centro criptológico nacional

Guía de Seguridad de las TIC
CCN STIC 1230

Procedimiento de Empleo Seguro
Bitdefender Gravityzone

Enero 2025

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

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-184-0
Fecha de Edición: enero de 2025

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
2026.01.16 07:18:36 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN

1. **Bitdefender GravityZone** proporcionan protección a los dispositivos Windows en los que sus **Agentes de Seguridad** se encuentren instalados. Estos agentes tienen funcionalidades de *antivirus* y de *Endpoint Detection Response*.
2. La administración de estos agentes se puede llevar a cabo de manera centralizada a través de la Consola de Control basada en web de Bitdefender Gravityzone **Control Center**.
3. **Control Center** se proporciona como un servicio en la nube capaz de centralizar la gestión, monitorización y administración de los diferentes **Agentes de Seguridad**.
4. El producto proporciona protección al *endpoint* en múltiples niveles que van desde la detección de *malware* basada en ficheros, al análisis heurístico y de comportamiento de los procesos. La protección puede ser personalizada por el administrador en función de las necesidades de la compañía aplicando diferentes políticas a cada uno de los **Agentes de Seguridad** instalados.
5. **Control Center** permite monitorizar de manera centralizada todos los eventos e incidencias producidas en cada uno de los dispositivos controlados por un **Agente de Seguridad**.

2 OBJETO Y ALCANCE

6. En la presente guía se recoge el procedimiento de empleo seguro del servicio **Bitdefender Gravityzone** incluyendo **Control Center** y sus **Agentes de Seguridad** ejecutándose en dispositivos Windows y ejerciendo la funcionalidad de EDR.
7. Puede consultar la versión cualificada de Bitdefender Gravityzone en las familias “EDR (Endpoint Detection and Response), Anti-virus / EPP (Endpoint Protection Platform)” en el Catálogo alojado en el sitio web del CPSTIC.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado **4**. En este apartado se recogen los requisitos o recomendaciones asociadas a la fase previa de instalación del producto.

b) Apartado **5**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de instalación segura del producto.

c) Apartado **6**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de configuración.

d) Apartado **7**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de operación y mantenimiento.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Una vez se haya adquirido **Bitdefender GravityZone**, el usuario deberá acceder a su cuenta de administración de **Control Center** (https://gravityzone.bitdefender.com) antes de iniciar el proceso de instalación de los agentes.
9. Para ello, se deberán seguir los pasos indicados en la sección **First Steps** de la guía online de **Bitdefender GravityZone** [REF1]. Siguiendo esos pasos, será posible crear o acceder a la cuenta de administración de **Control Center** dependiendo del tipo de compra del producto realizada.
10. El **Agente de Seguridad** de **Bitdefender GravityZone** se podrá descargar directamente desde el portal de administración de **Control Center** a través de **Network > Packages**. Para generar un paquete de instalación del **Agente de Seguridad** se deberán seguir los pasos que se indicarán a lo largo de esta guía.

4.2 CONSIDERACIONES PREVIAS

11. Una vez se ha adquirido **GravityZone**, se deberá acceder a **Control Center** a través de la web (https://gravityzone.bitdefender.com). Desde dicha web podrán configurarse y descargarse los paquetes que contienen el **Agente de Seguridad**.
12. El hardware del equipo donde se instale el **Agente de Seguridad** deberá cumplir los siguientes requisitos:

CPU		
TARGET SYSTEMS	**CPU TYPE**	**SUPPORTED OPERATING SYSTEMS**
Workstations	Intel® Pentium compatible processors, 2 GHz or faster	Microsoft Windows desktop OSes
Smart devices	Intel® Pentium compatible processors, 800 MHZ or faster	Microsoft Windows
Servers	Minimum: Intel® Pentium compatible processors, 2.4 GHz	Microsoft Windows Server
	Recommended: Intel® Xeon multi-core CPU, 1.86 GHz or faster	

Tabla 1. requisitos de CPU

MEMORIA RAM DISPONIBLE DURANTE LA INSTALACIÓN (MB):						
OS	**Single Engine**					
	Local Scanning		**Hybrid Scanning**		**Centralized Scanning**	
	AV Only	**Full Options**	**AV Only**	**Full Options**	**AV Only**	**Full Options**
Windows	1024	1200	512	660	256	400

Tabla 2. Requisitos de memoria RAM durante la instalación

MEMORIA RAM DISPONIBLE PARA USO DIARIO (MB):									
OS	Antimalware (single engine)			Protection modules					
	Local	Hybrid	Centralized	Advanced Threat Control	Firewall	Content Control	Power User	Update Server	Advanced Anti-Exploit
Windows	75	55	30	+13	+17	+41	+29	+80	+13

Tabla 3. Requisitos de memoria para uso diario

ESPACIO DE ALMACENAMIENTO DURANTE LA INSTALACIÓN (MB):										
OS	Single Engine						Dual Engine			
	Local Scanning		Hybrid Scanning		Centralized Scanning		Centralized + Local Scanning		Centralized + Hybrid Scanning	
	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options
Windows	1024	1200	500	700	350	570	1024	1200	500	700

Tabla 4. Requisitos de espacio de almacenamiento durante la instalación

ESPACIO DE ALMACENAMIENTO PARA USO DIARIO (MB):									
OS	Antimalware (single engine)			Protection modules					
	Local	Hybrid	Centralized	Advanced Threat Control	Firewall	Content Control	Power User	Update Server	Advanced Anti-Exploit
Windows	410	190	140	+12	+5	+60	+80	+10	+12

Tabla 5. Requisitos de espacio de almacenamiento para uso diario

13. El **Agente de Seguridad** es compatible con los siguientes sistemas operativos:

- Windows 11 September 2022 Update (22H2)
- Windows 11 (initial release)
- Windows 10 November 2021 Update (21H2)
- Windows 10 May 2021 Update (21H1)
- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10 (initial release)
- Windows 8.1
- Windows 8
- Windows 7
- Windows Server 2022

- Windows Server 2019 Core
- Windows Server 2019
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

14. La edición del sistema operativo Windows sobre el que se instale el **Agente de Seguridad** no podrá ser la edición *"Home"*.

15. El administrador deberá asegurarse de que se dispone de permisos de administración en el sistema operativo en el que se instalará el agente. Estos permisos serán necesarios durante el proceso de instalación del mismo.

5 FASE DE INSTALACIÓN

5.1 INSTALACIÓN DE LOS AGENTES DE SEGURIDAD

5.1.1 CONFIGURACIÓN DE LOS CIPHERSUITES DEL SISTEMA OPERATIVO

16. Se deberá configurar una política de Windows para restringir el uso de algunas *suites* de cifrado. Para ello, se deberán seguir los siguientes pasos:

    - Desde el Sistema operativo, se accederá al *Editor de directivas de grupo local*. Esto se puede lograr mediante la herramienta *Editar directiva de grupo* del panel de control.
    - Desde esta aplicación, se accederá a *Configuración de Equipo > Plantillas Administrativas > Red > Opciones de configuración SSL*.
    - Se editará la política *Orden de conjuntos de cifrado SSL* haciendo doble clic en la misma.
    - Se marcará la opción *Habilitada*.
    - Se incluirá la siguiente lista de suites de cifrado en el formulario *Conjuntos de cifrado SSL* bajo las *opciones*:
      TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CCM,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CCM,TLS_EMPTY_RENEGOTIATION_INFO_SCSV
    - Se hará clic en Aplicar y Aceptar.
    - Se cerrará el Editor de directivas de grupo local.
    - Para que los cambios tomen efecto, se deberá reiniciar el dispositivo.

5.1.2 CONFIGURACIÓN DE PAQUETES

17. Con el objetivo de instalar el **Agente de Seguridad**, se deberá generar un paquete de instalación desde **GravityZone Control Center**.

18. Para ello, desde **Control Center** se deberá acceder con una cuenta de usuario con el rol *Company Administrator* a ***Network > Installation Packages*** en la parte izquierda de la interfaz de administración. Dentro de dicha interfaz, se hará clic en el botón ***Create***, que aparece en la parte superior de la interfaz, lo que nos permitirá generar un nuevo paquete de descarga.

19. Una vez seleccionada la opción ***Create***, aparecerá la ventana titulada ***Create Installation Package,*** donde se podrán configurar las diferentes funcionalidades del **Agente de Seguridad**. Ésta ventana cuenta con opciones para introducir nombre, descripción, idioma, módulos, roles del Agente, modo de escaneo, configuraciones de la ruta de instalación y configuración de la entidad que despliega dicho agente.

20. Para configurar el **Agente de Seguridad**, se deberá elegir un nombre de manera obligatoria. Con el objetivo de alcanzar un nivel de seguridad adecuado, se deberán al menos seleccionar los siguientes módulos de protección:

    - Antimalware
    - Advanced Threat Control
    - Advanced Anti-Exploit
    - Firewall
    - Network Protection
    - Content Control
    - Network Attack Defense
    - Integrity Monitoring
    - EDR Sensor

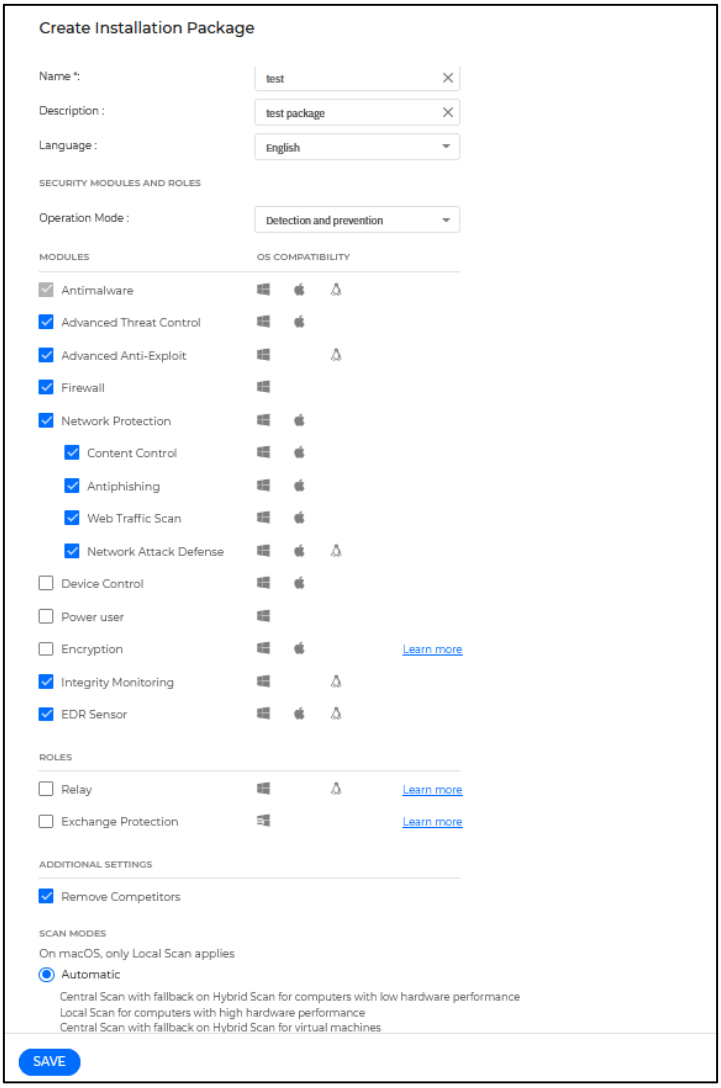

Ilustración 1 - Ejemplo de Configuración del Agente

21. Es recomendable marcar la opción *Remove Competitors* para que el **Agente de Seguridad** tenga una funcionalidad más efectiva.

22. El resto de opciones se seleccionarán en función de las necesidades del usuario, dejando sus valores por defecto en caso de que no se quiera activar ninguna funcionalidad u opción adicional.
23. Tras guardar esta configuración, el nuevo paquete de descarga aparecerá con el nombre previamente asignado en la lista de paquetes.

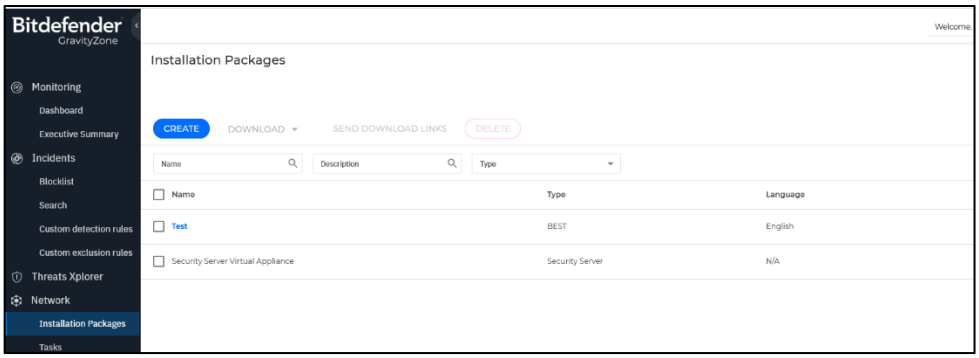

Ilustración 2 - Listado de Paquetes

5.1.3 DESCARGA E INSTALACIÓN DEL PAQUETE

24. Esta parte sólo se podrá ejecutar en el dispositivo dónde se vaya a instalar el agente. Una vez el paquete ha sido creado, entrando en la web desde el *endpoint*, se seleccionará el paquete previamente creado y se descargará.
25. Para descargarlo se seleccionará el paquete y la opción de descarga se activará. De las opciones elegidas, se escogerá la que corresponda con la arquitectura del dispositivo en el que se va a instalar. Se descargará un .zip que se tendrá que extraer para la correcta instalación del agente. Una vez extraído, se ejecutará la aplicación que se encuentra dentro de la carpeta y la instalación se producirá de manera automática:

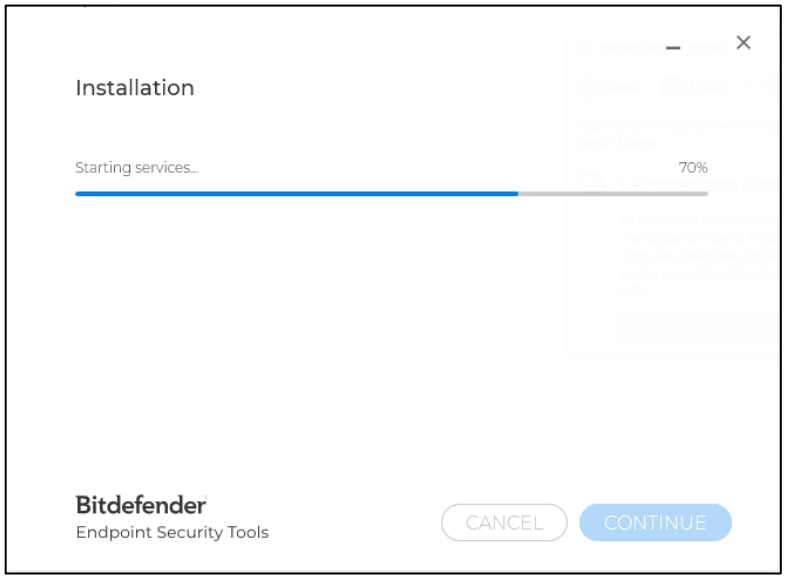

Ilustración 3 - Instalación

26. Una vez finalizada la instalación, se deberá hacer clic en *Finish*.

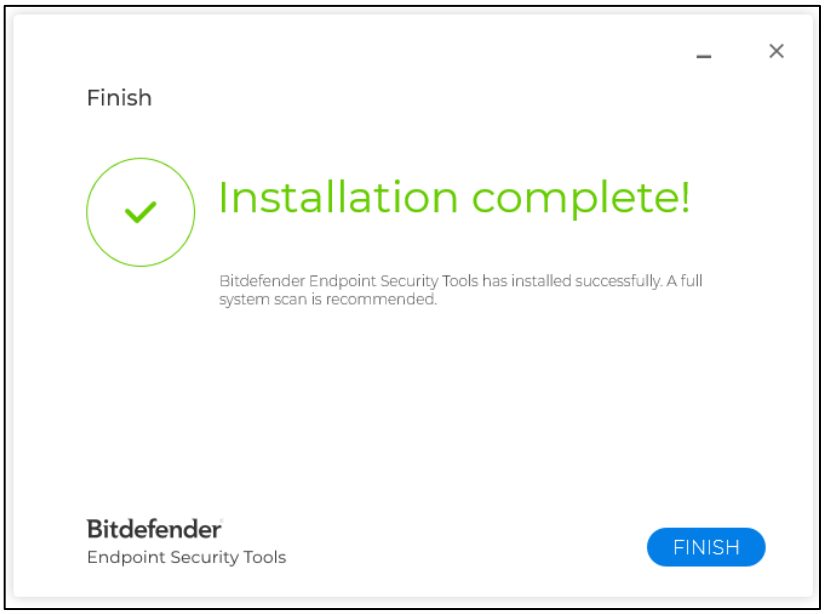

Ilustración 4 - Finalizar Instalación

27. De esta manera, el agente con la configuración que aporta el paquete se instalará en el *endpoint* deseado.

5.2 CONFIGURACIÓN POR DEFECTO

28. La configuración con la que este nuevo agente está desplegado es una configuración básica en la que se puede comprobar que muchos de los módulos no están activados. Para alcanzar un mayor nivel de protección que cumpla con todas las políticas de seguridad, será necesario asignar una política personalizada cuya configuración mínima se expondrá en la siguiente sección.

6 FASE DE CONFIGURACIÓN

29. Una vez el agente quede instalado, se podrá observar que en la política de protección hay ciertos módulos que están en modo *Off* (*Device Control*, *Application Control* y *Encryption*). Para activarlos, habrá que modificar la política que tiene asignada el agente. Esta configuración se realizará de forma remota desde el **Servidor de Control,** tal y como se define en la sección **6.2 CONFIGURACIÓN DE POLÍTICAS** de este mismo documento.

6.1 ADMINISTRACIÓN

30. Los Agentes de Seguridad sólo se podrán administrar de manera remota a través de web proporcionada por **Control Center**, desde dónde se manejarán los datos, políticas y configuraciones de los **Agentes de Seguridad**. Es por esto que la administración de los agentes siempre será remota.

6.1.1 CONFIGURACIÓN DE ADMINISTRADORES

31. A partir de la cuenta creada durante la primera configuración de *GravityZone* se podrán crear nuevas cuentas con diferentes niveles de administración. En la opción *Accounts* de la columna izquierda, se podrán crear estas cuentas pulsando el botón *Add* dentro de dicha opción. Para completar la configuración de administradores habrá que aportar un nombre, dirección de correo, una zona horaria y el rol que dicho administrador tendrá. Hay cuatro tipos de roles:

    - ***Company Administrator***: este administrador gozará de todos los derechos (control sobre las redes, la herramienta *GravityZone*, usuarios y la subscripción de la compañía a *GravityZone*).
    - ***Network Administrator*****:** este administrador no podrá configurar la herramienta GravityZone pero gozará del resto de los derechos.
    - ***Security Analyst***: este administrador sólo tendrá acceso a los datos para poder analizarlos.
    - ***Custom***: este administrador tendrá los derechos que se le asignen, es totalmente configurable.

6.1.2 CONFIGURACIÓN DE CONTRASEÑA

32. Tras crear una cuenta, el usuario recibirá un email en el correo electrónico indicado. El correo contendrá un enlace que permitirá al usuario establecer una contraseña para su cuenta.

33. Las contraseñas creadas deberán cumplir los siguientes requisitos:

    a) Longitud mínima de 12 caracteres (recomendable 15 caracteres).

    b) Debe contener al menos un dígito

    c) Debe contener al menos una letra mayúscula y una minúscula

    d) Debe contener al menos un carácter especial

6.1.3 CAMBIO DE CONTRASEÑA

34. Adicionalmente, es posible que los usuarios modifiquen su propia contraseña desde **Control Center**.

35. Una vez el usuario ha accedido a **Control Center** podrá cambiar su contraseña seleccionando el icono de usuario en la esquina superior derecha de la pantalla y accediendo al menú *My account*.

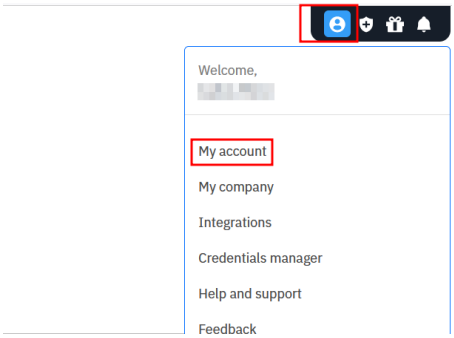

Ilustración 5 – Acceso al Menú My Account

36. En dicho menú, el usuario deberá seleccionar la opción *Change password:*

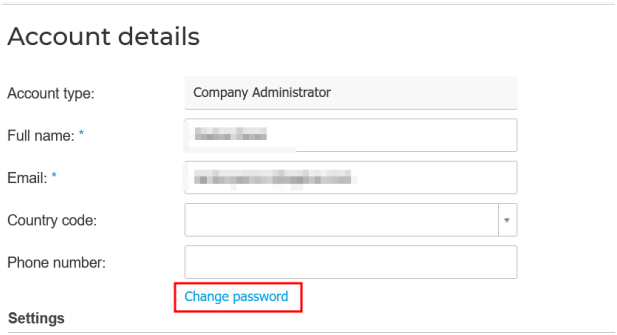

Ilustración 6 – Cambio de Contraseña

37. Una vez seleccionada dicha opción, se requerirá que el usuario introduzca su contraseña actual, la nueva contraseña y la confirmación de la nueva contraseña. Tras ello, se deberá seleccionar el botón *Save* para establecer la nueva contraseña.

38. Tal y como se indicará en un mensaje que se le mostrará por pantalla al usuario durante el cambio de contraseña, las contraseñas creadas deberán cumplir los siguientes requisitos:

    a) Longitud mínima de 12 caracteres (recomendable 15 caracteres).

    b) Debe contener al menos un dígito

    c) Debe contener al menos una letra mayúscula y una minúscula

    d) Debe contener al menos un carácter especial

6.2 CONFIGURACIÓN DE POLÍTICAS

39. En la opción *Policies* de la interfaz de gestión del Servidor de Control, se podrá ver que sólo hay una política configurada con el nombre *Default policy (default)*. Será necesario configurar una política adicional para aplicársela posteriormente al agente. Para ello, se deberá pulsar el botón *Add* que hay en la parte superior de esa misma ventana. La interfaz cambiará y aparecerán los siguientes desplegables a la izquierda:

    - General
    - Antimalware
    - Sandbox Analyzer
    - Firewall
    - Network Protection
    - Patch Management
    - Application Control
    - Device Control
    - Relay
    - Exchange Protection
    - Encryption
    - Incidents Sensor.

40. En todos los desplegables que haya una casilla en la parte superior de su interfaz, se marcará dicha casilla. De esta manera se activarán los módulos que estaban en estado *Off*. De manera adicional, también se tendrán que seleccionar algunas opciones para alcanzar la configuración segura de los Agentes de Seguridad. En la opción *General>Notifications* se tendrá que seleccionar las opciones *Display alert pop-ups* y *Display notification pop-ups*. Con estas opciones se habilitará la opción de que el usuario reciba una notificación cuando se detecte una amenaza. El caso de *Encryption* también es especial ya que también habrá que marcar la opción *Encrypt* que aparece más abajo.

41. Una vez terminado, se deberá hacer clic en *Save* en la parte inferior de la pantalla.

42. Tras ello, la nueva política aparecerá en la lista de políticas. Si la nueva política no aparece, se deberá pulsar la opción *Refresh*.

6.3 APLICACIÓN DE POLÍTICAS

43. Una vez generada una política, se deberá aplicar a cada uno de los agentes que se han configurado.

44. Para ello, se deberá acceder al menú *Network* y localizar el agente al que se quiere aplicar la política dentro de la carpeta del grupo al que haya sido asignado.

45. Una vez localizado el agente, se seleccionará marcando la casilla de su izquierda. Cuando se seleccione el agente, se desbloqueará la opción *Assign Policy* con la cual se podrá aplicar la política recientemente creada. Entrando en dicha opción, se seleccionará la opción *Assign the following policy template* y la política creada anteriormente. Finalmente, se completará el proceso de aplicación pulsando el botón *Finish* de la parte inferior.

46. Se podrá comprobar que la política está funcionando entrando en *Network*, haciendo clic en el nombre del agente y accediendo a su menú *Policy*, donde se verificará que la política asignada es la correcta y que su estado es “Applied”.

6.4 CONFIGURACIÓN DE LOGS

47. El producto no viene con los registros de auditoría configurados por defecto, es por ello que se tendrá que configurar cuáles se querrán mostrar. Dentro de los registros de auditoría, se pueden diferenciar dos grupos distintos:

    a) registros de auditoría de actividades del usuario y

    b) registros de auditoría de la funcionalidad de antivirus.

48. Los **registros de auditoría de actividad del usuario** no necesitan de configuración adicional. Para acceder a ellos, habrá que entrar en la sección *Accounts* > *User Activity* y pulsando el botón *Search* aparecerán todos los eventos relacionados con los usuarios, la configuración del sistema e incluso las actualizaciones. Pulsando sobre cualquiera de los eventos, en la parte inferior de la interfaz aparecerá más información al respecto.

49. Los **registros de auditoría de funcionalidad de antivirus** los veremos a través de la Consola de Control en la parte derecha de la interfaz, bajo la columna *Notifications*. Para ver todos los registros de auditoría, tendremos que configurarlo a través de la configuración de las notificaciones, pulsando en el símbolo de engranaje situado a la derecha de *Notifications*. Una vez dentro de esta opción, habrá una lista con casillas para marcar en la parte inferior de la nueva interfaz. Marcando todas las casillas y posteriormente pulsando sobre la opción *Save*, aparecerán todas las notificaciones posibles en la columna derecha de la interfaz principal. En el caso de querer saber más sobre un evento de la columna de *Notifications*, pulsando sobre el link con el nombre *Show more* de dicha notificación, la Consola de Control mostrará toda la información acerca de ese evento.

50. Adicionalmente, será posible acceder a los **registros de arranque y parada del servicio del agente** en el propio sistema operativo Windows en el que el agente se encuentra instalado. Para ello se deberán seguir los siguientes pasos:

    - Se accederá al Visor de Eventos de Windows.
    - En el Visor de Eventos se accederá a la categoría Registros de Windows y dentro de la misma a la categoría de Aplicación.
    - En dicha categoría se podrán encontrar los eventos de inicio y parada del producto bajo el nombre del servicio del mismo (“epag”).

51. Los eventos de inicio y parada del producto sirven, además, para identificar el arranque y parada de las funciones de auditoría, ya que éstas se encuentran ligadas al propio servicio del agente. Durante el arranque, se genera un evento que indica que el servicio ha sido iniciado. La parada del servicio “epag” viene ligada a la parada del sistema operativo, ya que se ejecuta como un servicio del sistema, por lo que los eventos de detención del sistema operativo Windows servirán para determinar que se ha detenido el servicio del producto, así como sus funciones de auditoría.

52. En casos excepcionales como los procesos de actualización, el producto se detendrá y arrancará por sí mismo. En estos casos el registro de auditoría de Windows almacenará registros del arranque y parada del servicio “epag”.

6.5 ACTUALIZACIONES

53. Las actualizaciones se podrán realizar de dos maneras: de manera manual o automatizada.
54. Para **actualizar** el Agente de Seguridad de **manera automática** se configurará en la opción *Configuration>Update* de la columna de la derecha y se marcará la casilla *Enable automatic GravityZone product updates.* Con esta casilla el agente se actualizará cuando lo necesite.
55. Para **actualizar** el Agente de Seguridad de **manera manual**, habrá que hacerlo desde la opción *Network* de la columna de la izquierda. Desde ahí, entrando en el grupo *Custom Groups* y seleccionando la casilla del agente a actualizar, se desbloquearán acciones en la opción de *Tasks* (símbolo de un papel con un tick situado por encima de todos los agentes). Una de las acciones desbloqueadas será *Update client*, dónde se seleccionará la casilla *Use policy-defined components*. Una vez se haya completado la acción pulsando el botón *Update*, aparecerá el desarrollo de la actualización en la opción *Network>Tasks*.

7 FASE DE OPERACIÓN Y MANTENIMIENTO

7.1 RECOMENDACIONES PARA LA FASE DE OPERACIÓN

56. El correcto funcionamiento del producto requiere de características que deben estar presentes en el entorno. Es la responsabilidad del administrador autorizado asegurar que el entorno operacional cumple con los requisitos enumerados a continuación:

    a) El producto estará instalado y será mantenido en un entorno físico seguro. Esto incluye un edificio seguro con control de acceso o un entorno móvil controlado por el administrador.

    b) Los administradores deben estar correctamente entrenados en el uso y la correcta operación del producto, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías e indicaciones presentes.

    c) Los administradores se asegurarán de que el producto cuenta con las últimas actualizaciones de firmware y software para preservar al mismo de amenazas y vulnerabilidades conocidas.

    d) Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.

    e) Los administradores deben eliminar toda la información residual sensible que pudiera quedar resultante de operar con el producto después de terminar la vida útil de este.

    f) Los auditores se encargarán de examinar de forma periódica los registros de auditoría buscando eventos específicos relacionados con los cambios de la configuración del sistema y que puedan indicar que éste ha sido comprometido.

57. Con el fin de prevenir que los administradores escojan contraseñas inseguras, estas deben de cumplir con los siguientes requisitos:

    - Deberán observarse y tenerse en cuenta las recomendaciones expuestas en la guía *CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40* .
    - Las contraseñas deben de tener una longitud recomendada de 15 caracteres.
    - Deben de estar compuestas por una combinación de caracteres pertenecientes, al menos, a 3 o 4 de los siguientes grupos de caracteres: letras en minúscula, letras en mayúscula, números y los caracteres especiales: *“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”*.

58. **No se debe emplear la interfaz de administración SSH del dispositivo de ninguna forma durante la operación del mismo**. El acceso a través de dicha interfaz se encuentra protegido mediante contraseña. Sin embargo, los usuarios del producto solo deberán usar las interfaces CLI e interfaz web para administrar el producto.

8 REFERENCIAS

[REF1] Bitdefender GravityZone Online Guide, 2022-06-10. [En línea] https://bitdefender.com/business/support/en/77209-79841.

[REF2] CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40

9 ABREVIATURAS

AV	Antivirus
CLI	Command Line Interface
CPU	Central Processing Unit
CPSTIC	Catálogo de Productos de Seguridad TIC
EDR	Endpoint Detection and Response
ENS	Esquema Nacional de Seguridad
EPP	Endpoint Protection Platform
RAM	Random Access Memory
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer

PUBLICACIONES DE DEFENSA

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