Directivas de prevención de Ransomware

Dentro de sus elementos diferenciadores, **centralANTIVIRUS** pone a disposición de los usuarios una serie de directivas preconfiguradas para su libre utilización.

Además, con el objetivo de crear una comunidad colaborativa y viva en contenido, las directivas definidas por los distintos usuarios estarán disponibles para su utilización si así se precisa.

Directiva centralANTIVIRUS Anti-Ransomware:

Debido a la alta frecuencia y variabilidad con que el ransomware se libera en nuestros días, y aprovechando uno de los módulos de protección con más potencia de Endpoint Security. Se han establecido directivas con una serie de reglas que ayudan a prevenir un gran número de infecciones por ransomware del tipo Cryptolocker, Cryptowall, Locky o Teslacrypt entre otros.

Estas directivas, además, serán actualizadas de forma periódica por el equipo de centralANTIVIRUS.

NOTA IMPORTANTE: Antes de asignar estas directivas a un sistema o grupo, se recomienda encarecidamente revisar la configuración establecida en cada una de las reglas, ya que en ocasiones la configuración definida para prevenir determinados tipos de acción que el ransomware realiza, pasa por impedir o bloquear determinadas acciones que pueden ser necesarias en algunos entornos de trabajo.

Estas directivas están disponibles para su asignación, pero también pueden ser duplicadas y modificadas con las exclusiones o configuración que se considere oportuno tal y como se explica en el documento de "Gestión de directivas".

centralANTIVIRUS no se hace responsable del uso y las funciones derivadas por la implementación de estas directivas.

Estas directivas se basan en la configuración de un conjunto de reglas del módulo "Protección de acceso" de Endpoint Security Threat Prevention que bloquean determinados comportamientos que suele llevar a cabo el ransomware actual.

A modo de ejemplo sencillo:
- Bloquear que un archivo ejecutable (.exe) pueda crear otro dentro de la carpeta 'Roaming' del usuario.

Entre todas estas reglas (que serán actualizadas periódicamente) se incluye el bloqueo de muchos otros comportamientos detectados en las principales variantes del ransomware actual. Con esto se pretende que no sea bloqueado exclusivamente el ransomware ya conocido sino también aquellas nuevas variantes con comportamientos similares.

NOTA IMPORTANTE: centralANTIVIRUS No puede garantizar que aquellos sistemas que apliquen estas directivas vayan a estar protegidos al 100% frente a este tipo de amenazas.

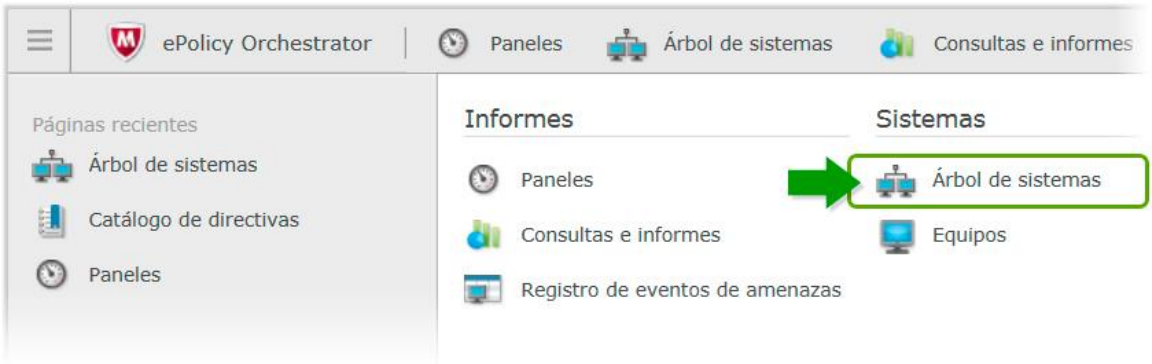
La nomenclatura de las directivas Anti-Ransomware suministradas por centralANTIVIRUS tiene el siguiente formato:

centralANTIVIRUS Anti-Ransomware [Rev.X] [Standard]

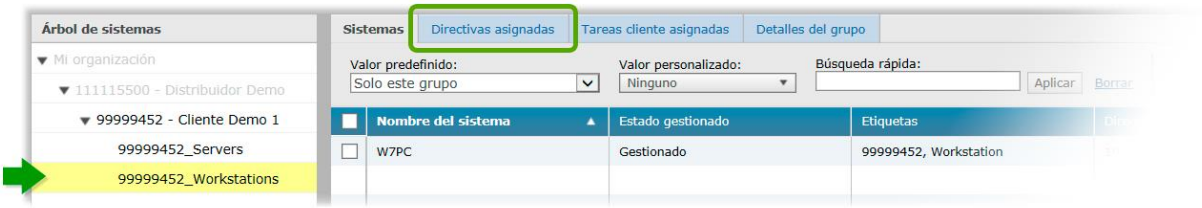
[Rev.X]: La versión de la directiva se identifica con una letra. Cuanto más actual es la directiva, más alto será el valor de letra.
[Standard / Agressive]: Determinadas versiones de esta directiva pueden tener distintos niveles de agresividad en base a las reglas configuradas. Es recomendable revisar la configuración de las directivas antes de su utilización.

Cómo asignar una directiva centralANTIVIRUS Anti-Ransomware predefinida:

Dirigirse a: Menú > Árbol de sistemas



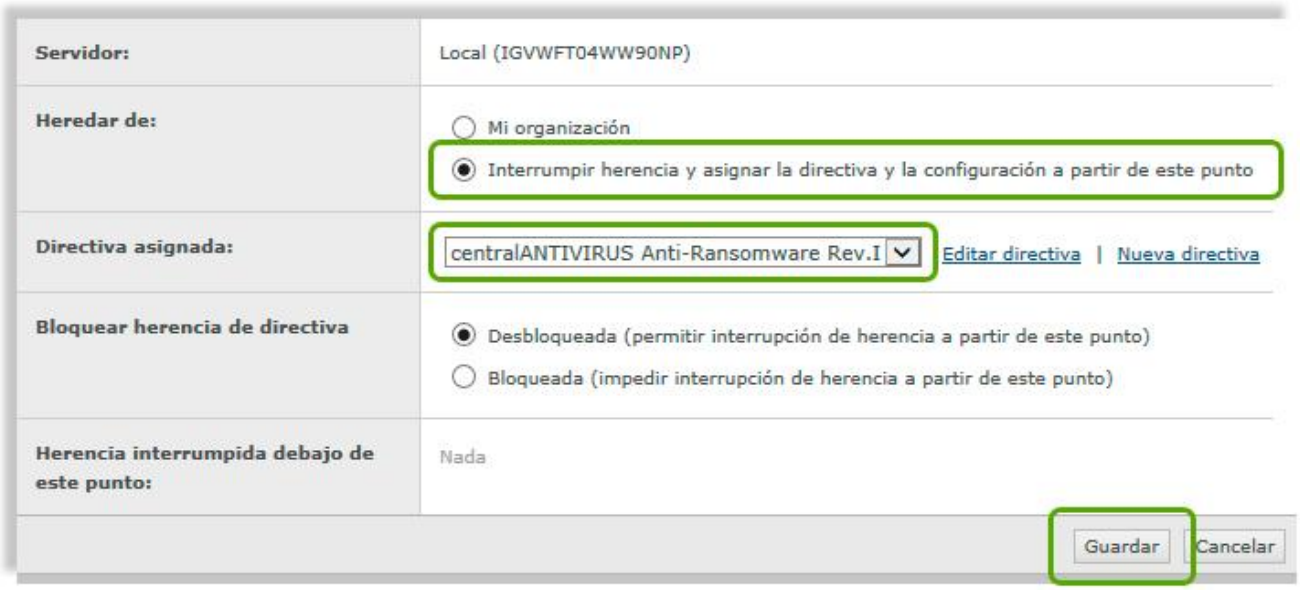
A continuación, seleccionar la rama del árbol de sistemas correspondiente al grupo de sistemas donde se quiere asignar la directiva y posteriormente, hacer clic en la pestaña **"Directivas asignadas".**



Una vez en la pantalla de **"Directivas Asignadas"**, seleccionar en el desplegable de producto el módulo **"Endpoint Security Threat Prevention"** y posteriormente buscar la categoría **"Protección de Acceso"**.

Una vez localizada la categoría a la que corresponde la directiva que se va a modificar, hacer clic en la parte de la derecha donde indica **"Editar asignación".**

En la siguiente pantalla, seleccionar la opción “Interrumpir herencia y asignar la directiva y la configuración a partir de este punto” y seleccionar en el desplegable la directiva **“centralANTIVIRUS Anti-Ransomware Rev.X”** como figura en la siguiente imagen:



Finalmente, hacer clic en **“Guardar”** y la directiva habrá sido asignada al grupo correspondiente.

NOTA IMPORTANTE: Recordar que tal y como se indica en el documento de Gestión de directivas, no es necesario asignar la directiva a una rama completa de servidores o workstations, las directivas pueden ser asignadas a un único sistema o a varios de ellos.