Diagrama procedimental aseguramiento de servidores

Aseguramiento de servidores

Medellín
Noviembre de 2021

Índice

1. OBJETIVO.

Garantizar un nivel de aseguramiento en la infraestructura de la organización, el cual surge de las líneas de inventario general y de los inventarios generados desde las diferentes consolas de seguridad, con el fin de llevar a cabo un mejor control y gestión sobre los servidores (Windows), logrando construir un análisis de los equipos que cuentan con los diferentes tipos de protección y así filtrarlos para sacar una estadística completa y prevenir futuras amenazas y vulnerabilidades. El aseguramiento debe lograrse independientemente de la versión de Windows con la que cuente un servidor.

2. ALCANCE.

Este procedimiento aplicará a todos los servidores Wintel, ya sean controlados individualmente, compartidos, independientes o en red. Para el correcto aseguramiento se efectuará:

1. Identificación del activo: S.O, Direccionamiento de red, controles de seguridad, etc.
2. Identificación funcionalidades de los servidores: Servicios Web, Aplicaciones, BD, etc.
3. validación del correcto acceso a servidores para su gestión.
4. Verificación e instalación de controles de protección: Antimalware, EDR, Parcheo Virtual.
5. Clasificación del activo y asignación de políticas técnicas en consolas de seguridad.

2.1. DEFINICIONES.

- Activo de Información:Todo aquello a lo que la organización directamente le asigna un valor y, por lo tanto, la organización debe proteger.
- Amenaza:Está asociada con la ocurrencia de incidencias que pueden generar un impacto negativo, por lo que se puede definir como la frecuencia con la que ocurre una incidencia con impacto potencialmente negativo para la organización.
- EDR:Es una herramienta que proporciona monitoreo y análisis continuo del endpoint y la red.
- Parcheo Virtual:Protección contra vulnerabilidades, actúa como una medida de seguridad contra amenazas que aprovechan vulnerabilidades conocidas y desconocidas.
- Amenazas avanzadas:Software de McAfee que tiene como objetivo impedir los ataques de robo de información o espionaje.
- CMDB:Base de datos que contiene detalles relevantes de cada CI (ítem/elemento de configuración) y de la relación entre ellos.

3. GENERALIDADES ASEGURAMIENTO DE SERVIDORES

Relación de inventarios: Solicitud de inventarios línea base, los cuales son actualizados cada mes por el personal de infraestructura con el fin de tener los datos depurados.

Generación de reportes en consolas de seguridad: Se genera el inventario en la consola de seguridad y posteriormente se exporta, se tabula la información y se seleccionan los campos de interés como:

- Nombre del equipo
- Dirección IP
- Versión del producto

Nota: un activo categorizado por un nivel de criticidad alto debería contar con todas las protecciones.

4. Requerimientos

- La informacíon suminstrada de los inventarios debe ser actualizada.
- En la fase de reconocimiento de los activos se debe tener claridad con los campos, la información ligada a cada campo debe coincidir con la información de la consola Cualquier nombre diferente, caracter agregado o espacio en blanco adicional estropea la precision del proceso.
- Se precisa de la información adicional que desea ser agregada al documento para dar continuidad al proceso.

5. Requerimientos

En la Figura(1) se presenta el diagrama procedimental para el aseguramiento de servidores.

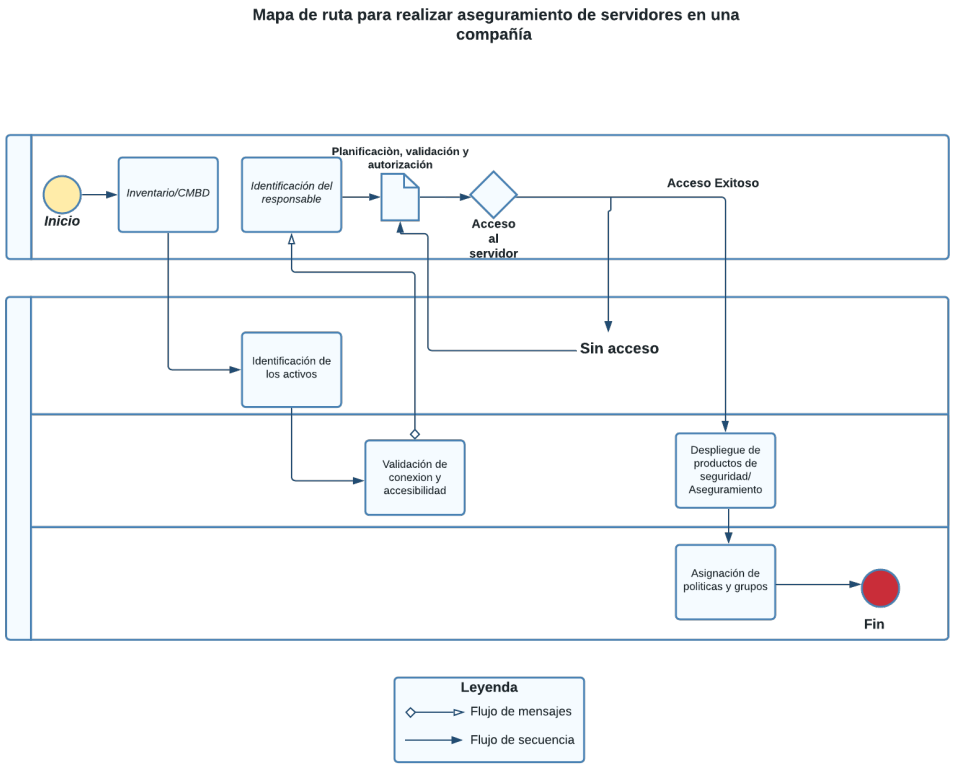

Figura 1: Diagrama