DISEÑO E IMPLEMENTACIÓN DE UN PROCESO DE HARDENING

OSCAR ALONSO CRUZ MORENO

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍA Y CIENCIAS BASICAS
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2017

DISEÑO E IMPLEMENTACIÓN DE UN PROCESO DE HARDENING

OSCAR ALONSO CRUZ MORENO

Trabajo de Grado presentado como requisito para obtener el título de
Ingeniero de Sistemas

Asesor
LUIS EDUARDO BAQUERO REY
Docente Investigador

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERÍA Y CIENCIAS BASICAS
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.
2017

Nota de aceptación

_____

_____

_____

_____

Firma Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

_____

Bogotá D.C., 8 de junio 2017

DEDICATORIA

A mis padres, mi familia, mi novia y todas esas personas que creen en mí, por el apoyo incondicional durante mi etapa académica, porque en gran parte gracias a ellos hoy en día veo más cerca la meta y mi sueño de ser ingeniero y para todos aquellos que de alguna u otra forma fueron partícipes en este largo camino.

AGRADECIMIENTOS

Expreso mi agradecimiento en primer lugar a Dios por brindarme la fortaleza necesaria para afrontar todas las adversidades y obstáculos que se presentaron durante mi etapa profesional, por darme la oportunidad de presentar esta investigación en esta universidad, al ingeniero Luis Eduardo Baquero por guiarme en desarrollo de este proceso con sus amplios conocimientos en la parte de seguridad informática.

RESUMEN

La seguridad de un entorno informático, inicia con la elección del sistema operativo y las características implementadas en su instalación las cuales por ningún motivo deben ser parametrizadas por defecto. Hardening, es un método que permite implementar tantas estrategias como herramientas en busca de elevar el nivel de seguridad del sistema operativo. En el presente trabajo, se da a conocer en detalle, un proceso de Hardening implementado en servidores Windows, las actividades técnicas que se deben tener en cuenta para su paso a entornos productivos.

En el presente trabajo, se analizan algunas herramientas relacionadas en el uso de una estrategia de seguridad Hardening. Luego de la instalación de un sistema operativo hay vulnerabilidades abiertas por defecto, las cuales deben ser objeto de análisis y de esta manera considerar cuáles deben mantenerse abiertas y cuáles deben cerrarse.

Además, se parametrizan las plantillas de aseguramiento para sistemas operativos Windows 7 y Windows server 2012 R2, las cuales contienen configuraciones definidas por el mínimo privilegio. La implementación por medio de un GPO, garantiza que las estaciones de trabajo y servidores repliquen estas configuraciones de manera automática.

Al finalizar esta implementación en los equipos piloto de Hardening, se debe poder evidenciar una reducción considerable de vulnerabilidades al realizar el aseguramiento de los sistemas operativos de la organizacion. Como Anexo, se presentan las configuraciones realizadas en las GPO.

Palabras Claves: Hardening, Sistemas Informatica, Seguridad Operativos, Seguridad en Redes.

INTRODUCCIÓN

El presente documento tiene como propósito dar a conocer la propuesta de proyecto de grado que trata del diseño e implementación de un proceso de Hardening para este caso en particular se realizo la ofuscación de algunos datos, ya que este proeso puede ser implementado en cualquier organizacion, el alcance de las configuraciones se realizó en sistemas operativos Windows, este proceso de aseguramiento tiene como base de referencia el análisis de vulnerabilidades del primer trimestre en el cual se logra evidenciar que el proceso de aseguramiento actual es poco eficiente.

El Proceso de análisis de vulnerabilidades se realizó sobre el segmento de red completo donde se encuentran los servidores piloto, estos resultados son el punto de partida para lograr medir la reducción de vulnerabilidades.

La metodología presentada de aseguramiento para sistemas operativos, logra reducir significativamente los riesgos sobre la infraestructura tecnológica, ya que se puede actuar de manera proactiva, impidiendo que alguna de estas amenazas se materialice y ponga en riesgo la información del negocio, la cual es el activo de mayor valor para una organización.

Tabla de Contenido

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

1. CONTEXTO DE LA INVESTIGACIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA

En la actualidad la organización objeto de estudio tiene 22 años en el mercado posicionándose como líder en ventas de planes de financiamiento comercial, para adquisición de vehículos hyunday en Colombia, cuenta con una fuerza comercial distribuida por todo el país con presencia en cada uno de los concesionarios.

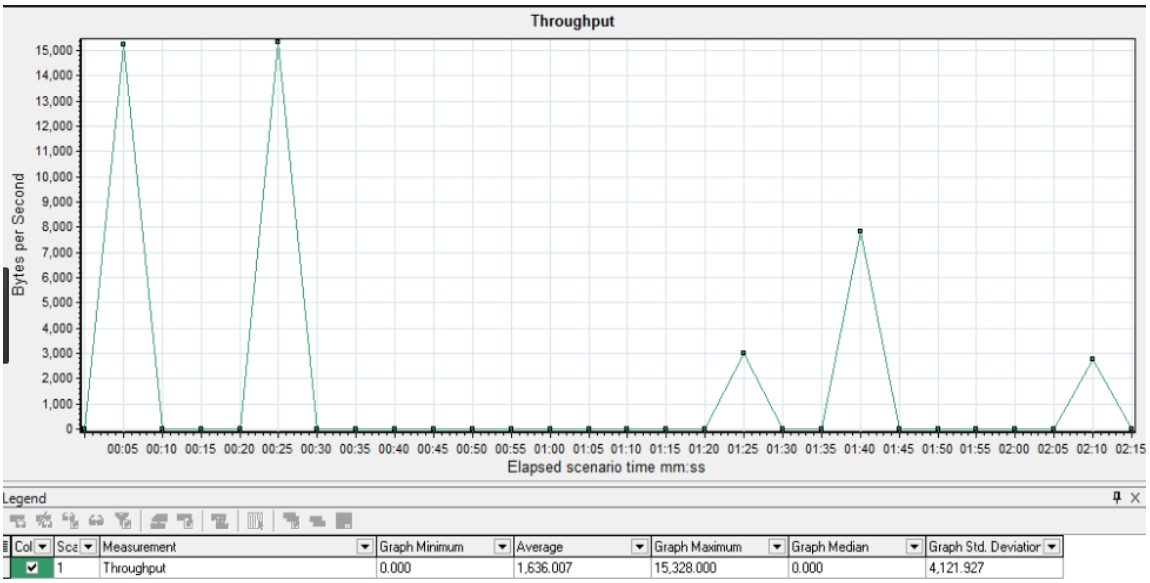
La organizacion posee servicios y aplicaciones expuestos a internet para apoyar sus procesos de negocio e impulsar su fuerza de ventas en búsqueda de clientes potenciales en el mercado colombiano, todos los datos referentes a clientes, proveedores, empleados, procesos internos son almacenados en sistemas de información, que debido a su criticidad para el negocio pueden ser vulnerables a cualquier ataque.

La plataforma tecnológica que soporta esta operación, se compone de un Centro de Datos con 10 Servidores Físicos de referencia HP ProLiant DL380p Gen6 con sistemas operativos Windows Datacenter y Windows server 2012 R2, 4 servidores Lenovo system x5580 m3 con sistemas operativos VMWARE VSphere, 1 servidor Lenovo x5580 con sistema operativo centos linux 12 , el proyecto de actualización tecnológica contempla por cada servidor entre de 6 y 7 sistemas operativos virtuales, los sistemas de producción son replicados en ambientes de pre-producción y pruebas, con ello garantizando que los controles de cambios aplicados en la infraestructura no afecten la operación de la compañía.

Diariamente el flujo de almacenamiento de oficina principal y concesionarios supera los 25Gb en almacenamiento y los throughput de red superan los 15Mbytes del canal principal (Ver Figura 1. Throughput de red), cuyo ancho de banda es de 50Mbytes, para el manejo de estos volúmenes de información la organizacion

cuenta con una SAN con arreglos de Disco rápidos de IOPS superiores a 10K y 15k, además de discos de estado sólido con un tamaño total de 25 Terabytes.

Figura 1. Throughput de red



Fuente: [Herramienta Nagios 2016]

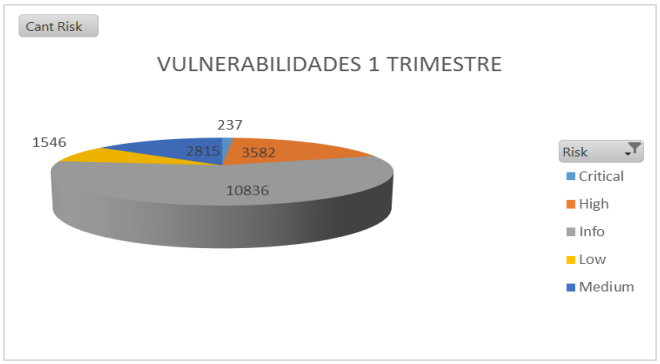
Dado que la seguridad de la información es uno de los aspectos más relevantes para la organización, finalizando el año 2016 se realizó en la organizacion un ethical hacking en búsqueda de detectar vulnerabilidades y amenazas latentes sobre los servicios internos y expuestos a internet, se encontraron fallos de seguridad sobre diferentes plataformas y servicios internos, los cuales representan un riesgo inminente, se hace necesario implementar un plan de mitigación de vulnerabilidades, ya que algunos de estos hallazgos requieren un tratamiento inmediato, para evitar que puedan ser explotadas causando indisponibilidad de los servicios de la organización.

En el informe presentado se detectaron 237 vulnerabilidades críticas sobre la infraestructura, como se observa en la figura 2 Vulnerabilidades Detectadas, las cuales requieren un tratamiento inmediato, entre las que se encuentran:

- Fallos de seguridad en sistemas operativos.
- Aplicación de actualizaciones de seguridad de Windows update.

- Cambio de versiones en software instalado sobre la infraestructura.
- Vulnerabilidades de tipo Network (Puertos abiertos, acceso a RDP, Control de equipos) entre otras amenazas de seguridad.

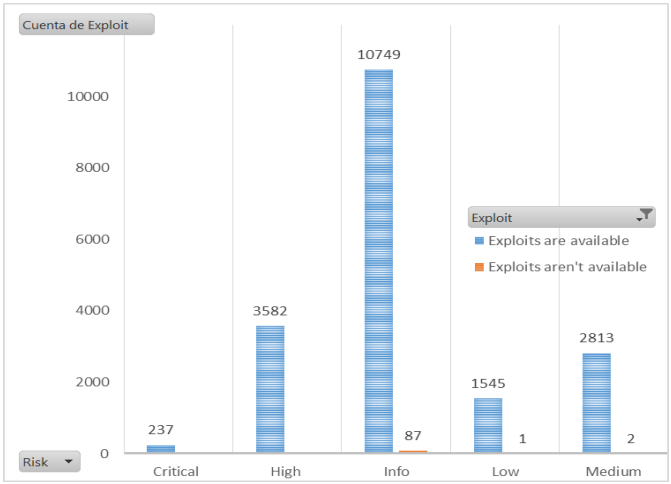
Figura 2. Vulnerabilidades Detectadas



Fuente: [Ethical hacking 2016]

Es importante resaltar que las 237 vulnerabilidades críticas detectadas, ya cuentan con Exploit disponible en la red, lo cual pone en riesgo la infraestructura (Ver Figura 2. Vulnerabilidades Detectadas), se categorizaron las vulnerabilidades que cuentan con un desarrollo para atacar estas fallas de seguridad.

Figura 3. Exploit Desarrollados



Fuente: [Ethical hacking 2016]

Estas fallas de seguridad ponen en riesgo la operación de la organización, ya que en la red este tipo de desarrollos maliciosos pueden explotar los huecos de seguridad encontrados, hay que definir un tratamiento priorizado para mitigar las vulnerabilidades detectadas sobre la infraestructura de la organizacion.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál debe ser la metodología adecuada para llevar a cabo un proceso de Hardening para reducir las vulnerabilidades encontradas en los sistemas operativos que soportan los servicios críticos de la organizacion?

1.3 JUSTIFICACIÓN

Las organizaciones son objeto de innumerables intentos de vulneración abusiva de sus sistemas, para extraer su información por parte de delincuencia informática, muchas empresas hoy en día son víctimas de estos ataques dirigidos a su infraestructura, ya que para algunos nunca fue una de sus prioridades capacitar el personal, tomar medidas de seguridad para prevenir o minimizar los ataques.

El desarrollo de este proyecto está enfocado al aseguramiento de los sistemas operativos para la plataforma Windows cualquier organizacion, es una necesidad latente preparar a las empresas ante cualquier amenaza que pueda afectar su operación, poniendo en conocimiento las diferentes herramientas disponibles en pro de elevar su nivel de seguridad en las plataformas y hacer una detección oportuna de las vulnerabilidades encontradas en los sistemas de información.

Con el conocimiento de las herramientas utilizadas para hacer Hardening, se puede definir el diseño de implementación para iniciar con la mitigacion las fallas de seguridad encontradas dentro de la organización y de esta manera generar unas políticas que permitan hacer el análisis, detección y tratamiento de vulnerabilidades de seguridad, periódicamente para prevenir ataques e intrusiones en los puntos más débiles de nuestra infraestructura.

1.4 OBJETIVOS

1.4.1 Objetivo General. Definir un proceso de Hardening para el aseguramiento de la infraestructura tecnológica de la organizacion.

1.4.2 Objetivos Específicos.

- Identificar riesgos, vulnerabilidades o fallas de seguridad sobre los sistemas operativos de la organización.
- Generar recomendaciones para mitigar los fallos o vulnerabilidades encontradas sobre la infraestructura tecnológica
- Implementar el aseguramiento de sistemas operativos endurecimiento sobre la plataforma de pruebas de la organizacion.

1.5 ALCANCES Y LIMITACIONES

1.5.1 Alcance. Este proyecto de investigación tiene como alcance crear unas plantillas de aseguramiento de sistemas operativos, basado en la metodología enunciada y utilizando las mejores prácticas de administración de infraestructura al menor privilegio, para el piloto de este proyecto, se realizará el proceso de aseguramiento a 6 servidores de pruebas, los cuales son réplicas de sistemas productivos y contienen sistemas operativos Windows server 2008, Windows server 2012 R2 y 1 Cliente Windows 7.

Sobre estos servers asignados por la organización se van a ejecutar las herramientas de análisis de vulnerabilidades y luego se realizará el Hardening utilizando como base las plantillas de aseguramiento que se desarrollarán durante este proyecto.

1.5.2 Limitaciones. Las presentes limitaciones restringirán la investigación:

- Falta de disponibilidad de recursos tecnológicos, ya que por ser una investigación aplicada y sus características técnicas es indispensable el acceso a diferentes servidores y dispositivos perimetrales de la organización, ya que con base a los indicadores de vulnerabilidad se realizará el aseguramiento de la infraestructura.

- Disposición por parte de la organización para brindar la información o disponer tiempo de alguno de los recursos de infraestructura, para soportar y probar que las aplicaciones no se hallan impactado.

1.6 LÍNEA DE INVESTIGACIÓN

Este proyecto se enmarca dentro de la línea de investigación institucional de Seguridad Informática, que desde el grupo de investigación y desarrollo en nuevas tecnologías de la información y las comunicaciones (GRIDNTIC) se enfoca en todo lo relacionado con arquitecturas de seguridad en los sistemas de información, elementos perimetrales, dispositivos de redes y comunicaciones, servidores, estaciones de trabajo en busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la triada CID (confidencialidad, integridad, disponibilidad de la información).

Para ello es de especial interés la aplicación de las técnicas de aseguramiento, de detección y prevención de intrusiones, el análisis de vulnerabilidades, la aplicación de herramientas criptográficas durante la transmisión, procesamiento y almacenamiento de la información, el uso de las mejores prácticas de seguridad en el software, esta investigación de implementación de un proceso de Hardening hace especial énfasis en los sistemas operativos, y finalmente la aplicación de técnicas de verificación y auditoria a los procesos que se ejecutan dentro de un servidor entorno a la información, partiendo de la consigna del mínimo privilegio, las plantillas de aseguramiento garantizan la aplicación de controles usando las técnicas documentadas.

El objetivo que se plantea en esta línea es llegar, por medio del funcionamiento de todos los elementos descritos en esta investigación, a desarrollar una estrategia integral para atender la necesidad de seguridad en los sistemas de operativos de la organizacion.

2. MARCO REFERENCIAL

2.1 MARCO TEÓRICO

2.1.1 Hardening en Sistemas Operativos. Hardening es un proceso cuya finalidad es la reducción de posibles vulnerabilidades en los sistemas que son previamente configurados por defecto. La cantidad de posibles vulnerabilidades aumenta dependiendo sus prestaciones y la cantidad de entornos que se ejecuten en estos sistemas. La implementación se requiere para reducir el nivel de riesgo para los siguientes factores: software desactualizado, usuarios inactivos, inicios de sesión innecesarios y la desactivación servicios que no se tengan dentro del inventario y que puedan facilitar su administración y control por medio de un ataque.

Se organizan múltiples estrategias para la aplicación de Hardening, pero el proceso debe ser personalizado y adecuado a cada entorno específico en función de sus necesidades para no incurrir en negación de servicios que puedan afectar la operación o las aplicaciones que ya se encuentran dentro de un entorno productivo.

Todas las organizaciones tienen al menos un servicio o recurso que consideran crítico, ya sea una aplicación Core o un servidor web de e-Commerce de altas transacciones online, un servidor de base de datos que contenga datos sensibles con información personal o financiera de los clientes, o un servidor de correo que se encarga de las comunicaciones corporativas confidenciales. Es por esto que las organizaciones hacen uso de estas estrategias para endurecer y fortalecer la seguridad en sus sistemas y garantizar la protección de los servidores, software, y de la información que contienen.

2.1.2 Actividades técnicas Preliminares. Para llevar a cabo un proceso de aseguramiento se deben tener en cuenta las actividades preliminares necesarias las cuales son:

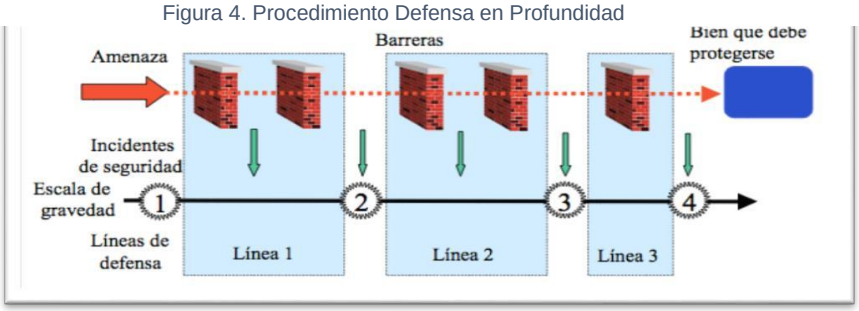
- Configuraciones seguras**:** Esta actividad es importante a la hora de implementar Hardening en un sistema operativo, ya que la mayoría de

intrusiones son habilitadas por no realizar una adecuadafin gestión técnica o la no existencia de políticas de seguridad en los sistemas operativos. Los permisos a usuarios y servicios mal configurados fortalecen el acceso a información que pueda facilitar aún más la intrusión, por lo cual una configuración de seguridad y un dispositivo perimetral puede evitar que el atacante tome control total del sistema operativo manipulándolo de forma que se pueda acceder a otros equipos en red.

- La asignación de contraseñas seguras: su longitud debe ser superior a los 8 caracteres y dificultad es importante para limitar el acceso, se puede asignar tanto en el LDAP como política, para que sistema operativo y aplicaciones hagan uso del Single Sign On, con esto se fortalece las autenticaciones de usuarios por medio de un controlador de domino.

2.1.3 Defensa en Profundidad. Los ataques direccionados son ataques con los que se logra tener un alto nivel de intrusión por su estructura y técnicas utilizadas, es importante implementar el aseguramiento de los sistemas operativos aplicando el concepto de seguridad en profundidad (Ver Figura 4. Líneas de defensa)

Figura 4. Procedimiento Defensa en Profundidad



Fuente: http://www.ssi.gouv.fr/archive/es/confianza/documents/methods/mementodep-V1.1_es.pdf

En la imagen anterior se puede observar claramente el proceso de protección que se maneja para aplicar el concepto de defensa en profundidad, se denomina líneas a cada nivel de seguridad que se presenta frente a cada amenaza, cada uno de estos ataques dependiendo de su agresividad es tratado de manera diferente y filtrado en cada línea de seguridad que se manifiesta al tener un ataque informático.

Cada amenaza se clasifica según su impacto y se define en una escala de gravedad donde se puede afirmar la penetración del ataque según la línea de defensa que vulnera, con esto se puede analizar qué tipo de ataque, su efectividad, información del mismo y la forma de vulnerar las líneas de defensa.

Las líneas que componen la defensa en profundidad pueden ser estáticas o dinámicas, esto hace flexible las políticas de seguridad y elementos de seguridad que se implementen en cada línea de seguridad, los usuarios hacen parte importante en este proceso ya que estos identifican consciente o inconscientemente los problemas de seguridad que puedan causar daños o no. Para lo anterior es importante tener claras diferentes procedimientos donde se incluyen Log de actividades, bitácoras de incidentes y alertas de posibles intrusiones sobre la infraestructura que permitan actuar de manera inmediata ante un ataque, esto con el fin de determinar y el activo a proteger.

Este modelo de defensa es de gran ayuda a la hora de protegerse de vulnerabilidades de día 0, ya que por ser códigos que se explotan para tener control de los sistemas operativos el aseguramiento en líneas de seguridad ayuda a minimizar el ataque y evitar que se propague en otros sistemas causando daños significativos.

Los Exploit de día 0 son aquellos que no cuentan con una remediación inmediata frente a un problema de seguridad, por ello se hacen tan peligrosos, estos al penetrar la primera línea de seguridad dependiendo de su configuración y código malicioso puede lograr acceso al sistema manipulándolo a voluntad del atacante, para ello la línea de seguridad basada en herramientas perimetrales entra a ser importante frente al ataque, estas herramientas puede ser firewall o IDS los cuales pueden interactuar y bloquear el ataque de manera proactiva y reactiva

2.1.3 Firewall. El firewall es un dispositivo que apoya el bloqueo de conexiones entrantes y salientes de una red, esto con el fin de limitar accesos no deseados que puedan vulnerar los equipos de la red. Existen firewall de red o de host, los de red son implementados para proteger los equipos y sistemas de información de una red y los de host protegen a los equipos de cómputo o servidores directamente desde su núcleo de conexiones.

Para los equipos con firewall de host el aseguramiento tecnológico es clave ya que por medio de este se minimiza las posibles intrusiones y se bloquea accesos por medio de vulnerabilidades que afecten las aplicaciones o programas que estén en los equipos de cómputo o servidores, los firewall de host permiten por medio de reglas restringir conexiones externas a servicios y puertos del equipo, el firewall de red restringe tráfico de red y limita desde el perímetro accesos vulnerables a los sistemas.

Su configuración igualmente debe ser analizada para evitar falsos positivos los cuales podrían afectar servicios que hagan parte de la interacción con los usuarios y las aplicaciones. Existen firewall para sistemas operativos Windows y basados en Linux varia en la facilidad e interacción con el usuario final.

Figura 5. Conexión Firewall dentro de una Red Básica

Fuente: http://soluciones-ip.pe/ip/wp-content/uploads/2014/07/f1.jpg

2.1.4 Virus informático. Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador. Aunque no todos son tan dañinos. Existen unos un poco más inofensivos que se caracterizan únicamente por ser molestos.

Figura 6. Virus

Fuente:https://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1.do

Algunos métodos de infección:

- Mensajes dejados en redes sociales como Twitter o Facebook.
- Archivos adjuntos en los mensajes de correo electrónico.
- Sitios web sospechosos.
- Insertar USB, DVD o CD con virus.
- Descarga de aplicaciones o programas de internet.
- Anuncios publicitarios falsos.

2.1.6 Criptografía. La palabra Criptografía proviene etimológicamente del griego Kruiptoz (Kriptos-Oculto) y Grajein (Grafo-Escritura) y significa "arte de escribir con clave secreta o de un modo enigmático"

Aportando luz a la definición cabe aclarar que la Criptografía hace años que dejó de ser un arte para convertirse en una técnica que tratan sobre la protección (ocultamiento ante personas no autorizadas) de la información.

Es decir que la Criptografía es la ciencia que consiste en transformar un mensaje legible en otro que no lo es (mediante claves que sólo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

Figura 7. Criptografía 3DES

Fuente: https://it-skull.com/images/headers/Skytale_Fotor.jpg

Criptograma: La importancia de la Criptografía radica en que es el único método actual capaz de hacer cumplir el objetivo de la Seguridad Informática: "mantener la Privacidad, Integridad, Autenticidad..." y hacer cumplir con el No repudio, relacionado a no poder negar la autoría y recepción de un mensaje enviado.

Criptoanálisis: Es el arte de estudiar los mensajes ilegibles, encriptados, para transformarlos en legibles sin conocer la clave, aunque el método de cifrado empleado siempre es conocido.

Criptosistema:"Un Criptosistema se define como la quíntupla (m, C, K, E, D), donde:

m Representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.

C Representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.

K representa el conjunto de claves que se pueden emplear en el Criptosistema.

E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de m para obtener un elemento de C. Existe una transformación diferente Ek para cada valor posible de la clave K.

D es el conjunto de transformaciones de descifrado, análogo a E.

Todo Criptosistema cumple la condición Dk (Ek (m)) =m, es decir, que, si se tiene un mensaje m, se cifra empleando la clave K y luego se descifra empleando la misma clave, se obtiene el mensaje original m."

Algoritmos Simétricos Modernos (Llave Privada): La mayoría de los algoritmos simétricos actuales se apoyan en los conceptos de Confusión y Difusión vertidos por Claude Shannon sobre la Teoría de la Información a finales de los años cuarenta.

Estos métodos consisten en ocultar la relación entre el texto plano, el texto cifrado y la clave (Confusión); y repartir la influencia de cada bit del mensaje original lo más posible entre el mensaje cifrado (Difusión).

Algoritmos Asimétricos (Llave Privada-Pública): Estos algoritmos han demostrado su seguridad en comunicaciones inseguras como Internet. Su principal característica es que no se basa en una única clave sino en un par de ellas: una conocida (Pública) y otra Privada. Actualmente existen muchos algoritmos de este tipo, pero han demostrado ser poco utilizables en la práctica ya sea por la longitud de las claves, la longitud del texto encriptado generado o su velocidad de cifrado extremadamente largos.

Autentificación: Es cualquier método que permita garantizar alguna característica sobre un objeto dado. Se debe comprobar la autentificación de:

- Un Mensaje mediante una firma: se debe garantizar la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación. A este mecanismo se lo conoce como Firma Digital y consiste en asegurar que el mensaje m proviene del emisor E y no de otro.
- Un Usuario mediante una contraseña: se debe garantizar la presencia de un usuario autorizado mediante una contraseña secreta.

- Un Dispositivo: se debe garantizar la presencia de un dispositivo válido en el sistema, por ejemplo, una llave electrónica.

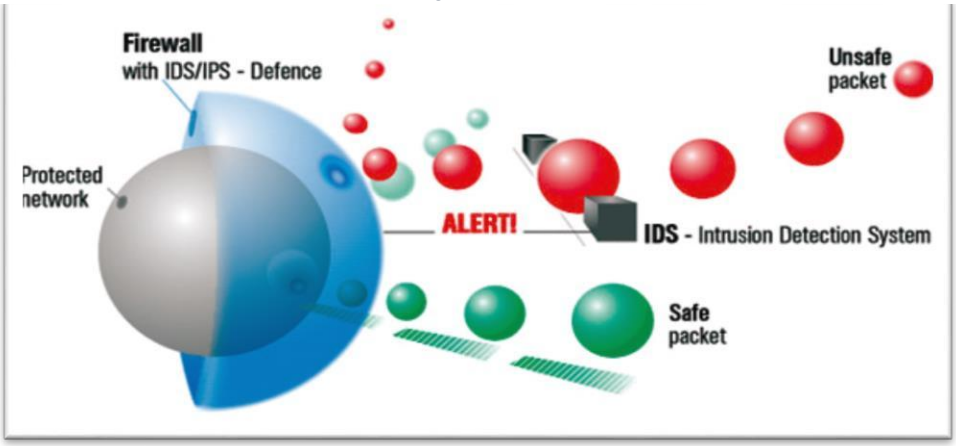
2.1.7 PGP (PRETTY GOOD PRIVACY). Este proyecto de "Seguridad Bastante Buena" pertenece a Phill Zimmerman quien decidió crearlo en 1991 "por falta de herramientas criptográficas sencillas, potentes, baratas y al alcance del usuario común.

Actualmente PGP es la herramienta más popular y fiable para mantener la seguridad y privacidad en las comunicaciones tanto para pequeños usuarios como para grandes empresas.

2.1.8 IDS. El término IDS (Sistema de detección de intrusiones) “hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión (Ver Figura 8. IDS).

Son equipos que permiten por medio de patrones y comportamientos de conexiones o tipos de ataques de red limitar el acceso o evitar las intrusiones a los sistemas. Los IDS permiten igualmente monitorear las diferentes técnicas de instrucción

Figura 8. IDS



Fuente: http://www.trendcorp.com.pe/img/dummies/intruso.jpg

de red e interactuar con el firewall y bloquear el acceso, el firewall que tienen internamente

Ayuda a eliminar las conexiones que son activadas por medio de una vulnerabilidad o un escaneo de red que pueda exponer información de los equipos y redes de una compañía.

A diferencia del firewall, los IDS son equipos proactivos y son configurados para que eliminen el riesgo antes de que se active o sea efectivo, estos riesgos van desde accesos a redes o equipos hasta la explotación de fallos en aplicaciones o software que estén instalados en los equipos de cómputo o servidores de aplicaciones.

Igualmente, los IDS se configuran para generar alertas proactivas y activas, los registros o LOG determinan los comportamientos de los sistemas y posibles intrusiones, esto apoya al administrador de seguridad para mejorar la configuración y proteger los sistemas.

2.1.9 Fingerprinting. El Fingerprinting es una técnica que consiste en analizar las huellas que deja un sistema operativo en sus conexiones de red. Está basada en los tiempos de respuesta a los diferentes paquetes, al establecer una conexión en el protocolo TCP/IP, que utilizan los diferentes sistemas operativos.

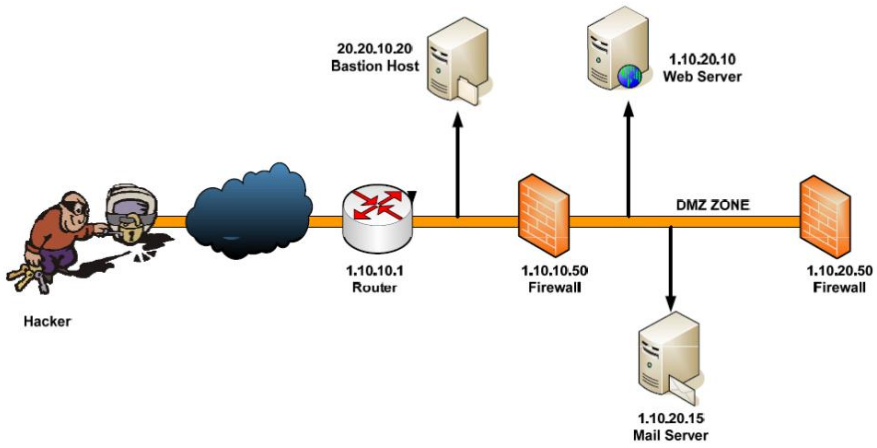
Los programas que se utilizan para realizar OS Fingerprinting se basan en dos filosofías, escáner pasivo o activo:

En un escáner activo la herramienta envía paquetes esperando una respuesta del sistema operativo y la compara con su base de datos. Suele usar técnicas como: inundación de paquetes SYN, envió de flags TCP incorrectos, envió de paquetes FIN, estas técnicas son fáciles de detectar.

En un escáner pasivo la herramienta escucha el tráfico para identificar las maquinas que actúan en la red comparando sus tiempos de respuesta, pero sin actuar en la red. Es una técnica más difícil de detectar, pero tiene dos inconvenientes: algunas veces hay que esperar mucho tiempo si el sistema a identificar no envía paquetes, no podemos identificarlo y al no enviar peticiones la herramienta no genera respuestas esto limita su acción al ámbito de broadcast, se puede solucionar con técnicas de envenenamiento de la cache ARP.

2.1.10 Footprinting. Consiste en la recogida de información de la víctima/objetivo, para conseguir vectores de ataque, esto quiere decir que, a más información recogida más vectores de ataque a explotar, esta fase pertenece al sistema que se utiliza para auditar redes, o incluso páginas web, este punto es una de las fases más importantes antes de intentar penetrar un sistema.

Figura 9. FootPrinting

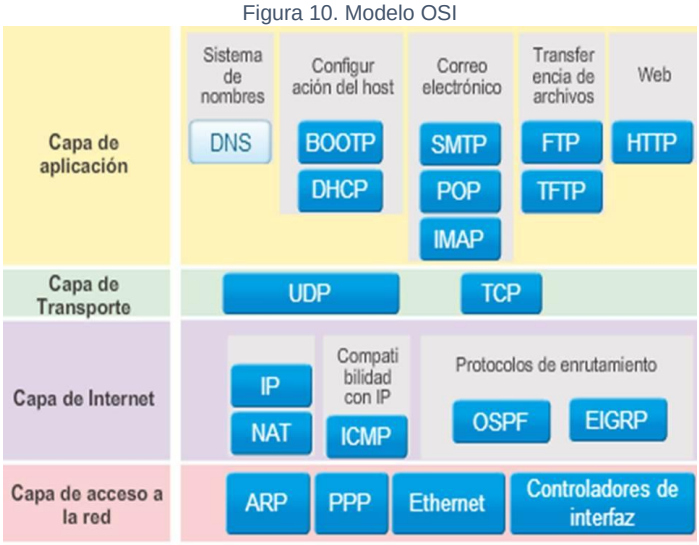


Fuente: http://hardsoftsecurity.es/index.php/2015/10/26/introduccion-al-footprinting-con-kali-linux-2-0/

2.1.11 Modelo OSI. El modelo OSI (Open Systems Interconection) es la propuesta que hizo la ISO (International Standards Organization) para estandarizar la interconexión de sistemas abiertos. Un sistema abierto se refiere a que es independiente de una arquitectura específica. Se compone el modelo, por tanto, de un conjunto de estándares ISO relativos a las comunicaciones de datos, para efectos de los sistemas operativos la capa 7 de aplicación debe contar con la seguridad dispuesta como interfaz para los usuarios finales, ya que los Exploit intentan explotar vulnerabilidades de las aplicaciones finales (Ver Figura 10. Modelo OSI).

El modelo OSI establece los lineamientos para que el software y los dispositivos de diferentes fabricantes funcionen juntos. Aunque los fabricantes de hardware y los de software para red son los usuarios principales del modelo OSI, una comprensión general del modelo llega a resultar muy benéfica para el momento en que se expande la red o se conectan redes para formar redes de área amplia (WAN).

Figura 10. Modelo OSI



Fuente: https://mateorendona.files.wordpress.com/2014/08/diapositiva16.jpg

Capa 7

La capa de Aplicación funciona como el acceso a los servicios que proporciona la red, así como de proporcionar al sistema operativo servicios como el de la transferencia de archivos.

2.1.12 Seguridad en Redes. Sin importar que estén conectadas por cable o de manera inalámbrica, las redes son indispensables para las actividades diarias. Las personas como las organizaciones dependen de sus equipos informáticos y de las redes para funciones como correo electrónico, acceso a aplicaciones, servicios internos de la organización y acceso a file Server de archivos.

Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo, los ataques a una red pueden ser nefastos y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de archivos importantes.

A los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se les denominan “Piratas Informáticos”. Una vez que un pirata tiene el acceso a una red pueden surgir 4 tipos de amenazas:

- Robo de información
- Robo de identidad
- Perdida y manipulación de datos
- Interrupción del servicio.

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa:

- Amenazas externas: Provienen de personas que no tienen autorización para acceder al sistema o a la red de computadoras. Logran introducirse principalmente desde Internet, enlaces inalámbricos o servidores de acceso por marcación o dial.
- Amenazas internas: Por lo general, conocen información valiosa y vulnerable o saben cómo acceder a esta. Sin embargo, no todos los ataques internos son intencionados.

Estos son los delitos informáticos más frecuentes en la red:

- Abuso del acceso a la red por parte de personas que pertenecen a la organización.
- Virus.
- Suplantación de identidad.
- Uso indebido de la mensajería instantánea.
- Denegación de servicio, caída de servidores.

Acceso no autorizado a la información:

- Robo de información de los clientes o de los empleados.
- Abuso de la red inalámbrica
- Penetración en el sistema.
- Fraude financiero.
- Detección de contraseñas.
- Registro de claves.
- Alteración de sitios web.
- Uso indebido de una aplicación web pública.

Hay diversos tipos de ataques informáticos en redes, algunos son:

- Ataques de denegación de servicios (DOS): es un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.
- Man in the middle (MITM): es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre las 2 partes y falsifica los intercambios para hacerse pasar por una de ellas.
- Ataques de replay: una forma de ataque de red en el cual una trasmisión de datos válida es maliciosa o fraudulentamente repetida o recalcada, es llevada

a cabo por el autor o por un adversario que intercepta la información y la retransmite posiblemente como parte de un ataque enmascarado.

2.1.13 Buenas Prácticas en Sistemas Operativos. Mantener actualizado el sistema operativo y las aplicaciones con sus correspondientes parches de seguridad, nombre que recibe el código que soluciona una debilidad en un SO o aplicación.

Códigos maliciosos como Slammer, Sasser o Zotob, que infectaban los sistemas a través de vulnerabilidades (debilidades en el código de los SO y aplicaciones en cuanto a este aspecto de la seguridad, las medidas prácticas de prevención se enfocan en:

- No descargar actualizaciones desde sitios de dudosa reputación y hacerlo sólo desde sitios de confianza. Descargar las actualizaciones desde sitios no oficiales implica un potencial riesgo de infección.
- Descargar las actualizaciones a través de los mecanismos ofrecidos por el fabricante. En el caso de las actualizaciones de productos de Microsoft, la disponibilidad de los mismos es informada el segundo martes de cada mes, aunque puede haber excepciones en casos de vulnerabilidades críticas.

Para las plataformas Microsoft se puede:

- Acceder al sitio web de Windows Update1 para obtener los últimos parches de seguridad
- Configurar en el Centro de Seguridad de Windows la automatización, o no, de descarga de actualizaciones
- Utilizar herramientas gratuitas como MBSA2 (Microsoft Baseline Security Analyzer) para verificar la falta de actualizaciones en el sistema operativo, o PSI3 (Personal Software Inspector) de la empresa para chequear las aplicaciones

- Implementar (en entornos corporativos) los WSUS (Windows Server Update Services) de Microsoft
- También en entornos corporativos, y sin importar la plataforma, se aconseja preparar políticas de gestión de actualizaciones claras, que permitan coordinar y administrar los parches de seguridad tanto de los sistemas operativos como de las aplicaciones. Lo ideal es que esta política de gestión forme parte de la PSI (Política de Seguridad de la Información)

2.1.14 Aseguramiento del Sistema operativo. Otro de los aspectos importantes en materia de prevención, radica en configurar el sistema operativo para hacerlo más seguro. Entre las buenas prácticas que se pueden tener en cuenta se encuentran:

- Deshabilitar las carpetas compartidas. Esto evita la propagación de gusanos que aprovechen ese vector como método de infección.
- Utilizar contraseñas fuertes. El empleo de contraseñas fáciles de recordar es otra de las debilidades que los códigos maliciosos suelen aprovechar para propagarse por los recursos de información.
- Crear un perfil de usuario con privilegios restringidos [6]. Por defecto, el usuario que crean las plataformas Windows al momento de su implementación posee privilegios administrativos. Esto es un factor que aumenta la probabilidad de infección.
- Deshabilitar la ejecución automática de dispositivos USB. Los dispositivos de almacenamiento removibles que se conectan al puerto USB constituyen un vector de ataque muy empleado por el malware para la propagación, sobre todo, de gusanos.
- De ser posible, migrar hacia plataformas (sistemas operativos) modernas. En la actualidad, los sistemas operativos antiguos (Microsoft Windows9x, NT, XP, WK3) no cuentan con soporte técnico ni con actualizaciones de

seguridad por parte de Microsoft, lo cual constituye un punto que permite la explotación de vulnerabilidades

- Configurar la visualización de archivos ocultos ya que la mayoría de los códigos maliciosos se esconden en el sistema con este tipo de atributos.
- Configurar la visualización de las extensiones de archivos [10] para poder identificar las extensiones de los archivos descargados y no ser víctimas de técnicas como la doble extensión.

2.1.15 Protección en el correo electrónico. El correo electrónico constituye uno de los canales de propagación/infección de malware más utilizados por atacantes; por lo tanto, es importante que los usuarios incorporen como hábito determinadas prácticas que permitan prevenir los ataques realizados a través de códigos maliciosos.

En consecuencia, a continuación, se presenta una serie de medidas preventivas orientadas a aumentar la seguridad durante el uso del correo electrónico.

2.1.16 Spam. El spam es el correo electrónico que promociona diferentes productos y servicios a través de publicidad no solicitada, enviada masivamente a las direcciones de correo de los usuarios.

Constituye uno de los principales medios de propagación de una importante cantidad de códigos maliciosos y por lo tanto se recomienda:

- No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Esto asegura que no se ejecutará un malware.
- Cuando se reciben adjuntos, prestar especial atención a las extensiones de los mismos, ya que suelen utilizar técnicas de engaño como la doble extensión o espacios entre el nombre del archivo y la extensión del mismo.

- Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats, entre otros. Esto minimiza la posibilidad de que la dirección se guarde en la base de datos de los spammers
- Utilizar filtros anti-spam que permitan el filtrado del correo no deseado.
- No responder jamás el correo spam. Es preferible ignorarlos y/o borrarlos, ya que si se responde se confirma que la dirección de correo se encuentra activa.
- En lo posible, evitar el re-envío de mensajes en cadena (por lo general son hoax), ya que suelen ser utilizados para recolectar direcciones de correo activas.
- Si de todos modos se desea enviar mensajes en cadena, es recomendable hacerlo siempre Con Copia Oculta (CCO) para que quien lo recibe lea solo la dirección del emisor.
- Proteger la dirección de correo utilizando una cuenta alternativa durante algún proceso de registro en sitios web y similares. Esto previene que la dirección de correo personal sea foco del spam.
- Utilizar claves seguras y cambiar la contraseña con periodicidad si se utiliza web mail.

2.1.17 Phishing. El phishing es una modalidad delictiva de estafa realizada a través de Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico. Entre las buenas prácticas de seguridad que se recomiendan a los usuarios, para que éstos eviten ser víctimas del phishing, están las siguientes:

- Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de este medio, de esta manera se minimiza la posibilidad de ser víctima de esta acción delictiva.

- Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles ya que suelen ser métodos de Ingeniería Social.
- No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden re direccionar hacia sitios web clonados o hacia la descarga de malware.
- Asegurarse de que la dirección del sitio web al cual se accede comience con el protocolo https. La" s" final, significa que la página web es segura y que toda la información depositada en la misma viajará de manera cifrada.
- Verificar la existencia de un certificado digital en el sitio web. El certificado digital se despliega en pantalla al hacer clic sobre la imagen del candado.
- Revisar que el certificado digital no haya caducado, ya que el mismo podría haber sido manipulado intencionalmente con fines maliciosos.
- Comunicarse telefónicamente con la compañía para descartar la posibilidad de ser víctimas de un engaño, si se tiene dudas sobre la legitimidad de un correo.
- Jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico, ya que la comunicación podría ser interceptada y robada.
- Habituarse a examinar periódicamente la cuenta bancaria, a fin de detectar a tiempo alguna actividad extraña relacionada con la manipulación de la cuenta o transacciones no autorizadas.

2.1.18 Seguridad en la navegación. En los últimos años, Internet se ha transformado en una plataforma de ataque donde acciones delictivas se llevan a cabo a través de diferentes técnicas como por ejemplo el Drive-by-Download. En consecuencia, es fundamental navegar con cautela y tener presente las recomendaciones más importantes. Entre ellas:

- Evitar el ingreso a sitios web con contenidos que, dependiendo el país, son ilegales, como aquellos que ofrecen cracks y programas warez; ya que constituyen canales propensos a la propagación de malware.
- Impedir la ejecución de archivos desde sitios web sin verificar previamente que es lo que dice ser. Es importante no hacer clic sobre el botón ejecutar ya que esto provoca que el archivo se ejecute automáticamente luego de descargado, dejando al margen la posibilidad de verificar su integridad.
- Descargar programas de seguridad solamente desde el sitio oficial del mismo, para evitar la descarga de archivos que pudieran ser previamente manipulados con fines delictivos.
- Si es posible, leer atentamente las políticas de privacidad de las aplicaciones descargadas desde sitios web no oficiales o de dudosa reputación, antes de instalarlas.
- No realizar la instalación de complementos extras como barras de tareas o protectores de pantallas sin verificar previamente su autenticidad.
- Configurar el navegador web para minimizar el riesgo de ataques a través del mismo.
- Instalar, en lo posible, un programa antivirus con capacidades proactivas, como ESET NOD32, que permita detectar códigos maliciosos incluso desconocidos y explorar con el mismo cada archivo descargado.
- Disponer, además, de un Firewall personal que permita bloquear comunicaciones entrantes y salientes., por ejemplo, incorpora un Firewall personal de manera integrada.
- Tratar de no acceder a servicios como Home-Banking desde lugares públicos (ciber, bibliotecas, cafés, hoteles, etc.).
- Si se navega desde sitios públicos, es recomendable eliminar los archivos temporales, caché, cookies, direcciones URL, contraseñas y formularios donde se haya ingresado datos.

2.1.19 Seguridad en redes P2P. Las redes Punto a Punto, más conocidas como P2P, forman otro de los canales por donde se propagan diferentes amenazas informáticas y cuya relación con códigos maliciosos es muy activa. Esta situación obliga a tener en cuenta una serie de medidas preventivas tendientes a fortalecer la seguridad del sistema, entre las cuales se destacan:

- Explorar con una solución antivirus de alta efectividad en la detección de amenazas conocidas y desconocidas, como ESET NOD32, absolutamente todos los archivos que se descargan a través de esta red, sin importar su extensión.
- Evitar el almacenamiento de información confidencial y sensible en la misma computadora donde se comparten archivos por redes P2P, para evitar que la misma sea robada.
- Verificar que el programa cliente de intercambio de archivos no instale o descargue componentes extras, ya que en la mayoría de los casos son códigos maliciosos del tipo Adware/Spyware.
- Asegurarse de que los archivos a descargar no se encuentren sometidos a métodos de engaño como doble extensión, debido a que se trata de una técnica muy empleada por el malware.
- Controlar que exista coherencia entre el tamaño original del archivo descargado y el tamaño aproximado que debería tener, para descartar la posibilidad de que se esté en presencia de programas troyanos.
- Chequear que la carpeta de intercambio de archivos contenga sólo los archivos que se desea compartir.
- Revisar la configuración de seguridad del programa cliente. Esto ayuda a maximizar la seguridad durante el proceso de descarga de archivos.

2.1.20 Seguridad en Dispositivos Removibles. Los dispositivos de almacenamiento removibles que se conectan a través del puerto USB (memorias, cámaras digitales, filmadoras, teléfonos celulares, etc.), constituyen otro de los mayores focos de propagación/infección de códigos maliciosos. Por lo tanto, es necesario tener presente alguna de las siguientes medidas que ayudan a mantener el entorno de información con un nivel adecuado de seguridad, ya sea en entornos corporativos como en entornos hogareños:

- Establecer políticas que definan el uso correcto de dispositivos de almacenamiento removibles. Esto ayuda a tener claro las implicancias de seguridad que conlleva el uso de estos dispositivos.
- Brindar acceso limitado y controlado de los usuarios que utilizan estos dispositivos, para controlar la propagación de potenciales amenazas y el robo de información.
- De ser necesario, registrar el uso de los mismos y/o habilitar/deshabilitar puertos del tipo USB. Esto permite un mayor control sobre el uso de dispositivos de este estilo.
- En casos extremos es recomendable bloquear, por medio de políticas de grupo, de dominio o corporativas, el uso de estos dispositivos.
- Si se transporta información confidencial en estos dispositivos, es recomendable cifrarla. De esta forma, en caso de robo o extravío, la información no podrá ser vista por terceros.
- Ya sea en el hogar o en las organizaciones, se recomienda implementar una solución antivirus con capacidades proactivas como ESET NOD32 Antivirus y administrar cada nodo de la red de manera centralizada con ESET Remote Administrator.
- Es recomendable explorar con el antivirus cualquier dispositivo que se conecte a la computadora para controlar a tiempo una posible infección.
- Deshabilitar la ejecución automática de dispositivos en los sistemas operativos Microsoft Windows, ya que muchos códigos maliciosos

aprovechan la funcionalidad de ejecución automática de dispositivos de las plataformas Microsoft para propagarse a través de un archivo Autorun.inf

2.1.21 CVSS (Common Vulnerability Scoring System). La metodología CVSS utiliza tres grupos de métricas, la base, temporal y ambiental. En este informe se utiliza el grupo métrica Base para ayudar en la realización de análisis de riesgos cualitativa. El informe se centrará en las puntuaciones de CVSS de 4,0 a 10,0.

Hay dos grupos sub de la Base métricas, la métrica de acceso y las métricas de impacto. La métrica de acceso asigna un nivel de riesgo basado en el vector utilizado para obtener acceso al sistema de destino.

Las métricas de acceso incluyen:

- El acceso del vector: que refleja los métodos utilizados para aprovechar una vulnerabilidad
- Acceso Complejidad: que mide la dificultad o complejidad de que un atacante se enfrenta a aprovechar una vulnerabilidad una vez obtenido el acceso
- Autenticación: que mide cómo se requieren muchas repeticiones de autenticación para explotar con éxito una vulnerabilidad

Las métricas de impacto usan la tríada de la CIA (confidencialidad, integridad, disponibilidad) para asignar una puntuación de impacto a una vulnerabilidad. Las métricas de impacto incluyen:

- Impacto confidencialidad: Mide la confidencialidad después de explotar con éxito, es decir, qué tan bien los accesos de usuarios no autorizados se pueden prevenir y limitar el acceso a la información que podría ayudar aún más el ataque encubierto
- Integridad Impacto: Medidas en qué medida la información almacenada en el sistema se ve afectada cuando se explota con éxito, es decir, el impacto de

la exactitud y fiabilidad de la información almacenada en el sistema de la víctima

- Impacto Disponibilidad: mide qué recursos del sistema se efectúan por la vulnerabilidad se aproveche, algún ataque puede consumir CPU, red, u otros recursos disponibles en sistema de destino

El informe CVSS muestra vulnerabilidades dentro de cada uno de los diferentes rangos de puntuación CVSS (4,0 - 4,9, 5,0 a 5,9, 6,0 - 6,9, 7,0 a 7,9, 8,0 a 8,9, 9,0 - 9,9, y 10,0). Los colores para CVSS puntuaciones son de color naranja de gravedad media con una calificación de 4,0 - 6,9, rojo para los altos niveles de gravedad que tienen una calificación de 7,0 - 9,9, y la púrpura para severidades críticos con una calificación de 10.0.

2.2 ANTECEDENTES

La seguridad de la información para una organización depende de diferentes frentes: el físico, referente a la infraestructura donde se almacena dicha información; el contexto laboral, relacionado con el grado de confidencialidad del personal que la manipula, y el lógico, que se refiere a la configuración de sus niveles de disponibilidad e integridad. Es así como técnicamente se ha caracterizado que un esquema seguro debe corresponder al ajuste de los niveles de confidencialidad, integridad y disponibilidad de la información, según la norma ISO 27001.

Cuando se describe la triada de seguridad, se encuentran implícita la información como activo más importante, por lo que las organizaciones deben adelantar un proceso SGSI (Sistema de Gestión de la seguridad de la Información), estableciendo controles, métricas en pro de elevar sus niveles de seguridad y respuesta ante incidentes informáticos.

En la actualidad, la determinación del nivel de inseguridad (visto desde la óptica de vulnerabilidad y riesgo) de la información trasciende los niveles de su uso y/o

operatividad, de forma que es necesario asegurar su fuente de origen, almacenamiento y los medios por los que se transmite, donde se abren nuevas configuraciones al fraude, a la alteración y al uso indebido; esto establece la importancia al aseguramiento de sistemas operativos y redes por medio de parametrizaciones de seguridad para fortalecer los controles establecidos sobre la información.

Para este proyecto de investigación se identificaron por medio de un análisis de vulnerabilidades varios problemas sobre la infraestructura que soporta la información para la organizacion, por la ausencia de un proceso de mitigación de vulnerabilidades por parte del grupo de infraestructura, o por una mala gestión de las mismas.

De acuerdo al informe presentado correspondiente a las vulnerabilidades del primer trimestre, el 18% de las vulnerabilidades encontradas son puntuadas por la herramienta Nessus como críticas, estas amenazas cuentan con un Exploit disponible en la red y se pueden ejecutar dentro de la organizacion, este porcentaje es significativo, pues su impacto en la organización puede ser fatal, dado que los atacantes internos se pueden considerar delincuentes informáticos y para su identificación se puede utilizar el modelo SKRAM (sigla en inglés de: Habilidad, Conocimiento, Recursos, Acceso y Motivo).

El modelo de negocio de la organizacion se está encaminando al uso de las tecnologías de la información en la nube y el uso de comunicaciones en entornos de alta disponibilidad, aumentando el uso de los recursos informáticos por parte de los usuarios y las probabilidades de ser vulnerables por delincuentes informáticos. El área de riesgos operativos identifico algunos costos ocultos que tiene la reingeniería de procesos para la implementación de políticas de seguridad en el caso de esta empresa en particular y por medio de una matriz de riesgos definió el valor corporativo que representa si alguno de estos riesgos llegara a materializarse.

Es por este motivo que este proyecto toma importancia, al tener una metodología clara para identificar y cuantificar las vulnerabilidades para mitigarlas en los procesos posteriores, la implementación de un sistema de gestión de la seguridad de información es necesario para realizar la gestión y mitigación de vulnerabilidades, para el cumplimiento de objetivos, reducir el riesgo y proteger la información.

2.3 MARCO CONCEPTUAL

Las teorías que se utilizaron durante el desarrollo de la investigación, involucran la terminología relacionada con la seguridad informática.

- Amenaza: Es un hecho, incidente o persona que puede generar daños a un sistema informático, donde puede causar pérdida de información, destrucción de información o problemas funcionales de un sistema o red informática.
- Antivirus: es un software diseñado para la detección de software con código malicioso o destructivo.
- Botnet: Es una red de equipos donde se controlan desde un servidor el cual puede ejecutar instrucciones a los equipos infectados y realizar tareas de forma masiva.
- Caballo de Troya: Es un código malicioso donde se logra integrar en un software legitimo otro con intensiones mal intencionadas, regularmente se activa el software legitimo e instantáneamente el software malicioso.
- Cracker: Es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- Estafador: Utiliza el correo electrónico u otro medio para engañar a otras personas para que brinden información confidencial como número de cuenta o contraseñas.
- Exploits o programas intrusos: Son códigos diseñados para aprovechar vulnerabilidades de sistemas operativos, programas o aplicaciones con debilidades en su estructura de desarrollo.

- Firewall: Es un dispositivo perimetral que identifica y bloquea intentos de intrusión a una red informática.
- Gusanos: Es un código malicioso que logra auto propagarse por medio de vulnerabilidades o procedimientos no consientes de los usuarios.
- Ingeniería social: es un método de engaño donde se motiva al usuario a dar información personal como datos privados o contraseñas de acceso a sistemas de información.
- Hacker: Un experto en programación. Recientemente este término se ha utilizado con frecuencia con un sentido negativo para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- Hacker de sombrero blanco: Una persona que busca vulnerabilidades en los sistemas o en las redes y a continuación informa a los propietarios del sistema para que lo arreglen.
- Hacker de sombrero negro: utilizan su conocimiento de las redes o los sistemas informáticos para beneficio personal o económico, un cracker es un ejemplo de hacker de sombrero negro.
- Host (sistema anfitrión, sistema principal / albergar, dar albergue): equipo que mediante la utilización de los protocolos tcp/ip, permite a los usuarios comunicarse con otros sistemas anfitriones de una red.
- IP address (dirección IP): Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.345.
- Keystroke logger o programa de captura de teclado (keylogger): Es un código que al ser instalado en un computador captura las pulsaciones del teclado y los registra en un archivo de texto o los envía a un correo electrónico o servidor ftp.
- Pharming: Es la alteración de los archivos host donde se puede redirigir el tráfico de un dominio a una ip determinada y capturar datos personales o instalar software malicioso.

- Phishing: Técnica de captura de información por medio de páginas web falsas.
- Spyware: software diseñado específicamente para el robo de información, se activa por medio del uso de programas o vulnerabilidades de los sistemas operativos.
- Phrieaker: Persona que manipula la red telefónica para que realice una función que no está permitida. Por lo general, a través de un teléfono público para realizar llamadas de larga distancia gratuitas.
- Spammer: Persona que envía grandes cantidades de mensajes de correo electrónico no deseado, por lo general, los spammers utiliza virus para tomar control de las computadoras domésticas y utilizarlas para enviar mensajes masivos.
- Unix: Sistema operativo interactivo y de tiempo compartido creado en 1969 por ken Thompson. Reescrito a mitad de la década de los ’70 por AT&T alcanzó enorme popularidad en los ambientes académicos y, más tarde en los empresariales, como un sistema portátil robusto, flexible y portable, muy utilizado en los ambientes internet.

2.4 BUENAS PRÁCTICAS Y MARCO LEGAL

2.4.1 Políticas de seguridad. Una política de seguridad informática es una forma de establecer responsabilidades y lineamientos, en función de recursos y servicios informáticos. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger, el personal debe ser consiente del uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

Estos son los estándares, normas, guías y/o buenas prácticas utilizadas para el desarrollo del marco arquitectónico del modelo de seguridad y para el desarrollo en la selección, análisis y extracción de riesgos y controles para el marco de seguridad

de la información para centros de datos alojados en las instalaciones propias o de un proveedor.

2.4.2 ISO/IEC 27001:2013. Norma o estándar para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información, con un enfoque basado en procesos. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones. La norma define los controles que deben implementarse para la adopción de un sistema de seguridad, pero no indica cómo; la ISO 27001:2005 es una norma certificable (ISO, ISO/IEC 27001, 2005).

2.4.3 ISO/IEC 27002:2013. Estándar de seguridad que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. No es certificable. Tiene los mismos controles de la ISO 27001:2005 pero esta norma además incluye guía de implementación de los controles (ISO, ISO/IEC 27002, 2005).

4.4 ISO/IEC 20000:2005. Estándar que recoge las mejores prácticas para el proceso de GSTI (Gestión de Servicios de T.I) identificando SLA's (Services Level Agreement) basados en métricas de seguridad que sean relevantes para medir y monitorear el desempeño de seguridad de los servicios de computación en la nube.

2.4.5 ISO/IEC 27001:2005. La norma 27001 establece modelos de seguridad de la información que garantizan las tres características principales de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

2.4.6 Ley 1581 de 2012. Esta ley se da como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

2.5 MARCO INSTITUCIONAL

Esta Sociedad Administradora de Planes de financiamiento Comercial es una empresa de HYUNDAI MOTOR COMPANY y la red de concesionarios Hyunday de todo el país, está vigilada por la Superintendencia de Sociedades. En 20 años de operación con la organizacion, más de 74.000 familias colombianas han estrenado un Hyunday cero kilómetros a un costo muy bajo y al mes de enero de 2015, el 12% de las ventas de la marca se hacen por este exitoso sistema.

Esta empresa es una marca multinacional con cobertura regional y representa el Sistema de financiamiento Comercial en Colombia y Bolivia.

Es un Sistema de financiamiento Comercial exclusivo para adquirir un Hyunday 0 km., sin endeudarse y sin intereses, mediante la creación de grupos de personas que con sus cuotas netas mensuales conforman un fondo común para la adquisición de los vehículos Hyunday ofrece planes con cuotas mensuales desde $ 14.114 por millón. El cliente elige el plan de financiamiento para el Hyunday de su preferencia a un plazo de 60, 72 y 84 meses dependiendo de la cuota que se ajuste a su capacidad de pago.

El cliente entra a formar parte de un grupo de 150, 180 o 200 personas dependiendo del plazo, paga la cuota mensual que, unida a los aportes de los demás suscriptores del grupo, forman un fondo común administrado por una fiduciaria, con el que se adquieren los vehículos Hyunday 0 km. Los vehículos se adjudican mensualmente

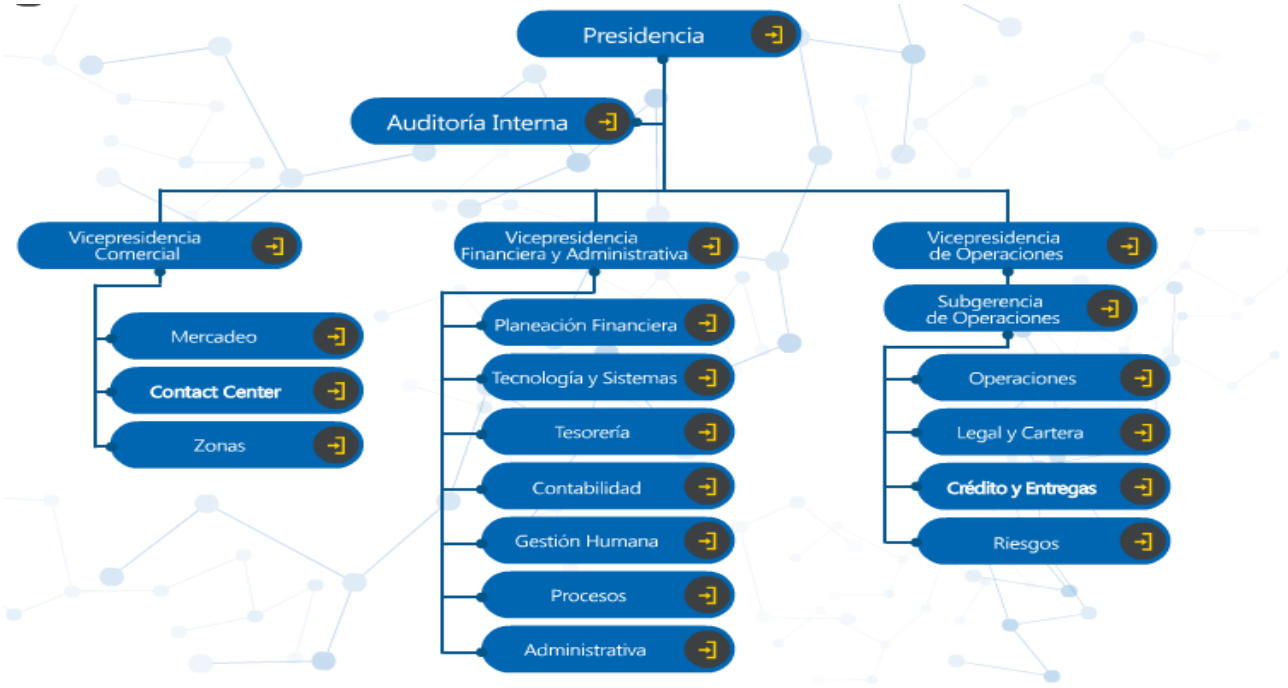
en una Asamblea de Adjudicación mediante sorteo u oferta. A cada integrante del grupo se le asigna un número de afiliación con el cual participa.

Método Asamblea

Mensualmente se realiza una asamblea que se realizan el undecimo segundo día hábil de cada mes públicamente en Bogotá por medio de un servicio VPN se interconectan la sede principal con la en la Cámara de Comercio: Sede Centro Empresarial calle 26 ubicada en la Calle 26 No. 8 – 32/44, también se tiene previsto un servicio streaming en vivo en la página web de la organización. Las cuales son supervisadas por un delegado de la Oficina de Apoyo a Localidades de la Alcaldía Mayor y un testigo. La adjudicación se realiza mediante el orden de extracción al azar, a través de un sorteo automatico que permite la selección aleatoria del número de afiliación, generando el orden de adjudicación de los vehículos. Se favorece el primer número de afiliación extraído de la balotera que cumpla con el pago oportuno de la cuota. El cliente puede obtener su vehículo por el sistema de sorteo u oferta; el número de adjudicaciones de los vehículos depende del estado de caja de cada una de las listas.

La estructura organizacional (Ver Figura 11. Organigrama) de la compañía establece que el área encargada de soportar sus recursos tecnológicos es el área de tecnología y sistemas, cuya responsabilidad de innovar, mantener, gestionar, operar y soportar la operación de los recursos tecnológicos es de la gerencia de sistemas.

Figura 11. Organigrama



Fuente: Intranet

Actualmente los recursos tecnológicos con los que cuenta la organizacion para estaciones de trabajo son un lote de 300 equipos con características iguales o superiores a Equipos Core I5 de 4Gb RAM, discos de 500Gb, sistemas operativos Windows 7, 8, 8.1 y 10, los cuales son gestionados y asignados por el área de soporte técnico.

Además, para soportar la fuerza de ventas nacional se cuentan con cerca de 180 equipos y una conexión VPN para el acceso al aplicativo Core del Negocio para brindar información de manera oportuna y veraz de los diferentes estados del cliente.

La plataforma tecnológica que soporta esta operación, se compone de un Centro de Datos con 10 Servidores Físicos de referencia HP ProLiant DL380p Gen6 con sistemas operativos Windows Datacenter y Windows server 2012 R2, 1 servidores Lenovo system x5550 con sistemas operativos VMWARE VSphere, 1 servidor Lenovo x5550 con sistema operativo UNIX , el proyecto de actualización tecnológica

contempla por cada servidor entre de 6 y 7 sistemas operativos virtuales, los sistemas de producción son replicados en ambientes de pre-producción y pruebas, con ello garantizando que los controles de cambios aplicados en la infraestructura no afecten la operación de la compañía.

Diariamente el flujo de almacenamiento de oficina principal y concesionarios es muy alto por tal motivo la compañía cuenta con un balanceador de carga con dos canales dedicados para su conexión de aplicaciones y brindando una alta disponibilidad.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

El tipo de Investigación que contempla este proyecto es la Investigación aplicada, ya que su principal objetivo, se basa en resolver un problema práctico de gestión de vulnerabilidades, con un alcance determinado y limitado. De este modo se generan pocos aportes al conocimiento científico desde un punto de vista teórico, pero se logran poner en práctica los conocimientos adquiridos en el desarrollo de cada una de estas etapas.

3.2 FASES METODOLÓGICAS

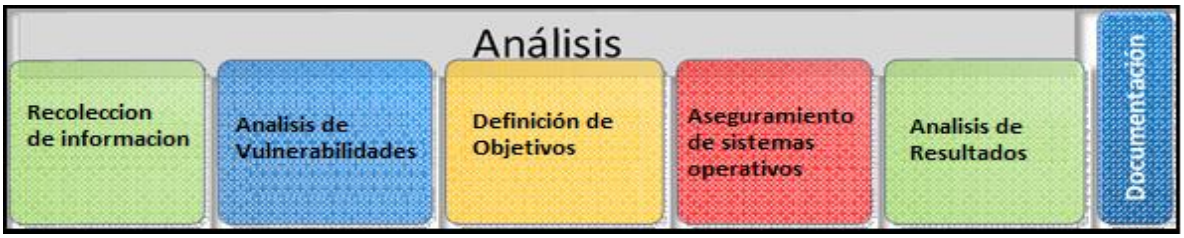
La metodología definida para implementar a futuro en este proyecto se encuentra basada en la metodología internacionalmente reconocida OWASP (Ver Figura 12. Metodología OWASP), esta metodología tiene un enfoque centralizado en el análisis de riesgos y pruebas de seguridad.

Figura 12. Metodología OWASP

Fuente: Ethical hacking 2016

para el desarrollo de este proyecto se tomarán como base de referencia algunas de sus fases, las cuales se complementarán con otras etapas de la investigación. (Ver Figura 13. Metodología Hardening).

Figura 13. Metodología Hardening



Fuente: Autor

3.2.1 Fase 1. Recolección de Información. Recolección de Información para identificar objetivos específicos (servidores, enrutadores, firewalls, RAS y demás elementos que se describen en el alcance) en las redes objetivo. De acuerdo al escenario escogido de las pruebas, se pueden dar las siguientes situaciones o Pruebas Ciegas, en donde no se proporciona ningún tipo de información y se lleva a cabo la tarea de descubrimiento de la misma, para la planeación del análisis de vulnerabilidades. En este escenario las pruebas toman más tiempo por cuanto se debe recolectar más información inicialmente se realizan las siguientes pruebas:

- Pruebas con Información, donde el cliente proporciona información básica de sus redes, servidores, elementos etc. y se puede optimizar el tiempo de pruebas orientándolas a los objetivos específicos definidos.
- Pruebas con cuenta creada y validada a nivel de un usuario nivel medio.
- Pruebas sin protección de los dispositivos de protección de perímetro (Tomando todas las precauciones para proteger los sitios a explorar).

3.2.2 Fase 2. Análisis de Vulnerabilidades. Consiste en determinar problemas de seguridad en los puntos hallados en la fase 1 Recolección de Información. Estos problemas de seguridad se pueden determinar usando herramientas especializadas orientadas al análisis de vulnerabilidades específico de protocolos. Dependiendo del tipo de herramienta utilizada y la arquitectura, el análisis de las vulnerabilidades detectadas puede tardar más tiempo, ya que, para tener mayores probabilidades de éxito, es necesario determinar los falsos positivos. Como resultado del análisis de vulnerabilidades, se determina la estrategia a seguir durante las pruebas de seguridad.

3.2.3 Fase 3. Aseguramiento de Sistemas Operativos. Asegurar los objetivos seleccionados en la fase anterior mitigando las vulnerabilidades descubiertas. Dentro de la etapa del análisis de vulnerabilidades, se prueba el cierre real de las vulnerabilidades encontraras en las etapas anteriores, para así determinar el nuevo nivel de riesgo de las mismas. Dentro del desarrollo del aseguramiento, pueden surgir nuevas vulnerabilidades no detectadas en las fases anteriores, las cuales serán incluidas dentro de esta etapa, para su verificación.

3.2.4 Fase 4. Análisis de Resultados. Análisis de resultados del aseguramiento. Al lograr la disminución de los riesgos encontrados para alcanzar la meta se repite el ciclo volviendo a la fase 1. Si la meta ha sido alcanzada o se define el fin de las pruebas, se sigue al último paso. Adicionalmente, con base en un análisis del servicio y la topología de vulnerabilidades encontradas, se desarrollan nuevos controles de aseguramiento que permitan combinar o usar los hallazgos encontrados previamente para crear nuevos y más elaborados controles, lo que permitiría determinar el impacto real de cada vulnerabilidad al darle la posibilidad al implementador del proyecto de ver el trasfondo y el alcance de dicha vulnerabilidad sobre el ambiente (pruebas) en el que se encuentra.

3.2.5 Fase 5. Análisis Final. Generación de un informe detallado con los resultados obtenidos durante todo el proceso de ejecución de la prueba, con el correspondiente análisis de dicha información para poder ser interpretada de manera correcta y entender las implicaciones a nivel de seguridad sobre la infraestructura tecnológica con las recomendaciones necesarias para solucionar dichos problemas de aseguramiento.

3.3 HERRAMIENTAS DE SOFTWARE

La guía metodológica establece los procedimientos para el Hardening y la elaboración de las plantillas de aseguramiento.

Herramientas para recolección de vulnerabilidades y posibles soluciones:

- Nessus (Licenciada por la Organización): Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y Nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.
- Baseline (Free Windows): Es una herramienta de software publicado por Microsoft para determinar la seguridad del estado evaluando faltan actualizaciones de seguridad y la configuración de seguridad menos seguras dentro de Microsoft Windows, los componentes de Windows, como Internet Explorer, IIS servidor web, y los productos de Microsoft SQL Server y Microsoft Office configuración de macros.
- GPO: Directiva de grupo es un conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo. Directiva de grupo proporciona la gestión centralizada y configuración de sistemas operativos, aplicaciones y configuración de los usuarios en un entorno de Active Directory, por medio del envió de políticas a equipos de un dominio se pueden predefinir características de seguridad para grupos específicos de usuarios.

4. IMPLEMENTACIÓN DEL PROCESO

4.1 FASE 1. RECOLECCIÓN DE INFORMACIÓN

En esta fase se recolectaron todas las medidas de seguridad informática que se evaluaban al momento de instalar un sistema operativo base para clientes o servidores, antes de iniciar con el aseguramiento, para esto se realizó un inventario de toda la infraestructura tecnológica con sistemas operativos Windows (Ver Anexo A. Hojas de vida Servidores Piloto).

Para iniciar con el levantamiento de la información correspondiente a mapeo de red, tipo de servicio de cada servidor, se reunió al área de infraestructura, para determinar los responsables de proporcionar esta información correspondiente a las configuraciones de seguridad en los diferentes equipos y poder hacer un boceto del posible escenario de pruebas en los que se realizara la configuración de las plantillas y se definirán los controles de cambios para el paso a producción.

Por medio de las hojas de vida realizadas (Ver Anexo A. Hojas de vida Servidores Piloto). Se identificaron servidores, configuraciones, roles, aplicaciones, conexiones físicas, software base y se validaron los servicios que proporciona cada servidor a la organizacion, la responsabilidad del profesional de infraestructura es realizar las configuraciones solicitadas a cada servidor, ya que él es el responsable de la infraestructura tecnológica.

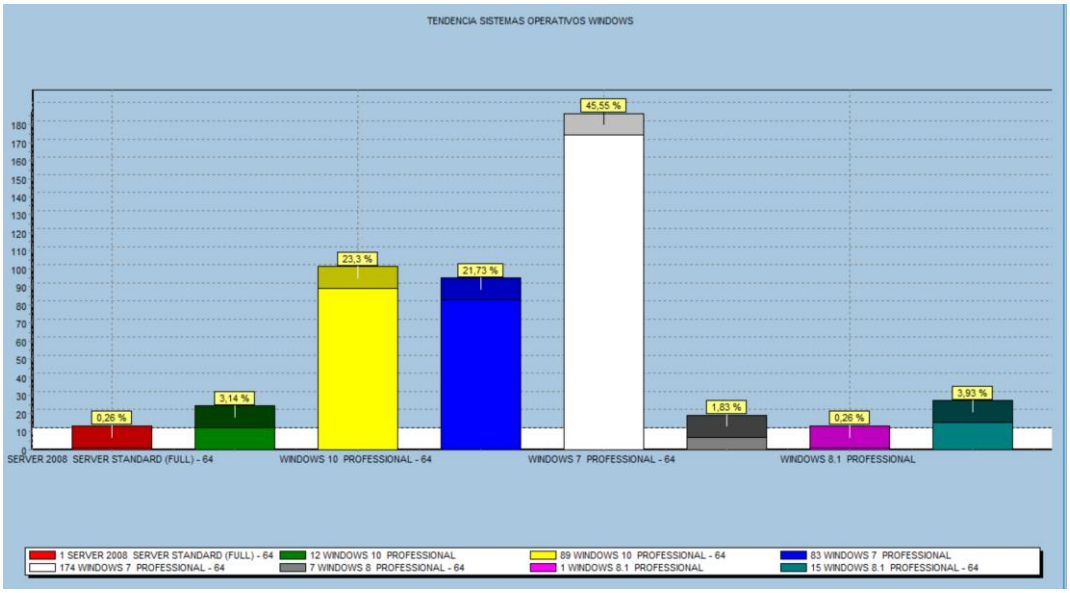
Por medio del levantamiento de información realizado, se documentaron los servidores que son expuestos directamente a Internet (servidores Web), la configuración en el firewall Checkpoint el cual se compone de reglas de acceso desde la red interna y hacia Internet, la administración del WSUS que es el Servidor de Actualizaciones de Windows Server (Ver Figura 17. WSUS) para considerar los parches de seguridad de Windows es responsabilidad del coordinador de soporte técnico quien es el encargado de aprobar y denegar las actualizaciones en las

estaciones de trabajo cliente, se tiene una solución de antivirus NOD el encargado de mantener actualizada la base de datos de la firma del antivirus, segmentar las redes para ambientes de desarrollo, pruebas y producción es el operador de infraestructura.

Como norma de seguridad se tiene una política de control de acceso los servidores, en una área protegida, por lo que la empresa cuenta con un centro de cómputo en condiciones adecuadas para el buen estado de los servidores y accesible sólo a personas autorizadas, existen cámaras de seguridad a la entrada y dentro del centro de cómputo, equipo biométrico que permitía el paso con la huella digital, clave o tarjeta magnética, además existía la política que los operadores de centro de cómputo llevan un registro de todo aquel que ingrese y salga del centro de cómputo.

Para recolectar los diferentes sistemas operativos cliente se realizó el levantamiento de información por medio de la herramienta de soporte técnico Aranda, en la cual se identificaron los diferentes sistemas operativos que soportan la operación de los colaboradores (Ver 14. Figura Sistemas Operativos).

Figura 14. Sistemas Operativos



Fuente: Herramienta Discovery

Para el control de algunas configuraciones de dominio de tiene habilitada la GPO por defecto y en la cual se parametrizaron las opciones básicas para el control de contraseña, cuentas de servicio, de habilitación de reproductor de Windows media, y algunas otras. (Ver Anexo B. Default Policy).

La empresa tiene establecido un procedimiento para paso a producción ,el cual es que primero debe existir un requerimiento o una necesidad , luego se asigna un gestor del cambio responsable de esta actividad en ambiente de controlado de desarrollo, luego se realizan un control de cambios pruebas con el requerimiento de infraestructura y es probado por el usuario solicitante y el gestor del cambio en ambiente de pruebas, una vez confirmado que está 100% funcional se presenta al comité de controles de cambios y si es aprobado se programa el paso a producción dependiendo los prerrequisitos solicitados.

Para esta fase especifica se utilizaron herramientas de Discovery de servidores para determinar los rangos de ip a los cuales de direccionaran las herramientas de análisis de vulnerabilidades, para ello se recurrió a la herramienta de Microsoft Baseline Security Analyzer Versión 2.3 para determinar el estado de los servidores en cuanto a parches de seguridad y vulnerabilidades de productos Microsoft (Ver Figura 15. Baseline).

Figura 15. Baseline

Fuente: Baseline

4.2 FASE 2. ANÁLISIS DE VULNERABILIDADES

El área de infraestructura realizo la asignación para el análisis de vulnerabilidades y aseguramiento de sistemas operativos 6 servidores virtuales de prueba en middleware Hyper V Microsoft con la siguiente configuración:

Tabla 1. Equipos Piloto Hardening

Servidor de Pruebas	Cantidad
Servidor SQL 2012 r2 2 virtual Core 24 Gb RAM	1
Servidor ad Windows server 2012 r2 1 virtual Core 8 Gb RAM	1
Servidor web Windows server 2012 1 virtual Core 8 Gb RAM	2
Servidor file Server Windows server 2012 1 virtual Core 8 Gb RAM	1
estación de trabajo Windows 7	1

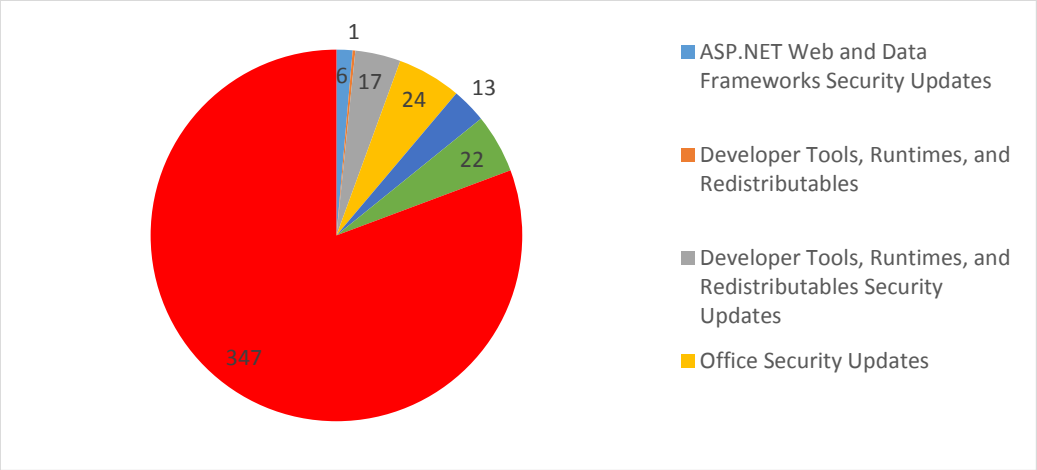
Luego del análisis realizado con la herramienta (Ver Figura 15. Baseline). Se realizó una separación de vulnerabilidades por criticidad y por tipo de producto, en las cuales se encontraron dentro de los servidores asignados por el área de infraestructura para realizar la parametrización las siguientes vulnerabilidades:

Tabla 2. Vulnerabilidades Críticas

Tipo vulnerabilidad	Actualizaciones
Asp.net web and data frameworks security updates	6
Developer tools, runtimes, and redistributables	1
Developer tools, runtimes, and redistributables security updates	17
Office security updates	24
Silverlight security updates	13
SQL server security updates	22
Windows security updates	347
Total, General	430

En la Figura 16. Vulnerabilidades Baseline se pueden identificar la cantidad de vulnerabilidades de parcheo de seguridad las cuales se tienen que tratar cola parametrización de la herramienta WSUS en el plan de trabajo de aseguramiento de sistemas operativos esta actividad se debe automatizar en las estaciones de trabajo.

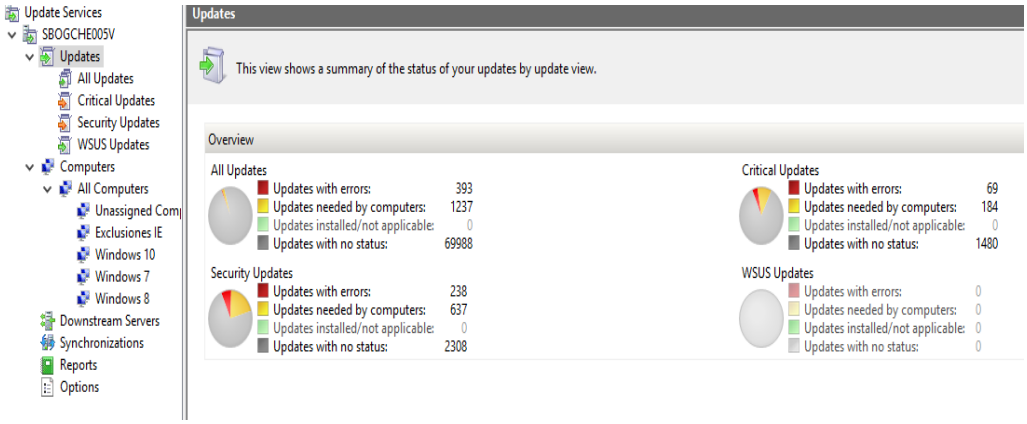
Figura 16. Vulnerabilidades Baseline



Fuente: Autor

Los controles de actualización de los equipos clientes se encuentra en total abandono, ya que de las 330 máquinas activas que reporta Discovery, en el WSUS solo reportan 231 de las cuales el 80% se encuentran sin gestión de despliegue de parches de seguridad (Ver Figura 17. WSUS).

Figura 17. WSUS

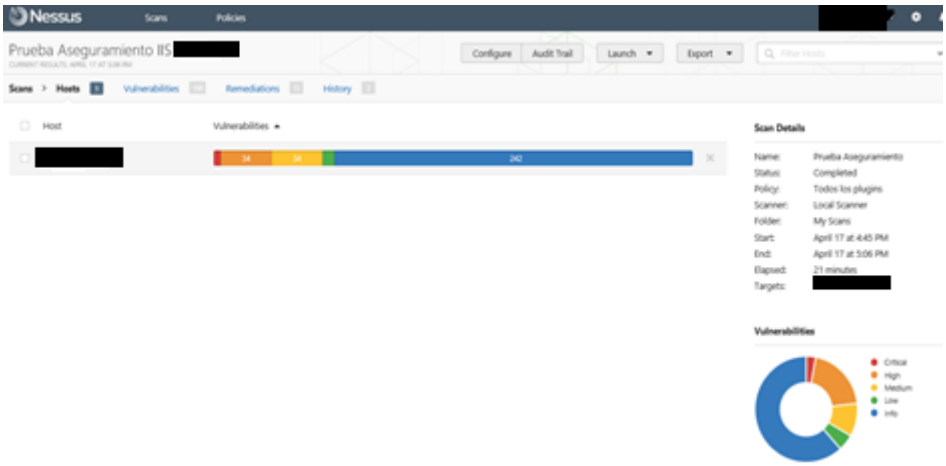


Fuente: Autor

Se realizó la descarga de las políticas default configuradas del controlador de dominio principal, para poder analizar la configuración y realizar la posterior parametrización de las guías de aseguramiento para ser enviadas por GPO (ver anexo B. Default Policy).

Por medio de la herramienta Nessus se realizó el análisis de servicios y vulnerabilidades de servidores para identificar la severidad y las acciones correctivas que mitigan el riesgo (Ver Anexo C. Informe Nessus).

Figura 18. Herramienta Nessus



Fuente: Autor

Esta herramienta proporciona un link de posibles soluciones proporcionado por la herramienta con un ID de plugin de tenable, también nos relaciona un grado de severidad que va desde el Informativo, medio, alto y crítico.

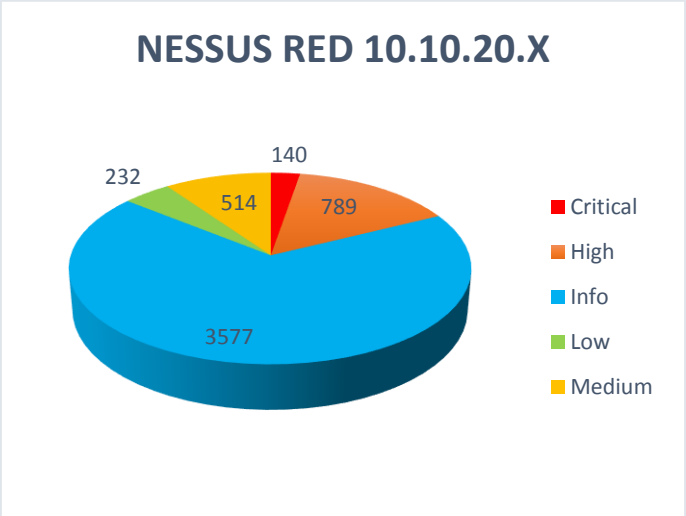
Por medio del análisis realizado logramos identificar sobre el segmento de red 10.10.20.x donde se encuentran los servidores de pruebas asignados para el piloto de Hardening, diversas vulnerabilidades entre las más significativas relacionamos parches críticos de seguridad proporcionados por Microsoft para deshabilitar el servicio SMB v1 y con el ello evitar la propagación de ransomware WannaCry los cuales se identifican por los boletines MS017-10 sobre los sistemas operativos cliente y servidores, deshabilitar servicios de SSL v1, v2, v3 y TLS 1.0 los cuales

son inseguros para cifrado de datos en ambientes web, service pack de productos Microsoft como SQL, Net Framework, Visual Studio etc.

El informe de análisis con la herramienta Nessus cuantifico las vulnerabilidades de acuerdo a su escala de nivel riesgo la cual se mide con sistema de puntuación CVSS (Common Vulnerability Scoring System).

El informe CVSS muestra vulnerabilidades dentro de cada uno de los diferentes rangos de puntuación CVSS (4,0 - 4,9, 5,0 a 5,9, 6,0 - 6,9, 7,0 a 7,9, 8,0 a 8,9, 9,0 - 9,9, y 10,0). Los colores para CVSS puntuaciones son de color naranja de gravedad Medium con una calificación de 4,0 - 6,9, rojo para los altos niveles High que tienen una calificación de 7,0 - 9,9, y la púrpura para severidades críticas con una calificación de 10.0.

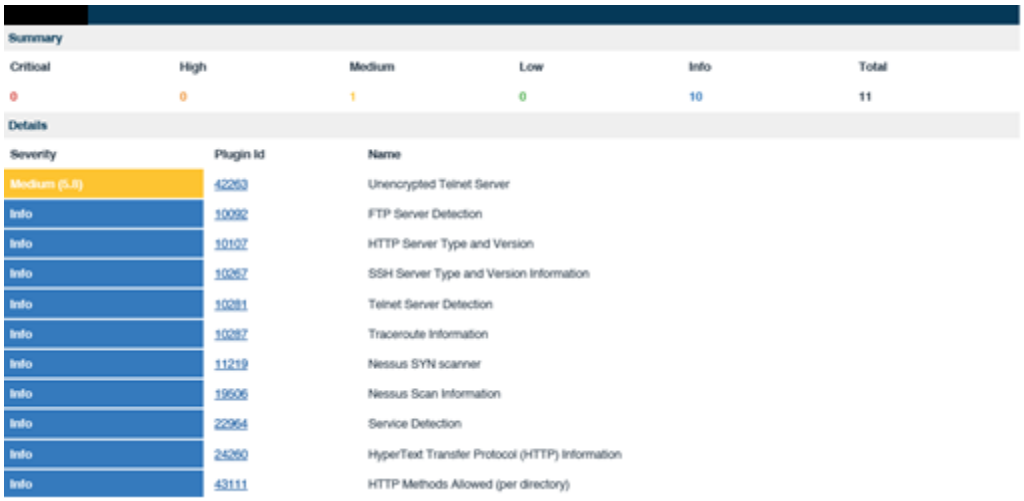
Figura 19. Nessus Red 10.10.20.x



Fuente: Autor

Dentro de la red Analizada 10.10.20.0/24 se identificaron 140 Critical, 789 High y 514 Medium (Ver Anexo C. Informe Nessus).

Figura 20. Informe Nessus



Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	10	11

Details

Severity	Plugin Id	Name
Medium (5.8)	42263	Unencrypted Telnet Server
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10267	SSH Server Type and Version Information
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	43111	HTTP Methods Allowed (per directory)

Fuente: Autor

La política default configurada dentro del controlador de dominio no tiene inferencia sobre los servidores de la organización, ya que dentro de la OU forzada, no hay ningún contenedor que incluya servidores por tal motivo no se pueden controlar las diferentes condiciones:

- No se tiene una GPO para el control de bloqueo y contraseñas de servidores.
- No se tiene una GPO para conexión con el WSUS
- No se tienen definidos Log de Eventos para acceso Satisfactorio y fallido
- No se tienen definidos Log de Elevación de Privilegios
- No se tienen parametrizadas cuentas de inicio de sesión como servicio

Ya con el análisis realizado a la infraestructura, ya se tienen una base de conocimiento para el inicio del aseguramiento de los sistemas operativos server y cliente, se realizará la configuración de las plantillas y su posterior implementación en los equipos de prueba asignados.

4.3 FASE 3. ASEGURAMIENTO DE SISTEMAS OPERATIVOS

Para la implementación de las plantillas de aseguramiento se definió un ID de control el cual está compuesto por numero entero en un rango del 1 al 5, un objetivo de control el cual es una descripción breve de la configuración, ubicación que es donde se va parametrizar el control dentro de la política y un valor para el componente DWORD dentro del REGEDIT.

Las plantillas de aseguramiento para sistemas de estaciones de trabajo (ver Anexo E. guía de aseguramiento Windows 7) son cinco y se componen de la siguiente manera:

- Eventos: dentro de esta configuración se relacionan el Log de eventos que se deben almacenar para una correcta trazabilidad de las acciones realizadas por los usuarios para temas de auditoria.

Figura 21. Anexo Plantilla Eventos W7

EVENTOS			
Control	**Objetivo de control**	**Ubicación**	**Valor**
1.1	Establecer 'Tamaño máximo del registro' - Aplicación	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application\Maximum Log Size (KB)	32768
1.2	Establecer 'Conservar eventos antiguos' - Aplicación	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application\Retain old events	Deshabilitado
1.3	Establecer 'Retener los eventos antiguos' - Seguridad	*Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Retain old events*	Deshabilitado
1.4	Establecer 'Tamaño máximo del registro' - Seguridad	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Maximum Log Size (KB)	81920
1.5	Establecer 'Tamaño máximo del registro' - Sistema	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System\Maximum Log Size (KB)	32768

Fuente: Autor

- Políticas de Usuario: Se establecen políticas de contraseña, cambio, longitud, reusó, cifrado bloqueo por intentos fallidos, bloqueo de estaciones de trabajo.

Figura 22. Anexo Plantilla Políticas de Usuario W7

POLITICAS DE USUARIO			
Control	**Objetivo de control**	**Ubicación**	**Valor**
2.1	Establecer 'Duración de bloqueo de cuenta'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration	0
2.2	Establecer 'Umbral de bloqueo de cuenta'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold	5
2.3	Establecer 'Restablecer contador de bloqueo de cuenta después de' a '15' o superior	*Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after*	30
2.4	Establecer 'Guardar contraseñas mediante cifrado reversible'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption	Deshabilitado
2.5	Establecer 'Longitud mínima de la contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length	8

Fuente: Autor

- Administración remota: Políticas de acceso por conexiones RDP seguras con autenticación de contraseñas.

Figura 23. Anexo Plantilla Administración Remota

ADMINISTRACION REMOTA			
Control	**Objetivo de control**	**Ubicación**	**Valor**
3.1	Establecer 'No permitir que las contraseñas se guarden'	Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client\Do not allow passwords to be saved	Habilitado
3.2	Establecer 'Asistencia remota solicitada'	Computer Configuration\Administrative Templates\System\Remote Assistance\Solicited Remote Assistance	Habilitado
3.3	Establecer 'Siempre pedir contraseña al conectar'	Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon	Habilitado

Fuente: Autor

- Opciones de seguridad: Configuración de servidor wsus, cuentas de para iniciar como servicio, inicio de sesión interactivo, limitación de cuentas locales, limpiezas de archivos de paginación memorias RAM, no almacenar contraseñas en el almacén de Windows.

Figura 24. Anexos Plantilla Opciones de seguridad W7

OPCIONES DE SEGURIDAD			
Control	Objetivo de control	Ubicación	Valor
4.1	Servidor WSUS de la organización	Computer Configuration\Administrative Templates\Windows Components\Windows Update\Specify intranet Microsoft update service location	http://10.10.19.2:8530
4.2	Establecer 'Enumerar cuentas de administrador'	Computer Configuration\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation	Deshabilitado
4.3	Establecer 'Restricciones para clientes RPC no autenticados'	Computer Configuration\Administrative Templates\System\Remote Procedure Call\Restrictions for Unauthenticated RPC clients	Habilitado, Autenticado

Fuente: Autor

- Norma de cumplimento PCI DSS: Normativa PCI para el uso de franquicias de tarjetas de crédito, restricciones de comandos Shell, acceso a panel de control, des habilitación de opciones avanzadas de directorios.

Figura 25. Anexo Plantilla PCI DSS W7

PCI DSS			
Control	Objetivo de control	Ubicación	Valor
5.1	Deshabilitar CMD	(gpedit.msc)Configuración de usuario > Plantillas administrativas > Sistema > Impedir el acceso al símbolo del sistema	Habilitada
5.2	Deshabilitar Recortes (Snipping Tool)	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Tablet PC > Accesorios > No permitir la ejecucion de Recortes	Habilitada
5.3	Deshabilitar opción de conectar y desconectar unidades de red	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Componentes de Windows > Explorador de Windows > Quitar "Conectar a unidad de red" y "Desconectar de unidad de red"	Habilitada
5.4	Deshabilitar cambios en el proxy	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Componentes de Windows > Internet Explorer > Deshabilitar el cambio de configuración de proxy	Habilitada
5.5	Deshabilitar el acceso al panel de control	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Panel de Control > Prohibir el acceso al Panel de Control	Habilitada

Fuente: Autor

Esta plantilla se configuro dentro de una política configurada con el nombre de Hardening7 dentro del controlador de dominio con Windows server 2012R2 en la OU de usuarios equipos, esto con la finalidad que solo sea forzada para estaciones de trabajo identificadas con sistemas operativo Windows 7, ya que dentro de ella se configuro la des habilitación del servicio SMBv1 este servicio es vulnerable a la propagación del ransomware wannacry el cual usa este servicio por el puerto 445 para propagarse en la red

Las plantillas de aseguramiento para sistemas de Windows server 2012 servidores (ver Anexo D. guía de aseguramiento servers Windows 2012 R2) son cuatro y se componen de la siguiente manera:

- Política de Cuentas: Se establecen políticas de contraseña, cambio, longitud, reusó, cifrado bloqueo por intentos fallidos, bloqueo de estaciones de trabajo.

Figura 26. Anexos Plantilla Políticas de Cuenta Server

POLITICAS DE CUENTA			
Control	Objetivo de control	Ubicación	Valor
1.1	Establecer 'Imponer historial de contraseñas'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history	8
1.2	Establecer 'Máxima edad de contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age	60
1.3	Establecer 'Edad mínima de la contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age	1
1.4	Establecer 'Longitud mínima de la contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length	8
1.5	Establecer contraseña debe cumplir con los requisitos de complejidad '	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements	Habilitado
1.6	Almacenar contraseñas con cifrado reversible	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption	Deshabilitado

Fuente: Autor

- Políticas Locales: Políticas de acceso locales a los servidores con autenticación de contraseñas locales y de dominio, cambios de atributos para Súper Usuarios, modificaciones a nivel de registro.

Figura 27. Anexos Plantilla Políticas Locales Server

POLITICAS LOCALES			
Control	Objetivo de control	Ubicación	Valor
2.1	determina qué cuentas de usuario puede modificar la etiqueta integridad de los objetos None	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label	None.
2.2	Establecer 'Copia de seguridad de archivos y directorios' en 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories	Administrators
2.3	Establezca 'Generar auditorías de seguridad' en 'Servicio local, Servicio de red'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits	Local Service, Network Service
2.4	Establecer 'Crear un archivo de paginación' en 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile	Administrators
2.5	Establezca 'Modificar valores de entorno de firmware' en 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values	Administrators
2.6	Establecer 'Bloqueo de la fuerza desde un sistema remoto' a 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system	Administrators

Fuente: Autor

- Auditoria: Se parametrizan los registros de seguimiento para obtener la trazabilidad de inicios de sesión, cambios de privilegios, políticas, inicio de servicios etc.

Figura 28. Anexo Plantillas Administración de Cuentas Server

ADMINISTRACION DE CUENTAS			
Control	Objetivo de control	Ubicación	Valor
4.1	Establezca 'Auditoría de administración de cuentas de equipo' en 'Satisfactoria y Fallida' (puntuación)	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Computer Account Management	Success and Failure
4.2	Establecer 'Gestión de grupo de seguridad de auditoría' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Security Group Management	Success and Failure
4.3	Establecer 'Auditoría de la gestión de cuentas de usuario' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: User Account Management	Success and Failure

Fuente: Autor

- Templates: Des habilitación de reproducción automática de medios, control de usuarios, Actualizaciones automáticas.

Figura 29. Anexo Plantillas Administración de Cuentas Server

ADMINISTRACION DE CUENTAS			
Control	Objetivo de control	Ubicación	Valor
5.3	Establecer 'Desactivar Reproducción automática' a 'Habilitado: Todas las unidades'	Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay\Turn off Autoplay	'Enabled:All drives'
5.4	*Establecer 'Instalar siempre con privilegios elevados' en 'Desactivado'*	User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges	*'Disabled'*
5.5	*Establecer 'Iniciar sesión en último usuario interactivo automáticamente después de un reinicio iniciado por el sistema' a 'Desactivado'*	Computer Configuration\Administrative Templates\Windows Components\Windows Logon Options\Sign-in last interactive user automatically after a system-initiated restart	*'Disabled'*
5.6	*Establecer 'Configurar actualizaciones automáticas' en 'Habilitado'*	Computer Configuration\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates	'Enabled'

Fuente: Autor

- Reconocimiento de equipos con WSUS.

  Se adjunta a la GPO de equipos inicio de sesión este script .bat para el reconocimiento o Discovery de equipos en la herramienta WSUS, con la finalidad de reducir las vulnerabilidades de parcheo de Windows, realizando un despliegue automático.

```
net stop wuauserv
reg Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v
PingID /f
reg Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v
AccountDomainSid /f
reg Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v
SusClientId /f
reg Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v
SusClientIDValidation /f
net start wuauserv
wuauclt.exe /resetauthorization /detectnow
pause
```

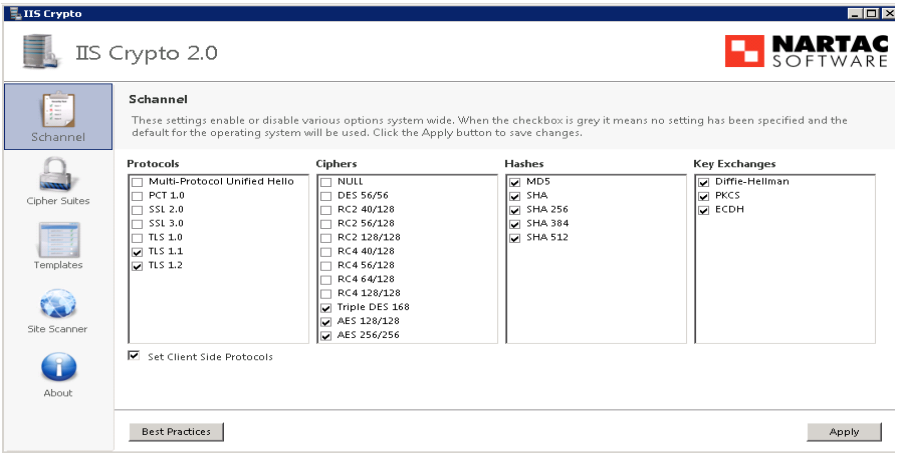
- Des habilitación de protocolos SSL V1, SSL V2, SSL V3, TLS 1.0

  El protocolo SSL y sus variantes, v2, v3, TLS ofrecen muchas combinaciones de protocolos de intercambio de claves, cifrado, etc. que han ido evolucionando en el tiempo para introducir mejoras y arreglar problemas de seguridad.

  La configuración predeterminada de IIS (y de cualquier servidor Web) estar predefinida para ser compatible para una amplia gama de clientes, pero esto deja abiertos protocolos obsoletos o inseguros.

  Para el cierre de estos protocolos por medio del REGEDIT se implementa la herramienta free IISCrypto, (Ver Figura 30. Software IIS Crypto) esta aplicación permite parametrizar las mejores prácticas de seguridad, deshabilitando el uso de protocolos inseguros.

Figura 30. Software IIS Crypto



Fuente: Autor

4.4 FASE 4. ANÁLISIS DE RESULTADOS

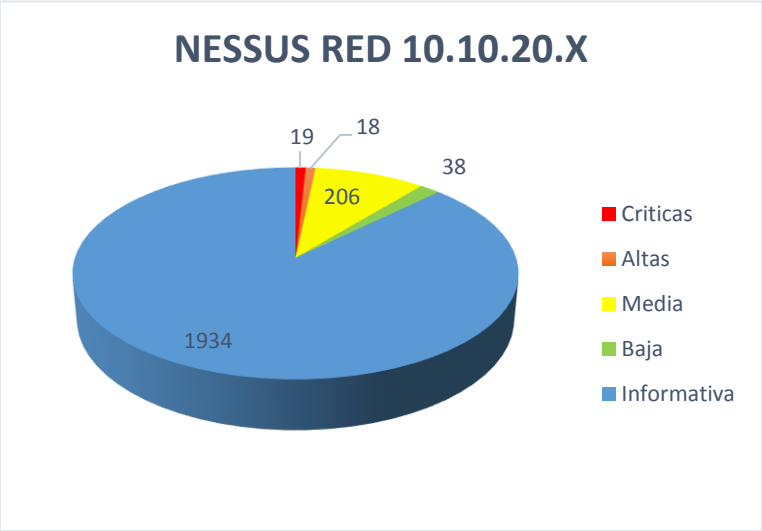
Para realizar el análisis comparativos entre la fase 2 y la fase de implementación del aseguramiento fase 3, fue necesaria la ejecución de las herramientas de análisis de vulnerabilidades sobre el segmento de red 10.10.20.x (ver Anexo F. Análisis de Vulnerabilidades 2), identificando una remediación del 87% respecto a la fase 2, en la cual se realizó el análisis inicial de la gestión de Vulnerabilidades previo a la implementación del proceso de Hardening a los equipos piloto proporcionados la organizacion.

Tabla 3. Fase 4 Análisis de Vulnerabilidades

RISK	CANTIDAD RISK
Criticas	19
Altas	18
Media	206
Baja	38
Informativa	1934

Por medio del grafico (Ver Figura 31. Fase 4 Análisis de Vulnerabilidades) se pueden observar una remediación significativa de vulnerabilidades respecto a las identificadas en la fase 2.

Figura 31. Fase 4 Análisis de Vulnerabilidades



Fuente: Autor

Las vulnerabilidades mitigadas en la fase 3 fueron cerradas, siguiendo las soluciones de remediación proporcionadas por los Plugin de Nessus los cuales brindan una respuesta documentada.

14 Vulnerabilidades fueron mitigadas con el despliegue de las actualizaciones automáticas e instalación de parches específicos reportados por la herramienta Baseline, esta herramienta utilizo el servicio de ejecución remota de código para analizar las instalaciones de actualizaciones de seguridad en los servidores conectados en la red de pruebas.

Figura 32. Vulnerabilidades Criticas Nessus red 10.10.20.x

Critical (10.0)	Critical	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	MS14-026
Critical (10.0)	Critical	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	MS14-057
Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection	
Critical (10.0)	Critical	MS13-067: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)	MS13-067
Critical (10.0)	Critical	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	MS14-026
Critical (10.0)	Critical	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	MS14-057
Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection	
Critical (10.0)	Critical	MS16-077: Security Update for WPAD (3165191)	MS16-077
Critical (10.0)	Critical	MS16-077: Security Update for WPAD (3165191)	MS16-077
Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection	
Critical (10.0)	Critical	MS13-067: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)	MS13-067
Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection	
Critical (10.0)	Critical	MS16-077: Security Update for WPAD (3165191)	MS16-077
Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection	

Fuente: Autor

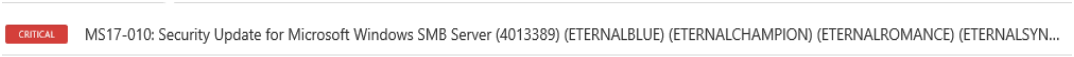
30 Vulnerabilidades fueron mitigadas con el reporte de la consola ESET NOD32, los equipos del segmento 10.10.20.x, no alcanzaban el segmento de red donde se encontraba el repositorio de actualizaciones y por este motivo no reportaban sus estados en la consola, se realizaron los cambios a nivel de red para la propagacion de la vlan de pruebas en las reglas del firewall que permiten esta conexión.

Figura 33. Vulnerabilidades Nod32

Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
Critical (10.0)	Critical	NOD32 Antivirus Detection and Status

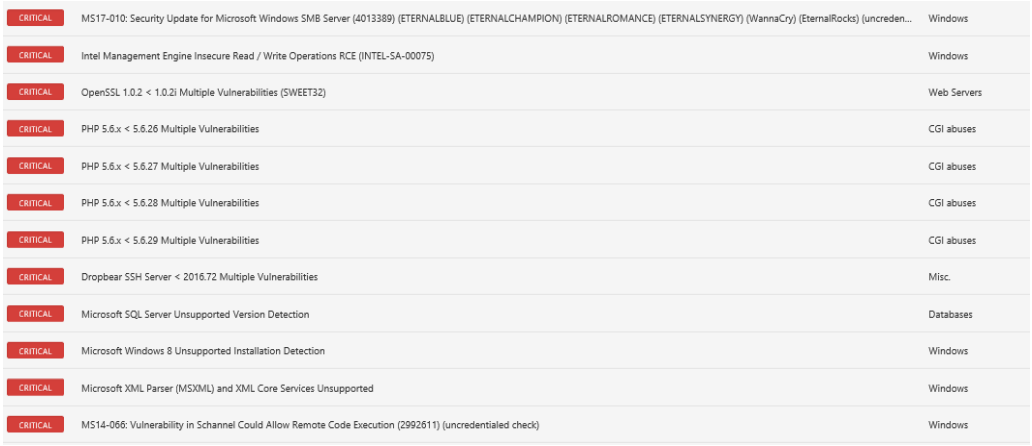
Fuente: Autor

A principios del mes de mayo Microsoft notifica la propagacion de un ransomware el cual utiliza una vulnerabilidad ya reportada en el boletin MS17-010 y se define un plan de accion inmediato de despliegue de actualizaciones por medio de la herramienta WSUS para clientes y despliegue manual para servidores incluyendo la vlan de pruebas donde se encuntran los equipos pilotos de Aseguramiento.



50 equipos no contaban con este parche especifico el cual deshabilita el servicio smb v1, encargado de la propagación de ransomware WannaCry, se realizó el despliegue del parche especifico por medio de la herramienta WSUS para equipos cliente.

Figura 34. Reporte Nessus MS17-010

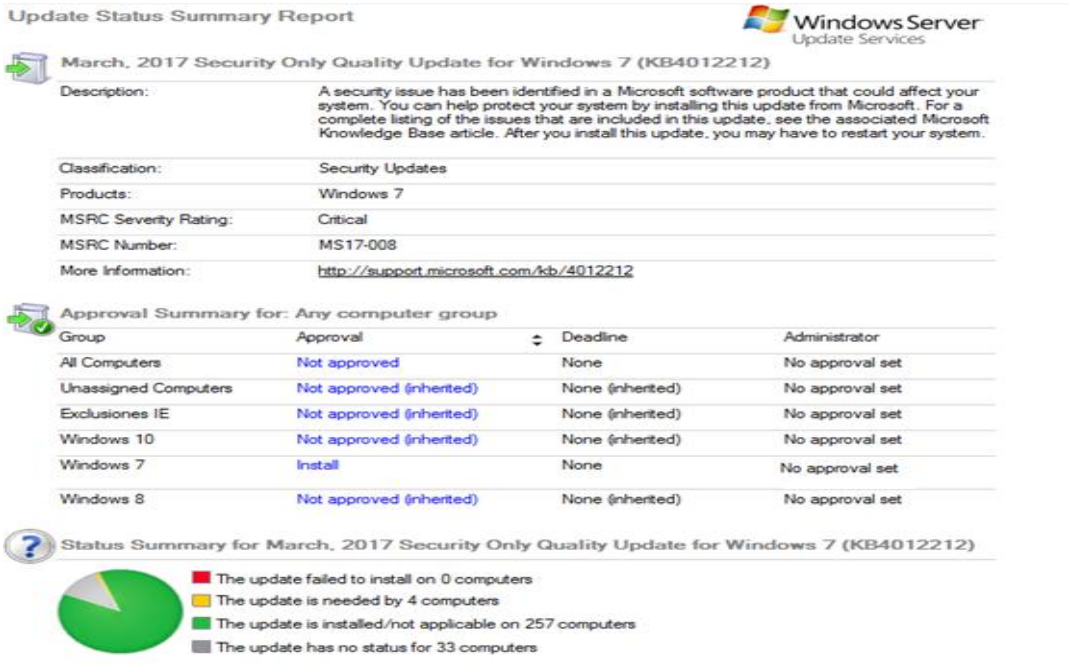


CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (uncreden...	Windows
CRITICAL	Intel Management Engine Insecure Read / Write Operations RCE (INTEL-SA-00075)	Windows
CRITICAL	OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32)	Web Servers
CRITICAL	PHP 5.6.x < 5.6.26 Multiple Vulnerabilities	CGI abuses
CRITICAL	PHP 5.6.x < 5.6.27 Multiple Vulnerabilities	CGI abuses
CRITICAL	PHP 5.6.x < 5.6.28 Multiple Vulnerabilities	CGI abuses
CRITICAL	PHP 5.6.x < 5.6.29 Multiple Vulnerabilities	CGI abuses
CRITICAL	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	Misc.
CRITICAL	Microsoft SQL Server Unsupported Version Detection	Databases
CRITICAL	Microsoft Windows 8 Unsupported Installation Detection	Windows
CRITICAL	Microsoft XML Parser (MSXML) and XML Core Services Unsupported	Windows
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Windows

Fuente: Autor

Se logró obtener un reporte de despliegue proporcionado por la herramienta WSUS del estado de actualización del equipo cliente de la organizacion, el cual indica el despliegue automático con aprobación, para la actualización de seguridad KB4012212 correspondiente al boletín MS17-010.

Figura 35. Reporte WSUS despliegue MS17-010



Fuente: Autor

15 Vulnerabilidades presentadas por Nessus para los servidores de pruebas fueron mitigadas utilizando las mejores prácticas del software IIS CRYTO (Ver Figura 30.

Software IIS Crypto), esta herramienta realiza los cambios en los registros de los servidores web expuestos, forzando su conexión web a trabajar sobre los protocolos seguros TLS v1.1, ya que las herramientas de análisis detectan como vulnerables los protocolos inferiores SSL 1, 2, 3.

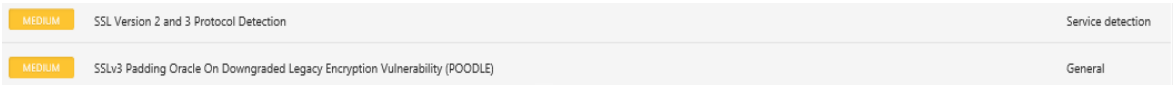
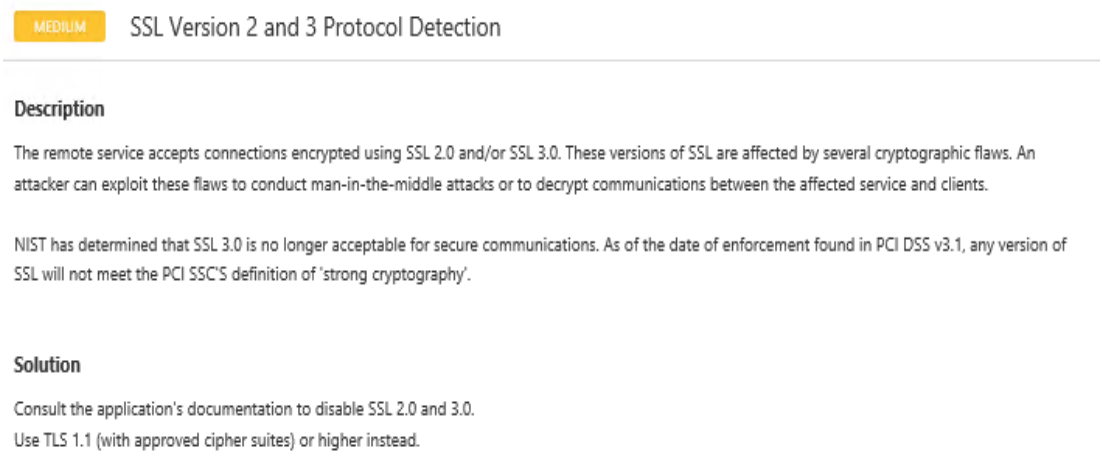


Figura 36. SSL Inseguro



Fuente: Autor

4.5 FASE 5. ANÁLISIS FINAL

A continuación, se presenta un resumen de los resultados obtenidos en las pruebas de aseguramiento de sistemas operativos. A modo general, se puede calificar el nivel de exposición en seguridad informática en un nivel Bajo el segmento de red para pruebas 10.10.20.x, teniendo en cuenta el riesgo que implicaban para la red interna las vulnerabilidades encontradas, el objetivo de esta actividad se concentró en mitigar las vulnerabilidades críticas con actividades puntuales de aseguramiento.

Los resultados de las pruebas se obtuvieron de la siguiente manera:

- Inicialmente, ser realizó un proceso de identificación de servicios, aplicaciones e infraestructura de Pruebas, así como la ejecución de múltiples herramientas de escaneo de vulnerabilidades. Por medio de un proceso de

fuerza bruta realizado por la herramienta Nessus, fue posible determinar vulnerabilidades críticas y obtener información sensible de fallas de seguridad de diferentes servicios.

- Fue posible acceder a la información de actualizaciones críticas de servidores por medio del servicio de ejecución remota de código la cual es una debilidad de instalación de sistemas operativos por default sin privilegios de administrador. De esta forma puede ser posible acceder a otros servicios, obtener información de usuarios válidos y finalmente, privilegios de administrador sobre el servidor.

- Luego, de la implementación de las plantillas de aseguramiento desplegadas desde la GPO del controlador de dominio, se logró configurar las estaciones de trabajo que hacían parte del segmento de red 10.10.20.x bajo la consigna del mínimo privilegio.

- Las aplicaciones web en los servidores de pruebas, se forzaron por medio del software IIS CRYPTO para que establezcan la comunicación por medio de protocolos seguros TLS 1.1 y 1.2, con lo que fue posible mitigar gran parte de las vulnerabilidades calificadas como Medium por Nessus.

- Se mitigaron las vulnerabilidades de uso del protocolo SMB v1 con el despliegue de actualizaciones para estaciones de trabajo desde el servidor WSUS.

- Se definió una GPO para el control automático de configuraciones default para servidores con sistema operativo Windows server 2012 R2, esto garantiza minimizar las debilidades al momento de instalar un servidor de manera automática.

El fortalecimiento de sistemas operativos por medio de plantillas de aseguramiento, garantiza que el proceso sea automatizado y controlado en diferentes plataformas,

para este caso específico, por medio del uso de las herramientas de despliegue de directivas de seguridad, se logró reducir de manera significativa las vulnerabilidades encontradas sobre el segmento de red donde se encontraban los sistemas operativos piloto proporcionados por la organización.

Esta metodología debe ser complementada, revisada y por medio de un control de cambios ejecutada con una periodicidad trimestral, con el objetivo de tener indicadores de gestión de vulnerabilidades y controlar todas estas amenazas que se encuentran sobre las plataformas de manera proactiva, controlando de manera inmediata las que cuenten con una calificación crítica y alta.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Con este proyecto de investigación se pudo establecer el impacto de no realizar una gestión adecuada de vulnerabilidades, en caso de materializar estas amenazas altas y criticas pueden llevar a la perdida de confidencialidad, integridad o disponibilidad de información de la organización, afiliados y clientes.

La gran mayoría de vulnerabilidades internas se encuentran asociadas a la actualización de aplicaciones, sistemas operativos y parches de seguridad que no han sido aplicados, también se encuentran aplicaciones y sistemas operativos sin soporte que representan un riesgo importante para la infraestructura de la organización.

En general se concluye que la organización está protegida frente a ataque básicos externos con acceso solamente a través de internet; sin embargo, un atacante con el tiempo suficiente para realizar la exploración y explotación de vulnerabilidades medias y avanzadas le permitirían comprometer la seguridad de la organización.

Un atacante interno puede llegar a generar una afectación grave para la organización, sin embargo, algunas de las vulnerabilidades identificadas como críticas fueron mitigadas en gran medida implementando herramientas de actualización y aseguramiento de sistemas operativos.

5.2 RECOMENDACIONES

Con base en los resultados obtenidos, se tienen las siguientes recomendaciones para mejorar el proceso de aseguramiento:

- Es necesario implementar una gestión de vulnerabilidades con una periodicidad no superior a 3 meses para tener un indicador de mitigación y una bitácora de seguimiento de incidentes de seguridad.
- Se deben priorizar los ajustes de parametrización de los sistemas operativos de otras plataformas, con el fin de corregir las configuraciones default de acuerdo a las plantillas de aseguramiento.
- Para el paso a producción de las plantillas de aseguramiento implementadas en los equipos piloto, se deben garantizar las pruebas totales de funcionalidad de las aplicaciones y documentar todos los cambios requeridos, para ser expuestos al comité de gestión del cambio y autorizar su despliegue en entornos productivos.

6. TRABAJOS FUTUROS

Cumpliendo con los alcances iniciales de implementación de un proceso de Hardening para sistemas operativos, se proponen las siguientes mejoras para ser ejecutadas en los próximos análisis de aseguramiento:

- Automatizar las actividades de parametrización y restricción de privilegios en estaciones de trabajo por medio de una directiva de grupo.
- Monitoreo de la gestión de vulnerabilidades por parte de una auditoria externa.
- Asegurar sistemas operativos de diferentes plataformas, de acuerdo a las mejores prácticas.
- Realizar el aseguramiento de los dispositivos de red y perimetrales para poder evaluar su nivel de seguridad.

7. REFERENCIAS BIBLIOGRÁFICAS

Proyecto de Seguridad Informática – UNAD trabajo de grado (http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3833/3/13483233.pdf)

Microsoft Free Security Tools – Microsoft Baseline Security Analyzer (https://blogs.technet.com/b/security/archive/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer.aspx)

Buenas prácticas de seguridad para servidores Windows – Microsoft Security Recomendaciones.
(www.atencion.ula.ve/documentacion/seguridad/recomendaciones_adm_windows.pdf)

Microsoft Windows Server 2008 R2 - Secure Your Windows Server: (http://technet.microsoft.com/en-us/magazine/hh987048.aspx)

Guía paso a paso de la opción de instalación Server Core - Windows Server 2008
(http://technet.microsoft.com/es-es/library/cc753802(v=ws.10).aspx)

Microsoft Free Security Tools – Microsoft Baseline Security Analyzer (https://blogs.technet.com/b/security/archive/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer.aspx)

Other Misc. Documentation Windows 2008R2 Server Hardening Checklist. https://wikis.utexas.edu/display/ISO/Windows+2008R2+Server+Hardening+Checklist

José F. Torres. Practicas básicas de de seguridad en Windows. 2da. Escuela Venezolana de Seguridad de Cómputo. Agosto 2006.
Universidad Autónoma de Madrid. Guía básica de seguridad para Windows.
http://www.uam.es/servicios/ti/servicios/ss/rec/winnt.html

Fingerprint – Definiciones Fingerprint en S.O Windows
http://www.gurudelainformatica.es/2009/11/herramienta-de-os-fingerprinting.html

Aseguramiento de Sistemas – Eset Aseguramiento de sistemas Operativos
www.welivesecurity.com/wp-content/.../buenas_practicas_seguridad_informatica.pdf

Seguridad en Microsoft Windows. Kit de recursos, Smith, Ben, McGrawHill/Interamericana de España

Mastering Windows Server 2008 R2. Server 2008 en versión R2, Mark Minasi, Editorial: Sybex

Diseño de un sistema de gestión de seguridad de información, Óptica ISO 27001:2005, Alberto G, Alexander, Editorial: ALFAOMEGA

8. ANEXOS

A. HOJAS DE VIDA SERVIDORES PILOTO.

	NOMBRE REGISTRO FICHA TÉCNICA SERVIDORES	
	CATEGORIA: SERVIDORES	Fecha de Modificación: 02-05-2017

HARDWARE	Descripción
Nombre del Servidor	[redacted]
Ubicación	[redacted]
Función	CONTROLADOR DOMINIO PRINCIPAL
Marca	HP
Modelo	G7
Serial	
Marca Procesador	INTEL XEON 8CORE
Modelo Procesador	E5640
Velocidad de procesador	2.67 Ghz
Memoria RAM	16Gb
Disco Duro	
Drive	
CD-ROM	SI
Tape Backup	
Tarjeta de Red	1 NIC VLAN 10
Otros periféricos	

			Licenciamiento	
SOFTWARE	Descripción	Versión	Licenciadas	Instaladas
Marca de sistema operativo	MICROSOFT			
Tipo de sistema operativo	WINDOWS SERVER	2008 R2 ESTÁNDAR		
Idioma de sistema operativo	Español			
Aplicaciones Instaladas	DIRECTORY ACTIVE	CATALOGO GLOBAL		

CONTIGENCIAS	Descripción
Arreglo de disco	RAID1
Mirror o espejo de disco	2 DD SAS 300GB
Conexión a UPS	SI
CARACTERÍSTICAS GENERALES	
Nombre de Dominio	PRUEBAS
No de usuarios actuales	
No de usuarios potenciales	
Dirección IP Pública	10.10.20.2
Dirección IP Privada	
Service Pack y/o parches	
Protocolos instalados	
Política de Backup	[redacted]

ATP-S

	NOMBRE REGISTRO FICHA TÉCNICA SERVIDORES	
	CATEGORIA: SERVIDORES I	Fecha de Modificación: 02-05-2017

HARDWARE	Descripción
Nombre del Servidor	[redacted]FP002F
Ubicación	[redacted]
Función	CONTROLADOR DOMINIO SEGUNDARIO
Marca	DELL
Modelo	PowerEdge R710
Serial	
Marca Procesador	INTEL XEON | INTEL XEON 16CORE
Modelo Procesador	E5620 | E5620
Velocidad de procesador	2.4 Ghz | 2.4 Ghz
Memoria RAM	8 Gb
Disco Duro	C: 146 Gb
Drive	
CD-ROM	SI
Tape Backup	
Tarjeta de Red	1 NIC
Otros periféricos	

			Licenciamiento	
SOFTWARE	Descripción	Versión	Licenciadas	Instaladas
Marca de sistema operativo	MICROSOFT			
Tipo de sistema operativo	WINDOWS SERVER	2008 R2 Enterprise		
Idioma de sistema operativo	INGLES			
Aplicaciones Instaladas	DIRECTORY ACTIVE	CATALOGO GLOBAL		

CONTIGENCIAS	Descripción
Arreglo de disco	RAID1 | RAID5
Mirror o espejo de disco	2 DD SAS 146GB | 4 DD 146 GB
Conexión a UPS	SI
CARACTERISTICAS GENERALES	
Nombre de Dominio	PRUEBAS
No de usuarios actuales	
No de usuarios potenciales	
Dirección IP Pública	10.10.20.25
Dirección IP Privada	
Service Pack y/o parches	

	NOMBRE REGISTRO FICHA TÉCNICA SERVIDORES	
	CATEGORIA: SERVIDORES	Fecha de Modificación: 02-05-2017

HARDWARE	Descripción
Nombre del Servidor	[redacted]
Ubicación	[redacted]
Función	BACKUP
Marca	HP
Modelo	G7
Serial	
Marca Procesador	INTEL XEON 8CORE
Modelo Procesador	E5640
Velocidad de procesador	2,67 Ghz
Memoria RAM	16 Gb
Disco Duro	C: 146GB | E: 560 GB
Drive	
CD-ROM	SI
Tape Backup	
Tarjeta de Red	1 NIC VLAN 10 | 1 NIC SAN
Otros periféricos	TARJETA FIBRE CHANNEL A LIBRERIA
	CONEXIÓN SERIAL PBX

			Licenciamiento	
SOFTWARE	Descripción	Versión	Licenciadas	Instaladas
Marca de sistema operativo	MICROSOFT			
Tipo de sistema operativo	WINDOWS SERVER	2008 R2 ESTANDAR		
Idioma de sistema operativo	Ingles			
Aplicaciones instaladas	[redacted]	15		
	[redacted]	15		
	TFTP			
	UCENCIAS TELNET PRO			
	[redacted]			

CONTIGENCIAS	Descripción
Arreglo de disco	RAID1 | RAID 5
Mirror o espejo de disco	2 DD SAS 146GB | 4 DD SAS 300GB
Conexión a UPS	SI
CARACTERISTICAS GENERALES	
Nombre de Dominio	PRUEBAS
No de usuarios actuales	
No de usuarios potenciales	

	NOMBRE REGISTRO FICHA TÉCNICA SERVIDORES	
	CATEGORIA: SERVIDORES	Fecha de Modificación: 02-05-2017

HARDWARE	Descripción
Nombre del Servidor	[redacted]
Ubicación	
Función	INTRANET
Marca	HP
Modelo	G7
Serial	
Marca Procesador	INTEL XEON 8 CORE
Modelo Procesador	E5640
Velocidad de procesador	2.67 Ghz
Memoria RAM	16 Gb
Disco Duro	C: 70GB D: 230GB
Drive	
CD-ROM	SI
Tape Backup	
Tarjeta de Red	1 NIC VLAN 2
Otros periféricos	

SOFTWARE	Descripción	Versión	Licenciamiento Licenciadas	 Instaladas
Marca de sistema operativo	MICROSOFT	64BITS		
Tipo de sistema operativo	WINDOWS SERVER	2008 R2 ESTANDAR		
Idioma de sistema operativo	[redacted]			
Aplicaciones instaladas		2010		
	IIS PUBLICACIONES			
	TAREAS PROGRAMADAS			

GoogleUpdateTaskMachineC...	Ready	Multiple triggers defined
GoogleUpdateTaskMachineUA	Ready	At 05:09 p.m. every day - After triggered, repeat every 1 hou
User_Feed_Synchronization-...	Ready	At 04:00 p.m. every day - Trigger expires at 16/08/2026 04:0
User_Feed_Synchronization-...	Ready	At 09:40 a.m. every day - Trigger expires at 08/09/2023 09:4
User_Feed_Synchronization-...	Ready	At 06:51 p.m. every day - Trigger expires at 17/04/2022 06:5

CONTIGENCIAS	Descripción
Anegio de disco	RAID1 1
Mirror o espejo de disco	2 DD SAS 300GB
Conexión a UPS	SI
CARACTERISTICAS GENERALES	
Nombre de Dominio	PRUEBAS
No de usuarios activos	

	NOMBRE REGISTRO	
	FICHA TÉCNICA SERVIDORES	
	CATEGORIA: SERVIDORES	Fecha de Modificación: 02-05-2017

HARDWARE	Descripción
Nombre del Servidor	[redacted]
Ubicación	[redacted]
Función	PRUEBA FTP
Marca	HP
Modelo	G7
Serial	
Marca Procesador	INTEL XEON 6 CORES | 2 PROCESADORES
Modelo Procesador	X5670
Velocidad de procesador	2.93 Ghz
Memoria RAM	24 Gb
Disco Duro	C:146GB | D: 146GB
Drive	
CD-ROM	SI
Tape Backup	
Tarjeta de Red	1 NIC VLAN 10
Otros periféricos	

			Licenciamiento	
SOFTWARE	Descripción	Versión	Licenciadas	Instaladas
Marca de sistema operativo	MICROSOFT	64BITS		
Tipo de sistema operativo	WINDOWS SERVER	2008 R2 ESTÁNDAR		
Idioma de sistema operativo	Inglés			
Aplicaciones instaladas	FTP	BANCOS		
	[redacted]			
	[redacted]			
	[redacted]			
	[redacted]			
	IIS			
	TAREAS PROGRAMADAS			
CONTIGENCIAS	Descripción			

	NOMBRE REGISTRO FICHA TÉCNICA SERVIDORES	
	CATEGORIA: SERVIDORE!	Fecha de Modificación: 02-05-2017

HARDWARE	Descripción
Nombre del Servidor	[redacted]
Ubicación	[redacted]
Función	
Marca	HP
Modelo	G7
Serial	
Marca Procesador	INTEL XEON 6 CORES | 2 PROCESADORES
Modelo Procesador	X5690
Velocidad de procesador	3.47 Ghz
Memoria RAM	32 Gb
Disco Duro	C: 146 Gb | D: 146 Gb | E: 146 Gb
Drive	
CD-ROM	SI
Tape Backup	
Tarjeta de Red	1 NIC VLAN 10
Otros periféricos	

			Licenciamiento	
SOFTWARE	Descripción	Versión	Licenciadas	Instaladas
Marca de sistema operativo	MICROSOFT	64BITS		
Tipo de sistema operativo	WINDOWS SERVER	2008 R2 ESTANDAR		
Idioma de sistema operativo	Inglés			
Aplicaciones instaladas	[redacted]	2008 R2		
		v12 x64		
	:			

CONTIGENCIAS	Descripción
Arreglo de disco	RAID1 | RAID1 | RAID1
Mirror o espejo de disco	2 DD SAS 146GB | 2 DD SAS 146GB | 2 DD SAS 146GB
Conexión a UPS	SI
CARACTERISTICAS GENERALES	
Nombre de Dominio	PRUEBA
No de usuarios actuales	
No de usuarios potenciales	
Dirección IP Pública	10.10.20.85
Dirección IP Privada	
Service Pack y/o parches	

	NOMBRE REGISTRO FICHA TÉCNICA SERVIDORES	
	CATEGORIA: SERVIDORES I	Fecha de Modificación: 02-05-2017

HARDWARE	Descripción
Nombre del Servidor	[redacted]
Ubicación	
Función	SERVIDOR DE CORREO
Marca	HP
Modelo	G7
Serial	
Marca Procesador	INTEL XEON 12 CORES | 2 PROCESADORES
Modelo Procesador	X5670
Velocidad de procesador	2,93 Ghz
Memoria RAM	32 Gb
Disco Duro	C: 146 Gb |
Drive	
CD-ROM	[redacted]
Tape Backup	
Tarjeta de Red	10G
Otros periféricos	Lun[redacted] E: 450GB RECOVERY
	Lun[redacted] F: 80GB LOGS
	Lun[redacted] G:500GB

SOFTWARE	Descripción	Versión	Licenciamiento Licenciadas	Licenciamiento Instaladas
Marca de sistema operativo	MICROSOFT	64BITS		
Tipo de sistema operativo	WINDOWS SERVER	2008 R2 ESTANDAR		
Idioma de sistema operativo	Ingles			
Aplicaciones instaladas	[redacted]	2010		

CONTIGENCIAS	Descripción
Arreglo de disco	RAID1 |
Mirror o espejo de disco	2 DD SAS 300GB |
Conexión a UPS	SI
CARACTERISTICAS GENERALES	
Nombre de Dominio	PRUEBA
No de usuarios actuales	
No de usuarios potenciales	
Dirección IP Pública	10.10.30.19
Dirección IP Privada	
Service Pack y/o parches	

B. POLÍTICAS DEFAULT.

Default Domain Policy

Data collected on: 3/16/2017 3:33:08

General

Details

Domain	
Owner	
Created	10/23/2006 1:01:04 PM
Modified	11/22/2016 6:03:50 PM
User Revisions	178 (AD), 178 (SYSVOL)
Computer Revisions	270 (AD), 270 (SYSVOL)
Unique ID	{31B2F340-016D-11D2-945F-00C04FB984F9}
GPO Status	Enabled

Links

Location	Enforced	Link Status	Path
	No	Enabled	

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
	Edit settings, delete, modify security	No
	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	12 passwords remembered
Maximum password age	30 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	0 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure

C. INFORME NESSUS.

Plugin Id	Host	Severity	Risk	Name	Update
73985	10.10.20.3	Critical (10.0)	Critical	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	MS14-026
78432	10.10.20.3	Critical (10.0)	Critical	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	MS14-057
96982	10.10.20.3	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.4	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
23910	10.10.20.4	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)	
62758	10.10.20.4	Critical (10.0)	Critical	Microsoft XML Parser (MSXML) and XML Core Services Unsupported	
96982	10.10.20.4	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.5	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
23910	10.10.20.5	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)	
64784	10.10.20.5	Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection	
69827	10.10.20.5	Critical (10.0)	Critical	MS13-067: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)	MS13-067
96982	10.10.20.5	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
96982	10.10.20.7	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
96982	10.10.20.8	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
96982	10.10.20.9	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
73985	10.10.20.10	Critical (10.0)	Critical	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)	MS14-026
78432	10.10.20.10	Critical (10.0)	Critical	MS14-057: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)	MS14-057
96982	10.10.20.10	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.11	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
96982	10.10.20.11	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.12	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
48987	10.10.20.12	Critical (10.0)	Critical	PHP Unsupported Version Detection	
96982	10.10.20.12	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.13	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
64784	10.10.20.13	Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection	
96982	10.10.20.13	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.14	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
96982	10.10.20.14	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.34	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
62758	10.10.20.34	Critical (10.0)	Critical	Microsoft XML Parser (MSXML) and XML Core Services Unsupported	
96982	10.10.20.34	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
23910	10.10.20.35	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)	
96982	10.10.20.35	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.37	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
23910	10.10.20.37	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)	
91600	10.10.20.37	Critical (10.0)	Critical	MS16-077: Security Update for WPAD (3165191)	MS16-077
96982	10.10.20.37	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.38	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
23910	10.10.20.38	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)	
62758	10.10.20.38	Critical (10.0)	Critical	Microsoft XML Parser (MSXML) and XML Core Services Unsupported	
96982	10.10.20.38	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.39	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
23910	10.10.20.39	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)	
96982	10.10.20.39	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.40	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
62758	10.10.20.40	Critical (10.0)	Critical	Microsoft XML Parser (MSXML) and XML Core Services Unsupported	
84874	10.10.20.40	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (July 2015 CPU) (Bar Mitzvah)	
86742	10.10.20.40	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (October 2015 CPU)	
88045	10.10.20.40	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (January 2016 CPU) (SLOTH)	
91600	10.10.20.40	Critical (10.0)	Critical	MS16-077: Security Update for WPAD (3165191)	MS16-077
92516	10.10.20.40	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (July 2016 CPU)	
96982	10.10.20.40	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.41	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
96982	10.10.20.41	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
96982	10.10.20.42	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.44	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
64784	10.10.20.44	Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection	
96982	10.10.20.44	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	
21608	10.10.20.45	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status	
96982	10.10.20.45	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)	

96982	10.10.20.56	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.57	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
64784	10.10.20.57	Critical (10.0)	Critical	Microsoft SQL Server Unsupported Version Detection
96982	10.10.20.57	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
84729	10.10.20.66	Critical (10.0)	Critical	Microsoft Windows Server 2003 Unsupported Installation Detection
96982	10.10.20.66	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
84729	10.10.20.67	Critical (10.0)	Critical	Microsoft Windows Server 2003 Unsupported Installation Detection
96982	10.10.20.67	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
84729	10.10.20.68	Critical (10.0)	Critical	Microsoft Windows Server 2003 Unsupported Installation Detection
96982	10.10.20.68	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.73	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.73	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
35466	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU) (BEAST)
57939	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)
59462	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)
62593	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (October 2012 CPU)
62738	10.10.20.73	Critical (10.0)	Critical	Microsoft XML Parser (MSXML) and XML Core Services Unsupported
64434	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (February 2013 CPU)
64790	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (February 2013 CPU Update 1)
65995	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (April 2013 CPU)
66932	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (June 2013 CPU)
70472	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (October 2013 CPU)
71966	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (January 2014 CPU)
73570	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (April 2014 CPU)
76432	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (July 2014 CPU)
78481	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (October 2014 CPU)
80608	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (January 2015 CPU) (POODLE)
82820	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (April 2015 CPU) (FREAK)
84824	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (July 2015 CPU) (Bar Mitzvah)
86742	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (October 2015 CPU)
88045	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (January 2016 CPU) (SLOTH)
92516	10.10.20.73	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (July 2016 CPU)
96982	10.10.20.73	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.74	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.74	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
96982	10.10.20.74	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.75	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.75	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
96982	10.10.20.75	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.76	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.76	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
96982	10.10.20.76	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.77	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.77	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
96982	10.10.20.77	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.78	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.78	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
96982	10.10.20.78	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.79	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.79	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
96982	10.10.20.79	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.80	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.80	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
96982	10.10.20.80	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)
21608	10.10.20.81	Critical (10.0)	Critical	NOD32 Antivirus Detection and Status
23910	10.10.20.81	Critical (10.0)	Critical	Compromised Windows System (hosts File Check)
84824	10.10.20.81	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (July 2015 CPU) (Bar Mitzvah)
86742	10.10.20.81	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (October 2015 CPU)
88045	10.10.20.81	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (January 2016 CPU) (SLOTH)
92516	10.10.20.81	Critical (10.0)	Critical	Oracle Java SE Multiple Vulnerabilities (July 2016 CPU)
96982	10.10.20.81	Critical (10.0)	Critical	Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check)

D. GUÍA DE ASEGURAMIENTO SERVERS WINDOWS 2012 R2

POLITICAS DE CUENTA			
Control	Objetivo de control	Ubicación	Valor
1.1	Establecer 'Imponer historial de contraseñas'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history	8
1.2	Establecer 'Máxima edad de contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age	60
1.3	Establecer 'Edad mínima de la contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age	1
1.4	Establecer 'Longitud mínima de la contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length	8
1.5	Establecer contraseña debe cumplir con los requisitos de complejidad '	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements	Habilitado
1.6	Almacenar contraseñas con cifrado reversible	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption	Deshabilitado
1.7	Duracion de bloqueo de la cuenta	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration	60
1.8	Umbral de bloqueo de cuenta	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold	3
1.9	Restablecer contador de bloqueo de cuenta después de	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after	0

POLITICAS LOCALES			
Control	**Objetivo de control**	**Ubicación**	**Valor**
2.1	determina qué cuentas de usuario puede modificar la etiqueta integridad de los objetos None	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label	None.
2.2	Establecer 'Copia de seguridad de archivos y directorios' en 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories	Administrators
2.3	Establezca 'Generar auditorías de seguridad' en 'Servicio local, Servicio de red'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits	Local Service, Network Service
2.4	Establecer 'Crear un archivo de paginación' en 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile	Administrators
2.5	Establezca 'Modificar valores de entorno de firmware' en 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values	Administrators
2.6	Establecer 'Bloqueo de la fuerza desde un sistema remoto' a 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system	Administrators
2.7	Establecer 'Acceso a este equipo desde la red' a 'Administradores, Usuarios autenticados,	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network	Administrators, Authenticated Users, ENTERPRISE DOMAIN

	CONTROLADORES DE DOMINIO DE EMPRESA'		CONTROLLERS.
2.8	Establecer 'Permitir el inicio de sesión a través de Servicios de Escritorio remoto' en 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services	Administrators
2.9	Establezca 'Cambiar la hora del sistema' en 'LOCAL SERVICE, Administrators'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time	LOCAL SERVICE, Administrators.
2.10	Establecer 'Habilitar las cuentas de equipo y de usuario que se deben confiar para la delegación' a 'None	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable computer and user accounts to be trusted for delegation	None.
2.11	Establecer 'Bloquear páginas en la memoria' a 'None'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory	None.
2.12	Establecer 'Agregar estaciones de trabajo al dominio' a 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Add workstations to domain	Administrators
2.13	Establecer 'Denegar el acceso a este equipo desde la red' a 'Invitados'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network	Guests
2.14	Establezca 'Reemplazar un token de nivel de proceso' en 'Servicio local, servicio de red'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token	Local Service, Network Service
2.15	Establecer 'Denegar inicio de sesión como un trabajo por lotes' a 'Invitados'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job	Guests
2.16	Establecer 'Apagar el sistema' a 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system	Administrators
2.17	Establecer 'Permitir inicio de sesión local' a 'Administradores'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally	Administrators
2.18	Establecer 'Seguridad de red: permitir que el sistema local utilice identidad de equipo para NTLM' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM	Habilitado

2.19	Establecer 'Consola de recuperación: Permitir copia de disquete y acceso a todas las unidades y todas las carpetas' a 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Recovery console: Allow floppy copy and access to all drives and all folders	Deshabilitado
2.20	Establecer 'Seguridad de red: Permitir la suspensión de la sesión NULL de LocalSystem' a 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback	Deshabilitado
2.21	Establecer 'Cuentas: Estado de cuenta de invitado' en 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status	Deshabilitado
2.23	Establecer 'Control de cuentas de usuario: Comportamiento del mensaje de elevación para administradores en Modo de aprobación de administrador' en 'Solicitar consentimiento en el escritorio seguro' (puntuación) '	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop' (Scored)
2.24	Configuracion de Dispositivos: Permitido formatear y expulsar medios extraíbles' a 'Administrators'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media	Administrators
2.26	Establecer 'Controlador de dominio: rechazar la contraseña de la cuenta de la máquina' en 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Refuse machine account password changes	Deshabilitado
2.27	Establecer 'Control de cuentas de usuario: Ejecutar todos los administradores en modo de aprobación de administrador' a 'Activado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode	Habilitado
2.28	Establecer 'Controlador de dominio: Permitir que los operadores de servidor programar tareas' en 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Allow server operators to schedule tasks	Deshabilitado
2.29	Establecer 'Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta de administrador incorporada' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account	Habilitado
2.30	Establecer 'Seguridad de red: Permitir que las solicitudes de autenticación PKU2U a este equipo	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication	Deshabilitado

	utilicen identidades en línea' en 'Desactivado'	requests to this computer to use online identities	
2.31	Establecer 'Objetos del sistema: Requiere insensibilidad de mayúsculas y minúsculas para subsistemas no Windows' a 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Require case insensitivity for non-Windows subsystems	Habilitado
2.33	Establecer 'Consola de recuperación: Permitir inicio de sesión administrativo automático' a 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Recovery console: Allow automatic administrative logon	Deshabilitado
2.34	Establecer 'Seguridad de red: Forzar el cierre de sesión cuando las horas de inicio de sesión caduquen' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Force logoff when logon hours expire	Habilitado
2.36	Defina 'Miembro del dominio: deshabilitar los cambios de contraseña de la cuenta del equipo' en 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes	Deshabilitado
2.37	Conjunto 'Miembro del dominio: cifra digitalmente los datos de canal seguro (' cuando ')' a 'Activado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)	Habilitado
2.38	Establecer 'Acceso a la red: Permitir SID anónimo / Traducción de nombres' a 'Desactivado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation	Deshabilitado
2.39	Set 'Miembro del dominio: Cifrar o firmar datos de canal seguro (siempre)' a 'Habilitar	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)	Habilitado
2.40	Establecer 'Servidor de red de Microsoft: Firmar digitalmente las comunicaciones (si el cliente acepta)' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)	Habilitado
2.41	Set 'Seguridad de red: Seguridad de sesión mínima para servidores NTLM basados en SSP (incluidos RPC seguros)' a 'Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security,Require 128-bit encryption

2.42	Establecer 'Acceso a la red: modelo de compartición y seguridad para cuentas locales' en 'Clásico - los usuarios locales se autentican como si mismos'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves
2.43	Establecer 'Control de cuentas de usuario: permite que las aplicaciones de UIAccess solicite elevación sin usar el escritorio seguro'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Deshabilitado
2.44	Conjunto de cuentas: Limitar el uso de cuentas locales en blanco para el inicio de sesión de la consola sólo a Activado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Limit local account use of blank passwords to console logon only	Habilitado
2.45	Establecer 'servidor de red Microsoft: Firmar digitalmente las comunicaciones (siempre)' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)	Habilitado
2.46	Set 'Miembro del dominio: Máxima contraseña de la cuenta de la máquina'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age	60
2.47	Establecer 'Acceso a la red: Restringir el acceso anónimo a Canalizaciones y Acciones con nombre' a 'Activado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares	Habilitado
2.48	Establecer 'Control de cuentas de usuario: Cambiar al escritorio seguro al solicitar la elevación' a 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation	Habilitado
2.50	Set 'Miembro del dominio: Firmar digitalmente los datos del canal seguro (cuando sea posible)' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (when possible)	Habilitado
2.51	Establecer 'Cliente de red de Microsoft: Enviar contraseña no cifrada a servidores SMB de terceros' a 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers	Deshabilitado
2.52	Establecer 'Objetos del sistema: Refuerza los permisos predeterminados de objetos internos del sistema (por ejemplo, enlaces simbólicos)' a 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Habilitado

2.53	Establecer 'Acceso a la red: no permitir enumeración anónima de cuentas y recursos compartidos de SAM' a 'Activado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares	Habilitado
2.54	Establecer 'Control de cuentas de usuario: Virtualizar errores de escritura de archivos y registros en ubicaciones por usuario' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations	Habilitado
2.55	Establezca 'Inicio de sesión interactivo: Comportamiento de eliminación de tarjetas inteligentes' en 'Bloquear estación de trabajo'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior	Lock Workstation
2.57	Establecer 'Inicio de sesión interactivo: no requieren CTRL + ALT + SUPR' a 'Desactivado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL	Deshabilitado
2.58	Establecer dispositivos: evitar que los usuarios instalen los controladores de impresora 'en' Habilitado '	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers	Habilitado
2.60	Establecer 'MSS: (AutoAdminLogon) Habilitar inicio de sesión automático (no recomendado)' a 'Desactivado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Deshabilitado
2.61	Establecer 'Cliente de red de Microsoft: Firmar digitalmente las comunicaciones (siempre)' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)	Habilitado
2.62	Establecer 'Acceso a la red: no permitir enumeración anónima de cuentas SAM' a 'Activado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts	Habilitado
2.63	Establecer 'Apagar: Permitir que el sistema se cierre sin tener que iniciar sesión' en 'Desactivado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on	Deshabilitado
2.64	Establecer 'Auditoría: forzar la configuración de la subcategoría de la política de auditoría (Windows Vista o posterior) para sustituir la configuración de la categoría de la política de auditoría' a 'Activado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Habilitado

2.65	Establecer 'Acceso a la red: permite que todos los permisos se apliquen a usuarios anónimos' a 'Desactivado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users	Deshabilitado
2.66	Configurar 'Control de cuentas de usuario: Detectar instalaciones de aplicaciones y solicitar elevación' a 'Activado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation	Habilitado
2.67	Establecer 'Cliente de red de Microsoft: Firmar digitalmente las comunicaciones (si el servidor está de acuerdo)' con 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees)	Habilitado
2.68	Configurar 'Inicio de sesión interactivo: Texto del mensaje para los usuarios que intentan iniciar sesión'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting to log on	@LOGON_TEXT@
2.69	Establecer 'Inicio de sesión interactivo: no mostrar el último nombre de usuario' a 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name	Habilitado
2.70	Set 'Seguridad de red: No almacene el valor de hash de LAN Manager en el siguiente cambio de contraseña' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change	Habilitado
2.71	Set 'Inicio de sesión interactivo: Solicitar al usuario que cambie la contraseña antes de la expiración'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration	Entre 5 and 14 dia(s).
2.72	Set 'Miembro del dominio: Requiere clave de sesión fuerte (Windows 2000 o posterior)' en 'Habilitado'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key	Habilitado
2.73	Set 'Servidor de red de Microsoft: Cantidad de tiempo de inactividad requerido antes de suspender la sesión'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session	15
2.74	Set 'Inicio de sesión interactivo: Número de inicios de sesión anteriores a la caché (en caso de que el controlador de dominio no esté disponible)'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available)	4

2.75	Establecer 'Control de cuentas de usuario: sólo elevar las aplicaciones UIAccess que se instalan en ubicaciones seguras' en 'Habilitado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations	Habilitado
2.76	Configure 'Auditoría: Cierre el sistema inmediatamente si no puede registrar las auditorías de seguridad' en 'Desactivado	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits	Deshabilitado
2.77	Set 'Acceso a la red: Acciones a las que se puede acceder de forma anónima'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously	Enabled:None.
2.78	Establecer 'Rendimiento del sistema de perfiles' en 'Administradores, NT SERVICE \ WdiServiceHost'	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token	Administrators, NT SERVICE\WdiServiceHost'
2.79	Configurar 'Cuentas: Renombrar cuenta de administrador'	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account	Administrator || "Admin"

ADMINISTRACION DE CUENTAS			
Control	**Objetivo de control**	**Ubicación**	**Valor**
4.1	Establezca 'Auditoría de administración de cuentas de equipo' en 'Satisfactoria y Fallida' (puntuación)	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Computer Account Management	Success and Failure
4.2	Establecer 'Gestión de grupo de seguridad de auditoría' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Security Group Management	Success and Failure
4.3	Establecer 'Auditoría de la gestión de cuentas de usuario' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: User Account Management	Success and Failure

4.4	Establecer 'Auditar el acceso al servicio de directorio' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service Access	Success and Failure
4.5	Set 'Cambios en el servicio de directorio de auditoría' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service Changes	Success and Failure
4.6	Set 'Auditoría del uso de privilegios sensibles' to 'Satisfactoria y Fallida	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Policy: Privilege Use: Sensitive Privilege Use	Success and Failure
4.7	Establecer 'Cambio de la política de auditoría de auditoría' en 'Satisfactorio y fracaso'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Audit Audit Policy Change	Success and Failure
4.8	Establecer 'Controlador IPsec de auditoría' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: IPsec Driver	Success and Failure
4.9	Establecer 'Cambio de estado de seguridad de auditoría' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: Security State Change	Success and Failure
4.10	Establecer 'Extension del sistema de seguridad de auditoría' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: Security System Extension	Success and Failure
4.11	Establezca 'Auditoría de otros eventos del sistema' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: Other System Events	Success and Failure
4.12	Establecer 'Cerrar sesión de auditoría' en 'Satisfactorio'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Logoff	Success
4.13	Establecer 'Validación de credenciales de auditoría' en 'Satisfactorio y falla'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Credential Validation	Success and Failure
4.14	Establecer 'Creación de procesos de auditoría' en 'Satisfactorio'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking: Process Creation	Success

4.15	Establecer 'Gestión de grupo de distribución de auditoría' en 'Satisfactorio y fracaso'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Distribution Group Management	'Success and Failure'
4.16	Establecer 'Auditoría de otros eventos de administración de cuentas' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Other Account Management Events	'Success and Failure'
4.17	*Establecer 'Bloqueo de cuenta de auditoría' en 'Satisfactorio'*	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Logoff	*'Success'*
4.18	*Establecer 'Inicio de sesión de auditoría' en 'Satisfactorio y error'*	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Other Logon/Logoff Events	'Success and Failure'
4.19	Establecer 'Auditoría de otros eventos de inicio de sesión / cierre de sesión' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Other Logon/Logoff Events	'Success and Failure'
4.20	*Establecer 'Inicio de sesión especial de auditoría' en 'Satisfactorio'*	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Special Logon	Success'
4.21	*Establezca 'Cambiar la política de autenticación de auditoría' en 'Satisfactorio'*	*Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Authentication Policy Change*	*'Success'*
4.22	*Establecer 'Integridad del sistema de auditoría' en 'Satisfactorio y fracaso'*	*Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: System Integrity*	*'Success and Failure'*

ADMINISTRACION DE CUENTAS			
Control	**Objetivo de control**	**Ubicación**	**Valor**
5.3	Establecer 'Desactivar Reproducción automática' a 'Habilitado: Todas las unidades'	Computer Configuration\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay\Turn off Autoplay	'Enabled:All drives'
5.4	*Establecer 'Instalar siempre con privilegios elevados' en 'Desactivado'*	User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges	*'Disabled'*
5.5	*Establecer 'Iniciar sesión en último usuario interactivo automáticamente después de un reinicio iniciado por el sistema' a 'Desactivado'*	Computer Configuration\Administrative Templates\Windows Components\Windows Logon Options\Sign-in last interactive user automatically after a system-initiated restart	*'Disabled'*
5.6	*Establecer 'Configurar actualizaciones automáticas' en 'Habilitado'*	Computer Configuration\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates	'Enabled'
5.7	*Establecer 'Configurar Actualizaciones Automáticas: Día de instalación programada' a '0 - Todos los días'*	*Computer Configuration\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day*	'0 - Every day'"
5.15	Establecer 'Instalar siempre con privilegios elevados' en 'Desactivado'	User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges	'Disabled'

E. GUÍA DE ASEGURAMIENTO WINDOWS 7

EVENTOS			
Control	Objetivo de control	Ubicación	Valor
1.1	Establecer 'Tamaño máximo del registro' - Aplicación	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application\Maximum Log Size (KB)	32768
1.2	Establecer 'Conservar eventos antiguos' - Aplicación	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application\Retain old events	Deshabilitado
1.3	Establecer 'Retener los eventos antiguos' - Seguridad	*Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Retain old events*	Deshabilitado
1.4	Establecer 'Tamaño máximo del registro' - Seguridad	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security\Maximum Log Size (KB)	81920
1.5	Establecer 'Tamaño máximo del registro' - Sistema	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System\Maximum Log Size (KB)	32768
1.6	Establecer 'Retener los eventos antiguos' - Sistema	Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System\Retain old events	Deshabilitado
1.7	Directiva de auditoría: Inicio de sesión-cierre de sesión: bloqueo de cuenta	Computer Configuration\Administrative Templates\Windows Components\Advanced Audit Configuration\Logon/Logoff\Audit Account Lockout	Success, Failure
1.8	Directiva de auditoría: Inicio de sesión: Cerrar sesión	Computer Configuration\Administrative Templates\Windows Components\Advanced Audit Configuration\Logon/Logoff\Audit Logoff	Success, Failure
1.9	Directiva de auditoría: Inicio de sesión: Cerrar sesión	Computer Configuration\Administrative Templates\Windows Components\Advanced Audit Configuration\Logon/Logoff\Audit Logon	Success, Failure
1.10	Directiva de auditoría: Acceso a objetos: Registro	Computer Configuration\Administrative Templates\Windows Components\Advanced Audit Configuration\Object Access\Audit Registry	Success, Failure
1.11	Directiva de auditoría: Acceso a objetos: SAM	Computer Configuration\Administrative Templates\Windows Components\Advanced Audit Configuration\Object Access\Audit SAM	Success, Failure
1.12	Política de auditoría: Uso de privilegios: uso confidencial de privilegios	Computer Configuration\Administrative Templates\Windows Components\Advanced Audit Configuration\Privilege Use\Audit Sensitive Privilege Use	Success, Failure

POLITICAS DE USUARIO			
Control	Objetivo de control	Ubicación	Valor
2.1	Establecer 'Duración de bloqueo de cuenta'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration	0
2.2	Establecer 'Umbral de bloqueo de cuenta'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold	5
2.3	Establecer 'Restablecer contador de bloqueo de cuenta después de' a '15' o superior	*Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after*	30
2.4	Establecer 'Guardar contraseñas mediante cifrado reversible'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption	Deshabilitado
2.5	Establecer 'Longitud mínima de la contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length	8
2.6	Establecer 'Máxima edad de contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age	30
2.7	Establecer 'Imponer historial de contraseñas'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history	8
2.8	Establecer 'Edad mínima de la contraseña'	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age	1
2.9	Establecer contraseña debe cumplir con los requisitos de complejidad '	Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements	Habilitado
2.10	Establecer 'Habilitar protector de pantalla'	User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver	Habilitado
2.11	Establecer 'Tiempo de espera del protector de pantalla'	User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver timeout	900
2.12	Set 'Contraseña proteger el protector de pantalla'	User Configuration\Administrative Templates\Control Panel\Personalization\Password protect the screen saver	Habilitado

ADMINISTRACION REMOTA			
Control	Objetivo de control	Ubicación	Valor
3.1	Establecer 'No permitir que las contraseñas se guarden'	Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client\Do not allow passwords to be saved	Habilitado
3.2	Establecer 'Asistencia remota solicitada'	Computer Configuration\Administrative Templates\System\Remote Assistance\Solicited Remote Assistance	Habilitado
3.3	Establecer 'Siempre pedir contraseña al conectar'	Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon	Habilitado
3.4	'Establecer conexión de cliente'	Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level	High Level

ADMINISTRACION DE CUENTAS			
Control	**Objetivo de control**	**Ubicación**	**Valor**
4.1	Establezca 'Auditoría de administración de cuentas de equipo' en 'Satisfactoria y Fallida' (puntuación)	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Computer Account Management	Success and Failure
4.2	Establecer 'Gestión de grupo de seguridad de auditoría' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Security Group Management	Success and Failure
4.3	Establecer 'Auditoría de la gestión de cuentas de usuario' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: User Account Management	Success and Failure
4.4	Establecer 'Auditar el acceso al servicio de directorio' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service Access	Success and Failure
4.5	Set 'Cambios en el servicio de directorio de auditoría' en 'Satisfactoria y Fallida'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Policy: DS Access: Directory Service Changes	Success and Failure
4.6	Set 'Auditoría del uso de privilegios sensibles' to 'Satisfactoria y Fallida	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Policy: Privilege Use: Sensitive Privilege Use	Success and Failure
4.7	Establecer 'Cambio de la política de auditoría de auditoría' en 'Satisfactorio y fracaso'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Audit Policy Change	Success and Failure

4.8	Establecer 'Controlador IPsec de auditoría' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: IPsec Driver	Success and Failure
4.9	Establecer 'Cambio de estado de seguridad de auditoría' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: Security State Change	Success and Failure
4.10	Establecer 'Extension del sistema de seguridad de auditoría' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: Security System Extension	Success and Failure
4.11	Establezca 'Auditoría de otros eventos del sistema' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: Other System Events	Success and Failure
4.12	Establecer 'Cerrar sesión de auditoría' en 'Satisfactorio'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Logoff	Success
4.13	Establecer 'Validación de credenciales de auditoría' en 'Satisfactorio y falla'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Policy: Account Logon: Credential Validation	Success and Failure
4.14	Establecer 'Creación de procesos de auditoría' en 'Satisfactorio'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Policy: Detailed Tracking: Process Creation	Success
4.15	Establecer 'Gestión de grupo de distribución de auditoría' en 'Satisfactorio y fracaso'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Distribution Group Management	'Success and Failure'
4.16	Establecer 'Auditoría de otros eventos de administración de cuentas' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Policy: Account Management: Other Account Management Events	'Success and Failure'
4.17	*Establecer 'Bloqueo de cuenta de auditoría' en 'Satisfactorio'*	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Logoff	*'Success'*
4.18	*Establecer 'Inicio de sesión de auditoría' en 'Satisfactorio y error'*	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Other Logon/Logoff Events	'Success and Failure'

4.19	Establecer 'Auditoría de otros eventos de inicio de sesión / cierre de sesión' en 'Satisfactorio y error'	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Other Logon/Logoff Events	'Success and Failure'
4.20	*Establecer 'Inicio de sesión especial de auditoría' en 'Satisfactorio'*	Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Policy: Logon-Logoff: Special Logon	Success'
4.21	*Establezca 'Cambiar la política de autenticación de auditoría' en 'Satisfactorio'*	*Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Policy: Policy Change: Authentication Policy Change*	*'Success'*
4.22	*Establecer 'Integridad del sistema de auditoría' en 'Satisfactorio y fracaso'*	*Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Policy: System: System Integrity*	*'Success and Failure'*

PCI DSS			
Control	Objetivo de control	Ubicación	Valor
5.1	Deshabilitar CMD	(gpedit.msc)Configuración de usuario > Plantillas administrativas > Sistema > Impedir el acceso al símbolo del sistema	Habilitada
5.2	Deshabilitar Recortes (Snipping Tool)	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Tablet PC > Accesorios > No permitir la ejecucion de Recortes	Habilitada
5.3	Deshabilitar opción de conectar y desconectar unidades de red	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Componentes de Windows > Explorador de Windows > Quitar "Conectar a unidad de red" y "Desconectar de unidad de red"	Habilitada
5.4	Deshabilitar cambios en el proxy	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Componentes de Windows > Internet Explorer > Deshabilitar el cambio de configuración de proxy	Habilitada
5.5	Deshabilitar el acceso al panel de control	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Panel de Control > Prohibir el acceso al Panel de Control	Habilitada
5.6	Deshabilitar Power Shell	(gpedit.msc)Configuración de usuario > Plantillas administrativas > Sistema > No ejecutar aplicaciones de Windows especificadas	Habilitada > powershell.exe
5.7	Deshabilitar Busquedas en Active Directory	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum]	{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}"=dword:00000001
5.8	Deshabilitar agregar impresoras	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Panel de Control > Impresoras > Impedir la adicion de impresoras en la red	Habilitada
5.9	Deshabilitar eliminar impresoras	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Panel de Control > Impresoras > impedir eliminacion de impresoras en la red	Habilitada
5.10	Deshabilitar teclado virtual	(gpedit.msc)Configuración de usuario > Plantillas administrativas > Sistema > No ejecutar aplicaciones de Windows especificadas	Habilitada > osk.exe
5.11	Deshabilitar tecla "Impr Pant"	[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout]	"Scancode Map"=hex:00,00,00,00,00,00,00,00,
5.12	Deshabilitar opción de compartir carpetas	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Componentes de Windows > Uso compartido de red > Impedir que los usuarios compartan archivos dentro de su perfil	Habilitada
5.13	Quitar menu "ejecutar" del menú inicio	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Menú Inicio y barra de tareas > Quitar el menú Ejecutar del menú inicio	Habilitada
5.14	Quitar explorar red	[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum]	"{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}"=dword:00000001
5.15	Deshabilitar menú contextual	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Explorador de windows > Quitar el menú contextual predeterminado del Explorador de windows	Habilitada
5.16	Quitar menú "Archivo" del explorador de windows	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Explorador de windows > Quitar el menú archivo del explorador de windows	Habilitada
5.17	Quitar la opción "Opciones de carpeta" del menú herramientas	(gpedit.msc) Configuración de usuario > Plantillas administrativas > Explorador de windows > Quitar el menú opciones de carpeta del menú Herramientas	Habilitada

F. ANÁLISIS DE VULNERABILIDADES 2

Severity	Plugin Id	Name
High (7.2)	65057	Insecure Windows Service Permissions
High (7.2)	65057	Insecure Windows Service Permissions
High (7.2)	65057	Insecure Windows Service Permissions
Critical (10.0)	93656	PHP 5.6.x < 5.6.26 Multiple Vulnerabilities
Critical (10.0)	93815	OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32)
Critical (10.0)	94106	PHP 5.6.x < 5.6.27 Multiple Vulnerabilities
Critical (10.0)	94955	PHP 5.6.x < 5.6.28 Multiple Vulnerabilities
Critical (10.0)	95874	PHP 5.6.x < 5.6.29 Multiple Vulnerabilities
High (9.3)	93077	PHP 5.6.x < 5.6.25 Multiple Vulnerabilities
High (7.8)	96451	Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)
High (7.8)	96799	PHP 5.6.x < 5.6.30 Multiple DoS
High (7.8)	96873	OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities
High (7.2)	65057	Insecure Windows Service Permissions
Critical (10.0)	97997	Intel Management Engine Insecure Read / Write Operations RCE (INTEL-SA-00075)
Critical (10.0)	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
Critical (10.0)	88561	Microsoft Windows 8 Unsupported Installation Detection
High (7.2)	65057	Insecure Windows Service Permissions
High (7.2)	65057	Insecure Windows Service Permissions
Critical (10.0)	97997	Intel Management Engine Insecure Read / Write Operations RCE (INTEL-SA-00075)
High (7.2)	65057	Insecure Windows Service Permissions
High (7.5)	69552	Oracle TNS Listener Remote Poisoning
High (7.2)	65057	Insecure Windows Service Permissions
Critical (10.0)	62758	Microsoft XML Parser (MSXML) and XML Core Services Unsupported
Critical (10.0)	64784	Microsoft SQL Server Unsupported Version Detection
High (9.3)	35327	SizerOne ActiveX Control AddTab Method Remote Buffer Overflow
High (9.3)	48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
High (9.3)	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
High (9.3)	87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)