Análisis de vulnerabilidades en la Empresa TELEPERFORMANCE mediante la herramienta RETINA (Network Security Scanner) para la evaluación de la seguridad en la red

Martin David Naranjo Correa

Luis Manuel Contrera Muñoz

FACULTAD DE INGENIERÍAS

Ingeniería de Sistemas

Director

MSc. Héctor Fernando Vargas Montoya

INSTITUTO TECNOLÓGICO METROPOLITANO

2018

RESUMEN

El presente informe final tiene como objetivo principal proponer el uso de la herramienta de software o aplicación especializada RETINA, (herramienta comercial para la evaluación de vulnerabilidades en la red) en un ambiente productivo real, éste software hace posible la recolección de información sobre brechas de seguridad de la infraestructura de red, servicios y sistemas informáticos, mediante una evaluación de vulnerabilidades internas, lo que permitirá identificar algunos de los problemas de exposición en materia de seguridad informática. Con los resultados obtenidos de los análisis de vulnerabilidades, se puede priorizar las medidas de mitigación de dichas brechas de seguridad a nivel de la intranet y sus diferentes servicios informáticos, dicha implementación y análisis se realizó en la empresa TELEPERFORMANCE S.A.S. (dada las necesidades de la misma empresa), lo que permitió dar cumplimiento a los objetivos propuestos, esto es, se configuró un servidor, se adecuó la herramienta RETINA y se ejecutó el análisis de vulnerabilidades, y a partir de los hallazgos arrojados por la herramienta, se analizaron y entregaron las recomendaciones para la remediación acorde al nivel de criticidad encontrado.

En éste mismo sentido, se dejó por escrito a la empresa todos los manuales y el proceso completo de manejo de vulnerabilidades, teniendo como fin completar el ciclo de cierre de las vulnerabilidades encontradas y sus respectivas remediaciones.

Palabras clave: RETINA, controles, riesgos, remediaciones, vulnerabilidades, infraestructura de red.

RECONOCIMIENTOS

La realización de este proyecto fue posible gracias a la colaboración y confianza brindada por la empresa TELEPERFORMANCE S.A.S., y a nombre personal de **Ana Lucia Gómez Osorio** (IT Security Manager), quien nos ayudó con la autorización e información requerida para que este proyecto se implementará de la mejor forma.

También, se reconoce la labor acertada y certera del asesor Prof. **Héctor Fernando Vargas Montoya** del ITM (Instituto Tecnológico Metropolitano).

ACRÓNIMOS

En esta sección se listan los acrónimos, siglas, símbolos y abreviaturas propias de la temática tratada en el desarrollo del trabajo de grado:

CVS Grupo de investigación en integración de soluciones con tecnología de información y comunicación.

CVE Common Vulnerabilities and Exposures, Vulnerabilidades y exposiciones comunes.

TI Tecnologías de la Información.

CVSS Common Vulnerability Scoring System SIG CVSS, El Sistema común de puntuación de vulnerabilidad.

CMDB Configuration Management Database.

ITIL Information Technology Infrastructure Library.

CDE Cardholder Data Environment.

CHDM Cardholder Data Matrix.

PCI Payment Card Industry

Tabla de Contenido

Tabla de Figuras

1.INTRODUCCIÓN

Las tecnologías digitales se han tomado el mundo de los negocios, impactando todo tipo de industria, compañía o empresa; las políticas de seguridad de la información de cualquier compañía, permiten brindar confianza a los clientes y establecer prioridades sobre las normas de seguridad para los datos (en tránsito o almacenados) y activos sensibles de la empresa.

Sin embargo, para una correcta gestión de seguridad fue necesario trabajar en varios frentes que nos permitieron lograr una visión de las problemáticas existentes, en ese sentido se realizó un análisis completo del estado de vulnerabilidades a nivel de seguridad informática, así mismo, se orientó a la posible implementación de acciones de mejora continua para la empresa TELEPERFORMANCE S.A.S. En éste sentido, para dar cumplimiento con ésta actividad y subsanar la necesidad que dicha empresa posee, se definieron como objetivo principal un "*Análisis de vulnerabilidades en la Empresa TELEPERFORMANCE mediante la herramienta RETINA (Network Security Scanner) para la evaluación de la seguridad en la red*", de igual forma, con los resultados arrojados se planeó un grupo de acciones para remediaciones de brechas de seguridad, los cuales eventualmente están a cargo del equipo IT de la empresa TELEPERFORMANCE S.A.S, dicha área ejecuta diferentes acciones para cerrar vulnerabilidades que atenten contra la integridad, disponibilidad o confidencialidad de la información.

Es de anotar que, la implementación se realizó en un ambiente productivo real, para la empresa TELEPERFORMANCE S.A.S, en las sedes principales de las ciudades de Bogotá y Medellín. Para tal fin, se contó con la carta de aprobación del IT Security Manager (se adjunta para su verificación) y se ejecutó bajo los procedimientos de control de cambios estipulados por la empresa, así mismo, alguna información interna considerada

confidencial no estará en éste documento, sin que esto haya afectado el logro de los objetivos.

A continuación, se detallan los objetivos específicos plateados y logrados para alcanzar los resultados deseados:

1. Identificar el alcance de la red y los servicios informáticos para evaluación de vulnerabilidades.
2. Diseñar el servidor donde estará instalada la suite de RETINA.
3. Establecer la configuración especifica de RETINA acorde al alcance de la red y servicios para la ejecución del análisis.
4. Sintetizar el informe de las vulnerabilidades, amenazas y riesgos existentes con el respectivo plan de remediación.

Éste informe final se ha dividido en varias sesiones, partiendo de un resumen general y la introducción, un marco teórico, el desarrollo de la metodología planteada y los resultados obtenidos (con su respectivo análisis), finalmente se entregan las conclusiones, recomendaciones y trabajo futuro, así como la sesión de anexos.

2.MARCO TEÓRICO

A continuación, se referencia a los diferentes conceptos y términos que se requieren para comprender el desarrollo de los objetivos y la metodología, que se utilizaron para la implementación y documentación del programa de escaneo de vulnerabilidades en la Red usando la herramienta RETINA Network Security Scanner (evaluación de vulnerabilidades en la red); En la empresa TELEPERFORMANCE SAS:

La necesidad inicial parte de la empresa TELEPERFORMANCE S.A.S desde su área de Seguridad Informática, ésta necesidad radicaba en tener un procedimiento para la gestión de vulnerabilidades en seguridad, por lo cual han adquirido una nueva herramienta de escaneo de vulnerabilidades. Se necesitaba una solución capaz de soportar un escaneo simultáneo de varias IP, además de generar informes rápidos, confiables y amigables para el usuario final o analista encargado; la implementación de dicha herramienta favorece los intereses de la compañía y la funcionalidad requerida, dado el alto número de componentes de la infraestructura tecnológica dentro de la compañía (Servidores de varios tipos, switches, etc.).

(Beyondtrust.com, 2017), RETINA NETWORK SECURITY SCANNER, del proveedor **Beyondtrust**, "*Disponible como una aplicación independiente o como parte de la solución de gestión de vulnerabilidades empresariales de Retina CS, Retina Network Security Scanner le permite identificar de manera eficiente las exposiciones de TI y priorizar la corrección en toda la empresa*"; lo que supone que es una herramienta completa para la identificación y gestión de vulnerabilidades, en dónde los resultados deben ser analizados acorde a los procesos internos, dando un nivel de criticidad y planteando las acciones de mejora, esto ayudará al fortalecimiento de los procesos y procedimientos de seguridad en cuanto a la identificación y remediación de vulnerabilidades.

(FIRST — Forum of Incident Response and Security Teams, 2017), Common Vulnerability Scoring System SIG CVSS, es el Sistema común de puntuación de vulnerabilidad, proporciona una forma de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad. El puntaje numérico puede traducirse en una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidad. Actualmente la escala de calificación se encuentra en su versión 3, en el capítulo de la metodología se detalla sobre el ranking que se usó para este proyecto.

Vulnerabilidad Informática, (Descargas.pntic.mec.es, 2017), debilidad de cualquier tipo que compromete la seguridad del sistema informático, se puede presentar a nivel de software o hardware para cualquier componente que conforman el sistema informático (Servidores, routers, switches, ect), una vulnerabilidad es un hueco o fallo de seguridad que permite a un posible atacante explotar riesgos no previstos, generando impactos negativos en el sistema.

Para la gestión interna de los procedimientos de control de cambios, la empresa TELEPERFORMANCE S.A.S cuenta con la herramienta **CA Service Desk Manager** la cual es un software de la empresa CA Technologies y se utiliza para la gestión y administración los procesos y procedimientos de TI (Tecnología de la información) basado en ITIL de cualquier empresa que tenga implementado sistemas informáticos. Dentro de esta herramienta se pueden crear tipos de tareas como es la OC (Order Change) u orden de cambio, la cual se crea para realizar un trabajo programado el cual puede tener afectación en los ambientes de Pre-Producción y Producción y contiene un flujo de aprobación. Para el caso de escaneo de vulnerabilidades se creó una orden de cambio - OC, la cual fue aprobada por el comité de cambios de la empresa para su correcta ejecución y cumplimiento de los procesos internos.

TELEPERFORMANCE S.A.S (Colombia), es el resultado de la adquisición por parte de Teleperformance SA de Teledatos, una compañía colombiana con 15 años de experiencia que está posicionada como el número 1 en prestación de servicios de contact center y BPO (business process outsourcing) en el mercado colombiano.

Servidor, (Aprenderaprogramar.com, 2017) Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que les suministran a estos, todo tipo de información. Con el fin de realizar este trabajo se eligieron para el escaneo los siguientes tipos de servidores que se manejan en la compañía (No se hace referencia al sistema operativo, porque todos son del proveedor Microsoft Windows):

- **Servidor Controlador de Dominio:** (Es.wikipedia.org, 2017), Los controladores de dominio tienen una serie de responsabilidades, y una de ellas es la autenticación: es el proceso de garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red.
- **Servidor de Antivirus:** Este tipo de servidores son primordiales en toda compañía, su función original es administrar los antivirus y realizar escaneos a tráfico de archivos que puedan causar un impacto negativo en la red corporativa.
- **Servidor de Correo:** (Culturación, 2017) Un servidor de correo es una aplicación informática que tiene como objetivo, enviar, recibir y gestionar mensajes a través de las redes de transmisión de datos existentes, con el fin de que los usuarios puedan mantenerse comunicados con una velocidad muy superior a la que ofrecen otros medios de envío de documentos.
- **Servidor Card Holder:** (PCI Hispano, 2017) Es un servidor de uso exclusivo para guardar la información y gestionar las transacciones con tarjetas de pago (CDE: Cardholder Data Environment). Para TELEPERFORMANCE S.A.S. estos servidores son los de más alta criticidad por el nivel de información del negocio.

- **Servidor CallCopy:** Estos servidores se usan para la grabación las llamadas telefónicas, como característica principal tienen un alto tráfico.

Escaneo de vulnerabilidades, es un procedimiento que se realiza para la identificación, análisis y reporte de vulnerabilidades técnicas de seguridad que terceros y personas no autorizadas pueden utilizar para explotar y amenazar la confidencialidad, integridad y disponibilidad de la información técnica y del negocio.

Ping (Es.wikipedia.org, 2017) es una utilidad que hace parte del protocolo ICMP (Internet Control Message Protocol por sus siglas en inglés) y se usa como prueba de comunicación entre dos computadoras, desde el servidor local se envía un paquete de solicitud y desde el servidor remoto se contesta con paquetes de respuesta.

Dirección IP (Es.wikipedia.org, 2017) es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, Smartphone) que utilice el protocolo IP (Internet Protocol).

Remediación (Repository.libertadores.edu.co, 2017) proceso de ejecución que consiste en actualizar, desinstalar o configurar el software para corregir vulnerabilidades informáticas.

Programa de Gestión de vulnerabilidades procedimiento en el cual se busca, analiza y se aplica acciones correctivas a una vulnerabilidad encontrada. Este proceso comprende el ciclo completo de gestión de vulnerabilidades: identificación, ejecución de la prueba, plan de remediación, ejecución del plan y re-test nuevamente para la validación del cierre de la vulnerabilidad.

3.METODOLOGÍA

La compañía **TELEPERFORMANCE S.A.S.** desde su área de Seguridad Informática, planeó realizar la implementación de la Herramienta **RETINA** (Network Vulnerability Assessment - Evaluación de Vulnerabilidad de Red) para la gestión de las vulnerabilidades en la seguridad informática, para lo cual, el proyecto implementó y ejecuto un análisis de vulnerabilidades, a continuación, se muestra en la figura 1 en forma de diagrama, el flujo para la gestión de vulnerabilidades.

Diagrama de flujo para la gestión de vulnerabilidades

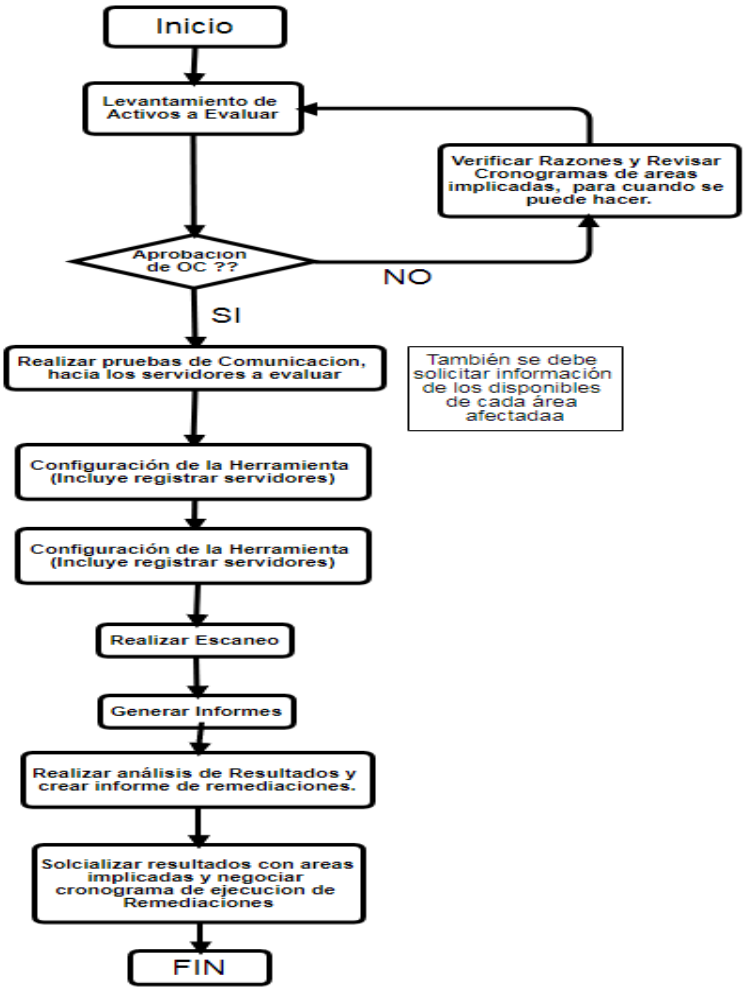


Figura 1. Flujo para la gestión de vulnerabilidades. Fuente: Los autores.

Una vez se socializan los resultados, se debe iniciar por parte de las áreas responsables, la ejecución del plan de remediación de éstas, cuando la ejecución técnica de la remediación se ejecute, se haría nuevamente un análisis de vulnerabilidades para la verificación de cierre. Luego de conocer el ciclo de vida de las vulnerabilidades, se indica a continuación la implementación y ejecución del proyecto realizada por fases:

FASE 1

En Cumplimiento al flujo para la gestión de las vulnerabilidades, se eligieron los servidores críticos que fueron evaluados (23 en total), la Tabla 1 indica la información de los mismos.

Tabla 1 *Listado de servidores a evaluar*

Nombre	Rol
TPCV359-114	Antivirus
TPCV356-114	Antivirus
TPCV453-41	Controlador de Dominio
TPCF453-100	Controlador de Dominio
TPCF453-116	Controlador de Dominio
TPCV359-54	Controlador de Dominio
TPCF359-249	Controlador de Dominio
TPCV356-52	Controlador de Dominio
TPCF356-53	Controlador de Dominio
TPCF715-50	Controlador de Dominio
TPCV359-150	Correo
TPCV359-151	Correo
ZF-APP1	Card Holder
ZF-KEY1	Card Holder
ZF-APP2	Card Holder
tpcf359-184	CallCopy
tpcf359-185	CallCopy
tpcf360-186	CallCopy
tpcf360-187	CallCopy
tpcf360-189	CallCopy
tpcf360-190	CallCopy
tpcv359-178	CallCopy
tpcv359-168	CallCopy

NOTA. La información de los servidores de ambiente productivo de la compañía es confidencial, se ilustra la tabla anterior con fines académicos.

Como se ilustra en la tabla anterior, son diferentes servidores y servicios que deben ser evaluados, lo que se logró es una buena muestra representativa de la red interna.

FASE 2

Se hace uso de la herramienta RETINA Network Security Scanner que se eligió con un estudio previo donde se tuvieron en cuenta además las siguientes herramientas: **GFI Languard y Alient Vault.** Los factores que inclinaron a elegir RETINA fueron: precio, numero de IP soportadas, versatilidad en los informes, soporte de primera línea para posibles inconvenientes con la herramienta y el buen nombre que tiene la herramienta, lo

anterior, dado que la herramienta hasta entonces utilizada (Qualys) no brindaba las suficientes alternativas y funcionalidades requeridas.

En la tabla 1 se ilustra las características comparativas de las herramientas para la ejecución de los análisis, como se puede apreciar, la herramienta RETINA tienen mejores características:

Tabla 2 *Información de las herramientas*

PROVEEDOR	HERRAMIENTA	DEMO GRATUITO	PRECIO ANUAL (Dólares)	CAPACIDAD DE IP´S
GFI Software	GFI LanGuard	30 días	40.000 USD	8.000
Alien Vault	Unified Security Management™ (USM™)	14 días	19.600 USD	Ilimitada
Beyonf Trust	Retina Network Security Scanner	Dependiendo de necesidad (Mayor a 30 días incluso)	2.034 USD	Ilimitada

Teniendo en cuenta la herramienta seleccionada, el paso siguiente, fue realizar la instalación de la suite RETINA Network Security Scanner; esta instalación tiene unos requisitos mínimos de instalación (Para Teleperformance Colombia) que se deben tener en cuenta y se muestran en la figura 2.

Operating Systems	Windows 7 Professional SP1 (64-bit)
Software	MSXML 6.0 SP1 (revisar) Microsoft .Net Framework 4.5.2
Network	*- TCP/IP – Required for communicating with the* BeyondInsight console, license validation, and scanning remote machines ***(Not Apply for Colombia)*** *- Ports 443 and 21690 are required for integration with BeyondInsight* ***(Not Apply for Colombia)*** - Network Interface Card (NIC) with TCP/IP enabled
Processor	Intel Core 7 2.50 Ghz (compatible)
Memory (RAM)	8 GB
Hard Drive	452 GB
Minimum Screen Resolution	1024x768

Figura 2. Requisitos mínimos de instalación de RETINA Network Security Scanner, Tomada de manual de instalación oficial anexo en el proyecto

Luego se continuó con la instalación de la aplicación; en el anexo 1 (*TP Colombia_Retina Installation Guide_V3*) se indican los pasos para la instalación correcta de la aplicación RETINA (en idioma inglés, tomados de la guía de instalación del producto (E-spincorp.com, 2017)).

La arquitectura de la solución se muestra en la figura 3:

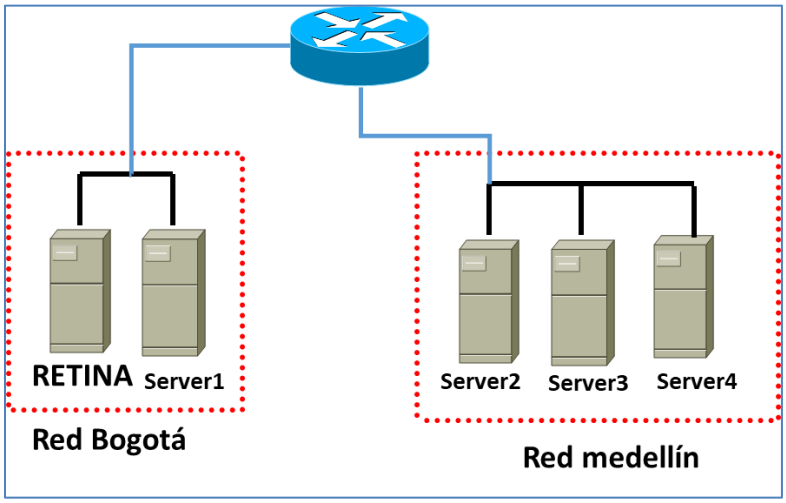


Figura 1. Arquitectura de red para RETINA. Fuente, los autores

Desde el servidor central en dónde está RETINA, una vez se tiene alcanzabilidad técnica a los servidores objetivos, se ejecuta los diferentes análisis de vulnerabilidades, dado que desde un punto central se debe ejecutar el análisis, es necesario que exista la conectividad entre RETINA y los servidores.

FASE 3

Después de implementar la instalación de manera exitosa, la aplicación cada vez que se ejecute, realizará una actualización automática, que mantendrá a RETINA con la última versión del sistema de calificación o puntaje de vulnerabilidades (CVSS Common Vulnerability Scoring System SIG CVSS, (el Sistema común de puntuación de vulnerabilidad). Este sistema se usa para determinar el impacto que representa una vulnerabilidad y se utiliza una escala que va del 0 al 10, en la actualidad se usa la versión 3, como se muestra en figura 4.

Clasificacion	CVSS Puntaje
Ninguna	0.0
Bajo	0.1 - 3.9
Medio	4.0 - 6.9
Alto	7.0 - 8.9
Crítico	9.0 - 10.0

Figura 2. Escala de calificación de gravedad cualitativa

NOTA. Figura tomada de https://www.first.org/cvss/specification-document.

Así mismo, dentro del sistema de puntuación de la CVSS, se tiene en cuenta si existe o no una remediación, y además si existe una solución que indica si es temporal, definitiva o si aún no existe una solución conocida.

(FIRST — Forum of Incident Response and Security Teams, 2017), las soluciones provisionales o las revisiones pueden ofrecer soluciones intermedias hasta que se emita un parche o actualización oficial. Cada una de estas etapas respectivas ajusta la puntuación temporal hacia abajo, lo que refleja la urgencia decreciente a medida que la corrección se vuelve definitiva. La lista de posibles valores se presenta en la Tabla 2. Cuanto menos oficial y permanente sea una solución, mayor será el puntaje de vulnerabilidad.

Tabla 3 Nivel de Remediación

Valor métrico	Descripción
No definido (X)	> La asignación de este valor a la métrica no influirá en la puntuación. Es una señal a una ecuación de puntuación para saltear esta métrica.
No disponible (U)	No hay ninguna solución disponible o es imposible de aplicar.
Solución alternativa (W)	Existe una solución no oficial, no de proveedores disponible. En algunos casos, los usuarios de la tecnología afectada crearán un parche propio o darán los pasos para evitar o mitigar la vulnerabilidad.
Arreglo temporal (T)	Hay una solución oficial pero temporal disponible. Esto incluye instancias donde el vendedor emite una revisión, herramienta o solución temporal.
Solución oficial (O)	Una solución de proveedor completa está disponible. O bien el proveedor ha emitido un parche oficial, o hay una actualización disponible.

NOTA. Figura tomada de https://www.first.org/cvss/specification-document.

Luego del análisis de los requisitos e instalación de la aplicación, se continuó con la validación de los permisos de comunicación entre el computador donde se instaló la herramienta y los servidores que se van a evaluar (es fundamental antes de iniciar el análisis, verificar que exista comunicación entre RETINA y el sistema informático a evaluar). Este es un control previo que se debe realizar con anticipación a la realización del escaneo de vulnerabilidades, a pesar de que el computador está dentro de la red de la compañía siempre se debe realizar esta verificación; ésta prueba de comunicación se realiza a través de un ping desde el servidor donde se instaló RETINA Network Security Scanner hacia el servidor a evaluar, este comando se realiza desde la consola de comando de Windows (ejemplo: ping NOMBRE O IP SERVIDOR) como se muestra en la figura 4.

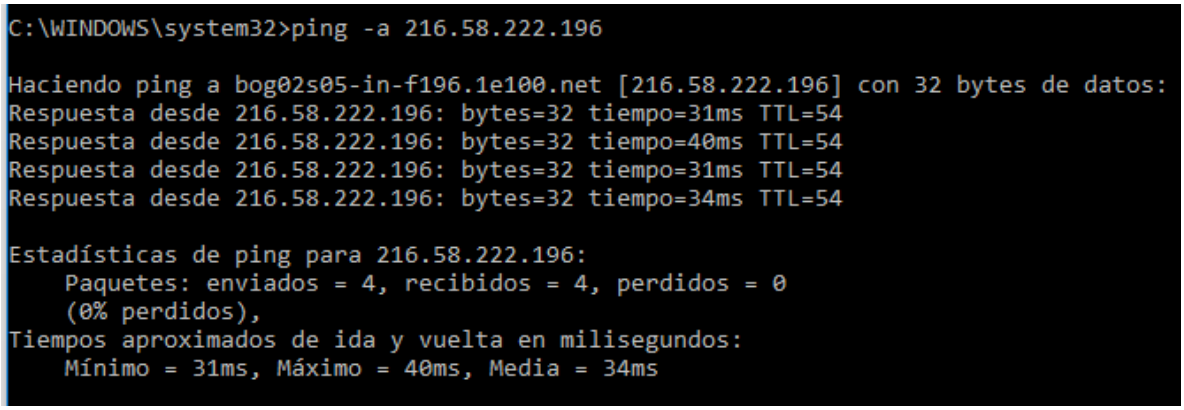


Figura 3. Comando ping que se usa como prueba de comunicación entre dos host.

En el orden de las ideas, se hace una recolección de la información de los servidores a escanear. También se realizó la instalación de la aplicación y se ejecutaron pruebas básicas de comunicación que son necesarias antes de realizar el escaneo; paso siguiente y previo al inicio del escaneo de vulnerabilidades, se creó una **OC** (Change Order, es un flujo de trabajo para la ejecución de varias tareas que involucran varias personas o responsables) orden de cambio en la herramienta **CA Service Desk Manager**, dentro de los procedimientos internos de la compañía, se debe tener un registro de todas las actividades a ejecutar sobre las redes y sistemas, la OC en particular creada, se describe y

solicita la ejecución de un escaneo de vulnerabilidades que se va a realizar; para lo cual, se deben registrar todos los servidores que estén en la lista de escaneo y también se debe registrar el tiempo de duración de la ventana (en caso de que aplique) y tener a la mano los números telefónicos de los líderes y personas encargadas de las áreas de Red, servidores, aplicaciones y cualquier otra área que pueda tener afectación, del mismo modo, una vez creada la OC, ésta se socializa con las personas involucradas y partícipes del comité de cambios. En el **Anexo 2** se precisa los pasos para la creación de la OC. La herramienta RETINA fue implementada configurando los perfiles necesarios para realizar la prueba de seguridad, dentro de lo configurado se encuentra:

1 - Instalación de la licencia otorgada por el proveedor Beyond Trust, en un servidor dedicado al área de seguridad de la información: allí, solo se puede acceder con las credenciales del usuario autorizado a nivel de AD (Directorio Activo) y desde red interna, es decir, desde red de Teleperformance. Así, no será posible entonces acceder a la herramienta desde una red externa, evitando ingresos no autorizados.

2 - Por ser cliente instalado dentro del servidor, no se requiere un usuario de RETINA exclusivo para autenticación de ingreso a la herramienta. La aplicación funciona con recurso instalado sin inconveniente alguno.

3 - Para los tipos de escaneo e informes requeridos, se realizó la selección del PCI Compliance, que es un equivalente al reporte prioritario de acuerdo a las necesidades del negocio y a los lineamientos corporativos de TP, al ser este tipo de clientes su mayor fuente de ingreso económico. La configuración PCI compliance, permite realizar un análisis técnico considerando el cumplimiento mismo de la norma, como vulnerabilidades de tipo inyección, control de acceso, problemas de contraseñas, falencia en parches, controles criptográficos, entre otros.

4- Se realizó la configuración, de cada grupo de dispositivos-servidores críticos (Domain Controller, Antivirus, CHE, Call Copy) con todas las las IP´s recolectadas e identificadas dentro del alcance de dichos dispositivos, para mayor facilidad al momento de ejecutar un escaneo, dando independencia a cada uno de estos grupos y brindando facilidad y consistencia en el tipo de reporte requerido por servidor.

Ejecución del análisis

En este punto de la metodología, una vez configurado el tipo de análisis a realizar, se da inicio a la ejecución del análisis de vulnerabilidades acorde a la orden de cambio ya aprobada, se finaliza con la entrega de informes de los escaneos, para lo cual, se debe tener en cuenta la lista de servidores mostrada en la figura 1. La configuración se muestra el escaneo con la suite de RETINA para una sola dirección ip – servidor (figura 6):

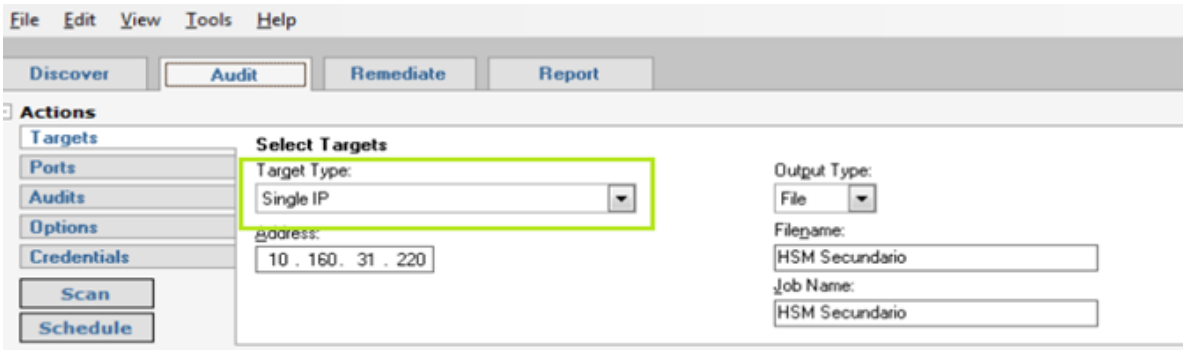


Figura 4. Escaneo en RETINA para una sola IP, fuente: Herramienta RETINA implementada

En la siguiente ilustración (figura 7), se muestra la configuración de un escaneo para varias direcciones ip – servidor:

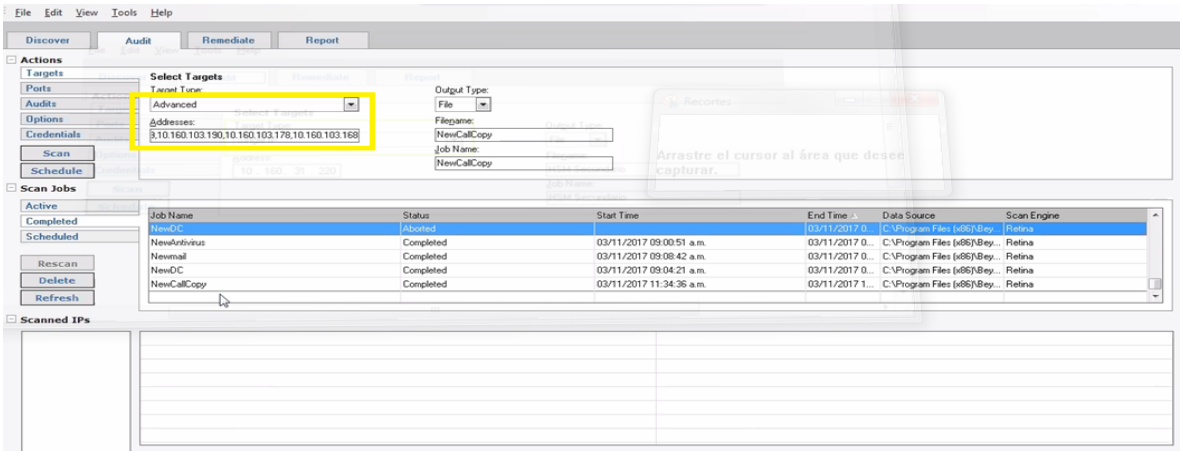


Figura 5. Escaneo en RETINA para varias IPs

En la figura 8, se muestra el escaneo en estado **Running** (Ejecutando)

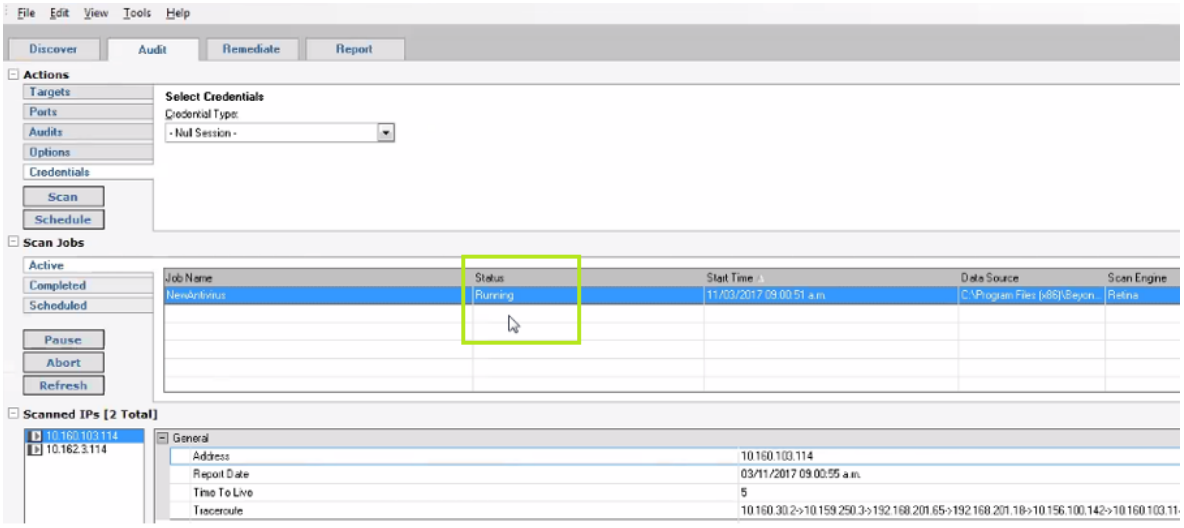


Figura 6. Escaneo en RETINA en estado Running.

Luego de finalizar los escaneos, para todos los tipos de servidores se realiza el exporte de los resultados, en la imágenes 9 y 10. Importante aclarar que se exporta bajo el formato de PCI Compliance (Payment Card Industry), siendo esta la certificación de mayor peso y reconocimiento a nivel global para el estándar de cumplimiento en seguridad transaccional con información de tarjeta de crédito; uno de los pilares en Teleperformance Colombia en compromiso con sus clientes.

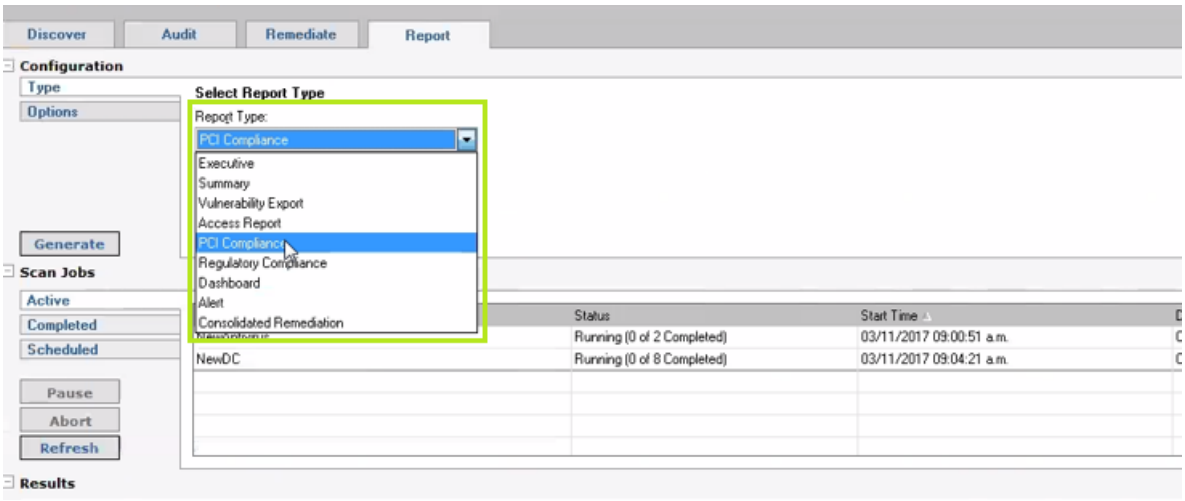


Figura 7. Generación de Informes.

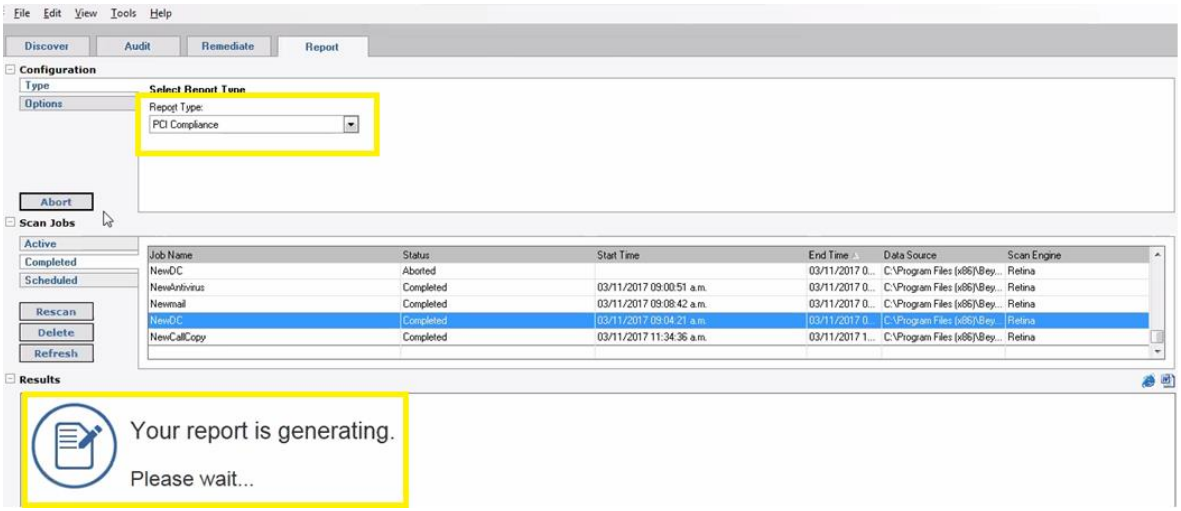


Figura 8. Generación de informes parte 2.

4.RESULTADOS Y DISCUSIÓN

4.1. Resumen general de hallazgos

A continuación, se listan los resultados (en barras) de los escaneos realizados sobre los servidores críticos anteriormente visualizados en la **Tabla 1**, para lo cual, el análisis de vulnerabilidades fue exitoso, obteniendo información relevante e importante de seguridad que es necesario analizar acorde a los procesos de la compañía.

Lo que se busca, es dar de una manera clara, concisa y precisa, los tipos de vulnerabilidades existentes dentro de la red interna de la compañía, con una breve descripción de cada una de ellas y a su vez, la instrucción que debe ser tenida en cuenta para eliminar o subsanar la brecha de seguridad encontrada.

Nota: *el listado completo de nombre de servidores, IP, rol del servidor, estado general de cumplimiento dentro del alcance del reporte del escaneo, total de posibles vulnerabilidades encontradas, vulnerabilidad y descripción, posible remediación, comentarios adicionales y fechas exactas de los escaneos, fue entregado a la compañía como documento confidencial, para lo cual se tiene el siguiente resumen de hallazgos:*

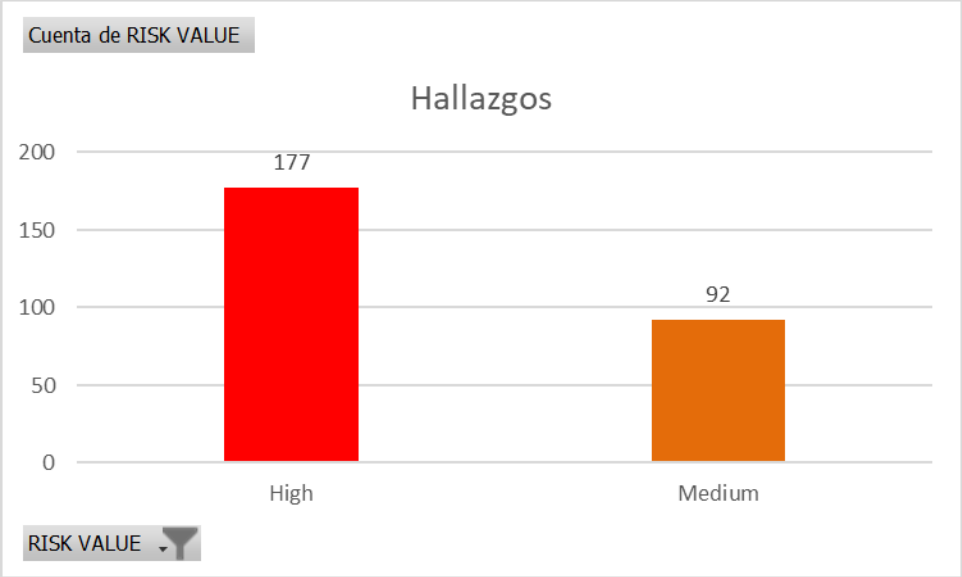


Figura 9. Resultado del análisis de vulnerabilidades

Acorde a la figura 11, se puede indicar como resumen general:

- Se listan por su prioridad, un total de **177** vulnerabilidades consideradas ALTAS (HIGH) fueron encontradas en todos los sistemas y 92 hallazgos fueron considerados de criticidad media, lo que supone un alto riesgos de seguridad en la infraestructura tecnológica.
- Para la organización, se brinda nombre específico del hallazgo, en este caso llamado RISK – FINDINGS, bajo el cual se identifica que tipo de remediación es posible efectuar, según su complejidad y riesgo para la compañía.

4.2. Resumen de hallazgos por rol del servidor

A continuación (figura 12), se incluyen los datos estadísticos por grupo de servidores acorde a los hallazgos:

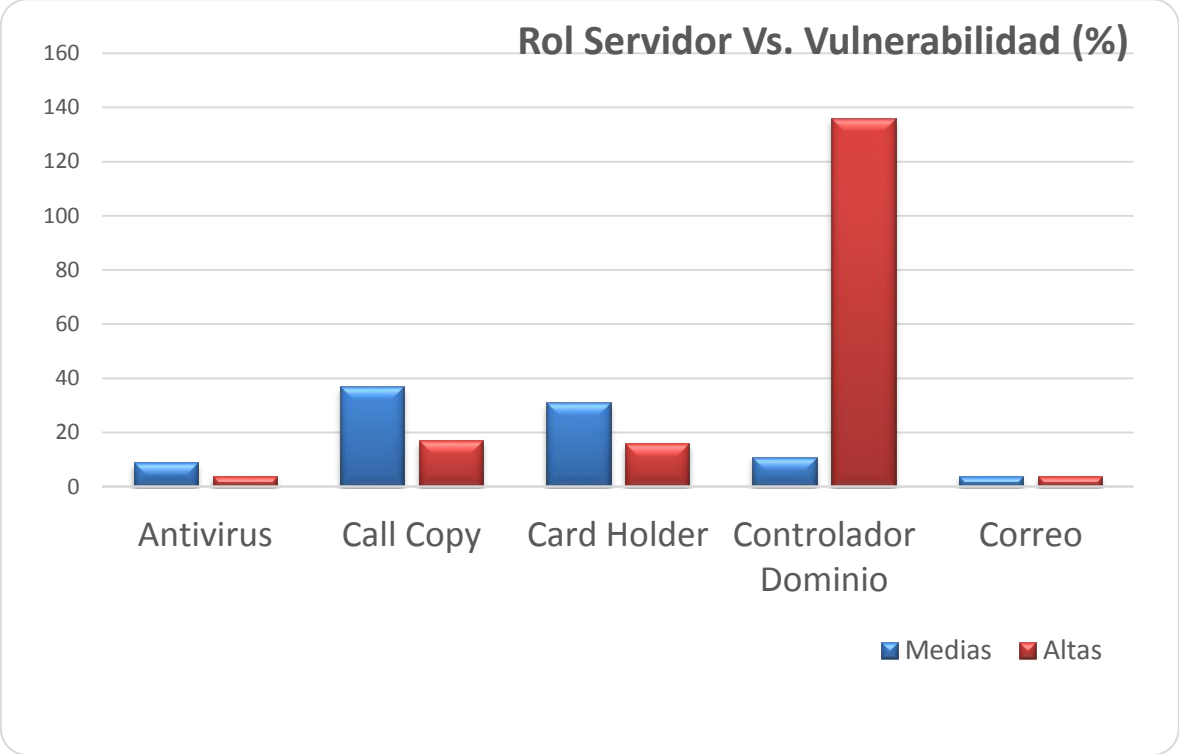


Figura 10. Resultado de Vulnerabilidades por tipo de Servidor

En estos resultados, se ve claramente que los controladores de dominio presentan el nivel más alto de hallazgos (más de 120 vulnerabilidades consideras de nivel alto), lo que genera una alerta a los responsables de éste componente informático, toda vez que se debe generar un plan de mitigación más completo.

Tabla 3 *Resultados Cuantitativos por Servidor*

ANÁLISIS DE VULNERABILIDADES			
Roles de los Servidores	Medias	Altas	Total general
Antivirus	9	4	13
Call Copy	37	17	54
Card Holder	31	16	47
Controlador Dominio	11	136	147
Correo	4	4	8
Total general	**92**	**177**	**269**

NOTA. Se muestra el número de vulnerabilidades por tipos de servidores evaluados.

Acorde a la figura 12 y la Tabla 3, se indica a continuación el análisis vs la solución de las vulnerabilidades encontradas, teniendo en cuenta el contexto del negocio para los tipos de servidores analizados:

- Según los resultados obtenidos, se brindará prioridad a las remediaciones de los servidores con rol de controlador de dominio, ya que tienen una alta importancia, para mantener seguro y administrables los usuarios y recursos de red, y proporcionan compatibilidad a las aplicaciones habilitadas para el directorio como Microsoft® Exchange Server.
- En segunda instancia, se trabajarán las remediaciones para los servidores con rol de Call Copy, debido a que allí se almacena la información referente a las grabaciones de llamadas, que son prioritarias para las operaciones de cada cliente pasa sus seguimientos desde el área de calidad, mejorando la producción y cumpliendo con requerimientos contractuales cada uno de los clientes suscritos a Teleperformance Colombia S.A.S.
- El tercer servidor con rol de Card Holder (y no menos importante por estar en este lugar), se tiene en proceso de análisis con las áreas de infraestructura tecnológica, debido a que las remediaciones a implementar, deben ser revisadas y monitoreadas durante su ejecución, debido al impacto negativo que pueden causar los cambios con las aplicaciones de Cliente utilizadas en los procesos de sus operaciones.

- Por último, se trabajarán en conjunto las remediaciones en conjunto, de los servidores con roles de Antivirus y Correo, ya que al interior de los equipos de infraestructura se ha determinado que las vulnerabilidades identificadas no representan un alto riesgo dentro de las remediaciones propuestas, porque se cuenta con controles de mitigación al interior de dicha área, como son el soporte con el proveedor de servicios.

4.3. Propuestas de remediación

Bajo los estándares corporativos de Teleperformance S.A.S., el plan de remediaciones debe ser entregado en inglés, ya que, en algunas ocasiones, las opciones de ejecución de remediaciones pueden requerir consultas a la casa matriz en USA, lo que brinda agilidad en el tratamiento de la información correspondiente con cada una de las áreas involucradas.

De esta manera, las recomendaciones se hacen para cada hallazgo, acorde al siguiente formato:

- El tipo de vulnerabilidad (Password, SSL, TLS, Certificates, etc.)
- Su descripción y explicación del riesgo que representa, en conjunto de como dicha vulnerabilidad puede ser explotada.
- Remediación sugerida para implementación, la cual, de acuerdo a la necesidad del negocio y el riesgo que representa para la compañía, puede ser ejecutada o en su defecto, validada con los expertos en las áreas de infraestructura, su afectación a nivel funcional dentro de operaciones con los clientes dentro de la organización, entre otros.

Para ilustrar las recomendaciones entregadas se tienen los siguientes 2 casos:

- **De tipo:** Password Does Not Expire
- **Descripción del riesgo:** *If a user password does not expire you allow a remote attacker endless amount of time to try to figure out your users password. It is recommended that you make all users passwords expire unless the user account is used for a system service. Note, Linux/Unix based systems running Samba are also affected by this notification*
- **Posible Remediación:** *Remove the password never expires option from the user account.*

  1. Open User Manager.

  2. Select the user from the list.

  3. Select Properties from the User menu.

  4. Uncheck "Password Never Expires".

  5. Click "OK".

- **De tipo:** SSL/TLS RC4 Cipher Suites Supported
- **Descripción del riesgo:** *The remote host allows the use of RC4 cipher suites. The RC4 cipher generation of a pseudo-random stream of bytes is flawed to allowsmall biases into the stream, decreasing its randomness. If plaintext is encrypted over and over and an attacker is able to obtain millions of ciphertexts, the attacker may be able to retrieve the plaintext from the stream.*
- **Posible Remediación:** *If possible, disable the use of RC4 ciphers in the application or its host operating system.4. Uncheck "Password Never Expires".*

Todos los resultados obtenidos, fueron entregados a las áreas internas de TELEPERFORMACE SAS para que realicen un plan de mitigación de vulnerabilidades sobre los sistemas involucrados. Una vez se inicien las implementaciones de las remediaciones propuestas, se procederá a ejecutar las fases 1, 2 y 3, con el objetivo de verificar que los

riesgos identificados si se cerraron o cuales aún permanecen abiertos y es necesario realizar otro plan de mitigación y un proceso de aceptación del riesgo.

5.CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

En la actualidad la gran mayoría de compañías tienen sus procesos digitalizados, en sistemas de computación; la empresa TELEPERFORMACE SAS con presencia en varios países tiene la premisa de proteger el activo más valioso en su negocio, la información. Haciendo referencia a lo anterior y como estudiantes de Ingeniería en Sistemas, la compañía brindó la oportunidad a dos estudiantes de la institución Instituto Tecnológico Metropolitano – ITM para realizar la implementación de un procedimiento de sistema de gestión de vulnerabilidades, para lo cual, tanto la instalación, como la ejecución y las recomendaciones entregadas a la compañía fueron exitosas, cumpliendo con los objetivos planteados.

Como consecuencia de la necesidad descrita por la **Ana Lucia Gómez Osorio** (IT Security Manager), se logró el objetivo planteado como proyecto, que fue el de analizar las vulnerabilidades de seguridad informática y su posible mitigación en un ambiente de producción real de IT, mediante el uso de la herramienta de escaneo RETINA en la empresa TELEPERFORMANCE S.A.S en las ciudades de Medellín y Bogotá, en consecuencia, todos los objetivos específicos también se lograron alcanzar con éxito:

1. Identificar el alcance de la red y los servicios informáticos para evaluación de vulnerabilidades: entregando en listado completo de los equipos a realizar la prueba de seguridad.
2. Diseñar el servidor donde estará instalada la suite de RETINA: Entregando los requerimientos técnicos necesarios para la implementación de RETINA.
3. Establecer la configuración específica de RETINA acorde al alcance de la red y servicios para la ejecución del análisis: Configurando la herramienta y ejecutando el análisis de vulnerabilidades.
4. Sintetizar el informe de las vulnerabilidades, amenazas y riesgos existentes con el respectivo plan de remediación: entregando los informes de seguridad con las respectivas recomendaciones a la empresa.

Se realizó por parte de TELEPERFORMACE SAS la compra de la herramienta **RETINA Network Security Scanner**, después de un previo estudio por parte de los analistas, se logró crear un manual específico para Colombia y se adjunta éste como anexo, adicional a esto, se deja como **apéndice A**, las líneas de comandos para la instalación.

Se hace aclaración de los Requisitos de máquina, que se requieren para la instalación, esta lista se crea para efectos de la Empresa TELEPERFORMACE SAS en Colombia, con el fin de dejar todo el proceso documentado y funcional, lo que se entrega es valor agregado a los objetivos inicialmente planteados.

Por otra parte, se entiende y reconoce las diferentes escalas de medición de las vulnerabilidades, para poder plasmar en el informe final un estado de la seguridad en la red. Es importante destacar las pruebas de comunicación que se hacen previas al escaneo, estas pruebas son básicas pero importantes para garantizar el correcto proceso de gestión de las vulnerabilidades, si llegase a haber falla desde el área de red corporativa se otorgan los permisos para garantizar la comunicación desde el servidor de retina hacia los servidores a evaluar.

El presente trabajo también se caracteriza por adaptarse a los lineamientos de la empresa a nivel de procesos, donde se explica de forma detallada como crear la **Orden de Cambio** (OC) desde el software **Service Desk** (Herramienta de Gestion de TI usada por la compañía), esta tarea es requerida para preparar la ejecución del escaneo de vulnerabilidades con RETINA y en la metodología se redacta de forma detallada y también en el documento anexo 3: **PROCEDIMIENTO PARA EL MANEJO VULNERABILIDADES INTERNAS Y SUS REMEDIACIONES PLANTEADAS**, está redactado quien es el encargado de realizar esta actividad.

Por último, la recomendación general y trabajo futuro a desarrollar, es que la compañía designe un área responsable o una persona que logre sacar adelante la implementación de las recomendaciones de seguridad entregadas, dado que éstas acciones no hacen parte de éste proyecto, pero desde el punto de vista de seguridad, es fundamental su solución y

cierre del ciclo de vulnerabilidades, así mismo, cree un programa de ejecución periódica de análisis de vulnerabilidades (al menos cada 6 meses).

A continuación se muestra el diagrama de flujo del programa creado para la compañía, donde se detalla el proceso completo para el manejo de las vulnerabilidades en la compañía TELEPERFORMANCE SAS.

6. REFERENCIAS

Sheets, D. and Security..., R. (2017). Retina Network Security Scanner - BeyondTrust. [online] BeyondTrust. Available at: https://www.beyondtrust.com/resources/data-sheet/retina-network-security-scanner/ [Accessed 5 Nov. 2017].

FIRST — Forum of Incident Response and Security Teams. (2017). Common Vulnerability Scoring System SIG. [online] Available at: https://www.first.org/cvss/ [Accessed 5 Nov. 2017].

Aprenderaprogramar.com. (2017). Cite a Website - Cite This For Me. [online] Available at: https://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftppop3-y-smtp-dhcp&catid=57&Itemid=179 [Accessed 5 Nov. 2017].

Es.wikipedia.org. (2017). Controlador de dominio. [online] Available at: https://es.wikipedia.org/wiki/Controlador_de_dominio [Accessed 5 Nov. 2017].

Culturación. (2017). ¿Qué es un servidor de correo? - Culturación. [online] Available at: http://culturacion.com/que-es-un-servidor-de-correo/ [Accessed 6 Nov. 2017].

PCI Hispano. (2017). CardHolder Data Matrix (CHDM): ¿Qué es y para qué se utiliza? - PCI Hispano. [online] Available at: https://www.pcihispano.com/cardholder-data-matrix-chdm-que-es-y-para-que-se-utiliza/ [Accessed 6 Nov. 2017].

Gestión y Desarrollo Tecnológico. (2017). Teleperformance SAS. [online] Available at: https://luchomurcia.wordpress.com/2015/03/04/teleperformance-sas/ [Accessed 6 Nov. 2017].

Es.wikipedia.org. (2017). Ping. [online] Available at: https://es.wikipedia.org/wiki/Ping [Accessed 6 Nov. 2017].

Es.wikipedia.org. (2017). Dirección IP. [online] Available at: https://es.wikipedia.org/wiki/Dirección_IP [Accessed 6 Nov. 2017].

Repository.libertadores.edu.co. (2017). Cite a Website - Cite This For Me. [online] Available at: http://repository.libertadores.edu.co/bitstream/handle/11371/1300/hernandezyohan2017.pdf?sequence=1 [Accessed 6 Nov. 2017].

E-spincorp.com. (2017). Cite a Website - Cite This For Me. [online] Available at: http://e-spincorp.com/pdf/product/eEye/Retina-Installation-Guide-E-SPIN.pdf [Accessed 6 Nov. 2017].

FIRST — Forum of Incident Response and Security Teams. (2017). CVSS v3.0 Specification Document. [online] Available at: https://www.first.org/cvss/specification-document [Accessed 6 Nov. 2017].

7.ANEXOS

7.1. Anexo 1: Manual de instalación de RETINA

Este manual se anexa en el entregable

7.2. Anexo 2: Creación y gestión de la Orden de Cambio - OC

1. Creación: se muestra ejemplo con la figura 13. Se deben tener en cuenta los campos resaltados en color verde: Reported By, Category, Group, Location.

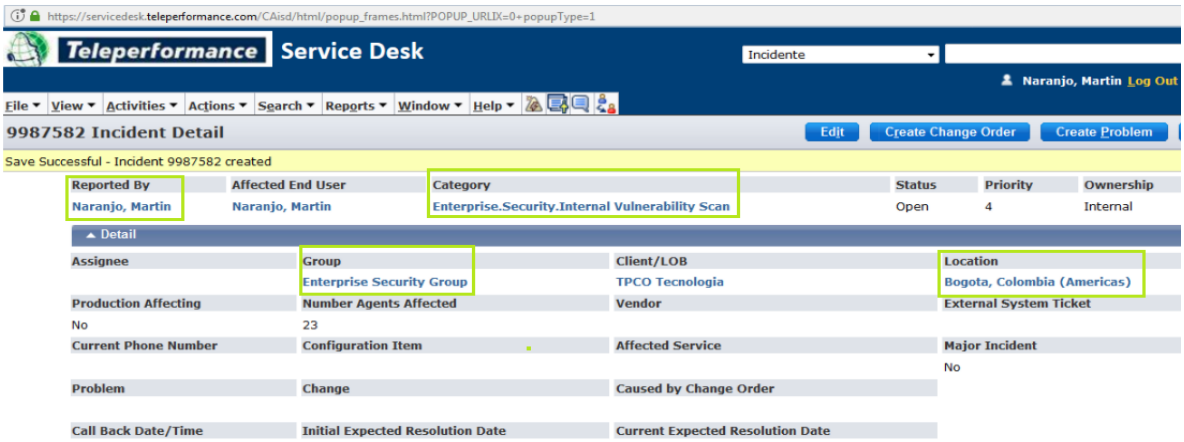


Figura 11. Herramienta Servicie Desk para Teleperformance

2. Luego de la creación de la OC, se prosigue con la asignación de la tarea a realizar, en este caso es: **internal vulnerability assessment** (evaluación de vulnerabilidad interna) y la hora de inicio, como se muestra un ejemplo en la figura 14

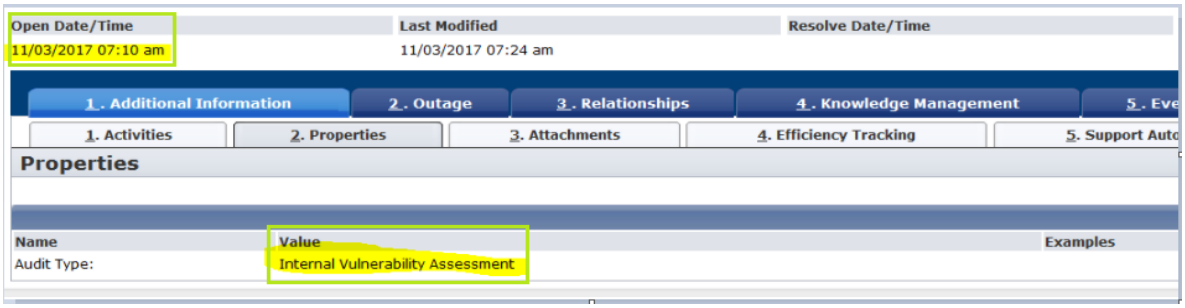


Figura 12. Asignación de la tarea a realizar

3. Paso seguido en Service Desk, se deben dejar por escrito todas las recomendaciones necesarias, como se muestra a continuación en la figura 15:

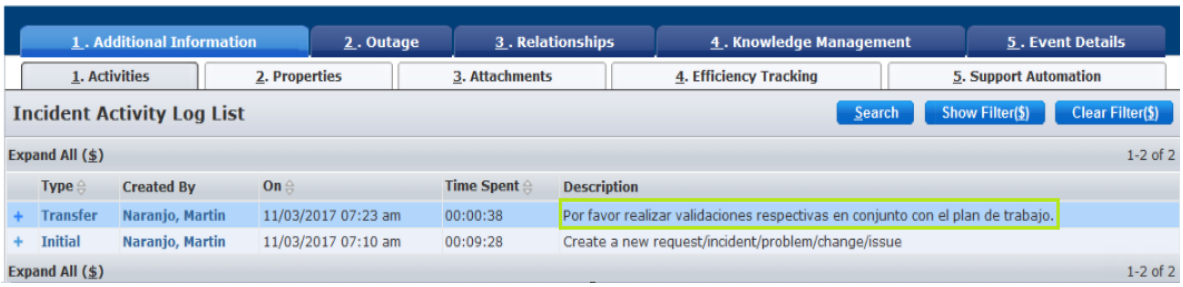


Figura 13. Asignación de la tarea a realizar

4. Para finalizar se debe documentar (log comment) los servidores que serán intervenidos en el escaneo, como se observa en la figura 16

Figura 14. Documentación de los servidores

5. La orden de cambio (OC) queda en estado inicial **Open** (Abierto) como se muestra en la figura 17, al momento de iniciar se debe cambia a estado **en Progreso** (figura 18), cuando se termine el escaneo se debe dejar en estado **Análisis Completado** (figura 19) y al finalizar se debe documentar, adjuntar los reportes y cambiar a estado **Cerrado** (figura 20)

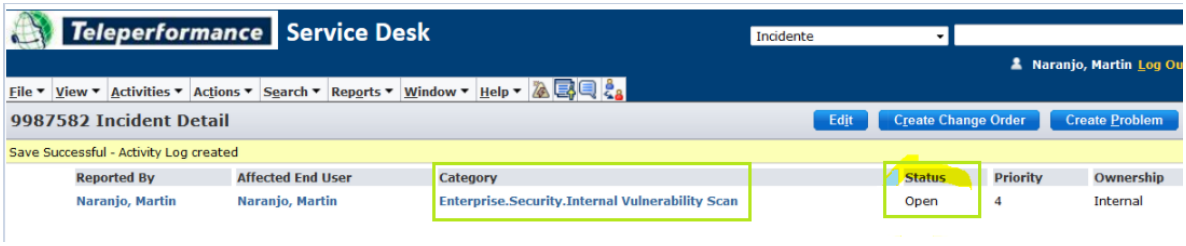


Figura 15. Orden de Cambio en estado Abierto

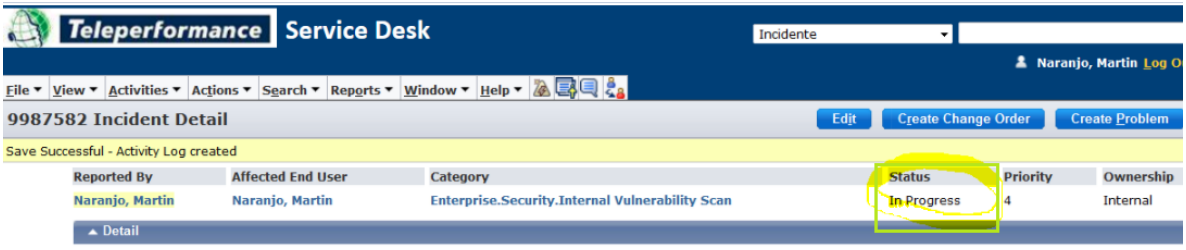


Figura 16. Orden de Cambio en estado En Progreso

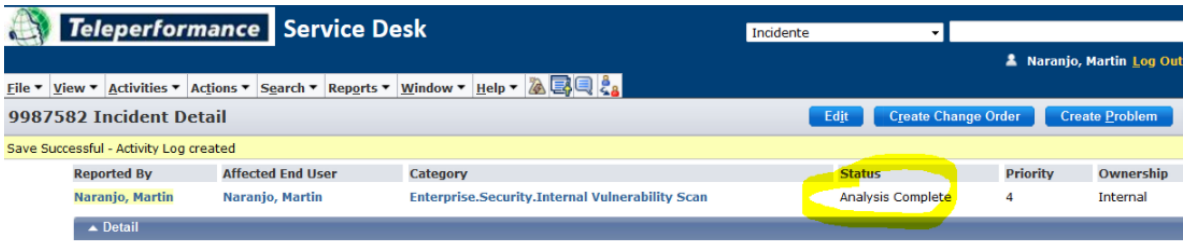


Figura 17. Orden de Cambio en estado Análisis Completado

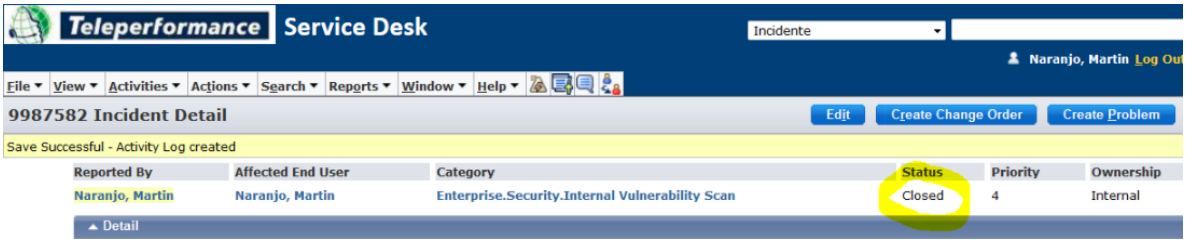
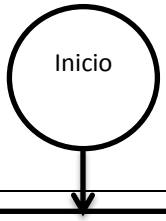
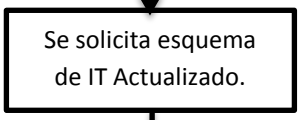
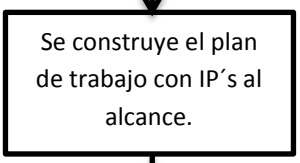
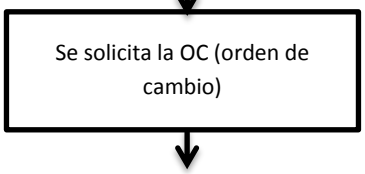
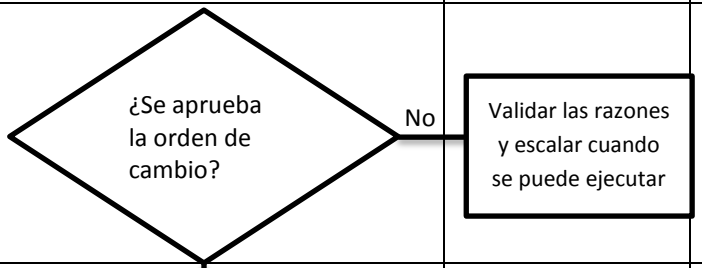
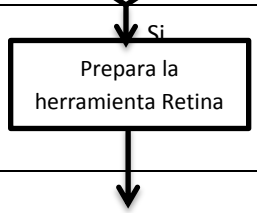
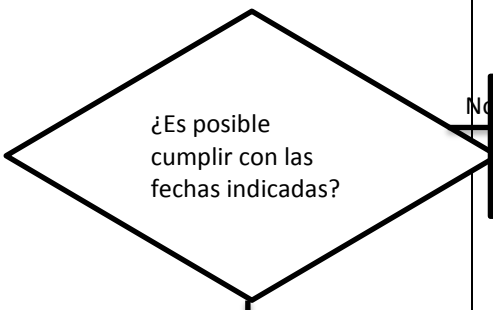
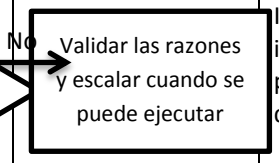
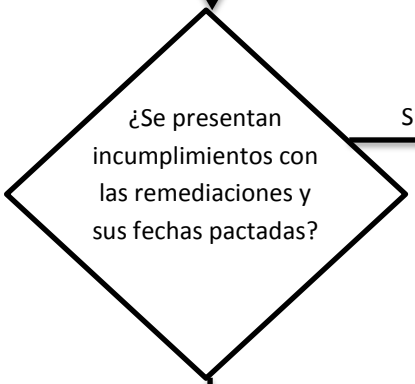
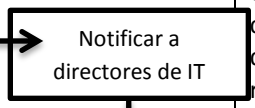


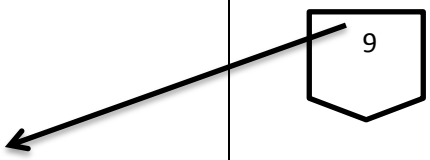
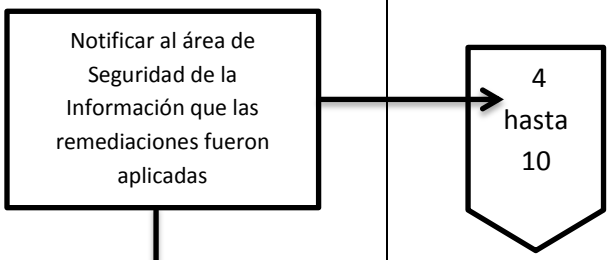
Figura 18. Orden de Cambio en estado Análisis Completado

7.3. Anexo 3: Procedimiento para el manejo vulnerabilidades internas y sus remediaciones planteadas

El siguiente flujograma ilustra el procedimiento para la ejecución de un análisis de vulnerabilidades, de la misma forma, se anexa el procedimiento como documento complementario:

Ítem	MANEJO VULNERABILIDADES	TPCO	OBSERVACIONES
1			Inicio de la planeación del proyecto.
2			Analista de Seguridad IT solicita al área de infraestructura IT el esquema actualizado.
3			Reporte inmediato de trabajo para informar a los equipos involucrados.
4			Creación de la orden de cambio por medio del analista de seguridad de la información, en la herramienta Service Desk.
5			Validar con los equipos de infraestructura, cuando es posible aprobar la orden de cambio.
6			Se ejecuta escaneo de Ip´s al alcance con la herramienta Retina.

7			Clasificación de vulnerabilidades encontradas a nivel interno según su nivel de criticidad (altas y medias, ya que las bajas no aplican a remediación).
8			Se notifica a Notifica a Seguridad de la Información sobre los inconvenientes presentados, para ser documentados. El plan de trabajo original, debe ser modificado y entregado de nuevo a los equipos con las fechas nuevas.
9			Se brinda asesoría a los equipos de infraestructura IT por parte d Seguridad de la información. (de acuerdo a los lineamientos corporativos). Se vela por el cumplimiento de políticas de seguridad en la compañía y se validan los posibles clientes afectados.
10			El área de Seguridad de la Información, notifica dicho incumplimientos de las áreas comprometidas a sus directores de IT respectivos. El proceso comienza de nuevo, una vez los directores notifiquen al área de Seguridad de la Información.

11			Se remite al Ítem 9 de nuevo. Una vez finalizado el paso de ejecución de propuesta de remediación, se continúa con el Ítem 12.
12			De esta forma se debe proceder con un re-escaneo para validar si efectivamente las vulnerabilidades fueron remediadas. Se ejecutan los pasos de la cadena desde el Ítem 4 hasta el 10.
13			Entrega de reporte limpio. Se notifican las áreas involucradas durante todo el proceso y se brindan sugerencias/mejoras al procedimiento establecido según las dificultades presentadas.
14			Fin del procedimiento

8.APÉNDICE

8.1. Apéndice A. Código Para Instalación por Comando de RETINA

Los siguientes comandos son para instalar Retina, se toman de la guía de instalación.

REINSTALLMODE=”amus”

Cause all files to be overwritten.

/qn

Completely silent.

User interface does not display. If a reboot is required, Windows Installer automatically reboots the system at the end of installation.

/qb

Basic user interface.

Only a progress dialog is displayed to the user. If a reboot is required, Windows Installer prompts the user to reboot.

INSTALLDIR=”…”

Installation folder where … is the path to install.

Set this property to change the default installation path.

CREATEDESKTOPICON=”0”

Disables creation of a desktop icon for Retina.

This option is enabled by default. Set to 0 to prevent creation of the icon.

/l*v “C:\RetinaInstallLog.txt”

Enables full logging.

This should only be used for debugging if problems occur during installation.

REBOOT=”ReallySuppress”

Used to suppress the automatic reboot when using the /qn silent option. The reboot still needs to occur, for the software to run properly.

SERIALNUMBER="…"

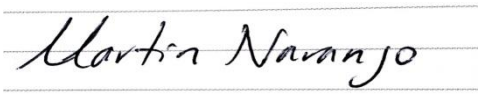
Sets the serial number where … is the actual serial number.

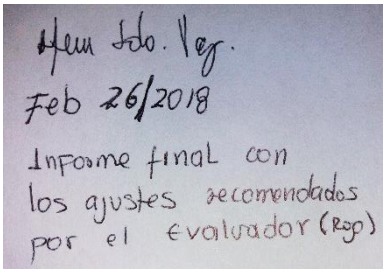
CFPATH="…"

Path for Common BeyondTrust files, such as Auto Update.

If another BeyondTrust product is installed, this parameter is ignored since the common path must be the same for all BeyondTrust products.

FIRMA ESTUDIANTES 



FIRMA ASESOR 

FECHA ENTREGA: **26/02/2017**_____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____