

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

Maestría en Sistemas de Información Gerencial

“IMPLEMENTAR UNA INFRAESTRUCTURA PARA LA GESTIÓN, SEGURIDAD E
INTEGRACIÓN DE EQUIPOS APPLE EN UNA INSTITUCIÓN FINANCIERA SN
FINES DE LUCRO”

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

LUZURIAGA AMADOR LUIS ALBERTO
PORTILLA CASTILLO MARIO ALBERTO

GUAYAQUIL – ECUADOR

AÑO: 2018

AGRADECIMIENTO

En primer lugar, agradecemos a Dios por habernos ayudado en cada paso de esta investigación, facilitando y abriendo caminos, y sobre todo por habernos inspirado.

A los formadores, por ser una inspiración para todo estudiante de la maestría, y por ser unos excelentes educadores, personas de gran sabiduría quienes se han esforzado para ayudarnos a llegar al punto en el que nos encontramos.

Sencillo no ha sido el proceso, pero gracias a las ganas de transmitirnos sus conocimientos y dedicación que los ha regido, hemos logrado importantes objetivos como culminar el desarrollo de la tesis con éxito y obtener una afable titulación profesional.

Finalmente al Director de la maestría Ing. Lenin Freire y a la universidad porque nos permitió que se imparta esta maestría, y en fin a todos aquellos que han aportado a que este proyecto se haya realizado.

Luis Luzuriaga, Mario Portilla

DEDICATORIA

Lleno de regocijo, de amor y esperanza, dedico este proyecto, a cada uno de mis seres queridos, quienes han sido mis pilares para seguir adelante.

Es para mí una gran satisfacción poder dedicarles a ellos, que con mucho esfuerzo, esmero y trabajo me lo he ganado.

A mis padres, porque ellos son la motivación de mi vida mi orgullo de ser lo que seré.


A mis hermanos, porque son la razón de sentirme tan orgulloso de culminar esta meta, gracias a ellos por confiar siempre en mí.

Y sin dejar atrás a toda mi familia por confiar en mí, gracias por ser parte de mi

vida y por permitirme ser parte de su
orgullo.

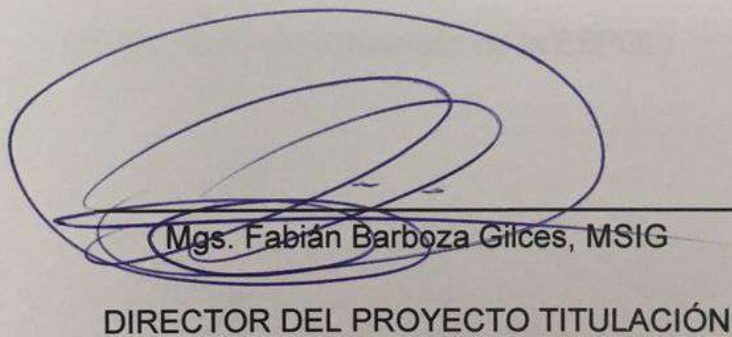
Luis Luzuriaga, Mario Portilla

TRIBUNAL DE SUSTENTACIÓN



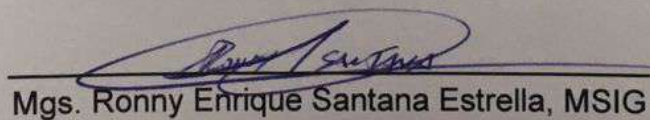
Mgs. Lenin Eduardo Freire Cobo, MSIG

DIRECTOR MSIG



Mgs. Fabián Barboza Gilces, MSIG

DIRECTOR DEL PROYECTO TITULACIÓN



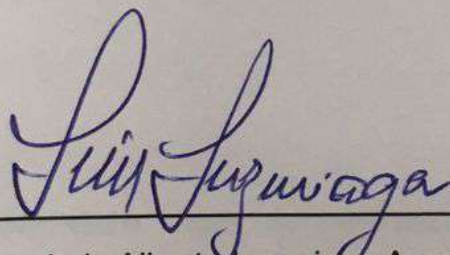
Mgs. Ronny Enrique Santana Estrella, MSIG

MIEMBRO DEL TRIBUNAL

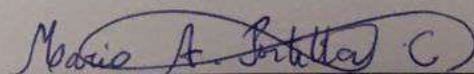
DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Trabajo de titulación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL”

(Reglamento de Graduación de la ESPOL)



Luis Alberto Luzuriaga Amador



Mario Alberto Portilla Castillo

RESUMEN

El objetivo fundamental que persigue el proyecto de tesis es implementar una infraestructura para la gestión, seguridad e integración de equipos Apple en una institución financiera sin fines de lucro, se encuentra estructurado en base a las políticas y procesos de seguridad del estándar manejado en dicha institución.

El presente proyecto, en su desarrollo, se incursiona en los siguientes objetivos específicos que ayudan a alcanzar el objetivo principal, entre los cuales tenemos para analizar el estado de infraestructura referente a la aplicación de actualizaciones del fabricante Apple.

Implementar una infraestructura capaz de centralizar el proceso de descarga y gestionar la distribución de software y parches de seguridad para estaciones de trabajo marca Apple, luego de realizar un proceso de diseño.

Los resultados de la implementación de la infraestructura de las actualizaciones de software y parches de seguridad para equipos Apple son indispensables para mitigar los riesgos de parches que presentan estos equipos y son indispensables para la institución financiera de manera que aportan en los proyectos estratégicos que están encaminados al crecimiento y aporten valor para la organización.

ÍNDICE GENERAL

RESUMEN	VIII
ÍNDICE GENERAL.....	IX
ABREVIATURAS Y SIMBOLOGÍA	XII
ÍNDICE DE FIGURAS.....	XIV
ÍNDICE DE TABLAS	XVI
INTRODUCCIÓN	XVIII
CAPÍTULO 1 GENERALIDADES.....	1
1.1 Antecedentes.....	1
1.2 Descripción del Problema.....	2
1.3 Solución propuesta	3
1.4 Objetivo General	3
1.5 Objetivos Específicos	4
1.6 Metodología	4
CAPÍTULO 2 MARCO TEÓRICO	8
2.1 Seguridad de la Información	8
2.2 Riesgo informático (ISO 17799)	16
2.3 Análisis del riesgo (ISO 27001)	19
2.4 Políticas de seguridad (ISO 17799)	22
2.5 Amenazas a sistemas Apple.....	23

2.6	Métodos de actualización (Apple)	28
CAPÍTULO 3 DEFINICIÓN DE PROCESOS ORGANIZACIONALES		29
3.1	Antecedentes de la empresa.....	29
3.2	Infraestructura de la empresa	29
3.3	Proceso actual de parchado.....	31
3.4	Identificación de amenazas	37
3.5	Probabilidad de las amenazas	38
3.6	Descripción general de Sistema Centralizado para Administración de Actualizaciones - SCAA	39
CAPÍTULO 4 ANÁLISIS Y DISEÑO		42
4.1	Análisis de la situación actual y diseño propuesto	42
4.2	Configuración de ambiente propuesto.....	51
4.3	Calidad de servicio de comunicación.....	55
4.4	Integración con Active Directory	57
4.5	Definición de políticas de aplicación de actualizaciones	57
CAPÍTULO 5 IMPLEMENTACIÓN Y PRUEBAS		60
5.1	Instalación de la herramienta en el medio de almacenamiento.....	60
5.2	Configuración de los componentes de la nueva Infraestructura	61
5.3	Plan de pruebas	63
5.4	Pruebas en ambientes no productivos	67
5.5	Planificación de parchado para ambientes productivos.....	69
CAPÍTULO 6 ANÁLISIS DE RESULTADOS.....		73

6.1	Análisis de resultados de acuerdo a la implementación	73
6.2	Evaluación de eficiencia de la implementación.....	75
CONCLUSIONES Y RECOMENDACIONES		77
BIBLIOGRAFÍA.....		81
ANEXOS.....		83

ABREVIATURAS Y SIMBOLOGÍA

AD:	Directorio activo
APPLE:	Empresa estadounidense de equipos electrónicos
CIS:	Center for Internet Security
DNS:	Sistema de nombres de dominio
GEP:	Gestión del proyecto
HW:	Hardware
IOS:	Sistema operativo móvil de Apple
IP:	Protocolo de Internet
ISO/IEC 27017:	Estándar para la seguridad de la información o norma de controles de seguridad
OSX:	Sistema operativo de Apple

PMP:	Administración de Profesional de Proyectos
QoS:	Calidad de servicio
QA:	Aseguramiento de la calidad
SW:	Software
SCAA:	Sistema centralizado para administración de actualizaciones
URL:	Localizador Uniforme de recursos
WSUS:	Windows Server Update Service

ÍNDICE DE FIGURAS

Figura 1.1: Calendarización de actualizaciones	2
Figura 1.2: Calendarización de la operación.	2
Figura 1.3: Iteración Scrum.....	5
Figura 2.1: Resultados del ISO Survey 2016.[7]	22
Figura 3.1: Arquitectura del Servicio de Actualización de Software.....	30
Figura 3.2: Arquitectura del Sistema Centralizado para la Administración de Actualizaciones.....	30
Figura 3.3: Grupos de GPO's para WSUS.....	32
Figura 3.4: Grupos de distribución creados.....	33
Figura 3.5: Aprobación de parches para actualizaciones en equipos.....	35
Figura 3.6: Verificación de actualización en servidor piloto.	35
Figura 3.7: Despliegue de Aprobación de parches para actualizaciones en equipos.....	36
Figura 3.8: Apple no tiene inmunidad a las amenazas.....	39
Figura 3.9: Descripción general de Sistema Centralizado para Administración de Actualizaciones a implementar.	40
Figura 4.1: Diagrama organizacional del proyecto.	44
Figura 4.2: Diagrama de Gantt de actividades.	46

Figura 4.3: Esquema de enlace de red.	56
Figura 4.4: Monitoreo del tráfico.	57
Figura 5.1: Ingreso al servidor para configuración.	60
Figura 5.2: Configuración en el servidor.	62
Figura 5.3: Configuración de alertas.	65
Figura 5.4: Actualización de productos (Software Update).....	66
Figura 5.5: Elección de actualización a desplegar.	66
Figura 5.6: Ejecución para actualización de SW.	68
Figura 5.7: Ejecución para actualización de SW mediante comando.	69
Figura 5.8: Ejecución en fase de producción para actualización de SW.	70
Figura 6.1: Consumo de ancho banda durante el despliegue.	76

ÍNDICE DE TABLAS

Tabla 1: Control de línea base.....	11
Tabla 2: Control de software autorizado.	12
Tabla 3: Control de protección de dispositivos.....	13
Tabla 4: Control de software SCCM.	14
Tabla 5: Control de permisos.....	16
Tabla 6: Control de procedimientos internos y herramientas.....	18
Tabla 7: Control de seguridades.	21
Tabla 8: Cantidad de certificados válidos en los estándares de gestión ISO registrados en todo el mundo en el año 2016. [7]	24
Tabla 9: Herramientas Apple.	26
Tabla 10: Factor de riesgos potenciales.....	28
Tabla 11: Estimación inicial.	46
Tabla 12: Previsión inicial y final en horas.....	47
Tabla 13: Costo de recursos humanos.	49
Tabla 14: Costos de recursos humanos real del Proyecto.	49
Tabla 15: Costo de hardware.....	50
Tabla 16: Costo de software.....	50
Tabla 17: Costos totales.....	51

Tabla 18: Documento de control de política de actualización.	59
Tabla 19: Puertos necesarios.	63
Tabla 20: Estatus de control de actualizaciones del proyecto piloto (Elaboración propia).....	75

INTRODUCCIÓN

En el presente trabajo la empresa que será sujeta al análisis se desarrolla en el ámbito del sector financiero – bancario. Esta institución establece sus proyectos estratégicos en función de las necesidades del cliente, regulaciones del sector público y privado, de sus empleados y de mejoras tecnológicas. Los proyectos que en ella se desarrollan se realizan en base a la experiencia de sus gerencias y están enmarcadas en los procedimientos internos que se regulan la operación en cada área. El parque de equipos de trabajo de usuario final está distribuido en tres fabricantes: Dell, HP y Apple.

A continuación, se expondrá la problemática de no contar con las actualizaciones de parches de software en los equipos de ambiente Apple que han generado un impacto al riesgo de la información. Para esto se analizará, desarrollará y se realizará la gestión de parches e implementación de este servicio para centralizar los procesos de actualizaciones de software y parches de seguridad para equipos de productos Apple.

Iniciaremos revisando en el capítulo 1 la problemática de la empresa financiera frente al marco de actualizaciones de software para productos Apple y ejecución de sus proyectos para establecer el objetivo a seguir. Se desarrollarán los objetivos específicos que ayuden a establecer un camino a seguir hacia el objetivo general de

la tesis. Adicionalmente, es necesario indicar la solución propuesta, por lo que en este primer capítulo se definirá el alcance de la propuesta de proyecto.

Una vez que hayamos definido la problemática y sus objetivos específicos, en el capítulo 2 se revisará el marco teórico a aplicar, el análisis de riesgo que afecta a la empresa, sus seguridades y sus amenazas. Además, revisaremos los aspectos de métodos de actualización de software para productos Apple (iMac y MacBook Pro).

Continuando con el capítulo 3 se iniciará con el levantamiento de información de los procesos y procedimientos y se expondrá la infraestructura utilizada en la empresa. Una vez realizada la propuesta del proceso de parchado que administrará la empresa financiera. Así mismo, se propondrá la estrategia a seguir para la ejecución e implementación de la metodología.

Luego en el capítulo 4 se ejecutará un análisis y diseño de la implementación que usaremos un Sistema centralizado para administración de actualizaciones (SCAA), como se manejará su administración, almacenamiento y operación del SCAA. Sin embargo, se dejará los requerimientos de la capacidad y ancho de banda en el uso del SCAA para obtener buen resultado en la aplicación de las políticas de actualización de parches y software para productos Apple.

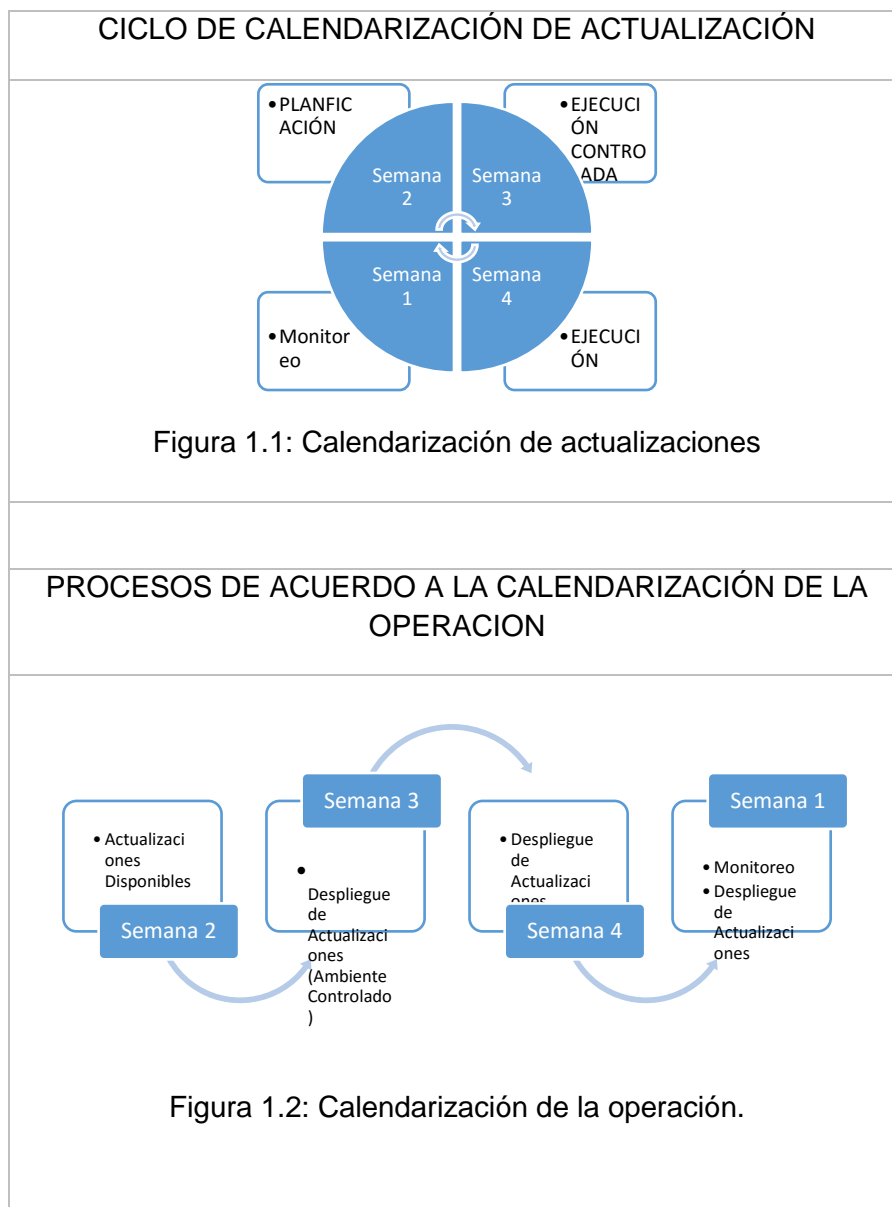
Seguimos con el capítulo 5 con la implementación y pruebas de la herramienta, para lo cual ya definimos el medio de almacenamiento a usar, la configuración de políticas del AD, configuración de la red y la instalación, configuración y ejecución de la herramienta de parchados para los productos Apple en los ambientes de producción. Finalmente, se realizará un análisis de los resultados, conclusiones y recomendaciones del proyecto con los beneficios obtenidos y las mejoras por aplicar en la empresa del sector financiero - bancario.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

La empresa financiera a evaluar está dedicada a ofrecer los servicios bancarios de calidad a través de un modelo de gestión de negocios exitoso, entre los productos más destacados están los créditos para personas y empresas, cobros en línea, facturación de comercializadoras, gestión de su tarjeta de crédito y manejo de cuentas de ahorros y corrientes en diferentes canales electrónicos y aspira ser el primero en tener tecnología de punta y ser innovador en la aferencia y consumo de sus servicios y productos. Su cobertura únicamente tiene soporte para equipos que usan productos del fabricante Microsoft; la periodicidad del servicio de actualización es mensual y se calendariza de la siguiente manera:



Esta institución busca en convertirse en el principal apoyo del desarrollo productivo del país, con una amplia red de puntos y canales que le permitirán atender a un mayor número de clientes en todas las provincias, con la mejor calidad de servicio, innovación en productos y servicios, programas diferenciadores de responsabilidad social sustentables, apoyándose siempre la tecnología como un medio para proponer un excelente servicio.

1.2 Descripción del Problema

La problemática planteada está localizada dentro de una institución financiera donde se identificó las siguientes novedades:

- Las estaciones de trabajo de usuario final de marca Apple, no cuentan con las últimas actualizaciones de software disponibles y publicadas por parte de su fabricante.
- No se cuenta con la capacidad de servicio para incorporar en la operativa actual de distribución de parches y actualizaciones de los equipos del fabricante Apple.
- Existe un riesgo potencial para la institución ya que al no contar con las actualizaciones que se basan en las recomendaciones del fabricante Apple.

1.3 Solución propuesta

La solución propuesta a la problemática evidenciada, se desarrollará bajo el siguiente contexto.

- Para el problema de las actualizaciones de estaciones de trabajo de usuario final de marca Apple, se realizará una gestión para la administración de parches e implementación del servicio de centralizar los procesos de actualizaciones de software y parches de seguridad.
- Se instalará un servidor físico Mac OSX que será utilizado como base para habilitar un sistema centralizado para la administración de las actualizaciones a través de una consola.
- Mitigar la brecha de desactualización del sistema operativo y de las actualizaciones de software emitidas por los fabricantes Apple a través de la solución propuesta.

1.4 Objetivo General

Implementar una infraestructura para la gestión, seguridad, e integración de equipos Apple en una institución financiera, sin fines de lucro.

1.5 Objetivos Específicos

El cumplimiento de los objetivos específicos establecidos a continuación ayudará a alcanzar el objetivo general de este proyecto.

- Analizar el estado de infraestructura referente a la aplicación de actualizaciones del fabricante Apple.
- Implementar una infraestructura capaz de centralizar el proceso de descargas y gestionar la distribución de software y parches de seguridad para estaciones de trabajo marca Apple, luego de realizar un proceso de diseño.
- Analizar los resultados obtenidos luego de un proceso de pruebas en la infraestructura de actualizaciones de software y parches de seguridad para equipos Apple.

1.6 Metodología

Nuestro marco de estudio de la institución que emplea lineamientos y busca cubrir los riesgos altos en tecnología, al integrar soluciones tecnológicas focalizadas en resolver los problemas de actualizaciones de software y parches de seguridad en equipos Apple, homologar sus procesos individuales en busca de estandarizarlos a los macro procesos de la organización con el propósito de mitigar la brecha de desactualización del sistema operativo y de las actualizaciones de software emitidas por los fabricantes y que dichas actualizaciones no afecten mi nivel de operatividad de los usuarios finales. En

esta tesis se ha seguido una metodología ágil, esta metodología permite adaptarnos a los cambios que surjan en este, esta metodología de desarrollo ágil se implementó con varias iteraciones de poco tiempo. Las iteraciones pueden tomar de 1 a 2 semanas, en cada una de ellas se mantiene una reunión con el jefe de proyecto para el seguimiento, se desarrollan las diversas funcionalidades planificadas al completo es decir se basará en un ciclo de prueba para las actualizaciones de software y los parches de seguridad en los equipos clientes.

Scrum

Como hemos mencionado, se usa una metodología de desarrollo ágil para elaborar el proyecto, en concreto, vamos a centrarnos en la metodología aplicada. Scrum es una metodología de desarrollo muy simple, la gestión se basa en la adaptación continua a las circunstancias de la evolución del proyecto, permitiendo realizar cambios si son necesarios.



Figura 1.3: Iteración Scrum.

Cada uno de los ciclos del desarrollo de proyecto es una iteración (sprint) que produce un incremento terminado, cada sprint puede durar entre 1 o 2 semanas, en cada iteración se analiza el proyecto a través de reuniones breves de seguimiento en las que todo el equipo revisa el trabajo realizado desde la reunión

anterior y el previsto hasta la reunión siguiente, de esta manera se puede reconducir una desviación del proyecto de las circunstancias del producto.

Retroalimentación del cliente

El cliente dará retroalimentación una vez cada dos semanas sobre el seguimiento del proyecto para que este no se desvíe de los principales objetivos que se quieren conseguir con esta aplicación.

Pruebas unitarias

Vamos a someter la aplicación desde el principio a pruebas consiguiendo así la detección de errores de diseño en la implementación y corregirlos.

Herramientas de seguimiento

Para el seguimiento del proyecto se han utilizado varias herramientas que nos facilitan la comunicación entre todas las personas involucradas en el proyecto.

Email: Es la principal herramienta de comunicación con el cliente y el resto del equipo involucrado en el proyecto.

Método de validación

La validación del proyecto es realizada por el cliente, ya que es quien tiene la capacidad de comprobar si el proyecto cumple los requisitos esperados. Además, se prueba continuamente la implementación para asegurar que se encuentra fuera de errores y funciona correctamente.

Los supuestos que manejaremos a lo largo del proyecto serán los siguientes:

- La institución financiera nos otorgará la información necesaria.
- Se cuenta con la aprobación de la institución para poder implementar un demo en las actualizaciones de software y parches en los equipos Apple.

- El proyecto cuenta con un plazo de cumplimiento, el mismo que es establecido durante su planeación.
- Se contará con el apoyo de los directivos de la empresa financiera.
- Existe el interés de la institución en utilizar e implementar dicho proyecto.

Las restricciones que se considerarán en el desarrollo de la tesis son las siguientes:

- Por seguridad de la información no se incluirá el nombre de la institución financiera.
- El presupuesto asignado para este proyecto es parte de las actividades de los funcionarios de la empresa financiera.
- El personal estará capacitado para la administración de esta herramienta.
- El plan de implementación estará alineado en los reglamentos que se rigen en la institución financiera siguiendo sus normas de seguridad e infraestructura utilizada.
- El manejo de los abastecimientos de equipos no es parte del presente proyecto puesto que la empresa financiera ya cuenta con los servicios del proveedor.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Seguridad de la Información

La presente propuesta establece las expectativas de seguridad utilizando como marco regulatorio controles CIS[1], proponiendo a la institución una solución que se basa en: acción técnica y desarrollo de controles operaciones eficientes, la cual se basa en un enfoque que se adopte al principio de Pareto[2] en donde la idea principal es tomar solo una parte de todas las medidas de seguridad que se puedan tomar para un alto elevado porcentaje de los beneficios que se obtienen por haber tomado estas posibles acciones.

Como principio especial debemos tener en consideración que luego de las personas, la información es el principal activo de la institución[3] y la tecnología en la que se sustenta se integran de tan manera que son considerados el corazón de la empresa; los empleados de la institución no pueden instalar software de manera autónoma o trasladar datos dentro y fuera de ella en sus bolsillos. Se ha establecido que la aceptación cultural dentro de la organización es fundamental

para poder implementar los cambios necesarios y que los controles técnicos sean respetados en consecuencia el éxito de la prevención de ciberataques.

En este aspecto, se considera el reto más grande que la organización debe superar para lo cual se ve indispensable el refuerzo por parte de la alta gerencia. No existe una solución “por arte de magia” que le permita a la institución obtener soluciones inmediatas, como todo proceso dentro de la institución es fundamental que se desarrollen y operen a partir de un nuevo control para mejorar la prevención de ciberataques.

Por experiencia cuando se introducen nuevos controles dentro de una organización, lo primero que hay que sortear son: la resistencia al cambio y los paradigmas al interno sobre que los objetivos propuestos son exageradamente altos o inalcanzables. Sin embargo, al llevar el ejercicio a la práctica esto dista de la realidad. Una exitosa implementación de los controles requerirá que la organización cambie su chip en la forma de pensar sobre el rol que juega la ciberseguridad y la forma en que abordan las operaciones y la salvaguardia de las tecnologías de información.

La implantación de nuestra propuesta que se basa en que los controles CIS al igual que cualquier otra definición, se debe realizar bajo un enfoque por etapas o fases, empezando por algunos controles y subcontroles de manera temprana e implementando otros de acuerdo a un plan principal que debe ser coordinado y establecido en consenso con la alta Administración (Presidente Ejecutivo) o delegado por la Administración Superior (Directorio/Junta de Accionistas).

Al ser la Organización una institución financiera donde se lleva a cabo la observación de la problemática evidenciada, la organización cuenta con seguridad sólida y que continuamente está revisando y actualizando su postura en cuanto a ciberseguridad y que supervisan sus defensas ante posibles amenazas, se sugiere asumir los esfuerzos de que tomara en promedio alcanzar nivel de inicial de conformidad con los controles teniendo como alcance el procedimiento de actualización de software para equipos Apple (iMac y MacBook Pro). El proceso de implantación de los controles CIS se debe planificar al interno de la organización de manera cuidadosa y bajo la premisa de; cómo realizar una ciberhigiene apoyándose en la estructura de la organizacional para asegurar el éxito.

La propuesta planteada deberá ser trabajada conjuntamente con Gobierno de Riesgo Corporativo, sin embargo, al interno del área de Tecnología se asignarán administrador/administradores de programas para coordinar las tareas relacionadas con la implementación de controles CIS en el siguiente ámbito:

- Administradores de servidores
- Especialistas en estaciones de trabajo
- Ingenieros de redes
- Desarrolladores de software
- Profesionales externos al área de tecnología de la información, tales como: especialistas en recursos humanos/capacitadores, oficiales de negocio, de cumplimiento, entre otros.

Para la defensa de la ciberseguridad el enfoque de implantación no debe ser exclusivamente bajo el contexto técnico, al realizarlo por fases se contribuye a garantizar los beneficios más importantes logrados mediante la implementación

de los controles de mayor prioridad, la propuesta sugiere los primeros cinco controles CIS:

- Implementación del inventario de activos (Controles CIS 1 y 2)
- Las configuraciones estándar (Control 3)

Los primeros cinco controles de seguridad crítica de CIS a menudo se denominan "higiene" de ciberseguridad, ya que varios estudios muestran que la implementación de los primeros cinco controles proporciona una defensa eficaz contra los ciberataques más comunes (~ 80% de los ataques).

CSC 1 | Inventario de dispositivos autorizados y no autorizados.[4]

Objetivo	El objetivo principal no es únicamente identificar que los dispositivos de usuario final que se encuentran conectados a la red sino también comprender qué hay en la red para poder defenderla	
Línea base	3,200 aprox. Estaciones de usuario final.	Revisión Mensual
Control	Como herramienta de apoyo a la gestión de T.I. se utiliza Microsoft System Center Configuration Manager.	Revisión Mensual
Control	Se controla el acceso físico a la red a través Cisco ISE y el acceso lógico a través de autenticación en el dominio.	Revisión Mensual
Procedimiento	Manual de procedimiento para la Administración de Activos de TI	Revisión Anual

Tabla 1: Control de línea base

El objetivo de este control es ayudar a las organizaciones a definir una línea de base de lo que se debe defender en nuestro caso las estaciones de trabajo de usuario final, para tener una comprensión de qué dispositivos están conectados a la red se utiliza la herramienta Microsoft System Center Configuration Manager[5] y de manera complementaria se apoya en el procedimiento de Control de Activos de la Organización para efectos de una administración integral de activos de T.I. Para evitar que los dispositivos no autorizados se unan a una red se destaca: en la capa física del modelo OSI[6] el bloqueo de puertos físicos, a la implementación de la autenticación a nivel de red, el objetivo principal no es únicamente evitar que dispositivos no autorizados se unan a la red, sino también comprender qué hay en la red para poder defenderla.

CSC 2 | Inventario de software autorizado y no autorizado.

Objetivo	El objetivo principal es permitir la ejecución de software autorizado	
Línea base	3,200 aprox. Estaciones de usuario final.	Revisión Mensual
Control	Políticas y Procedimiento de la Organización para la instalación de software autorizado.	Revisión Anual
Control	Como herramienta de apoyo a la gestión de T.I. se utiliza Microsoft System Center Configuration Manager.	Revisión Mensual
Procedimiento	Manual de procedimiento para la Administración Delegada de Servicios de T.I.	Revisión Anual

Tabla 2: Control de software autorizado

El objetivo de este control es garantizar que solo se permite la ejecución de software autorizado en los sistemas de información de una organización para lo cual se apoya en el procedimiento de instalación de Software autorizado que tiene como premisa que únicamente se instalara software de fabricantes que cuente con licenciamiento vigente activos y soporte. Para el inventario de software se apoya herramienta de Microsoft System Center Configuration Manager, y se apoya en el control más importante que una organización puede implementar aquí es la inclusión en la lista blanca de aplicaciones a nivel de antivirus, lo que limita la capacidad de ejecutar aplicaciones solo a aquellas que están explícitamente aprobadas. Este Control a menudo se considera uno de los más efectivos para prevenir y detectar ataques de ciberseguridad. Este esfuerzo requiere que la organización mantenga su modelo operativo donde los usuarios no pueden instalar el software cuando y donde quieran. Este Control, ya implementado proporciona devoluciones inmediatas a una organización que intenta prevenir y detectar ataques específicos.

CSC 3 | Configuraciones seguras de hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores.

Objetivo	El objetivo principal es asegurar que las configuraciones	
Línea base	4,000 aprox. Objetos.	Revisión Mensual
Control	Como herramienta de apoyo a la gestión de T.I. se utiliza Microsoft Active Directory	Revisión Mensual
Procedimiento	Manual de procedimiento de Seguridad de la Información.	Revisión Anual

Tabla 3: Control de protección de dispositivos

Para que los sistemas tecnológicos se instalen con un enfoque en la facilidad de uso y no necesariamente en la seguridad, estos deben tener la capacidad de ser protegidos, mantener las consideraciones para atender configuraciones de sistemas o subsistemas que requieran garantizar una alta seguridad y a su vez que permita configurar de manera segura sus sistemas a escala, en nuestro caso los objetos de directiva de grupo de Microsoft Active Directory ya están establecidos en las Organización. Ya que, al utilizar estándares de configuración o puntos de referencia, como los definidos por el Centro para la Seguridad de Internet, o que se encuentran en el Repositorio del Programa de Lista de Verificación Nacional del NIST asegura las configuraciones requeridas para los activos de T.I.

CSC 4 | Evaluación continua de la vulnerabilidad y remediación.

Objetivo	El objetivo principal es comprender las debilidades técnicas del software que existen en los sistemas de información	
Línea base	Sistema Centralizado para Administración de Actualizaciones	Revisión Mensual
Control	Verificar que el sistema de administración de actualizaciones está cumpliendo su objetivo para ello se utiliza Microsoft System Center Configuration Manager.	Revisión Mensual.
Control	Hacking Ético	Revisión Anual
Procedimiento	Manual de procedimiento para la Administración Delegada de Servicios de T.I.	Revisión Anual

Tabla 4: Control de software SCCM

El objetivo de este Control es comprender las debilidades técnicas del software que existen en los sistemas de información de una organización y eliminar o remediar esas debilidades para lo que la organización implemento un sistema de administración de parches que cubren vulnerabilidades tanto de sistemas operativos Microsoft y Apple como de aplicaciones de los fabricantes citados previamente. Esto permite la instalación automática, continua y proactiva de las actualizaciones para abordar las vulnerabilidades del software. Además, el sistema de administración de parches de la organización se complementa con una revisión de hacking ético para darse la posibilidad de detectar dónde existen vulnerabilidades de software explotables actualmente para que puedan ser remediadas.

CSC 5 | Uso controlado de privilegios administrativos.

Objetivo	El objetivo principal es eliminar permisos o permisos innecesarios del sistema	
Línea base	3,200 aprox. Estaciones de usuario final.	Revisión Mensual
Control	Para verificar que en las estaciones de usuario final no cuentan con usuarios ajenos a la organización se utiliza Microsoft System Center Configuration Manager.	Revisión Mensual.
Control	Administración de plantillas de permisos de acuerdo a las funciones que desempeñan los usuarios	Revisión Anual

Procedimiento	Manual de procedimiento para la Administración Delegada de Servicios de T.I.	Revisión Anual
---------------	--	----------------

Tabla 5: Control de permisos

El objetivo de este control es garantizar que los miembros de la fuerza laboral únicamente cuenten con los derechos, privilegios y permisos de acceso a los sistemas que necesitan para desempeñar sus funciones, ni más ni menos de lo necesario. Con las herramientas de apoyo y el soporte técnico de la operación se asegura que las estaciones de usuario final no tengan un usuario de sistema local o que los usuarios de dominio no tengan derechos de administrador sobre el equipo para evitar que sean utilizados de manera inapropiada en consecuencia se eliminarán permisos o permisos innecesarios del sistema dentro de la organización.

La implementación de los controles CIS es proporcional al tamaño de la organización, sin embargo, se estima el ahorro de los costos generales para la empresa debido a que: se requerirán menos sistemas y administradores de infraestructura para la administración del entorno de ciberseguridad de la organización.

La organización debe tener en cuenta de que el protegerse de los ciberataques se ha convertido en un coste imprescindible asociado al uso de la tecnología (era de Internet) como una herramienta de apoyo al corazón del negocio en la actualidad

2.2 Riesgo informático (ISO 17799)

Para entender el concepto de riesgo informático hay que tener en cuenta que se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

Ante un riesgo, una organización puede optar por tres alternativas:

- Asumirlo sin hacer nada.
- Aplicar medidas para disminuirlo.
- Transferirlo.
- Anularlo.

A la hora de dotar de seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema. Para garantizar la seguridad de los archivos del sistema en la organización, nos apoyaremos en el marco de estándar internacional ISO/IEC 17799 -12.4 que indica: Lineamiento de implementación: Para minimizar el riesgo de corrupción de los sistemas operacionales, se debieran considerar los siguientes lineamientos para controlar los cambios:

- a) Las aplicaciones y bibliotecas de programas sólo deben ser revisadas por administradores capacitados.
- b) Los sistemas operacionales sólo deben mantener códigos ejecutables aprobados y no códigos de desarrollo o compiladores.
- c) El software de las aplicaciones y el sistema de operación sólo se debiera implementar después de una prueba extensa y satisfactoria; las pruebas debieran incluir pruebas de utilidad, seguridad, efectos sobre los sistemas y facilidad para el usuario; y se debieran llevar a cabo en sistemas separados (ver también 10.1.4).

- d) Se debiera utilizar un sistema de control de configuración para mantener el control de todo el software implementado, así como la documentación del sistema.
- e) Se debiera establecer una estrategia de “regreso a la situación original” (rollback) antes de implementar los cambios;
- f) Se debiera mantener un registro de auditoría de todas las actualizaciones a las bibliotecas del programa operacional;
- g) Se debieran mantener las versiones previas del software de aplicación como una medida de contingencia;
- h) Se debieran archivar las versiones antiguas del software, junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte durante todo el tiempo que se mantengan la data en archivo.

En la siguiente tabla se resume los procedimientos internos y las herramientas de TI que se alinean a la solución propuesta:

Procedimiento	Herramienta	Cumple
Actualización del software operacional de la organización	Sistema Centralizado para la Administración de Actualizaciones - SCAA para la configuración y control de todo el software implementado	a, b, c, e, f
Administración de Software y control de licenciamiento	Sistema de control de configuración para mantener el control de todo el software implementado	d, g, h

Tabla 6: Control de procedimientos internos y herramientas

Se puede concluir de manera preliminar que para evitar situaciones de riesgo informático hay que tener las siguientes consideraciones:

- Destinar los recursos para la organización a través de su departamento de comunicación organización lleve a cabo campañas de concientización de ciberseguridad.
- De manera organizada llevar a cabo simulacros en sitio que pongan a prueba los mecanismos de prevención impartidos.
- Revisiones periódicas en sitio a través de un muestreo para verificar el estado de las actualizaciones de sistema operativo.

2.3 Análisis del riesgo (ISO 27001)

Haciendo una revisión del alcance de los dominios del anexo A del estándar ISO/IEC27001:2013 se puede observar de una forma más clara la manera en la que se puede aplicar la seguridad de la información a través de un sistema de gestión para el análisis de riesgos, la propuesta utiliza ISO/IEC 27001:2013 que tienes como objetivo principal: Proteger la confidencialidad, la integridad y la disponibilidad de la información en una empresa; y lo hace averiguando qué potenciales problemas podrían ocurrirle a la información (es decir, evaluación de riesgos) y luego definiendo qué se debe hacer para evitar que ocurran dichos problemas (es decir, mitigación de riesgos o tratamiento de riesgos). Por lo tanto, la filosofía principal de ISO/IEC 27001:2013 12.1, 14.1 y 14.2 se establece en gestión de riesgos indicando donde se da estos riesgos y cómo podemos tratarlos de manera sistemática.

A continuación, en la siguiente tabla se declara su aplicabilidad:

Clausula	Sección	Objetivo de control	Aplica	Justificación
Seguridad de las operaciones	12			
	12.1	Procedimientos y responsabilidades operacionales		
	12.1.2	Documentación de procedimientos operacionales	Si	Actualización de procedimientos para las operaciones de TI donde operan las estaciones de usuario Apple tales como: gestión de redes, gestión de incidencias, administración de TI, seguridad de TI, seguridad física.
Adquisición, implementación y mantenimiento de los SI	14			
	14.1	Requisito de seguridad en los SI		
	14.1.1	Análisis de requisitos y especificaciones de SI	Si	Actualización de políticas, procedimientos y registros relacionados al análisis de requisitos de seguridad para la adquisición de sistemas y software. Actualización de procedimientos para todos los nuevos equipos.
	14.2	Seguridad en el desarrollo de aplicaciones y en procesos de soporte		

	14.2.3	Revisión técnica de los aplicativos por cambios o salida de nuevo sistema operativo	Si	Incorporar dentro del proceso de validación las actualizaciones en sistema operativo Apple.
	14.2.4	Restricciones a los cambios en los paquetes de software	Si	Incorporar dentro del proceso de validación las actualizaciones sobre programas estándar Apple y comprobar la compatibilidad con otro software en uso.

Tabla 7: Control de seguridades

Se justifica el uso de este marco referencial en el incremento de la demanda en las empresas por implementar sistema de gestión estándares, teniendo que: ISO/IEC 27001 experimentó un crecimiento anual del 21%[7] respecto al año 2015.

Estándar	Número de certificados en 2016	Número de certificados en 2015	Cambio	Cambio en %
ISO 27001	33,290	27,536	5,754	+21%

Tabla 8: Cantidad de certificados válidos en los estándares de gestión ISO registrados en todo el mundo en el año 2016. [7]

ISO 27001



Figura 2.1: Resultados del ISO Survey 2016.[7]

2.4 Políticas de seguridad (ISO 17799)

Las políticas de seguridad informática serán fijadas mediante mecanismos y procedimientos que deberá adoptar la empresa para salvaguardar sus sistemas y la información que estos contienen. Serán diseñadas a medida para así recoger las características propias de la organización. Las políticas en su contenido incluirán:

- Generalidades, dentro de este punto se incluirá: objetivo, alcance, responsabilidad, medidas a tomar en caso de incumplimiento de la política.
- Estructura de la política. - Seguridad física, seguridad lógica, seguridad en redes y seguridad en los recursos humanos.

La propuesta de implantación de SCAA utiliza políticas que se basan en las normas y estándares de seguridad informática como ISO/IEC 17799 12.5.3 en cuanto a:

- La utilización únicamente de los paquetes de software suministrados por el fabricante y sin modificaciones.
- Realizar el proceso de descarga de actualizaciones de manera centralizada y desde el sitio oficial del fabricante.

Al descargar software de terceros se debe considerar los siguientes puntos:

- El riesgo de comprometer los controles incorporados y los procesos de integridad.
- Si se debiera obtener el consentimiento del vendedor; a posibilidad de obtener del vendedor los cambios requeridos como actualizaciones del programa estándar.
- El impacto de si como resultado de los cambios, la organización se hace responsable del mantenimiento futuro del software.

2.5 Amenazas a sistemas Apple

En la empresa Apple a través de su portal promueve el uso de las herramientas y recomendaciones necesarias con el propósito de salvaguardar la información, para ello se apoya en los servicios que se detallan a continuación:

Servicio	Objetivo	Fabricante
Actualizaciones de software	Proteger tu Mac involucra usar siempre el software más reciente te ayudan a mantener tu Mac segura.	Apple te envía una notificación cada vez que hay una nueva actualización disponible.

Gatekeeper	Descargar aplicaciones “apps” desde su tienda “App Store” de manera segura.	<p>Apple revisa cada una de las apps antes de autorizar su distribución, y si llega a haber un problema con alguna la retira de inmediato</p> <p>Si una app no está firmada por un desarrollador, Gatekeeper bloquea su instalación y te advierte que no proviene de un desarrollador identificado</p>
FileVault 2	Encripta datos	<p>Encripta todo el disco duro de tu Mac para proteger tus datos mediante el cifrado XTS-AES 128</p> <p>El borrado instantáneo primero elimina las claves de cifrado de tu Mac para que sea imposible acceder a los datos</p>
Llavero de iCloud	Guarda tus contraseñas	Almacena tus nombres de usuario y contraseñas, sincroniza esa información entre los dispositivos que

		<p>elijas: Mac, iPhone, iPad y iPod touch.</p> <p>Información protegida gracias al cifrado AES de 256 bits.</p>
Sandboxing	Bloqueo el código malicioso	<p>La zona protegida de macOS se asegura de que las apps sólo hagan lo que deben hacer al aislarlas de los componentes principales del sistema de tu Mac, de tus datos y de tus otras apps.</p> <p>La zona protegida la bloquea de forma automática para mantener a salvo tu computadora y tu información</p>
Runtime.	Protección en el núcleo mismo.	<p>Brinda protección contra el malware que intenta engañar a la Mac para que trate los datos como si fueran un programa con el fin de vulnerar tu sistema.</p>

Antiphishing	Protección contra sitios web fraudulentos	La tecnología antiphishing del navegador Safari puede protegerte de estas estafas al detectar estos sitios web fraudulentos, desactivando la página y mostrando un aviso para alertarte sobre el posible fraude.
Seguridad avanzada	Touch ID	Nunca guarda la imagen de tu huella digital, sino una representación matemática imposible de reconstituir.[8]

Tabla 9: Herramientas de Apple

Con los mecanismos propuestos por el fabricante Apple se trabaja a fin de minimiza el nivel de los riesgos por amenazas sobre una infraestructura desactualizada. Entre los datos que recoge el informe financiero anual de Apple, el formulario 10-K[9] requerido por la SEC a todas las empresas que cotizan en Bolsa, se incluye un pormenorizado catálogo de los riesgos a los que deberá enfrentarse la compañía en el futuro. Entre todas las amenazas identificadas por la empresa de Cupertino, hay algunas que son obvias, como el contexto económico general, los riesgos de operaciones internacionales, los cambios en el marco regulatorio, etc. Pero el informe también señala algunos riesgos específicos que conviene destacar[10].

Apple sabe que su pervivencia depende de la capacidad de desarrollar productos y tecnologías innovadores[11]. La siguiente discusión de los factores de riesgo contiene declaraciones prospectivas. Estos factores de riesgo pueden ser

importantes para comprender otras declaraciones en este Formulario 10-K. La siguiente información debe leerse junto con la Parte II, Ítem 7, "Discusión y Análisis de la Administración sobre la Condición Financiera y Resultados de las Operaciones" y los estados financieros consolidados y notas relacionadas en la Parte II, Ítem 8, "Estados Financieros y Datos Complementarios" de esta Forma 10-K.

El negocio, la situación financiera y los resultados operativos de la Compañía pueden verse afectados por una serie de factores, conocidos o desconocidos, que incluyen, entre otros, los que se describen a continuación, uno o más de los cuales podrían, directa o indirectamente, causar la condición financiera real y los resultados de operación varían materialmente desde el pasado, o desde el futuro anticipado, la situación financiera y los resultados operativos.

Cualquiera de estos factores, en todo o en parte, podría afectar material y adversamente los negocios, la situación financiera, los resultados de operación y el precio de las acciones de la Compañía:

Factores de Riesgo potenciales	
1	Los inversionistas no deben usar tendencias históricas para anticipar resultados o tendencias en el futuro períodos
2	el desempeño financiero pasado no debe considerarse como un indicador confiable de desempeño futuro
3	Dependencia de las condiciones económicas globales y regionales podrían afectar significativamente a la Compañía.
4	Disminución de los ingresos o valores de los activos y otros factores

5	Competencia a través de precios agresivos y estructuras de muy bajo costo, y emulando los productos de la Compañía y violando su propiedad intelectual
---	--

Tabla 10: Factor de riesgos potenciales

Los productos y servicios de la Apple compiten en mercados globales altamente competitivos que se caracterizan por una competencia de precios agresiva lo que ha derivado en la presión a la baja sobre los márgenes brutos, introducción frecuente de nuevos productos, ciclos de vida del producto cortos que se alinean estratégicamente a estándares industriales cambiantes.

2.6 Métodos de actualización (Apple)

En este proceso de actualizaciones de seguridad la compañía Apple con el fin de proteger a sus clientes, esta empresa no revela, ni confirma sus problemas de seguridad que se presentan hasta que haya llevado a cabo una investigación y estén seguros de las revisiones o las versiones necesarias. El fabricante proporciona una lista de las versiones más recientes en la página actualizaciones de seguridad de Apple[8].

CAPÍTULO 3

DEFINICIÓN DE PROCESOS ORGANIZACIONALES

3.1 Antecedentes de la empresa

El área enfocada a la implementación de los servicios de actualizaciones de software y parches de seguridad para equipos Apple es el área de Medios Tecnológicos – Infraestructura el cual forma parte del proceso de apoyo para los dispositivos del área del negocio. Todo requerimiento de implementación de un proyecto de actualizaciones de software y parchados proviene por parte de Producción Servidores quienes administraran este proceso basándose en normas y políticas de Seguridad.

3.2 Infraestructura de la empresa

El servicio de actualización de software implementado en esta institución es considerado como uno de los servicios críticos que se encuentra en funcionamiento de forma distribuida a nivel nacional, está basado en la herramienta de Microsoft Windows Server Update Services - WSUS para equipos de arquitectura Windows.

El detalle de la arquitectura del servicio para WSUS se detalla en lo siguiente:

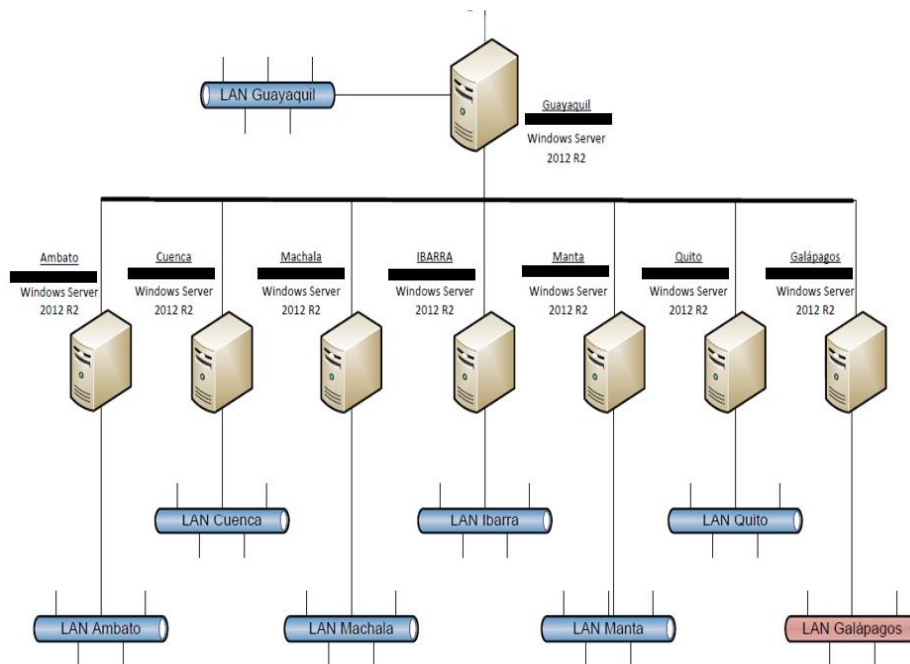


Figura 3.1: Arquitectura del Servicio de Actualización de Software.

Para la infraestructura de equipos Apple se ha diseñado una implementación de una infraestructura capaz de centralizar el proceso de descarga y gestionar la distribución de software y parches de seguridad para estaciones de trabajo marca Apple.



Figura 3.2: Arquitectura del Sistema Centralizado para la Administración de Actualizaciones.

3.3 Proceso actual de parchado

En este documento detallamos el proceso y consideraciones especiales relacionadas al servicio de distribución de parches de seguridad en plataformas Windows basado en WSUS (Windows Server Update Service). Podemos citar que es uno de los servicios críticos que se implementó en esta institución para eliminar posibles amenazas. Está implementado de forma distribuida basándose en la herramienta WSUS de Microsoft que tiene las siguientes características:

Herramienta	Versión	Service Pack
Windows Server Update Service (WSUS)	3.0	SP2

Como parte de la distribución de estos parches de seguridad se consideran los siguientes: Servidores Windows y estaciones Windows de usuarios finales (Estaciones de escritorio y estaciones portables). Se manejan políticas en WSUS tanto para servidores y estaciones creando grupos de gestión de parches a nivel nacional mediante el AD, detallándolos:

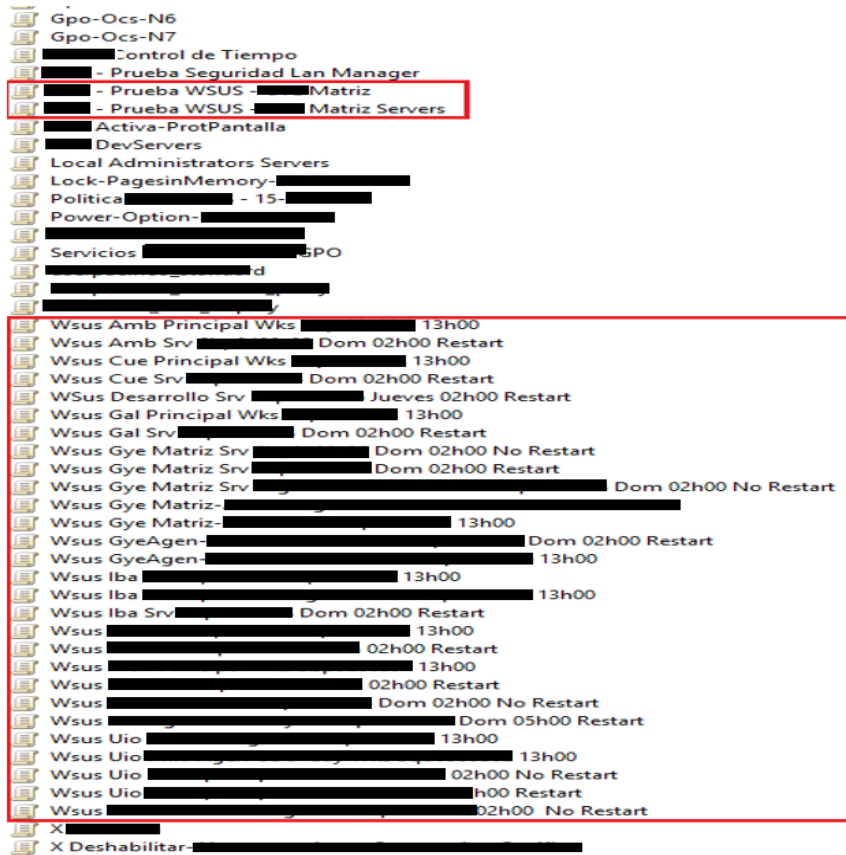


Figura 3.3: Grupos de GPO's para WSUS.

Contamos con un proceso de grupos de distribución para la distribución del parchado a los equipos, detallamos la función de cada grupo de distribución en la consola de distribución de WSUS:

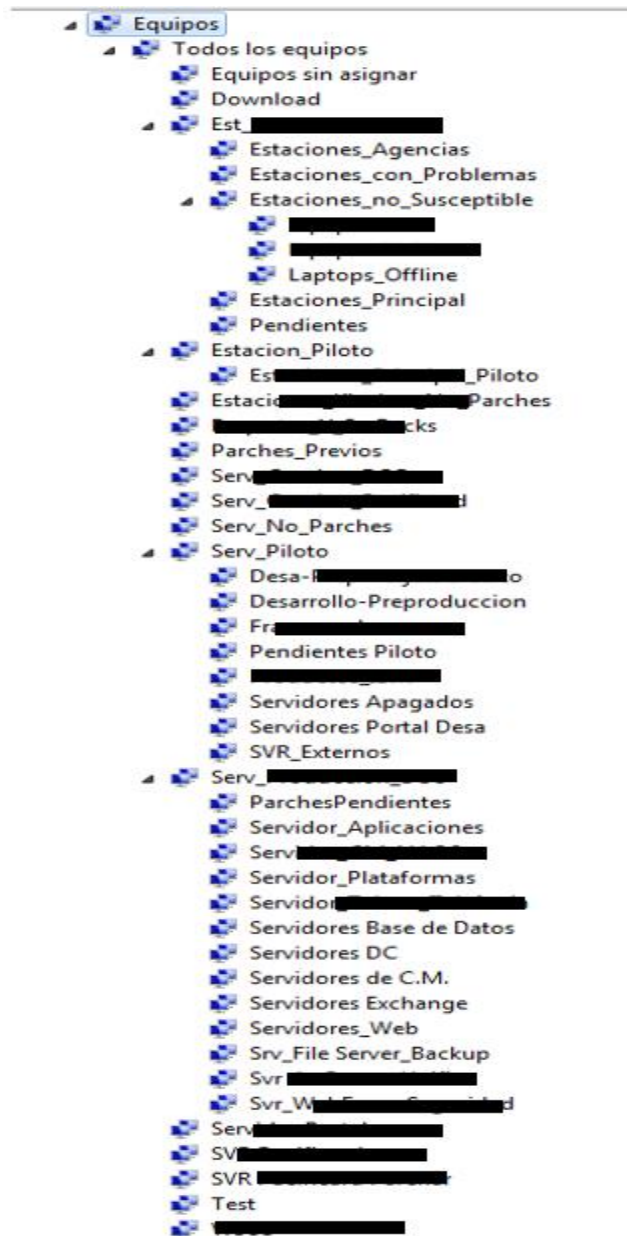


Figura 3.4: Grupos de distribución creados.

Además, tenemos detallado un proceso de despliegue e instalación de actualización mensual de parches de seguridad para estaciones de trabajo y servidores Microsoft que pertenecen a esta institución. Las actualizaciones se realizan en 2 fases:

- Fase Piloto.
- Fase de Producción.

En esta fase piloto tiene como propósito asegurar la estabilidad del entorno antes de instalar las actualizaciones solicitadas en los servidores y estaciones de producción, para lo cual se efectúa la instalación de las actualizaciones de la siguiente manera:

- Servidores:
 - Ambiente Desarrollo.
 - Ambiente Pre –producción.
- Estaciones de trabajo:
 - Área de Producción.
 - Área de Infraestructura.
 - Área de Desarrollo.
 - Área de CYC.
 - Área de proveedor de IT. (Mesa de Ayuda e Soporte Técnico).
 - Área de Seguridad Bancaria.

Estas estaciones de trabajo seleccionadas no afectan directamente a los clientes de esta institución en su operativa diaria y no manejan servicios críticos. Las pruebas se realizan en un período de pruebas de al menos 48 horas donde se realizan las acciones necesarias para verificar que no existan novedades con las aplicaciones instaladas en los servidores y estaciones de trabajo de usuarios. En esta fase el área de Seguridad Bancaria Sección Seguridad de la Información solicita la aplicación de estos parches basándose en el boletín de Seguridad de Microsoft para el mes en curso, el mismo que esta liberado por Microsoft el segundo martes de cada mes. En la siguiente se muestra las aprobaciones de los parches de actualización:

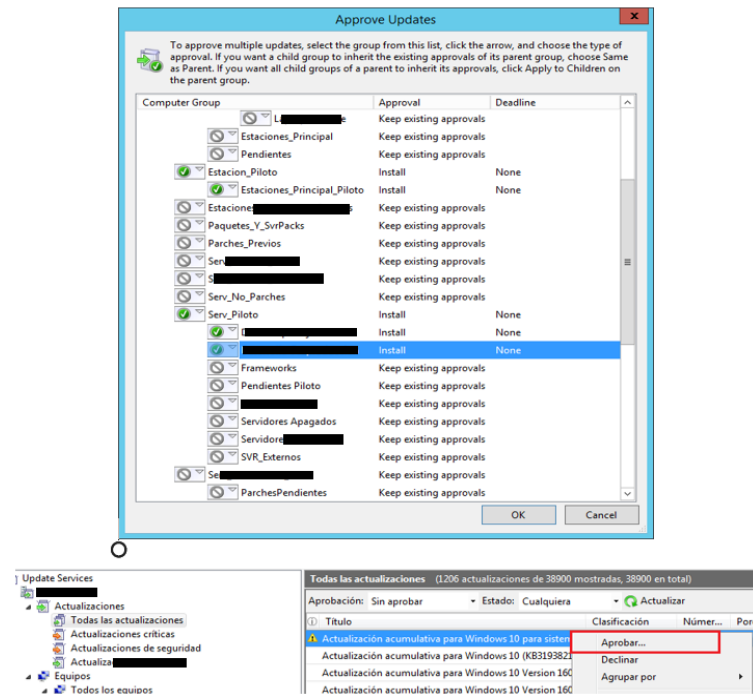


Figura 3.5: Aprobación de parches para actualizaciones en equipos.

En el servidor se verifica que las actualizaciones hayan sido instaladas en los servidores piloto, se realizan revisiones que las actualizaciones fueron instaladas en los equipos y estos fueron reiniciados:

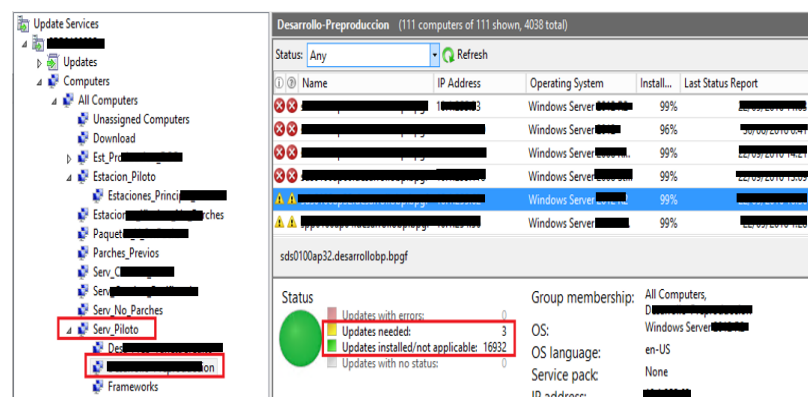


Figura 3.6: Verificación de actualización en servidor piloto.

En esta fase de producción tiene como finalidad distribuir las actualizaciones que en la fase piloto ya se instalaron tanto en estaciones como en servidores de

lanzamiento del boletín de Microsoft hasta el momento en que entregan el informe de gestión con la información de los equipos actualizados en el mes. Para equipos de infraestructura Apple se está diseñando una implementación capaz de centralizar el proceso de descarga y gestionar la distribución de software y parches de seguridad para estaciones de trabajo marca Apple. Se ha manejado mediante descarga de sus actualizaciones a través del App Store, lo que buscamos es centralizar y gestionar los parches necesarios para mantener los equipos actualizados y evitar amenazas en nuestra red.

3.4 Identificación de amenazas

Como todos sabemos la compañía Apple proporciona actualizaciones de seguridad para los equipos (iMac y Mac) a través de update de software y de su sitio de descarga, los clientes o usuarios debemos ser cautelosos siempre en el ingreso de su información personal para evitar cualquier amenaza tanto en el uso de su cuenta para descargar como en la instalación. Es por eso que vamos a centralizar este proceso para evitar este tipo de problemas.

Por normativa interna de la institución que se requiere implementar este proyecto se vio que no exista un procedimiento relacionado con la distribución en ambientes de Sistema Operativo para equipos MAC (IOS) que incluya el involucramiento de las áreas necesarias para las aprobaciones de los niveles pertinentes evitando cualquier riesgo de seguridad y software no deseados que sean instalados por los usuarios.

Por eso buscamos incorporar en la normativa interna un procedimiento de actualizaciones de seguridad y su sistema operativo que no sea Windows (MAC, IOS) considerando también los equipos móviles Apple que se conectan en nuestra

red alámbrica interna debe estar protegidos y seguros. Vamos a basarnos en la Norma ISO/IEC 27017 en los siguientes aspectos o referencias normativas:[12]

- Protección contra software malicioso (malware) en donde podemos revisar en el ítem (véase 12.2).
- Control del software operacional (véase 12.5)
- Restricciones a las instalaciones y uso del software (véase 12.6.2).
- Privacidad y protección de datos personales (véase 18.1.4).

3.5 Probabilidad de las amenazas

Durante mucho tiempo Apple ha presumido ser una plataforma libre de amenazas tanto en sus aplicativos, sistema operativo y malware. Durante los últimos años por lo que concierne a los dispositivos móviles, como para los ordenadores y los equipos portátiles ha habido una expansión increíble, es por eso que este éxito ha llamado también la atención a los cibercriminales.

Hoy en día la realidad es que ninguna plataforma sea Microsoft, Apple u otro es inmune a las amenazas externas, tampoco Apple. De hecho, no solo por parte de los hackers, sino también por investigadores informáticos que encuentran vulnerabilidades en el sistema y diseñan nuevos exploits para dispositivos móviles, para ordenadores tradicionales y hasta para los servicios basados en la nube.

Recientemente un grupo de investigadores que el sistema operativo IOS para dispositivos móviles de Apple detectaron diferentes debilidades en la forma que Apple genera sus contraseñas predeterminadas, estos investigadores crackearon en menos de 1 minuto las contraseñas de los hotspot wifi de IOS. Otro episodio fue el lanzamiento de la versión beta del IOS7 que era mucho más vulnerable esta

fue hackeado por jóvenes españoles en engañar en el bloque de la pantalla. También podemos decir que el popular reproductor de música iTunes y App Store fueron víctimas de ataques de phishing y violaciones de cuenta.

En definitiva, no importa el tipo de plataforma que estés utilizando, si existe la posibilidad de ganar dinero o datos relevantes lo mejor es estar atentos y vigilar, utilizar un software de seguridad poderoso y actualizar siempre los dispositivos, es por eso que se busca implementar una plataforma que gestione, controle y distribuya los parches de actualizaciones del sistema operativo y del software de los equipos MAC – Apple, se ilustra en la figura#8 las posibilidades de amenazas a equipos MAC –Apple.



Figura 3.8: Apple no tiene inmunidad a las amenazas.

3.6 Descripción general de Sistema Centralizado para Administración de Actualizaciones - SCAA

Para llevar a cabo el servicio de SCAA usaremos lo detallado, un servidor Mac OSX Server debido a que en nuestra propuesta su dimensión a implementar

contiene a sistemas operativos de servidores Apple, se plantea como contexto un servidor que permitirá llevar a cabo SCAA para Apple, en donde los administradores puedan modelar un servidor que ejecute SCAA dentro de su firewall corporativo, mediante el cual sincronice el contenido directamente con las actualizaciones, parches de seguridad descargados y poder distribuir las actualizaciones entre los equipos clientes (iMac y MacBook) de forma práctica, planificada y haciendo un uso eficiente en la utilización de sus canales de comunicación a internet, lo que le permitirá a la organización una gestión integral de las actualizaciones.

Podemos indicar que mediante el uso de servidores SCAA solo los ordenadores clientes acceden solo a actualizaciones de software que se permita desde las listas de software instalados mejorando su capacidad de gestionar las actualizaciones de software. Esto es con el objetivo de centralizar las actualizaciones en un servidor y que los equipos clientes puedan actualizarse accediendo al servidor.

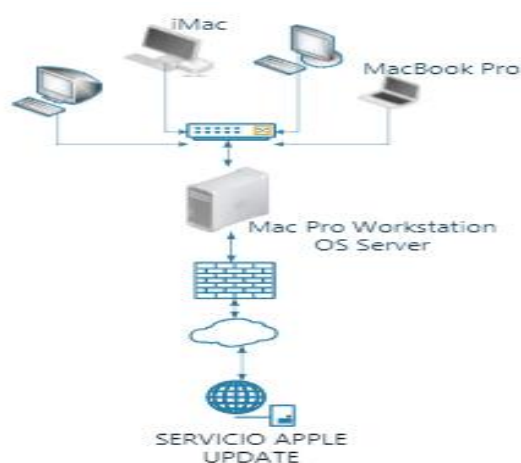


Figura 3.9: Descripción general de Sistema Centralizado para Administración de Actualizaciones a implementar.

Como utilidad a la solución propuesta tendremos la mitigación de vulnerabilidades del sistema operativo de Macintosh (Equipos IMac y MacBook) mediante la aplicación de actualizaciones de acuerdo a las recomendaciones y mejores prácticas del fabricante.

CAPÍTULO 4

ANÁLISIS Y DISEÑO

4.1 Análisis de la situación actual y diseño propuesto

Esta institución en su aspiración de ser los primeros en tener tecnología de punta ha venido adquiriendo equipos Apple para los diferentes departamentos, los cuales necesitan actualizarse periódicamente con salida total a internet para bajarse e instalarse las actualizaciones generando un entorno vulnerable en su red.

En busca de mantener actualizada las estaciones de trabajo de usuario final de marca Apple, se realizará una gestión para la administración de parches e implementación del servicio de centralizar los procesos de actualizaciones de software y parches de seguridad para estos equipos de marca Apple, de una forma práctica, planificada y eficiente en el uso de sus canales de comunicación a internet, permitiendo a la organización una gestión organizada para dichas actualizaciones.

Ante la situación de inseguridad creada por la necesidad de actualización en los equipos, la entidad financiera para el diseño propuesto decide implementar este

servicio mediante la siguiente estructura que utilizaremos; se requiere un servidor de actualizaciones de Apple, para centralizar las actualizaciones en un solo equipo (Servidor) y que los equipos clientes puedan actualizarse a su vez accediendo al servidor.

Se adquiere un equipo Mac Pro con características robustas para el papel de servidor de actualizaciones y se instala en el equipo la AppmacOS Server 5.2. En la actualidad, la actualización de software le ofrece modos de gestionar dichas actualizaciones de software para equipos de Apple en su red. En un entorno no controlado, los usuarios podrían conectarse a servidores de actualización de software de Apple en cualquier momento y actualizar sus ordenadores con software no aprobado por el grupo que maneja esta administración.

Mediante el uso de servidores locales de actualización de software, sus ordenadores cliente acceden solo a las actualizaciones de software que serán permitidos desde listas de software que sean controlados, mejorando su capacidad de gestionar las actualizaciones de software en las estaciones de trabajo de Apple.

Para llevar a cabo esta operación contamos con el siguiente diagrama organizacional del proyecto:

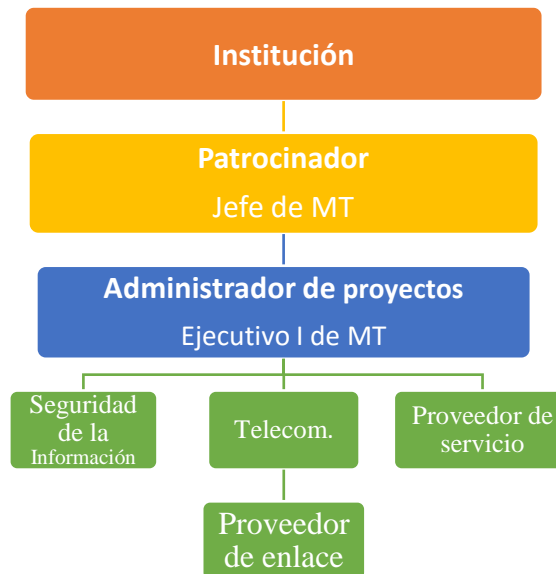


Figura 4.1: Diagrama organizacional del proyecto.

Esta fase del proyecto tiene como objetivo diseñar e implementar una aplicación que permita distribuir las actualizaciones a los equipos Mac y definir las funcionalidades que dicha herramienta realiza, por lo tanto, se describe qué hace dicha herramienta y cómo lo hace internamente. Para ello, se han realizado las siguientes tareas:

- **Análisis de requisitos:** La institución (Cliente) sabía abstractamente lo que quería, pero no como plasmarlo en una herramienta. Se elaboró la toma de requisitos para definir las funcionalidades que esta herramienta realizará.
- **Diseño gráfico de la aplicación:** Se diseña la arquitectura de la herramienta a nivel de interfaz de usuario. Se detalla las diversas acciones a ejecutar para realizar estas tareas de actualizaciones.
- **Arquitectura de la herramienta:** Se detalla cómo funciona la aplicación internamente, se realiza el diagrama de red, configuración en el servidor y como se realizarán el despacho o distribución de los

parches del software y sus actualizaciones.

Construcción

Una vez diseñadas las funcionalidades que forman la herramienta, se pasa a la fase de implementación, que consiste en traducir a desarrollar el diseño de la herramienta previamente realizado.

Despliegue

Una vez la herramienta ha sido implementada y probada, se envía dichas actualizaciones a los equipos Mac (Apple) dependiendo las políticas que tiene esta institución.

Cierre del proyecto

Una vez finalizado el desarrollo e implementación y pruebas, se confecciona la memoria final del documento para su posterior uso.

Estimación de tiempo inicial

En la siguiente tabla se verá un resumen de las tareas que se han estimado antes de iniciar el proyecto y las horas. La duración es de 360 horas.

Tarea	Horas
Gestión del proyecto (GEP)	80
Análisis y Diseño	40
Construcción	160

Pruebas	20
Despliegue	40
Cierre del Proyecto	20
Total	360

Tabla 11: Estimación inicial.

Diagrama de Gantt

En el diagrama de Gantt se pueden observar las tareas que se han de realizar a lo largo de los días, además de ver las posibles dependencias de tareas:

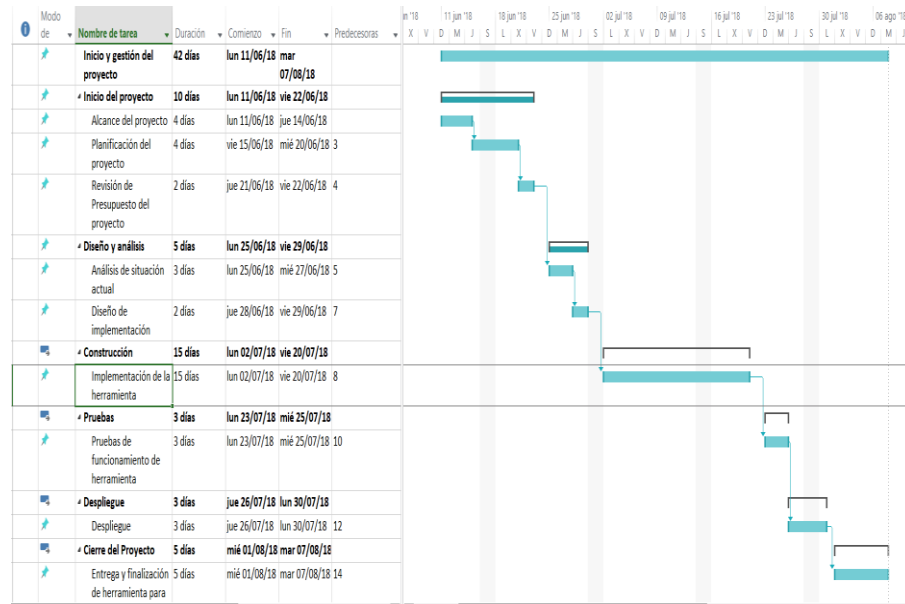


Figura 4.2: Diagrama de Gantt de actividades.

Las dependencias de precedencia que se detallan en el diagrama de Gantt se puede observar como existen tareas que no pudieron ser empezadas hasta que no finalizaron las anteriores.

La dependencia de precedencia más importante se da entre la construcción de la aplicación y el diseño y análisis, ya que hasta que no son recogidos los requisitos y se diseña la herramienta no se puede realizar pruebas.

Con el proyecto finalizado, podemos comparar la planificación final con la planificación que se realizó al inicio del proyecto, analizando donde se desvió el proyecto y que acción se llevó a cabo para terminarlo.

Tarea	Horas planificadas	Horas reales
Gestión del proyecto (GEP)	80	80
Análisis y Diseño	40	40
Construcción	160	180
Pruebas	20	30
Despliegue	20	10
Cierre del Proyecto	40	40
Total	360	380

Tabla 12: Previsión inicial y final en horas.

Como se puede ver en la figura 12, la duración final del proyecto se ha visto aumentada en 20 horas. La implementación del proyecto aumento en 20 horas a causa de que se realizaron cambios en la iteración del desarrollo. Po otro lado, se quería asegurar que la herramienta en el despliegue funcionase perfectamente antes de lanzarse a producción. El despliegue de la herramienta

se vio reducido en 10 horas, ya que lanzar la aplicación a producción no hubo ninguna complejidad.

Para desarrollar el proyecto son necesarios ciertos equipos tecnológicos, a nivel de hardware como software, además de necesitar el equipo humano para el desarrollo.

Hardware:

- Apple iMac 27"
- MacBook Pro.
- Mac Pro.

Software:

- Apple Remote Desktop.

Recurso Humano:

- Patrocinador del Proyecto.
- Administrador del Proyecto.
- Proveedor del servicio a implementar.
- Personal de Telecomunicaciones.

El presupuesto que se mostrará es el costo total de la planificación final, el costo total mostrado en este apartado es el costo que el cliente ha pagado por el proyecto, detallando los distintos tipos de costos como hardware, software y costo del recurso humano.

El proyecto fue llevado a cabo por el equipo del proyecto con asesoría de proveedor de servicio, aunque la mayoría de roles han sido realizados por una

sola persona (Proveedor de servicio) con la ayuda del personal de la institución que se encuentra en el diagrama organizacional del Proyecto.

Rol	Precio por hora
Patrocinador del proyecto (PP)	\$ 0, 00 (Sueldo del trabajador)
Administrador del proyecto (AP)	\$ 0, 00 (Sueldo del trabajador)
Proveedor del servicio (PS)	\$ 30, 00
Personal de Telecomunicaciones (PT)	\$ 0, 00 (Sueldo del trabajador)

Tabla 13: Costo de recursos humanos.

A continuación, se muestran los costos de recursos humanos según las tareas que se han realizado en el proyecto.

Tarea	Horas previstas	Rol	Coste
Gestión del proyecto (GEP)	80		\$ 2400,00
Análisis y Diseño	40		\$ 1200,00
Construcción	180		\$ 5400,00
Pruebas	30		\$ 900,00
Despliegue	10		\$ 300,00
Cierre del Proyecto	40		\$ 1200,00
Total	380		\$ 11.400,00

Tabla 14: Costos de recursos humanos real del Proyecto.

Costo de hardware

Se requiere de hardware específico para implementar estas actualizaciones y realizar las pruebas necesarias, podemos observar en la siguiente tabla el hardware necesario.

Producto	Precio	Unidades	Total
Apple iMac 27"	\$ 5433,00	1	\$ 5433,00
MacBook Pro	\$ 3273,00	2	\$ 6546,00
Mac Pro	\$ 7263,00	2	\$ 14526,00
Total			\$ 26.505,00

Tabla 15: Costo de hardware.

Costo de software

A parte de hardware, también se requiere de cierto software para la administración de computadoras Mac en la red, este distribuye software para realizar las pruebas en estos dispositivos. La mayoría de software a usar es de empresas propietarias o del fabricante Apple.

Producto	Precio	Unidades	Total
Apple Remote Desktop	\$ 79,99	3	\$ 239,97
Total			\$ 239,97

Tabla 16: Costo de software.

Costo total

Después de detallar los diferentes costos del proyecto vamos a calcular en la siguiente tabla el total del costo del proyecto.

Rol	Total
Recursos humanos	\$ 11.400,00
Hardware	\$ 26.505,00
Software	\$ 239,97
Total	\$ 38.144,97

Tabla 17: Costos totales.

4.2 Configuración de ambiente propuesto

Para realizar la configuración en nuestro caso se realizó la instalación en un equipo MacPro al cual se le instaló sistema operativo Mac OS Sierra 10.12 previo a la instalación de macOS Server. Se detallan los requisitos para dicha instalación:

Requisitos para la instalación de macOS Server 5.2

- Mac con MacOS Sierra.
- A partir de 4 GB RAM.
- 10 GB de espacio libre en disco; algunas prestaciones requieren espacio adicional.

Servicios integrados con macOS Server 5.2

- Almacenamiento en caché
- Calendario
- Contactos
- Compartir Archivos
- Mail

- Mensajes
- Gestor de Perfiles
- Time Machine
- VPN
- Sitios web
- Wiki
- Xcode

Servicios Avanzados

- DHCP
- DNS
- FTP
- NetInstall
- Open Directory
- Xsan

Debemos considerar que para la instalación y configuración de macOS Server 5.2 debemos de tener lo siguiente; descargar de macOS Server 5.2 desde App Store, instalación de la aplicación sobre Mac OS Sierra 10.12, configuración del servidor macOS Server con el nombre del host y dirección IP de accesibilidad que son puntos muy relevantes para el funcionamiento.

Una vez instalado y configurado nuestro servidor macOS, hay que utilizar el panel de actualización de software de la app Server para activar o desactivar actualizaciones de software, descargar y comprobar si hay actualizaciones, también podemos quitar actualizaciones de software y ver las actualizaciones de software disponibles.

Cuando iniciemos una actualización, se contactará con el servidor de actualización de software de Apple y solicitará una lista de software disponible para descargar localmente. Puede descargar cualquier paquete de la lista y ponerlo a la disponibilidad de los usuarios. Sin embargo; al activar el servidor de actualización de software, puede elegir el modo a utilizar puede ser automático o manual. En modo automático, las actualizaciones de software se descargarán y activarán automáticamente para que sean instaladas por los clientes. En el modo manual, usted elegirá qué actualizaciones desea descargar y activar para que sean instaladas en los clientes. Las actualizaciones de su servidor se guardarán hasta que las elimine explícitamente. Para realizar estas configuraciones deben de elegir lo siguiente:

- Seleccione actualización de software en la lista de servicios avanzados.
- Vaya a Ajustes y seleccione el modo sea Automático o Manual.

En el modo manual, puede configurar las nuevas actualizaciones para que se descarguen automáticamente seleccionando la opción “Descargar automáticamente las actualizaciones nuevas” en el panel de Actualizaciones. Además, puede buscar nuevas actualizaciones realizando lo siguiente:

- Seleccione actualizaciones en el panel “Actualización de software”.
- Seleccione “Buscar actualizaciones”

Cuando su servidor de actualizaciones de software se encuentra en modo manual, puede descargar las actualizaciones o descargarlas y activarlas. Si elige descargar actualizaciones, estas se descargarán en su servidor

actualización de software. Para que las actualizaciones estén disponibles para que las instalen sus clientes, deberá activarlas realizando lo siguiente:

- Seleccione Actualizaciones en el panel “Actualización de software”.
- En la lista de actualizaciones, seleccione las actualizaciones que desee actualizar.
- Elegir Descargar o “Descargar y activar”.

Es muy importante dirigir a los clientes u ordenadores a un servidor de actualizaciones de software, esto lo realizaremos utilizando el comando `softwareupdate` en Terminal para dirigir a los ordenadores cliente a un servidor de actualizaciones de software. Debe ser administrador para poder utilizar el comando `softwareupdate`.

- Realice una copia de seguridad del archivo/Library/Preferences/com.apple.SoftwareUpdate.plist file, si existe.
- En el cliente, abra Terminal (situado en el directorio Aplicaciones/Utilidades/).
- Introduzca el siguiente comando: `$ sudo softwareupdate --set-catalogURL`

En nuestro caso URL se sustituye por `http://osxgye00ap00.lulumapc.org:8088/index.sucatalog`.

Luego verificamos que actualizaciones están disponibles para ser instaladas mediante el siguiente comando: `$ sudo softwareupdate --list` o `$ sudo softwareupdate -l`.

Para los equipos clientes es necesario que se instala Apple Remote Desktop 3.9 para realizar las tareas de actualización en los equipos clientes de los usuarios.

4.3 Calidad de servicio de comunicación

Las tendencias en el campo de las redes de comunicación han evolucionado y se han constituido con el objetivo de obtener diversas funcionalidades entre ellas podemos acotar la comunicación entre personas y equipos, acceso a información distribuida, gestión y creación de servicios, incremento en la fiabilidad de los sistemas, incremento en la productividad. Es por eso que en las redes de comunicación es necesario cumplir con los requerimientos de protección frente a fallos y alta inmunidad a fenómenos electromagnéticos presente en los ambientes, para lo cual se recurre a incluir inteligencia a los dispositivos con el fin de detectar eventos que reporten daños en la comunicación. Es por eso que en esta institución se debe recurrir a la inclusión de equipos redundantes (2 enlaces) que tomen el control del proceso de comunicación en caso de fallo[13].

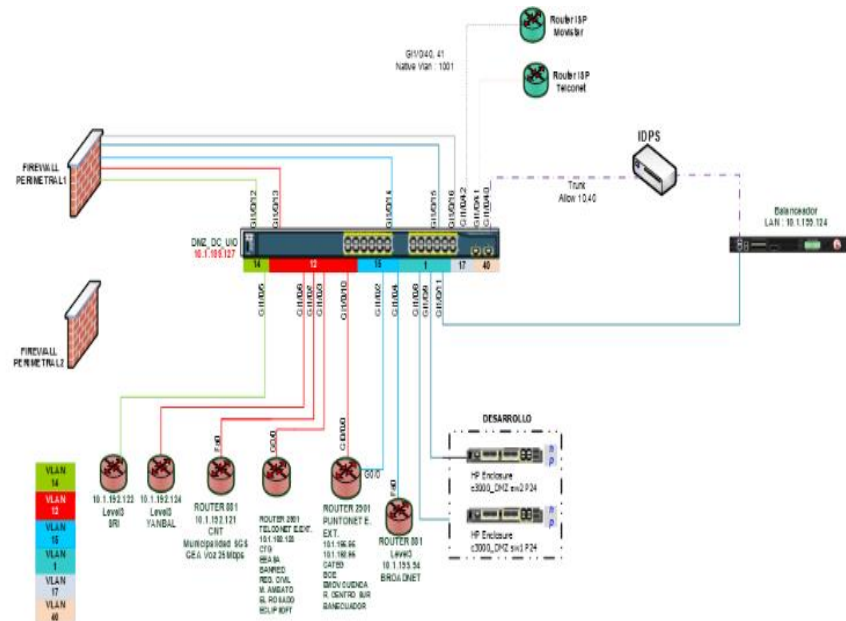


Figura 4.3: Esquema de enlace de red.

Sin embargo; la institución para obtener un mejor beneficio y salvaguardar la calidad en la comunicación en los servicios que ofrece, está implementando herramienta de monitoreo de redes, en la cual se emplean QoS en los servicios ofrecidos que tiene la capacidad de monitorización de hardware, tráfico de red y servicios; entre las ventajas tenemos que es fácil de utilizar, gran interfaz gráfico, es un muy buen sistema de balanceo de carga, permite sacar reportes y es un sistema flexible de alertas.

	LIMIT (% OR KBPS)	KBPS LAST HOUR	KBPS LAST 24 HOURS
class-default	4,096 Mbps	1,486 Mbps	688,628 kbps
qosAgencia4Mbps			
class-default		1,031 Mbps	493,074 kbps
servermatriz	1,024 Mbps	225,744 kbps	72,956 kbps
trafico_ruido	128,0 kbps	127,581 kbps	74,767 kbps
voz	512,0 kbps	93,277 kbps	43,728 kbps
DVR	1,024 Mbps	8,083 kbps	4,103 kbps

Figura 4.4: Monitoreo del tráfico.

4.4 Integración con Active Directory

Para la integración con el AD el equipo principal (macOS Server) debe encontrarse en la red de la institución y dominio para que cuando se ingrese un equipo cliente (MAC) por el personal de soporte, este equipo pueda verse y descubrirse en la consola solo los equipos que se encuentra en producción.

Este proceso de actualizaciones es un proceso que cumple un ciclo, este depende de las actualizaciones del lanzamiento de una nueva versión del software que puede ser mensual o anual para este tipo de dispositivos marca Apple, para tener la gestión de la información actualizada en el AD de estos equipos. Se realizará una validación a nivel del servidor y estaciones mensualmente y podemos también compararlos contra el inventario de activos.

4.5 Definición de políticas de aplicación de actualizaciones

Tiene como finalidad definir políticas para distribuir las actualizaciones de software tanto en las estaciones como en el servidor de producción, asegurando la

instalación de forma segura y controlada, este proceso de aplicación de actualizaciones se realiza una vez terminada la descarga y previo a la autorización de aplicación de actualizaciones en producción por parte del personal de la sección de Controles de Seguridad del departamento de Seguridad de la Información, y se ejecutará hasta el último día del mes en curso.

Además, podemos definir en dicha política el reinicio del equipo y la distribución a estos equipos, en dicho procedimiento detallamos la administración y ejecución del proceso de actualización de parches de software para estas estaciones.

Este despliegue de la política de actualización de software en equipos Apple se detalla lo siguiente:

- Personal de la sección Controles de Seguridad del departamento de Seguridad de la Información solicita la aplicación de parches basado en las actualizaciones que tenemos descargadas para la distribución.

- Personal de soporte procede con el envío de correo al Personal de la sección Controles de Seguridad del departamento de Seguridad de la Información y personal de Medios Tecnológicos con las fechas de instalación de actualizaciones en estaciones para las pruebas correspondientes, dentro del mail debe adjuntarse:
 - Fecha y hora de inicio de fase de actualización.
 - Fecha y hora de finalización de fase de actualización.
 - Listado de actualizaciones pendientes del mes anterior.

En este correo se especifica que si no se recibe reporte de novedades hasta la finalización de la fase de actualización se procede a seleccionar las

actualizaciones que van a ser aprobadas para su despliegue. Una vez que finalice el periodo de la fase de actualización, se procede a enviar un correo en el cual se indica el fin del periodo de actualización, detallando los equipos actualizados y las novedades presentadas.

Control de Aplicación de parches	
Justificación	
Autorizado por	
Software afectados	
Novedades presentadas	
Responsables	
<hr style="width: 20%; margin: 0 auto;"/> Firma C.I:	

Tabla 18: Documento de control de política de actualización.

CAPÍTULO 5

IMPLEMENTACIÓN Y PRUEBAS

5.1 Instalación de la herramienta en el medio de almacenamiento

Para llevar a cabo la implementación se realizó la instalación de lo siguiente:

- Realizar la configuración en el computador administrador.
- Instalación de Apple remote desktop 3.9 que se descargó en el equipo cliente que se descargó bajo el App Server para realizar las tareas de actualización en los clientes.
- Realizar la configuración del servicio en el ordenador a controlar

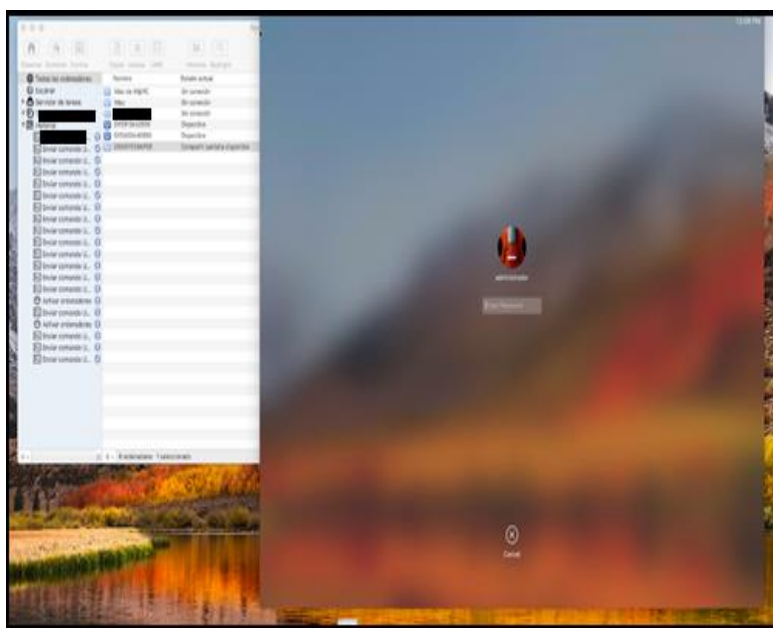


Figura 5.1: Ingreso al servidor para configuración.

En el computador administrador: Se debe descargar la herramienta Apple Remote Desktop para proceder a acceder al servidor. Una vez ingresado al servidor podemos realizar configuraciones en el equipo. Instalación de Apple Remote Desktop; se descarga este aplicativo para realizar las tareas de actualización de los clientes.

En la configuración del servicio en el ordenador a controlar (Cliente); debemos de ir a ejecutar el programa de Preferencias del sistema, ingresamos al panel Compartir, elegir Gestión remota, a continuación, dejamos marcado la selección de gestión remota. En el botón de ajustes del ordenador deberemos tener activa las opciones.

En los equipos clientes usados fueron equipos Apple con las características requeridas por esta institución, dichas pruebas se las realizó en equipos (iMac y MacBook Pro) del área de Tecnología y Desarrollo.

5.2 Configuración de los componentes de la nueva Infraestructura

Entre las configuraciones a realizar tenemos la siguiente:

- Configuración de la red.
- Configuración de la consola de Administración.
- Permisos a puertos.

Para la configuración de la red en los equipos Mac Pro se tomaron en consideración los permisos y accesos necesarios que están en el sitio web de

Apple que recomienda para las implementaciones en un servidor de actualizaciones.

Instalación de Prerrequisitos:

Los prerrequisitos son:

- Descarga de MacOS Server 5.2 desde App Store.
- Instalación de la aplicación sobre MacOS Sierra 10.12.
- Configuración del servidor MacOS Server.

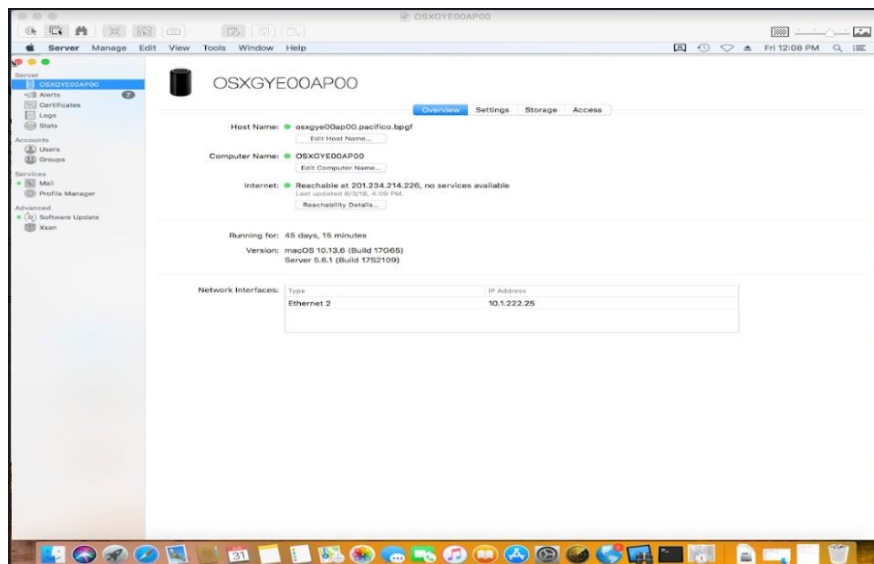


Figura 5.2: Configuración en el servidor.

Para la configuración de la consola de administración en el servidor se descargan MacOS Server 5.2 desde App Store y se ejecuta en el equipo para que funcione la consola de administración. Al momento de la configuración recibirá un mensaje de bienvenida, de ahí escogerá Gestionar y a continuación escoge el nombre del servidor configurado en la Mac Pro, de ahí elegirá el nombre del administrador y su contraseña para su ingreso.

Para los permisos a los puertos se detallan los primordiales que se requieren para el correcto funcionamiento: En el servidor para la distribución de actualizaciones (OSXServer):

Puerto	Número
TCP	311
TCP	626
UDP	626
TCP	660
TCP	687
TCP	8088
TCP	311
TCP	312
TCP	1640
UDP	1701
TCP	1723
TCP/UDP	3659
TCP	5432
TCP	8008
TCP	8080
TCP	8085-8087
TCP	8089
TCP	8096
TCP	8800
TCP	8843
TCP	9006
TCP	10548

En cambio, para el uso del Apple Remote Desktop debemos de solicitar los siguientes puertos:

Puerto	Número
TCP	5900-5909
TCP	3283
UDP	3283
TCP	5988

Tabla 19: Puertos necesarios.

5.3 Plan de pruebas

Este plan de pruebas constituye un universo en el mundo de la ingeniería y su tarea principal es asegurar que se cumpla la calidad y el método de actualizaciones de los productos de software en esta tecnología Apple.

Podemos indicar que para el plan de pruebas en la industria del software a través de su historia se ha definido aspectos fundamentales vinculados directamente a su proceso productivo[14]:

- Los costos y el tiempo: la dificultad de planear proyectos de hardware y software trae consigo problemas en la estimación de sus tiempos y por ende altos costos asociados; creación de métricas y procesos de planeación eficientes han ayudado a amortiguar el peso de estos factores en el desarrollo del software.
- La calidad: debido a la competitividad del mercado en el desarrollo de proyectos de hardware y software la calidad se convierte en un factor determinante a la hora de comercializar los productos. Igualmente, permite disminuir los tiempos de mantenimiento al obtener productos con menor cantidad de errores inyectados y por ende más confiables.

La importancia de las pruebas se puede visualizar teniendo como referencia algunos autores:

- Las pruebas de software permiten pasar de forma confiable del cómodo ambiente planteado por la ingeniería de software, es decir del controlado ambiente de análisis, diseño y construcción o desarrollo, al exigente mundo real en el cual los entornos de producción someten los productos a todo tipo de fatiga.
- La necesidad de productos de hardware y software de alta calidad ha obligado al mercado a identificar y cuantificar factores de calidad como: capacidad de uso, capacidad de prueba, capacidad de mantenimiento, capacidad de ser medible, capacidad de ser confiable y a desarrollar

prácticas de ingeniería que contribuyen a la obtención de productos de alta calidad.

Dentro de nuestro plan de pruebas definimos los siguientes escenarios a utilizar:

- Métodos de actualizaciones
- Productos a actualizar.
- Clasificación de las actualizaciones.

Los métodos de actualizaciones a usar en los equipos Apple se realizarán de forma centralizada desde el servidor Mac Pro a los diferentes dispositivos (iMac, MacBook Pro). En este servidor podemos definir alertas.

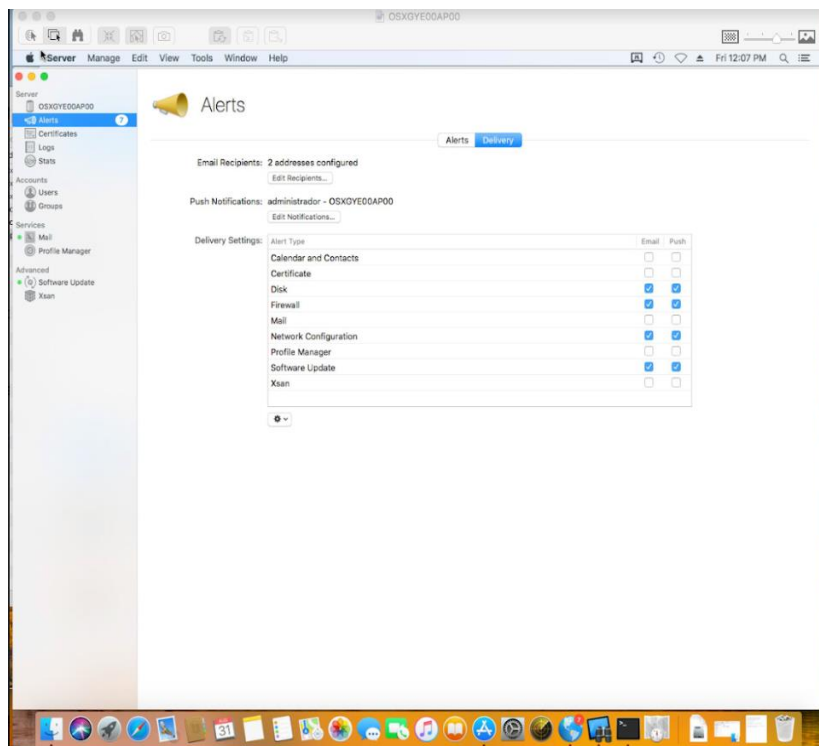


Figura 5.3: Configuración de alertas.

En cambio, en los productos a actualizar; se actualizarán en los equipos Apple a través del servidor Mac Pro a los diferentes dispositivos (iMac, MacBook Pro). Serán aquellas aplicaciones que forman parte del sistema operativo del equipo.

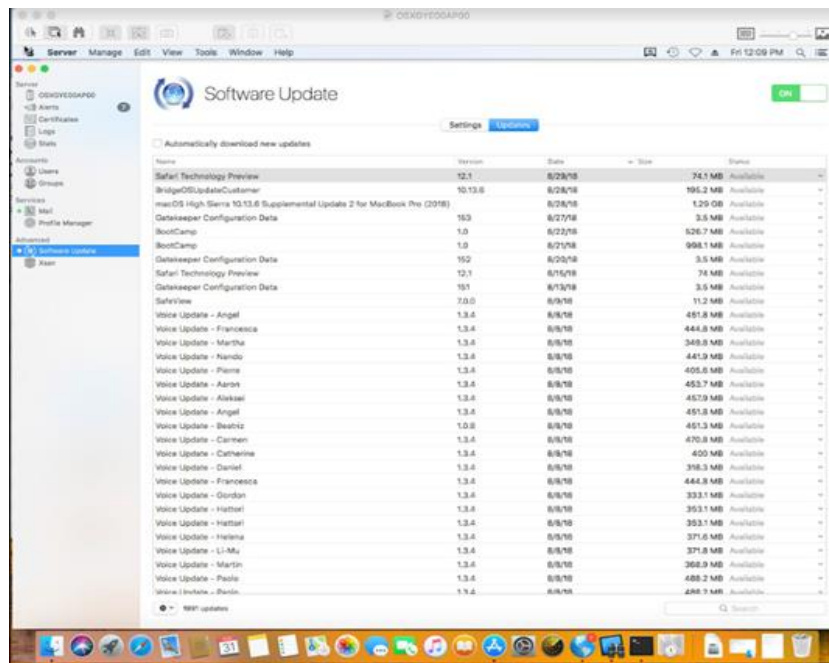


Figura 5.4: Actualización de productos (Software Update).

Sin embargo, en la clasificación de las actualizaciones estas se realizarán de acuerdo al sistema operativo del equipo del cliente, la misma que se almacenarán en los catálogos según se encuentre disponible en el servidor de actualizaciones de los equipos Apple.

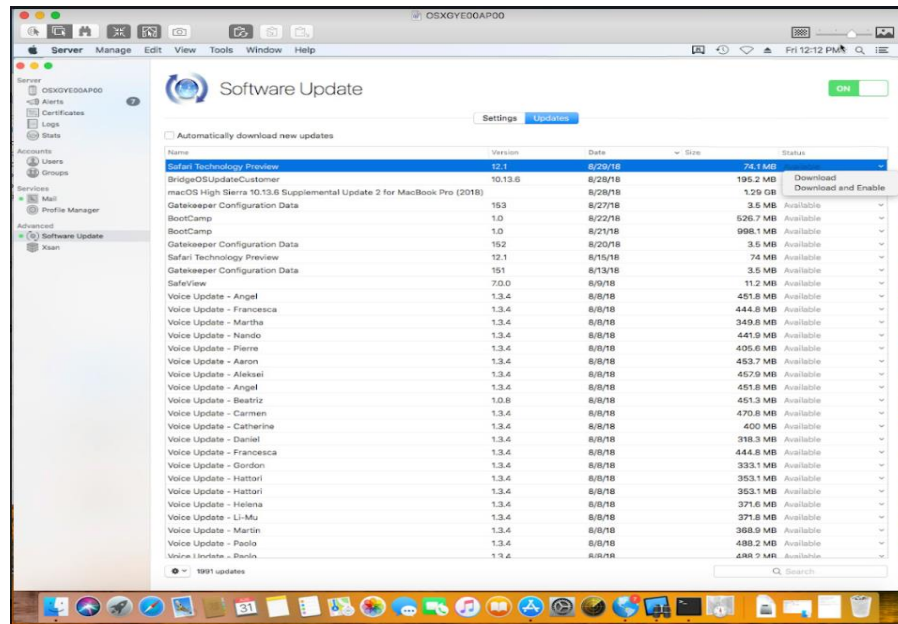


Figura 5.5: Elección de actualización a desplegar.

5.4 Pruebas en ambientes no productivos

La definición de pruebas tiene diferentes connotaciones que en algunos casos llevan a malas interpretaciones. La definición de pruebas de software podemos decir es: “Las pruebas son el proceso de ejecución de un programa con la intención de encontrar errores”, además, esta es una parte fundamental del aseguramiento de la calidad del producto como del software (QA, por sus siglas en inglés), ya que ayuda a asegurar que el producto cumpla con los requisitos.

Estas pruebas realizadas en ambientes no productivos se realizaron de la siguiente manera; utilizamos los equipos Apple (iMac y MacBook Pro) utilizados por el personal de Tecnología y Desarrollo, en donde los equipos estaban ingresados al dominio para poder buscarlo. Sin embargo, utilizamos 2 métodos para estas pruebas de actualizaciones de software:

- Método atendido.
- Método desatendido.

En el método atendido, realizaremos la búsqueda del equipo o equipos Apple (iMac o MacBook Pro) a los que le realizaremos la actualización de parches de

software o aplicativo para enviar a ejecutar la distribución del update al equipo, se ejecutará y quedará actualizado el aplicativo o S.O en caso de haber enviado esta actualización.

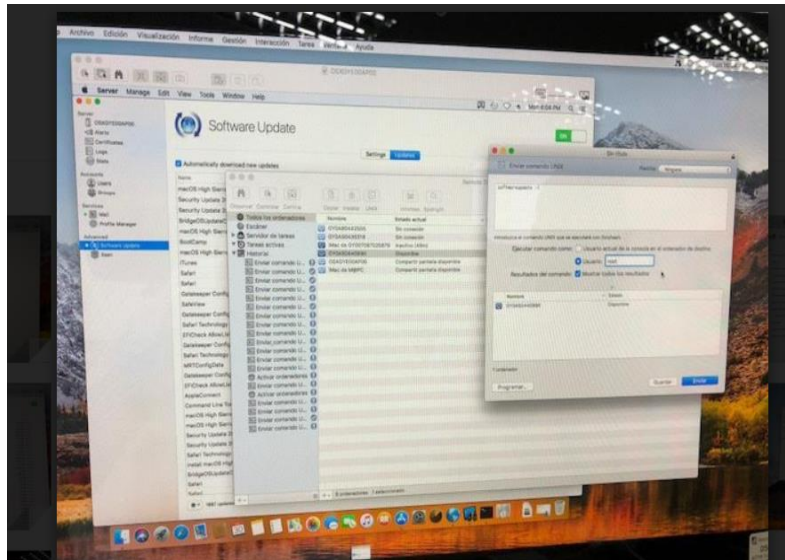
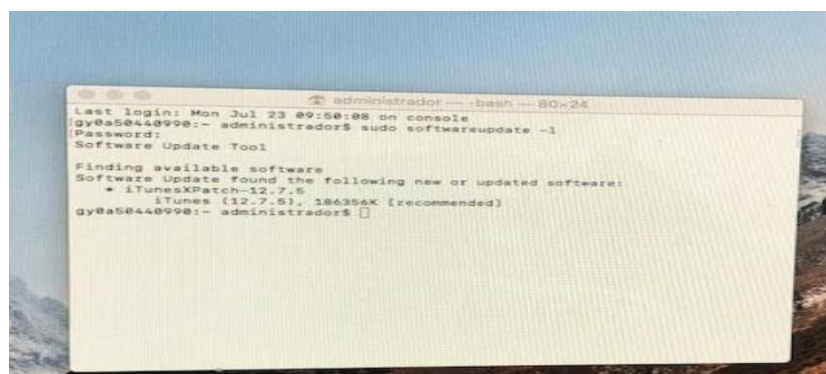


Figura 5.6: Ejecución para actualización de SW.

En el método desatendido, realizaremos la búsqueda del equipo o equipos Apple (iMac o MacBook Pro) a los que le realizaremos la actualización de parches de software o aplicativo para enviar a ejecutar la distribución del update al equipo, en caso de enviar la actualización y este no se ejecute tendremos que realizarlo por este método en el equipo del usuario afectado, realizando la ejecución del comando `sudo softwareupdate -l` en el equipo, esperamos que se ejecute y quedará actualizado el aplicativo o S.O en caso de haber enviado esta actualización.





```

administrador — -bash — 80x24
Last login: Thu Aug 30 13:06:32 on console
[gy0a50440990:~ administrador$ sudo softwareupdate --set-catalog http://osxgye00ap00.pacifico.bpgf:8088/index.sucatalog
[Password:
]
Changed catalog to http://osxgye00ap00.pacifico.bpgf:8088/index.sucatalog
[gy0a50440990:~ administrador$ sudo softwareupdate -l
Software Update Tool

Finding available software
No new software available.
gy0a50440990:~ administrador$ █

```

Figura 5.7: Ejecución para actualización de SW mediante comando.

5.5 Planificación de parchado para ambientes productivos

Dentro de la planificación del parchado a los equipos, esto se definirá de acuerdo a las políticas; el procedimiento detalla la administración y ejecución del proceso de actualización de parches de software en estaciones de trabajo Apple (iMac, MacBook Pro) pertenecientes a la institución financiera.

- Las actualizaciones se realizan en fase:
 - Fase de Producción.

Esta fase de producción tiene como finalidad distribuir el parchado o actualizaciones en estaciones de trabajo Apple (iMac, MacBook Pro), asegurando la instalación de forma segura y controlada, este proceso de aplicación de actualizaciones de parches en software o S.O, se realiza una vez previo a la autorización de aplicación de actualizaciones en producción por parte del personal de la sección de Controles de Seguridad del departamento de Seguridad de la Información y se ejecutará una vez aprobado.

Su despliegue en la fase de Producción con la autorización por parte del personal de la sección de Controles de Seguridad del departamento de Seguridad de la

Información, se procede con el despliegue de actualizaciones a partir del día indicado a las 20:00. Para esta fase, se procede a seleccionar las actualizaciones que fueron aprobadas durante dicha fase:

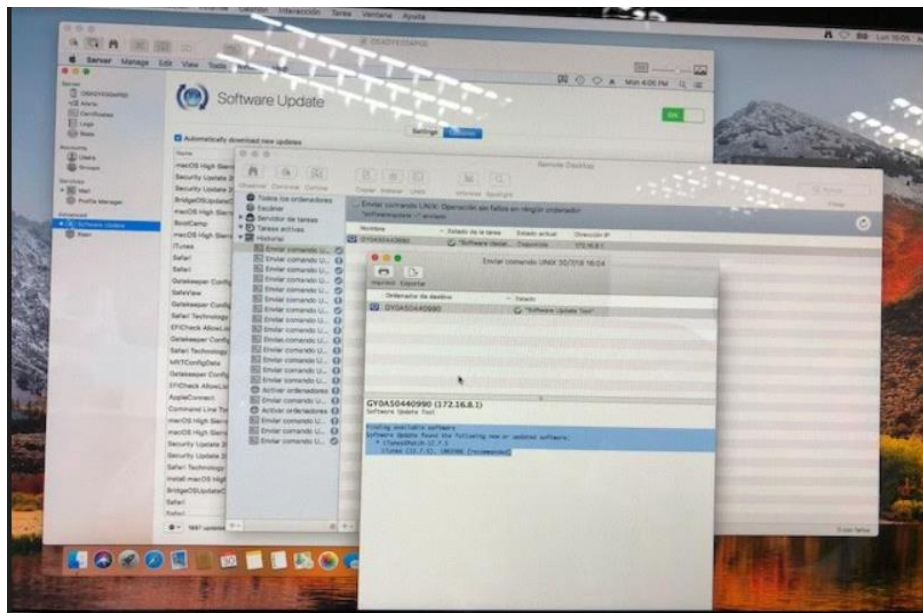


Figura 5.8: Ejecución en fase de producción para actualización de SW.

Debemos de tener en consideración que, al escoger los parches, estos serán habilitados y descargados para en lo posterior ejecutar los comandos desde el servidor o desde la consola de administración que realizarán la actualización a los equipos clientes.

La aplicación de actualizaciones a los equipos Apple se hace de forma asistida, y se deben de seguir los siguientes pasos:

- Informar de las actualizaciones a realizar para que se proceda después de la aplicación de parches a reinicio de los equipos.
- Se revisa y se solicita la aprobación de los parches o actualizaciones a distribuir por parte de Seguridad de la Información.

- En caso de presentarse algún inconveniente es necesario informar al personal (Producción Servidores) para que proceda a la revisión y realizar los escalamientos de notificación necesarios a la institución financiera.
- Al finalizar el proceso se informa de su culminación del proceso de parchado en las estaciones.
- Obtener un reporte preliminar del estado de aplicación de parches en las estaciones y debe ser enviado a los responsables (Producción Servidores, Seguridad de la Información y personal de Soporte de estaciones de usuario final) para que tomen las acciones correspondientes para los equipos a los que no se ha alcanzado a realizar la aplicación de parches de manera automática.
- Una vez que se han llegado a todos los equipos en Producción (o a todos los equipos disponibles), es necesario realizar un informe sobre el estado del proceso para el mes siguiente, para lo cual es necesario realizar el reporte de gestión mensual.

Debemos de tener las siguientes consideraciones:

- Cuando se ingresa un equipo o se elimina, el personal de soporte que realiza el cambio debe realizar la solicitud de Ingreso/Eliminación del equipo de los servicios de AD, DNS para de esta manera mantener un inventario de equipos actualizados y tener en la consola solo los equipos que se encuentren en Producción.
- El proceso de actualizaciones es un proceso que cumple un ciclo puede ser mensual, trimestral estos dependen del lanzamiento del boletín de parches de actualizaciones a los aplicativos o IOS de los equipos Apple.

- En caso de que se liberen actualizaciones dentro del mes pero que estas hayan estado disponibles y no hayan sido ejecutadas, quedarán para ser instaladas en el siguiente ciclo.
- Se realizará la validación a nivel de estaciones y servidor, contra el inventario.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 Análisis de resultados de acuerdo a la implementación

En el capítulo anterior se estableció la implementación y pruebas en el desarrollo del plan del proyecto de distribución de las actualizaciones de parches. Para el proceso de despliegue se establecieron métodos de actualizaciones para realizar el seguimiento oportuno, así mismo para el proceso de monitoreo y control del despliegue, se establecieron métricas de rendimiento las cuales formaron parte del seguimiento, el detalle de los mismos se presenta a continuación[15]:

Control de distribución de parches de software en ambiente de equipos Apple
Software a actualizar: Office 2016, Spotify
Autorizado por: Seguridad de la Información – Controles, Producción Servidores
Justificación: Programas necesitan estar actualizados para el trabajo diario de los usuarios.
Novedades presentadas: N/A
Responsables:
Equipos afectados: Personal de IT (Equipo de FV, Equipo de JS, Equipo de PZ)

<p>_____</p> <p>Firma</p> <p>C.I:</p>

Administración de uso de la red por despliegue de parches o actualizaciones de equipos Apple					
#	Evento	Riesgo	Factor de riesgos		Medidas a tomar
			Personas	Procesos	
1	Ancho de banda adecuado	Moderado	X		Ninguna, fue mitigado ese riesgo.
2	Permisos para despliegue de parches a los equipos	Alto	X		Seguimiento a todas las actividades por permisos a usuarios.
3	Fallas de partes o componentes de aplicativos a actualizar	Moderado	X		Ninguno, todos los componentes se encuentran en perfecta condiciones

Métricas de rendimiento		
Métrica	Valor	Observación
Variación en rendimiento de red por despliegue	0	No hay variación.
Variación en cronograma	0 %	Depende de la disponibilidad del recurso humano en el proyecto
Índice del rendimiento de la red	1.00	No existe afectación en la red.
Índice del rendimiento del cronograma	1.0%	Cronograma según lo previsto

Lecciones Aprendidas	

Control de Cambios	
Justificación	
Autorizado por	
Software afectados	

Tabla 20: Estatus de control de actualizaciones del proyecto piloto (Elaboración propia).

Las herramientas presentadas en este capítulo nos permiten analizar los resultados del proyecto en la implementación para el despliegue de las actualizaciones de parches del software para equipos Apple (iMac y MacBook Pro). En este caso, el proyecto no tuvo afectación con el manejo de tiempo y rendimiento de la red. Los valores obtenidos de las métricas nos muestran y ayudan al seguimiento al proyecto.

6.2 Evaluación de eficiencia de la implementación

Para la evaluación de la eficiencia de la implementación del proyecto de despliegue de actualizaciones y parches se utilizó la herramienta de monitoreo de consumo de la red que permita justificar dichos resultados de la implementación de la infraestructura de las actualizaciones de software y parches de seguridad para equipos Apple para la cual se monitoreaba el consumo de ancho de banda durante el despliegue de las actualizaciones de los aplicativos mostrando un consumo moderable.

Podemos indicar que la configuración de la red de la empresa y el uso de ancho de banda que tienen asignados en esta institución financiera podemos enviar las actualizaciones a los equipos Apple (iMac y MacBook Pro) sin ningún problema ni afectación en la red y estos son indispensables para mitigar los riesgos de parches que presentan estos equipos de manera que aportan en los proyectos estratégicos que están encaminados al crecimiento y aporten valor para la organización.

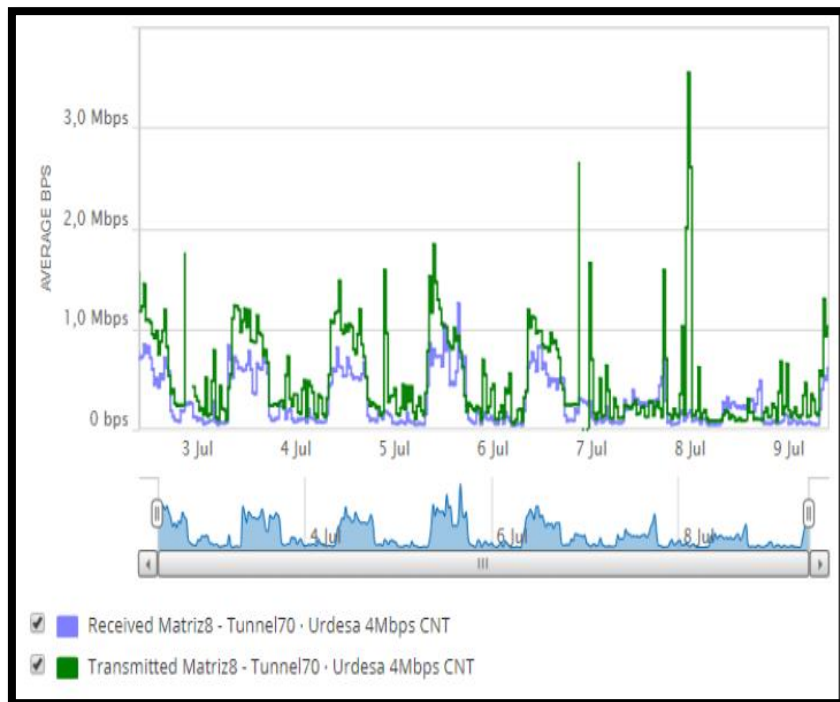


Figura 6.1: Consumo de ancho banda durante el despliegue.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. Se implementó una infraestructura centralizada en el proceso de descarga y gestión de la distribución de actualizaciones para software, se usó la metodología en el proceso de análisis, construcción, diseño y cierre; así como en la implementación de cada proceso como el alcance, recurso humano, tiempo, costo y la integración. Se ejecutó un plan piloto de pruebas implementando un servidor SCAA para satisfacer las necesidades de administración, seguridad y control de las actualizaciones para luego ponerlo en producción y así haber mitigado todos los sucesos que se suscitaron. Esto ayudó a la empresa a mantener un sistema de mejora continua y mitigar los riesgos que se habían relacionados por estas actualizaciones.
2. Se ejecutó el método de despliegue mediante un proyecto piloto y en su fase de producción, dentro de los resultados se observó que a través de las herramientas utilizadas en el proyecto fue posible gestionar y distribuir sus actualizaciones sin tener variación en la red, su cronograma y riesgo del proyecto. De esta manera, se puede concluir que la implementación presentada permite su distribución de actualizaciones a los diferentes equipos usados en este proyecto sin problema, mejorando la gestión, seguridad e integración de estos dispositivos en un ambiente controlado, sobretodo

produce satisfacción en la mitigación de las vulnerabilidades que se encontraban expuestos porque les brinda tranquilidad de que existe un control efectivo en dicha implementación.

3. Podemos indicar que a nivel de red y el ancho de banda utilizado para el mecanismo del despliegue de las actualizaciones de los parches para los equipos Apple (iMac y MacBook Pro) no hubo novedades y su disponibilidad en el servicio no existió afectación en el servicio implementado. Su tasa de transferencia fue de 800kbps.
4. Se identificó la metodología de trabajo de la institución financiera para estas actualizaciones, se pudo determinar que sus procedimientos no estaban orientados bajo las mejores prácticas de seguridad para estas actualizaciones de los equipos Apple. Se incluyó el método de actualizaciones para estos equipos, sin que afecte algún riesgo de seguridad y su adaptabilidad para este tipo de implementación.
5. Se desarrolló una propuesta analizando el estado de la infraestructura referente a la aplicación de actualizaciones a los aplicativos del fabricante Apple, basándonos en medir los riesgos en tener los equipos conectados a internet desde la red interna, validando desde la gestión e integración de estos equipos desde el servidor capaz de centralizar el proceso de descarga y gestionar la distribución de software y parches de seguridad para estaciones de trabajo marca Apple. Se ha buscado es centralizar y gestionar los parches necesarios para mantener los equipos actualizados y evitar amenazas en nuestra red.
6. Podemos indicar que se cumplieron con los objetivos planteados en el presente trabajo de titulación, ya que se logró de forma eficiente cumplir con la implementación de la solución propuesta.

Recomendaciones:

1. Luego de los resultados obtenidos en el presente trabajo, se recomienda a la institución financiera utilizar esta implementación para realizar la gestión, seguridad, control e integración de equipos Apple. Para esto, es necesario que la alta directiva de TI lidere este proyecto y siga realizando mejoras con el fin de tener una infraestructura controlada de todos los equipos Apple (iMac, MacBook Pro) según el crecimiento que se vaya realizando en esta tecnología obteniendo sus beneficios.
2. Se recomienda, además, que se realice un respectivo mantenimiento en los equipos Apple (iMac, MacBook Pro), velando que se ingresen y eliminen estas estaciones de trabajo de Apple de acuerdo a los cambios de los equipos en AD para así mantener un inventario de equipos actualizados y tener en consola solo los equipos que se encuentran en producción.
3. Podemos indicar que se recomienda mantener un enlace de contingencia en dicha institución para el caso de saturación o caída del enlace y así mantener el servicio estable en el despliegue de los parches de actualizaciones y evitar retrasos en el despliegue o riesgos en estos equipos.
4. Otra recomendación es que dicha institución pueda contratar un servicio de Help Check por una empresa externa para asegurarse que la infraestructura que se encuentra implementada cumpla con todas las normas y requisitos propuestos y recomendados.
5. Finalmente, aun cuando no se encuentra dentro del alcance del este proyecto, se recomienda tener un equipo backup (Servidor) como parte de la infraestructura del

servicio para proceder a aplicar el procedimiento de contingencia en caso de algún problema en el servidor.

BIBLIOGRAFÍA

- [1] CIS Center for Internet Security, 2010

- [2] Juran, J.M., "Pareto. Lorenz, Cournot Bernoulli, Juran and Others," Industrial Quality Control, October 1950, p. 25. Pareto n.d.

- [3] Baguer A. El Nuevo Modelo De Organización Empresarial: La persona, principal activo de una organización por procesos. Madrid: Editorial Capital Humano; 2001.

- [4] CIS Controls, Version 7, March 18, 2018. CIS Controls n.d.
<https://www.cisecurity.org/controls/> (accessed September 23, 2018).

- [5] System Center Configuration Manager Documentation | Microsoft Docs n.d.
<https://docs.microsoft.com/en-us/sccm/> (accessed September 23, 2018).

- [6] Lammle T. CCNA Cisco Certified Network Associate Deluxe Study Guide. John Wiley & Sons; 2011.

- [7] GlobalSTD. ISO Survey 2016 - GlobalSTD n.d.
<https://www.globalstd.com/component/k2/iso-survey-2016> (accessed September 30, 2018).

- [8] Actualizaciones de seguridad de Apple. Apple Support n.d.
<https://support.apple.com/es-es/HT201222> (accessed September 29, 2018).

- [9] COMISIÓN NACIONAL DEL MERCADO DE VALORES n.d.
<https://www.sec.gov/Archives/edgar/data/320193/000119312514383437/d783162>

- [10] Educación - Apple Distinguished Schools. Apple (España) n.d.
<https://www.apple.com/es/education/apple-distinguished-schools/> (accessed October 1, 2018).
- [11] Disterer G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security* 2013;04:92–100.
doi:10.4236/jis.2013.42011.
- [12] Rodríguez T, Jonathan P. Diseño de una red privada virtual para la optimización de las comunicaciones en la empresa comunicaciones e informática SAC caso: redes de datos 2017.
- [13] Newell MW. Preparing for the project management professional (PMP) certification exam. Amacom Books; 2005.

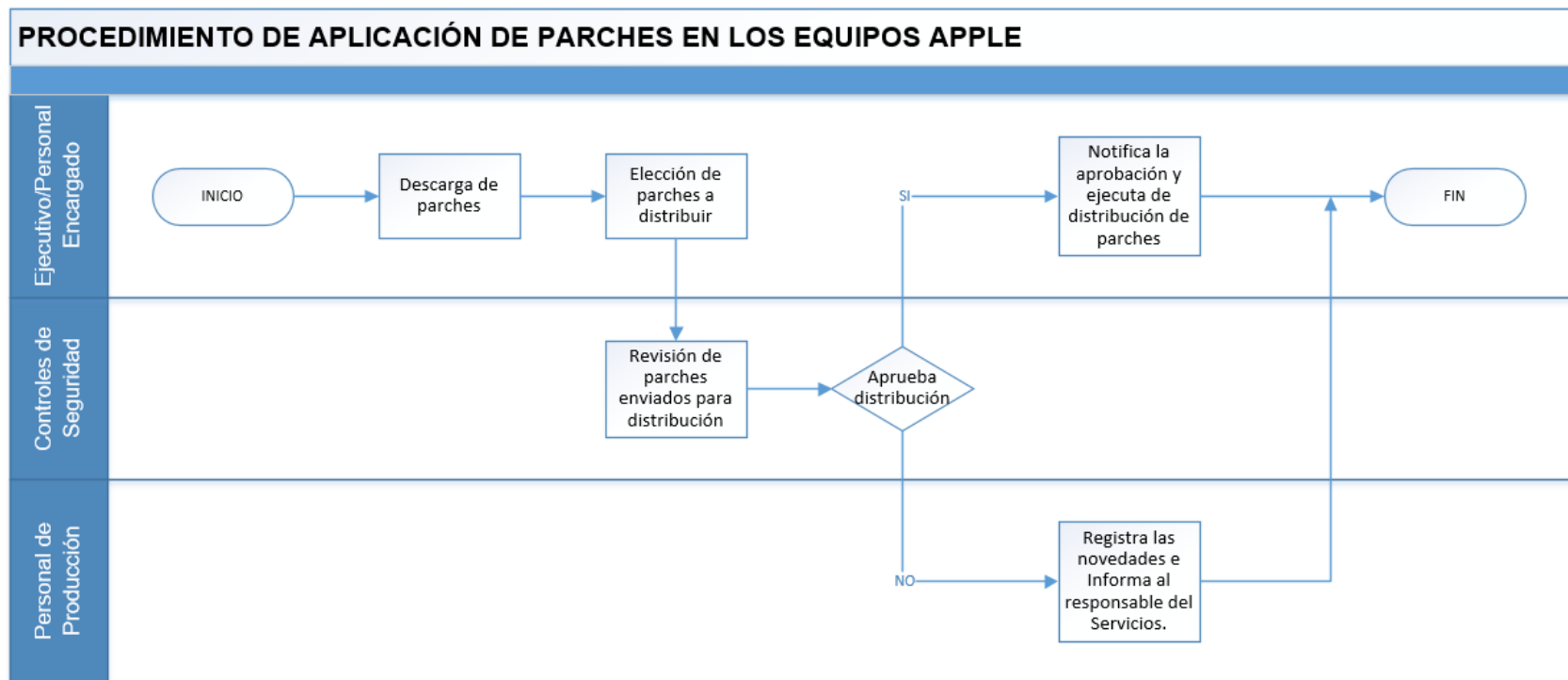
ANEXOS

MATRIZ DE ACTUALIZACIÓN DE SOFTWARE

MATRIZ DE ACTUALIZACIÓN DE SOFTWARE	
Área:	Software a actualizar:
Autorizado por:	
Justificación:	
Novedades presentadas:	
Responsables:	
Equipos afectados:	
Control de Cambios	
Fecha de actualización	
Ejecutado por	
Comentarios	
<hr style="width: 30%; margin: 0 auto;"/> Firma C.I:	

CRONOGRAMA COMPLETO DEL PROYECTO

🚀	Inicio y gestión del proyecto	42 días	lun 11/06/18	mar 07/08/18		
🚀	Inicio del proyecto	10 días	lun 11/06/18	vie 22/06/18		
🚀	Alcance del proyecto	4 días	lun 11/06/18	jue 14/06/18		
🚀	Planificación del proyecto	4 días	vie 15/06/18	mié 20/06/18	3	
🚀	Revisión de Presupuesto del proyecto	2 días	jue 21/06/18	vie 22/06/18	4	
🚀	Diseño y análisis	5 días	lun 25/06/18	vie 29/06/18		
🚀	Análisis de situación actual	3 días	lun 25/06/18	mié 27/06/18	5	
🚀	Diseño de implementación	2 días	jue 28/06/18	vie 29/06/18	7	
🚀	Construcción	15 días	lun 02/07/18	vie 20/07/18		
🚀	Implementación de la herramienta	15 días	lun 02/07/18	vie 20/07/18	8	
🚀	Pruebas	3 días	lun 23/07/18	mié 25/07/18		
🚀	Pruebas de funcionamiento de herramienta	3 días	lun 23/07/18	mié 25/07/18	10	
🚀	Despliegue	3 días	jue 26/07/18	lun 30/07/18		
🚀	Despliegue	3 días	jue 26/07/18	lun 30/07/18	12	
🚀	Cierre del Proyecto	5 días	mié 01/08/18	mar 07/08/18		
🚀	Entrega y finalización de herramienta para la operación	5 días	mié 01/08/18	mar 07/08/18	14	

PROCEDIMIENTO DE APLICACIÓN DE PARCHES EN LOS EQUIPOS APPLE

PLANTILLA ACTA DE CONSTITUCIÓN DEL PROYECTO

ACTA DE CONSTITUCIÓN DEL PROYECTO		
Fecha	Revisión	Nombre del Proyecto
Fecha de inicio del proyecto		Fecha tentativa de finalización del proyecto
Definición del Alcance del proyecto		
Deberá delimitarse cuál es el alcance que tendrá el proyecto		
Justificación o propósito del proyecto (Aporte y resultados específicos)		
Descripción del servicio que generará el proyecto-Entregables finales del proyecto		
Descripción específica y medible de los productos que el proyecto debe entregar		
Supuestos		
Factores que consideramos como ciertos para efectos de planeación y que tendrán que confirmarse a medida que avance el proyecto.		
Restricciones		

Factores que limitan al equipo ejecutor	
Patrocinador y Administrador del proyecto (firmas de aceptación)	
Patrocinador	Administrador del Proyecto

CICLO PHVA

Ciclo PHVA	PROCESOS
Planear (Plan)	<p>Establecer el contexto. Alcance y Limites Definir Política del SGSI Definir Enfoque de Evaluación de Riesgos Identificación de riesgos Análisis y Evaluación de riesgos Evaluar alternativas para el Plan de tratamiento de riesgos Aceptación de riesgos Declaración de Aplicabilidad</p>
Hacer (Do)	<p>Implementar plan de tratamiento de riesgos Implementar los controles seleccionados Definir las métricas Implementar programas de formación y sensibilización Gestionar la operación del SGSI Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad</p>
Verificar (Check)	<p>Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI</p>
Actual (Act)	<p>Implementar las mejoras identificadas para el SGSI Implementar las acciones correctivas y preventivas pertinentes. Comunicar acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.</p>

MATRIZ COBIT

COBIT en su versión 4.1, al ser un marco de Gobierno de las Tecnologías de la Información basado en procesos permite:

- Crear valor dentro de la organización
- Garantizar la optimización los riesgos
- Asegurar la entrega de beneficios
- Optimizar los recursos
- Garantizar la transparencia de recursos
- Cumplimiento de normas
- Reglamentos y políticas.

Considerando que la madurez del gobierno de la Tecnología de Información mejora si aumenta o se intensifica la participación de todos los grupos implicados. Para el desarrollo del proceso DS5. Garantizar la Seguridad de los Sistemas, se debe realizar las métricas detalladas en la siguiente tabla:

Desde	Entradas
PO2	Arquitectura de Información; clasificación de datos asignados
PO3	Estándares de tecnología
PO9	Evaluación de riesgo
AI2	Especificaciones de controles de seguridad en las aplicaciones
DS1	OLAs

Salidas	Hacia
Definición de incidentes de seguridad	DS8
Requerimientos específicos de entrenamiento sobre conciencia de seguridad	DS7
Reportes de desempeño del proceso	ME1
Cambios de seguridad requeridos	AI6
Amenazas y vulnerabilidades de seguridad	P09

MATRIZ RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir y mantener un plan de seguridad de TI	I	C	C	A	C	C	C	C	I	I	R
Definir, establecer y operar un proceso de administración de identidad (cuentas)			I	A	C	R	R	I			C
Monitorear incidentes de seguridad, reales y potenciales				A	I	R	C	C			R
Revisar y validar periódicamente los privilegios y derechos de acceso de los usuarios				I	A	C					R
Establecer y mantener procedimientos para mantener y salvaguardar las llaves criptográficas				A		R			I		C
Implementar y mantener controles técnicos y de procedimientos para proteger el flujo de información a través de la red				A	C	C	R	R			C
Realizar evaluaciones de vulnerabilidad de manera regular		I		A	I	C	C	C			R

Una matriz RACI identifica quien es Responsable, quien debe rendir cuentas (A), quien debe ser Consultado y/o Informado

Meta	Proceso	Actividades
Proteger y mantener registro de los activos de T.I.	Identificar, monitorear y reportar vulnerabilidades	Pruebas de seguridad regulares
Cantidad de incidentes con impacto al negocio	Cantidad y tipo de acceso reales y de sospechadas.	Cantidad y tipo de cuentas obsoletas