta restricción, es necesario especificar las carpetas del árbol de grupos a las cuales la cuenta de usuario tiene acceso.

c) **Juego de permisos:** determina las acciones concretas que las cuentas de usuario pueden ejecutar sobre los equipos que pertenecen a los grupos definidos como accesibles.

158. A continuación, se enumeran los tipos de roles disponibles, así como sus características asociadas:

a) Rol Control Total

- Una licencia de uso de Adaptive Defense 360 incluye un rol de Control Total predefinido. A este rol pertenece la cuenta de administración creada por defecto, y con ella es posible ejecutar todas las acciones disponibles en la consola sobre los equipos integrados en Adaptive Defense 360.
- El rol Control Total no se puede borrar, modificar, ni acceder a sus detalles. Cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola Web.

b) Rol Solo Lectura

- Este rol permite el acceso a todos los componentes de la consola, pero no permite crear, modificar o borrar configuraciones, tareas, etc. Por lo que permite una visión total del entorno, pero sin ninguna interacción. Está especialmente indicado para aquellos administradores de red encargados de la vigilancia del parque informático, pero no poseen los permisos suficientes para realizar modificaciones, como por ejemplo editar configuraciones o lanzar análisis bajo demanda.

- El rol Solo Lectura no se puede borrar, modificar ni acceder a sus detalles. Cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola Web.

159. Para crear o modificar un rol deberán seguirse los pasos mostrados a continuación:

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

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

c) Introducir el nombre y descripción.

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

e) Activar o desactivar los permisos asignados al rol.

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

7.4.2.1 CRITERIOS PARA LA CREACIÓN DE ROLES

160. 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 *tablets*, servidores de correo etc.

161. Para más información, se recomienda consultar el apartado “Concepto de rol” de la Guía de Administración del producto **[REF4]**.

7.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

162. Para acceder a la consola web, la comunicación se realizará a través del puerto 443 con la última versión de un navegador compatible. Se recomienda consultar el punto 23 de este documento.

163. Como requisito para plataformas macOS, se requieren libres los puertos 3127, 3128, 3129 y 8310 para el funcionamiento del filtrado web y la detección web del malware.

164. Para que el servicio de protección funcione correctamente es necesario que los equipos de la red puedan conectar con los servidores. Consulta el punto 4.4.3 para obtener un listado de URLs que deben ser accesibles por los equipos de la red.

165. Para poder instalar Adaptive Defense 360 de forma remota, es necesario que los equipos cumplan con los requisitos indicados a continuación:

    a) Abrir los puertos UDP 21226 y 137 para el proceso *System.*

    b) Abrir el puerto TCP 445 para el proceso *System*.

    c) Habilitar el protocolo NetBIOS sobre TCP.

    d) Permitir las resoluciones DNS.

    e) Habilitar la administración remota.

166. Requisitos para usar un equipo con el rol de caché en modo automático:

    a) Configurar el cortafuegos para permitir el tráfico SSDP (uPnP) entrante y saliente en el puerto UDP 21226 y 18226 TCP.

7.6 GESTIÓN DE CERTIFICADOS

167. Para el funcionamiento correcto del producto, es necesario mantener actualizados los certificados incluidos en los equipos de usuario y servidores que tengan el Sistema Operativo Windows instalado. En caso de no cumplir este requisito, algunas funcionalidades, como la comunicación en tiempo real del producto con la consola de administración, podrían dejar de funcionar.

168. El propio Sistema Operativo Windows mantiene actualizados los certificados raíz a través del servicio Windows Update. Para los equipos que presentan problemas de actualización o tienen este servicio deshabilitado, Panda Security ofrece una herramienta que comprueba de forma automática la validez de los certificados instalados del Sistema Operativo, y descarga aquellos que falten o no estén actualizados. La herramienta, denominada "**wescertcheck**", es accesible desde la URL https://www.pandasecurity.com/resources/tools/wescertcheck.zip **[REF5]**

7.7 SERVIDORES DE AUTENTICACIÓN

169. Dado que se trata de un servicio gestionado, el cliente Adaptive Defense 360 no requiere configurar integraciones con software o productos de terceros.

7.8 SINCRONIZACIÓN

170. Se recomienda sincronizar la fecha y hora de los equipos protegidos, por ejemplo, empleando un servidor NTP. Aunque no representan un problema estricto de

seguridad, los equipos con un desfase horario pueden mostrar los siguientes problemas:

a) Si el desfase es mayor de 5 minutos se pueden presentar fallos esporádicos en la conexión con la nube.

b) Los eventos mostrados en los informes aparecen con la fecha del equipo donde se detectó: se mostrará falseada si es una fecha anterior, o no se mostrará el evento en absoluto si es una fecha posterior, hasta que la fecha registrada sea anterior a la real.

c) Las comprobaciones de certificados pueden fallar en función de si eran válidos o habían expirados en esa fecha. En caso de fallo, la comunicación en tiempo real se perderá, aunque no afecta a otros tipos de comunicación.

d) Las tareas de análisis mostrarán fechas que no se corresponden con la realidad.

e) El filtrado web por franjas horarias no funcionará como se espera.

171. Para más información al respecto, se recomienda consultar el apartado "Sincronización horaria de los equipos (NTP)" de la Guía de Administración del producto **[REF4]**.

7.9 ACTUALIZACIONES

172. Adaptive Defense 360 es un servicio *cloud* gestionado, por esta razón las Organizaciones no necesitan implantar procedimientos que actualicen las infraestructuras que soportan los servicios de protección; sin embargo, sí es necesaria la actualización del software instalado en los equipos de la red, así como iniciar la actualización de la consola de administración, en caso de que así se desee.

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

a) Agente de comunicaciones Adaptive Defense 360.

b) Motor de la protección Adaptive Defense 360.

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

174. 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 Adaptive Defense 360	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.

7.9.1 CONFIGURACIÓN DE EQUIPOS CACHE

175. 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.

7.9.1.1 ASIGNACIÓN DEL ROL CACHE

176. Para asignar el rol de caché a un equipo Windows de la red, deberán seguirse los pasos descritos a continuación:

a) Hacer clic en el menú superior Configuración, menú lateral Configuración de red, pestaña Caché, botón Utilizar automáticamente los equipos caché vistos en la red o Utilizar los siguientes equipos caché (por orden de preferencia).

b) Seleccionar 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.

7.9.1.2 REQUISITOS DE CACHE

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

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

7.9.2 ACTUALIZACIÓN DEL AGENTE DE COMUNICACIONES

179. Es el componente software instalado en los puestos de usuario y servidores que hace de puente entre el módulo de protección y la nube. El agente Adaptive Defense 360 gestiona las comunicaciones, eventos y configuraciones de seguridad implementadas por el Administrador desde la consola web.

180. La actualización del agente se ejecuta bajo demanda. Adaptive Defense 360 incluirá una notificación en la consola de administración indicando la existencia de una nueva versión del agente, y el administrador podrá lanzar la actualización cuando lo desee. La actualización del agente no requiere reinicio del equipo del usuario.

181. Para comprobar la versión del agente publicado Adaptive Defense 360, hacer clic en el icono del menú superior y en el menú **Acerca de**. Se mostrará una ventana con la información del agente publicado.

7.9.3 ACTUALIZACIÓN DEL MOTOR DE PROTECCIÓN ADAPTIVE DEFENSE 360

182. 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.

7.9.3.1 ACCESO A LA CONFIGURACIÓN DE ACTUALIZACIONES DEL MOTOR DE PROTECCIÓN

183. Para visualizar o modificar la configuración de la actualización del motor de protección Adaptive Defense 360, se seguirán los pasos mostrados a continuación:

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

b) En la sección Actualizaciones activar Actualizar automáticamente Adaptive Defense 360 en los equipos.

c) Configurar cuándo se actualizará el motor de protección. Adaptive Defense 360 permite definir fechas y períodos configurables de actualización, así como la aplicación de actualizaciones en cualquier momento.

- Seleccionar la franja horaria o **A cualquier hora.**
- Seleccionar la fecha de actualización.

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

184. Para más información, se recomienda consultar el apartado “Actualización del motor de protección”, de la Guía de Administración del producto **[REF4]**.

7.9.3.2 CONFIGURACIÓN DE ACTUALIZACIÓN DEL MOTOR DE PROTECCIÓN RECOMENDADA

185. A continuación, se muestra la configuración recomendada para la actualización del motor de protección en las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		BÁSICA	MEDIA	ALTA
Ajustes por equipo – Sección Actualizaciones				
Actualizar automáticamente Adaptive Defense 360 en los equipos	Actualiza el motor de protección cuando se detecte una nueva versión publicada en los servidores de Panda.	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.

7.9.4 ACTUALIZACIÓN DEL ARCHIVO DE IDENTIFICADORES/FICHERO DE FIRMAS PARA LA PROTECCIÓN ANTIVIRUS TRADICIONAL

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

7.9.4.1 ACCESO A LA CONFIGURACIÓN DE LA ACTUALIZACIÓN DEL FICHERO DE FIRMAS

187. Para visualizar o modificar la configuración de la actualización del motor de protección Adaptive Defense 360 en equipos Windows, Linux y MacOS, se seguirán los pasos mostrados a continuación:

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

b) En la sección **General > Actualizaciones** activar **Actualizaciones automáticas de conocimiento**.

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

188. Para visualizar o modificar la configuración de la actualización del motor de protección en dispositivos Android, deberán seguirse los pasos mostrados a continuación:

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

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

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

d) Si se ha creado una nueva configuración, deberá asignarse a los grupos de equipos pertinentes en el árbol de equipos.

7.9.4.2 CONFIGURACIÓN DE LA ACTUALIZACIÓN DEL FICHERO DE FIRMAS RECOMENDADA

189. A continuación, se muestra la configuración recomendada para la actualización del fichero de firmas en las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		BÁSICA	MEDIA	ALTA
Seguridad (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.

190. Para más información, consultar el apartado “Actualización del conocimiento” de la Guía de Administración del producto **[REF4]**.

7.9.5 ACTUALIZACIÓN DE LA CONSOLA DE ADMINISTRACIÓN

191. El administrador de la red puede indicar el momento en el que iniciar el proceso para actualizar la versión de la consola en los servidores. En caso contrario, Adaptive Defense 360 actualizará de forma automática a la consola de administración a la última versión disponible.

192. A continuación, se enumeran los pasos para llevar a cabo la actualización de la consola de administración:

a) Hacer clic en el icono **Notificaciones web** situado en la parte derecha del menú superior. Se desplegarán las notificaciones pendientes de leer.

b) Si hay una actualización de la consola disponible, se muestra el mensaje **Nueva versión de la consola de Administración** con el enlace **Nuevas características y mejoras,** la versión de la consola a la que se actualizará, y el botón **Actualizar la consola ahora.**

c) Al hacer clic en el botón, la petición de actualización entra en la cola del servidor para ser procesada. El tiempo de permanencia máximo de la petición en la cola del servidor son 10 minutos.

d) Una vez procesada la petición, se inicia el proceso de actualización y la notificación muestra el texto **Actualización en curso**. Si alguna cuenta de usuario inicia la sesión en la consola será expulsada y, mientras dure el proceso de actualización, no será posible iniciar sesión en la consola de administración.

e) Al cabo de un tiempo que depende del número de equipos administrados y de los datos almacenados en la consola, se finalizará el proceso de actualización a la nueva versión.

193. Para más información, consultar el apartado **Actualización del producto**, de la Guía de Administración del producto **[REF4]**.

7.10 ALTA DISPONIBILIDAD

194. Adaptive Defense 360 es una plataforma alojada en Azure, operativa el 99.9% del tiempo. Se recomienda consultar el SLA (*Service Level Agreement*) de Azure, en el enlace https://azure.microsoft.com/es-es/support/legal/sla/summary/ **[REF6]**, para obtener una descripción detallada de los compromisos de disponibilidad de los diferentes módulos que componen esta plataforma.

7.11 REGISTRO Y AUDITORÍA

195. Adaptive Defense 360 registra todas las acciones efectuadas por los administradores de red en la consola web de gestión para determinar quién realizó un cambio, en qué momento y sobre qué elemento.

a) Registro de sesiones.

- La sección de sesiones lista todos los accesos a la consola de administración, los exporta a formato CSV y filtra la información. En el listado de sesiones se muestra la fecha y hora en la que se produjo el acceso, el usuario que llevó a cabo el acceso, la actividad ejecutada por esa cuenta, y la dirección IP desde la que se produjo el acceso.

b) Registro de acciones de usuario.

- La sección de Acciones de usuario lista todas las acciones ejecutadas por las cuentas de usuario, exporta las acciones a formato CSV y filtra la información. En el listado de acciones se muestra la fecha y hora en la que

se produjo la acción, el tipo de operación ejecutada, el tipo del objeto de la consola sobre el cual se ejecutó la acción, y el objeto de la consola sobre el cual se ejecutó la acción.

c) Eventos del sistema.

- Lista los eventos que se producen en Adaptive Defense 360 y que no tienen una cuenta de usuario como origen, sino que son desencadenados por el propio sistema.

7.11.1 ACCESO A LA ACTIVIDAD DEL ADMINISTRADOR

196. Para mostrar la actividad del Administrador en la consola web deberán seguirse los pasos mostrados a continuación:

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

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

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

7.11.2 ACCESO A LOS EVENTOS DEL SISTEMA

197. Para mostrar la actividad de Adaptive Defense 360 en la consola web, seguir los pasos mostrados a continuación:

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

b) Seleccionar el tipo de información a mostrar en el listado: **Eventos del sistema** y el intervalo a mostrar.

7.12 BACKUP

7.12.1 BACKUP DE FICHEROS BORRADOS POR PANDA DATA CONTROL

198. Los ficheros borrados por Panda Data Control **[REF11]** no se eliminan definitivamente del disco duro de los equipos. En su lugar se mueven a un área de *backup* donde residen durante 30 días, pasados los cuales el fichero es eliminado por completo. Esta área es excluida automáticamente del inventario, de las búsquedas y de la monitorización de ficheros, y es inaccesible para el software instalado en el equipo de usuario.

7.12.2 RESTAURACIÓN DE FICHEROS PREVIAMENTE BORRADOS POR EL ADMINISTRADOR

199. Panda Data Control permite la restauración en su ruta original de los ficheros previamente borrados por el administrador desde la consola, siempre que estos ficheros se encuentren en el área de *backup*. La restauración de estos ficheros es iniciada por el administrador de la red desde la consola, y se produce cuando el agente recibe una petición desde el servidor.

200. A continuación, se enumeran los pasos a seguir para restaurar los ficheros borrados por el administrador.

a) Acceso a la funcionalidad de restauración:

- En el menú superior **estado**, panel lateral **Mis listados** hacer clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.
- Elegir el listado **Archivos eliminados por el administrador**. Se mostrará el listado de ficheros PII encontrados en la red que el administrador borró o restauró previamente.
- En el menú superior **Estado**, panel lateral Panda Data Control hacer clic en el widget **Archivos eliminados por el administrador**. Se abrirá el listado **Archivos eliminados por el administrador** sin filtros preconfigurados.

b) Para restaurar varios ficheros:

- Hacer clic en las casillas de selección asociadas a los ficheros a recuperar.
- Hacer clic en el icono de la parte superior de la ventana. Se mostrará una ventana pidiendo confirmación.
- Si se confirma la recuperación del fichero, éste pasará al estado **Restaurando**.

c) Para restaurar un único fichero:

- Utilizar el menú de contexto asociado al fichero que se desee recuperar.
- Hacer clic en la opción **Restaurar**. Se mostrará una ventana pidiendo confirmación.
- Si se confirma la recuperación del fichero, éste pasará al estado **Restaurando**.

7.12.3 GESTIÓN DE LA ZONA DE BACKUP/CUARENTENA

201. La cuarentena en Adaptive Defense 360 es el área de *backup* donde se copian los elementos eliminados por haber sido clasificados como amenaza. Los elementos eliminados se almacenan en el propio equipo del usuario, en el directorio *Quarantine* de la carpeta donde se instaló el software. Se trata de una carpeta inaccesible al resto de procesos del equipo y cifrada, de manera que no es posible

el acceso ni la ejecución de los programas allí contenidos de forma directa, si no es a través de la consola Web.

202. Adaptive Defense 360 no borra ningún fichero del equipo del usuario. Todos los elementos eliminados son enviados al área de *backup*.

7.12.4 RESTAURACIÓN DE ELEMENTOS EN CUARENTENA

203. El administrador visualiza los elementos introducidos en cuarentena mediante los listados y los widgets del panel de control indiciados a continuación:

a) Actividad de malware.

b) Actividad de PUPs.

c) Amenazas detectadas por el antivirus.

204. Para obtener el listado de elementos introducidos en cuarenta es posible utilizar la herramienta de filtrado **Acción**, asignarla a **Movido a cuarentena o eliminado** y hacer clic en el botón **Filtrar**.

205. Para restaurar elementos de la cuarentena hacer clic en el botón **Restaurar y no volver a detectar**. Esta acción no solo copia el fichero a su ubicación original, sino que restaura los permisos, propietario, entradas del registro referidas al fichero y otra información. A continuación, se enumeran los pasos a seguir para restaurar desde la cuarentena/*backup* un elemento borrado, y no volver a detectarlo:

a) Hacer clic en el menú superior **Estado**, panel lateral **Seguridad**.

b) Hacer clic en el panel apropiado según el tipo de elemento a restaurar de la cuarentena: **Actividad del malware**, **Actividad de PUPs**, **Actividad de Exploits** o **Amenazas detectadas por el Antivirus.**

c) En el listado, seleccionar la amenaza cuyo campo **Acción** muestre **Movido a Cuarentena** o **desinfectado**.

d) Hacer clic en el icono del campo **Acción**. Se mostrará una ventana explicando el motivo del movimiento del elemento a cuarentena.

e) Hacer clic en el enlace **Restaurar y no volver a detectar**. El elemento se moverá a su ubicación original. Se restaurarán también los permisos, propietario, entradas del registro referidas al fichero y otra información.

7.13 SEGURIDAD DEL AGENTE

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

7.13.1 ACCESO A LA CONFIGURACIÓN DE SEGURIDAD FRENTE A MANIPULACIONES NO DESEADAS DE LAS PROTECCIONES

207. Para visualizar o modificar la configuración de la seguridad frente a manipulaciones no deseadas de las protecciones, hacer clic en el menú superior **Configuración**,

menú lateral **Ajustes por equipo**, seleccionar una configuración de la lista y en la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**, activar las opciones necesarias.

7.13.2 CONFIGURACIÓN RECOMENDADA DE LA SEGURIDAD DEL AGENTE

208. A continuación, se muestra la configuración recomendada para la seguridad del agente en las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		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 autorizado 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

7.13.2.1 PROTECCIÓN DEL AGENTE MEDIANTE CONTRASEÑA

209. Para evitar que el usuario modifique las características de protección o desinstale completamente el software, el administrador puede establecer una contraseña local.

210. A continuación, se indican los pasos a seguir para establecer una contraseña local:

a) Hacer clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.

b) Hacer clic en una configuración existente, o seleccionar **Añadir** para crear una nueva.

c) Desplegar la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**:

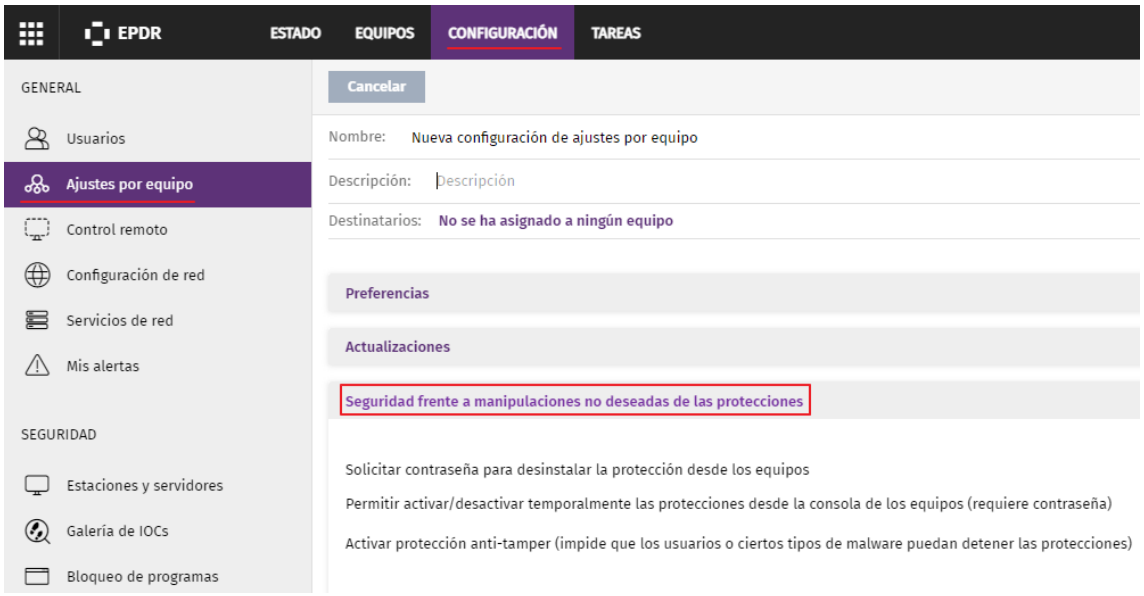

Figura 18: Menú Configuración > Ajustes por equipo > Seguridad frente a manipulaciones no deseadas de las protecciones

- **Solicitar contraseña para desinstalar Adaptive Defense 360 desde los equipos**: evita que el usuario desinstale el software protegiéndolo con una contraseña.
- **Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos**: permite administrar las capacidades de seguridad del equipo desde la consola local. Requiere el establecimiento de una contraseña.

7.14 USO DE LA RED Y PRIVACIDAD

211. 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 mostrados en la consola web. 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.

212. A continuación, se incluyen diferentes parámetros referentes a acciones ejecutadas por un malware, y detectadas por Adaptive Defense 360. Para más información, se recomienda consultar el apartado “Campos mostrados en fichero exportado” en el

punto "Listado de Actividad de malware / PUP", página 454 de la Guía de Administración del producto **[REF4]**.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado la amenaza.	Cadena de caracteres
Amenaza	Nombre de la amenaza detectada.	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado.	Cadena de caracteres
Acción	Acción aplicada sobre el malware.	- Movido a cuarentena - Bloqueado - Desinfectado - Eliminado - Permitido
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos	Binario
Excluido	La amenaza ha sido excluida por el administrador para permitir su ejecución.	Binario
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual la amenaza se ha ejecutado.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Equipo origen de la infección	Nombre del equipo si el intento de infección viene de un equipo de la red del cliente	Cadena de caracteres
IP origen de la infección	Dirección IP del equipo si el intento de infección viene de un equipo de la red del cliente.	Cadena de caracteres
Usuario origen de la infección	Usuario registrado en el equipo origen de la infección.	Cadena de caracteres.

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

214. Para más información, consultar los apartados "**Privacidad**" y "**Uso de la red**", de la Guía de Administración del producto **[REF4]**.

7.14.1 ACCESO A LA CONFIGURACIÓN DEL USO DE LA RED Y DE LA PRIVACIDAD

215. 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, hacer clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**, seleccionar una configuración de la lista y en la sección **Protección avanzada** indicar las opciones siguientes:

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

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

7.14.2 CONFIGURACIÓN RECOMENDADA DEL USO DE LA RED Y LA PRIVACIDAD

216. A continuación, se muestra la configuración recomendada para el uso de la red y la privacidad en las tres categorías de sistemas definidas en el Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		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.

7.14.3 FUNCIONAMIENTO DEL USO DE LA RED Y LA PRIVACIDAD

217. Adaptive Defense 360 incluye el nombre, la ruta completa de los ficheros y el usuario que inició la sesión en el equipo cuando envía los archivos a la nube de para su análisis. Esta información se utiliza posteriormente en los informes y las herramientas de análisis forense mostradas en la consola web. Si no se desea que esta información sea enviada a la nube, se deberá desactivar la casilla apropiada en la pestaña **Privacidad.**

218. 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 megabytes que un agente podrá enviar en una hora, se introducirá el valor y haz clic en **Ok**. Para establecer transferencias ilimitadas se dejará el valor a 0.

7.15 CRITERIOS DE CONFIGURACIÓN DE ADAPTIVE DEFENSE 360

219. 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 Esquema Nacional de Seguridad (ENS).

Funcionalidad	Descripción	Categoría		
		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 capacidad de procesamiento	Op.	Op.	Op.
Analizar comprimidos en disco (No recomendado)	Descomprime los archivos encontrados en el sistema de ficheros. Requiere un extra de capacidad de procesamiento.	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 capacidad de procesamiento.	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 firewall.	Op.	N.A	N.A
La configuración firewall la	El Administrador establece la configuración del cortafuegos	Op.	Aplica	Aplica

establece el usuario de cada equipo (desactivado)	para los puestos de usuario y servidores.			
Red pública	Añade reglas 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 excepto aquellos explícitamente permitidos.	Op.	Op.	Aplica
Activar las reglas de Adaptive Defense 360	Agrega reglas básicas de protección de programas.	Op.	Aplica	Aplica
Reglas de conexión Activar las reglas de Adaptive Defense 360	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
Dispositivos Android – Sección Antirrobo				
Protección antirrobo		Op.	Aplica	Aplica
Informar de la localización del dispositivo	El dispositivo envía sus coordenadas GPS a los servidores de Panda Security para poder geolocalizarlo.	Op.	Op.	Aplica

Sacar foto al tercer intento de desbloqueo y enviarla por email	Si el usuario del dispositivo falla tres veces consecutivas al desbloquearlo, se tomará una fotografía y se enviará por correo electrónico a las direcciones de correo separadas por coma introducidas en la caja de texto.	Op.	Aplica	Aplica
Permitir al usuario activar el modo privado	El usuario puede impedir la toma de fotografías y el registro de las coordenadas GPS del dispositivo y posterior envío al servidor de Panda aunque el Administrador haya establecido esta configuración.	Op.	Aplica	N.A
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
Unidades de almacenamiento extraíbles		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	Bloquea el acceso a páginas web sin categoría temática asociada.	N.A.	Op.	Aplica

cuya categoría sea desconocida				
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.**	Aplica	Aplica	Aplica

	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.			
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 – Filtrado de contenidos 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
Bloqueo de programas				
Activar bloqueo de aplicaciones		Op.	Aplica	Aplica
Introduce los nombres de los programas que quieres bloquear:	Nombres de los ficheros a los que Adaptive Defense 360 impedirá su ejecución. En esta caja de texto acepta listas de nombres de ficheros copiadas / pegadas y separados por retorno de carro. No se admiten comodines para evitar configuraciones demasiado amplias que comprometan el buen funcionamiento del equipo.	Op.	Aplica	Aplica
Introduce los códigos MD5 de los programas que quieres bloquear:	MD5 de los ficheros a los que Adaptive Defense 360 impedirá su ejecución. En esta caja de texto acepta listas de MD5s copiadas /	Op.	Aplica	Aplica

	pegadas y separados por retorno de carro.			
Informar a los usuarios de los equipos de los bloqueos	Muestra una ventana desplegable al usuario del equipo indicando el motivo por el cual la ejecución del programa se encuentra bloqueada.	Op.	Aplica	Op.
Ajustes por equipo – Sección Preferencias				
Mostrar icono en la bandeja del sistema	En función de si el servicio de seguridad está completamente administrado o no por la Organización, muestra u oculta el icono del agente en el área de notificaciones de los equipos.	Op.	Aplica	Aplica
Ajustes por equipo – Sección Actualizaciones				
Actualizar automáticamente Adaptive Defense 360 en los equipos	Actualiza el motor de protección cuando se detecte una nueva versión publicada en los servidores de Panda.	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.
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	Adaptive Defense 360 solo se podrá desinstalar si el usuario	Aplica	Aplica	Aplica

desinstalar la protección desde los equipos	tiene la contraseña de administración.			
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 mediante contraseña 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 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. FASE DE OPERACIÓN

220. Durante la dase de operación, se deberán llevar a cabo, al menos, las siguientes tareas de mantenimiento:

a) **Comprobaciones periódicas del software** para asegurar que no se ha introducido software no autorizado.

b) **Aplicación regular de los parches de seguridad**, con objeto de mantener una configuración segura.

c) **Mantenimiento de los registros de auditoría**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.

d) **La información de auditoría se guardará en las condiciones** y por el periodo establecido en la normativa de seguridad.

e) **Auditar**, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

f) **Actualización periódica de las bases de datos** de firmas de amenazas conocidas.

g) **Realización periódica de copias de seguridad** de la información del producto.

9. REFERENCIAS

REF1 ¿Qué programas se desinstalan automáticamente con Adaptative Defense y Endpoint Protection?
https://www.pandasecurity.com/spain/support/card?id=50021

REF2 Cómo crear una imagen para entornos virtuales persistentes y no persistentes (VDI) en Windows con productos basados en Aether platform
https://www.pandasecurity.com/spain/support/card?id=710050

REF3 Group Policy Management Console with Service Pack 1 – Español
https://www.microsoft.com/es-ES/download/details.aspx?id=21895

REF4 Guía de administración Panda Adaptive Defense 360 EPDR
https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/v11/ADAPTIVEDEFENSE360oAP-guia-ES.pdf

REF5 Herramienta para comprobar la validez de los certificados raíz instalados en equipos con sistema operativo Windows
https://www.pandasecurity.com/resources/tools/wescertcheck.zip

REF6 Resumen de SLA para los servicios de Azure
https://azure.microsoft.com/es-es/support/legal/sla/summary/

REF7 Panda Aether Tool
https://www.pandasecurity.com/es/support/card?id=700005

REF8 Herramienta nslookup
https://docs.microsoft.com/es-es/windows-server/administration/windows-commands/nslookup

REF9 Herramienta dig
https://docs.oracle.com/es-ww/iaas/Content/DNS/Tasks/testingdnsusingdig.htm

REF10 Comando “host”
https://www.hscripts.com/es/tutoriales/linux-commands/host.html

REF11 Panda Data Control
https://www.watchguard.com/wgrd-products/endpoint-security/watchguard-data-control

REF12 Panda Systems Management
https://www.pandasecurity.com/es/support/card?id=300100

REF13 Guía de Buenas Prácticas para la Puesta en Marcha de Panda Adaptive Defense 360 sobre Aether
https://www.pandasecurity.com/es/support/card?id=700054

REF14 Activar el doble factor de autenticación
https://www.cytomic.ai/es/soporte/id-700088/

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL