ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN PROCESO Y POLÍTICAS PARA LA GESTIÓN DE ACTUALIZACIONES DE SOFTWARE Y PARCHES DE SEGURIDAD DE PRODUCTOS MICROSOFT EN UNA INSTITUCIÓN SIN FINES DE LUCRO."

TRABAJO DE TITULACIÓN

Previa la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Stalin Miguel Meza Montoya

José Luis Zambrano Pinto

GUAYAQUIL – ECUADOR

AÑO 2018

AGRADECIMIENTO

Agradezco a Dios por ser mi guía en todo camino y por las bendiciones que me ha dado.

A mi madre que desde el cielo me sigue dando fortaleza, amor incondicional y perseverancia en casa momento de mi vida. A mi padre por todo el apoyo brindado.

A mi esposa y a mi hija por su amor incondicional.

A mis hermanos por todo el apoyo brindado en cada día de mi vida.

A todos los profesores por brindar sus conocimientos.

STALIN MIGUEL MEZA MONTOYA

Agradezco Dios por la oportunidad de conocer a las personas que hoy por hoy forman parte fundamental de mi vida en el plano personal y profesional.

A mi Familia ya que gracias a su valioso apoyo he logrado llegar a esta instancia, en la cual el esfuerzo y dedicación se ven reflejados.

JOSE LUIS ZAMBRANO PINTO

DEDICATORIA

A Dios, a nuestras familias, maestros, amigos y todas aquellas personas que día a día están con nosotros.

LOS AUTORES

TRIBUNAL DE SUSTENTACIÓN

DIRECTOR MSIG/MSIA

MGS. LENÍN FREIRE

DIRECTOR DEL PROYECTO DE GRADUACIÓN

MGS. LENÍN FREIRE

MIEMBRO DEL TRIBUNAL

MGS. OMAR MALDONADO

DECLARACIÓN EXPRESA

"Declaramos de forma expresa que todo el contenido de este Trabajo de Titulación es de nuestra completa autoría y responsabilidad, por lo que damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Stalin Miguel Meza Montoya

José Luis Zambrano Pinto

RESUMEN

Implementar políticas, procesos y una herramienta de administración centralizada para la gestión de actualizaciones de software y parches de seguridad de productos Microsoft, mediante WSUS para lograr dicho objetivo. El uso de esta herramienta permitirá administrar de manera adecuada y organizada las actualizaciones y parches de seguridad de los productos Microsoft, al igual que el consumo del ancho de banda para la red interna, de tal manera que se puedan instaurar controles y ejecutar la valoración necesaria para contrarrestar las vulnerabilidades y amenazas y con ello optimizar la eficacia y eficiencia de la organización.

Al tener productos Microsoft dentro de la organización que brindan servicios tanto interno como externos, su grado de criticidad para el negocio es fuerte por lo que debe tener en cuenta el uso de los tres atributos básicos de la seguridad de la información que son: la confidencialidad, integridad y disponibilidad.

La herramienta permitirá tener un control sobre el estado de los productos Microsoft en referencias a las actualizaciones y parches de seguridad, con esto se tendrá una visión clara para implementar procesos de controles y poder contrarrestar vulnerabilidades que puedan llegar a afectar a la infraestructura teniendo en cuenta la evaluación del riesgo y su tratamiento.

ÍNDICE GENERAL

AGRADECIMIENTO I

DEDICATORIA III

TRIBUNAL DE SUSTENTACIÓN IV

DECLARACIÓN EXPRESA V

RESUMEN VI

ÍNDICE GENERAL VII

ÍNDICE DE FIGURAS XI

ÍNDICE DE TABLAS XIII

INTRODUCCIÓN XIV

CAPÍTULO 1 1

GENERALIDADES 1

1.1 ANTECEDENTES 1

1.2 DESCRIPCIÓN DEL PROBLEMA 2

1.3 SOLUCIÓN PROPUESTA 3

1.4 OBJETIVO GENERAL 5

1.5 OBJETIVOS ESPECÍFICOS 5

1.6 ALCANCE 5

1.7 METODOLOGÍA 6

CAPÍTULO 2 8

MARCO TEÓRICO 8

2.1 SEGURIDAD INFORMÁTICA 8

2.2 SEGURIDAD DE LA INFORMACIÓN 10
2.3 RIESGO INFORMÁTICO 12
2.4 ANÁLISIS DE RIESGOS 14
2.5 POLÍTICAS DE SEGURIDAD 18
2.6 AMENAZAS A SISTEMAS MICROSOFT 20
2.7 ACTUALIZACIONES MICROSOFT 23
2.8 DESCRIPCIÓN GENERAL DE WSUS 3.0 SP2 25
CAPÍTULO 3..... 29
LEVANTAMIENTO DE INFORMACIÓN 29
3.1 ANTECEDENTES DE LA EMPRESA 29
3.2 INFRAESTRUCTURA DE LA EMPRESA 31
3.3 PROCESO ACTUAL DE PARCHADO 35
3.4 IDENTIFICACION DE AMENAZAS 36
3.5 CÁLCULO DE PROBABILIDAD DE LAS AMENAZAS 42
3.6 PLAN DE TRATAMIENTOS DE RIESGOS 45
CAPÍTULO 4..... 52
ANÁLISIS Y DISEÑO 52
4.1 TIPOS DE IMPLEMENTACIÓN DE WSUS 56
4.2 TIPO DE ADMINISTRACIÓN DE WSUS 59
4.3 TIPO DE BASE DE DATOS PARA WSUS 62
4.4 ALMACENAMIENTO WSUS 63
4.5 OPCIONES DE ANCHOS DE BANDA 64
4.6 DETERMINANDO LOS REQUERIMIENTOS DE CAPACIDAD 65
4.7 INTEGRACIÓN CON ACTIVE DIRECTORY 66

4.8 DEFINICIÓN DE POLÍTICAS DE APLICACIÓN DE ACTUALIZACIONES 68
CAPÍTULO 5..... 79
IMPLEMENTACIÓN Y PRUEBAS 79
5.1 INSTALACIÓN SERVIDOR 79
5.2 CONFIGURACIÓN DE POLÍTICAS AD 81
5.3 CONFIGURACIÓN DE LA RED 84
5.4 INSTALACIÓN PRERREQUISITOS 85
5.5 INSTALACIÓN WSUS 87
5.6 CONFIGURACIÓN CONSOLA DE ADMINISTRACIÓN 88
5.7 CONFIGURACIÓN WSUS 91
5.7.1 CONFIGURACIÓN SERVIDOR PRIMARIO 91
5.7.2 SELECCIONAR LENGUAJE DE ACTUALIZACIONES 91
5.7.3 SELECCIONAR PRODUCTOS PARA ACTUALIZAR 92
5.7.4 SELECCIONAR CLASIFICACIÓN DE ACTUALIZACIONES 93
5.7.5 CONFIGURACIÓN PROGRAMACIÓN DE SINCRONIZACIONES 94
5.8 CREACIÓN GRUPOS DE EQUIPOS EN WSUS 94
5.9 CREACIÓN DE REPORTES PARA WSUS 98
5.10 PRUEBAS EN SERVIDORES AMBIENTES NO PRODUCTIVOS 99
5.11 PLANIFICACIÓN DE PARCHADO PARA AMBIENTES PRODUCTIVOS 102
5.12 EJECUCIÓN DE PARCHADO EN AMBIENTES PRODUCTIVOS 103
CAPÍTULO 6..... 106
ANÁLISIS DE RESULTADOS 106
6.1 ANÁLISIS DE RESULTADOS DE ACUERDO A LA IMPLEMENTACIÓN 106
6.1.1 PROCESO DE PARCHADO 106

6.1.2 ANÁLISIS CON HERRAMIENTAS MICROSOFT 108

6.2 EVALUACIÓN DE EFICIENCIA SEGÚN LA IMPLEMENTACIÓN 110

CONCLUSIONES Y RECOMENDACIONES…….. 112

BIBLIOGRAFÍA 115

ANEXOS 117

GLOSARIO.....119

ÍNDICE DE FIGURAS

FIGURA 2.1 PILARES FUNDAMENTALES DE LA SEGURIDAD DE LA INFORMACIÓN 9
FIGURA 2.2 FACTORES QUE CONTRIBUYEN A RIESGOS DE SEGURIDAD. 14
FIGURA 2.3 EL PROCESO DE ADMINISTRACIÓN DE RIESGO..... 15
FIGURA 2.4 SISTEMAS MÁS VULNERABLES 21
FIGURA 2.5 SERVIDORES WEBS MÁS USADOS 21
FIGURA 2.6 VULNERABILIDADES POR AÑOS EN SISTEMAS MICROSOFT 22
FIGURA 2.7 TIPO DE VULNERABILIDADES FRECUENTES..... 23
FIGURA 2.8 COMO FUNCIONA WSUS..... 27
FIGURA 3.1 DISTRIBUCIÓN DE DOMINIO PRINCIPAL..... 32
FIGURA 3.2 DISTRIBUCIÓN DE SERVIDORES MICROSOFT. 34
FIGURA 3.3 PROCESO ACTUAL DE PARCHADO..... 36
FIGURA 3.4 ELEMENTOS DE ANÁLISIS DEL RIESGO. 40
FIGURA 3.5 MATRIZ DE ACEPTACIÓN DE RIESGO. 43
FIGURA 3.6 ELEMENTOS DE ANÁLISIS DEL RIESGO RESIDUAL. 46
FIGURA 4.1 FRAMEWORK A USAR EN EL PROYECTO. 52
FIGURA 4.2 DISEÑO DE FRAMEWORK SCRUM + PMI EN EL PROYECTO WSUS. 54
FIGURA 4.3 DISEÑO BÁSICO DE WSUS 58
FIGURA 4.4 DISEÑO MÚLTIPLES SERVIDORES DE WSUS 59
FIGURA 4.5 DESCARGAS DIFERIDAS DE ACTUALIZACIONES. 65
FIGURA 5.1 POLÍTICA DE PARCHADO AUTOMÁTICO 83
FIGURA 5.2 POLÍTICA DE PARCHADO MANUAL 84
FIGURA 5.3 CONSOLA DE ADMINISTRACIÓN WSUS. 90
FIGURA 5.4 GRUPOS DE EQUIPOS EN WSUS..... 97
FIGURA 5.5 REPORTES WSUS. 99

FIGURA 5.6 SERVIDORES FASE PILOTO. 100

FIGURA 5.7 EJECUCIÓN FASE NO-PRODUCCIÓN MODO AUTOMÁTICO. 101

FIGURA 5.8 SERVIDORES FASE PRODUCCIÓN. 102

FIGURA 5.9 EJECUCIÓN FASE PRODUCCIÓN MODO AUTOMÁTICO. 104

FIGURA 5.10 EJECUCIÓN FASE PRODUCCIÓN MODO MANUAL. 104

FIGURA 6.1 ANÁLISIS SOBRE SERVIDOR PARCHADO. 109

FIGURA 6.2 ANÁLISIS SOBRE SERVIDOR NO PARCHADO. 110

ÍNDICE DE TABLAS

TABLA 1 DETALLE DE DOMAINS CONTROLLERS 32
TABLA 2 CONFIGURACIÓN DE DOMAINS CONTROLLERS 33
TABLA 3 DISTRIBUCIÓN DE DOMAINS CONTROLLERS 33
TABLA 4 IDENTIFICACIÓN DE ACTIVOS 37
TABLA 5 TABLA DE VALORACIÓN DE ACTIVOS 38
TABLA 6 VALORACIÓN DE ACTIVOS 38
TABLA 7 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES. 40
TABLA 8 TABLA DE PROBABILIDAD DE OCURRENCIA. 42
TABLA 9 NIVELES DE TRATAMIENTO DEL RIESGO. 43
TABLA 10 CÁLCULO DE PROBABILIDAD DE LAS AMENAZAS 43
TABLA 11 CONTROLES PARA EL TRATAMIENTO DEL RIESGO 48
TABLA 12 MATRIZ DE GUÍA DEL PROYECTO 56
TABLA 13 TABLA DE CLASIFICACIÓN DE ACTUALIZACIONES 61
TABLA 14 TABLA DE CAPACIDADES WSUS 66
TABLA 15 ROLES Y RESPONSABILIDADES PROCESO DE PARCHADO 69
TABLA 16 CARACTERÍSTICAS SERVIDOR WSUS 80
TABLA 17 DEFINICIÓN DE PROCESO DE PARCHADO POR AMBIENTES 81
TABLA 18 CONFIGURACIÓN DE POLÍTICA PARA PARCHADO AUTOMÁTICO 82
TABLA 19 CONFIGURACIÓN DE POLÍTICA PARA PARCHADO MANUAL 83
TABLA 21 APLICACIÓN INICIAL DE PARCHES EN AMBIENTES NO-PRODUCTIVOS 117
TABLA 22 APLICACIÓN INICIAL DE PARCHES EN AMBIENTE PRODUCTIVOS 118

INTRODUCCIÓN

La información es el activo más valioso de toda institución, por lo que es de fundamental importancia emplear las medidas y procedimientos para proteger su disponibilidad, confidencialidad e integridad. Hoy por hoy existe un alto nivel de exhibición de este activo, que está conexo con la utilización e implementación de nuevos medios informáticos que si bien es cierto contribuyen a optimar la productividad y conseguir mejores resultados pero que lo posicionan en el foco de posibles vulnerabilidades y amenazas.

La organización hoy en día debe estar atenta a las actualizaciones de software y sistemas operativos por la seguridad de la información. No es solo tener actualizado las funcionalidades de un programa con versiones nuevas, sino y lo más importante es mantener la seguridad a medida que se van descubriendo vulnerabilidades, se debe tener claro que se desea proteger y como se lo va a hacer para el correcto movimiento del negocio, armando una táctica que le permita seguir con sus rutinas en caso de que llegare a suceder algún incidente.

En cada sistema operativo existente, Windows Linux, Apple OSX, etc. Hay estándares de actualizaciones. Microsoft por ejemplo, lanza boletines de seguridad y con ellos se parchan las vulnerabilidades, los agujeros que un atacante podría usar para acceder a través de sus productos y tomar control de la información, muchas organizaciones no valoran el riesgo de un ataque y consideran otras prioridades para su negocio, pero aunque el riesgo sea bajo, el

nivel de daño que un atacante puede ocasionar a nuestra organización a nivel financiero, operacional y tecnológico es muy grande, en este caso se pregunta ¿son importante las actualizaciones?, y la respuesta es muy fácil, son fundamentales.

Este proyecto de titulación se basa en un análisis e implementación de procesos y políticas para parchado con la herramienta WSUS, como un sistema centralizado para la administración de las actualizaciones automáticas que provee de los recursos necesarios para gestionar y distribuir los parches la seguridad lanzados al mercado a través de Microsoft Update a los equipos de la red.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

Las empresas en un mundo de tecnologías y específicamente en la informática, viven en constante actualización. Los sistemas operativos, software y plataformas sufren cambios, al estar prácticamente siempre conectados al mundo están en constante riesgo.

En la mayoría de las empresas el proceso de actualización se realiza de manera correcta, ya sea de forma desatendida o automática para el caso de pequeñas empresas, pero para el caso de empresas donde se maneja un volumen más alto de equipos y se usan aplicaciones que afectan directamente al negocio se necesita una mejor centralización de las actualizaciones, en este caso un proceso más acorde a la situación de la empresa, es decir manejar equipos de pruebas para probar actualizaciones, definir momentos para aplicar en equipos productivos sin que afecte a la operatividad y desde Microsoft se cuenta con una poderosa herramienta para llevar a cabo un proceso tan necesario como crítico.

Es por esta razón que a través de WSUS los equipos quedan vinculado a esta herramienta, convirtiéndolos en equipos administrados y así poder tener un control sobre que actualización aplicar y que no aplicar.

1.2 DESCRIPCIÓN DEL PROBLEMA

Dentro de la Institución se detectó que el parque de servidores no posee un nivel estandarizado de parches lo cual constituye un riesgo inherente ya que al no tener actualizado un producto basado en las recomendaciones del fabricante (Parches Críticos y de Seguridad), se crean brechas de seguridad lo cual puede comprometer de manera directa la integridad de la información, la infraestructura de la empresa actualmente es de 253 servidores Windows, divididos en 4 ambientes (Producción, Preproducción, QA y Desarrollo).

Las actualizaciones para aplicaciones y sistemas operativos dentro de una organización es uno de los principales requisitos para cumplir con los estándares de seguridad, los principales ataques a organizaciones se dan principalmente cuando se tiene sistemas operativos obsoletos, software no actualizados ya que generalmente tienden a tener bugs o agujeros de seguridad que permite a un atacante aprovecharse de esta vulnerabilidad.

Para las grandes organizaciones existe un riesgo mayor, al intentar solucionar el problema de las actualizaciones, nos podemos encontrar con el detalle de como poder actualizar los equipos y software sin que se vea afectado el nivel de operatividad, como lograr verificar que un parche no afecte a las aplicaciones críticas, la mayoría de las organizaciones que no siguen los estándares adecuados no tienen un ambiente de prueba para los parches de seguridad y actualizaciones

de software ya que muchas veces confiamos directamente en que en este caso Microsoft tiene certificadas las mismas.

Generalmente y en este escenario la organización no tiene un control sobre las actualizaciones, no se tiene una herramienta que centralice todo el proceso que implica actualizar un servidor, no tenemos una forma de medir este proceso y ver qué tan propenso a ataques podemos estar.

1.3 SOLUCIÓN PROPUESTA

La solución que se plantea es la creación de una política de gestión de parches e implementación del servicio Windows Server Update (WSUS) integrándose a su vez con el directorio Activo de la organización, de esta formar permitir la distribución de parches y actualizaciones de forma centralizada para todos los productos Microsoft, de forma práctica, eficiente y programada, permitiendo a la organización una gestión más correcta de las actualizaciones y del uso del ancho de banda.

Este componente se puede instalar en Windows Server 2008 y versiones superiores dentro del firewall corporativo. El servidor WSUS permite a los administradores, distribuir actualizaciones a través de una consola de administración, la cual puede instalarse en cualquier equipo Windows en el dominio. Además, un servidor WSUS puede ser el origen de actualizaciones para otros servidores WSUS dentro de la organización. Al menos un servidor WSUS de la red debe conectarse a Microsoft Update para obtener información acerca de las actualizaciones disponibles. En función de la seguridad y la configuración de la red, se puede determinar si los otros servidores deberán conectarse directamente a Microsoft Update.

Esta solución es altamente integrada con AD pudiendo crear políticas para los equipos de las organizaciones, se puede manejar un ambiente de pruebas para validar los parches que mensualmente envía Microsoft para sus productos, así con esto podemos verificar la correcta aplicación de estas.

Al aplicar esta solución en una organización que cuenta con un gran volumen de activos, la operatividad de la red no se verá afectada por las actualizaciones, además que los equipos no estarán conectados a internet para las descargas, permitiendo que nuestra red sea segura.

WSUS es lo bastante flexible como para satisfacer las necesidades de administración de actualizaciones de la organización, desde la pequeña empresa hasta las empresas más grandes con miles de usuarios distribuidos entre múltiples lugares. En función del tamaño de la organización, de su ubicación y de su infraestructura de conectividad, se pueden determinar la manera más eficaz de escalar horizontalmente los servidores WSUS, una decisión en la sé que puede implicar a un servidor WSUS, o a varios.

A continuación, se muestra el escenario sugerido a implementar de acuerdo con las necesidades de la organización:

Un solo servidor WSUS

Dado que dentro del alcance a implementar abarca a sistemas operativos de Servidores Windows, se plantea como escenario un solo servidor WSUS, de esta forma se puede configurar un servidor que ejecute WSUS dentro del firewall corporativo, el cual sincroniza el contenido directamente con Microsoft Update y distribuye las actualizaciones entre los equipos cliente.

Como beneficio directo de la solución propuesta se obtendrán La mitigación de vulnerabilidades del sistema operativo mediante la aplicación de actualizaciones de acuerdo con las recomendaciones y mejores prácticas del fabricante.

1.4 OBJETIVO GENERAL

Implementar un proceso y políticas para la gestión de actualizaciones de software y parches de seguridad de productos Microsoft en una institución sin fines de lucro.

1.5 OBJETIVOS ESPECÍFICOS

- Estudiar la situación de la empresa en base a la actual infraestructura.
- Desarrollar el levantamiento de información en base al proceso de actualizaciones de productos Microsoft.
- Diseñar plan de implementación de Microsoft Windows Server Update Services (WSUS).
- Implementar y configurar servicios Microsoft Windows Server Update Services (WSUS) y Active Directory para aplicación de actualizaciones.
- Analizar los resultados, conclusiones y certificar que se realicen los objetivos planteados.

1.6 ALCANCE

- Desarrollar una administración correcta de equipos para parchado.
- Establecer que las actualizaciones sean aplicadas de forma adecuada.
- Alcanzar resultados que sean medibles.
- Optimizar la aplicación de las actualizaciones sin degradar la red interna.
- Mejorar los controles sobre las actualizaciones.

1.7 METODOLOGÍA

Para la implementación de este proyecto se unirán las metodologías SCRUM y PMI, para el análisis de riesgo nos guiaremos con la metodología MAGERIT y para los controles nos guiaremos con el anexo de la norma ISO2701, con esto estableceremos un conjunto de directrices que orientarán la gestión y dirección del proyecto. Los procesos resultantes de esta unión serán los definidos para un proyecto PMI:

- Inicio
- Planificación
- Ejecución
- Supervisión
- Cierre

La metodología para con la que se abordara el proyecto es SCRUM, la misma permite abordar proyectos complejos desarrollados en entornos dinámico y cambiante de un modo flexible, a través de entregas parciales sobre el avance del proyecto.

SCRUM es un proceso en que de manera regular se aplican un conjunto de buenas prácticas para trabajar colaborativamente, en equipo, y obtener el mejor resultado de un proyecto, esta metodología también se utiliza para resolver situaciones en que no se están entregando al cliente lo que necesita.

En Scrum un proyecto se ejecuta en bloques temporales cortos y fijos (iteraciones que normalmente son de 2 semanas, aunque en algunos equipos son de 3 y hasta 4 semanas, límite máximo de feedback y reflexión). Cada iteración tiene que

proporcionar un resultado completo, un incremento de producto final que sea susceptible de ser entregado con el mínimo esfuerzo al cliente cuando lo solicite.

Es esencial decir que la mayor parte de los problemas de seguridad de las diferentes organizaciones, ocurren por el poco uso y conocimiento de las políticas y normas implementadas para tratar la seguridad de la información, por ello deben formar parte de la cultura organizacional, para de este modo tratar de minimizar los riesgos o amenazas que pudieren causar problemas al negocio y en este caso todo el ambiente informático y más que todo el proceso de actualizaciones.

CAPÍTULO 2

MARCO TEÓRICO

2.1 SEGURIDAD INFORMÁTICA

La seguridad informática ayuda a resguardar los medios informáticos de una organización, permitiendo asegurar la confidencialidad, integridad y disponibilidad de los datos diseñando normas, procedimientos, métodos y técnicas para de esta forma conseguir sistemas confiables y seguros [1] [2].

El objetivo principal de la seguridad informática es mantener la Integridad, disponibilidad y privacidad de la información manejada por cualquier sistema informático.

a) **Integridad:** Se refiere a que los datos deben ser consistentes.
b) **Confidencialidad:** Se refiere a que los datos deben ser seguros y privados.
c) **Disponibilidad:** Se refiere a que los datos deben estar siempre accesibles.

FIGURA 2.1 Pilares fundamentales de la seguridad de la información
Fuente: Autor

Uno de los errores más comunes que cometen las organizaciones es pensar que, por tener un dispositivo o un software de seguridad, están a salvo de ataques, cabe recalcar que estas aplicaciones son de gran ayuda para la organización, pero no necesariamente garantizan la seguridad informática.

Aunque la tecnología permite a las organizaciones ser más productivas y permite estar conectados en un mundo globalizado con un solo clic, también conlleva una serie de problemas de seguridad. Si la información de la organización queda expuesta a un atacante las consecuencias pueden ser desbastadoras. De repente, las organizaciones podrían perder millones de dólares, enfrentar enjuiciamientos y sufrir daños a la a su reputación, para evitar en la mediad que sea posible estas amenazas se tiene que tener un pleno conocimiento de las mismas, es decir saber a qué es lo se enfrentan, con la finalidad de poder contrarrestarlas, implementando los mecanismos necesarios para ello [3] .

Definir un punto exacto en el que podemos considerar estar seguro presenta un gran desafío, pues esta es una de las preguntas que generalmente se hacen las empresas ¿Cuál es el máximo grado de seguridad que puedo obtener? Está claro que la seguridad absoluta no existe, puesto que al no conocer en qué momento ocurrirá una amenaza, el riesgo siempre estará presente, por ello es de vital importancia tener un modelo o marco que podamos utilizar como base o punto de referencia que nos proporcione un conjunto de terminologías y conceptos a los que como la organización pueda hacer referencia cuando surgen problemas de seguridad.

2.2 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se define como “proteger la información y los sistemas de información del acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción”, de acuerdo con la legislación de los EE.UU [1]. Básicamente, significa que queremos proteger nuestros datos (donde sea que se encuentren) y los activos de aquellos que intenten utilizarlos de manera incorrecta.

En general, seguridad significa proteger nuestros activos. Esto puede significar protegerlos de atacantes que invaden nuestras redes, virus/gusanos, desastres naturales, condiciones ambientales adversas, fallas de energía, robo o vandalismo u otros estados indeseables. En última instancia, intentaremos protegernos contra las formas más probables de ataque, en la medida de lo razonablemente posible, dado nuestro entorno.

En nuestros esfuerzos por asegurar nuestros activos, también debemos considerar las consecuencias de la seguridad que elegimos implementar. Hay una frase muy conocida que dice: "El único sistema verdaderamente seguro es el que está

apagado, en el interior de un bloque de hormigón y sellado en una habitación con vestimenta de plomo con guardias armados, e incluso entonces tengo mis dudas" [2]. Aunque podríamos decir con certeza que un sistema en tal estado podría considerarse razonablemente seguro, seguramente no es útil ni productivo. A medida que aumentamos el nivel de seguridad, generalmente disminuimos el nivel de productividad. Con el sistema mencionado en nuestra cita, el nivel de seguridad sería muy alto, pero el nivel de productividad sería muy cercano a cero. El objetivo de un plan de seguridad es encontrar el equilibrio entre protección, usabilidad y costo.

Además, al asegurar un activo, sistema o entorno, también debemos considerar cómo el nivel de seguridad se relaciona con el valor del artículo que se está asegurando. Podemos, si estamos dispuestos a dar cabida a la disminución del rendimiento, aplicar niveles muy altos de seguridad a todos los activos de los que somos responsables. Podemos construir una instalación de miles de millones de dólares rodeada de alambradas y patrullada por guardias armados, y colocar cuidadosamente nuestro activo en una bóveda herméticamente sellada en el interior para que nuestra información nunca sea vulnerada, pero eso no tendría mucho sentido. Sin embargo, en algunos entornos, tales medidas de seguridad podrían no ser suficientes. En cualquier entorno en el que planeamos implementar niveles elevados de seguridad, también debemos tener en cuenta el costo de reemplazar nuestros activos si los perdemos.

En consecuencia, debe considerarse la propagación de dichas medidas para garantizar que sean cumplidas y que están conforme con la situación del negocio. Por ello la seguridad de la información es de vital importancia ya que constituye una responsabilidad de fortalecimiento y concienciación de la información por la

organización, estableciendo objetivos y direccionando medios tanto económicos como humanos para lograr el objetivo [4].

2.3 RIESGO INFORMÁTICO

Para poder hablar más específicamente sobre riesgo informático, necesitamos introducir algunos nuevos elementos de terminología. Cuando consideramos el potencial de un ataque en particular para afectarnos, podemos hablar de él en términos de amenazas, vulnerabilidades y el riesgo asociado que podría acompañarlos.

Amenazas

Una amenaza es algo que tiene el potencial de causarnos daño. Las amenazas tienden a ser específicas para ciertos entornos, particularmente en el mundo de la seguridad de la información. Por ejemplo, aunque un virus puede representar una amenaza para un sistema operativo Windows, es poco probable que el mismo virus tenga algún efecto en un sistema operativo Linux**.**

Vulnerabilidades

Las vulnerabilidades son debilidades que pueden usarse para dañar un entorno. En esencia, son agujeros que pueden ser explotados por amenazas para causarnos daño. Una vulnerabilidad puede ser un sistema operativo sin parchar o una aplicación específica que estamos ejecutando, una ubicación física donde hemos elegido colocar nuestro edificio de oficinas, un centro de datos que está poblado por la capacidad de su sistema de aire acondicionado, la falta de generadores de respaldo, u otros factores.

Riesgo

El riesgo es la probabilidad de que algo malo suceda. Para que tengamos un riesgo en un entorno particular, debemos tener tanto una amenaza como una vulnerabilidad que se pueda explotar. Por ejemplo, si tenemos una estructura que está hecha de madera y la prendimos fuego, tenemos una amenaza (el fuego) y una vulnerabilidad que coincide con ella (la estructura de la madera). En este caso, definitivamente tenemos un riesgo.

Del mismo modo, si tenemos la misma amenaza de incendio, pero nuestra estructura está hecha de concreto, ya no tenemos un riesgo creíble, porque nuestra amenaza no tiene una vulnerabilidad que explotar. Podemos argumentar que una llama suficientemente caliente podría dañar el concreto, pero este es un evento mucho menos probable.

A menudo tendremos discusiones similares sobre el riesgo potencial en entornos informáticos, y posibles, pero poco probables, ataques que podrían ocurrir. En tales casos, la mejor estrategia es dedicar nuestro tiempo a mitigar los ataques más probables. Si hundimos nuestros recursos en el intento de planificar cualquier ataque posible, por improbable que sea, nos dispersaremos y tendremos falta de protección donde más lo necesitemos.

Algunas organizaciones, como la Agencia de Seguridad Nacional de los EE. UU. (NSA), agregan un factor adicional a la ecuación de amenaza / vulnerabilidad / riesgo, en forma de impacto. Si consideramos que el valor del activo se ve amenazado como un factor, esto puede cambiar independientemente de si vemos un riesgo como presente o no. Por ejemplo, en caso de perder una cinta de copia de seguridad sin cifrar y estipulamos que las mismas contienen solo información no relevante, es posible que en realidad no corramos ningún riesgo. Los datos que se

exponen no nos causarán ningún problema, ya que no tienen nada de sensible, y podemos realizar copias de seguridad adicionales a partir de los datos de origen. En este caso particular, podemos decir con seguridad que no tenemos ningún riesgo. A la inversa, si la información de propiedad crítica de una empresa se viera comprometida, podrían terminar cerrando.

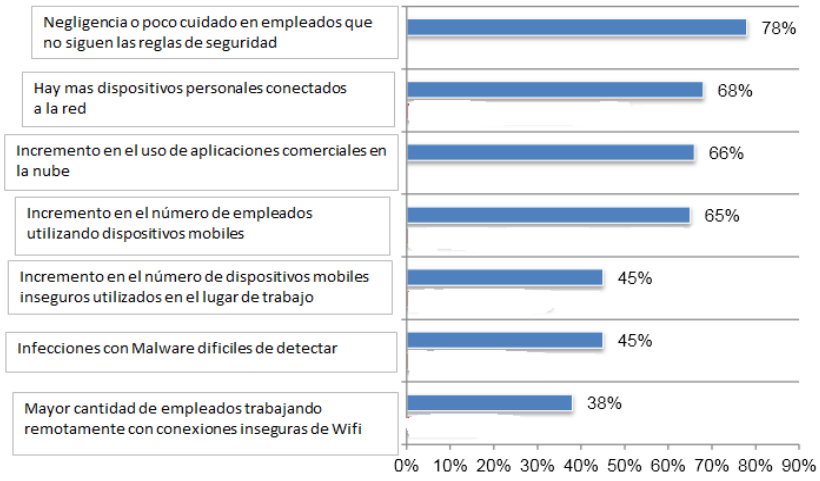


FIGURA 2.2 Factores que contribuyen a riesgos de seguridad
Fuente: PONEMON INSTITUTE (Año 2.014)

2.4 ANÁLISIS DE RIESGOS

Para compensar los riesgos que ocurren en nuestro entorno, es muy importante implementar y seguir el proceso de gestión de riesgos. Este programa debe ser administrado a nivel de altos directivos de la organización e implementado por todos (no solo por el personal técnico). En un nivel alto, necesitamos identificar nuestros activos importantes, identificar las posibles amenazas en su contra, evaluar las vulnerabilidades que tenemos presentes y luego tomar medidas para mitigar estos riesgos, como se muestra en la Figura 2.3 [1].

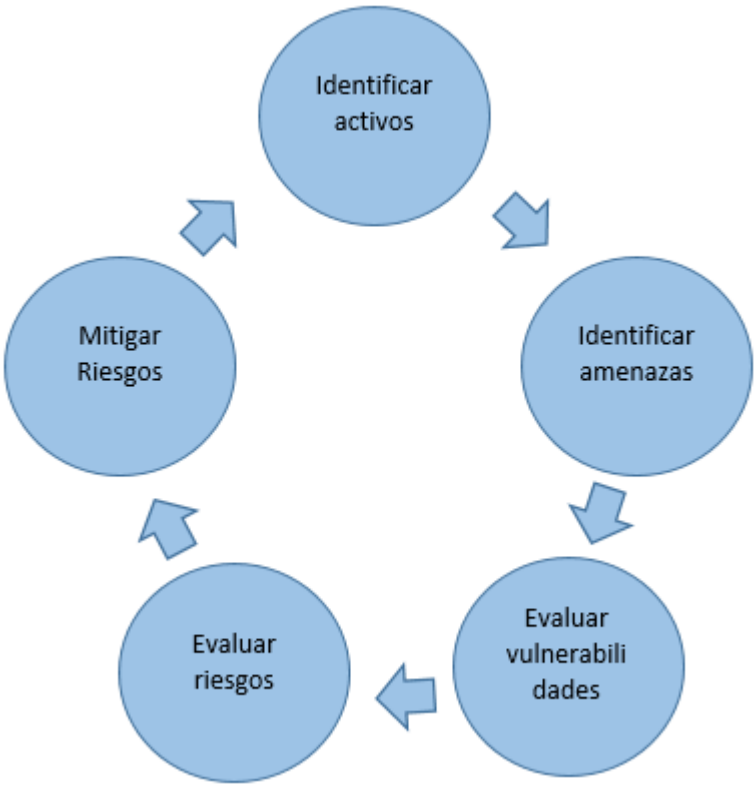


FIGURA 2.3 El proceso de administración de riesgo
Fuente: Los fundamentos de la seguridad de la información, 2da edición (Año 2.014)

Identificar activos

Una de las primeras y, posiblemente, una de las partes más importantes del proceso de gestión de riesgos es identificar y categorizar los activos que protegemos. Si no podemos enumerar los activos que tenemos y evaluar la importancia de cada uno de ellos, protegerlos puede convertirse en una tarea muy difícil.

Identificar amenazas

Una vez que hemos enumerado nuestros activos críticos, podemos comenzar a identificar las amenazas que podrían afectarlos. A menudo es útil tener un marco dentro del cual discutir la naturaleza de una amenaza dada. Por ejemplo, si examinamos las amenazas que podríamos enfrentar contra una aplicación que procesa pagos con tarjeta de crédito:

- **Confidencialidad:** si exponemos los datos de manera inapropiada, tenemos una potencial infracción.
- **Integridad:** si los datos se corrompen, podemos procesar los pagos de manera incorrecta.
- **Disponibilidad:** si el sistema o la aplicación se caen, no podemos procesar pagos.

Si bien este es un paso de alto nivel para evaluar las amenazas para cualquier entorno, sí se señala algunas áreas problemáticas de inmediato. Debemos preocuparnos por no perder el control de los datos, mantener datos precisos y mantener el sistema en funcionamiento. Dada esta información, podemos comenzar a observar las áreas de vulnerabilidad y riesgo potencial.

Evaluar vulnerabilidades

Cuando analicemos las vulnerabilidades, debemos hacerlo en el contexto de amenazas potenciales. Cualquier activo dado puede tener miles o millones de amenazas que podrían afectarlo, pero solo una pequeña fracción de ellas realmente será relevante. El problema de identificarlos se reduce considerablemente al analizar primero las amenazas potenciales.

Evaluar riesgos

Una vez que hemos identificado las amenazas y vulnerabilidades para un activo determinado, podemos evaluar el riesgo general. Como discutimos anteriormente en este capítulo, el riesgo es la conjunción de una amenaza y una vulnerabilidad. Una vulnerabilidad sin amenaza coincidente o una amenaza sin vulnerabilidad coincidente no constituye un riesgo.

Mitigar riesgos

Para mitigar el riesgo, podemos implementar medidas para ayudar a garantizar que se tenga en cuenta un determinado tipo de amenaza. Estas medidas se conocen como controles. Los controles se dividen en tres categorías: físicos, lógicos y administrativos.

- **Físico**: Los controles físicos son aquellos que protegen el entorno físico en el que se encuentran nuestros sistemas, o donde se almacenan nuestros datos. Dichos controles también controlan el acceso dentro y fuera de dichos entornos. Los controles físicos lógicamente incluyen elementos tales como, cerraduras, protecciones y cámaras, pero también incluyen sistemas que mantienen el entorno físico, como sistemas de aire acondicionado, sistemas de extinción de incendios y generadores de energía de respaldo.
- **Controles lógicos y técnicos:** Los controles lógicos, a veces llamados controles técnicos, son aquellos que protegen los sistemas, redes y entornos que procesan, transmiten y almacenan nuestros datos. Los controles lógicos pueden incluir elementos tales como contraseñas, cifrado, controles de acceso lógico, firewalls y sistemas de detección de intrusos.
- **Administrativo:** Los controles administrativos se basan en reglas, leyes, políticas, procedimientos, directrices y otros elementos. En esencia, los

controles administrativos establecen las reglas sobre cómo esperamos que se comporten los usuarios de nuestro entorno. Según el entorno y el control en cuestión, los controles administrativos pueden representar diferentes niveles de autoridad. Es posible que tengamos una regla simple, como "apague la cafetera al final del día", con el objetivo de garantizar que no cause un problema de seguridad física al quemar nuestro edificio por la noche. También podemos tener un control administrativo más estricto, como uno que requiere que cambiemos nuestra contraseña cada 90 días.

2.5 POLÍTICAS DE SEGURIDAD

Una política de seguridad de la información es el pilar fundamental de un programa de seguridad de la información. Debe reflejar los objetivos de la organización para la seguridad y la estrategia de gestión (leyes, normas y prácticas) acordada para asegurar la información.

Para que la política sea útil debe ser formalmente acordado por la gerencia ejecutiva. Esto significa que, para redactar un documento de política de seguridad de la información, una organización debe tener objetivos de seguridad bien definidos y una estrategia de gestión acordada para proteger la información. Si hay un debate sobre el contenido de la política, el debate continuará a través de los intentos subsiguientes de aplicarlo, con la consecuencia de que el programa de seguridad de la información en sí será disfuncional.

Existe una gran cantidad de productos de política de seguridad en el mercado, pero pocos de ellos serán formalmente acordados por la gerencia ejecutiva sin que un profesional de la seguridad lo explique en detalle. Esto no es probable debido a limitaciones de tiempo inherentes a la gestión ejecutiva, incluso si fuese posible que

la gerencia respalde de inmediato una política comercial, no es el enfoque correcto para intentar enseñarle a la administración cómo pensar sobre la seguridad. Más bien, el primer paso para componer una política de seguridad es descubrir cómo la administración ve la seguridad. Como una política de seguridad es, por definición, un conjunto de mandatos de gestión con respecto a la seguridad de la información, estos mandatos proporcionan las órdenes de marcha para el profesional de la seguridad. Si, en cambio, el profesional de seguridad proporciona mandatos a la dirección ejecutiva para que firmen, es probable que se pasen por alto los requisitos de gestión.

Un profesional de la seguridad cuyo trabajo consiste en elaborar una política de seguridad debe, por lo tanto, asumir el papel de esponja y escriba para la gestión ejecutiva. Una esponja es un buen oyente que puede absorber fácilmente el contenido de la conversación de cada persona, independientemente de la diversidad del grupo con respecto a las habilidades de comunicación y la cultura. Un escriba documenta ese contenido fielmente sin adornos ni anotaciones. Una buena esponja y escriba podrá capturar temas comunes de las entrevistas de gestión y preparar una declaración positiva sobre cómo la organización en su conjunto quiere que su información esté protegida. El tiempo y el esfuerzo invertidos para obtener un consenso ejecutivo sobre la política darán frutos en la autoridad que presta al proceso de aplicación de políticas.

Por supuesto, un profesional de seguridad con experiencia también tendrá consejos sobre cómo moldear la opinión de la gerencia con respecto a la seguridad en una estrategia organizacional integral. Una vez que está claro que el profesional de seguridad entiende completamente las opiniones de la administración, debería ser posible introducir un marco de seguridad que sea coherente con él. El marco será la base del Programa de seguridad de la información de la organización y, por lo

tanto, servirá como guía para crear un esquema de la política de seguridad de la información.

A menudo, se utiliza un documento de estándares de la industria de seguridad como marco de referencia. Por ejemplo, el Estándar de Buenas Prácticas del Foro de Seguridad [5], la serie de Gestión de Seguridad de la Organización Internacional de Estándares (27001, 27002, 27005) [19] y los Objetivos de Control de la Asociación de Auditoría y Control de Sistemas de Información (CoBIT) [6]. Este es un enfoque razonable, ya que ayuda a garantizar que la política sea aceptada como adecuada no solo por la administración de la empresa, sino también por auditores externos y otras personas que puedan tener interés en el Programa de seguridad de la información de la organización.

2.6 AMENAZAS A SISTEMAS MICROSOFT

Existen un gran número de amenazas diferentes que pueden comprometer nuestra seguridad y nuestra privacidad al conectarnos a una red e incluso frente a usuarios no autorizados que tengan acceso físico al ordenador. Todos los años estas amenazas son explotadas y utilizadas por piratas informáticos para conseguir atacar a sus víctimas.

Microsoft cuenta con la mayor cuota del mercado según sitios especializados en estadísticas de software, esto lo hace un blanco atractivo de piratas informáticos en busca de vulnerabilidades que logren romper la seguridad de estos sistemas, según el sitio de análisis estadístico de mercado de software statcounter.com, Windows domina el mercado a diciembre del 2017 con el 83% del total de sistemas de escritorios.

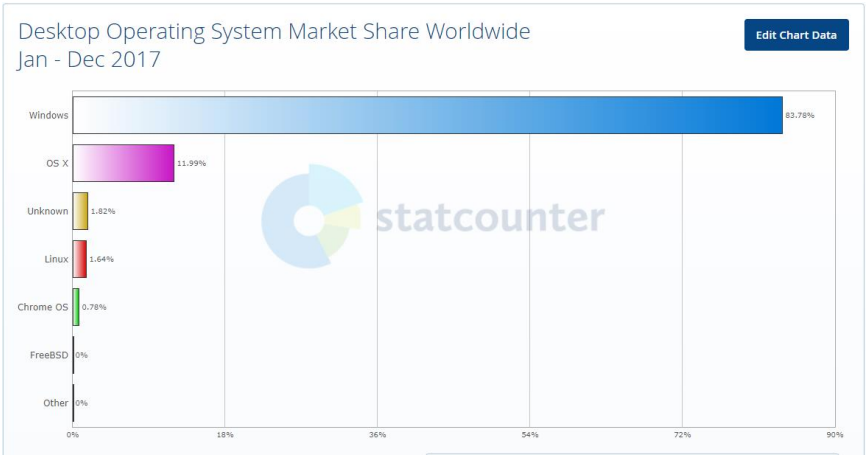


FIGURA 2.4 Sistemas más vulnerables
Fuente: port80software.com

A nivel de servidores, según datos del sitio w3techs que se basa en sitios públicos, Microsoft compite con Unix este último domina este mercado con un 66.8%, basados en el tráfico de sitios web públicos, pero estas cifras cambian rotundamente a nivel privado ya que según el portal port80software [7] en una encuesta llevada en el mes de Julio del 2017 sobre el top 1000 de empresas según la revista fortune, los resultados muestran que el 55% de las empresas usan IIS como su web server.

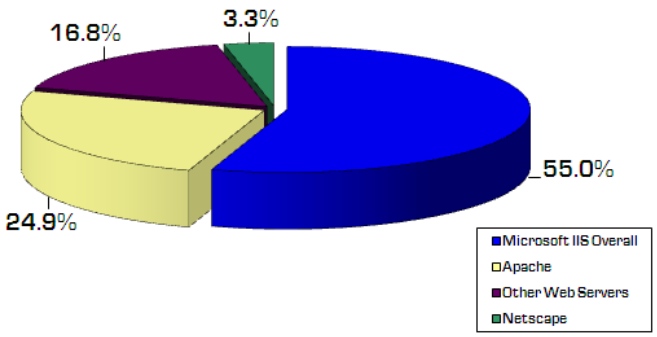


FIGURA 2.5 Servidores Webs más usados
Fuente: port80software.com

Es importante recalcar que todos los años los sistemas operativos están expuestos a nuevas vulnerabilidades, pero en el caso puntual de Microsoft Windows cada año se encuentran vulnerabilidades graves. Los más explotados son en IIS, MS-SQL e Internet Explorer, invertiblemente todos los sistemas operativos contienen vulnerabilidades y exposiciones que pueden ser el objetivo de los hackers y creadores de virus. Aunque las vulnerabilidades de Windows reciben la mayor publicidad debido a la cantidad de equipos que ejecutan este sistema.

El crecimiento de vulnerabilidades en sistemas Windows es constante cada año [8], al 2018 en general a nivel de productos Microsoft se han encontrado 5412 vulnerabilidades críticas, siendo los ataques de ejecución de código malicioso las más usadas, a nivel de sistemas operativos los más afectados por vulnerabilidades conocidas es Windows server 2008 con un total de 1022 a la fecha, seguido por Windows server 2012, pero lo más preocupante es la cantidad de vulnerabilidades en el nuevo sistemas para servidor 2016 ya que a la fecha se han detectado 300 casos críticos.

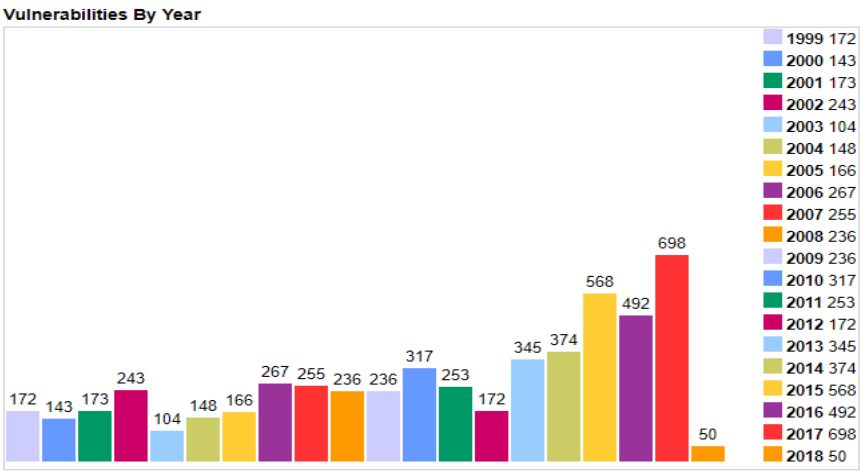


FIGURA 2.6 Vulnerabilidades por años en Sistemas Microsoft
Fuente: cvedetails.com

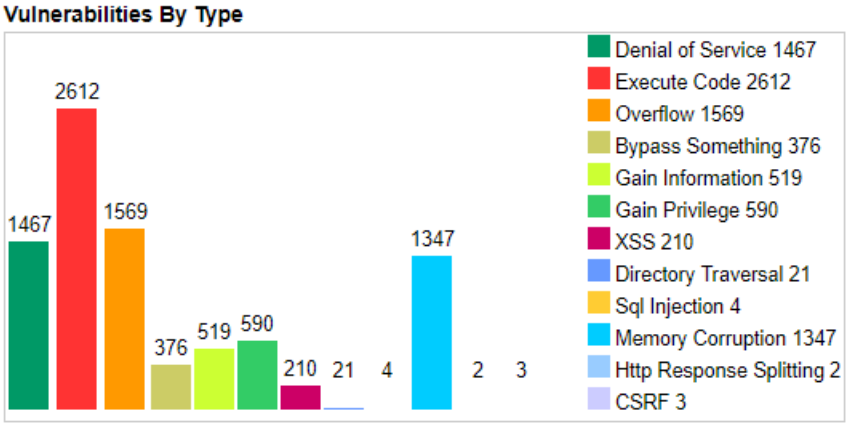


FIGURA 2.7 Tipo de vulnerabilidades Frecuentes
Fuente: cvedetails.com

En base a estos datos se debe remarcar la importancia de las actualizaciones de seguridad para software, sistemas operativos e inclusive firmware de PC, para esto Microsoft y otros fabricantes emiten parches para vulnerabilidades criticas rápidamente para mitigar los riesgos que está en constante crecimiento.

2.7 ACTUALIZACIONES MICROSOFT

Hasta cierto punto, sobrestimamos lo vulnerable que el software puede ser, al menos su impacto en el mundo real. Los principales proveedores de software, hardware o servicios han aprendido a reparar de más; es decir, los paquetes mensuales de innumerables parches por lo general incluyen algunos cuya importancia es en gran medida teórica y/o solo afectará a unas pocas personas.

La seguridad de un sistema operativo a veces se considera directamente proporcional a la cantidad total anual de parches que requiere (bajo el supuesto de que cuanto más a menudo requiere la instalación de parches, seguramente es más vulnerable). Sin embargo, también se puede sugerir que, si bien todos los sistemas

operativos complejos necesitan parches a medida que se descubren nuevos errores y aparecen nuevos exploits, la instalación frecuente de parches en realidad es una medida de diligencia profesional y no de inseguridad. De hecho, el número de variables que intervienen en la metodología, la eficacia y el despliegue de los parches hace que cualquiera de ambos puntos de vista parezca demasiado simplistas.

Microsoft para solventar estas necesidades incorpora en todos sus sistemas operativos el módulo de Windows Update a través de una red de actualizaciones, tratando de hacer más fácil las búsquedas de las mismas, este módulo no solo busca actualizaciones para sistemas operativos Windows, sino que de forma automática busca actualizaciones de todos los productos Microsoft asociadas al equipo.

El servicio de Windows Update ofrece una localización para descargar las actualizaciones, parches, arreglos de la seguridad, y mejoras que pueden ser libremente seleccionada por los usuarios, además detecta automáticamente cualquier producto y proporciona actualizaciones cunad estén disponibles, las mayorías de actualizaciones se lanzan el segundo martes de cada mes.

Microsoft publica boletines de seguridad cada mes donde describe las actualizaciones que se publican para dicho mes, en ellos se describen las soluciones y se proporciona vínculos a las actualizaciones correspondientes del software afectado, cada boletín va acompañado de un artículo de Knowledge Base exclusivo en el que se proporciona información sobre las actualizaciones.

Desafortunadamente muchas empresas toman días o meses para aplicar los parches que corrigen las vulnerabilidades encontradas. Generalmente las

vulnerabilidades, permiten a un atacante ejecutar código remoto y obtener el control completo del sistema con permisos administrativos.

Debido a que Windows e Internet Explorer son sistemas muy utilizados a nivel mundial, los ciberdelincuentes, no piensan dos veces para crear un exploit para aprovechar una vulnerabilidad presente en el sistema antes de aplicar el parche. Es por eso, que es importante que las organizaciones tomen conciencia y apliquen siempre los parches de Seguridad que Microsoft publica mes a mes.

Pero a nivel de grandes organizaciones que contienen una gran cantidad de equipos, cada uno de ellos necesitaría actualizarse constantemente lo que incurriría en un gran consumo de ancho de banda y para el caso de servidores y estaciones criticas sería un riesgo incorporar directamente las mismas por el tema de compatibilidad de algunas aplicaciones, pero para esto Microsoft desarrollo una solución llamada Windows Server Update Services (WSUS).

2.8 DESCRIPCIÓN GENERAL DE WSUS 3.0 SP2

Windows Server Update Services (WSUS) implementa las actualizaciones de productos de Microsoft. Con WSUS, se pueden gestionar de lleno la distribución de actualizaciones que se publican en Microsoft Update para los equipos de una organización [9].

WSUS facilita las características necesarias para gestionar y distribuir actualizaciones mediante una consola de administración. Además, WSUS puede ser el origen de actualización para otros servidores WSUS de la organización. El WSUS que actúa como origen de actualización es el servidor que precede en la cadena. En una implementación de WSUS, al menos un servidor WSUS debe

conectarse a Microsoft Update para obtener información sobre actualizaciones disponibles.

La gestión de actualizaciones es el proceso por el cual se controla la implementación y el mantenimiento de versiones provisionales de software en entornos de producción. Le permite resguardar la eficacia operativa, mitigar vulnerabilidades de seguridad y conservar la solidez del entorno de producción. Si la organización no puede establecer y conservar un nivel estable de confianza en sus sistemas operativos y softwares, y podría tener una serie de vulnerabilidades de seguridad que, si se explotan, afectarían los ingresos y la propiedad intelectual. Minimizar esta amenaza requiere que se tenga sistemas correctamente configurados, que usen el software más reciente y que se instalen los parches recomendados.

Los casos principales en los que WSUS ayuda al negocio son los siguientes:

- Administración centralizada de actualizaciones.
- Automatización de administración de actualizaciones.

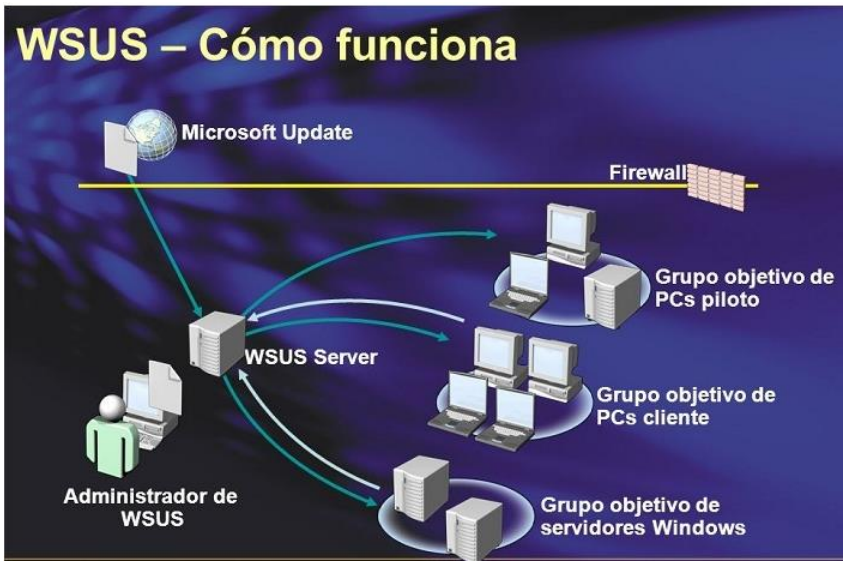


FIGURA 2.8 Como Funciona WSUS
Fuente: hackpuntes.com

WSUS proporciona una infraestructura de administración que consta de los siguientes componentes:

- **Microsoft Update**

Es el sitio web de Microsoft que distribuye actualizaciones para productos de Microsoft.

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

Es el componente de servidor que está instalado en una computadora que ejecuta un sistema operativo compatible dentro del firewall corporativo. El software de servidor WSUS permite a los administradores administrar y distribuir actualizaciones a través de una consola administrativa.

Un servidor WSUS puede obtener actualizaciones de Microsoft Update o de otro servidor WSUS. Al menos un servidor WSUS en la red debe conectarse a Microsoft Update para obtener las actualizaciones disponibles. Según la configuración de red, el ancho de banda y las consideraciones de seguridad.

- **Consola de administración de WSUS**

La Consola de administración de WSUS se instala automáticamente en el servidor WSUS, y también se puede instalar en cualquier computadora que se ejecute en un sistema operativo compatible. Puede usar la Consola de administración de WSUS para administrar cualquier servidor WSUS en cualquier dominio con el que tenga una relación de confianza.

- **Actualizaciones automáticas**

El componente de software de computadora del cliente que está integrado en los sistemas operativos de Windows. Actualizaciones automáticas permite que el servidor y las computadoras cliente reciban actualizaciones de Microsoft Update o de un servidor WSUS.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1 ANTECEDENTES DE LA EMPRESA

La empresa es una institución privada benéfica sin fines de lucro que opera en el Ecuador desde hace ciento treinta años con sucursales en Guayaquil. Esta organización no gubernamental se encarga de la dirección, administración y construcción de varios hospitales, casas de socorro, asilos y de la organización de juegos de azar a nivel nacional.

La autogestión se realiza por medio de los juegos de azar, el sector funerario y el sector Inmobiliario; que generan fondos que le permiten continuar con la obra social. Adicionalmente los Hospitales cuentan con el servicio de clínicas y pensionados a precios competitivos, lo que contribuye, en alguna medida, a subvencionar los costos de mantenimiento y operatividad de los hospitales generales que atienden a la comunidad de menores recursos.

La junta de directores define de manera global como se llevará el proceso de ventas de los productos antes mencionados, más es el departamento de Operaciones, encargada por el Gerente de Operaciones los responsables de establecer los controles que darán cumplimiento a las normas establecidas por las organizaciones regulatorias.

Los servicios que ofrece la empresa cuentan con sus propios sistemas informáticos tanto web como de escritorio, los mismos que se manejan con el modelo cliente servidor, siendo estos vulnerables a cualquier ataque informático, para lo cual cuenta con varios departamentos encargados de velar por la seguridad de los mismos, por lo tanto, son los encargados de hacer la evaluación inicial del riesgo que representan estos servicios.

Al realizar una evaluación de riesgos se encontró que los servidores y aplicaciones Microsoft no se contaban con un proceso de parchado, lo cual representa una gran amenaza a los servicios, por lo cual el gerente de operaciones debe ser el encargado de la mitigación inicial del riesgo que representa la información que está a su cargo, clasificándolo de la siguiente forma:

- **Riesgo Moral**

Al ser una institución que maneja temas de salud y juegos de azar donde la información vinculada a los usuarios es tan critica que se debe tener un alto grado de confidencialidad, es de suma importancia evitar que estos sean utilizados de forma incorrecta, por el cual se transforma en una obligación de la compañía el colaborar con la sociedad para que todos sus actos estén dentro de actividades lícitas y de honestidad.

- **Riesgo físico**

La información de los clientes y los datos de los juegos de azar deben ser validados para comprobar que sea perceptible y que se encuentre en buen estado, que no sea modificada por personal no autorizado y que pongan en riesgo a la organización.

- **Riesgo Operativo**

Está emparentado en forma directa con la función del negocio y para nuestro tema con el proceso de salud y juegos de azar, de lo que se deriva:

a) Mal de ingreso de datos de pacientes.
b) Mal en el diseño del producto de juegos de azar.
c) Mal establecimiento de políticas inadecuadas de seguridad.

3.2 INFRAESTRUCTURA DE LA EMPRESA

La empresa a nivel de infraestructura de TI está dividida en 4 grandes dependencias desde donde se centralizan todos los departamentos a nivel del negocio, para nuestro caso por la implementación de WSUS y por ser directamente sobre productos Microsoft hemos detallado en el siguiente grafico la distribución del domino principal.

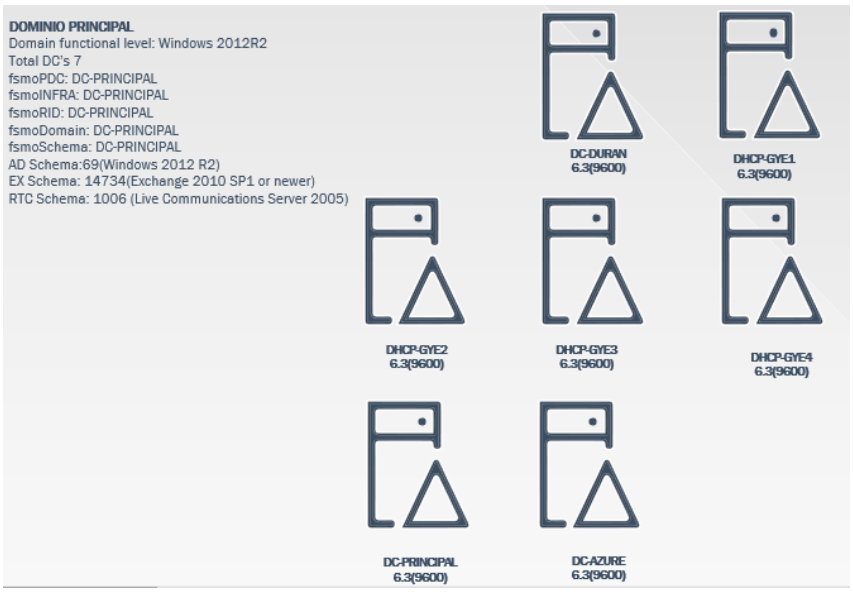


FIGURA 3.1 Distribución de Dominio Principal
Fuente: Autor

Tabla 1 Detalle de Domains Controllers
Fuente: Autor

Dominio	Domain Controllers	Relación de Confianza	Nivel Funcional Dominio	Nivel Funcional Forest
Central	7	N/A	Windows Server 2012 R2	Windows Server 2012 R2

Tabla 2 Configuración de Domains Controllers
Fuente: Autor

Central	
Versión Esquema AD	69 (Windows 2012 R2)
Versión Esquema EX	14734 (Windows 2010 SP1)
Schema master	DC-Principal
Domain naming master	DC-Principal
RID master	DC-Principal
PDC emulator	DC-Principal
Infrastructure master	DC-Principal
NetBIOS Name	CENTRAL
Total DC's	7
Total Site	6

Se han identificado 7 controladores de dominio, donde el principal se encuentra ubicado en datacenter Duran, en este datacenter se tiene un controlador de domino secundario como contingencia en modo activo-activo, adicional existe un controlador de dominio ubicado en la nube específicamente en el servicio AZURE proporcionado por Microsoft, los 4 controladores restantes cumplen la función de DHCP para controlar y tener una mejor administración de los equipos y servidores de las dependencias.

Tabla 3 Distribución de Domains Controllers
Fuente: Autor

Sitios (central)		
Sitio	**Nombre DC**	**Cantidad**
GYE1	DHCP-GYE1	1

Sitios (central)		
Sitio	**Nombre DC**	**Cantidad**
Duran	DC-Principal DC-Duran	2
GYE2	DHCP-GYE2	1
Azure	DC-Azure	1
GYE3	DHCP-GYE3	1
GYE4	DHCP-GYE4	1

En la infraestructura actual de la organización se realizó un levantamiento de información de los servidores que actualmente brindan servicio, de los cuales se detectó 253 son sistemas operativos Microsoft, y estos se los divide en dos grupos de servidores, servidores de producción y servidores de desarrollo.

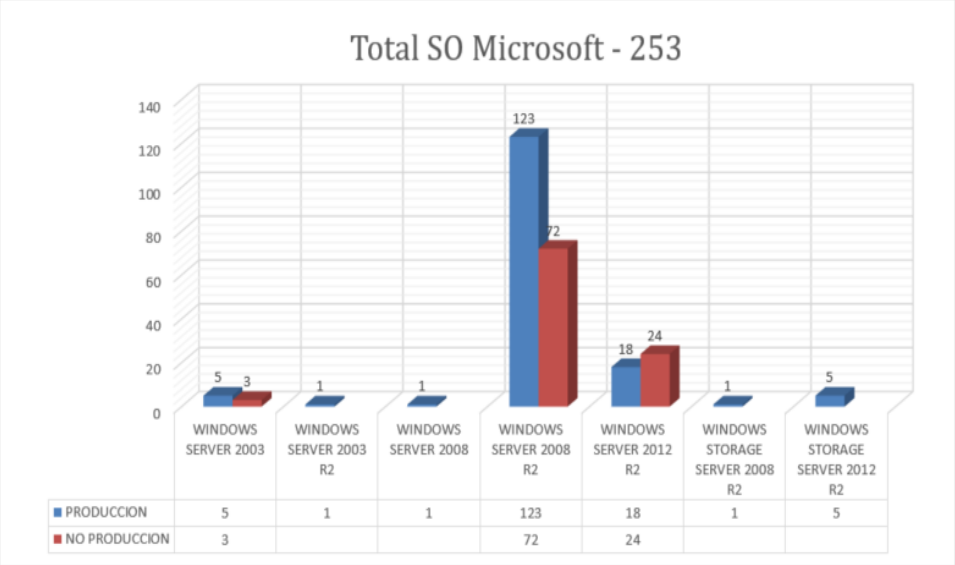


FIGURA 3.2 Distribución de Servidores Microsoft
Fuente Autor

Toda las capacidades y números de estos servidores corresponden a la infraestructura existente que ha sido provista por la organización, por lo cual estar propenso a cambias a lo largo del proyecto.

3.3 PROCESO ACTUAL DE PARCHADO

La organización no cuenta con un sistema centralizado ni administrado para la aplicación de parches, en este caso los servidores se parchan en un modo reactivo en lugar de un modo proactivo, esto debido a que el departamento de sistemas no podía manejar el volumen de parches que se liberan a una velocidad inmanejable, se tiene dificultad para determinar que parche debe ser aplicado por lo que la administración era casi nula.

Algunos servidores tienen salida a internet por lo cual el servicio de Windows Update se conecta directamente a internet y descarga parches, esto provoca un alto consumo de ancho de banda, y caída de servicios en servidores de producción, al no tener un control sobre los parches se instalaban acorde llegaban desde la web de Microsoft esto adicional al reinicio provocaba que algunas aplicaciones fallen y no se tenía plan de reverso para estos parches.

La problemática que se tiene es muy crítica, ya que afecta tanto a la operación como el negocio, a nivel de seguridad los servidores están con muchas vulnerabilidades que no pueden ser controladas, el parchado no se encuentra como proceso y esto hace que existan muchas quejas al departamento de sistemas, ya sea desde los usuarios hasta la alta gerencia.

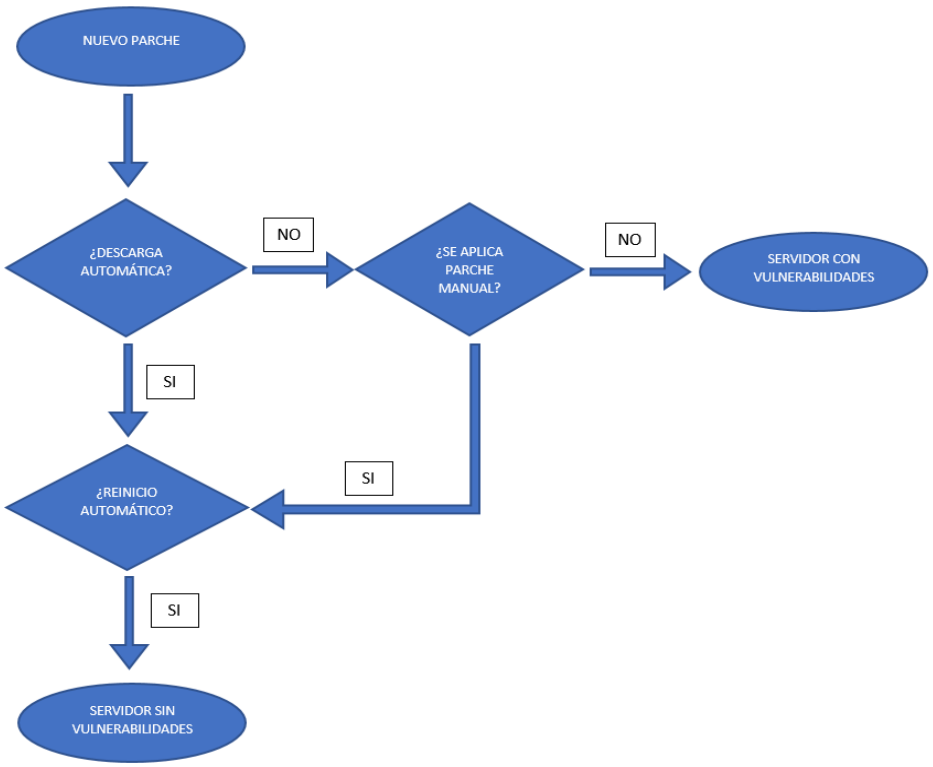


FIGURA 3.3 Proceso Actual de Parchado
Fuente: Autor

3.4 IDENTIFICACION DE AMENAZAS

Según lo indicado por el libro Magerit las amenazas son “cosas que ocurren”. Y, de todo lo pueda ocurrir, interesa lo que pueda pasar a nuestros activos. Basado en Magerit los activos son “Componentes o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos”. Los activos informáticos son una parte fundamental de una organización, por este motivo deben ser identificados para lograr determinar el grado de criticidad y exposición y en base a esto

establecer políticas a implementar para que no sean vulnerables a cualquier amenaza y ponga en riego el negocio, tanto operativo como financiero.

Bajo el concepto Magerit para un análisis de riesgo e identificación de amenazas primero debemos determinar los activos relevantes para nuestra organización, su interrelación y su valor, en el sentido del coste que supondría su degradación. A continuación, enlistamos los activos involucrados en el proceso de parchado:

Tabla 4 Identificación de Activos
Fuente: Autor

ID.	Activo	Tipo
1	Servidores	Hardware
2	Computadores/Laptops	Hardware
3	Sistemas Operativos	Software/ Información
4	Aplicaciones Corporativas	Software/ Información
5	Aplicaciones de Terceros	Software/ Información
6	Sitios Webs	Servicio
7	Servicio de correo electrónico	Servicio
8	Red de área local e inalámbrica	Comunicaciones
9	Administradores de Sistemas	Personal
10	Usuarios	Personal
11	Desarrolladores	Personal

La valoración del activo es algo muy crítico, con esto podemos determinar qué tan impórtate es un activo para la organización y cuál es el nivel de protección que necesitamos en la dimensión de seguridad que sean necesarios, para un activo debemos dimensionar su valor en base a su confidencialidad, su integrada y su disponibilidad.

Para realizar la valoración de los activos referente al proceso de parchado nos guiaremos de la siguiente tabla:

Tabla 5 Tabla de valoración de activos
Fuente: Autor

Valor			Criterio
5	Muy alto	MA	Daño muy grave a la organización.
4	Alto	A	Daño grave a la organización.
3	Medio	M	Daño importante a la organización.
2	Bajo	B	Daño menor a la organización.
1	Muy Bajo	MB	Irrelevante a efectos prácticos.

Tabla 6 Valoración de Activos
Fuente: Autor

Activo	Dimensiones			
	[D]	[I]	[C]	[VA]
Servidores	5	5	5	5
Computadores/Laptops	3	5	5	4.33
Sistemas Operativos	5	5	5	5
Aplicaciones Corporativas	4	4	4	4
Aplicaciones de Terceros	3	3	5	3.66
Sitios Webs	4	3	3	3.33
Servicio de correo electrónico	4	5	5	4.66
Red de área local e inalámbrica	4	4	4	4
Administradores de Sistemas	5	5	4	4.66
Usuarios	3	3	4	3.33
Desarrolladores	3	3	5	3.66

Bajo el concepto de que las amenazas es la posibilidad de que una vulnerabilidad afecte a nuestros activos; es de suma importancia identificarlas para la creación y validación de procesos que permitan mitigarla. De acuerdo con lo indicado en Magerit entre las amenazas más comunes tenemos:

- De origen natural: Terremotos, inundaciones o desastres de tipo natural.
- Del entorno: Contaminación, fallos eléctricos o cualquier anomalía de tipo industrial.
- De defecto: Defectos de aplicaciones y problemas técnicos en equipos.
- De forma accidental: Causado por personas por problemas no intencionados.
- De forma deliberada: Causadas por problemas intencionales con ánimo de causar daño.

Los activos cuando son víctimas de amenazas no necesariamente se ven afectados en todas sus dimensiones, por ello se tiene que valorar su influencia en el daño que pueden cuásar por un incidente en el caso que ocurra, por esta razón hay que valorar el activo en dos sentidos:

- Degradación: cuán perjudicado resultaría el valor del activo.
- Probabilidad: cuán probable o improbable es que se materialice la amenaza.

FIGURA 3.4 Elementos de análisis del riesgo
Fuente: www.secureit.es

En la siguiente tabla, se listan los activos con sus amenazas y respectivas vulnerabilidades:

Tabla 7 Identificación de Amenazas y Vulnerabilidades
Fuente: Autor

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada
Servidores	5	Infección de sistema	Ausencia de política de parchado
		Acceso privilegiado a Bases de Datos	
		Perdida de datos relevante para el negocio	
		Accesos privilegiados a aplicaciones del negocio	
		Robo de contraseñas	
		Acceso a la infraestructura de la red	
		Caída del sistema por agotamiento de recursos	
Computadores y Laptops	4.33	Perdida de datos relevante para el negocio	Ausencia de política de parchado
		Infección de sistema	
		Control de equipo por personal no autorizado	
		Ataques DOS	
		Manejo inadecuado de contraseñas	

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada
		Amenaza lógica	
Sistemas Operativo	5	Ataques de Hackers	Ausencia de política de parchado
		Ataques de virus y malware	
		Perdida de datos relevante para el negocio	
		Mal uso del equipo	
		Pérdida total de sistema operativo	
Aplicaciones Corporativas	4	Ataques de exploit por mal diseño de aplicaciones	Ausencia de política de parchado
		Perdida de datos relevante para el negocio	
		Afectación a aplicaciones financieras	
		Transacciones no autorizadas	
Aplicaciones de Terceros	3.66	Errores en la implementación	Ausencia de política de parchado
		Perdida de datos relevante para el negocio	
		Ataques de fallas de seguridad	
		Transacciones no autorizadas	
Sitios Webs	3.33	Caída de los servicios web, afectando el negocio	Ausencia de política de parchado
		Exposición de datos privados	
		Perdida de datos relevante para el negocio	
Servicio de correo electrónico	4.66	Spam	Ausencia de política de parchado
		Phishing	
		Propagación de códigos maliciosos	
		Spoofing	
		Ataque man-in-the-middle	
		Ataque DOS	
		Perdida de datos relevante para el negocio	
Red de área local e inalámbrica	4	Accesos no autorizados	Ausencia de política de parchado
		Caída de los enlaces y servicios	
		Transacciones no autorizadas	
Administradores de Sistemas	4.66	Manejo inadecuado de contraseñas	Ausencia de política de parchado
		Errores en configuraciones de sistemas	

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada
		Perdida de datos relevante para el negocio	
Usuarios	3.33	Manejo inadecuado de contraseñas	Ausencia de política de parchado
		Perdida de datos relevante para el negocio	
		Perdida de datos por errores	
Desarrolladores	3.66	Ataques mediante exploit por mal diseño de software	Ausencia de política de parchado
		Manejo inadecuado de contraseñas	
		Perdida de datos relevante para el negocio	

3.5 CÁLCULO DE PROBABILIDAD DE LAS AMENAZAS

Para el cálculo de la probabilidad de las amenazas deberemos tener presente lo validado en el capítulo anterior donde identificamos las amenazas y vulnerabilidades, se modelará la probabilidad de ocurrencia de una amenaza de manera numérica, tomando como guía la tabla de ocurrencia de Magerit., de esta manera quedaría:

Tabla 8 Tabla de Probabilidad de Ocurrencia
Fuente: Libro I MAGERIT PAG. 28

CÓDIGO	OCURRENCIA	FRECUENCIA	PROBABILIDAD	VALOR
MA	100	MUY FRECUENTE	A DIARIO	5
A	10	FRECUENTE	MENSUALMENTE	4
M	1	NORMAL	UNA VEZ AL AÑO	3
B	1/10	POCO FRECUENTE	CADA VARIOS AÑOS	2
MB	1/100	MUY POCO FRECUENTE	SIGLOS	1

Para el nivel de aceptación del riesgo nos manejaremos con las tablas que se muestran a continuación:

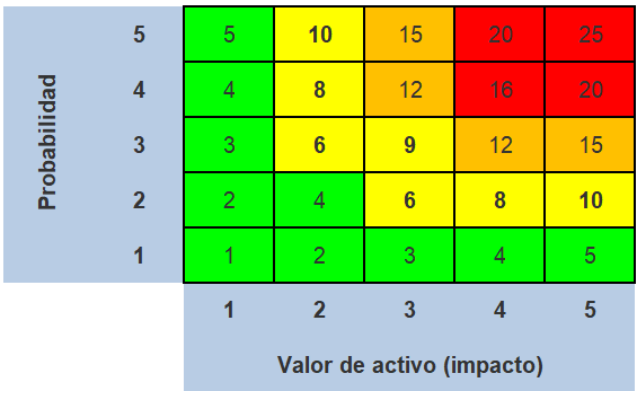


FIGURA 3.5 Matriz de Aceptación de Riesgo
Fuente: autor

Tabla 9 Niveles de Tratamiento del Riesgo
Fuente: Autor

RIESGO	NIVEL	TRATAMIENTO DEL RIESGO
1 - 5	Aceptable	Finaliza el proceso, no es necesario controles
6 – 10	Tolerable	Necesario control para subir a nivel de aceptación
11 – 15	Intolerable	Necesario control para subir a nivel de aceptación
16 - 25	Extremo	Necesario control para subir a nivel de aceptación

Tabla 10 Cálculo de Probabilidad de las Amenazas
Fuente: Autor

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada	P	R
Servidores	5	Infección de sistema	Ausencia de política de parchado	4	20
		Acceso privilegiado a Bases de Datos			
		Perdida de datos relevante para el negocio			
		Accesos privilegiados a aplicaciones del negocio			

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada	P	R
		Robo de contraseñas			
		Acceso a la infraestructura de la red			
		Caída del sistema por agotamiento de recursos			
Computadores y Laptops	4.33	Perdida de datos relevante para el negocio	Ausencia de política de parchado	4	17.3
		Infección de sistema			
		Control de equipo por personal no autorizado			
		Ataques DOS			
		Manejo inadecuado de contraseñas			
		Amenaza lógica			
Sistemas Operativo	5	Ataques de Hackers	Ausencia de política de parchado	4	20
		Ataques de virus y malware			
		Perdida de datos relevante para el negocio			
		Mal uso del equipo			
		Pérdida total de sistema operativo			
Aplicaciones Corporativas	4	Ataques de exploit por mal diseño de aplicaciones	Ausencia de política de parchado	4	16
		Perdida de datos relevante para el negocio			
		Afectación a aplicaciones financieras			
		Transacciones no autorizadas			
Aplicaciones de Terceros	3.66	Errores en la implementación	Ausencia de política de parchado	4	14.6
		Perdida de datos relevante para el negocio			
		Ataques de fallas de seguridad			
		Transacciones no autorizadas			
Sitios Webs	3.33	Caída de los servicios web, afectando el negocio	Ausencia de política de parchado	3	9.99

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada	P	R
		Exposición de datos privados			
		Perdida de datos relevante para el negocio			
Servicio de correo electrónico	4.66	Spam	Ausencia de política de parchado	3	13.9
		Phishing			
		Propagación de códigos maliciosos			
		Spoofing			
		Ataque man-in-the-middle			
		Ataque DOS			
		Perdida de datos relevante para el negocio			
Red de área local e inalámbrica	4	Accesos no autorizados	Ausencia de política de parchado	4	16
		Caída de los enlaces y servicios			
		Transacciones no autorizadas			
Administradores de Sistemas	4.66	Manejo inadecuado de contraseñas	Ausencia de política de parchado	4	18.6
		Errores en configuraciones de sistemas			
		Perdida de datos relevante para el negocio			
Usuarios	3.33	Manejo inadecuado de contraseñas	Ausencia de política de parchado	4	13.3
		Perdida de datos relevante para el negocio			
		Perdida de datos por errores			
Desarrolladores	3.66	Ataques mediante exploit por mal diseño de software	Ausencia de política de parchado	3	10.9
		Manejo inadecuado de contraseñas			
		Perdida de datos relevante para el negocio			

3.6 PLAN DE TRATAMIENTOS DE RIESGOS

Al analizar los resultados de los riesgos, es necesario establecer un plan de tratamiento de riesgos, para ello es necesario aplicar controles para disminuirlo y

con ello evitar que la organización este expuesta a nivel operativo y minimizar el impacto financiero.

Para Magerit las salvaguarda o controles son procedimientos o mecanismos tecnológico que reducen el riesgo, las medidas que se tomen ayudaran a mejorar la operatividad de la organización. Por este motivo es que dichos riegos deben ser evaluados de acuerdo con su importancia.

El efecto que tendrán estos controles entra en el cálculo del riesgo en dos formas:

- ✓ Reduciendo la probabilidad de las amenazas.
- ✓ Limitando el daño causado.

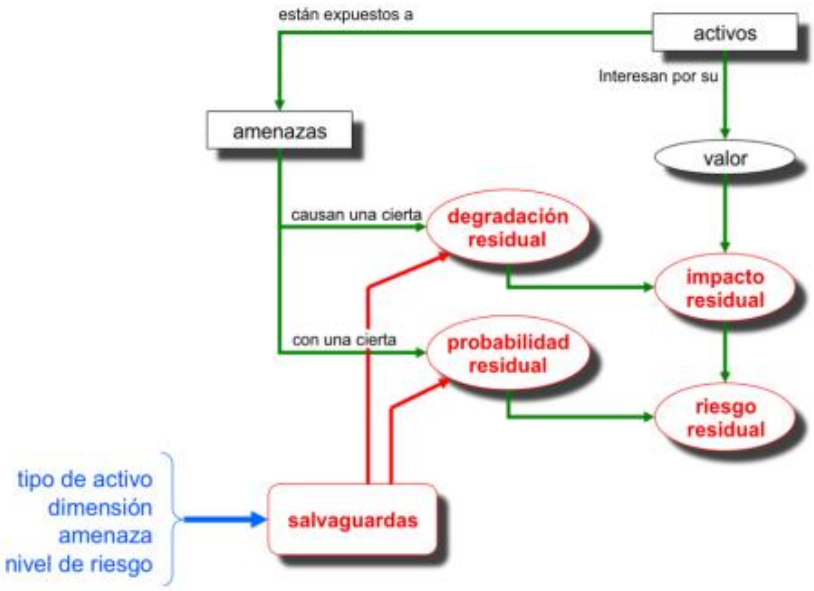


FIGURA 3.6 Elementos de análisis del riesgo residual
Fuente: MAGERIT

No todos los riesgos se generan igual y como vimos en la probabilidad de del riesgo no todos tienen el mismo impacto, para esto debemos tomar mediad que ayuden reducir o eliminar estos riegos y así salvaguardar la integridad y el desempeño de la empresa, para ello se manejan las siguientes formas para mitigar los riesgos:

a) Reducir el riesgo

Aplicar controles, como guía se puede usar el anexo A del ISO 27001.

b) Transferir el riesgo

Transferir el riesgo a otra parte, es decir tratar de asignar a terceros para que asuman el compromiso de velar por la seguridad.

c) Eliminar el riesgo

Tratar de eliminar una actividad o un proceso que causa el incidente.

d) Aceptar el riesgo

Cuando tratar de eliminar un riesgo tiene un costo muy alto para la organización existe la posibilidad de convivir con el riesgo, pero tratando de minimizar el mismo.

Para nuestra implementación aplicaremos el tratamiento de reducir el riesgo basándonos en los controles sugeridos por el anexo A de la norma ISO27001, pero cabe recalcar que no es posible bloquear todos los riesgos y que siempre existirá un riesgo residual, por ello es importante definir las políticas y soluciones para mitigar en lo más posible riesgo.

Tabla 11 Controles para el tratamiento del riesgo
Fuente: Autor

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada	P	R	Controles	
						Tratamiento del riesgo	Salvaguardas
Servidores	5	Infección de sistema Acceso privilegiado a Bases de Datos Perdida de datos relevante para el negocio Accesos privilegiados a aplicaciones del negocio Robo de contraseñas Acceso a la infraestructura de la red Caída del sistema por agotamiento de recursos	Ausencia de política de parchado	4	20	Reducción	• A.11.1.4 Protección contra amenazas externas y ambientales. • A.11.2.4 Mantenimiento de equipos. • A.11.2.8 Equipos de usuario desatendido. • A.5.1.1. Políticas para la seguridad de la información. • A.6.1.1 Roles y responsabilidades para la seguridad de la información. • A.6.1.2 Segregación de deberes. • A.7.1.2 Términos y condiciones del empleo. • A.7.2.2 Concienciación en la Seguridad de información, educación y entrenamiento. • A.8.1.1 Inventario de equipos.
Computadores y Laptops	4.33	Perdida de datos relevante para el negocio Infección de sistema Control de equipo por personal no autorizado Ataques DOS Manejo inadecuado de contraseñas	Ausencia de política de parchado	4	17.3	Reducción	

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada	P	R	Controles	
						Tratamiento del riesgo	Salvaguardas
		Amenaza lógica					• A.8.2.3 Manejo de activos. • A.9.1.1 Política de control de acceso. • A.9.2.3 Gestión de derecho de acceso privilegiado. • A.9.4.3 Sistema de control de contraseñas. • A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación. • A.12.1.1 Procedimientos de operación documentada. • A.12.2.1 Controles de código malicioso. • A.12.3.1 Respaldo de información. • A.12.4.1 Registro de eventos. • A.12.6.1 Control de vulnerabilidades técnicas. • A.12.7.1 Controles de auditoria sistemas de información.
Sistemas Operativo	5	Ataques de Hackers Ataques de virus y malware Perdida de datos relevante para el negocio Mal uso del equipo Pérdida total de sistema operativo	Ausencia de política de parchado	4	20	Reducción	
Aplicaciones Corporativas	4	Ataques de exploit por mal diseño de aplicaciones Perdida de datos relevante para el negocio Afectación a aplicaciones financieras Transacciones no autorizadas	Ausencia de política de parchado	4	16	Reducción	
Aplicaciones de Terceros	3.66	Errores en la implementación Perdida de datos relevante para el negocio Ataques de fallas de seguridad	Ausencia de política de parchado	4	14.6	Reducción	

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada	P	R	Controles	
						Tratamiento del riesgo	Salvaguardas
		Transacciones no autorizadas					• A.13.1.3 Segregación en redes. • A.14.2.6 Ambiente de Desarrollo seguro. • A.14.2.8 Pruebas de seguridad de sistemas. • A.16.1.1 Responsabilidades y procedimientos. • A.17.1.1 Planificación de la continuidad de la seguridad de la información. • A.18.2.2 Cumplimiento en las políticas y normas de seguridad. • .11.2.1 Instalación y protección de equipos.
Sitios Webs	3.33	Caída de los servicios web, afectando el negocio	Ausencia de política de parchado	3	9.99	Reducción	
		Exposición de datos privados					
		Perdida de datos relevante para el negocio					
Servicio de correo electrónico	4.66	Spam	Ausencia de política de parchado	3	13.9	Reducción	
		Phishing					
		Propagación de códigos maliciosos					
		Spoofing					
		Ataque man-in-the-middle					
		Ataque DOS					
		Perdida de datos relevante para el negocio					
Red de área local e inalámbrica	4	Accesos no autorizados	Ausencia de política de parchado	4	16	Reducción	
		Caída de los enlaces y servicios					
		Transacciones no autorizadas					
Administradores de Sistemas	4.66	Manejo inadecuado de contraseñas	Ausencia de política de parchado	4	18.6	Reducción	

Activo	Valor del Activo	Amenaza	Vulnerabilidad asociada	P	R	Controles	
						Tratamiento del riesgo	Salvaguardas
		Errores en configuraciones de sistemas					
		Perdida de datos relevante para el negocio					
Usuarios	3.33	Manejo inadecuado de contraseñas	Ausencia de política de parchado	4	13.3	Reducción	
		Perdida de datos relevante para el negocio					
		Perdida de datos por errores					
Desarrolladores	3.66	Ataques mediante exploit por mal diseño de software	Ausencia de política de parchado	3	10.9	Reducción	
		Manejo inadecuado de contraseñas					
		Perdida de datos relevante para el negocio					

CAPÍTULO 4

ANÁLISIS Y DISEÑO

Para nuestro proyecto aplicaremos un Framework ágil que incluye la metodología SCRUM adoptando herramientas y actividades de la guía de proyectos PMBOK, con SCRUM definiremos los roles y actividades del proyecto, dentro del proceso Sprint no se define y no se explica el desarrollo de estas reuniones por esto incluiremos PMBOK para el desarrollo.

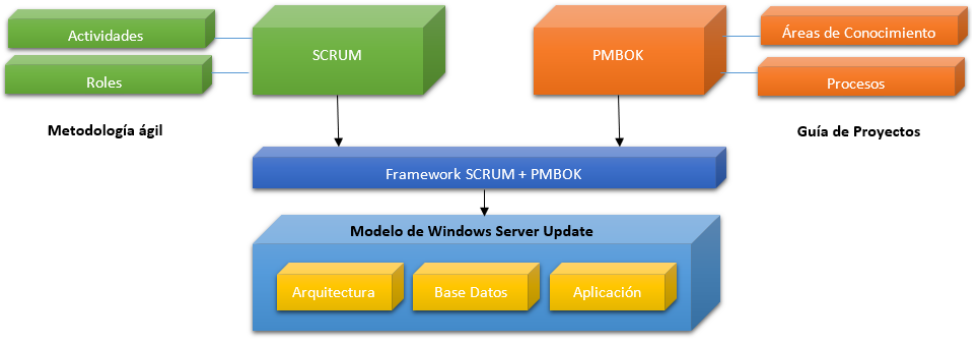


FIGURA 4.1 Framework a usar en el proyecto
Fuente: Autor

Para aplicar la metodología SRCUM hemos definidos las siguientes etapas y roles en la reunión de la planificación del sprint:

- **Product Backlog**

En la reunión inicial, se presentó el problema de no contar con un proceso de parchado, mostrando la información del análisis de riesgo y el daño que produciría no mitigar este riesgo, se facilitó varias propuestas de implementación de WSUS al cliente y se definió un proceso inicial y los roles respectivos siguiendo la metodología SCRUM.

- **Product Owner**

El product owner será el coordinador del área de seguridad de la organización, en este caso el cliente designo este cargo, el mismo será encargado de conseguir una buena definición de los objetivos del proyecto.

- **Scrum Master**

Sera el encargado de dirigir al equipo y velar para que el proyecto siga las reglas de SCRUM, en las reuniones será el encargado de moderar los temas.

- **Equipo (Team)**

El equipo estará confirmado por dos personas que pertenecen al grupo al grupo de los ejecutores y 2 personas que pertenecen al grupo de la organización y serán los encargados del desarrollo e implementación de WSUS, en este equipo se incluye el Product Owner y Scrum Master.

- **Sprint Backlog**

En una segunda reunión en la que SCRUM denomina Sprint Backlog o lista de tareas, se elabora cronograma de actividades con la intención de completar los objetivos y requisitos para demostrar al cliente la finalización del proyecto, dentro de esta reunión se definen los procesos PMI del PMBOK.

- **Sprint**

El sprint o iteraciones se denomina a las reuniones planificadas para proporcionar resultados del avance del proyecto, dentro de la planificación con la organización se definió 4 semanas para la conclusión del proyecto, cada día se realizarán pequeñas reuniones para verificar avances.

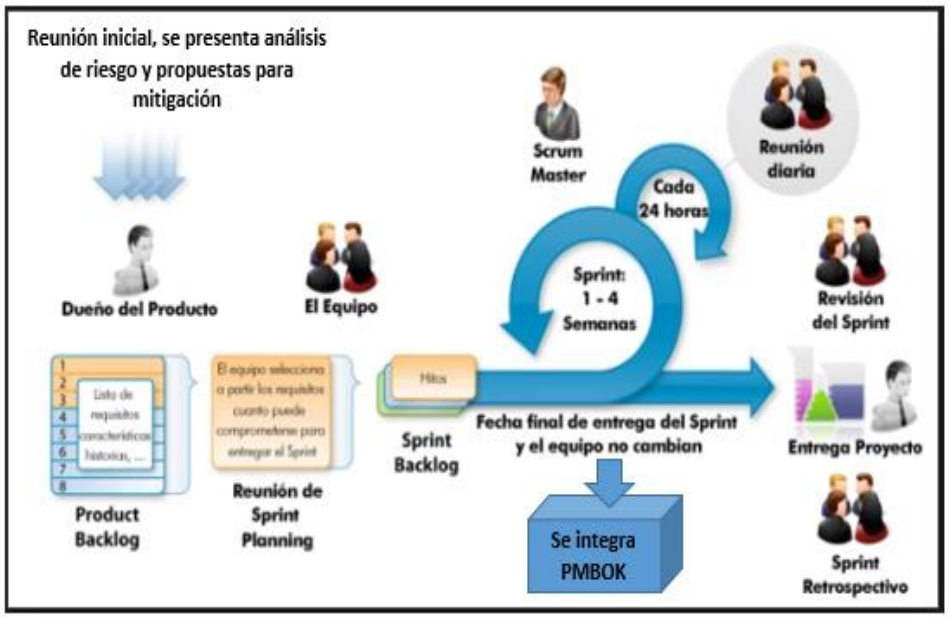


FIGURA 4.2 Diseño de Framework SCRUM + PMI en el proyecto WSUS
Fuente: Autor

Para completar nuestro Framework debemos incluir PMI como guía del proyecto, SCRUM al ser una metodología ágil no especifica cómo llevar el proyecto dentro de los sprints, es por esto que se deicidio implementar estas guías, PMI es muy extenso, pero nos centraremos en los 5 procesos principales que son, iniciación, planificación, ejecución, seguimiento-control y cierre.

PMI maneja áreas de conocimientos que son un conjunto de buenas prácticas en dirección de proyectos, las mismas que se detallan a continuación:

- Gestión de la integración.
- Gestión del alcance.
- Gestión del tiempo.
- Gestión de los costos.
- Gestión de la calidad.
- Gestión de los recursos humanos.
- Gestión de las comunicaciones.
- Gestión de los riesgos.
- Gestión de las adquisiciones.
- Gestión de los interesados.

En base a los procesos y las áreas de conocimiento se definió la siguiente matriz con la cual se inició el proyecto:

Tabla 12 Matriz de guía del proyecto
Fuente: Autor

ÁREA DE CONOCIMIENTO	INICIACIÓN	PLANIFICACIÓN	EJECUCIÓN	SEGUIMIENTO Y CONTROL	CIERRE
Gestión de la integración	Desarrollo del acta de constitución del proyecto	Desarrollo del plan de la dirección del proyecto	Dirigir y gestionar la ejecución de proyecto	Dar seguimiento y controlar el trabajo del proyecto	Cerrar proyecto o fases
Gestión del alcance		Recopilar requisitos		Validar y controlar el alcance	
Gestión del tiempo		Planificar el cronograma, definir actividades, estimar duración de actividades		Controlar el cronograma	
Gestión de los costos		Estimar costos		Controlar los costos	
Gestión de la calidad		Planificar la gestión de calidad	Realizar el aseguramiento de la calidad	Controlar la calidad	
Gestión de los recursos humanos			Planificar los recursos del proyecto		
Gestión de las comunicaciones	Identificar interesados	Planificar la gestión de las comunicaciones	Gestionar las comunicaciones del proyecto	Controlar las comunicaciones	
Gestión de los riesgos		Planificar e identificar los riesgos		Controlar los riesgos	
Gestión de las adquisiciones		Planificar la gestión de las adquisiciones	Ejecutar las adquisiciones	Controlar las adquisiciones	Cerrar adquisiciones
Extremo Gestión de los interesados	Identificar stakeholders			Gestionar la relación con los interesados	

4.1 TIPOS DE IMPLEMENTACIÓN DE WSUS

Luego de haber realizado un levantamiento de información, donde se incluía el análisis de amenazas y la probabilidad del riesgo que esto implicaba por la vulnerabilidad de no tener un proceso y políticas para la gestión de actualizaciones,

es necesario analizar los posibles escenarios para diseñar un ambiente que solvente esta necesidad.

La implementación más básica de WSUS consiste en un servidor dentro de la red corporativa que sirve como distribuidor de actualizaciones a las computadoras y servidores de la red privada, como se muestra en la Figura 4.3. El servidor WSUS se conecta a Microsoft Update en el internet para descargar actualizaciones. Esto se conoce como sincronización. Durante la sincronización, WSUS determina si hay actualizaciones nuevas disponibles desde la última vez que sincronizó. Si es la primera vez que sincroniza WSUS, todas las actualizaciones estarán disponibles para su descarga.

De forma predeterminada, el servidor WSUS usa el puerto 80 para el protocolo HTTP y el puerto 443 para el protocolo HTTPS para obtener actualizaciones de Microsoft. Para nuestro diseño, se deberá abrir estos puertos desde el firewall hasta el servidor para tener comunicación directa con el sitio de actualizaciones. Predeterminadamente, WSUS usa el puerto 8530 para el protocolo HTTP y el puerto 8531 para el protocolo HTTPS para gestionar actualizaciones a las estaciones y servidores.

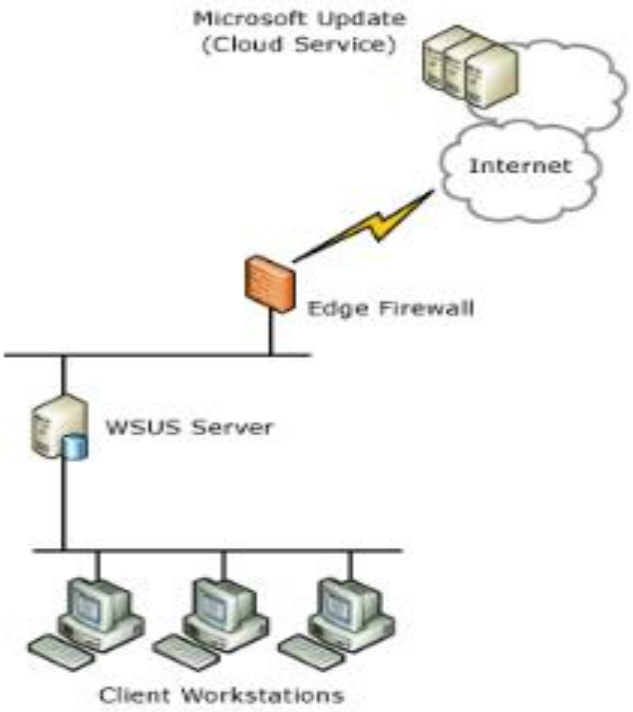


FIGURA 4.3 Diseño básico de WSUS
Fuente: Autor

Adicional se tiene un diseño donde se pueden implementar varios servidores que ejecutan WSUS y que sincronizan todo el contenido dentro de la red interna de la organización. En la Figura 4.2**,** solo un servidor está expuesto a Internet, este es el único servidor que descarga actualizaciones de Microsoft Update. Este servidor está configurado como el servidor ascendente y es la fuente desde donde se sincronizan los servidores descendentes. Con este diseño se tendría una mejor distribución de localidades en caso de crecimiento fuera de la ciudad de Guayaquil.

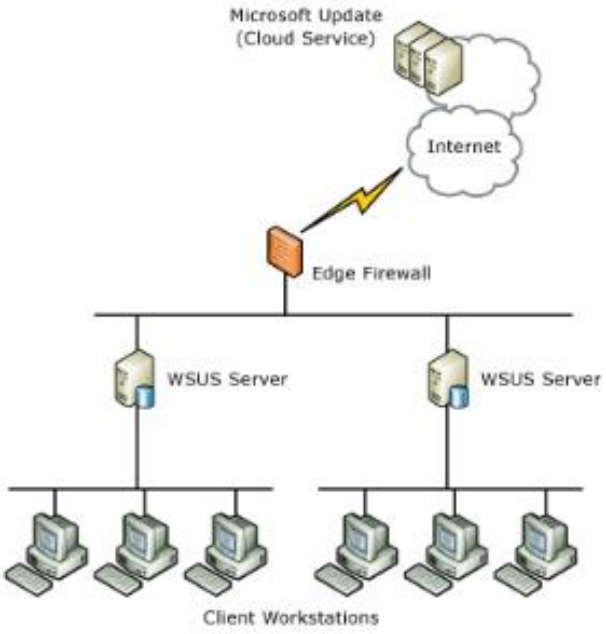


FIGURA 4.4 Diseño Múltiples Servidores de WSUS
Fuente: Autor

Para nuestro alcance del proyecto y de la organización se optará por la implementación de un diseño básico de WSUS, con esto se garantizará un bajo costo tanto en la implementación como en la operación, ya que al no contar la organización con sucursales fuera de la ciudad no es necesario expandir por el momento a más servidores WSUS.

4.2 TIPO DE ADMINISTRACIÓN DE WSUS

La administración de WSUS es uno de los puntos más importantes a la hora de implementar el proyecto, al ser una herramienta muy flexible los administradores tendrán una consola centralizada donde se debe verificar regularmente la página de inicio para ver el cumplimiento general de las actualizaciones y el estado de la red. Se podrá comprobar los registros de frecuencia de aplicación de

actualizaciones y demás errores que podrían causar el mal desempeño de la herramienta.

La administración de las actualizaciones que se generan mediante una sincronización entre el servidor WSUS e internet, se da mediante la descarga (metadatos y archivos de actualización) desde una fuente de actualización (Microsoft Update). También descarga nuevas clasificaciones y categorías de productos, los mismos pueden ser administradores y modificados según sea el caso de la necesidad de la organización. Cuando el servidor WSUS se sincroniza por primera vez, descargará todas las actualizaciones que haya especificado al configurar las opciones de sincronización. Después de la primera sincronización, el servidor WSUS solo descarga las actualizaciones de la fuente de actualización, así como las revisiones de los metadatos de las actualizaciones existentes y los vencimientos de las actualizaciones. La ubicación del directorio de las actualizaciones se especifica cuando ejecuta el procedimiento de instalación posterior a WSUS.

Dentro de la consola de administración encontraremos el nodo de Equipos que es punto central para administrar los equipos y dispositivos cliente de WSUS, debajo de esto se puede encontrar los diferentes grupos que se han configurado, adicional se encontrara el grupo Equipos no asignados que es el predeterminado donde encontraremos todos los equipos que se conecten al WSUS, desde aquí podremos organizarlos en los grupos correspondientes para una mejor organización.

Desde el nodo de Updates se administrará todo el catálogo de actualizaciones, desde este nodo podremos ver, filtrar, buscar, aprobar y declinar actualizaciones, dentro del catálogo de Microsoft una actualización o parche se compone de dos componentes:

- Metadata: Proporciona toda la información sobre la actualización, por ejemplo, las propiedades, los términos de licencia.
- Update files: Es el archivo real de la actualización necesario para la instalación.

Las actualizaciones disponibles en Microsoft se diferencian por producto y clasificación. Un producto es una edición especifica de un sistema operativo o aplicación. Las clasificaciones representan el tipo de actualización.

Tabla 13 Tabla de clasificación de actualizaciones
Fuente: Autor

Clasificación	Descripción
Critical Updates	Actualizaciones lanzadas para problemas críticos no relacionados con seguridad.
Definition Updates	Actualizaciones a definición de archivos (Windows Defender).
Drivers	Actualizaciones para admitir nuevos drivers.
Feature packs	Nuevas características para productos incorporados Microsoft.
Security updates	Soluciones para productos específicos, generalmente solucionan problemas de seguridad.
Service packs	Paquetes acumulativos de todas las revisiones de seguridad, actualizaciones críticas y actualizaciones lanzadas desde la creación del producto.
Tools	Utilidades o características que ayuda a mejorar una tarea para los productos Microsoft.
Update rollups	Conjunto de revisiones acumulativas que se empaquetan para facilitar su implementación. Dirigidas a un producto específico.
Updates	Soluciones para problemas específicos que abordan errores no críticos, que no están relacionados con la seguridad.

Después de sincronizar las actualizaciones con el servidor WSUS, se analizarán automáticamente en busca de relevancia para las computadoras cliente del servidor. Sin embargo, se debe aprobar las actualizaciones antes de

implementarlas en las estaciones y servidores. Cuando se aprueba una actualización, básicamente se le dice a WSUS qué hacer con ella (Instalar o Rechazar una nueva actualización). Se puede aprobar actualizaciones para el grupo Todos los equipos o para subgrupos. Si se no aprueba una actualización, su estado de aprobación permanece No aprobado, y el servidor WSUS permite a las estaciones y servidores evaluar si necesitan o no la actualización.

Dentro de las operaciones de actualizaciones tenemos:

- Aprobar Actualizaciones.
- Rechazar Actualizaciones.
- Reinstalar Actualizaciones Rechazadas.
- Cambiar una actualización aprobada a no aprobada.
- Aprobar actualizaciones para eliminar.

4.3 TIPO DE BASE DE DATOS PARA WSUS

WSUS utiliza dos tipos de sistemas de almacenamiento: una base de datos para almacenar la configuración de WSUS y metadatos de actualización, y un sistema de archivos local opcional para almacenar archivos de actualización. Antes de instalar WSUS, debemos decidir cómo se desea implementar el almacenamiento.

WSUS requiere una base de datos por cada servidor WSUS que se implemente, dentro de las versiones que soporta tenemos las siguientes:

- Windows Internal Database (WID).
- Microsoft SQL 2016.
- Microsoft SQL 2014.
- Microsoft SQL 2012.

- Microsoft SQL 2008 R2.

La base de WSUS almacena la siguiente información:

- Información de configuración del servidor WSUS.
- Metadatos que describe cada actualización.
- Información sobre computadoras cliente, actualizaciones e interacciones.

Durante la instalación de WSUS tenderemos la opción de escoger el motor de base de datos que usaremos, los mismos podrían ser instalados en el mismo servidor, para nuestra implementación y por costos de licencia se usara la base WID incluida en el producto, con esto tendremos capacidad para soportar el crecimiento a futuro de las dependencias y servicios de la organización.

4.4 ALMACENAMIENTO WSUS

WSUS puede almacenar archivos de actualización en el servidor WSUS local o se puede configurar para dejar actualizaciones aprobadas en los servidores web Microsoft Update. En el primer caso, las computadoras cliente descargarán las actualizaciones aprobadas del servidor local de WSUS, opción más adecuada para nuestro proyecto. En el último caso, las computadoras cliente descargarán las actualizaciones aprobadas directamente de Microsoft Update, pero esta no es la recomendable para la organización ya que hará uso del ancho de banda de la red a Internet.

El almacenamiento interno de archivos de actualización es la opción por default cuando se instala y se configura WSUS. Esta selección ahorrara ancho de banda en la conexión corporativa a Internet ya que los equipos cliente descargan actualizaciones directamente desde el servidor WSUS local. Esta opción requiere

que el servidor tenga bastante espacio en disco para depositar todas las actualizaciones necesarias. Como mínimo, WSUS requiere 20 GB para almacenar las actualizaciones.

Dentro de nuestro análisis hemos determinado las mejores prácticas para planificar de mejor manera el uso del almacenamiento y evitar errores y problemas a futuro, las mismas se detallan a continuación:

- ✓ Se deberá asegurar que el servidor WSUS este configurado solo para descargar actualizaciones aprobados, cuando el servidor se sincronice con Microsoft Update solo descargará los metadatos y archivos de actualización de las actualizaciones que se hayan aprobado.
- ✓ Se deberá aprobar solo las actualizaciones que realmente se necesiten para la organización y limitar los productos que realmente estén dentro de la organización.
- ✓ Sincronizar solo los idiomas de actualización que realmente estén dentro de equipos clientes dentro de la organización.
- ✓ Habilitar WSUS para depurar automáticamente las actualizaciones caducadas.

4.5 OPCIONES DE ANCHOS DE BANDA

Las actualizaciones de Microsoft pueden incluir paquetes con archivos muy grande. La descarga y distribución de las actualizaciones pueden consumir gran cantidad de recursos en la red, lo que puede ocasionar un deterioro en la operación, por lo cual es muy importante que se defina un horario adecuado para la descarga, distribución y aplicación de las mismas.

Para nuestra implementación se definirá horarios no laborales mediante políticas de dominio, las mismas serán evaluadas por el cliente para su respectiva aplicación en producción.

Se definirá políticas para descargar los metadatos antes de descargar los archivos de actualizaciones. Este método se lo conoce como descargas diferidas, Es decir que una actualización solo se descargara después que se apruebe, la actualización se pospondrá al horario de instalación para optimizar el ancho de banda de la red y espacio en disco.

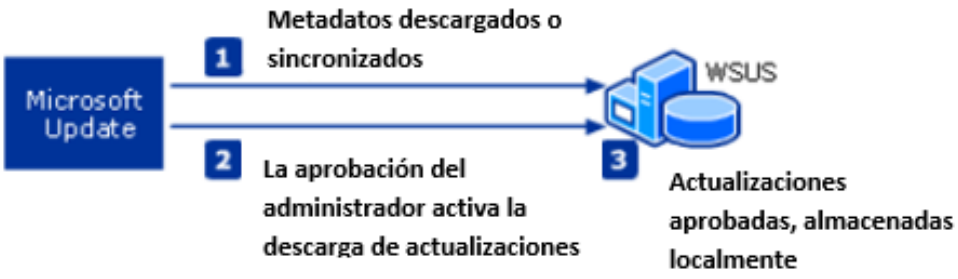


FIGURA 4.5 Descargas Diferidas de Actualizaciones
Fuente: Autor

Para nuestro caso, se implementarán grupos de servidores dentro de WSUS, con esto se controla el despliegue de las actualizaciones, se podrá crear distribuciones en horarios que no afecte la operatividad, y aprobar de forma secuencial grandes descargas.

4.6 DETERMINANDO LOS REQUERIMIENTOS DE CAPACIDAD

Basados en los requerimientos de capacidades provista por el fabricante y en base a el análisis de la organización deberemos definir un diseño que soporte la operación y capacidades, las capacidades mínimas proporcionadas por el

fabricante para un ambiente de WSUS con un servidor simple se detallan a continuación:

Tabla 14 Tabla de capacidades WSUS
Fuente: Autor

Configuración	Capacidad Máxima Soportada	Hardware y Software
Servidor único	100.000 computadoras cliente.	Hardware: Intel Core 2 Quad CPU Q6600, 2.40 GHz, 4 GB RAM o superior.
		Software: Windows Server 2008 Standard x64 Edition o superior.

4.7 INTEGRACIÓN CON ACTIVE DIRECTORY

En un entorno de Active Directory, se puede usar la directiva de grupo para definir cómo las computadoras y los usuarios se conecten e interactúen con los parches de Windows para obtener actualizaciones automáticas de WSUS.

La directiva de grupo permite especificar configuraciones administradas para los usuarios y equipos a través de la configuración de directiva de grupo y las preferencias de directiva de grupo, la administración de la configuración en un entorno de Servicios de dominio de Active Directory (AD DS) se da a través de la Consola de administración de directivas de grupo (GPMC).

Las herramientas de administración de directivas de grupo también se incluyen en el paquete de Herramientas de administración remota del servidor para poder administrar la configuración de directiva de grupo desde el escritorio.

Dentro la configuración de políticas GPO con WSUS se debe mencionar las más importantes al momento de su configuración:

- Configuración de política de actualización de Windows.
- Configuración de la política de mantenimiento.
- Configuración de la política de Windows Update.

Cada una de estas políticas contiene una configuración específica, a continuación, se detallan las más importantes:

- **Frecuencia de detección de actualizaciones automáticas**

Especifica las horas que Windows usará para determinar cuánto tiempo esperar antes de buscar actualizaciones disponibles.

- **Configurar actualizaciones automáticas**

Especifica si las actualizaciones automáticas están habilitadas para los equipos en la organización.

- **Reinicio de retardo para instalaciones programadas**

Especifica la cantidad de tiempo que las Actualizaciones automáticas esperarán antes de continuar con un reinicio programado.

- **No reiniciar con usuarios conectados para instalaciones programadas de actualizaciones automáticas**

Especifica que, para completar una instalación programada, las Actualizaciones automáticas esperarán a que cualquier usuario que inicie sesión reinicie la computadora, en lugar de hacer que la computadora se reinicie automáticamente.

- **No ajuste la opción predeterminada en "Instalar actualizaciones y apagar" en el cuadro de diálogo Cerrar Windows**

Esta configuración de directiva le permite especificar si la opción Instalar actualizaciones y Apagar está permitida como opción predeterminada en el cuadro de diálogo Cerrar Windows.

- **No mostrar la opción "Instalar actualizaciones y cerrar" en el cuadro de diálogo Cerrar Windows**

Especifica si la opción Instalar actualizaciones y Apagar se muestra en el cuadro de diálogo Cerrar Windows.

- **Vuelva a solicitar reiniciar con instalaciones programadas**

Especifica la cantidad de tiempo para que las Actualizaciones automáticas esperen antes de solicitar nuevamente con un reinicio programado.

- **Especificar la ubicación del servicio de actualización de intranet de Microsoft**

Especifica un servidor en la red interna para alojar actualizaciones de Microsoft Update. Luego se puede usar WSUS para actualizar automáticamente las computadoras en la red.

4.8 DEFINICIÓN DE POLÍTICAS DE APLICACIÓN DE ACTUALIZACIONES

Con el objetivo de definir políticas y normas que se utilizaran en el proceso de gestión de parches, se establecerá un acuerdo entre la organización y los ejecutores de este proyecto para la implementación del proceso de parchado, con

esto se debe reducir la exposición de los sistemas, bien en el tiempo o bien en el grado, sin provocar la aparición de nuevas fuentes de riesgo: inestabilidad, pérdida de funcionalidad, degradación del servicio o apertura de nuevos problemas y así alcanzar el menor impacto en la operación al aplicarse los parches, estas políticas y normas serán la vía oficial entre los ejecutores del proyecto y la organización.

Dentro de las políticas y normas se dividirán roles y responsabilidades de los involucrados en la entrega o soporte del proceso de gestión de parches, las responsabilidades incluyen, pero no se limitan a los enumerados para cada función, es decir varias funciones pueden ser realizadas por el mismo individuo, a continuación, se detallan los roles definidos en el proceso para la organización:

Tabla 15 Roles y Responsabilidades Proceso de Parchado
Fuente: Autor

Rol	Responsable
Security Patch Coordinator (PC)	Ejecutores Proyecto
Security Patch Monitor (PM)	Ejecutores Proyecto
Software Specialist (SS)	Ejecutores Proyecto
Patch Advisory Creator (PAC)	Ejecutores Proyecto
Technical Security Patch Specialist (TSPS)	Ejecutores Proyecto
Service Manager (SM)	Ejecutores Proyecto
Customer Representative (CR)	Organización
Compliance Team (CT)	Ejecutores Proyecto

- **Security Patch Coordinator (PC)**

El Security Patch Coordinator es responsable de:

- ✓ Definir e implementar el proceso Global de parches de los ejecutores alineado a la política de parches acordado con la organización.
- ✓ Mantener el proceso local de parches alineado al proceso Global definido por el fabricante.
- ✓ Mantener una lista de los sistemas / plataformas / middleware / aplicaciones de acuerdo con la infraestructura de la organización.
- ✓ Gestionar la disponibilidad de parches de Seguridad para las plataformas / sistemas monitoreadas.
- ✓ Registrar las acciones realizadas.

- **Security Patch Monitor (PM)**

El Security Patch Monitor es responsable de:

- ✓ Configuración de la suscripción de monitoreo de parches de seguridad en la herramienta de notificación de parches.
- ✓ Monitoreo de alertas para los parches de Seguridad de TI para el software solicitado.
- ✓ Se informará sobre la clasificación de severidad de los parches.
- ✓ Llevar el mantenimiento de una lista de suscriptores autorizados.
- ✓ Notificación de alerta a los suscriptores autorizados.
- ✓ Mantener un registro centralizado con información de parches de seguridad.

- **Software Specialist (SS)**

El Software Specialist es responsable de:

- ✓ Garantizar la asignación correcta de los parches a una plataforma / Software dado y documentación apropiada de los mismos.
- ✓ Asesorar al administrador de la herramienta de gestión de parches sobre la lista de software, incluyendo granularidad del software utilizado en la herramienta de gestión de parches.
- ✓ Soportar al monitoreo de los parches como parte de las actividades.

- **Patch Advisory Creator (PAC)**

El Patch Advisory Creator es responsable de:

- ✓ Recibir alertas de parches para plataformas específicas.
- ✓ Creación de registros maestros de parches en la herramienta de gestión de parches a las alertas recibidas.
- ✓ Notificación a los especialistas técnicos de los parches recibidos, si no se hace de forma automática a través de la herramienta de gestión de parches.
- ✓ Llevar a cabo la verificación periódica de parches recibidos contra el Maestro de parches abiertos.
- ✓ Mantener un registro de acciones realizados con fines de seguimiento de auditoría.

- **Technical Security Patch Specialist (TSPS)**

El Technical Security Patch Specialist es responsable de:

- ✓ Monitorear y recibir la notificación de parches del Creador de los avisos de parches o de la Herramienta de gestión de parches.
- ✓ Evaluar y soportar a la organización la aplicabilidad de los parches de seguridad en base a las pruebas realizadas.
- ✓ Gestionar la evaluación y la implementación del plan técnico para los parches de seguridad, incluyendo:
    - o Llevar un Control de cambio, la instalación de revisión de seguridad, gestión de problemas con la instalación, cierre de cambio de registro, cierre el registro de parches y almacenar evidencias requeridas.
    - o Monitoreo de las notificaciones de los parches e implementar acciones dentro de los plazos de acuerdo con la política.
- ✓ Creación de una lista de plataformas y/o sistemas con información sobre los parches a aplicar, este listado será provisto al Service Manager para la notificación al cliente, siempre y cuando la notificación no sea generada automáticamente por la herramienta.
- ✓ Gestionar con la organización una extensión de tiempo para la aplicación de los parches si la obtención de la aprobación e instalación excede del plazo definido en el proceso de parches (Un mes calendario).
- ✓ Verificar que el parche se aplicó con éxito.
- ✓ Mantener un registro de acciones realizados con fines de seguimiento de auditoría.

- **Service Manager (SM)**

El Service Manager es responsable de:

- ✓ El mantenimiento de la documentación sobre el entorno de la organización que incluya una lista de los sistemas de servidores, dispositivos y software.
- ✓ Notificar al habilitador del proceso cuáles sistemas / plataformas / middleware / aplicaciones están productivas e informar sobre cualquier cambio en los sistemas / plataformas / middleware / aplicaciones.
- ✓ Notificar al administrador de la herramienta de gestión de parches de actualizaciones del perfil del cliente con el fin de hacer cambios en la herramienta de gestión de parches.
- ✓ Notificar a la organización de la recepción inicial de alertas de parches de acuerdo con la política.
- ✓ Iniciar la creación del Departamento / cuenta de cliente en la herramienta de gestión de parches.
- ✓ Mantener una lista de servidores, sistemas, dispositivos y software, o cualquier otra herramienta, si no se hace de forma automática a través de la herramienta de gestión de parches.
- ✓ Asegurar que todas las plataformas soportadas, middleware y aplicaciones están implementadas. Comunicar el riesgo a la organización de SW no soportado.
- ✓ Asegurar la comunicación de riesgos a la organización si los Parches no se pueden implementar por razones técnicas o de la organización.
- ✓ Invocar el Subproceso de extensión si es necesario.
- ✓ Implementación de la Política de Seguridad.

- **Customer Representative (CR)**

El Representante de la organización es responsable de:

- ✓ Recibir las notificaciones acerca de la disponibilidad parches y los sistemas / plataformas / middleware / aplicaciones aplicables.
- ✓ Analizar internamente, la decisión de cómo y cuándo implementar el parche.
- ✓ Mantener la comunicación con el Service Manager en todas las acciones de los parches de seguridad de acuerdo a las políticas locales.
- ✓ Proveer acuerdos y la documentación asociada necesaria para la instalación de parches según sea requerido.
- ✓ Notificar a los ejecutores, acerca de actualizaciones o el reemplazo planificado de las plataformas y/o sistemas implementados.
- ✓ Recibir, revisar y aprobar o rechazar las solicitudes de aplicación de parches y/o prórrogas.
- ✓ Aceptar los riesgos si no hay aprobación para dar continuidad a la instalación de parches.

- **Compliance Team (CT)**

El Compliance Team es responsable de:

- ✓ Apoyar a la implementación de la política de seguridad de la organización.
- ✓ Recibir, revisar y aprobar / rechazar las fechas para las extensiones de implementación de parches.
- ✓ Ponerse en contacto con el solicitante de la extensión en caso se necesiten evidencias adicionales.

Los ejecutores del proyecto serán responsables de apoyar y asesorar a la organización, para desarrollar una ventana de cambios y un proceso de gestión de parches para software de sistemas, sistemas de infraestructura de red y dispositivos bajo gestión de los ejecutores que no hayan alcanzado el final de su ciclo de vida, validado eso se deben de tener las siguientes consideraciones:

a) Se informará sobre la severidad del riesgo para los avisos de parches basado en criterios de vulnerabilidad y categorías de explotabilidad para:
    - ✓ Productos cubiertos por el servicio de los ejecutores, las severidades serán asignadas dentro de los 3 días hábiles desde la publicación del fabricante.
    - ✓ Productos no cubiertos por el servicio de los ejecutores, la severidad será asignada dentro de los 10 días hábiles desde la publicación del fabricante.

b) Se notificará al área de Seguridad de la organización, sobre los parches clasificados como de severidad alta, media y baja, publicados por el fabricante dentro de los 3 días hábiles siguientes a la determinación del nivel de gravedad del riesgo.

c) Se instalará los parches clasificados como de severidad alta, media y baja aprobados por el área de Seguridad de la Información de la organización, según un plan de implementación acordado durante una ventana regular de cambios siguiendo el proceso de gestión de cambios.

d) Se diferirá la aplicación de parches previamente cancelados por el área de Seguridad de la Información de la organización, hasta la subsiguiente ventana regular de cambios de gestión de parches o cuando sea factible su aplicabilidad según información dada por parte de la organización. Se considerará que la organización, ha aceptado los riesgos asociados con la

no instalación de todos los parches programados en la ventana de cambios.

e) Se notificará al área de Seguridad de la Información de la organización, dentro de los 3 días hábiles de identificado que la instalación no se ha completado o que no se puede instalar en la ventana de cambios de gestión de parches aprobada. Se considerará que los avisos de parche serán prorrogados hasta la siguiente ventana de cambios de gestión de parches e instalados en ese momento, a menos que se haya establecido un acuerdo con una fecha alternativa. Una vez que se haya notificado, se considerará que la organización ha aceptado los riesgos asociados a la no instalación de los parches hasta que la instalación se haya completado.

Es responsabilidad de la organización proveer a los ejecutantes, la(s) ventana(s) de cambio de gestión de parches aprobada(s) para la implementación de los avisos de parches.

En conjunto se acordará un calendario o ventanas de implementación de los Avisos e Integridad (principalmente los parches críticos y de seguridad). Si las ventanas de cambios para implementar los parches no son entregadas tras la aprobación de la política, la organización comprende que sus sistemas estarán expuestos a amenazas o riesgos que los parches están diseñados a tratar. El calendario o ventanas de implementación de parches aprobados son válidos hasta el siguiente ciclo de revisión de política y su aprobación, para esto el calendario o ventanas de implementación de parches debe considerar lo siguiente:

- ✓ Una fase piloto destinado para tal efecto. Todo parche liberado por el fabricante deberá ser previamente aplicado en el (los) equipo(s) de prueba(s) antes de su instalación en los ambientes de producción.

- ✓ La disponibilidad de los sistemas a los que se aplicarán el(los) parche(s) para asegurar que no se producirán interrupciones en los procesos críticos a menos que así se desee.
- ✓ El número de sistemas a los que se aplicará el(los) parche(s).

El área de Seguridad de la Información de la organización evaluará las notificaciones enviadas por los ejecutantes sobre avisos de parches, con las siguientes consideraciones:

a) Proporcionará por escrito a los ejecutantes sobre la cancelación de la autorización de instalación de un parche al menos tres días hábiles antes de la fecha prevista de instalación del parche. Se considerará que los avisos de parche serán prorrogados hasta la siguiente ventana de cambios de gestión de parches e instalados en ese momento, incluyendo cualquier ventana de cambios de gestión de parches agendada que sea impactada por la cancelación de la aprobación. La cancelación de la autorización de instalación de un parche constituye el reconocimiento que los sistemas de la organización permanecerán expuestos a las amenazas u otros riesgos que el parche está destinado a resolver.

b) Si el aviso del parche es publicado durante o después del octavo día hábil anterior al inicio de una ventana de cambio de gestión de parches, el nuevo aviso de parche publicado no se implementará hasta la siguiente ventana de cambio, al menos que su aplicabilidad inmediata sea requerida basado en la criticidad definida por el fabricante.

c) Si se requieren pruebas previas a la implementación de un parche, la organización suministrará un entorno de pruebas adecuado para los parches publicados y realizará las pruebas necesarias. Los ejecutantes asistirán a la organización en esta actividad.

El proceso de instalación de parches se deberá realizar en 2 fases, las mismas se detallan a continuación:

- **Fase Piloto**

Tiene como finalidad asegurar la estabilidad del ambiente antes de instalar las actualizaciones en los sistemas bajo gestión de los ejecutantes, para lo cual los ejecutores efectuarán la instalación de los parches en el(los) equipo(s) de prueba destinados por la organización para tal fin. Las pruebas se llevarán a cabo durante 5 días hábiles a cargo del personal designado por la organización, en el cual se validará que no exista ninguna incompatibilidad con las aplicaciones instaladas en los servidores destinados para dichas pruebas. Los ejecutantes asegurarán la funcionalidad a nivel de sistema operativo y los subsistemas bajo gestión de los ejecutantes durante el mismo período de tiempo.

- **Fase Producción**

Tiene como finalidad distribuir las actualizaciones probadas en la fase piloto sobre los sistemas y subsistemas bajo gestión de los ejecutores, asegurando la aplicación de los parches de forma segura y controlada, este proceso de aplicación de actualización se realiza una vez terminada la fase piloto de acuerdo a la ventana de cambios aprobada por la organización.

CAPÍTULO 5

IMPLEMENTACIÓN Y PRUEBAS

5.1 INSTALACIÓN SERVIDOR

Para la implementación de WSUS se procederá con la instalación de Windows server 2008R2, esta es la sexta versión de Windows Server. Es la versión de servidor de Windows 7 y sustituye a Windows Server 2008. Durante el desarrollo, se lanzaron dos versiones preliminares, una vista previa del desarrollador y una versión beta. El software generalmente estaba disponible para los clientes a partir del 4 de septiembre de 2008.

Antes de continuar con la instalación, se detalla las características del servidor solicitado a la organización.

Tabla 16 Características servidor WSUS
Fuente: Autor

Características	
Tipo	Virtual
Fabricante	VMWARE
Procesador	Intel® Xeon™ CPU E5-2660 0 @ 2.20Ghz
Memoria	8GB
Discos	Local Fixed Disk - C: - TOTAL: 59.9GB Local Fixed Disk - D: - TOTAL: 20GB Local Fixed Disk - L: - TOTAL: 296.87GB Local Fixed Disk - T: - TOTAL: 100GB Local Fixed Disk - U: - TOTAL: 400GB

A continuación, se detalla los pasos necesarios para la instalación del servidor:

- ✓ Insertar el DVD de Windows Server 2008R2, y una vez que obtenga el siguiente mensaje “Press any Key to boot from CD or DVD…”, presione Enter para iniciar la configuración.
- ✓ Esperar hasta que la configuración cargue todos los archivos necesarios.
- ✓ Una vez que se carguen los archivos de configuración, la configuración comenzará. Se procede a cambiar de acuerdo con las necesidades de la aplicación.
- ✓ Una configurado, se inicia la instalación, haciendo clic en " Install now".
- ✓ Para nuestro caso se escogerá el idioma ingles y versión standard (predeterminado por la organización) del Windows server 2008R2.
- ✓ Se aceptan los términos de licencia y se configuran los discos.

- ✓ Una vez finalizada la instalación se ingresa al dominio de la organización para que se configuren las políticas asociadas.

5.2 CONFIGURACIÓN DE POLÍTICAS AD

Para continuar con el proceso de configuración deberemos definir las políticas a nivel de directorio activo asociadas para el proceso de parchado, como inicialmente se indicó en las políticas del proceso se aplicaran parches en dos fases, fase piloto y fase de producción, para esto se define que los servidores para la fase piloto serán los del ambiente de desarrollo, QA y preproducción, el mismo será un proceso automático; la fase de producción se escogerá los servidores productivos de los cuales se dividirá en 2 procesos, manual y automático, los servidores con proceso manual se definirá por el impacto y grado de afectación al negocio de los servidores más importantes, los mismos serán validados en conjunto con la organización.

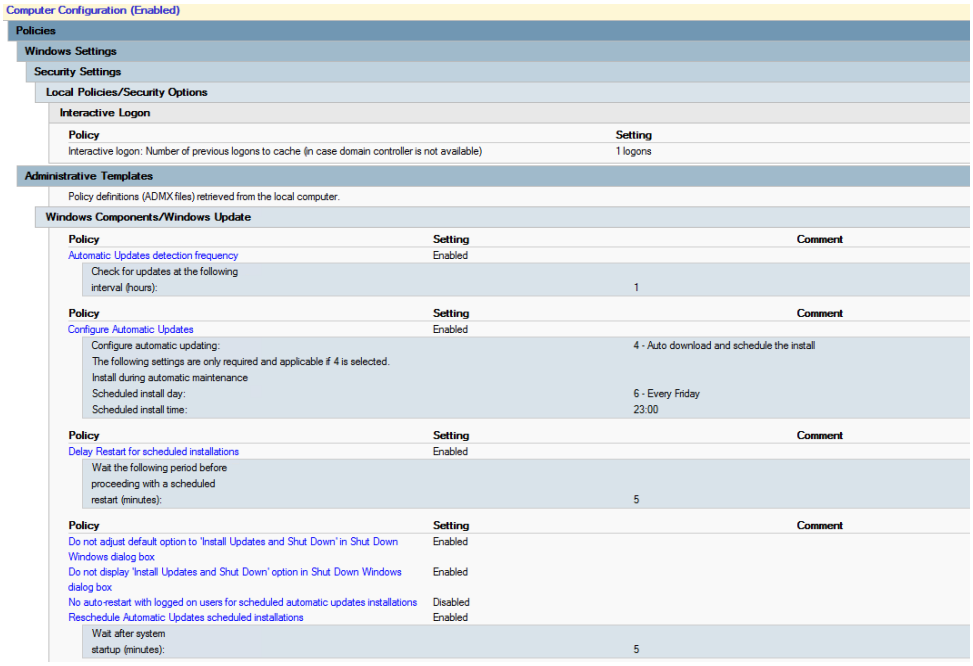
Tabla 17 Definición de proceso de parchado por ambientes
Fuente: Autor

Ambiente	Fase	Proceso
Producción	Producción	Manual/Automático
Desarrollo	Piloto	Automático
Preproducción	Piloto	
Quality Assurance	Piloto	

Una vez definido el proceso de parchado por políticas de dominio se crearán dos políticas que se aplicaran a los respectivos grupos del directivo activo, los horarios serán definidos en horas donde no se afecte la operatividad y por dependencia en conjunto con la organización, a continuación, se detallan las políticas a crear en grupo de políticas de dominio.

Tabla 18 Configuración de Política Para Parchado Automático
Fuente: Autor

Política	Estado	Detalle
Automatic Updates detection frequency	Enabled	Especifica que Windows verificará las actualizaciones disponibles en el intervalo especificado, para nuestro proyecto se configurará un intervalo de 1 hora.
Configure Automatic Updates	Enabled	Especifica si las actualizaciones automáticas están habilitadas para el equipo que pertenezca al grupo, por ser un proceso acutomatico se seleccionar la opción "**4- Auto download and schedule the install**", que automáticamente descarga e instala las actualizaciones.
delay Restart for scheduled installations	Enabled	Especifica que cuando finalice la instalación, se producirá un reinicio programado después de que haya expirado el número de minutos especificado, para nuestro caso después de 5 minutos.
Do not adjust default option to "Install Updates and Shut Down" in Shut Down Windows dialog	Enabled	Esta configuración de directiva permite especificar si la opción Instalar actualizaciones y Apagar está permitida como opción predeterminada en el cuadro de diálogo Cerrar Windows.
Do not display "Install updates and Shut Down" option in Shut Down Windows dialog	Enabled	Especifica que instalar actualizaciones y apagar no aparecerá como una opción en el cuadro de diálogo Cerrar Windows, incluso si las actualizaciones están disponibles para la instalación cuando el usuario selecciona la opción Apagar para apagar la computadora.
No auto-restart with logged on users for scheduled automatic updates installations	Disabled	Especifica que las Actualizaciones automáticas notificarán al usuario que la computadora se reiniciará automáticamente en cinco minutos para completar la instalación.
Reschedule Automatic Updates scheduled installations	Enabled	Especifica que una instalación programada que no tuvo lugar antes se producirá en una determinada cantidad de minutos después de que la computadora se inicie.
Specify intranet Microsoft update service location	Enabled	Especifica que el cliente se conecta al servidor WSUS especificado, en lugar de Windows Update, para buscar y descargar actualizaciones, para nuestro caso nuestro servidor WSUS en la intranet.



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/Security Options

Interactive Logon

Policy	Setting
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	1 logons

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Windows Update

Policy	Setting	Comment
Automatic Updates detection frequency	Enabled	
Check for updates at the following interval (hours):	1	

Policy	Setting	Comment
Configure Automatic Updates	Enabled	
Configure automatic updating:	4 - Auto download and schedule the install	
The following settings are only required and applicable if 4 is selected.		
Install during automatic maintenance		
Scheduled install day:	6 - Every Friday	
Scheduled install time:	23:00	

Policy	Setting	Comment
Delay Restart for scheduled installations	Enabled	
Wait the following period before proceeding with a scheduled restart (minutes):	5	

Policy	Setting	Comment
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled	
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled	
No auto-restart with logged on users for scheduled automatic updates installations	Disabled	
Reschedule Automatic Updates scheduled installations	Enabled	
Wait after system startup (minutes):	5	

FIGURA 5.1 Política de Parchado Automático
Fuente: Autor

Tabla 19 Configuración de Política para Parchado Manual
Fuente: Autor

Política	Estado	Detalle
Automatic Updates detection frequency	Enabled	Especifica que Windows verificará las actualizaciones disponibles en el intervalo especificado, para nuestro proyecto se configurará un intervalo de 1 hora.
Configure Automatic Updates	Enabled	Especifica si las actualizaciones automáticas están habilitadas para el equipo que pertenezca al grupo, por ser un proceso manual se seleccionar la opción "**3- Auto download and notify for install**", cuando se completan las descarga se notifica que existen actualizaciones para instalar.
Do not adjust default option to "Install Updates and Shut Down" in Shut Down Windows dialog	Enabled	Esta configuración de directiva permite especificar si la opción Instalar actualizaciones y Apagar está permitida como opción predeterminada en el cuadro de diálogo Cerrar Windows.
Do not display "Install updates and Shut Down" option in Shut Down Windows dialog	Enabled	Especifica que instalar actualizaciones y apagar no aparecerá como una opción en el cuadro de diálogo Cerrar Windows, incluso si las actualizaciones están disponibles para la instalación cuando el usuario selecciona la opción Apagar para apagar la computadora.
No auto-restart with logged on users for	Enabled	Las Actualizaciones automáticas no reiniciarán una computadora automáticamente durante una instalación programada si un usuario ha iniciado

Política	Estado	Detalle
scheduled automatic updates installations		sesión en la computadora. En cambio, las Actualizaciones automáticas le notificarán al usuario que reinicie la computadora.
Reschedule Automatic Updates scheduled installations	Enabled	Especifica que una instalación programada que no tuvo lugar antes se producirá en una determinada cantidad de minutos después de que la computadora se inicie.
Specify intranet Microsoft update service location	Enabled	Especifica que el cliente se conecta al servidor WSUS especificado, en lugar de Windows Update, para buscar y descargar actualizaciones, para nuestro caso nuestro servidor WSUS en la intranet.

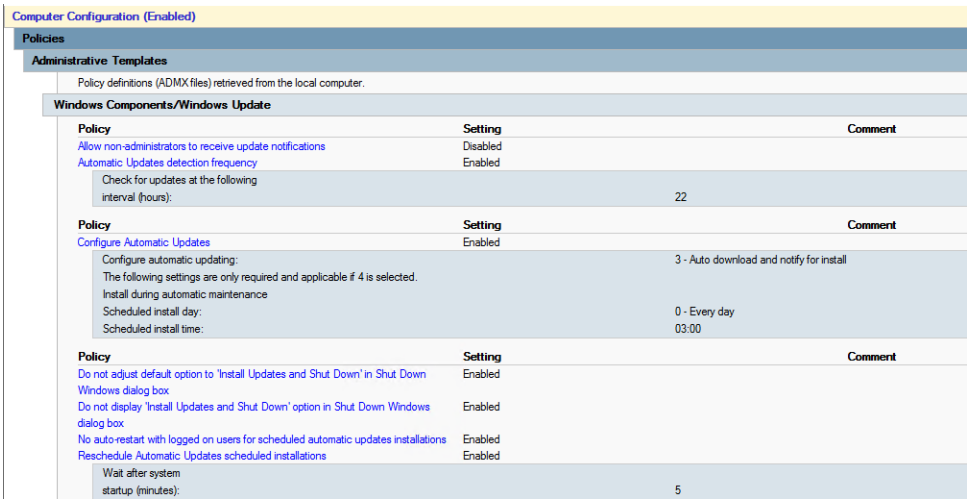


FIGURA 5.2 Política de Parchado Manual
Fuente: Autor

Con esto ya tendremos listas las políticas la cuales se asignarán de acuerdo al cronograma de parchado que se validara con la organización.

5.3 CONFIGURACIÓN DE LA RED

Dentro del proceso de implementación, se deberá trabajar en conjunto con el área de seguridad informática de la organización para crear las políticas de red a nivel de firewall, WSUS está configurado para usar Microsoft Update como la ubicación

desde donde se obtiene las actualizaciones para esto deberemos permitir que el firewall corporativo permita la conexión a internet al servidor y controlar el tráfico.

Para obtener actualizaciones de Microsoft Update, el servidor WSUS usa el puerto 443 para el protocolo HTTPS. En la organización el tráfico está restringido para el acceso a internet, por lo tanto, deberemos obtener autorización para permitir el acceso a Internet desde WSUS a la siguiente lista de URL:

- ✓ http://.windowsupdate.microsoft.com
- ✓ http://*.windowsupdate.microsoft.co
- ✓ https://*.windowsupdate.microsoft.co
- ✓ http://*.update.microsoft.co
- ✓ https://*.update.microsoft.co
- ✓ http://*.windowsupdate.co
- ✓ http://download.windowsupdate.com
- ✓ http://download.microsoft.com
- ✓ http://*.download.windowsupdate.co
- ✓ http://wustat.windows.com
- ✓ http://ntservicepack.microsoft.com
- ✓ http://go.microsoft.com

Para la conexión de las estaciones clientes se deberá configurar el firewall para que puedan tener acceso al puerto 8530 que es puerto por default del servidor WSUS, el tráfico debe ser de entrada y salida.

5.4 INSTALACIÓN PRERREQUISITOS

Una vez instalado nuestro servidor con Windows Server 2008R2 deberemos preparar nuestro servidor para la instalación del rol de WSUS, una de las principales características necesarias para el rol es tener habilitado el IIS, este rol es necesario

ya que aquí se crearán los servicios webs de WSUS, para proceder con la instalación a continuación se detallan los pasos.

a) Abrir el Administrador del servidor haciendo clic en el icono del Administrador del servidor en el escritorio.
b) En la ventana del Administrador del servidor, haremos clic en Agregar funciones y funciones, o en el menú Administrar y luego en Agregar roles y características. este comenzará con una página Antes de comenzar.
c) En la página Tipo de instalación, seleccionamos Instalación basada en funciones o basada en funciones para configurar un solo servidor.
d) En la página Selección de servidor, seleccionamos Seleccionar un servidor del grupo de servidores y luego seleccionamos un servidor.
e) En la página Funciones del servidor, seleccionar Servidor web (IIS).

Para la instalación de WSUS es necesario contar con un motor de base de datos, para nuestra implementación usaremos la instalación por defalult que instala una instancia de Windows Internal Database con el nombre de SUSDB.mdf. Esta base de datos se encuentra en la carpeta %windir%\ wid\data\, donde %windir% es la unidad local en la que está instalado el software del servidor WSUS.

WSUS admite la autenticación de Windows solo para la base de datos. No se puede usar la autenticación de SQL Server con WSUS. Si utiliza la base de datos interna de Windows para la base de datos de WSUS, el programa de instalación de WSUS crea una instancia de SQL Server denominada **server\ Microsoft##WID**, donde servidor es el nombre del servidor. El nombre de esta base de datos no es configurable.

5.5 INSTALACIÓN WSUS

Para continuar con la implementación del servidor WSUS es necesario instalar la función del servidor WSUS. El siguiente procedimiento describe cómo instalar la función del servidor WSUS utilizando el Administrador del servidor.

Durante el proceso de instalación, WSUS instalará lo siguiente de forma predeterminada:

- ✓ API .NET y cmdlets de Windows PowerShell.
- ✓ Windows Internal Database (WID), que es utilizado por WSUS.
- ✓ Servicios utilizados por WSUS, que son:
  - o Servicio de actualización.
  - o Servicio web de informes.
  - o Servicio web de cliente.
  - o Servicio Web de Autenticación Web Simple.
  - o Servicio de Sincronización de Servidor.
  - o Servicio web de autenticación DSS.

Para la instalación del rol de WSUS deberemos seguir los siguientes pasos.

a) Iniciar sesión en el servidor que se instalara el rol usando una cuenta que sea miembro del grupo Administradores locales.
b) En **Server Manager**, haga clic en **Manage** y luego en **Add Roles and Features**.
c) En la página Seleccionar tipo de instalación, confirme que la opción de **Role-based or feature-based installation** esté seleccionada y haga clic en Siguiente.

d) En la página **Select destination server**, elija dónde se encuentra el servidor. Después de seleccionar la ubicación, elija el servidor en el que desea instalar la función del servidor WSUS.

e) En la página **Select server roles**, seleccione **Windows Server Update Services**. Agregue las características que se requieren para Windows Server Update Services.

f) En la página **Select features**. Conservar las selecciones predeterminadas.

g) En la página de **Content location selection**, ingresaremos ubicación para almacenar la base de datos de las actualizaciones. Para nuestra implementación, crearemos una carpeta llamada WSUS en la raíz de la unidad D quedando la ruta D:\WSUS.

Una vez finalizada la instalación ya tendremos el rol de WSUS instalado en nuestro servidor.

5.6 CONFIGURACIÓN CONSOLA DE ADMINISTRACIÓN

Una vez instalado, podemos proceder a configurar WSUS. Para iniciar este proceso, abriremos la consola de WSUS desde el menú Herramientas en el Administrador del servidor.

Una vez abierto nos pedirá que ingresemos la ruta donde almacenaremos los paquetes de actualizaciones, para nuestra implementación seleccionaremos que almacene localmente las actualizaciones y la ruta para nuestra implementación será U:\WSUS.

Finaliza la configuración inicial, nos mostrara la pantalla principal de la consola de WSUS, desde aquí ya podemos administrar el servicio de WSUS, la consola de administración cuenta con un panel principal donde nos mostrara las siguientes opciones de administración que se detallan a continuación:

- **Updates**

Administración de actualizaciones desde esto ítem podremos aprobar, rechazar, eliminar y verificar cualquier registro de las actualizaciones dentro de nuestra consola WSUS.

- **Computers**

Desde este ítem podremos administrar todos los equipos clientes que recibirán las actualizase desde nuestro servidor WSUS.

- **Downstream Servers**

Desde este ítem podremos administrar servidores WSUS en caso de tener múltiples servidores WSUS.

- **Synchronizations**

Desde este ítem verificaremos la sincronización de nuestro servidor WSUS con la fuente de origen las actualizaciones.

- **Reports**

Reportes básicos de WSUS.

- **Options**

Ítem de configuración general de WSUS.

La configuración general del rol WSUS la podemos realizar desde la opción “Options”, aquí se encontrará la parte más importante de la consola de WSUS, a continuación, se detallan las opciones que contiene WSUS:

  - ✓ Update Source and Proxy Sever

- ✓ Products and Classifications
- ✓ Update Files and Languages
- ✓ Synchronization Schedule
- ✓ Aautomatic Approvals
- ✓ Computers
- ✓ Server Cleanup Wizard
- ✓ Reporting Rollup
- ✓ E-Mail Notifications
- ✓ Microsoft Update Improvement Program
- ✓ Personalization
- ✓ WSUS Server Configuration Wizard

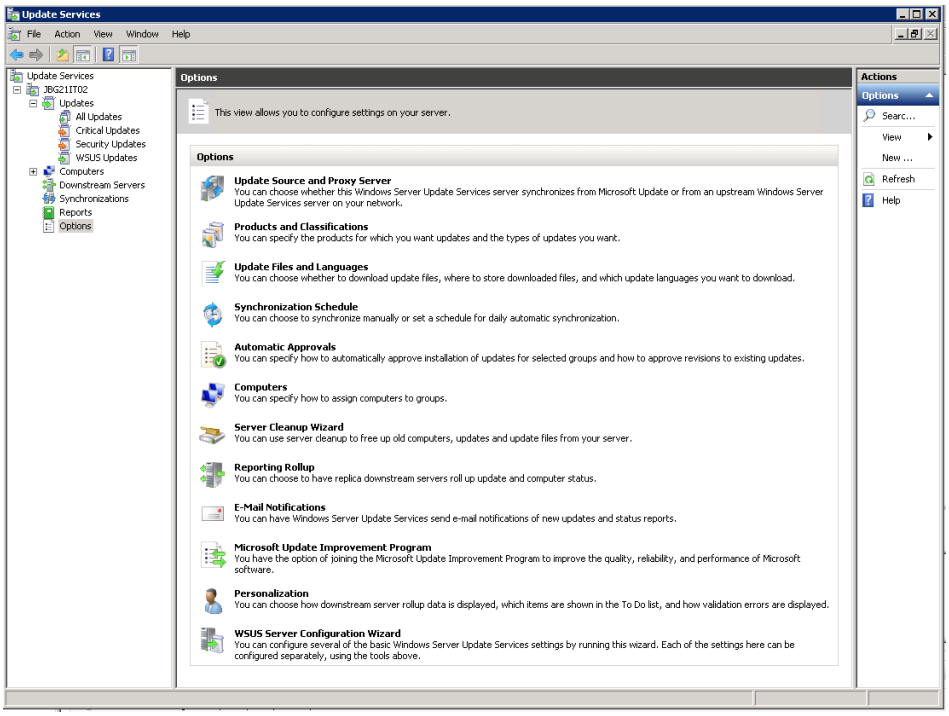


FIGURA 5.3 Consola de administración WSUS
Fuente: Autor

5.7 CONFIGURACIÓN WSUS

5.7.1 CONFIGURACIÓN SERVIDOR PRIMARIO

Para nuestra implementación se definió el esquema para la configuración de WSUS la cual se usará un díselo WSUS simple, para eso nuestro servidor WSUS será el servidor primario, por lo cual deberemos configurar desde donde se sincronizarán las actualizaciones, para esto realizaremos lo siguiente:

a) Seleccionaremos el ítem “Options” dentro de la consola de administración.
b) Seleccionamos “Update Source and Proxy Sever”.
c) En la pestaña “Update Source”, seleccionaremos la opción “Synchronize Source and Proxy Server”.

Con esto tendremos configurado nuestro servidor WSUS como servidor primario, las actualizaciones se descargarán de Microsoft Update y se almacenarán en el servidor en la ruta definida anteriormente.

5.7.2 SELECCIONAR LENGUAJE DE ACTUALIZACIONES

Una vez configurado nuestro servidor primario, deberemos seleccionar el idioma de las actualizaciones a descargar, por estándar de la organización todos los servidores se instalan con el idioma inglés, al no haber más idiomas disponibles, no podemos agregar otro idioma a la configuración de WSUS ya que el tamaño de nuestra ruta donde se guardan las actualizaciones crecerá y necesitaremos más espacio para poder soportar el resto de los idiomas, para esta configuración realizaremos los siguientes:

a) Seleccionaremos el ítem “Options” dentro de la consola de administración.
b) Seleccionamos “Update Files and Languages”.
c) En la pestaña “Update languages”, seleccionaremos el idioma ingles”.

5.7.3 SELECCIONAR PRODUCTOS PARA ACTUALIZAR

Microsoft cuenta con un sinnúmero de productos, como Windows, Windows server y aplicaciones propietarias, desde la consola de administración de WSUS podemos seleccionar los productos que deseamos actualizar, en conjunto con la organización se seleccionan los productos que actualmente tienen en producción, una vez seleccionados WSUS solo descargara actualizaciones de estos productos a continuación, se detallan los productos seleccionados:

- ✓ Active directory
- ✓ Report viewer
- ✓ Device Helth
- ✓ Eschange Server 2010
- ✓ Microsoft SQL Server (2005, 2008, 2008R2, 2012, 2014, 2016)
- ✓ Windows Server (2003, 2008, 2008R2, 2012, 2012R2, 2016)

Cabe indicar que si la organización adquiere un producto adicional de Microsoft se agregara según acuerdo a la consola de WSUS, para proceder con la configuración se realizara los siguientes pasos:

a) Seleccionaremos el ítem “Options” dentro de la consola de administración.

b) Seleccionamos “Products and Classifications”.

c) En la pestaña “Products”, seleccionaremos los productos acordados con la organización.

5.7.4 SELECCIONAR CLASIFICACIÓN DE ACTUALIZACIONES

WSUS cuenta con clasificaciones de actualizaciones las cuales una vez seleccionadas se descargarán los metadatos según los productos que se seleccionaron para las respectivas actualizaciones, a continuación, se detallan las clasificaciones disponibles en WSUS:

- ✓ Critical Updates
- ✓ Definition Updates
- ✓ Drivers
- ✓ Feature packs
- ✓ Security updates
- ✓ Service packs
- ✓ Tools
- ✓ Update rollups
- ✓ Updates
- ✓ Upgrades

Para nuestra implementación seleccionaremos todas las categorías, ya que como se mencionó anteriormente la selección solo descarga los metadatos de las actualizaciones, a continuación, se detalla el proceso de configuración:

a) Seleccionaremos el ítem “Options” dentro de la consola de administración.

b) Seleccionamos “Products and Classifications”.

c) En la pestaña “Classifications”, seleccionaremos las clasificaciones acordados con la organización.

5.7.5 CONFIGURACIÓN PROGRAMACIÓN DE SINCRONIZACIONES

Para finalizar la configuración deberemos configurar la programación de las actualizaciones desde nuestro servidor WSUS hacia el Microsoft Update, para esta configuración se definió que la sincronización se la realice todos los días a las 02:00AM.

A continuación, se detalla el proceso de configuración:

- ✓ Seleccionaremos el ítem “Options” dentro de la consola de administración.
- ✓ Seleccionamos “Synchronization and Schedule”.
- ✓ Seleccionamos “Sychronize automatically” y configuraremos la hora acordada con la organización.

5.8 CREACIÓN GRUPOS DE EQUIPOS EN WSUS

Nuestro servidor WSUS se encuentra listo para la aceptación de los equipos dentro de la consola, para tener una mejor distribución se crearán los respectivos grupos y tener una mejor administración de los equipos dentro de la consola de administración de WSUS, estos grupos fueron creados en conjunto con la organización, a continuación, se detallan los grupos creados.

- **All Computers**

Grupo donde se visualizarán todos los equipos que se sincronizan con WSUS, no se aprueban parches para este grupo.

- **Unassigned Computers**

Grupo donde se visualizarán los equipos que aún no se le han asignado un grupo en específico, no se aprueban parches para este grupo.

- **Exclusiones de parchado**

Grupo creado para ingresar servidores que deben ser excluidos del parchado y solo si es necesario y bajo la aprobación de la organización se parcharan de forma manual, generalmente servidores con aplicaciones que no soportan actualizaciones, no se aprueban parches para este grupo.

- **Fase Piloto**

Grupo creado para ingresar todos los servidores de Desarrollo, cualquier nuevo servidor que sea creado en el ambiente no productivo deberá ser ingresado en este grupo bajo mejor criterio de la organización, solo se aprueban parches críticos y de seguridad.

- **Fase Producción**

Grupo donde se ingresarán los servidores productivos, cualquier servidor creado en el ambiente de producción deberá ser ingresado a este grupo salvo mejor criterio de la organización, solo se aprueban parches críticos y de seguridad, este grupo se divide en dos subgrupos que se detallan a continuación:

  - Parchado Automático.
  - Parchado Manual.

- **Parchado Histórico**

En este grupo se creará en caso de que un servidor que no esté dentro del proceso de parchado y contenga alguna aplicación critica sea necesario parcharlo por temas de seguridad, se aprobaran solo parches con clasificación crítica y de seguridad, solo se aprueban parches críticos y de seguridad.

- **Servidores 2003**

Grupo creado para plan de actualización de servidores con WS2003, este producto ya se encuentra fuera de soporte y ya no recibe actualizaciones, pero la organización aun cuenta con servidores con esta versión que no se han parchado, en este grupo se aprobaran solo actualizaciones pasadas para WS2003, solo se aprueban parches críticos y de seguridad, este grupo se divide en dos subgrupos que detallan a continuación.

  - Desarrollo-Preproducción.
  - Produccion-2003.

- **Todos los Parches**

Grupo creado para servidores iniciales, en este grupo se aprobarán todos los parches lanzados por Microsoft, en la creación de un servidor antes de entregar a la organización el mismo debe contar con todos los parches distribuidos por Microsoft, una vez entregado la organización definirá en que grupo se colocará.

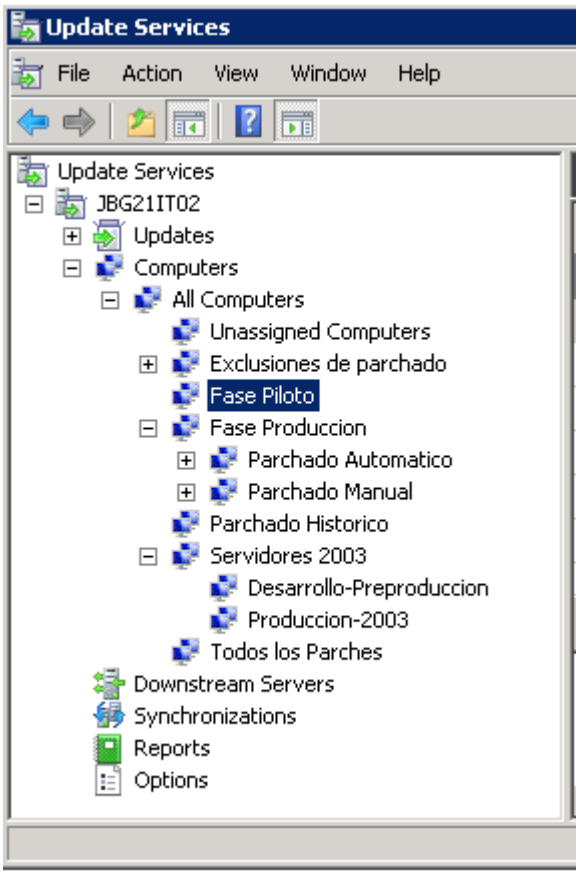


FIGURA 5.4 Grupos De Equipos en WSUS
Fuente: Autor

5.9 CREACIÓN DE REPORTES PARA WSUS

WSUS es bastante poderoso ya que puede proporcionarnos informes que contienen información útil sobre qué máquinas Windows tienen aplicadas las actualizaciones de Windows, lo que nos permite obtener una buena visión general de nuestro entorno a nivel de administración de WSUS.

Este tipo de información será útil si está obligado a realizar cualquier tipo de verificación de cumplimiento para garantizar que los servidores estén correctamente parcheados.

En total, hay 9 informes predeterminados diferentes que se pueden ejecutar desde la consola de administración. Simplemente se debe hacer clic en cualquiera de ellos y filtrar el tipo de información que se desee en el informe, como los tipos de clasificación de actualización, tipo de actualización del producto o grupos de computadoras, por ejemplo. Cada reporte puede ser exportado a PDF, Excel y Word.

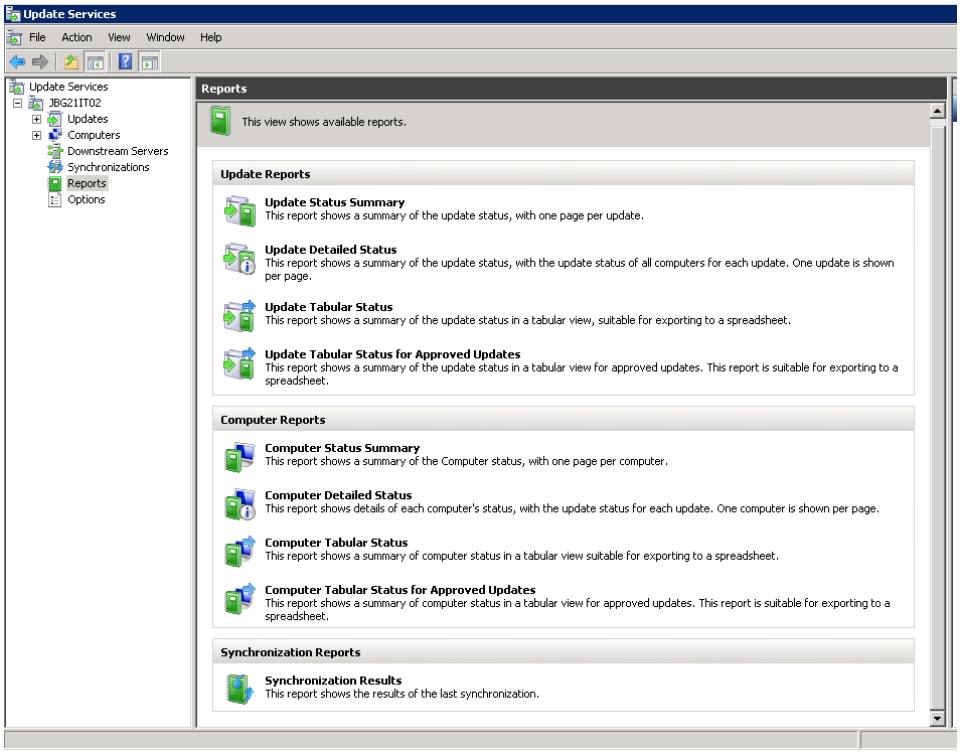


FIGURA 5.5 Reportes WSUS
Fuente: Autor

Estos reportes son administrativos para la parte técnica, para poder presentar un reporte gerencial y que sea de fácil compresión para la gerencia, se crea un reporte personalizado vía PowerShell, el cual los ejecutores validan la información y enviaran a la gerencia.

5.10 PRUEBAS EN SERVIDORES AMBIENTES NO PRODUCTIVOS

Como inicialmente se acordó el proceso de parchado se lo realizara en dos fases, como fase inicial y para validar el impacto de la aplicación de parches en los servidores se realizarán las respectivas pruebas en el ambiente de desarrollo, al

tener servidores que desde su creación no se han parchados se ha planificado en conjunto con la organización un plan para la aplicación de parches inicial.

Luego de determinar los servidores no-productivos, los cuales se ha dividido en dos etapas el proceso inicial de parchado: PILOTO I y PILOTO.

- PILOTO I: Corresponde a los servidores que se encuentran en ambientes de Preproducción y QUALITY ASSURANCE.
- PILOTO II: Corresponde a los servidores que se encuentran en ambientes de Desarrollo.

Para el proceso de parchado de toda la granja de servidores y en conjunto con la organización se define la cantidad de servidores a parchar, cabe indicar que fueron excluidos servidores por solicitud formal de la organización, se determinó que del total de servidores 57 serían los iniciales para las fases pilotos, 30 servidores para el PILOTO I y 27 para el PILOTO II.

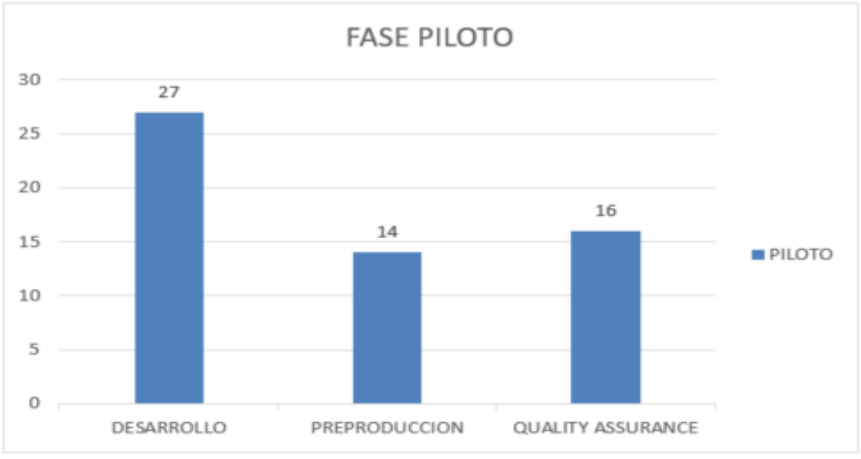


FIGURA 5.6 Servidores Fase Piloto
Fuente: Autor

La ejecución del parchado se la realizará de la siguiente manera:

- ✓ La fase piloto tomara 1 mes de aplicación, donde se parcharán semanalmente en horarios donde no se afecte la operación.
- ✓ Previo al parchado se generar un snap de los servidores como contingencia en caso de fallos en el parchado.
- ✓ Una vez parchado el área de desarrollo validara los servidores y en caso de que se necesite alguna consideración después del reinicio se notificara a los ejecutores.
- ✓ Una vez finalizado el proceso de parchado los servidores se distribuirán en los grupos correspondientes en la consola de WSUS, para que se continúe con el proceso mensual de parchado.

Finalizada la etapa de actualización a la fecha de los servidores no-productivos, para el proceso mensual automático de parchado, a continuación, se detalla la planificación:

SERVERS					
SEMANA PARCHADO	FASE PARCHADO	MODO PARCHADO	DÍA PARCHADO	HORA PARCHADO	Total
SEMANA 2	PILOTO	AUTO	VIERNES	23:00	50
		MANUAL	VIERNES	21:00	3
				23:00	4
TOTAL					57

FIGURA 5.7 Ejecución Fase No-Producción Modo Automático
Fuente: Autor

Para este proceso mensual y por solicitud de la organización 7 servidores no-productivos se les aplicara una revisión manual luego de la aplicación de parches.

5.11 PLANIFICACIÓN DE PARCHADO PARA AMBIENTES PRODUCTIVOS

Para los servidores productivos se definió dos procesos, el proceso manual y el proceso automático de parchado, esto depende el nivel de criticidad que la organización clasifique los servidores productivos.

Basados en este concepto la organización clasifico los servidores productivos, tanto como si aplicaban ser parchado y la criticidad de estos, de la granja de servidores productivos se seleccionaron 138 servidores divido en 56 para parchado automático y 82 para parchado manual.

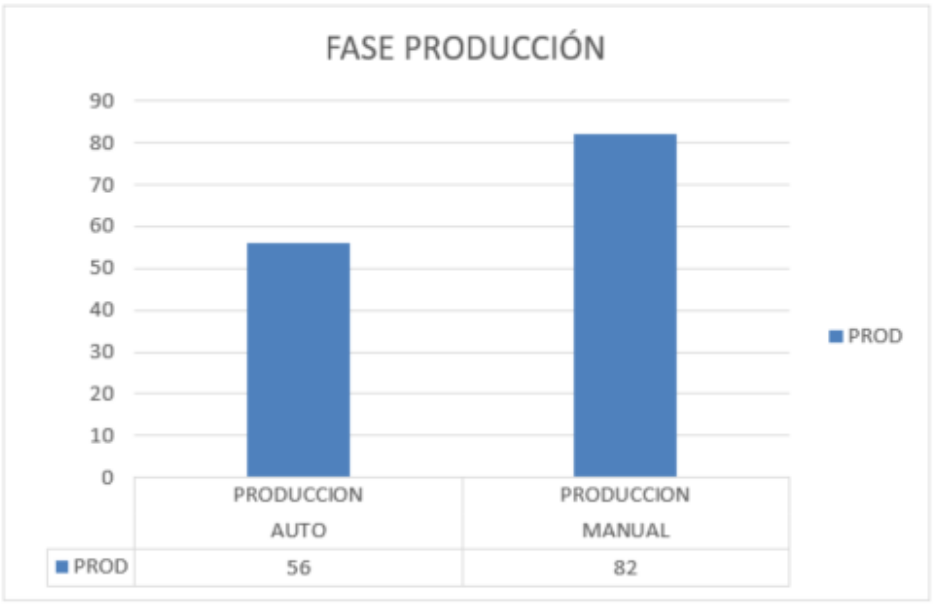


FIGURA 5.8 Servidores Fase Producción
Fuente: Autor

Para el proceso de parchado automático, inicialmente se debe actualizar los servidores a la fecha con los parches que ha publicado Microsoft ya que no están actualizados, esto como fase inicial del proceso de parchado productivo, la ejecución de este proceso se la realizara de la siguiente manera:

- ✓ La fase piloto tomara 2 meses de aplicación, donde se parcharán semanalmente en horarios donde no se afecte la operación.
- ✓ Previo al parchado se generar un snap de los servidores como contingencia en caso de fallos en el parchado.
- ✓ Una vez parchado los ejecutores y el área de desarrollo validaran los servidores y en caso de que se necesite alguna consideración después del reinicio se notificara a la organización.
- ✓ Una vez finalizado el proceso de parchado los servidores se distribuirán en los grupos correspondientes en la consola de WSUS, para que se continúe con el proceso mensual de parchado.

5.12 EJECUCIÓN DE PARCHADO EN AMBIENTES PRODUCTIVOS

Una vez finalizado la fase inicial de parchado donde los servidores fueron actualizados con los parches distribuidos a la fecha por Microsoft e ingresados en sus grupos respectivos en WSUS, debemos planificar la ejecución mensual del proceso de parchado tanto para los servidores no-productivos como para los servidores productivos.

Microsoft envía los boletines de actualizaciones mensuales el segundo martes de cada mes por lo cual la planificación de las actualizaciones comenzara desde el viernes de la segunda semana, teniendo para parchado la semana 2, semana 3 y semana 4 de cada mes.

Para el proceso automático de parchado para los servidores productivos, a continuación, se detalla la planificación:

SERVERS					
SEMANA PARCHADO	FASE PARCHADO	MODO PARCHADO	DÍA PARCHADO	HORA PARCHADO	Total
SEMANA 3	PROD	AUTO	MIERCOLES	3:00	9
			JUEVES	19:00	5
			VIERNES	23:00	22
			SABADO	20:00	1
				21:00	10
				23:30	9
TOTAL					56

FIGURA 5.9 Ejecución Fase Producción Modo Automático
Fuente: Autor

Para el proceso manual de parchado para los servidores productivos, a continuación, se detalla la planificación:

SERVERS					
SEMANA PARCHADO	FASE PARCHADO	MODO PARCHADO	DÍA PARCHADO	HORA PARCHADO	Total
SEMANA 2	PROD	MANUAL	VIERNES	23:00	2
			SABADO	23:00	1
SEMANA 3	PROD	MANUAL	VIERNES	23:00	2
			SABADO	20:00	1
				21:00	1
				22:30	6
				23:00	11
				23:30	22
SEMANA 4	PROD	MANUAL	DOMINGO	23:00	16
			MARTES	3:00	9
			SABADO	23:30	3
				3:00	2
			⊞		6
TOTAL					82

FIGURA 5.10 Ejecución Fase Producción Modo Manual
Fuente: Autor

Para el proceso de parchado en manual se deberá seguir los siguientes lineamentos como parte de la ejecución mensual:

a) Realizar un export del estado de los Servicios Windows previo al reinicio del servidor, nombre de archivo seguirá el siguiente formato de ejemplo: “EVIDENCIA_PREVIA”, en la siguiente ruta:

   D:\parches\MesX\SemanaX\Dia\NombreServidor) del servidor WSUS.

b) Ejecutar reinicio de Servidor previo a aplicación de parches (esto con la finalidad de validar el estado del servidor previo a la aplicación de parches).
c) Ejecutar la aplicación de parches liberados.
d) Realizar un export del estado de los Servicios Windows posterior a la aplicación de parches y reinicio del servidor el nombre de archivo seguirá el siguiente formato de ejemplo: “EVIDENCIA_POST_PARCHADO” (ubicarlo en la ruta D:\parches\MesX\SemanaX\Dia\NombreServidor, del servidor WSUS.
e) Identificar si existe alguna diferencia de servicio que no ha subido correctamente mediante.
f) Realizar una captura de pantalla donde se indique nombre del servidos y estado de los parches aplicados esta captura será guardada en la misma carpeta indicada en el punto a y d.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 ANÁLISIS DE RESULTADOS DE ACUERDO A LA IMPLEMENTACIÓN

Para detallar una idea más objetiva en cuanto a validar los resultados obtenidos con la implementación de WSUS, se realizó un cuestionario para de esta manera sea factible y tener una visión descriptiva, con ello se detectará detalles positivos y negativos en torno a la ejecución de la organización en la aplicación de parches. Detalles que se mostraran para cada uno de los casos vistos.

6.1.1 PROCESO DE PARCHADO

La principal amenaza que se logró detectar fue el no contar con un proceso de parchado para productos Microsoft acorde a las necesidades tecnológicas, esto causaba un gran problema tanto operativo como de seguridad en la organización. La encuesta se realizó a un total de cinco personas que pertenecen al área de seguridad:

¿Conoces del rol WSUS para productos Microsoft?

	Cantidad	Porcentaje
a) SI	2	40.00%
b) NO	3	60.00%
Total	5	100.00%

¿Conoces procesos para parchado en la organización para productos Microsoft?

	Cantidad	Porcentaje
a) SI	0	0.00%
b) NO	5	100.00%
Total	5	100.00%

En caso de alguna vulnerabilidad asociada a Producto Microsoft ¿Sabías que hacer?

	Cantidad	Porcentaje
a) SI	5	100.00%
b) NO	0	0.00%
Total	5	100.00%

¿Estás de acuerdo con el nuevo proceso de parchado?

	Cantidad	Porcentaje
a) SI	5	100.00%
b) NO	0	00.00%
Total	5	100.00%

¿Qué te parece la administración de la consola de WSUS?

	Cantidad	Porcentaje
a) Buena	4	80.00%
b) Regular	1	20.00%
c) Mala	0	0.00%
Total	5	100.00%

En base a la inducción de WSUS ¿Tienes dudas de la administración y del proceso?

	Cantidad	Porcentaje
a) SI	0	0.00%
b) NO	5	100.00%
Total	5	100.00%

Con estos resultados podemos determinar:

a) El área de seguridad informática conocía poco sobre el rol WSUS para productos Microsoft, solo por referencias, pero nada técnico.
b) Se desconocía de procesos documentado para parchado.
c) El departamento de seguridad en de que se notificar alguna vulnerabilidad realizaba un proceso manual para ciertos servidores para parchar solo la vulnerabilidad asociada.
d) Después de presentar el documento de políticas y procesos para parchado, el departamento quedo satisfecho con lo acordado.
e) En la inducción de la consola de administración, la única observación fue la opción de reportes la cual era muy básica, en base a esto se indicó que se creó un reporte personalizado vía PowerShell.
f) Finalizada la inducción se dio inicio al proceso mensual de parchado con la consola de WSUS, quedando aclarada cualquier duda inicial.

6.1.2 ANÁLISIS CON HERRAMIENTAS MICROSOFT

Para nuestro análisis de vulnerabilidad en los servidores Windows usaremos la herramienta **Microsoft Baseline Security Analyzer**, esta herramienta proporciona un método simplificado para identificar las actualizaciones de seguridad faltantes y las configuraciones incorrectas de seguridad comunes en productos Microsoft.

Para el análisis aplicaremos la herramienta en un servidor al cual no se le han aplicado parches y un servidor al que fue ingresado a la consola de WSUS y parchado con los últimos boletines de seguridad de Microsoft.

A continuación, se detalla el informe de la herramienta ejecutada sobre los servidores de producción antes mencionado:

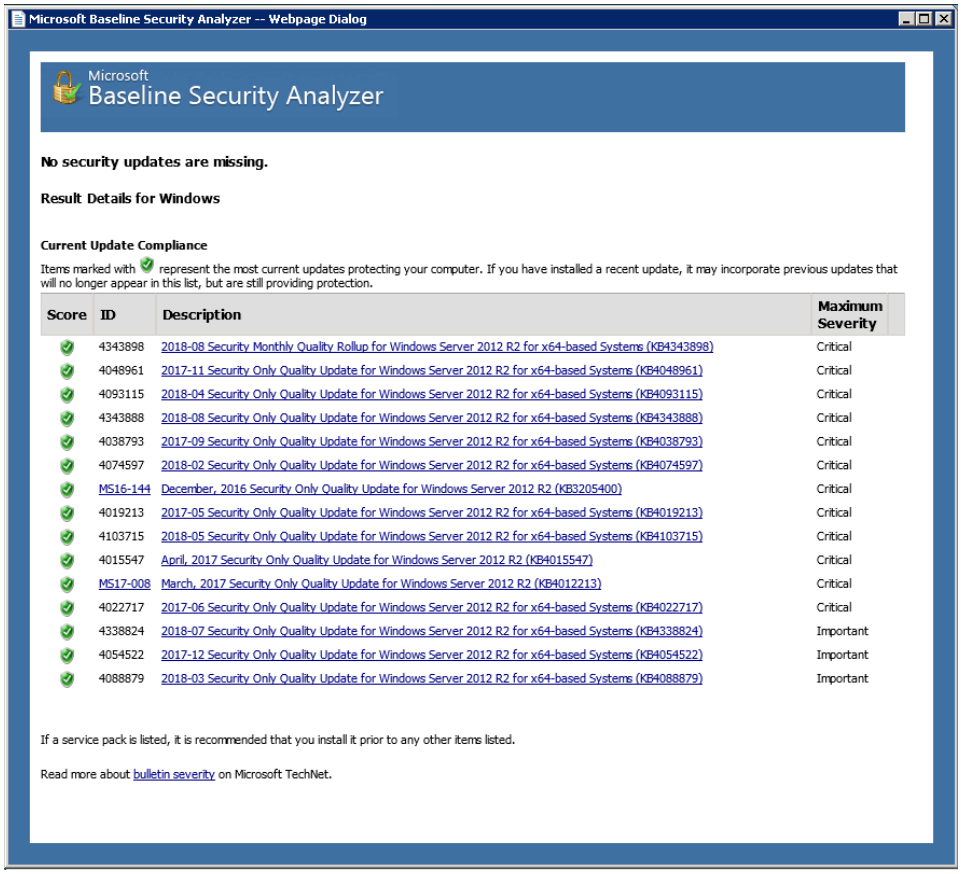


FIGURA 6.1 Análisis sobre servidor Parchado
Fuente: Autor

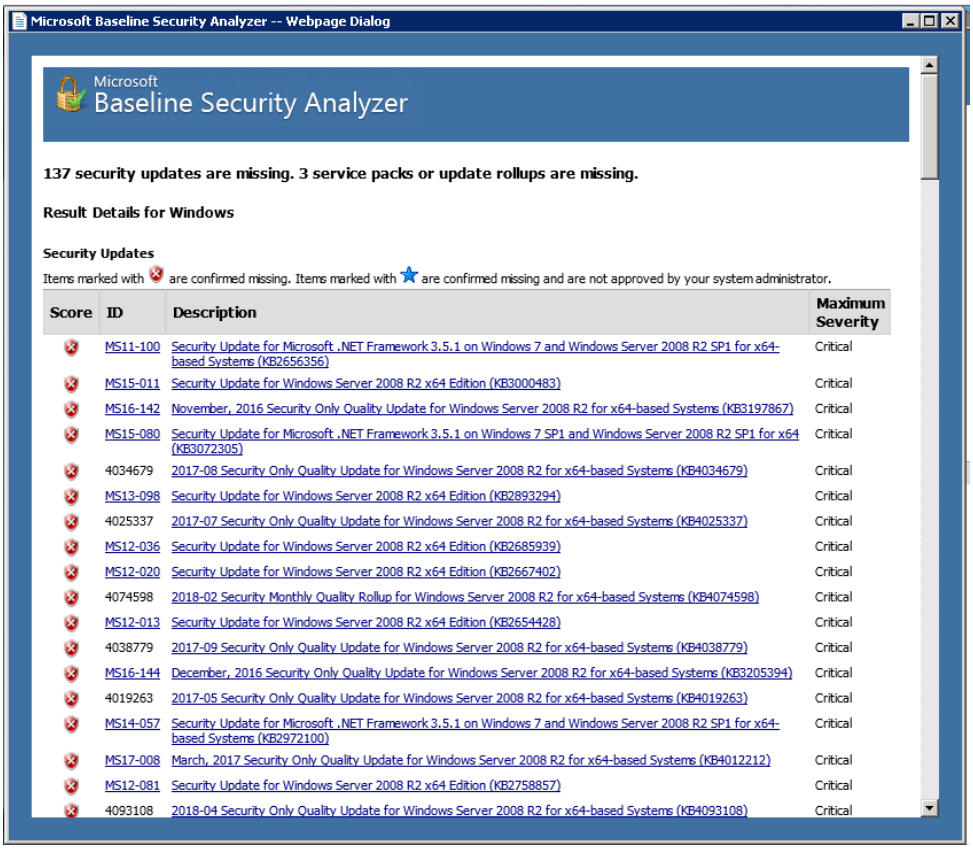


FIGURA 6.2 Análisis sobre servidor No Parchado
Fuente: Autor

En resumen, la herramienta nos indica que nuestro servidor parchado no tiene vulnerabilidades a nivel de parchado, mientras que el servidor no parchado muestra vulnerabilidades críticas.

6.2 EVALUACIÓN DE EFICIENCIA SEGÚN LA IMPLEMENTACIÓN

Basados en los casos presentados, se muestra a continuación las soluciones necesarias para el proceso de parchado.

a) Realizar la capacitación constante al personal de seguridad en el ámbito de la seguridad a nivel de productos Microsoft, con esto se tendrá personal más capacitado que tomará las decisiones correctas cuando el caso lo amerite.
b) Realizar la revisión constante de los procedimientos y procesos que se requieren para el proceso de parchado.
c) Realizar campañas que ayuden a la concientización en base a las responsabilidades que tiene cada persona con relación al proceso de parchado.
d) Dar a conocer la política de seguridad a nivel de parchado, a todas las áreas del departamento de sistemas.
e) Realizar la revisión de procesos con todas las áreas involucradas con el objetivo de encontrar posibles errores en dichos procesos.
f) Realizar reuniones mensuales entre los ejecutores y personal de la organización para ver avances y reportes de parchados.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La seguridad de la información y de los activos de los que cuenta la organización están sujetos a una correcta aplicación de los procesos y políticas para el proceso de parchado, lo cual lleva a la continuidad del negocio y mitiga el impacto de incidentes que puedan llegar a pasar.
2. La Confidencialidad, Integridad y Disponibilidad son parte fundamental de la seguridad de información y le aseguran a la organización garantizar y que todos los sistemas de información tengan un nivel de aseguramiento aceptable a la hora de mitigar alguna amenaza.
3. Es necesario que los empleados tomen precauciones en temas de seguridad, ya que esto llega a afectar a todos los activos informáticos, por ello se los debe capacitar para que estén aptos para identificar y responder ante inminentes incidentes.
4. Es importante continuar identificando problemas a nivel de seguridad en los activos informáticos, se deben implementar mejoras que satisfagan las necesidades de la organización para evitar problemas a futuro.

5. Todos los departamentos desde la alta gerencia deben estar involucrados tanto en el análisis y desarrollo de procesos y políticas de seguridad, tanto para activos físicos como lógicos, así como en un proceso de recuperación en cuanto pueda suceder un desastre.
6. La organización debe tener actualizado todos los inventarios de activos y definir constantemente la criticidad de los servidores y estar al día en las actualizaciones. Esto ayudará a reducir riesgos de amenazas.
7. Se debe cumplir a cabalidad las políticas y procesos acordados para la aplicación de los parches, definir mediante reuniones mensuales la correcta aplicación de estos procesos.
8. La administración de la consola deberá se inducida para nuevo personal, estar constantemente actualizados en nuevas características que mejoren el uso de esta.

RECOMENDACIONES

1. Establecer esquemas de mantenimiento para el servidor WSUS, se debe aplicar recomendaciones del fabricante para el mantenimiento de almacenamiento y catálogo de la base de datos.
2. Actualizar contantemente el documento de políticas y procesos, acorde al crecimiento de la organización.
3. Definir administradores para la consola, estos serán los encargados de la distribución de los parches a aplicar en la organización.
4. Realizar plan para la implementación de WSUS en las estaciones clientes (no servidores).
5. El departamento de seguridad de la organización debe tener un plan para la validación de errores en el parchado, cada parche puede provocar alguna inconsistencia en el sistema por lo cual se debe aplicar un reverso en caso de ser necesario.
6. En caso de que la organización se expanda a otras provincias, se puede implementar el esquema se servidor WSUS es cascada para atender el crecimiento.

BIBLIOGRAFÍA

[1] J. Andress, The Basics of Information Security, 2nd Edition. Syngress, 2014.

[2] J. R. Vacca, Computer and Information Security Handbook, 3rd Edition. Morgan Kaufmann, 2017.

[3] C. Fernández, «La seguridad de la información de una empresa | Apen: Soluciones informáticas».

[4] «El Despertar De La Seguridad Informática En Las Organizaciones |», Open IT, 23-may-2017.

[5] «Information Security Forum». [En línea]. Disponible en: https://www.securityforum.org/. [Accedido: 03-sep-2018].

[6] «Acerca de ISACA». [En línea]. Disponible en: http://www.isaca.org/spanish/Pages/default.aspx. [Accedido: 03-sep-2018].

[7] «55% de las empresas del Fortune 1000 prefieren IIS – Ruben Colomo». [En línea]. Disponible en: https://blogs.technet.microsoft.com/rubencolomo/2007/10/15/55-de-las-empresas-del-fortune-1000-prefieren-iis/. [Accedido: 03-sep-2018].

[8] «CVE security vulnerability database. Security vulnerabilities, exploits, references and more». [En línea]. Disponible en: https://www.cvedetails.com/. [Accedido: 03-sep-2018].

[9] Archiveddocs, «Windows Server Update Services Overview». [En línea]. Disponible en: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh852345(v%3dws.11). [Accedido: 03-sep-2018].

[10] «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método», p. 127.

[11] «Port80 Software | Web Application Security & Performance Tools for Microsoft IIS Servers». [En línea]. Disponible en: https://www.port80software.com/. [Accedido: 03-sep-2018].

[12] «Sistema de Seguridad de la Información es clave en la empresa | Vanguardia.com». [En línea]. Disponible en: http://www.vanguardia.com/economia/negocios/422841-sistema-de-seguridad-de-la-informacion-es-clave-en-la-empresa. [Accedido: 03-sep-2018].

[13] «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos», p. 75.

[14] «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas», p. 42.

[15] «Por qué instalar parches debería ser un hábito», WeLiveSecurity, 11-abr-2016. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2016/04/11/software-vulnerable-importancia-parches/. [Accedido: 03-sep-2018].

[16] Mortanauta, «Sistemas Operativos y sus vulnerabilidades», EnRedAndo, 20-may-2017.

[17] «Research Reports Vulnerability Review | Flexera». [En línea]. Disponible en: https://www.flexera.com/resources/research-reports/vulnerability-review.html. [Accedido: 03-sep-2018].

[18] «Seguridad informática en las organizaciones: los nuevos peligros». [En línea]. Disponible en: https://www.americaeconomia.com/analisis-opinion/seguridad-informatica-en-las-organizaciones-los-nuevos-peligros. [Accedido: 10-nov-2017].

[19] «ISO - International Organization for Standardization». [En línea]. Disponible en: https://www.iso.org/home.html. [Accedido: 03-sep-2018].

ANEXOS

Tabla 20 Aplicación inicial de parches en ambientes no-productivos.
Fuente: Autor

Nro.	Actividad	Personal requerido	Fecha de implementación	Hora de inicio	Hora final	Dependencia a validar	Aplicativo a validar	Tiempo de interrupción del servicio	Comentarios
Prerrequisitos									
1	OBTENER NOTIFICACIÓN FABRICANTE SOBRE BOLETÍN MENSUAL DE ACTUALIZACIONES	**EJECUTORES**	-	-	-				
2	OBTENER AUTORIZACIÓN POR EL DEPARTAMENTO DE SEGURIDAD PARA EL DESPLIEGUE EN SERVIDOR NO PRODUCTIVOS	**SEGURIDAD**	-	-	-				
3	OBTENER UN SNAPSHOT DEL SERVIDOR	**EJECUTORES**	-	-	-	-	-	-	
	APLICACION DE PARCHES AMBIENTES NO PRODUCTIVOS								
1	DESPLIEGUE EN LA CONSOLA WSUS DE PARCHES APROBADOS	**EJECUTORES**	-	-	-	N/A	N/A	-	
2	APLICACIÓN DE PARCHES EN SERVIDORES NO-PRODUCTIVOS	**EJECUTORES**	-	-	-	N/A	N/A	-	
3	REINICIO DE LOS SERVIDORES	**EJECUTORES**	-	-	-	N/A	N/A	-	
4	VALIDACIÓN DE SERVICIOS POR PARTE DEL ÁREA DE DESARROLLO	**DESARROLLO**	-	-	-	N/A	N/A	-	
5	NOTIFICAR ESTADO DE LOS SERVIDORES	**EJECUTORES**	-	-	-	N/A	N/A	-	
Plan de Reverso o Contingencia									
	POR INCONVENIENTES POSTERIOR A LA APLICACION DE PARCHES								
	RESTAURACIÓN DE SERVICIOS UTILIZANDO EL SNAPSHOT								
1	RESTAURACIÓN DEL SNAPSHOT PREVIAMENTE OBTENIDO DEL SERVIDOR	**EJECUTORES**	-	-	-				
2	VALIDACIÓN DE SERVICIOS POR PARTE DEL ÁREA DE DESARROLLO	**DESARROLLO**	-	-	-				
3	NOTIFICAR ESTADO DE LOS SERVIDORES	**EJECUTORES**	-	-	-				
4	ELIMINAR EL SNAPSHOT OBTENIDO DEL SERVIDOR	**EJECUTORES**	-	-	-				
	RESTAURACIÓN DE SERVICIOS SI SE PRESENTAN NOVEDADES CON EL SNAPSHOT								
1	DESINSTALAR LOS PARCHES APLICADOS	**EJECUTORES**	-	-	-				
2	VALIDACIÓN DE SERVICIOS POR PARTE DEL ÁREA DE DESARROLLO	**DESARROLLO**	-	-	-				
3	NOTIFICAR ESTADO DE LOS SERVIDORES	**EJECUTORES**	-	-	-				

Tabla 21 Aplicación inicial de parches en ambiente productivos.
Fuente: Autor

Nro.	Actividad	Personal requerido	Fecha de implementación	Hora de inicio	Hora final	Dependencia a validar	Aplicativo a validar	Tiempo de interrupción del servicio	Comentarios
Prerrequisitos									
1	OBTENER NOTIFICACIÓN FABRICANTE SOBRE BOLETÍN MENSUAL DE ACTUALIZACIONES	**EJECUTORES**	-	-	-				
2	OBTENER AUTORIZACIÓN POR EL DEPARTAMENTO DE SEGURIDAD PARA EL DESPLIEGUE EN SERVIDOR NO PRODUCTIVOS	**SEGURIDAD**	-	-	-				
3	OBTENER UN SNAPSHOT DEL SERVIDOR	**EJECUTORES**	-	-	-	-	-	-	
	APLICACION DE PARCHES AMBIENTES NO PRODUCTIVOS								
1	DESPLIEGUE EN LA CONSOLA WSUS DE PARCHES APROBADOS	**EJECUTORES**	-	-	-	N/A	N/A	-	
2	APLICACIÓN DE PARCHES EN SERVIDORES NO-PRODUCTIVOS	**EJECUTORES**	-	-	-	N/A	N/A	-	
3	REINICIO DE LOS SERVIDORES	**EJECUTORES**	-	-	-	N/A	N/A	-	
4	VALIDACIÓN DE SERVICIOS POR PARTE SOPORTE	**SOPORTE**	-	-	-	N/A	N/A	-	
5	NOTIFICAR ESTADO DE LOS SERVIDORES	**EJECUTORES**	-	-	-	N/A	N/A	-	
Plan de Reverso o Contingencia									
	POR INCONVENIENTES POSTERIOR A LA APLICACION DE PARCHES								
	RESTAURACIÓN DE SERVICIOS UTILIZANDO EL SNAPSHOT								
1	RESTAURACIÓN DEL SNAPSHOT PREVIAMENTE OBTENIDO DEL SERVIDOR	**EJECUTORES**	-	-	-				
2	VALIDACIÓN DE SERVICIOS POR PARTE SOPORTE	**SOPORTE**	-	-	-				
3	NOTIFICAR ESTADO DE LOS SERVIDORES	**EJECUTORES**	-	-	-				
4	ELIMINAR EL SNAPSHOT OBTENIDO DEL SERVIDOR	**EJECUTORES**	-	-	-				
	RESTAURACIÓN DE SERVICIOS SI SE PRESENTAN NOVEDADES CON EL SNAPSHOT								
1	DESINSTALAR LOS PARCHES APLICADOS	**EJECUTORES**	-	-	-				
2	VALIDACIÓN DE SERVICIOS POR PARTE SOPORTE	**SOPORTE**	-	-	-				
3	NOTIFICAR ESTADO DE LOS SERVIDORES	**EJECUTORES**	-	-	-				

GLOSARIO

Término	Definición
Actualizaciones automáticas	**Un servicio que se ejecuta en computadoras con Windows** (actualizaciones automáticas): se refiere al componente de computadora del cliente integrado en los sistemas operativos Microsoft Windows Vista, Windows Server 2003, Windows XP y Windows 2000 con SP3 para obtener actualizaciones de Microsoft Update o Windows Update. **Referencia casual** (actualizaciones automáticas): el término utilizado para describir cuándo Windows Update Agent programa y descarga actualizaciones automáticamente.
Servidor autónomo	Servidor de Windows Server Update Services (WSUS) en el cual los administradores pueden administrar los componentes de WSUS.
Servidor descendente	Servidor de Windows Server Update Services (WSUS) que obtiene actualizaciones de otro servidor WSUS en lugar de actualizaciones de Microsoft o Windows Update.
Política de grupo	Una colección de configuraciones en la política de grupo que se utilizan para controlar cómo los usuarios y las computadoras (a quienes se aplican las políticas) pueden configurar y usar varios servicios y características de Windows. Los administradores pueden usar WSUS con la Política de grupo para la configuración del cliente de Actualizaciones automáticas en el lado del cliente, para ayudar a garantizar que los usuarios finales no puedan deshabilitar o eludir las políticas de actualización corporativas. WSUS no requiere el uso de Active Directory o la política de grupo. La configuración del cliente también se puede aplicar utilizando la política de grupo local o modificando el registro de Windows.

Término	Definición
Servicio de actualización interna	Una referencia informal a una infraestructura de red que usa uno o más servidores WSUS para distribuir actualizaciones.
Servidor de réplica	Se usa para referirse a un servidor de Windows Server Update Services (WSUS) en sentido descendente que refleja las aprobaciones y configuraciones en el servidor ascendente al que está conectado. No puede administrar WSUS en un servidor de réplica.
Microsoft Update	**Un sitio de descarga de Microsoft basado en Internet:** un sitio de Internet de Microsoft que almacena y distribuye actualizaciones para computadoras con Windows (controladores de dispositivos), sistemas operativos Windows y otros productos de software de Microsoft.
Servicios de actualización de software (SUS)	SUS fue el producto predecesor para Windows Server Update Services (WSUS).
Actualizaciones	Cualquiera de una colección de revisiones de software, revisiones, service packs, paquetes de características y controladores de dispositivos que se pueden instalar en una computadora para ampliar la funcionalidad o mejorar el rendimiento y la seguridad.
Actualizar archivos	Los archivos necesarios para instalar una actualización en una computadora.
Información de actualización (también conocida como metadata de actualización)	La información sobre una actualización, a diferencia de los archivos binarios de actualización en un paquete de actualización. Por ejemplo, los metadatos proporcionan información para las propiedades de una actualización, lo que le permite saber cuál es la actualización útil. Los metadatos también incluyen los términos de licencia de software de Microsoft. El paquete de metadatos descargado para una actualización suele ser mucho más pequeño que el paquete de archivo de actualización real.
Fuente de actualización	La ubicación a la que se sincroniza un servidor de Windows Server Update Services (WSUS) para obtener archivos de actualización. Esta ubicación puede ser Microsoft Update o un servidor WSUS en sentido ascendente.

Término	Definición
Servidor ascendente	Un servidor de servicios de actualización de Windows Server (WSUS) que proporciona archivos de actualización a otro servidor WSUS, que a su vez se conoce como un servidor indirecto.
WSUS	Un programa de rol de servidor que se ejecuta en una o más computadoras con Windows Server en una red corporativa. Una infraestructura de WSUS le permite administrar actualizaciones para computadoras en su red para instalar. Puede usar WSUS para aprobar o rechazar actualizaciones antes del lanzamiento, para forzar la instalación de las actualizaciones en una fecha determinada y para obtener informes exhaustivos sobre las actualizaciones que requiere cada computadora en su red. Puede configurar WSUS para que apruebe ciertas clases de actualizaciones automáticamente (actualizaciones críticas, actualizaciones de seguridad, service packs, controladores, etc.). WSUS también le permite aprobar actualizaciones solo para "detección", para que pueda ver qué computadoras requerirán una actualización dada sin tener que instalar las actualizaciones. En una implementación de WSUS, al menos un servidor WSUS en la red debe poder conectarse a Microsoft Update para obtener las actualizaciones disponibles. En función de la seguridad y configuración de la red, el administrador puede determinar cuántos otros servidores se conectan directamente a Microsoft Update. Puede configurar un servidor WSUS para obtener actualizaciones a través de Internet desde lugares tales como: • la actualización pública de Microsoft. • la actualización pública de Windows. • la tienda de Windows.

Término	Definición
Windows Update	**Un sitio de descarga de Microsoft basado en Internet:** un sitio de Internet de Microsoft que almacena y distribuye actualizaciones para computadoras con Windows (controladores de dispositivos) y sistemas operativos Windows. **Servicio informático:** el nombre del servicio Windows Update que se ejecuta en las computadoras. Windows Update detecta, descarga e instala actualizaciones en computadoras con Windows. Dependiendo de la configuración de la computadora y la política, el agente de actualización de Windows puede descargar actualizaciones desde: • Actualización de Microsoft. • actualización de Windows. • Tienda de Windows. • Un servicio de actualización de Internet (red) (WSUS). Los equipos que no se administran en un entorno basado en WSUS suelen utilizar Windows Update para conectarse directamente, a través de Internet, a Windows Update, Microsoft Update o Windows Store para obtener actualizaciones.
Cliente WSUS	Una computadora que recibe actualizaciones de un servicio de actualización de intranet de WSUS. En el caso de la configuración de directiva de grupo que controla la interacción del usuario final con las actualizaciones automáticas: un usuario de una computadora en un entorno WSUS.