METODOLOGÍA DE ASEGURAMIENTO A SISTEMAS OPERATIVOS SERVER

CARLOS FERNANDO CORONADO PARGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2018

METODOLOGÍA DE ASEGURAMIENTO A SISTEMAS OPERATIVOS SERVER

CARLOS FERNANDO CORONADO PARGA

Proyecto para optar por el título de especialista en seguridad informática

Director de proyecto
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2018

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C., 20 de febrero de 2018

DEDICATORIA

A mis padres,
Por su amor, consejos y dedicación por el sacrifico en ciertos momentos difíciles que tuvimos, y que al final generó en mí los valores con los que vivo.

A mi Esposa e hijos,
Haciendo parte importante de mi vida siempre con su apoyo en las metas que quiero cumplir, por su comprensión y apoyo siempre compartiré con ellos todos mis éxitos como el lograr la realización de este postgrado en Seguridad Informática.

AGRADECIMIENTOS

Agradezco a mi familia madre, padre, esposa e hijos por el apoyo que me han brindado, a los compañeros de la universidad con quienes hemos trabajado y a los Tutores quienes nos han guiado, para lograr adquirir el conocimiento en todos los campos de este postgrado.

TABLA DE CONTENIDO

pág

GLOSARIO 12

INTRODUCCION 15

1 OBJETIVOS 16

1.1 OBJETIVO GENERAL 16

1.2 OBJETIVOS ESPECÍFICOS 16

2 MARCO DE REFERENCIA 18

2.1 MARCO TEORICO 18

2.1.1 Metodologías de análisis y gestión de riesgos de TI. 19

2.1.2 Mejores prácticas. 25

2.1.3 Herramientas. 27

2.1.4 Determinación de metodología y herramientas. 40

2.2 MARCO HISTORICO 40

2.3 MARCO CONCEPTUAL 42

2.4 MARCO LEGAL 44

3 MARCO METODOLOGICO 45

3.1 FORMA DE INVESTIGACIÓN 45

3.2 METODOS DE INVESTIGACION 45

4 CICLO DE ASEGURAMIENTO DE SERVIDORES WINDOWS SERVER 46

4.1 INVENTARIO DE ACTIVOS INFORMÁTICOS 47

4.2 SELECCIÓN DE HERRAMIENTA PREPARACIÓN DEL SERVIDOR 49

4.3 SELECCIÓN DEL ESCANER DE VULNERABILIDADES TI 50

4.4 SELECCIÓN DE UNA HERRAMIENTA DE DISTRIBUCIÓN DE ACTUALIZACIONES DE SEGURIDAD 51

4.5 SELECCIÓN DE UN SOFTWARE ANTIMALWARE 51

4.6 PLANEACIÓN ANÁLISIS DE VULNERABILIDADES 52
4.7 ESCANEO DE VULNERABILIDADES 53
4.8 ANÁLISIS DE INFORMES DE ESCANEOS 53
4.9 DESPLIEGUE DE ACTUALIZACIONES DE SEGURIDAD 54
4.10 CIERRE DE VULNERABILIDADES 54
4.11 PRUEBAS FUNCIONALES 55
4.12 METRICAS DE LA METODOLOGÍA 55
4.12.1 EFICACIA. 55
4.13 POLITICAS DEL CICLO DE ASEGURAMIENTO 57
4.13.1 Políticas de gestión de identidad. 57
4.13.2 Políticas generales de seguridad TI. 57
4.14 PROCEDIMIENTO DE ASEGURAMIENTO DE UN SERVIDOR WINDOWS SERVER 60
4.14.1 Preparación del Servidor. 61
4.14.2 Aseguramiento inicial del servidor. 63
4.14.3 Instalación software antimalware. 64
4.14.4 Instalación y validación de actualizaciones. 65
4.14.5 Configuración del Windows Firewall (WFAS). 66
4.14.6 Escaneo de vulnerabilidades. 68
4.14.7 Cierre de vulnerabilidades detectadas. 70
5 CONCLUSIONES 71
6 RECOMENDACIONES 72
BIBLIOGRAFÍA 73
ANEXOS 77

LISTA DE TABLAS

pág

Tabla 1. Comparativa entre metodologías. 24
Tabla 2. Nivel de eficacia de la metodología de aseguramiento de servidores Windows Server.....56

TABLA DE ILUSTRACIONES

pág

Ilustración 1. Hoja de Ruta de la Metodología OCTAVE Allegro.....20
Ilustración 2. Proceso para la administración del Riesgo.....21
Ilustración 3. Representación del Riesgo.....22
Ilustración 4. Estructura MAGERIT. 23
Ilustración 5. Editor de políticas de grupo local.....28
Ilustración 6. Active Directory.....29
Ilustración 7. Administrador de Políticas de grupo. 30
Ilustración 8. Fases guía gestión de riesgos.....31
Ilustración 9. Panel Principal Herramienta SCM. 32
Ilustración 10. SCW (Security Configuration Wizard).....33
Ilustración 11. Microsoft Baseline Security Analyzer.....34
Ilustración 12. Flujo funcional de WSUS en la entrega de Actualizaciones. 35
Ilustración 13. Clasificación de actualizaciones. 35
Ilustración 14. Portal Web Catalogo de Microsoft Update.....36
Ilustración 15. Listado de Actualizaciones de ejemplo. 36
Ilustración 16. Microsoft Malicious Software Removal Tool. 37
Ilustración 17. Panel principal de OpenVast. 38
Ilustración 18. Panel Principal Retina CS Community. 39
Ilustración 19. Consola de Gestión NeXpose Community Edition.....39
Ilustración 20. Ediciones de Microsoft Windows. 41
Ilustración 21. Ciclo de aseguramiento de Servidores Windows Server. 47
Ilustración 22. Cronograma de aseguramiento de servidores.....53
Ilustración 23. Flujograma Procedimiento de aseguramiento de un Servidor. 60
Ilustración 24. Instalación de Windows Server 2012 R2. 61
Ilustración 25. Actualizar el sistema antes de iniciar operación. 61
Ilustración 26. Selección Server Core o Server con GUI. 62
Ilustración 27. Selección de Roles Windows Server. 62
Ilustración 28. Selección de características Windows Server. 63
Ilustración 29. Aplicación de SCW Security Configuration Wizard. Reglas de seguridad de red 63
Ilustración 30. Aplicación de SCW Security Configuration Wizard, Configuraciones de registro. 64
Ilustración 31. Instalación de Antimalware Enterprise, sobre Windows Server. 65
Ilustración 32. Validación fecha de actualización Antimalware, y versión. 65
Ilustración 33. Chequear nuevas actualizaciones de Windows.....66
Ilustración 34. Matriz de comunicación para configuración del WFAS.....67
Ilustración 35. WFAS, Windows Firewall Advanced Security.....67
Ilustración 36. Configuración de reglas de entrada (Inbound).....68
Ilustración 37. Configuración de reglas de salida (Outbound).....68

Ilustración 38. MBSA. Microsoft Baseline Security Analyzer.....69
Ilustración 39. Reporte de vulnerabilidades encontradas.....69
Ilustración 40. Formato escaneo de vulnerabilidades. 70

TABLA DE ANEXOS

pág

Anexo A. Formato, Matriz activos de infraestructura TI de Servidores. 77
Anexo B. Formato, Escaneo vulnerabilidades Servidores. 78
Anexo C. Formato, Matriz de comunicación del servidor. 79
Anexo D. Formato, Cronograma de aseguramiento de Servidores……80

GLOSARIO

ACTIVO: se refiere a cualquier cosa que represente algún valor para la organización lo que conlleva a que debe ser protegido. Detallado aún más el concepto es cualquier elemento que manipula información.

AMENAZA: es la posibilidad de que ocurra cualquier tipo de evento o situación que pueda generar un daño sobre algún componente de un sistema, o en la Información.

ANTIVIRUS: herramienta informática desarrollada para la detección de código malicioso o destructivo.

ANTIMALWARE: herramienta desarrollada en software con la capacidad de la detección y control del código malicioso en forma de virus, troyano, spyware, entre otras capacidades de seguridad que pueden mantener.

BOTNET: nombre utilizado para denominar a cualquier grupo de computadores o dispositivos informáticos infectados y controlados por un atacante de forma remota.

CARACTERÍSTICAS: de un servidor Windows son programas de software disponibles en el sistema operativo que, aunque no pertenecen de manera directa en los roles de servidor, pueden complementar su funcionalidad. Estos pueden operar de manera independiente a los roles del servidor Windows.

CAUSA: en el proceso de análisis de riesgos se pueden encontrar factores internos o Externos. Las causas son las situaciones generadoras del riesgo.

CONFIDENCIALIDAD: es la propiedad que se le otorga a la información para que esta solo pueda ser accedida por usuarios o personas autorizadas.

CONTROL: dentro del ámbito de la gestión de riesgos se refiere al mecanismo preventivo y correctivo manual o automático que adopta una organización la cual permite una oportuna detección y corrección de desviaciones equivocas que pueden colocar en riesgo la misma.

CVE: Common Vulnerabilities and Exposures, en español Vulnerabilidades y exposiciones comunes, es un diccionario de nombres comunes o identificadores de manera estandarizada para las vulnerabilidades y exposiciones identificadas. Su objetivo lograr un lenguaje común en el intercambio de datos en el ámbito de la seguridad de la información. También tiene como objetivo ofrecer cuales son las herramientas más eficaces y adecuadas para los requerimientos de la organización.

DISPONIBILIDAD: es la característica de encontrar la información a disposición de quienes deben acceder a ella. Ya sean procesos, personas o aplicaciones.

HARDWARE: conjunto de elementos físicos o materiales que constituyen una computadora, servidor o un sistema de información.

IMPACTO: es la medida del daño que puede generarse debido a la materialización de un riesgo. Normalmente es una medida cuantitativa.

INTEGRIDAD: mantener los datos libres de modificaciones no autorizados. Garantizando que los datos sean consistentes.

MALWARE: esta palabra abrevia “Malicious software”, quien enmarca a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un error en el funcionamiento.

REMEDIACIÓN: es la actividad que se realiza para la corrección de una vulnerabilidad. La remediación se puede realizar de 3 formas, instalando un parche o actualización del sistema, modificando algún parámetro de configuración y desinstalando algún componente de software.

RIESGO: es toda aquella situación que puede originar que un objetivo no se cumpla, si lo tipificamos en el ámbito de la informática donde al riesgo lo denominamos “riesgo informático”, suponemos que estos riesgos son situaciones dentro de la informática que puede llegar a ocasionar que los objetivos informáticos no se cumplan.

ROLES: un rol de servidor es un conjunto de programas de software que, una vez que se instalan y configuran correctamente, permiten a un equipo realizar una función específica para varios usuarios u otros equipos de una red.

SERVICE PACK: es una actualización de Windows que por lo general combina actualizaciones anteriores y ayuda a que el sistema operativo sea más fiable. Lo cual ayuda a mejorar el rendimiento, seguridad y compatibilidad con nuevos tipos hardware.

SALVAGUARDA: es cualquier mecanismo que ayuda a reducir el riesgo. Este nombre es muy utilizado en la metodología española MAGERIT. Dentro de las funciones de las salvaguardas están los preventivos y los curativos.

- ✓ Las salvaguardas preventivas normalmente son utilizadas en la gestión de amenazas quienes son las que generan vulnerabilidades.
- ✓ Las salvaguardas curativas normalmente se utilizan en la gestión de Impactos.

SERVICIOS DE ROL: son programas de software que proporcionan funcionalidad de un rol. Al instalar un rol, puede elegir los servicios de rol que el rol proporcionará a otros usuarios y equipos de la empresa. Algunos roles, como Servidor DNS, tienen

una sola finalidad y, por lo tanto, no tienen servicios de rol disponibles. Otros roles, como Servicios de Escritorio remoto, tienen varios servicios de rol que pueden instalarse, en función de las necesidades de los equipos remotos de la empresa.

SISTEMA OPERATIVO: es un conjunto de programas que posibilita la administración de los recursos de una computadora. Este tipo de sistemas trabaja cuando se enciende el equipo para gestionar el hardware a partir de los niveles más bajos.

SISTEMA OPERATIVO SERVER: el nombre comercial se ha utilizado en las versiones Microsoft para servidores en PYMES y Grandes empresas.

SOFTWARE: conjunto de programas y rutinas que permiten al servidor realizar tareas determinadas y/o configuradas previamente.

VIRTUALIZACIÓN: es la creación a través de software de una versión virtual de algún recurso tecnológico ejemplo sistema operativo server, una plataforma de hardware, un dispositivo de almacenamiento entre otros.

VULNERABILIDAD: es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño. Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

WINDOWS SERVER: es una línea de productos para servidores desarrollada por Microsoft Corporation. El nombre comercial es utilizado por las versiones de Microsoft para servidores

INTRODUCCION

En el mundo actual las amenazas tecnológicas están todo el tiempo variando, generando nuevas técnicas para hacer daño o en función malintencionada y las cuales buscan cualquier debilidad del software o de un proceso o del ser humano denominado técnicamente como vulnerabilidad para lograr ser aprovechada logrando un acceso no autorizado un robo de identidad o robo de datos que pueden generar un impacto negativo y en algunos casos muy nocivos en las compañías que utilicen sistemas informáticos de las cuales se puede decir que en la actualidad esto puede darse en cualquier parte del mundo a cualquier nivel o sector de las organizaciones, por lo anterior todo fabricante de software de aplicaciones como de sistemas operativos está desarrollando todo el tiempo nuevas versiones o correcciones de sus productos, con el fin de reducir los riesgos latentes, en los que se pueden incurrir al tener estos sistemas expuestos. Estas vulnerabilidades pueden darse en cualquier capa del modelo OSI, las cuales deben ser remediadas para el caso de este proyecto el enfoque será la detección y remediación en los sistemas operativos Windows server versión 2008 r2 y 2012r2, para lo cual se hace importante en toda organización tener una metodología de aseguramiento a los sistemas operativos, la cual debe incluir sus respectivos procedimientos y herramientas informáticas para este fin. El siguiente proyecto pretende realizar una investigación y generar una metodología para el aseguramiento de los sistemas operativos Microsoft Windows Server el cual puede ser aplicado a cualquier organización.

Según investigaciones realizadas en algunas compañías que utilizan Servidores MS Windows Server se observa que no existe una metodología de aseguramiento de estos servidores que garantice la seguridad de la información que transita en ellos, se hace necesario diseñar y construir una metodología completa de aplicación práctica que sirva de guía a las áreas de seguridad informática de las organizaciones, en cuanto al aseguramiento de sistemas operativos MS Windows server. Esta metodología debe contemplar un modelo para el análisis y remediación de vulnerabilidades, procedimientos, formatos, políticas, roles y un documento de estudio de herramientas en el mercado que ayuden a automatizar el análisis y la remediación de las vulnerabilidades, enfocado a sistemas operativos MS Windows Server.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Construir un modelo documental aplicable a las organizaciones, a través de metodologías existentes para el aseguramiento de sistemas operativos MS Windows Server.

1.2 OBJETIVOS ESPECÍFICOS

- Investigar y documentar los conceptos el estado de arte de las metodologías, sus mejores prácticas y herramientas existentes para el aseguramiento de los sistemas operativos MS Windows Server.
- Determinar las metodologías, técnicas y herramientas para el aseguramiento de sistemas operativos MS Windows Server.
- Aplicar las metodologías de aseguramiento o fortalecimiento hardening en sistemas operativos MS Windows server para construir el modelo documental.
- Entrega del modelo documental denominado ciclo de aseguramiento de sistemas operativos MS Windows Server, que contiene procedimientos, políticas, formatos y estudio de la información analizada.

JUSTIFICACIÓN

Según investigaciones realizadas en algunas compañías que utilizan Servidores Microsoft Windows Server, se observa que no existe una metodología de aseguramiento de estos, que garantice la seguridad de la información que transita en ellos.

El proyecto denominado *Metodología de aseguramiento de servidores Windows Server,* busca crear un modelo que permita mejorar la seguridad en los sistemas operativos Microsoft Windows server, detectando las debilidades del sistema, así como provocando la contención en su mayor probabilidad de las amenazas latentes que los pueden afectar, prevenir una intrusión, endurecer un sistema y poder identificar acciones preventivas o correctivas evitando o reduciendo la posibilidad de un ataque informático (Acceso no autorizado, perdida de disponibilidad del sistema, o robo de información entre otras), lo que podría resultar en pérdidas económicas en las compañías, o en riesgos reputacionales a las mismas. Por lo anterior se propone una metodología apoyada en análisis de riesgos informáticos enfocado en su mayoría en vulnerabilidades, de las cuales, utilizando mejores prácticas, herramientas, recomendaciones y un proceso cíclico, controlar la seguridad de estos, desde que el servidor entra en operación en la organización hasta que este cumple su vida útil.

2 MARCO DE REFERENCIA

2.1 MARCO TEORICO

Los sistemas operativos Microsoft Windows Server han evolucionado a nivel de seguridad a lo largo del tiempo, debido a las exigencias del mercado cambiante y a las vulnerabilidades existentes. Las empresas en el mundo actual y con la revolución que tiene la tecnología deben afrontar el reto de garantizar la seguridad de su información a través de sus áreas de TI, apoyados en la seguridad informática.

En la actualidad las vulnerabilidades de los sistemas operativos en general sobre todo en los Windows Server crecen, por ser este el sistema operativo empresarial más comercial y uno de los más utilizados en el mundo y si estas vulnerabilidades no son remediadas con frecuencia o a tiempo se pone en riesgo la operación o la información de las organizaciones. Se ha observado que no existe un modelo que guie a las pequeñas medianas compañías en el proceso de gestión de aseguramiento de Sistemas Operativos Windows Server de manera puntual. Por esto se hace imprescindible diseñar un modelo metodológico para el análisis y remediación de vulnerabilidades sin importar que tipo de compañía o su tamaño o el sector en que esta labora.

Los sistemas operativos son la base principal de los equipos de cómputo y son las que ponen a hablar a las aplicaciones con el hardware. Hablando particularmente de los servidores se encuentra que los sistemas operativos Microsoft denominados Windows Server, son base importante de muchas compañías en donde se hacen las instalaciones o habilitaciones a los servicios que se requieren siendo estos de infraestructura como DHCP, DNS, Active Directory, Internet Information Services, FTP, File Services, correo entre otros o aplicaciones de negocio las cuales son aplicaciones de fabricantes como Microsoft o de terceros especializadas en funciones tipo ERP, CRM, contables, inventarios, personalizadas, etc. Algo importante para notar es que, entre más aplicaciones o servicios tenga un sistema operativo o servidor instalado más vulnerabilidades van a existir y por ende el riesgo crece, por lo anterior la gestión de las áreas de TI se incrementa en búsqueda de la gestión o remediación de estas, “una vulnerabilidad no gestionada es una amenaza para el funcionamiento del negocio”.

Dentro de las versiones de Microsoft Windows Server, se encuentran desde Windows NT puesta a producción en 1993 hasta la más actual Windows server 2016, este documento se enfocará en Windows server 2008 y Windows server 2012, para conocer aún más de estos sistemas como son sus roles y características[1] que

[1] MICROSOFT, Biblioteca de TechNet. [En línea]. 2017. Disponible en https://technet.microsoft.com/es-es/library.

pueden ser habilitadas desde el mismo sistema operativo, puede consultarse en el sitio web de Microsoft llamado “Biblioteca de TechNet”.

2.1.1 Metodologías de análisis y gestión de riesgos de TI.

En las investigaciones realizadas se encuentra que Microsoft, como fabricante vive preocupado por el tema de seguridad en sus sistemas operativos por lo anterior pone a disposición su fábrica de desarrollo y publica constantemente los parches o correcciones que deben realizarse a sus sistemas operativos o productos para corregir los riesgos detectados, así como sus mejores prácticas, dentro de su modelo de soporte se encuentra el portal llamado “Microsoft TechCenter de seguridad”,[2] en este sitio es posible encontrar noticias, webcast, descarga de herramientas, boletines de seguridad e información en general que apoyan en el aseguramiento correcto de los sistemas Microsoft en general.

A continuación de hace un barrido de algunas metodologías de gestión de riesgos que pueden ser utilizadas como base para el análisis de riesgos desde el punto de vista de las vulnerabilidades o el aseguramiento de los sistemas informáticos para el caso en sistemas operativos Windows siendo este un activo informático.

- **OCTAVE Allegro.** (Operationally Critical Threat, Asset and Vulnerability Evaluation).

Es una metodología desarrollada por la organización Computer Emergency Response Team (CERT), permite tener una evaluación amplia del riesgo operacional y con resultados robustos sin tener un conocimiento alto en el proceso de análisis de riesgos. Esta versión de OCTAVE se enfoca al análisis de riesgos de los activos de información en el contexto de cómo son utilizados, en donde son almacenados, su trasporte y como son procesados, así como son expuestos a las amenazas, vulnerabilidades y como son los resultados ante posibles interrupciones[3].

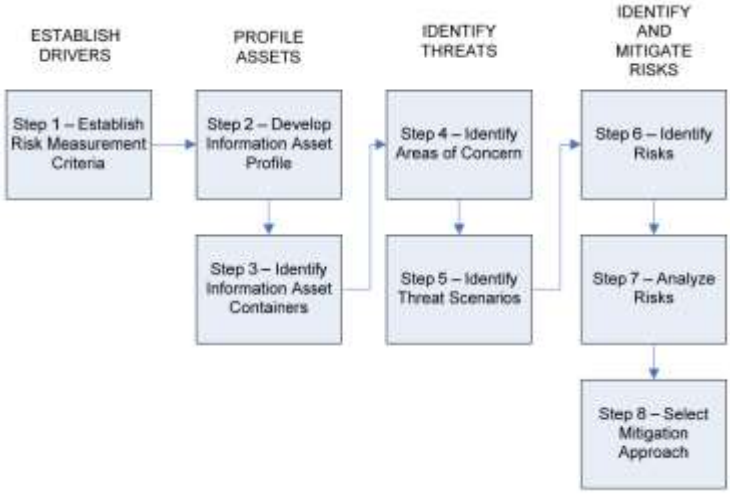
Esta metodología tiene la particularidad que se puede desarrollar de manera colaborativa o en forma de taller. La metodología está compuesta por ocho pasos que están organizados en cuatro fases así:

---

[2] MICROSOFT, TechCenter de seguridad. [En línea]. 2017. Disponible en https://technet.microsoft.com/es-es/security.

[3] Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson. Introducing OCTAVE Allegro. Improving the Information Security Risk., 2007. CMU/SEI-2007-TR-012.

Ilustración 1. Hoja de Ruta de la Metodología OCTAVE Allegro.



Fuente: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

1. La organización construye la valoración de riesgos confiables con controladores organizacionales.
2. La organización determina basado en perfiles la criticidad de los activos, teniendo en cuenta diferentes criterios de valoración.
3. Se identifican las amenazas de los activos basados en el contexto de donde son almacenados, trasportados o procesados
4. Se identifican los riesgos de los activos, en donde son analizados y se inicia la construcción de los controles de mitigación.

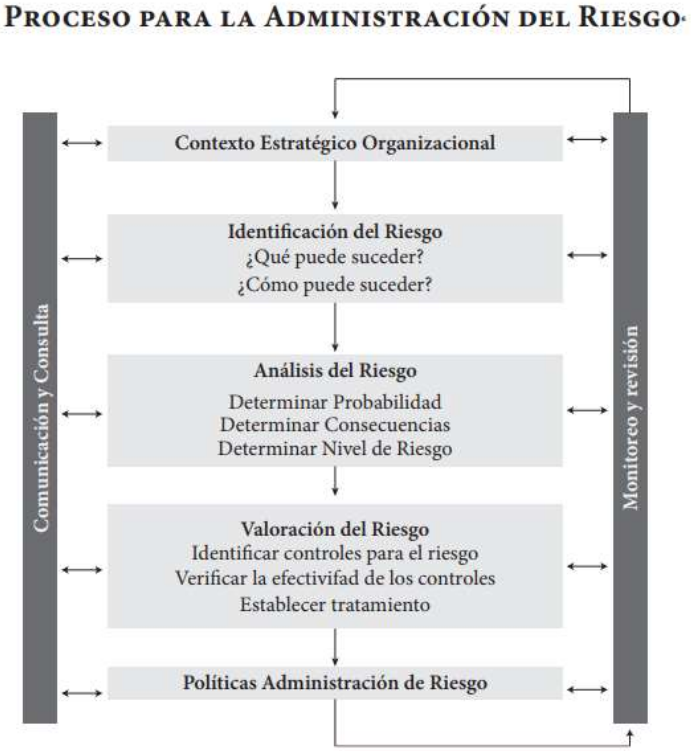
- **DAFP.** (Departamento Administrativo de la Función Pública). “Guía para la administración del riesgo”.

Este modelo sirve de guía para la implementación de la política de la administración del riesgo en las entidades públicas. Tiene como objetivo la protección de los activos de las entidades públicas e incluir los controles necesarios para la mitigación del riesgo. En todas las entidades del gobierno que implementan el proceso de administración del riesgo deben incluir la identificación, el análisis, la valoración de los riesgos y por último deben tener una política de administración de los riesgos.
En la metodología DAFP el proceso de análisis del riesgo depende de la investigación que realizó previamente en cuanto a la identificación y listado de riesgos observados.

Actividades claves del proceso de análisis de riesgos[4]:

1. Determinar la Probabilidad
2. Determinar las consecuencias
3. Clasificación del riesgo
4. Estimar el nivel de riesgo

Ilustración 2. Proceso para la administración del Riesgo.



Fuente: http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Dentro del proceso es importante definir la probabilidad de ocurrencia del riesgo y el impacto que pueda generar.
En las actividades básicas con respeto a la valoración del riesgo para este método se tiene lo siguiente:

1. Identificar los controles que existen en la organización

[4] COLOMBIA, DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA (DAFP), Guía Para La Administración Del Riesgo. [En línea]. Bogotá, septiembre 2011. Disponible en http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/

2. Validar la efectividad de los controles identificados
3. Planear las prioridades de los tratamientos de los riesgos.

- **OWASP.** (Open Web Application Security Project),

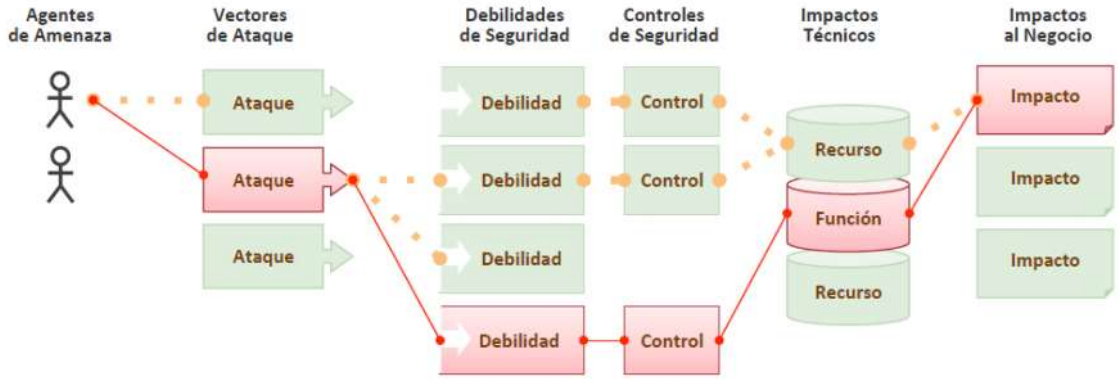
Esta organización presenta una metodología que la llama "Análisis de riesgos aplicando la metodología OWASP"[5], la cual está orientada al Riesgo de TI o riesgo encontrado en la Tecnología de la información, el cual se enfoca a realizar análisis en la perdida por caídas o errores detectados en los sistemas informáticos, cuyas causas se encuentran en errores de software entre otras posibles causas.

OWASP, considera dentro de su metodología que los riesgos son distintos dependiendo de la actividad o negocio y que la metodología debe ser adaptada particularmente al cada negocio.

Dentro de la metodología propuesta por OWASP se debe tener en cuenta los siguientes pasos:

1. Identificar los Riesgos
2. Identificar las Amenazas
3. Identificar las Vulnerabilidades
4. Determinar los Impactos
5. Estimar la probabilidad
6. Estimación de impacto (técnico y de negocio)
7. Priorizar planes de acción de mitigación de los riesgos.

Ilustración 3. Representación del Riesgo.



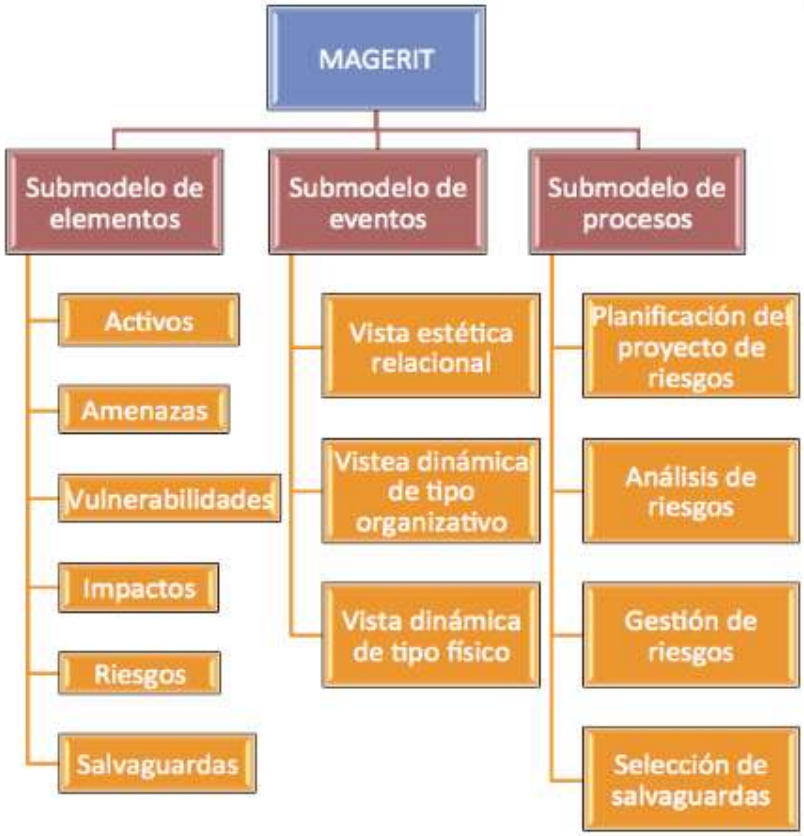
Fuente: OWASP Top 10 - 2013.

[5] OWASP, The Open Web Application Security Proyect, Análisis de riesgos aplicando la metodología OWASP. [En línea]. 2015. Disponible en https://www.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf

- **MAGERIT.** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Esta metodología encontrada soporta la fase AGR (Análisis y Gestión de Riesgos). MAGERIT apoya en gran medida la gestión en general de un sistema de seguridad de la información de una Compañía, basada en ISO27001, ya que contiene todas las etapas necesarias a nivel estratégico, desde la identificación organizada de los activos su valoración, la identificación de las amenazas, vulnerabilidades su impacto y frecuencia, la estimación del riesgo hasta las contramedidas o salvaguardas para la mitigación de los riesgos identificados a los activos de gran relevancia para la compañía[6]..

Esta metodología está compuesta por tres modelos, elementos, eventos y procesos.
Ilustración 4. Estructura MAGERIT.



Fuente: asijav.weebly.com.

[6] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. 2012. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

- **Comparativa entre Metodologías.**

Tabla 1. Comparativa entre metodologías.

	OCTAVE Allegre	DAFP	OWASP	MAGERIT
Ventajas	Aplicación Internacional	Aplicación País Colombia	Aplicación Internacional	No está limitada su aplicación
	Uso Interno Limitado, requiere compra de licencias	Uso en entidades Gubernamentales Colombianas	Uso libre	Uso libre
	Metodología orientada a pequeño equipo de trabajo	El Riesgo es identificado por la determinación de las causas o factores que infieren en el desarrollo de los procesos y objetivos institucionales	Esta metodología tiene en cuenta los riesgos, las amenazas, las vulnerabilidades, y calcula el impacto técnico y del negocio.	Metodología Reconocida por ENISA (European Network and Information Security Agency)
	Orientada al análisis de Activos de Información según su uso.	La identificación de riesgos es orientada a nivel general	OWASP, debido a su objetivo comercial presenta una experiencia amplia en Seguridad informática.	La identificación de activos, Completa y detallada
	Facilidad de utilización.	Esta metodología busca identificar los efectos o las consecuencias de los riesgos	Dentro de la metodología prioriza los planes de acción.	La metodología hace una identificación del riesgo basando en los activos inventariados
	Esta metodología tiene en cuenta los activos, sus amenazas, las vulnerabilidades, sus riesgos y los controles de mitigación			Esta metodología tiene en cuenta los activos, su valoración, sus amenazas, los riesgos, las vulnerabilidades, la probabilidad el impacto y los salvaguardas
Desventajas	Esta metodología no hace valoración de los activos y no analiza la probabilidad e impacto en la materialización de los riesgos.	Esta metodología no se basa en la identificación de los riesgos de los activos.	Esta metodología es bastante resumida y no se encuentra una documentación con mayor detalle de sus procesos o procedimientos.	Debido al proceso de determinación de todas las valoraciones en traducciones económicas lleva a que se vuelva compleja y costosa su aplicación.
	Esta metodología al ser tan simplificada omite detalles en el análisis de los Riesgos que pueden ocasionar se construyan Controles no efectivos o innecesarios.	La metodología no identifica las vulnerabilidades	OWASP se enfoca mayormente a la seguridad en Aplicaciones Web	

Fuente: El autor.

- **Determinación de la metodología de análisis y gestión de riesgos**.

En la descripción anterior de algunas de las metodologías que apoyan directa o indirectamente el proceso de análisis y gestión de riesgos como son OCTAVE Allegre, DAFP, OWASP y MAGERIT, se observan métodos similares a nivel procedimental lo que lleva a determinar que aunque todas las metodologías anteriores son aplicables para el caso expuesto en este documento, sin embargo debido a la precisión documental con la que se cuenta con la metodología MAGERIT y al tener sus documentos disponibles en internet siendo esta de uso libre tanto a nivel informativo como algunos ejemplos a nivel de formatos se convierte en la metodología más apropiada para que sea aplicada tanto al desarrollo de este proyecto como a cualquier organización y sobre todo aquellas en que su presupuesto puede ser corto.

Al observar a nivel procedimental todas las metodologías requieren una fase inicial de identificación o inventario de activos yéndonos al caso de TI estos activos son informáticos, luego se determinan mediante unas escalas su valor con el fin de concluir la importancia del mismo y definir el impacto que pueda ocasionar la caída o falla producto de una ataque o por un daño ocasional de alguno ante la organización, en el caso de MAGERIT se identifican las amenazas y vulnerabilidades, luego se hace una identificación de riesgos definidos a su entorno función etc, y se determinan probabilidades de ocurrencia de los mismos, de aquí se desprenden los planes de gestión de riesgos los cuales se componen de procedimientos como el de identificación y análisis de vulnerabilidades, implementación de salvaguardas o controles informáticos..

2.1.2 Mejores prácticas.

En esta sección se describirán diferentes procedimientos, técnicas y/o herramientas que se deben utilizar como mejor practica en proceso de aseguramiento de sistemas Informáticos para el caso Sistema operativos Windows Server 2008 y/o 2012.

- **Preparación de un Servidor**.

Uno de los primeros pasos dentro de la planeación de la seguridad antes de la instalación de un sistema operativo server, es la identificación de las medidas que reduzcan el área de ataque de una amenaza informática. Cuando se habla de reducir el área de ataque en un sistema es identificar solo el software o código a utilizar el cual será el único instalado, ya que entre más aplicaciones ejecutándose mayor probabilidad de vulnerabilidades que podrían ser explotadas.

El segundo paso se compone de la instalación de todos los parches disponibles actualizados por el fabricante en este caso Microsoft a sus sistemas operativos Windows Server según la versión utilizada en la compañía.

Como recomendación se debe configurar cada servidor con su sistema operativo server Microsoft para realizar una función específica. Por ejemplo, si se requiere un servicio de DNS, DHCP y un File Server, cada rol debería de tener un Servidor independiente con su sistema operativo independiente esto visto desde la seguridad. Esta sugerencia no solo disminuye el área de ataque informática, sino que puede disminuir la complejidad de solución de algún problema en el servidor, pues se independizan los servicios que se están prestando, así como sus componentes de software sin depender uno del otro.

También se recomienda tener los sistemas operativos server en forma virtual ya que esto puede ayudar en la reducción de los costos que deben invertir las organizaciones denominado esto como consolidación de servidores y dentro de la vista de la seguridad esto apoya temas como son las mejoras en disponibilidad, recuperación ante un incidente tipo desastre, ya que pueden ser utilizadas herramientas de virtualización como son las toma de Clones, Snapshots y se facilita la toma de backup (copias de seguridad) de las mismas en otras herramientas.

Es importante tener claro cuál es el sistema operativo server utilizado en las compañías 2003, 2008 o 2012 o posiblemente alguna versión posterior, clarificar el soporte dado por el fabricante (Ciclo de vida de los productos) y determinar la configuración adecuada para garantizar o buscar la mejora de la seguridad de la información que circulará a través de estos y el correcto licenciamiento de los sistemas operativos.

- **Firewall.**

Debido a las amenazas que se pueden observar a nivel de red, o ataques a puertos abiertos en el sistema, se debe tener como mejor práctica habilitado un sistema de firewall local en cada Sistema operativo servidor instalado en la organización, así como configurado correctamente sus excepciones a nivel de puertos o direcciones IPs requeridos para la operación. Los sistemas operativos Windows server analizados en este documento 2008 y 2012 cuentan ya con uno disponible el cual puede ser habilitado sin incurrir en costos adicionales a la compra de la licencia de Sistema operativo inicial. Para este está mejor practica se cuenta con una herramienta en una versión mejorada denominado Windows Firewall con seguridad avanzada (WFAS), el cual combina un firewall de host y el protocolo de seguridad de Internet (IPsec). Como ventaja que se tiene al habilitar este firewall es que la seguridad se puede dar de host a host y el cual puede requerir autenticación y la protección normal a nivel de direccionamiento IP o protocolos, en otras palabras, esta gran ventaja que trae tener esta herramienta habilitada es la contención de tráfico no interesante que pudiese desplazarse de manera horizontal por la red, tráfico que normalmente un firewall perimetral no logra observar ni detener.

- **Antimalware.**

Dentro de las mejores prácticas está la recomendación de tener instalado un software antimalware capaz de identificar y eliminar el mayor número de amenazas informáticas como software o código malicioso (Virus, Gusanos, Troyanos, Spyware), de igual manera se sugiere que estas herramientas se mantengan monitoreadas por un administrador del sistema y siempre estén en última versión tanto sus motores como sus bases de datos.

Microsoft no cuenta con un antimalware de uso no comercial para los sistemas operativos server, por lo anterior se debe realizar la adquisición de esta herramienta de seguridad. A continuación, se nombran algunas marcas que son los más utilizados en las grandes compañías, no solo por su eficacia sino por el soporte del fabricante, su modelo de gestión centralizado entre otros. También es importante nombrar que ya existen sistemas antimalware para sistemas virtuales, los cuales no requieren ser instalados en cada uno de los servidores virtuales, disminuyendo la carga a nivel de recursos. Para este caso existe el modelo en el cual se instala un motor de escaneo dentro del hipervisor el cual se encarga del escaneo de las máquinas virtuales dentro del mismo almacenamiento a nivel de archivos de disco virtual, en algunos modelos de estos sistemas antimalware ya vienen herramientas denominadas parcheo virtual, el cual tiene la capacidad de lograr el bloqueo de lagunas vulnerabilidades de los servidores virtuales, esta herramienta puede ser muy útil en aquellos casos donde es imposible la instalación de alguna actualización sobre el sistema operativo.

A continuación, se nombran algunas marcas de fabricantes de antimalware con soporte a sistemas operativos Windows Server o a nivel corporativo:

- Trend Micro
- Kaspersky Lab
- Mcafee
- Symantec
- Sophos
- Palo Alto Networks
- Eset
- Bitdefender

En caso de requerir un apoyo en la escogencia de la solución antimalware puede servir de referencia el cuadrante mágico de Gartner para “Endpoint Protection Platforms”.

2.1.3 Herramientas.

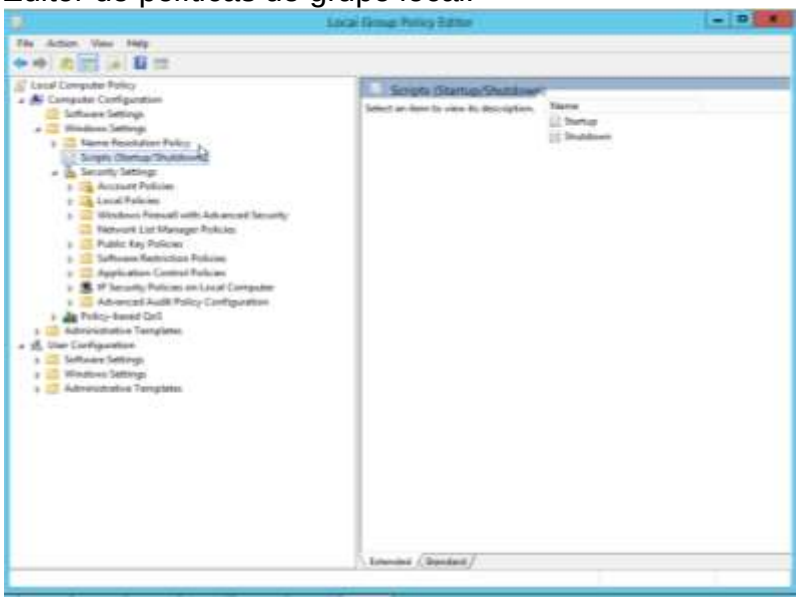
Dentro de las herramientas que apoyan la gestión de aseguramiento de los sistemas operativos Windows server, se observa la existencia de varias entre gratuitas, así

como comerciales o pagas, las cuales dependiendo del tamaño de la organización como del alcance requerido a nivel de compatibilidad y funcional se determina su escogencia.

- **Directivas de grupo.**

Esta herramienta hace parte de todos los sistemas operativos Microsoft Windows, permite en los casos de seguridad ajustar configuraciones a nivel de usuario o de equipo local de tal forma que puede operar con grados de seguridad personalizado o si se utilizan plantillas predefinidas entregadas por el fabricante hacer un hardening muy completo del sistema operativo. Una de las herramientas más utilizadas para orientar la mejor práctica de la configuración de las directivas de grupo basado en el rol es la entregada por Microsoft de forma gratuita llamada SCM (Security Compliance Manager). Para la configuración de estas políticas a nivel local, Windows trae una herramienta llamada "editor de políticas de grupo local", la cual puede ser iniciada ejecutando el comando de "gpedit.msc" [7].

Ilustración 5. Editor de políticas de grupo local.



Fuente: El autor.

Como se ilustra en la imagen anterior se observa a través de la herramienta de edición como están compuestas las diferentes opciones de políticas o directivas de grupo local que son posibles configurar, software settings, Windows settings y

[7] MICROSOFT, Introducción a las directivas de grupo. [En línea], 2017. Disponible en https://msdn.microsoft.com/es-es/library/hh831791(v=ws.11).aspx

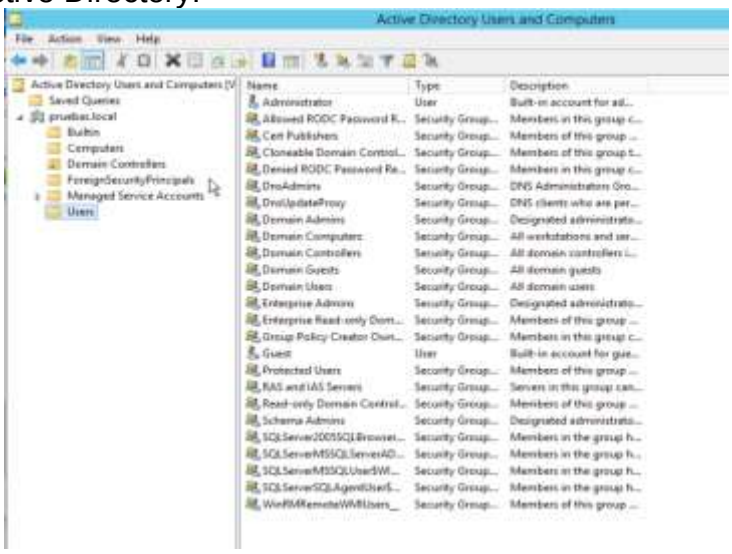
administrative templates, esta última permite configuraciones a través de plantillas que pueden ser importadas a la estructura de las directivas de grupo.

Para los casos de redes corporativas donde existe un servidor con el rol de AD DS Active directory Domain Services operativo, se logran realizar políticas sobre los equipos que se encuentran en el dominio y son administrados de manera centralizada por la herramienta de administración de servidores para este caso "consola de administración de directivas de grupo", la cual puede ser descargada de Microsoft de forma gratuita y como complemento para la administración remota de los servidores.

- **Active Directory[8].**

En compañías bien organizadas y basadas en sistemas operativos Microsoft lo más común es encontrar un servidor con el rol denominado AD DS (Active Directory Domain services), el cual tiene la función principal de tener el dominio o control de la red su estructura se compone de una base de datos con objetos de dominio (usuarios, equipos y otros dispositivos), como se observa en la ilustración siguiente. El nombre que se le da a este servidor es "Domain Controller".

Ilustración 6. Active Directory.



Fuente: El autor

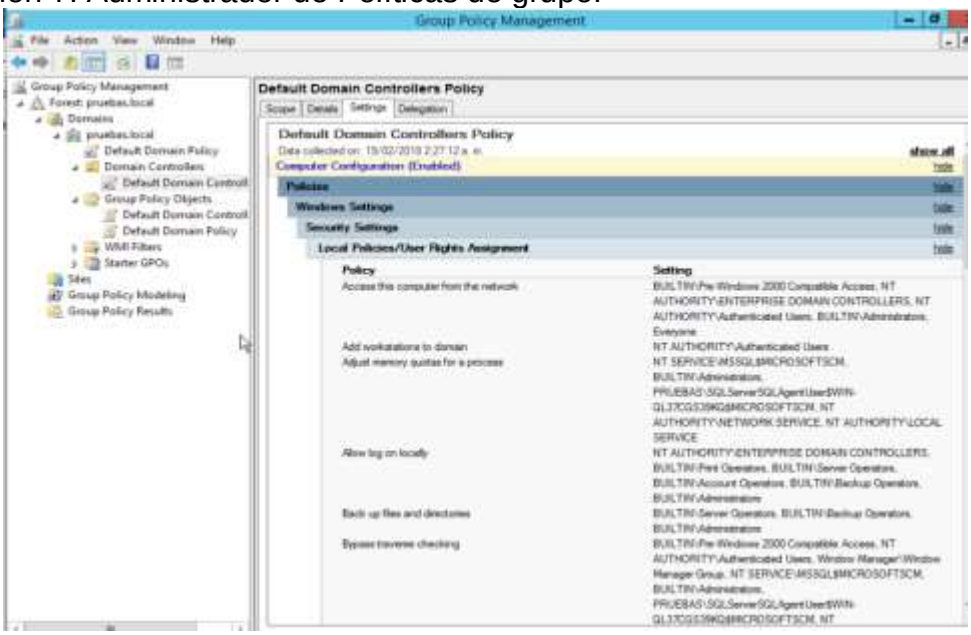
El active directory unido a las directivas de grupo en una red corporativa forman parte importante de la arquitectura de seguridad de la red de la compañía, ya que

[8] MICROSOFT, Introducción a los Servicios de dominio de Active Directory. [En línea], 2012. Disponible en https://msdn.microsoft.com/es-es/library/hh831484(v=ws.11).aspx.

allí se centran las identidades de los usuarios, se controlan los accesos a la mayoría de los recursos de la red y se configuran condiciones en forma de políticas de seguridad apoyando la mitigación de riesgos informáticos. Las ventajas que trae tener un active directory se observan sobre todo en redes grandes, ya que es posible de manera centralizada la administración de los recursos de red, siendo posible configurar de manera organizada ejemplo, por áreas la compañía dentro del árbol del active directory y lograr aplicar políticas de dominio por usuario, unidad organizativa, grupo de usuarios y por equipos.

El active directory jerárquicamente está compuesto por un bosque (forest), los dominios del bosque y las unidades organizacionales de cada dominio.
Esta herramienta, aunque viene dispuesta en cualquier Windows server requiere de un licenciamiento a nivel de usuario denomina “Client Access License” CAL.

Ilustración 7. Administrador de Políticas de grupo.



Fuente: El autor.

En la anterior ilustración se muestra a través de la herramienta de administración de políticas de grupo, como se conforma el árbol o forest, que dominio lo compone, las unidades organizativas etc, también mediante esta herramienta es posible hacer las configuraciones de directivas o políticas de grupo y en sí toda su la administración.

- **MSAT (Microsoft Security Assessment Tool).**

Es una herramienta gratuita diseñada por Microsoft para aquellas organizaciones que presentan menos de 1000 empleados mediante un cuestionario a base de más

de 200 preguntas bien orientadas y priorizadas que ayudan a evaluar las debilidades que presenta el entorno de seguridad TI, estas preguntas están categorizadas como, infraestructura, aplicaciones, operaciones y usuarios. Funciona haciendo evaluaciones continuas con el objetivo de siempre tener monitoreadas los puntos detectados buscando la fortificación de estos[9].

Ilustración 8. Fases guía gestión de riesgos.

Fuente: El autor.

Dentro de la evaluación que hace esta herramienta analiza la seguridad tanto en procesos, redes, servidores, usuarios, dispositivos móviles y los activos de datos. La herramienta tiene la capacidad de dar respuesta y recomendaciones a cada pregunta las cuales están basados en los estándares ISO 17799 y NIST-800x, así como recomendaciones presentadas por el Grupo Trustworthy Computing de Microsoft entre otras fuentes que trabajan en el área de la seguridad Informática.

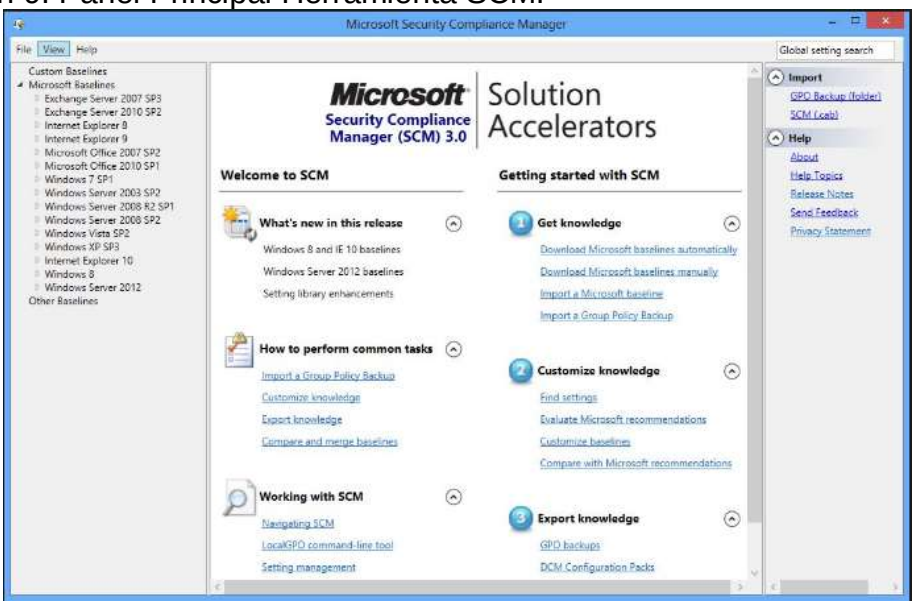
- **SCM (Security Compliance Manager).**

Esta herramienta construida por Microsoft la cual puede ser descargada de forma gratuita, e instalada en forma local o en red pretende realizar un análisis y verificar el cumplimiento de los servidores Windows para así mismo orientar los ajustes de seguridad que se deban realizar, sin embargo, Microsoft sugiere que la decisión de cada ajuste sea verificada y ajustada según la necesidad o también basada en la experiencia del profesional de tecnología. Esta herramienta puede ser descargada en forma gratuita para las versiones de los sistemas operativos[10].

[9] MICROSOFT, Herramienta de Evaluación de Seguridad de Microsoft (MSAT). [En línea]. 2018. Disponible en https://technet.microsoft.com/es-xl/library/cc185712.aspx.
[10] MICROSOFT, Security Compliance Manager (SCM). [En línea]. 2017. Disponible en https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx

- ✓ Windows Server, 2003, 2008, 2008R2, 2012 y 2016
- ✓ Windows Cliente, XP, Vista, 7, 8 y 10.

Ilustración 9. Panel Principal Herramienta SCM.



Fuente: El autor

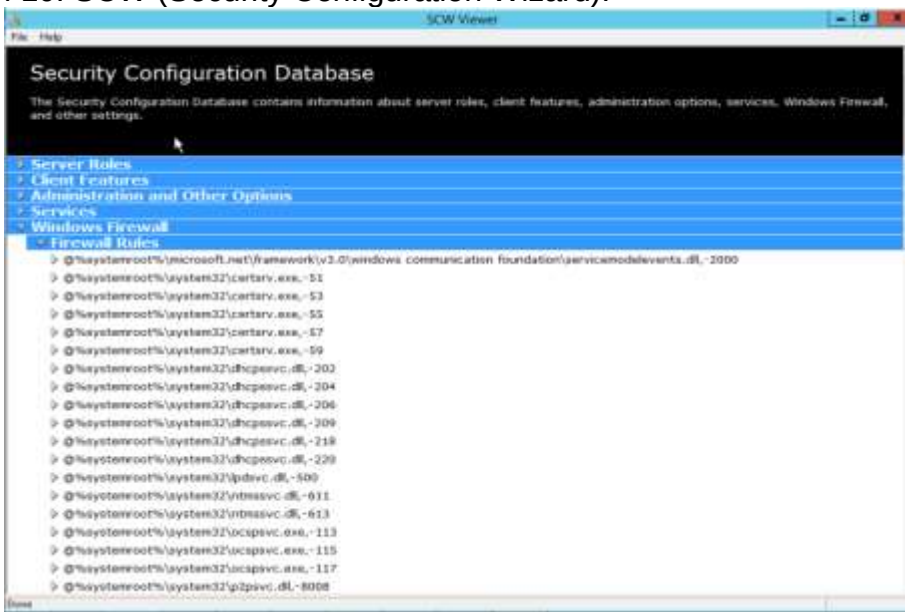
Dentro de la utilización de esta herramienta Microsoft la sugiere para servidores independientes que no estén conectados a un dominio, la cual puede llegar a entregar lineamiento o plantillas basadas en directivas de grupo para el endurecimiento del sistema basadas en la guía de seguridad de Microsoft. Dentro del alcance observado en la herramienta SCM, también existe la herramienta para asegurar el cumplimiento de Internet Explorer, Exchange y Office.

- **SCW (Security Configuration Wizard).**

Esta herramienta que está directamente disponible sin necesidad de instalación en un servidor Microsoft Windows Server 2008 R2 y Windows Server 2012, permite la construcción, edición o aplicación de una política de seguridad, generando un archivo tipo XML el cual puede llegar a configurar los servicios, las llaves de registro la seguridad de la red y una política de auditoria. Estas parametrizaciones se basan en los roles de Windows, lo cual puede generar el aseguramiento necesario para un servidor de archivos, un print server o un controlador de dominio, también tiene la capacidad de la configuración del Firewall de Windows[11]..

[11] MICROSOFT, Asistente de configuración de seguridad. [En línea], 2018. Disponible en https://technet.microsoft.com/en-us/library/cc754997(v=ws.11).aspx

Ilustración 10. SCW (Security Configuration Wizard).



Fuente: El autor.

En la ilustración anterior se muestra toda la base de datos de configuraciones que existe en la herramienta, con la cual se logran ajustes a nivel de Roles, características de cliente, servicios, firewall de Windows y otras opciones de administración. Al ejecutar el asistente este detecta los servicios o roles instalados en dicho servidor y lo va guiando al implementador hasta lograr la política ideal, al final configura una política de auditoria que servirá para algún tema de investigación.

- **MBSA (Microsoft Baseline Security Analyzer)**.

Herramienta tipo escáner gratuita construida por Microsoft la cual fue diseñada para el uso fácil de cualquier profesional de TI, en la que se pueden apoyar aquellas pequeñas o medianas empresas para identificar el estado de sus sistemas a nivel de seguridad y la cual entrega orientaciones a nivel de soluciones específicas puede ser utilizada en procesos de auditoria o escaneo de vulnerabilidades. Con esta herramienta se logran descubrir los errores más comunes de configuración a nivel de seguridad y las actualizaciones de seguridad faltantes en los sistemas informáticos, como sistemas operativos u otros productos Microsoft. Puede ser instalada de manera local en el servidor que se requiere analizar o desde un servidor realizar escaneos a través de la red a otros equipos o servidores. La última versión a la fecha tiene soporte para los sistemas operativos Windows XP, Vista, 7, 8, 8.1, Server 2003, 2008 R2, 2008, 2012 R2 y 2012.

Ilustración 11. Microsoft Baseline Security Analyzer.

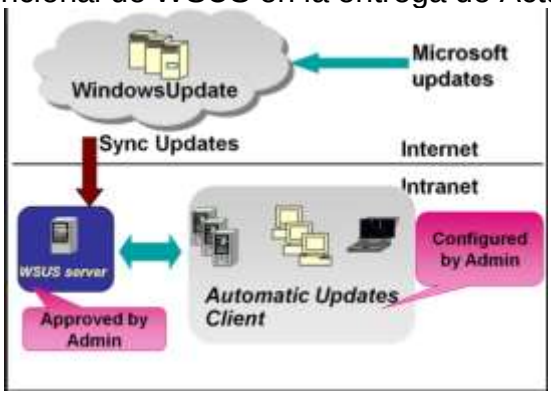
Fuente: El autor.

- **WSUS (Windows Server Update Services).**

Es una herramienta construida por Microsoft como complemento a la identificación de vulnerabilidades en los sistemas operativos Microsoft o en general software Microsoft. Tiene la capacidad de administrar y distribuir las actualizaciones liberadas por el fabricante Microsoft a través de su sitio público en internet Microsoft Update y que son requeridas por el software Microsoft que ha sido escaneado en la red. Esta herramienta se encuentra como un rol dentro de los sistemas operativos Windows Server, se recomienda siempre tener la versión más actualizada o superior a los sistemas operativos Microsoft o software Microsoft instalados en la organización para que se logre la entrega de las actualizaciones más cercanas y actualizadas liberadas por el fabricante.

WSUS es muy utilizada en las organizaciones que mantienen sistemas Microsoft, debido a su compatibilidad natural arquitectura flexible y fácil de implementar. Dentro de esta arquitectura se destaca que puede ser utilizada en organizaciones de muy pocos computadores o en organizaciones que presentan varias oficinas de manera distribuida, para este último caso WSUS puede ser instalado de manera distribuida y ser administrado en una sola consola o un solo servidor. Dentro de los requisitos para su configuración también se observa que puede habilitarse a través de políticas de dominio Windows lo cual es la mejor solución. también tiene la posibilidad de ser configurado individualmente modificando llaves de registros en todos los anfitriones que quieran entrar en la zona de entrega de actualizaciones.

Ilustración 12. Flujo funcional de WSUS en la entrega de Actualizaciones.



Fuente: blogs.msdn.microsoft.com.

En la solución de WSUS se tiene una clasificación de las actualizaciones, indispensable conocer para identificar las que son orientadas al aseguramiento de los productos Microsoft para el caso Windows Server, así como se pueden observar en la siguiente ilustración:

Ilustración 13. Clasificación de actualizaciones.

Clasificación de actualizaciones	Descripción
Actualizaciones críticas	Correcciones para problemas específicos que solucionan errores relacionados con seguridad no críticos.
Actualizaciones de definiciones	Actualizaciones de virus u otros archivos de definición.
Controladores	Componentes de software diseñados para admitir nuevo hardware.
Paquetes de características	Nuevas versiones de característica, normalmente incorporadas en los productos en la próxima versión.
Actualizaciones de seguridad	Correcciones de productos concretos, solución de problemas de seguridad.
Service Packs	Conjuntos acumulativos de todas las revisiones, actualizaciones de seguridad, actualizaciones críticas y actualizaciones creadas desde el lanzamiento del producto. Service packs también podrían contener un número limitado de características o cambios de diseño solicitados por el cliente.
Herramientas	Utilidades o características que ayudan a realizar una tarea o un conjunto de tareas.
Paquetes acumulativos de actualizaciones	Un conjunto acumulativo de revisiones, actualizaciones de seguridad, actualizaciones críticas y otras actualizaciones que se recopilan para facilitar la implementación. Un paquete acumulativo suele estar dirigido a un área específica, como la seguridad, o un componente específico, como Internet Information Services (IIS).
Actualizaciones	Correcciones para problemas específicos que solucionan errores relacionados con seguridad no crítico.

Fuente: www.microsoft.com.

- **Catálogo de Microsoft Update.**

Es una herramienta Online en forma de portal web creada por el fabricante Microsoft desde que salió la versión de Windows 2000 en donde expone todas aquellas actualizaciones para sus productos y en la cual puede encontrarse hasta los últimos

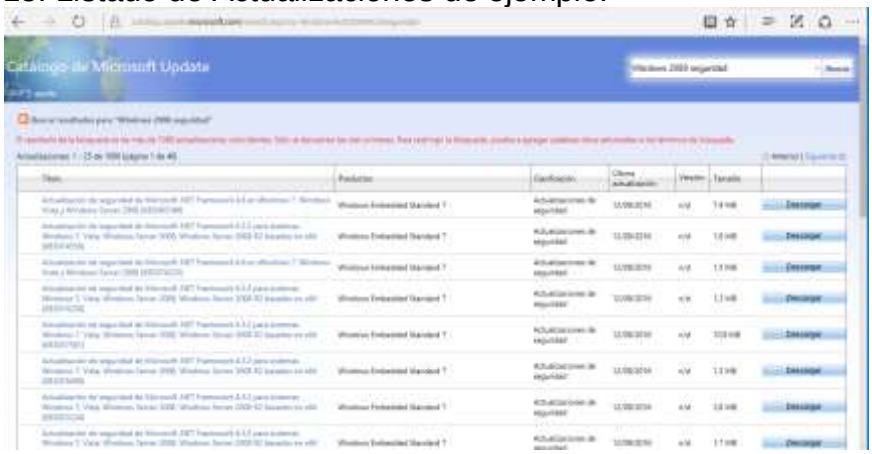
sistemas operativos lanzados, estas mismas actualizaciones son las entregadas por el servicio de Windows Update y por el cual se alimenta la herramienta WSUS, o todos los sistemas operativos Windows que se conectan a internet y requieren tomar actualizaciones directamente. En este portal no solo se encuentran actualizaciones de los sistemas operativos sino de la mayoría de los productos distribuidos por Microsoft, el portal comprende de un buscado en donde se puede obtener por producto lo requerido, y su descarga está relacionada a un código KB (Knowledge Base).

Para el acceso la url de este sitio es: ***https://www.catalog.update.microsoft.com.***

Ilustración 14. Portal Web Catalogo de Microsoft Update.

Fuente: El autor.

Ilustración 15. Listado de Actualizaciones de ejemplo.



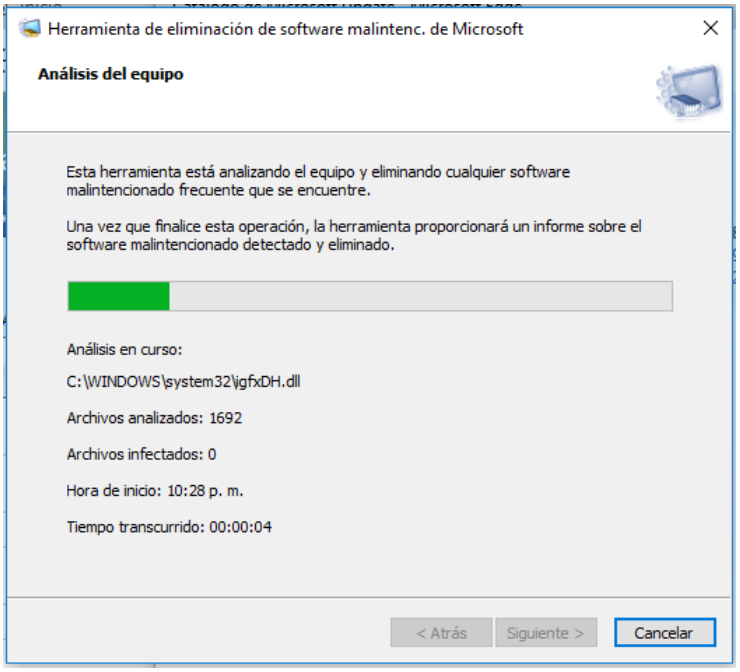
Fuente: El autor.

- **MSRT (Microsoft Malicious Software Removal Tool).**

Es una herramienta construida por Microsoft de descarga gratuita, quien tiene la habilidad de detectar y eliminar software y códigos maliciosos denominado también

malware en sistemas operativos Microsoft server o de estación de trabajo, desde Windows XP hasta Windows server 2012 R2.
Esta herramienta es publicada una vez al mes por Microsoft, luego de su descarga se ejecuta quien realiza un proceso de escaneo y limpieza del código o software malicioso como Blaster, Sasser o Mydom entre otros.

Ilustración 16. Microsoft Malicious Software Removal Tool.



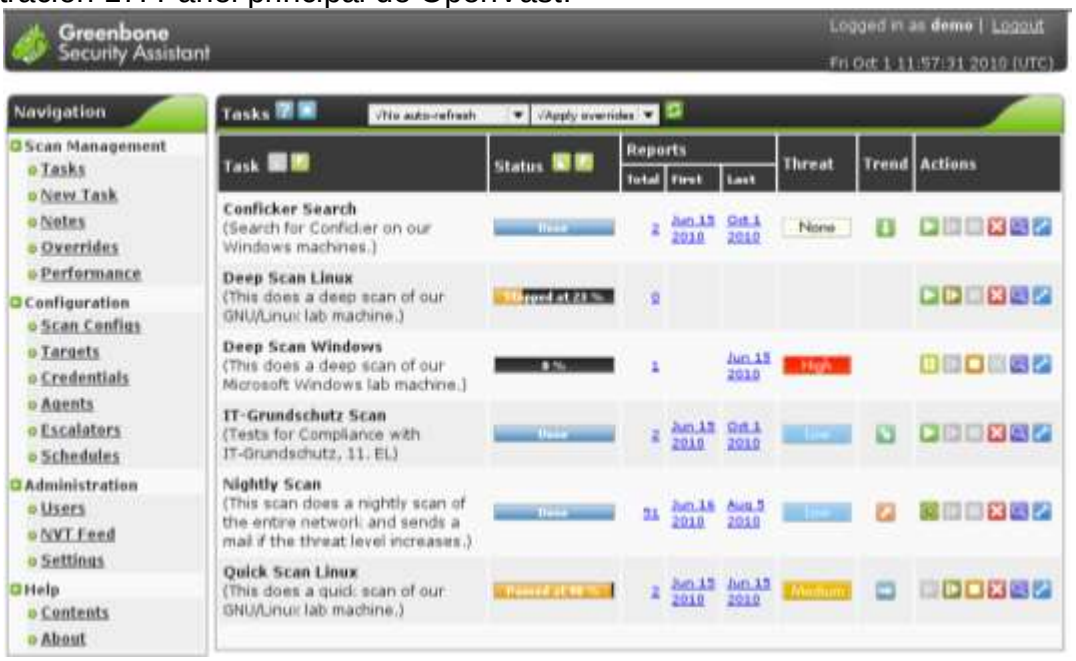
Fuente: El autor.

- **OpenVAS (Open Vulnerability Assessment System).**

En una herramienta libre de escaneo de vulnerabilidades o fallas de seguridad en los activos informáticos conectados a una red IP, licencia de uso bajo la GNU General Public License (GNU GPL). Su motor de escaneo solo es compatible en Sistemas Operativos Linux, pero sus clientes si pueden ser Windows. Este sistema recibe actualizaciones en sus bases de datos de los test de vulnerabilidad de red o Siglas en Ingles NVT, las cuales son más de 50000 en total.

Esta herramienta permite la configuración de activos agrupados, configuración de falsos positivos y configuración de tareas programadas para sus escaneos. Posee una interface gráfica de usuario GUI, ver Ilustración 13, así como una consola de comando desde donde puede ser administrado.

Ilustración 17. Panel principal de OpenVast.



Fuente: www.networkworld.com.

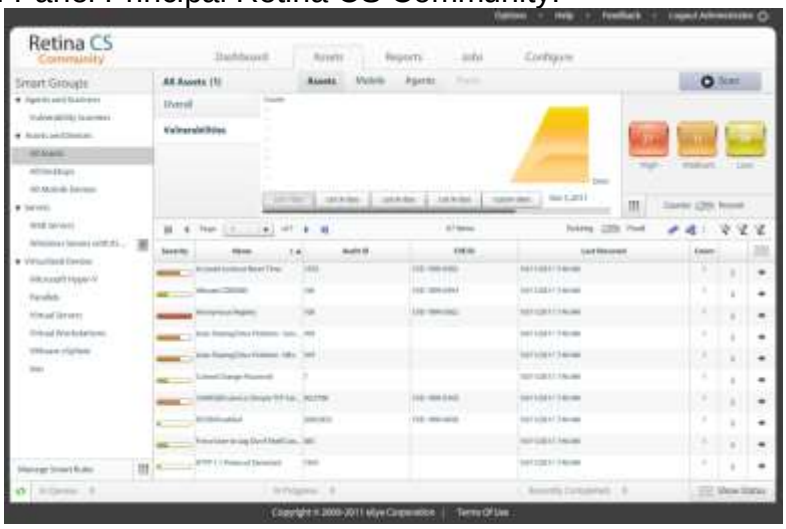
- **Retina CS Community.**

Es una herramienta basada en software que tiene la capacidad de escanear vulnerabilidades de día cero con ciertas limitantes en su edición libre, su capacidad de gestión máxima es de 256 direcciones IP. También tiene la capacidad de detectar vulnerabilidades en sistemas operativos Móviles, aplicaciones web, aplicaciones virtualizadas, servicios en la nube, problemas de configuración y determinar parches faltantes en los sistemas escaneados. También tiene la particularidad de detección de Malware y ataques.

En los requerimientos de instalación son Sistema Operativo Windows Server 2008 o superior, .NET Framework 3.5, Internet Información Services y Microsoft SQL 2008 o superior.

Para su gestión cuenta con una interface gráfica de usuario (GUI) en forma de cliente, ver Ilustración 14, y una interface WEB para gestión del sistema. Cuenta con una variedad de plantillas pres configurados que sirven de guía al administrador para las tareas de escaneo de vulnerabilidades.

Ilustración 18. Panel Principal Retina CS Community.

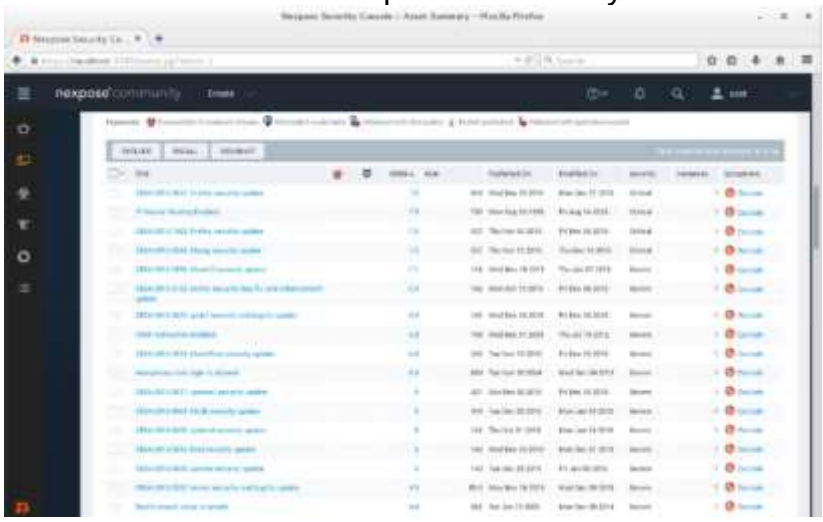


Fuente: www.networkworld.com.

- **NeXpose Community Edition.**

Es una herramienta de escaneo de vulnerabilidades con la capacidad de detección en Sistemas Operativos, aplicaciones web, bases de datos y sistemas virtualizados. Esta Versión está limitado al escaneo de 32 IPs simultáneas. Para su activación se debe solicitar una licencia de uso la cual debe ser renovada anualmente.
Esta herramienta puede ser instalada en Windows, Linux, Físicas o Virtualizadas y su interface de agestión es Web desde donde es administrada tanto la configuración de activos y tareas de escaneo requeridas Ver Ilustración 15. La presentación de sus informes no solo muestra las vulnerabilidades sino como deben ser corregidas.

Ilustración 19. Consola de Gestión NeXpose Community Edition.



Fuente: nexpose.help.rapid7.com.

2.1.4 Determinación de metodología y herramientas.

Según la investigación realizada anteriormente y expuesta en este documento en cuanto a las metodologías de análisis y gestión de riesgos, mejores prácticas y herramientas para el aseguramiento de sistemas informáticos, se ha concluido que la metodología para el objetivo de este proyecto, nace de tomar como base las anteriores metodologías investigadas para ofrecer una metodología enfocada y simplificada al aseguramiento de sistemas operativos, la cual se presentará como "*CICLO DE ASEGURAMIENTO DE SERVIDORES WINDOWS SERVER",* el cual podrá ser consultado en el capítulo 7 de este documento.

En la selección de las herramientas se observa que dependiendo del tamaño de la organización y a su vez del presupuesto de esta para las áreas de TI o Seguridad Informática se selecciona la más apropiada sin embargo para el caso de una empresa con pocos servidores, es suficiente escoger la siguiente configuración de herramientas:

- ✓ **SCM (Security Compliance Manager),** Herramienta gratuita con la que se Identificara el cumplimiento a nivel de seguridad.
- ✓ **MBSA (Microsoft Baseline Security Analyzer),** Herramienta gratuita con la cual a base de escaneos se detectarán las vulnerabilidades y errores de configuración del sistema operativo Windows Server.
- ✓ **WSUS (Windows Update Services).** Herramienta como solución ideal para la gestión y despliegue de parches o actualizaciones de seguridad a los sistemas operativos Windows Server.
- ✓ **Antimalware**, Solución no gratuita que se selecciona como una mejor practica que debe ser instalada sobre el sistema operativo Windows Server capaz de detectar y detener código malicioso.
- ✓ **WFAS (Windows Firewall Advanced Security),** Solución incluida en la licencia de Windows Server 2008 o 2012, la cual debe habilitarse y configurarse según funcionalidad y condición en la red del servidor.

2.2 MARCO HISTORICO

Revisando la historia del sistema operativo Microsoft Windows se encontró que la primera versión se llamaba Windows NT 3.1, la cual fue lanzada en julio de 1993, el cual podía funcionar en un entorno empresarial y trabajar en una red. Posteriormente para el año 1996 nace la versión NT 4.0 en el cual se implementa el sistema de archivos NTFS, el cual era compatible con otros sistemas operativos operando a 32 bits. Esta versión se empezó a trabajar en dos versiones WorkStation y Server, la primera se utilizaba para un entorno no empresarial pero que requería un procesamiento especial de datos y el segundo si totalmente orientado al trabajo

empresarial, esta versión venia en un entorno gráfico, multitarea y podía ser ejecutado en hardware de múltiples procesadores.
Para inicios del año 2000 es lanzada la versión Windows Server 2000 o versión NT 5.0, en la cual se hacen mejorar a nivel gráfico, así como mejoras en la operación dentro de un entorno de red, de esta versión nace una versión denominado profesional la cual fue muy utilizada en las casas y para correr juegos bastante exigentes.
Posteriormente para el año 2003 es lanzada la versión Windows Server 2003 o versión NT 5.2 uno de los sistemas operativos más utilizados y que aún existen compañías que lo tienen en producción debido a su estabilidad y compatibilidad a nivel ejemplo con ".NET".
En esta versión de sistema operativo es desarrollada la primera versión compatible con procesadores a 64 bits, el cual tenía cierto rendimiento beneficioso, así como la compatibilidad que podía ofrecer a nivel de memoria RAM.

Ilustración 20. Ediciones de Microsoft Windows.

NT Ver.	Nombre	Ediciones	Fecha lanzamiento
NT 3.1	Windows NT 3.1	Workstation, Advanced Server	Julio 1993
NT 3.5	Windows NT 3.5	Workstation, Server	Septiembre 1994
NT 3.51	Windows NT 3.51	Workstation, Server	Mayo 1995
NT 4.0	Windows NT 4.0	Workstation, Server, Server Enterprise Edition, Terminal Server, Embedded	Julio 1996
NT 5.0	Windows 2000	Professional, Server, Advanced Server, Datacenter Server	Febrero 2000
NT 5.1	Windows XP	Home, Professional, Media Center (2004 & 2005), Tablet PC, Starter, Embedded, N, 64 bit edition (IA-64)	Octubre 2001
NT 5.2	Windows Server 2003	Standard, Enterprise, Datacenter, Web, XP Pro x64	Abril 2003
NT 5.1	Windows Fundamentals for Legacy PC	Versión recortada de Windows XP con menos complementos, hecha especialmente para PCs con menores prestaciones.	Julio 2006
NT 6.0	Windows Vista	Starter, Home Basic, Home Premium, Business, Enterprise, Ultimate (la única versión que no está disponible para equipos de 64 bits es la versión Starter, ya que es una versión para equipos básicos)	Enero 2007
NT 6.0	Windows Server 2008	Standard, Enterprise, Datacenter, Web, Storage, Small Business Server	Febrero 2008
NT 6.1	Windows 7	Starter, Home Basic, Home Premium, Professional, Ultimate, Enterprise (al igual que en Vista, la versión Starter no dispone de soporte para 64 bits)	Octubre 2009
NT 6.1	Windows 7 N	Home Premium N, Professional N, Ultimate N	Octubre 2009
NT 6.2	Windows 8	Windows 8, Windows 8 Pro	Octubre 2012

Fuente: http://www.redtauros.com/.

En el año 2008 Microsoft lanza la versión de Windows Server 2008 o denominada versión NT 6.0, pero que posteriormente es lanzada la versión de Windows 2008 R2, al cual se hacen varias mejoras a nivel de características dentro de las relevantes esta PowerShell, Server core, entre otras. Esta versión muy utilizada en la actualidad sigue operando en bastantes compañías, dentro las opciones que se incorporan es el uso organizado de roles o características.

Windows Server 2012, el cual fue lanzado, en el año 2012, presenta una mejor apariencia, así como ofrece mayor cantidad de soporte a nivel de roles y caracteres, con Windows server 2012 se da inicio a la era del Sistema **Operativo Cloud.**

2.3 MARCO CONCEPTUAL

Aseguramiento del Sistema Operativo. Es el proceso con el cual se pretende disminuir cualquier riesgo informático detectado en estos, utilizando mejores prácticas, herramientas de protección o realizando actualizaciones o ajustes entregados por fabricante al software.

Sistema Operativo. Este es el programa o software imprescindible de una computadora, ya que es requerido o es la base para que funcionen otros programas, también tiene como función el manejo o el control de los puertos USB, Tarjeta de red, Video, información del disco duro, o el manejo de periféricos como teclado, impresora, etc. Existen muchos sistemas operativos de diferente marca y para diferente tipo de dispositivo, como lo son para estación de usuario final Windows, MAC OS, así como sistemas operativos para dispositivos móviles como, Android, IOS, BlackBerry, Palm OS, Firefox OS, Symbian Windows Mobile, Ubuntu Phone OS entre otros que pueden estarse desarrollándose en este momento, en esta clasificación también podemos encontrar que dentro de los sistemas operativos se encuentran para servidores de los cuales los más utilizados son Windows server, Unix, Linux, FreeBSD, Novel network, y Solaris.

Tipos de Sistemas operativos. Estos se pueden clasificar según la administración de tareas o por la administración de usuarios así:

- Monotarea, es capaz de procesar o ejecutar un solo programa o tarea al tiempo.
- Multitarea, Son aquellos que son capaces de ejecutar múltiples tareas o ejecutar múltiples programas, así como pueden ser manipulados por más de un usuario al tiempo. Este tipo sistema operativo son los más modernos.
- Monousuario, sistema operativo donde solo un usuario a la vez puede trabajar, aunque puede ejecutar cualquier operación en el mismo.

- Multiusuario, es al cual en donde varios usuarios ejecutar servicios al mismo tiempo o simultáneamente, en este caso se comparten recursos de hardware o software como lo es memoria, procesador y las aplicaciones o programas instalados sobre el mismo disco duro.
-

Aunque hemos hecho un recorrido resumido de lo que es un sistema operativo tipos marcas etc, nos vamos a orientar a trabajar solo en sistemas operativos Windows server.

Windows Server. Es un grupo de sistemas operativos que se consideran que están entre los más utilizados y populares del mundo desarrollado por Microsoft Corporation. Vienen en arquitecturas de 32 y 64 bits y las versiones que actualmente están en operación son las siguientes:

- Windows Server 2003, y 2003 R2. Aunque es un Sistema operativo que ya no tiene soporte por el fabricante desde mediados del 2015 ya que cumplió su ciclo de vida, todavía existen varias compañías que lo siguen utilizando, por lo anterior se le debe incluir en los procedimientos de soporte, pero también se debe ir pensando en su migración a sistemas operativos Windows actuales.

- Windows Server 2008, y 2008 R2. Este sistema operativo, siendo más reciente también presenta cierto grado de obsolescencia según políticas de uso de Microsoft, cuyo fin de soporte extendido está hasta el año 2020 solo aplica a aquellas empresas que pagan este soporte.

- Windows Server 2012, y 2012 R2. Es el sistema operativo Windows server más moderno que está en operación en varias compañías actualmente, aunque a la fecha ya se encuentra disponible la versión de Windows Server 2016, estas versiones están enfocadas para lograr trabajar o prestar sus servicios para la nube.

Escáner de Vulnerabilidades. Es un sistema basado en software el cual tiene la capacidad de detectar, analizar y valorar las redes IP descubriendo posibles vulnerabilidades en sus dispositivos conectados o activos informáticos y determinando el nivel de riesgo existente. Dentro de sus capacidades también tiene la de entregar las posibles soluciones para remediarlas.

Ciclo de remediación. En el proceso cíclico o repetido en el cual se realizan los procesos de detección, análisis y remediación o aseguramiento de vulnerabilidades del sistema operativo.

Vulnerabilidad informática. Es una debilidad o falta de control informático, el cual puede facilitar que una amenaza actúe provocando algún atentado sobre la información, los servicios o la infraestructura TI que los soportan. Las

vulnerabilidades se clasifican por el nivel de riesgo o la cantidad de daño que se pueda generar, para lo anterior se encuentran las vulnerabilidades clasificadas, en Informativas, bajas, medias y Altas o Criticas.

2.4 MARCO LEGAL

LEY 1273 DE 2009, *(5 de enero del 2009)*

> *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*[12]

[12] Ley 1273 de 2009, [en línea], Bogotá Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

3 MARCO METODOLOGICO

En esta sección se describe como se realizará el proceso de investigación y los métodos que se utilizarán para la recolección de la información.

3.1 FORMA DE INVESTIGACIÓN

Para lograr el objetivo de este proyecto quien esta alimentado por un proceso de investigación de herramientas mejores prácticas y metodologías de aseguramientos de servidores Windows server, se debe realizar un proceso investigativo y comparativo de información en internet, biblioteca, desde diferentes fuentes y fabricantes etc, con la cual se pueda distinguir unas razones concluyentes para encontrar la metodología que se va a diseñar.

3.2 METODOS DE INVESTIGACION

Esta investigación estará basada en toda la recolección y análisis de información tomada desde sus diferentes fuentes bibliográficas consultadas en Internet a diferentes fabricantes de software como Microsoft, o software para el apoyo de aseguramiento de sistemas informáticos o metodología de gestión de riesgos, para así definir el desarrollo de la propuesta de metodología de aseguramiento de servidores Microsoft Windows Server. Dentro de este método se realiza una aplicación de la metodología sugerida buscando con esto una mejor explicación de este al interesado.

4 CICLO DE ASEGURAMIENTO DE SERVIDORES WINDOWS SERVER

El fabricante Microsoft ha evolucionado sus sistemas operativos Windows server pasando de las versiones bases y antiguas NT a lo que hoy se conoce y que las organizaciones normalmente tienen activo Windows server 2003, 2008 y 2012 así como la nueva versión 2016. Temas como la seguridad sobre Windows, para Microsoft es bastante serio ya que por ser unos de los sistemas operativo más conocidos y fácil de utilizar es así mismo uno de los más atacados, por ello para Microsoft el ciclo de vida de las soluciones es algo que lo hacen cumplir a cabalidad, guiando con esto a las compañías para que mantengan sus sistemas operativos en versiones soportadas, estables y seguras. Todo lo anterior es ofrecido por el fabricante Microsoft, pero ahí es donde este proyecto a trabajar buscará el complemento entre los servicios de soporte en seguridad de Microsoft y una buena cultura organizacional utilizando las mejores prácticas en cuanto al aseguramiento de los sistemas operativos MS Windows server.

En la ilustración llamada “Ciclo de aseguramiento de Servidores Windows Server.”, muestra la metodología que se plantea con el objetivo de mantener un aseguramiento continúo enfocado exclusivamente a los servidores Windows Server, el cual se llama “**Ciclo de aseguramiento de servidores Windows Server**”.

Esta propuesta metodológica que pretende ser de fácil aplicación a cualquier organización está basada en las fases observadas de las metodologías como lo es MAGERIT, OCTAVE, OWASP básicamente, en las cuales se tienen en cuenta la identificación de activos como fase inicial, el análisis de riesgos de los mismos basados en las amenazas y vulnerabilidades detectadas y una fase final como son los planes de gestión de riesgos los cuales contemplan los salvaguardas o controles informáticos que apoyarán en la reducción de estos.

El enfoque principal de esta metodología es una configuración previa de manera ideal del servidor y luego unos ajustes a nivel de seguridad guiados por alguna herramienta de escaneo de vulnerabilidades, posteriormente este proceso deberá quedar operando de manera cíclica hasta el momento en que se de baja el servidor o activo informático en la organización. Los ajustes a os servidores Windows que entregan los escáneres de vulnerabilidades podrán contener directrices para aplicar un parche o actualización de Microsoft u otro software instalado en este, o configuraciones en alguna llave de registro.

Ilustración 21. Ciclo de aseguramiento de Servidores Windows Server.

Fuente: El Autor.

Preparación del aseguramiento de tecnología informática.
A continuación, se nombran algunos ítems relevantes y previos que se deben tener en cuenta en el proceso de aseguramiento de sistemas MS Windows server o en otros activos informáticos.

1. Tener un inventario de activos de TI.
2. Selección de un escáner de vulnerabilidades TI,
3. Selección de una herramienta de distribución de actualizaciones de seguridad.
4. Selección de un software antimalware.
5. Contratos con entidades de seguridad para realizar pruebas de penetración una o dos veces al año.

4.1 INVENTARIO DE ACTIVOS INFORMÁTICOS

En esta fase la cual se considera como la parte inicial y básica del análisis de riesgos informáticos, de la cual parte cualquiera de las metodologías de análisis y gestión de riegos como son MAGERIT, OCTAVE, OWASP y DAFP, se debe realizar un inventario de activos en los cuales se debe describir servidores, sistemas

operativos, servicios instalados o aplicaciones, base de datos, usuarios de servicios como los usuarios administradores del sistema autorizados para el acceso.

Para este inventario se debe tener dos formas de conseguir la información una puede ser manual en la cual se deben hacer análisis particulares por segmentos de red adicionalmente con la entrevista de cada administrador del sistema informático, o a través de un método mixto utilizando alguna herramienta de gestión e inventario de activos más las entrevistas con los administradores de los servicios TI, esto también dependiendo del tamaño de la organización, sin embargo se aconseja el segundo método ya que puede ser más preciso.

Para esta labor se sugiere un software de gestión de activos informáticos como lo son libres o comerciales que puedan cumplir con los estándares de gestión de las mejores prácticas ITIL (IT Infraestructura Library, biblioteca de infraestructura de TI). De igual manera este proceso se sugiere debe ir alineado con el proceso de Gestión de la configuración de ITIL si la organización lo tiene implementado.

Dentro del software que se recomienda utilizar se encuentra:

- **IT Asset Tool Management.** Software gratuito el cual no presenta a la fecha ninguna limitante en su utilización.

- **Aranda Asset Management.** Software comercial muy utilizado en la industria.

- **CA Asset Management**. Software comercial muy utilizado en la industria.

También se pueden utilizar las herramientas de escaneo de vulnerabilidades para inventariar o confirmar los activos informáticos conectados a la red de la organización.

Para lo anterior se propone se diligencia un formato que incluya la siguiente información requerida para el proceso de aseguramiento de los servidores, el cual debe estar siempre monitoreado y auditando continuamente garantizando que la información consignada siempre sea fiel y actualizada a los cambios realizados en la infraestructura TI de servidores.

<u>Matriz activos de infraestructura TI de Servidores:</u>

- ✓ Nombre del host
- ✓ Dirección IP
- ✓ Dirección Física
- ✓ Memoria RAM
- ✓ Procesador / Núcleos
- ✓ Disco duro

- ✓ Servidor (Físico / Virtual)
- ✓ Rol del servidor
- ✓ Sistema Operativo
- ✓ Servicios o aplicaciones Instalados
- ✓ Nombre Bases de datos
- ✓ Puertos, servicios o protocolos activos
- ✓ Usuarios de Servicio
- ✓ Usuarios administradores del sistema

Dentro de esta fase se debe tener determinado el nivel de importancia de los activos enfocados a servidores Windows como lo dictan las metodologías nombradas anteriormente, con lo cual dentro del ciclo de aseguramiento se le debe dar prioridad y mayor atención a estos. Esta actividad se vuelve importante para definir los tiempos y los planes de remediación a implementar dentro del ciclo.

4.2 SELECCIÓN DE HERRAMIENTA PREPARACIÓN DEL SERVIDOR

Esta etapa tiene como fin buscar la mejor alternativa a nivel de herramientas logrado que durante la preparación del servidor Windows Server, se logre la mejor configuración posible disminuyendo brechas de seguridad, llegando lo mejor posible a la siguiente etapa “Análisis de Vulnerabilidades”.

Para esta etapa encontramos herramientas incorporadas en los sistemas operativos Windows server como son las opciones a nivel de **Directivas de Grupo**, o si la compañía cuenta con un **Active Directory**, unas implementaciones de políticas de dominio.

En apoyo al aseguramiento de servidores Windows Server también existen dos herramientas que Microsoft pone a disposición y que son compatibles tanto con Windows server 2008 como con Windows server 2012 así:

- **SCM (Security Compliance Manager).** Software gratuito distribuido por Microsoft el cual puede instalarse localmente o en red y orienta a los administradores de TI en cuanto a los ajustes de seguridad que se requieran aplicar solo es compatible con sistemas operativos Windows. Esta herramienta se centra en entregar plantillas ajustadas con directivas de grupo entre otros ajustes dependiendo del rol del servidor como file server, Print server, domain controller, member server, etc.

- **SCW (Security Configuration Wizard).** Esta herramienta que está directamente disponible sin necesidad de instalación en un servidor Windows Server 2008 R2 y Windows Server 2012, permite la construcción, edición o

aplicación de una política de seguridad, generando un archivo tipo XML el cual puede llegar a configurar los servicios, las llaves de registro la seguridad de la red y una política de auditoria. Estas parametrizaciones se basan en los roles de Windows, lo cual puede generar el aseguramiento necesario para un servidor de archivos, un print server o un controlador de dominio, también tiene la capacidad de la configuración del Firewall de Windows.

4.3 SELECCIÓN DEL ESCANER DE VULNERABILIDADES TI

Esta etapa se vuelve indispensable después de que la organización entienda que tan importante es el cuidado de sus activos informáticos, teniendo en cuenta la cantidad de activos y el valor para la organización. Por lo anterior se debe realizar un análisis del costo beneficio y en donde dependiendo del gusto y el tamaño de la organización se puede escoger la solución de escaneo de vulnerabilidades.
Dentro de las opciones que se encuentran existen soluciones en software libre o software comercial, al igual que la herramienta de gestión de activos todos dependen de la organización, así como del tipo de cumplimiento que estas se les exija puede requerirse de herramientas de escaneo certificadas por alguna entidad en especial, importante que sean compatibles con CVM (Common Vulnerability and Exposure). A continuación, se nombran algunas que pueden ser utilizadas para esta labor:

- **MBSA (Microsoft Baseline Security Analyzer)**. Software gratuito distribuido por Microsoft el cual puede ejecutar escaneos de vulnerabilidades locales o en red y orienta en cuanto a los ajustes que se requieran hacer en los servidores analizados, solo es compatible con sistemas operativos Windows.

- **OpenVAS (Open Vulnerability Assessment System).** Escáner de vulnerabilidades el cual apoya en forma más amplia y generalizada en cuanto a las vulnerabilidades existentes en los activos conectados a la red, la ventaja de este tipo de escáner es que no limita la compatibilidad en cuanto a los sistemas operativos.

- **Retina CS Community.** Escáner de vulnerabilidades basado en software libre, el cual puede escanear vulnerabilidades en cualquier activo informático conectado a la red.

- **NeXpose Community Edition.** Escáner de vulnerabilidades basado en software libre, el cual puede escanear vulnerabilidades en cualquier activo informático conectado a la red. Existe una versión libre y otra versión

comercial la cual puede realizar escaneo a mayor cantidad de activos TI conectados a la red además contiene otros beneficios adicionales.

4.4 SELECCIÓN DE UNA HERRAMIENTA DE DISTRIBUCIÓN DE ACTUALIZACIONES DE SEGURIDAD

Es importante tener una buena herramienta que tenga la capacidad de entrega o despliegue de parches o software de actualización hacia los sistemas operativos servidor, dentro de estos se encuentran herramientas que entrega el fabricante Microsoft como de otros fabricantes la ventaja que tienen algunas herramientas de terceros es que adicionalmente a la entrega de los parches de Microsoft, también entregan actualizaciones a otras aplicaciones.

- **WSUS (Windows Server Update Services).** Esta herramienta dispuesta por Microsoft de forma ideal para los productos Microsoft debe ser implementada en cualquier organización que tenga sistemas operativos Microsoft Windows. Ya que sus servicios a nivel de gestión de actualizaciones de productos Microsoft puede ser administrada de manera centralizada sin importar el tamaño de la organización o la cantidad de sedes o servidores que pueda tener lo importantes es que estén conectadas entre sí de algún modo para que los servidores WSUS puedan sincronizarse.

  *Dentro de las opciones de WSUS se encuentra Offline Update***,** esta opción permite generar un archivo ISO el cual contendría las actualizaciones descargadas el cual puede ayudar en ciertos casos a disminuir consumo de ancho de banda o tiempo, sobre todo en los casos donde no se puede tener un servidor de WSUS y que se tenga un ancho de banda bajo. Este tipo de solución vuelve portable la solución.

4.5 SELECCIÓN DE UN SOFTWARE ANTIMALWARE

Esta etapa debe ser previa y hace parte importante del proceso de aseguramiento de los servidores Windows Server, ya que tiene como objetivo seleccionar un software antimalware el cual se instalará en el servidor Windows server y debe tener la capacidad de detectar y contener o eliminar cualquier código malicioso (virus, spyware, gusanos, etc) que logre llegar al servidor. En este proceso se debe escoger un software compatible de gestión centralizada sobre todo para empresas que tengan varios servidores y en última generación dentro de esta selección se pueden nombrar algunas marcas reconocidas:

- ✓ Trend Micro
- ✓ Kaspersky Lab
- ✓ Mcafee
- ✓ Symantec
- ✓ Sophos
- ✓ Palo Alto Networks
- ✓ Eset
- ✓ Bitdefender

4.6 PLANEACIÓN ANÁLISIS DE VULNERABILIDADES

En esta fase se debe establecer los cronogramas de escaneo de las vulnerabilidades, como la ventana requerida para la remediación o parcheo de los servidores. Se debe tener en cuenta que como el proceso lo indica esta labor es cíclica la cual debe repetirse indefinidamente hasta que la solución que esta puesta en producción desaparezca de la organización si esto se llega a dar.

Se deben configurar tareas de escaneos trimensuales como máximo en servidores en general, para los casos de servidores muy críticos o muy expuestos se deben programar estas tareas más seguidas, durante esta planeación se debe tener en cuenta el tiempo que puede tardar un administrador del sistema en dar cierre a las mismas o coordinar las ventanas de mantenimiento con la organización o sus asociados. Como ayuda a la programación y coordinación de estas actividades se debe tener en cuenta que en el caso de los servidores Windows el fabricante Microsoft publica parches o actualizaciones el segundo miércoles de cada mes, pero para casos de emergencia envía las actualizaciones de inmediato. Estas actualizaciones críticas o de emergencia deben ser instaladas lo antes posible ya que los agentes maliciosos intentarán explotarlas antes de que se logren la remediación en los sistemas afectados, por lo anterior aplicando un proceso en ITIL esto se puede considerar un “cambio de emergencia”.
Cronograma de tareas de Escaneo:

En este cronograma se deben listar todos los servidores a escanear y se colocaran sus fechas y horas determinadas. En organizaciones que tengan demasiados servidores es importante que estas tareas se ejecuten en grupos modestos de servidores y en horarios no productivos para no generar indisponibilidad o lentitud de los sistemas, así mismo se debe tener en cuenta las ventanas de mantenimiento teniendo en cuenta el impacto mínimo que esto pueda generar a la operación de la organización.

Ilustración 22. Cronograma de aseguramiento de servidores.

CRONOGRAMA DE ASEGURAMIENTO DE SERVIDORES
Escaneo y Remediación de Vulnerabilidades

AÑO 2017

ACTIVO TI	Horario Ventana	TIPO DE ACTIVIDAD	ENE		FEB		MAR		ABR		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC		TOTAL		PORCENTAJE EJECUTADO %
			Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	Programado	Ejecutado	
SERVIDOR_1	18:00	Escaneo Vul Srv	1	1					1	1					1	1					1						4	3	75
	3:00	Remediación Srv			1			1																			1	1	100
SERVIDOR_2	21:00	Escaneo Vul Srv					1	1					1	1					1	1					1	1	4	4	100
	2:00	Remediación Srv					1					1			1												2	1	50
SERVIDOR_3	21:00	Escaneo Vul Srv	1	1					1	1					1	1					1						4	3	75
	2:00	Remediación Srv			1			1																			1	1	100
SERVIDOR_4	0:00	Escaneo Vul Srv	1	1					1	1					1	1					1						4	3	75
	4:00	Remediación Srv			1			1																			1	1	100
SERVIDOR_5	0:00	Escaneo Vul Srv	1	1					1	1					1	1					1						4	3	75
	4:00	Remediación Srv			1			1																			1	1	100
SERVIDOR_6	0:00	Escaneo Vul Srv	1	1					1	1					1	1					1						4	3	75
	4:00	Remediación Srv			1			1																			1	1	100
																										TOTALES =	31	25	81

Fuente: El autor.

4.7 ESCANEO DE VULNERABILIDADES

En esta fase se deben configurar los equipos de escaneo de vulnerabilidades, en los cuales se deben configurar las plantillas que vienen prediseñadas, pero también se deben configurar las excepciones como son puertos, protocolos, servicios conocidos y en ciertos casos vulnerabilidades o riesgos aceptados.
También se debe hacer para una mejor gestión agrupamiento de servidores o servicios ya que su consolidación puede generar una labor posterior resumida referida al proceso de remediación de vulnerabilidades.
En esta parte también se deben realizar la configuración de los reportes o informes de vulnerabilidades, así como su entrega respectiva a cada administrador del servidor de TI.

4.8 ANÁLISIS DE INFORMES DE ESCANEOS

En esta fase se tiene como objetivo que se haga una revisión de cada informe generado para establecer en cada caso un plan de implementación de la solución a la vulnerabilidad encontrada, se sugiere en esta fase consolidar los parches o soluciones afín, lo cual puede disminuir el trabajo en el proceso de cierre de vulnerabilidades.
El autor sugiere se tenga clara la importancia de las vulnerabilidades ya que así mismo se puede determinar la importancia de la actualización de seguridad la cual se valora por su índice de severidad y el índice de explotabilidad.

4.9 DESPLIEGUE DE ACTUALIZACIONES DE SEGURIDAD

En esta fase se procede por parte del grupo de administradores de la herramienta de despliegue de actualizaciones o parches de seguridad a realizar el análisis de los informes de vulnerabilidades, contrastarlos con los boletines de seguridad entregados por Microsoft y definir las tareas de despliegue de estos, garantizando que lleguen a los destinos afectados.

Para esto se deben definir las políticas de despliegue en la herramienta, la agrupación de los servidores y las tareas por parte de la herramienta utilizada tanto automáticas como manuales.

4.10 CIERRE DE VULNERABILIDADES

Esta fase tiene como objetivo que el administrador de los servidores realice un análisis de los informes de vulnerabilidades entregados y defina los procedimientos de aplicación, ya sea la instalación de un parche, modificación de alguna llave de registro o desinstalación de algún componente de software. Dentro de este proceso se debe tener definidas unas ventanas las cuales deben ser fijas, pero para los casos especiales donde se requiera aplicación de algún parche de emergencia estas se definan de inmediato y se programe su ventana correspondiente.

Dentro de este proceso, aunque si existe un cambio en los sistemas se sugiere se maneje en un proceso de Gestión de cambios como un cambio estándar, el cual debe ser anunciado para evitar alguna correlación con las fallas cotidianas de las aplicaciones soportadas.

Se sugiere que las ventanas de actualización de los sistemas Operativos sean coordinadas con los procesos de negocio para evitar cualquier alteración en la operación.

Para este proceso se sugiere se deba disponer de un formato de hoja de vida por servidor, en el cual se pueda llevar cualquier histórico de cambios realizados sobre el mismo, en este se debe consignar la información del cierre de las vulnerabilidades, tener en cuenta si la vulnerabilidad pudo ser cerrada o por alguna situación esta vulnerabilidad no se puede cerrar y se debe aplicar alguna contingencia para disminuir el riesgo.

4.11 PRUEBAS FUNCIONALES

Esta fase tiene como propósito realizar las pruebas a los ambientes o servidores Windows server que fueron asegurados, con el objetivo de que su operación sea la definida originalmente y no se haya visto afectada su funcionalidad por alguno de los ajustes de seguridad realizados en la configuración del sistema operativo.

En esta fase es importante contar con un backup, snapshot, imagen o clon del servidor antes del proceso de aseguramiento para los casos que se requiera volver atrás por alguna falla detectada.

4.12 METRICAS DE LA METODOLOGÍA

En este ítem se encuentran las métricas que apoyan la medición de la metodología de aseguramiento de servidores Windows server, expuesta en este proyecto.

Uno de los indicadores que se puede obtener y hacerle seguimiento es el de eficacia.

4.12.1 EFICACIA.

Con este indicador se logra identificar que tan efectiva es la metodología para lograr el aseguramiento de los sistemas operativos en un valor aceptable.

Esta métrica se compone de las siguientes variables:

- **Vulnerabilidades detectadas (Vd),** este valor es el resultado del escaneo de vulnerabilidades con la herramienta que disponga la organización.

- **Vulnerabilidades remediadas (Vr),** este valor es el resultado luego del proceso de ajustes a nivel de seguridad (parches, políticas, llaves de registro etc), con el fin de dar cierre a las vulnerabilidades detectadas.

  La siguiente formula calcula el porcentaje de eficacia del proceso de.
  Este resultado dado en porcentaje se debe ubicar en la tabla siguiente.

  Eficacia = (Vr * 100%) / Vd

La siguiente tabla muestra la guía que determina que tan eficaz fue el proceso de aseguramiento, mostrado en unidades al aplicar todas las fases del ciclo de aseguramiento de sistemas operativos Windows server donde si el valor es 1 es

proceso fue ineficaz y si es 5 el proceso de aseguramiento es eficaz, los valores en medio son valores de eficacia regular.

Tabla 2. Nivel de eficacia de la metodología de aseguramiento de servidores Windows Server

Porcentaje Eficacia	Nivel de Eficacia
80 -100 %	5
60-80 %	4
40-60 %	3
20 -40 %	2
0 -20 %	1

Fuente: El autor.

A continuación, se expresa un ejemplo de aplicación de la métrica:

Se realiza un escaneo de vulnerabilidades a un servidor con Windows Server 2008r2, con alguna herramienta la cual genera un resultado de 80 vulnerabilidades críticas detectadas (Vd).

Se procede a la fase de remediación, en donde se aplican los diferentes ajustes sugeridos por la herramienta de escaneo o por alguna plantilla de seguridad de Windows.

Seguido se realiza un nuevo escaneo en donde se observa que las vulnerabilidades criticas remediadas fueron de 55 Vr.

Se aplica la formula de eficacia de la metodología

Eficacia= (55 * 100%) / 80 = 68,75 %

Con el resultado anterior revisamos la tabla de niveles de eficacia en donde se concluye que el nivel de eficacia es de 4, el cual genera un indicador deseable con tendencia a la mejora.

4.13 POLITICAS DEL CICLO DE ASEGURAMIENTO

Dentro de este ítem se manejarán todas aquellas políticas que se deben cumplir para que esta metodología denominada ciclo de aseguramiento de sistemas operativos Windows Server, tenga unos resultados óptimos y se vuelva de estricto cumplimento con el objetivo de dar resultados positivos a la organización, en cuanto al manejo del riesgo de los servidores Windows Server 2008 y 2012. De igual manera muchas de las políticas que se nombraran a continuación no solo aplicaran al modelo sino a la organización en general, quienes por estar directa o indirectamente relacionados con los servidores pueden provocar riesgos sobre estos activos TI.

4.13.1 Políticas de gestión de identidad.

Estas políticas están orientadas a la mejor práctica de uso y gestión de identidades de la organización (usuarios y contraseñas).

- ✓ Se debe garantizar de manera automática y exigida la renovación de las contraseñas cada 45 días como máximo.
- ✓ Se debe manejar un histórico de contraseñas las cuales no se pueden repetir pasadas 5 contraseñas utilizadas.
- ✓ Se debe garantizar de manera automática y exigida un bloqueo de cuenta tras 5 intentos fallidos.
- ✓ Se debe garantizar de manera automática y exigida un manejo de contraseña con la siguiente complejidad, mínimo de caracteres 6, debe estar compuesta por letras y números, una letra debe ser mayúscula y debe tener por lo menos un carácter simbólico.
- ✓ Para la entrega de las credenciales (Usuarios y Contraseñas), deben realizarse a sobre cerrado, esta cuenta debe exigir de manera automática el cambio de la contraseña en su primer inicio de sesión en el sistema.
- ✓ El proceso de gestión de identidad debe tener definido un estándar el cual contenga perfilado por cargos los permisos de los usuarios que operan en la organización cualquier activo informático.
- ✓ Para credenciales de acceso con permisos de administrador de dominio o administrativas del sistema en general o de servicio que son utilizadas en aplicaciones se debe exigir automáticamente una mayor complejidad en las contraseñas, en la cual el mínimo de caracteres debe ser de 10 y debe estar compuesta por letras y números, una letra debe ser mayúscula y debe tener por lo menos dos caracteres simbólicos.

4.13.2 Políticas generales de seguridad TI.

En este ítem se encuentran las políticas en general, adicionales que aplican al uso de cualquier elemento tecnológico que esté o se vaya a conectar a la red de datos IP, que pueda colocar en riesgo la información de la organización.

Acceso remoto.

- ✓ Para cualquier acceso remoto a la organización se debe garantizar una comunicación cifrada cumpliendo los estándares del momento que no incurran en vulnerabilidades conocidas, entre estos VPN IPsec.
- ✓ Solo se debe autorizar el acceso a remoto a personal de confianza y que por su labor no exista otro medio de conexión a los servicios e información de la compañía.
- ✓ Solo se admite conexiones remotas desde equipos confiables, estos equipos deben estar autorizados por la organización cumpliendo con los item de seguridad, a nivel de actualizaciones, antimalware y sistemas operativos actualizados.
- ✓ Para los casos de administración del sistema solo se debe autorizar a través de las VPNs IPsec y permisos a los protocolos de acceso remoto seguros (SSH, RDP o HTTPS).

Gestión de vulnerabilidades de TI.

- ✓ Se debe disponer de un equipo de personas especializadas en seguridad informática quienes operaran el sistema de SI, garantizando el proceso de gestión de vulnerabilidades y en sí el ciclo de aseguramiento de los servidores Windows server.
- ✓ La organización debe garantizar la infraestructura tanto de hardware como de software para el proceso de aseguramiento de Servidores Windows Server entre estos los escáneres de vulnerabilidades, la herramienta de despliegue de actualizaciones de seguridad y el software antimalware.
- ✓ Se debe disponer de un equipo de personas especializadas en la administración y gestión en general de servidores Windows Server, quienes deben garantizar la operación segura de estos activos informáticos.
- ✓ Todas las herramientas empleadas en el ciclo de aseguramiento como (escáner de vulnerabilidades, herramienta de despliegue de parches, consolas antimalware, etc.), deben estar debidamente actualizadas y operando satisfactoriamente.
- ✓ Seguridad informática debe hacer análisis y validación de los informes de vulnerabilidades detectados por los escáneres, se debe validar si existen falsos positivos de lo mismo para así mismo se haga entrega de informes reales o correctos.
- ✓ Todo dispositivo IP debe ser autorizado previamente para la conexión física a la red de datos de la organización.
- ✓ Todo equipo que esté en proceso de autorización de conexión a la red de datos de la organización debe pasar por un proceso de validación del aseguramiento de este, en donde se conectará a una red aislada se realizará un proceso de escaneo de vulnerabilidades y revisión del software antimalware.
- ✓ El proceso de pruebas u escaneo de vulnerabilidades del sistema debe hacerse de forma cíclica y periódica una vez cada mes sobre cada dispositivo que contenga una IP y esté conectado a la red de la organización o que

maneje o transite información de la organización. Esta política aplica para activos como Servidores, productivos o no productivos, PCs o portátiles, Switches, teléfonos IP, Firewall, NAS, o dispositivos móviles, o cualquier otro dispositivo autorizado a la conexión de la red IP de la organización.

- ✓ Todo dispositivo IP gestionado por la organización debe quedar registrado en una matriz o base de datos de activos TI con las características mínimas como son el nombre del host, tipo de dispositivo, Dirección Física, Marca y Modelo, así como el responsable de este.
- ✓ Todo servidor debe quedar registrado en el formato “Matriz activos de infraestructura TI de Servidores”, en donde obligatoriamente debe quedar registrado el nombre del host, Dirección Física, Marca y Modelo, así como el responsable de este, entre otros datos que se pueden exigir en la Matriz.
- ✓ Todo servidor Windows Server implementado y activo en la organización debe ingresar al proceso llamado ciclo de aseguramiento de servidores Windows server en donde debe quedar el respectivo registro de este adjunto a su hoja de vida, para esto se debe diligenciar el formato llamado “Escaneo_Vulnerabilidades_Servidores”.
- ✓ Los administradores de las plataformas de servidores Windows server son responsables de la remediación o cierre de vulnerabilidades reportadas por seguridad informática.
- ✓ Todas vulnerabilidades detectadas deben ser gestionadas con un tiempo máximo de 45 días, en donde se deben establecer los planes y programación de ventanas para la gestión requerida.
- ✓ Todas las vulnerabilidades detectadas que se estime no puedan ser cerradas se manejaran como riegos aceptados, esto debe quedar registrado, en el formato de “Escaneo_Vulnerabilidades_Servidores”, y si es posible se debe nombrar cualquier contingencia que se pueda implementar.
- ✓ Todos los servidores productivos deben presentar un plan de backup o contingencia, así como plan de recuperación ante desastres, esto debe ser activados en los procesos de remediación de vulnerabilidades.
- ✓ Todo cambio realizado en un servidor productivo debe quedar registrado en el proceso de gestión de cambios según ITIL y en el formato de hoja de vida del servidor, el cual debe llevar el histórico del mismo.
- ✓ Todos los servidores Windows server deben tener habilitado el WFAS (Windows Firewall Advanced Security), así como configurado únicamente la comunicación requerida por este, tener en cuenta para esto que se debe diligenciar el formato “Matriz_de_Comunicacion_del_Servidor”, el cual controlara la configuración de este.
- ✓ Todos los Servidores Windows Server deben tener el software antimalware de la organización habilitado y actualizado tanto sus motores como sus bases de datos de amenazas.
- ✓ Se deben dar prioridad a cualquier vulnerabilidad o amenazas que genere un riesgo alto a la organización, esto se debe tratar como un cambio de emergencia y debe ser gestionado en forma inmediata.

Capacitación.

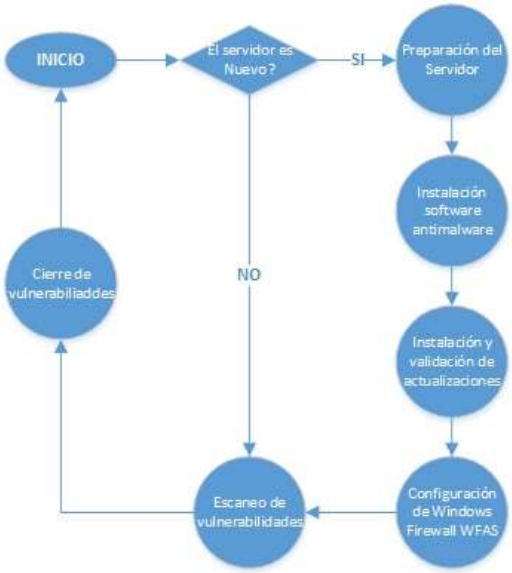
- ✓ Se deben garantizar planes de capacitación por parte de la organización mínimo dos veces por año, en la cual se deba educar especialmente a todos los integrantes del departamento de TI como de Seguridad Informática.
- ✓ También se debe mantener un plan de capacitación a os usuarios en forma de sensibilización con el objetivo que sirvan de apoyo en el fortalecimiento de la seguridad en general.

4.14 PROCEDIMIENTO DE ASEGURAMIENTO DE UN SERVIDOR WINDOWS SERVER

Antes de ejecutar este procedimiento se debe validar la existencia de los siguientes requisitos para el proceso de aseguramiento del servidor Windows Server:

1. Servidor de despliegue de actualizaciones (WSUS o Similar)
2. Permisos de Internet con acceso a los servicios de Windows Update desde el servidor que se asegurará. (Opcional).
3. Licencia e instalador del software antimalware compatible con Windows server según versión.
4. Herramienta de escaneo de vulnerabilidades (MBSA, OpenVAS, Retina CS Community, NeXpose etc).
5. Formato Matriz de comunicación del servidor diligenciada.

Ilustración 23. Flujograma Procedimiento de aseguramiento de un Servidor.



Fuente: El autor.

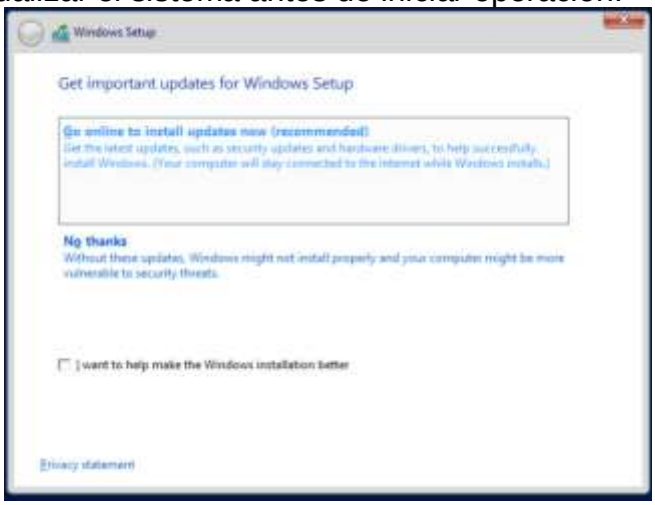
4.14.1 Preparación del Servidor.

El proceso de aseguramiento de un servidor comienza desde la misma instalación inicial en donde se debe instalar únicamente los componentes esenciales requeridos para su función final, en este proceso inicial tener en cuenta los roles o características de Windows que se deben habilitar así mismo el software adicional que se instalará, tener en cuenta que un adobe, o un java incensario sería una posible vulnerabilidad adicional o un software más para asegurar, también es importante tener en cuenta utilizar la última versión o la versión más segura y estable en ese momento de todos los componentes involucrados en la instalación.

Ilustración 24. Instalación de Windows Server 2012 R2.

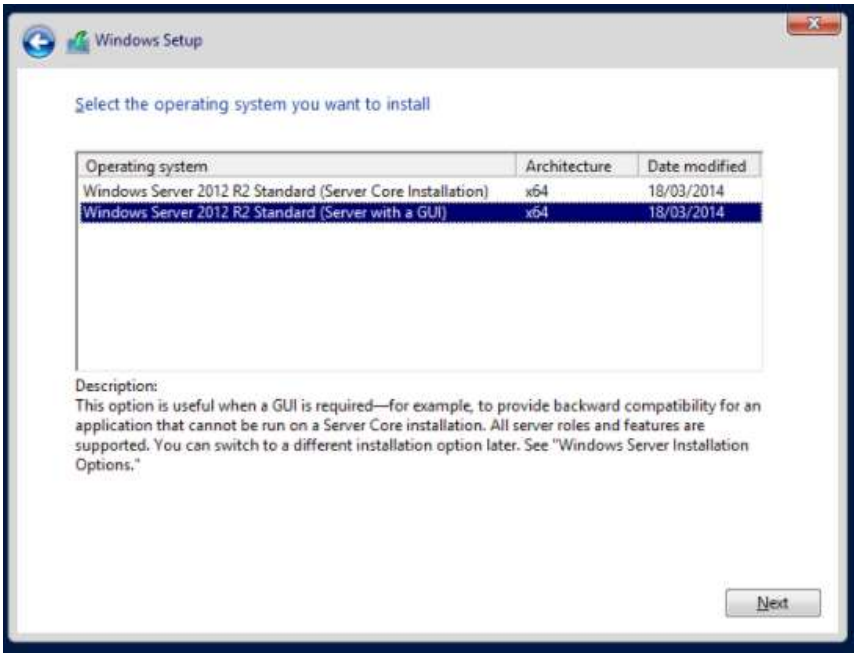
Fuente: El Autor.

Ilustración 25. Actualizar el sistema antes de iniciar operación.



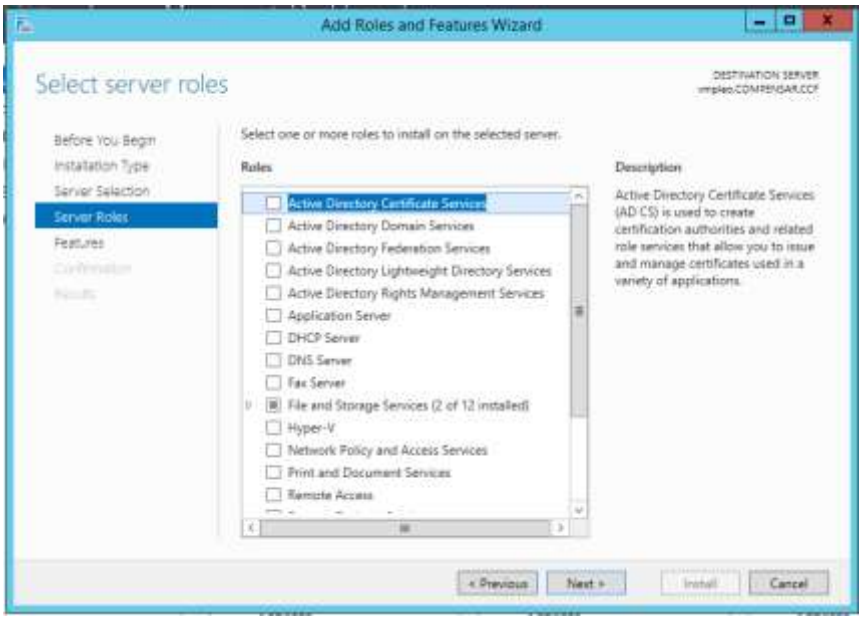
Fuente: El Autor.

Ilustración 26. Selección Server Core o Server con GUI.



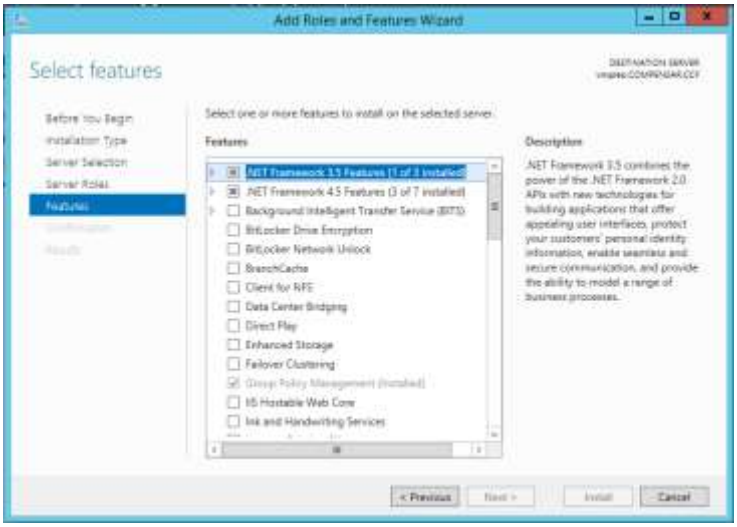
Fuente: El Autor.

Ilustración 27. Selección de Roles Windows Server.



Fuente: El Autor.

Ilustración 28. Selección de características Windows Server.

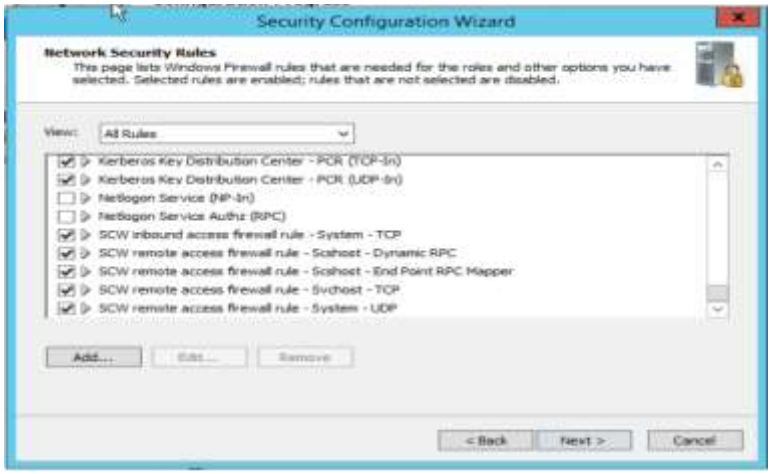


Fuente: El Autor.

4.14.2 Aseguramiento inicial del servidor.

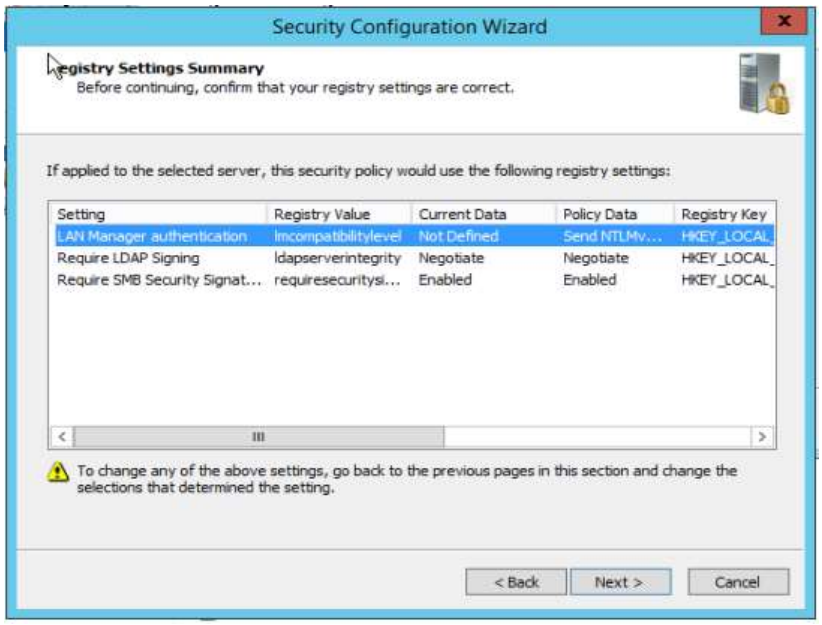
Es este paso es indispensable utilizar por facilidad o la herramienta SCM o utilizar el asistente que contiene el sistema operativo SCW, los cuales guiaran la mejor practica para ajustar la configuración de manera segura, aplicando políticas locales, basadas en rol, servicios, configuraciones de firewall y conformando la mejor opción de seguridad para el rol dispuesto el servidor en cuestión.

Ilustración 29. Aplicación de SCW Security Configuration Wizard. Reglas de seguridad de red



Fuente: El autor.

Ilustración 30. Aplicación de SCW Security Configuration Wizard, Configuraciones de registro.



Fuente: El autor

Aplicando SCW, lograremos la configuración de una política de seguridad basada en rol, servicios y configuraciones de firewall de Windows al igual que una política de auditoria, logrando asegurar los servicios para lo que va a operar el servidor.

4.14.3 Instalación software antimalware.

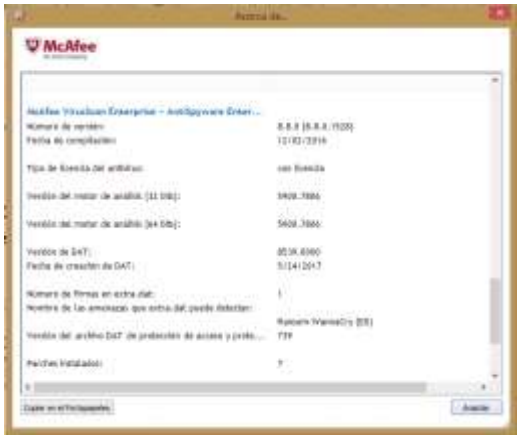
El paso siguiente luego del proceso de instalación inicial y de garantizar la actualización al máximo del sistema operativo a nivel de parches del sistema, es la instalación inmediata de un software antimalware, dentro de estos se debe tener en cuenta que debe ser compatible con sistemas operativos servidor y dentro de la recomendación adquirir una plataforma corporativa o Enterprise ya que esta contiene herramientas de gestión centralizada la cual hace más fácil la administración si existen muchos servidores, a nivel de entrega de actualizaciones políticas de excepción entre otras.

Ilustración 31. Instalación de Antimalware Enterprise, sobre Windows Server.

Fuente: El Autor.

Tener en cuenta luego de la instalación del software antimalware que este quede completamente actualizado a la fecha, tanto la versión del motor, así como el DAT File como esto para evitar cualquier ataque de malware cuando entre en operación.

Ilustración 32. Validación fecha de actualización Antimalware, y versión.



Fuente: El Autor.

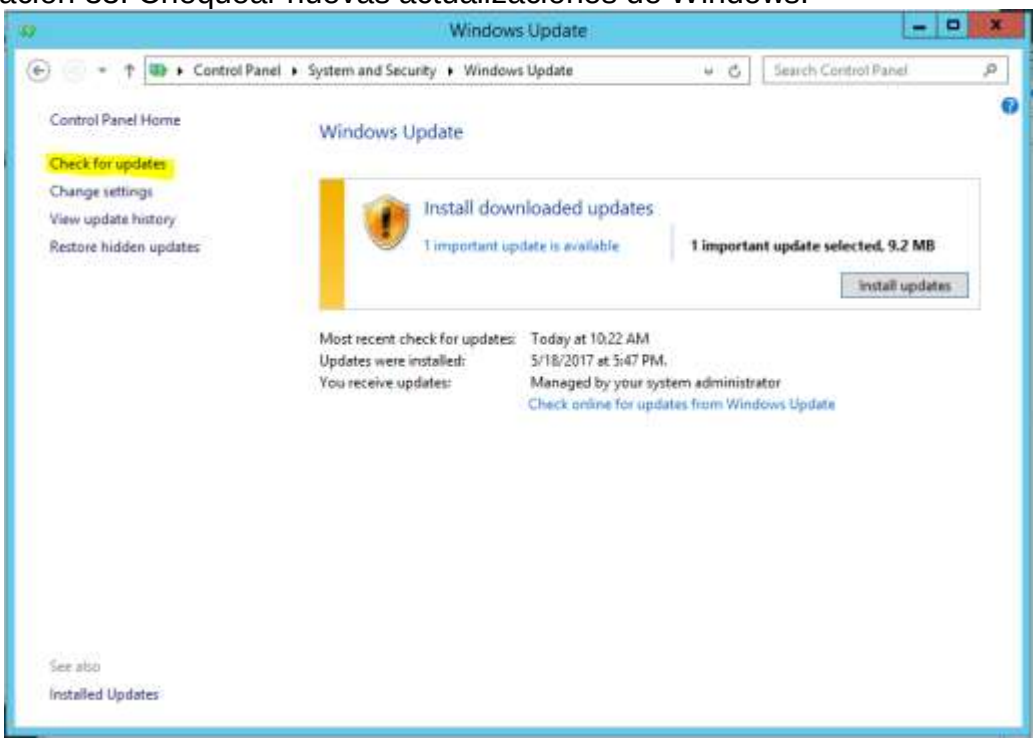
4.14.4 Instalación y validación de actualizaciones.

En este paso se sugiere hacer una validación adicional, de que el sistema operativo tenga todas las actualizaciones de Microsoft instaladas, para esto se debe ingresar a la herramienta que trae llamada *Windows Update*, y dar clic en “Check for Update”, como se puede ver en la ilustración siguiente, si se encuentran nuevas actualizaciones se da clic en el botón donde dice “Install Udpate”.

Posiblemente cada vez que se habilitan nuevos roles o características se requiere hacer alguna actualización de parches del sistema.

Para los casos donde se requiera alguna actualización adicional o particular se puede hacer uso del portal de Microsoft actualizaciones llamado “Catalogo de Microsoft Update”, en el siguiente link:
“https://www.catalog.update.microsoft.com/Home.aspx”.

Ilustración 33. Chequear nuevas actualizaciones de Windows.



Fuente: El Autor.

4.14.5 Configuración del Windows Firewall (WFAS).

Windows por defecto luego de la instalación deja habilitado el Firewall llamado WFAS que significa Windows Firewall Advanced, como se observa en la ilustración 30, Windows por defecto deja algunas reglas configuradas las cuales el ah detectado o el fabricante como plantilla las ha predeterminado, sin embargo, como este servidor nuevo entra a relacionarse con otro se debe ser configurado particularmente.

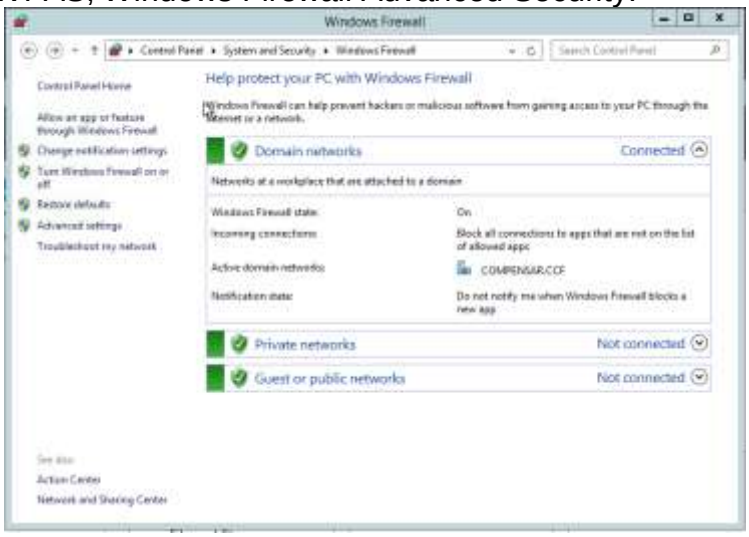
Por lo anterior lo que se debe hacer en este paso es configurar el WFAS, para esto se debe conocer todas las conexiones relacionadas con este servidor, para esta labor se sugiere se diligencie una Matriz como la de la ilustración 28, con las conexiones orígenes y destinos, así como los puertos. Protocolos, aplicaciones y una descripción de cada conexión requerida como se ve de ejemplo en la ilustración.

Ilustración 34. Matriz de comunicación para configuración del WFAS.

MATRIZ DE COMUNICACIÓN DEL SERVIDOR							
REGLA No.	IP ORIGEN	NOMBRE DE USUARIO	IP DESTINO	TIPO PROTOCOLO	PUERTO REMOTO	APLICACIÓN	DESCRIPCIÓN
1	192.168.0.10/32	NA	192.168.0.21/32	TCP	8081	SOAP	Conexión a Servidor aplicacón1
2	192.168.0.10/32	USUARIO/DOMINIO.INT	192.168.0.2/32	TCP/UDP	53	DNS	Conexión a serviodor de nombres de dominio
3	ANY		192.168.0.10/32	TCP	3389	RDP	Conexión desde cualquier IP a escritorio remoto solo a los usuarios del GRUPO_AD

Fuente: El Autor.

Ilustración 35. WFAS, Windows Firewall Advanced Security.



Fuente: El Autor.

Ilustración 36. Configuración de reglas de entrada (Inbound).

Fuente: El Autor.

Ilustración 37. Configuración de reglas de salida (Outbound).

Fuente: El Autor.

4.14.6 Escaneo de vulnerabilidades.

Es una buena práctica antes de salir a producción con un servidor nuevo o servicio nuevo realizar un escaneo de vulnerabilidades con alguna de las herramientas nombradas anteriormente para saber el estado de seguridad y si es requerido realizar las configuraciones o parcheos de seguridad requeridos o en casos extremos aplicar alguna contingencia sobre la debilidad encontrada.

Para el caso de ejemplo se utilizará la versión libre de Microsoft, la cual se instala y ejecuta en el mismo servidor Windows server como se observa en la ilustración siguiente:

Ilustración 38. MBSA. Microsoft Baseline Security Analyzer.

Fuente: El Autor

A continuación, se lanza el escaneo el cual, dependiendo de los recursos del servidor, así como la cantidad de software que tenga por analizar puede durar un buen tiempo. Finalmente, esta herramienta entrega un reporte como el de la ilustración 33, en donde se informa el Score o nivel de criticidad, así como la información de lo encontrado, pero también entrega información de cómo puede ser corregido.

Ilustración 39. Reporte de vulnerabilidades encontradas.

Fuente: El Autor.

4.14.7 Cierre de vulnerabilidades detectadas.

En este paso lo que se procede a realizar sn las diferentes correcciones al sistema operativo según lo indica el reporte de MBSA, para este paso es importante también contar con los parches o actualizaciones que se requieran por lo anterior la organización debe contar con un servidor de despliegue de parches o se puede utilizar el portal del catálogo de actualizaciones de Microsoft, para descargas puntuales.

En el ejemplo es un servidor nuevo, pero para el caso de ser un servidor en producción es importante registrar todos los cambios realizados en su hoja de vida, en donde se debe indicar la tarea realizada pero adicionalmente al reporte entregado por el proceso de escaneo se debe responder en cada vulnerabilidad si esta fue gestionada y si fue cerrada o no es posible cerrarla y se acepta el riesgo o se aplica alguna contingencia para mitigar o disminuir el riego posible.

Ilustración 40. Formato escaneo de vulnerabilidades.

REPORTES VULNERABILIDADES							CIERRE DE VULNERABILIDADES			
Nombre de Servidor	Sistema Operativo	Dirección IP	Rol Servidor							
SERVIDOR1	Windows Server 2012 R2	192.168.0.10	File Server				Estados disponibles para la gestión de las vulnerabilidades **Abierta**: (No es posible cerrar la vulnerabilidad) **Cerrada**: (Se logró cerrar la vulnerabilidad)			
RESUMEN DE VULNERABILIDADES										
Altas	1									
Medias	0									
Bajas	1									
Informativas	1									
Nivel de Gravedad	Nombre Vulnerabilidad	Descripción	Soluciónes y Herramientas	Identificador IDs CVE	Nombre del Servicio	Fecha de publicación de Vulnerabilidad	Estado	Observación	Nombre Administrador	Fecha de Gestión
Importante	MS11-025	Podría permitir la ejecución remota de código	https://technet.microsoft.com/library/security/ms11-025	CVE-2010-3190	Microsoft Visual Basic	12/04/2010	Abierta	No es posible la instalación, debido a incompatibilidades con el SO.	Carlos Coronado	25/05/2017

SERVIDOR

Fuente: El Autor.

Como se observa en la ilustración anterior, se muestra el reporte donde se documentan las vulnerabilidades encontradas, así mismo la gestión realizada, en este se debe indicar tanto el estado de la gestión (abierta o cerrada), hacer una observación, diligenciar el nombre del administrador que gestionó la vulnerabilidad y la fecha de gestión

5 CONCLUSIONES

- Se realizó investigación y documentación de metodologías, mejores prácticas y herramientas para el aseguramiento de los sistemas operativos MS Windows Server.

- Dentro del estudio realizado se deja identificadas sugerencias para la utilización de metodologías mejores prácticas y herramientas para el aseguramiento de sistemas operativos MS Windows Server.

- Se diseña modelo documental para los procesos del aseguramiento de sistemas operativos MS Windows Server, donde se sugieren las herramientas requeridas los pasos a seguir, así como los formatos requeridos en el proceso de aseguramiento de sistemas operativos MS Windows Server.

6 RECOMENDACIONES

- Se sugiere mantener en última versión las herramientas utilizadas en el proceso de descubrimiento de activos, escaneo de vulnerabilidades y despliegue de actualizaciones de seguridad, ya que las amenazas y las vulnerabilidades están cambiando constantemente.

- Se recomienda vigilar que se mantengan siempre actualizadas las bases de datos de todas las herramientas que se utilicen en el proceso de aseguramiento de los servidores, para garantizar que los informes entregados siempre estén al día con las vulnerabilidades o amenazas del momento.

- Se sugiere tener personal de seguridad informática dedicado solo al proceso de escaneo de vulnerabilidades y revisión de amenazas, este personal debe auditar que al final se aseguren los servidores Windows Server.

- Se sugiere tener personal diferente a seguridad informática dedicado solo al proceso de administrar u operar los servidores Windows server quienes deben garantizar las remediaciones o cierres de vulnerabilidades reportados y en si garantizar el aseguramiento de los servidores en general.

- Se sugiere se tenga un indicador de gestión de aseguramiento de los servidores Windows server, el cual debe ser comparado y revisado por las partes por lo menos una vez cada dos meses, esto debe garantizar que el índice de riesgo se mantenga en un valor moderado o tolerado por la organización.

- Se sugiere que la organización mantenga un plan de capacitación a todo el personal que opera tanto los servidores, así como el personal de seguridad informática que realizará los procesos de validación del aseguramiento del sistema

- Se sugiere que antes de cualquier proceso de aseguramiento de los servidores se tenga un informe previo del estado de este a nivel funcional, de igual manera se sugiere se programe las pruebas correspondientes al mismo luego del proceso de aseguramiento garantizando la operación de este de manera normal.

BIBLIOGRAFÍA

ASO - ADMINISTRACIÓN DE SISTEMAS OPERATIVOS, Disponible en: http://www.adminso.es/index.php/4._Medidas_de_seguridad_en_los_sistemas_inform%C3%A1ticos.

COLOMBIA, DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA (DAFP), Guía Para La Administración Del Riesgo. [En línea]. Bogotá, septiembre 2011. Disponible en http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/.

CASTELLANOS, Luis, 2014, 06.02. Sistemas Operativos para Servidores, Disponible en: https://lcsistemasoperativos.wordpress.com/2015/02/06/06-02-sistemas-operativos-para-servidores/.

DIDACTICA, Universidad Evangélica del salvador junio 2011, Disponible en: https://didacticauees.wordpress.com/marco-teorico/.

ENCICLOPEDIA DE CLASIFICACIONES, 2016, Tipos de sistemas operativos. Enciclopedia de tipos. Octubre de 2016 Disponible en: http://www.tiposde.org/informatica/15-tipos-de-sistemas-operativos/.

ERB MARKUS. Gestión de riesgo en la seguridad informática. Noviembre de 2016 Disponible en: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/.

INTERNET YA SOLUCIONES, Windows Server 2012 – Ediciones Datacenter y Estándar. Noviembre 2016 Disponible en: http://www.internetya.co/windows-server-2012-ediciones-datacenter-y-standard/.

LEY 1273 de 2009 Nivel Nacional, enero 5, Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

LOPEZ POLIN, Ignacio Bruna, BELT IBERICA S.A 2004, Confidencialidad, Integridad y disponibilidad de la información noviembre de 2016. Disponible en: http://www.belt.es/expertos/experto.asp?id=2245.

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I, Disponible en https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf.

MICROSOFT, Asistente de configuración de seguridad. [En línea], 2018. Disponible en https://technet.microsoft.com/en-us/library/cc754997(v=ws.11).aspx

MICROSOFT, Developer Network, Instalar roles de servidor y características en un servidor Server Core. Microsoft 2017. Disponible en: https://msdn.microsoft.com/es-es/library/jj574158(v=ws.11).aspx

MICROSOFT, El servicio de soporte ampliado de Windows Server 2003, noviembre de 2016. Disponible en https://www.microsoft.com/es-es/server-cloud/products/windows-server-2003/.

MICROSOFT, Herramienta de Evaluación de Seguridad de Microsoft (MSAT). [En línea]. 2018. Disponible en https://technet.microsoft.com/es-xl/library/cc185712.aspx.

MICROSOFT, Introducción a las directivas de grupo. [En línea], 2017. Disponible en https://msdn.microsoft.com/es-es/library/hh831791(v=ws.11).aspx

MICROSOFT, Introducción a los Servicios de dominio de Active Directory. [En línea], 2012. Disponible en https://msdn.microsoft.com/es-es/library/hh831484(v=ws.11).aspx.

MICROSOFT, Microsoft Technet, Guías de seguridad para sistemas operativos Windows, Disponible en: https://blogs.technet.microsoft.com/jorge_aguinaga/2009/02/04/guas-de-seguridad-para-sistemas-operativos-windows/.

MICROSOFT, MSDN Library, Implementación de Windows Server Update Services en la organización, Disponible en: https://msdn.microsoft.com/es-es/library/hh852340(v=ws.11).aspx.

MICROSOFT, Security Compliance Manager (SCM). [En línea]. 2017. Disponible en https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx

MICROSOFT, Windows Server, octubre 2016. Disponible en: https://msdn.microsoft.com/en-us/library/dn636873(v=vs.85).aspx.

MICROSOFT, Windows Server, Roles, Servicios de rol y características Disponible en: https://technet.microsoft.com/es-es/library/cc754923(v=ws.11).aspx.

MUY WINDOWS, Ya está disponible Windows server 2012, septiembre 2012 Disponible en: http://www.muywindows.com/2012/09/05/ya-esta-disponible-windows-server-2012.

OCTAVE®-S Implementation, Guide, Versión 1.0, 2005 05, Disponible en http://www.sei.cmu.edu/reports/04hb003.pdf.

OSANDNET, Baby Baldes, Características de función de Windows Server 2012 R2, Julio 2015 Disponible en: http://www.osandnet.com/caracteristicas-de-server-2012-r2/.

OWASP, The Open Web Application Security Proyect, Análisis de riesgos aplicando la metodología OWASP. [En línea]. 2015. Disponible en https://www.owasp.org/images/b/b3/Analisis_de_riesgo_usando_la_metodologia_OWASP.pdf.

SISTEMOPERWINDOWSSERVER, Information general Windows Server (NT, 2003, 2008). Disponible en: https://sistemoperwindowsserver.wikispaces.com/INFORMACION+GENERAL++WINDOWS+SERVER(NT,+2003,2008).

TESIS181, Metodología de Análisis de Vulnerabilidades para Empresas de Media y Pequeña Escala, Disponible en: http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf.

TIBOCHA ROA, Sandra Milena, Febrero 2014, Guía de aseguramiento de servidores Microsoft versión Windows server 2008 R2, Noviembre de 2016, Disponible en: http://www.anh.gov.co/Seguridad-comunidades-y-medio-ambiente/Pruebas%20de%20Cargue%20COMWARE/Guia%20de%20Aseguramiento_Microsoft%20Windows%20Server%202008%20R2_V01.pdf.

WINDOWS SERVER 2008, História de Windows NT y Server. Disponible en http://www.redtauros.com/Clases/Win_2008_R2/01_Introduccion.pdf.

6 ESCÁNERES DE VULNERABILIDADES DE RED GRATUITOS, 2014 05 09, Disponible en http://cioperu.pe/articulo/15863/6-escaneres-de-vulnerabilidades-de-red-gratuitos/

ANEXOS

Anexo A. Formato, Matriz activos de infraestructura TI de Servidores.

Matriz activos de infraestructura TI de Servidores														
ITEM	NOMBRE DEL HOST	DIRECCION IP	DIRECCIÓN FISICA	MEMORIA RAM	PROCESADOR /NUCLEOS	DISCO DURO	FISCO / VIRTUAL	ROL DEL SERVIDOR	SISTEMA OPERATIVO	SERVICIOS O APLICACINES INSTALADOS	NOMBRE DE BASE DE DATOS	PUERTO/SERVICIO /PROTOCOLOS	USUARIOS DE SERVICIO	USUARIOS ADMINISTRA DORES

Anexo B. Formato, Escaneo vulnerabilidades Servidores.

REPORTES VULNERABILIDADES							CIERRE DE VULNERABILIDADES			
Nombre de Servidor	Sistema Operativo	Dirección IP	Rol Servidor							
RESUMEN DE VULNERABILIDADES										
Altas										
Medias										
Bajas										
Informativas										
Nivel de Gravedad	Nombre Vulnerabilidad	Descripción	Soluciónes y Herramientas	Identificador IDs CVE	Nombre del Servicio	Fecha de publicación de Vulnerabilidad	Estado	Observación	Nombre Administrador	Fecha de Gestión

SERVIDOR

Anexo C. Formato, Matriz de comunicación del servidor.

MATRIZ DE COMUNICACIÓN DEL SERVIDOR							
REGLA No.	IP ORIGEN	NOMBRE DE USUARIO	IP DESTINO	TIPO PROTOCOLO	PUERTO REMOTO	APLICACIÓN	DESCRIPCIÓN

Anexo D. Formato, Cronograma de aseguramiento de Servidores.

CRONOGRAMA DE ASEGURAMIENTO DE SERVIDORES
Escaneo y Remediación de Vulnerabilidades

AÑO 2017

ACTIVO TI	Horario Ventana	TIPO DE ACTIVIDAD	ENE		FEB		MAR		ABR		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC		TOTAL		PORCENTAJE EJECUTADO %
			Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	Proyectado	Ejecutado	
SERVIDOR_1	18:00	Escaneo Vul Srv																									0	0	#DIV/0!
	3:00	Remediación Srv																									0	0	#DIV/0!
SERVIDOR_2	21:00	Escaneo Vul Srv																									0	0	#DIV/0!
	2:00	Remediación Srv																									0	0	#DIV/0!
SERVIDOR_3	21:00	Escaneo Vul Srv																									0	0	#DIV/0!
	2:00	Remediación Srv																									0	0	#DIV/0!
SERVIDOR_4	0:00	Escaneo Vul Srv																									0	0	#DIV/0!
	4:00	Remediación Srv																									0	0	#DIV/0!
SERVIDOR_5	0:00	Escaneo Vul Srv																									0	0	#DIV/0!
	4:00	Remediación Srv																									0	0	#DIV/0!
SERVIDOR_6	0:00	Escaneo Vul Srv																									0	0	#DIV/0!
	4:00	Remediación Srv																									0	0	#DIV/0!
																										TOTALES =	0	0	#DIV/0!

Anexo D. Resumen Analítico especializado RAE.

RESUMEN RAE	
1. **Título.**	METODOLOGÍA DE ASEGURAMIENTO A SISTEMAS OPERATIVOS SERVER
2. **Autor**	Carlos Fernando Coronado Parga
3. **Edición**	No presenta.
4. **Fecha**	Mayo 23 de 2018.
5. **Palabras Claves**	Activo, ciclo, amenaza, vulnerabilidad, escáner, remediación, aseguramiento, parche, actualizaciones, metodología.
6. **Descripción.**	Trabajo de grado para optar al título de especialista de seguridad informática de la UNAD.
7. **Fuentes.**	Se utilizaron 30 fuentes, de las cuales son consultas teóricas a nivel de Sistemas Operativos Microsoft Windows Server, Metodologías de Análisis y gestión de riesgos, mejores prácticas para el aseguramiento de sistemas operativos, herramientas libres o comerciales para el inventario de activos de TI, escaneo de vulnerabilidades y despliegue de actualizaciones a Sistemas Operativos Microsoft Windows Server. Este texto también está fundamentado en la experiencia vivida del autor en las organizaciones donde laboró administrando, e implementando soluciones para el aseguramiento de plataformas de TI.
8. **Contenidos.**	Este trabajo de grado fue producto de observar la no existencia de una guía o metodología concreta para el aseguramiento de servidores Windows Server que pueda apoyar a las organizaciones de cualquier tamaño o sector de la industria, por lo anterior en este documento se hace una investigación a nivel de la historia del sistema operativo Windows Server, así como una descripción de estos enfocado solo a Windows Server 2008 y Windows Server 2012 objetivo del trabajo a presentar. Dentro del proceso investigativo y comparativo también se hace un estudio de las diferentes metodologías de análisis de gestión de riesgos de TI, donde se encuentran “OCTAVE”, enfocada en el análisis de riesgos en el área de tecnologías de la información, esta metodología se basa en la identificación de los riesgos circundantes a los activos de TI, también se encuentra otra metodología llamada “DAFP”, Departamento Administrativo de la Función Pública, este modelo sirve de guía para la implementación de la política de la administración del riesgo en las entidades públicas. Otra metodología estudiada es la llamada “OWASP” Open Web

	Application Security Project, esta metodología está orientada al Riesgo de TI o riesgo encontrado en la Tecnología de la información, el cual se enfoca a realizar análisis en la perdida por caídas o errores detectados en los sistemas informáticos, cuyas causas se encuentran en errores de software entre otras, por ultimo también se revisó la metodología MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, ésta metodología soporta la fase AGR (Análisis y Gestión de Riesgos), apoya en gran medida la gestión en general de un sistema de seguridad de la información de una Compañía, basada en ISO27001, ya que contiene todas las fases requeridas a nivel estratégico. Dentro de este documento también se hace un estudio a nivel de mejores prácticas para el aseguramiento de sistemas operativos Windows Server, en donde se enuncia como primera medida la buena preparación de un servidor desde su construcción con el objetivo de que este quede instalado con lo mínimo requerido, los ajustes con directivas locales, también la utilización del firewall local de Windows configurado con sus políticas requeridas, también se nombra el tener un software antimalware el cual pueda proteger el servidor ante cualquier amenaza a nivel de código malicioso y se nombran algunas marcas conocidas y compatibles con Windows Server como Mcafee, Symantec, Kaspersky, Eset, TrenMicro y Microsoft. También se hace un recorrido nombrando soluciones antimalware ideales para servidores virtuales. También se hace investigación sobre herramientas utilizadas en estos procesos de aseguramiento de servidores en donde se nombras varias herramientas desde gratuitas hasta comerciales, así como las que entrega Microsoft también herramientas de terceros o no Microsoft. Dentro de esas herramientas están de Microsoft, Directivas de grupo, Active directory, MSAT (Microsoft Security, Assessment Tool), SCM (Security Compliance Manager), SCW (Security Configuration Wizard), MBSA (Microsoft Baseline Security Analizer), WSUS (Windows Server Update Services), Portal Catalogo de Microsoft Update y MSRT (Microsoft Malicious Software Removal Tool). En otras herramientas no Microsoft se encuentran OpenVAS (Open Vulnerability Assessment System), Retina CS Community y Nexpose Community edition.

	Dentro del documento se nombra a nivel legal la ley 1273 de 2009, la cual tiene relación con proyecto de aseguramiento de servidores. De la investigación realizada se concluye en una solución de proyecto cuyo nombre es “Ciclo de aseguramiento de servidores Windows server”, en el cual se plantea la metodología propuesta y que está compuesta de un ciclo donde se inicia con el inventario de activos informáticos, seguido, de un proceso de aseguramiento inicial del servidor, luego de un proceso de escaneo de vulnerabilidades, luego el análisis de informes de escaneos, un despliegue de actualizaciones de seguridad y finalmente el cierre de vulnerabilidades. Para todo el proceso anterior se nombran en cada fase las herramientas posibles a utilizar según estudio también se dan pautas o sugerencias de utilización de estas, así como se entregan las políticas los formatos para el control del proceso de aseguramiento o gestión de los servidores.
9. **Metodología**.	Para este trabajo se utilizó una metodología de investigación comparativa y práctica.
10. **Conclusiones**.	➢ Se realizó investigación y documentación de metodologías, mejores prácticas y herramientas para el aseguramiento de los sistemas operativos MS Windows Server. ➢ Dentro del estudio realizado se deja identificadas sugerencias para la utilización de metodologías mejores prácticas y herramientas para el aseguramiento de sistemas operativos MS Windows Server. ➢ Se diseña modelo documental para los procesos del aseguramiento de sistemas operativos MS Windows Server, donde se sugieren las herramientas requeridas los pasos a seguir, así como los formatos requeridos en el proceso de aseguramiento de sistemas operativos MS Windows Server.
11. **Autor del RAE.**	Carlos Fernando Coronado Parga