DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

Diagnóstico de Seguridad Informática utilizando la metodología de Análisis de Vulnerabilidades en la red del Banco Nacional de Fomento - Casa Matriz Quito-Ecuador

AUTORES: ESPINOZA BUCHELI ALAN MICHAEL

MONTOYA TAPIA DAVID ARMANDO

DIRECTOR: ING. ÑACATO CAIZA GERMÁN

CODIRECTOR: ING. ARROYO RUBÉN

SANGOLQUÍ

2016

CERTIFICACIÓN DEL DIRECTOR

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICACION

Certifico que el trabajo de titulación, "***DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA UTILIZANDO LA METODOLOGÍA DE ANÁLISIS DE VULNERABILIDADES EN LA RED DEL BANCO NACIONAL DE FOMENTO - CASA MATRIZ QUITO – ECUADOR***", realizado por los señores ***ESPINOZA BUCHELI ALAN MICHAEL*** y ***MONTOYA TAPIA DAVID ARMANDO***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores ***ESPINOZA BUCHELI ALAN MICHAEL*** y ***MONTOYA TAPIA DAVID ARMANDO*** para que lo sustenten públicamente.

Sangolquí, 24 de marzo del 2016

ING. NACATO CAIZA GERMAN

DIRECTOR

AUTORÍA DE RESPONSABILIDAD

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Nosotros, ***ESPINOZA BUCHELI ALAN MICHAEL,*** con cédula de identidad N° 1713468799 y ***MONTOYA TAPIA DAVID ARMANDO,*** con cédula de identidad N° 1719377150, declaramos que este trabajo de titulación "***DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA UTILIZANDO LA METODOLOGÍA DE ANÁLISIS DE VULNERABILIDADES EN LA RED DEL BANCO NACIONAL DE FOMENTO - CASA MATRIZ QUITO - ECUADOR***", ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 24 de marzo del 2016

ESPINOZA BUCHELI ALAN MICHAEL
C.C.: 1713468799

MONTOYA TAPIA DAVID ARMANDO,
C.C.: 1719377150

AUTORIZACIÓN

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, ***ESPINOZA BUCHELI ALAN MICHAEL*** y ***MONTOYA TAPIA DAVID ARMANDO,*** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "***DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA UTILIZANDO LA METODOLOGÍA DE ANÁLISIS DE VULNERABILIDADES EN LA RED DEL BANCO NACIONAL DE FOMENTO - CASA MATRIZ QUITO - ECUADOR***", cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, 24 de marzo del 2016

ESPINOZA BUCHELI ALAN MICHAEL
C.C.: 1713468795

MONTOYA TAPIA DAVID ARMANDO,
C.C.: 1719377150

DEDICATORIA

Dedico esta Tesis primeramente a Dios, por darme la vida por ser mi guía en todo momento, ser mi fortaleza y esperanza y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

En especial a mi abuelita Marujita Yánez por estar siempre conmigo, por quererme y apoyarme siempre, aunque ya no este con nosotros me enseñó a ser fuerte y siempre ser una persona de bien, a tu memoria abuelita te dedico y te debo todo lo ahora soy y estoy consiguiendo.

A mi esposa por su incondicional apoyo y tenacidad que me impulsó siempre a seguir adelante a no desmayar, por estar conmigo en todo momento, a mis hijos Josue y Dayanna que siempre serán mi fuerza y mi inspiración.

A mi Padres por confiar en mi y darme la oportunidad de estudiar en esta prestigiosa Universidad, a mis hermanos por quererme mucho, creer en mi y porque siempre me apoyaron durante toda mi carrera.

A ustedes les debo todo.

ALAN MICHAEL ESPINOZA BUCHELI

Con todo mi cariño y mi amor para las personas que hicieron todo en la vida para que yo pudiera lograr mis sueños, por motivarme y darme la mano cuando sentía que el camino se terminaba, a ustedes por siempre mi corazón y mi agradecimiento.

DAVID ARMANDO MONTOYA TAPIA

AGRADECIMIENTO

Quiero agradecer primeramente a Dios por bendecirme y darme fuerza para llegar hasta donde he llegado

A la prestigiosa Universidad de las Fuerzas Armadas ESPE por brindarme la oportunidad de poder estudiar y llegar a ser un profesional.

A mi Director de Tesis Ing. Germán Ñacato y mi Codirector Ing. Rubén Arroyo por su esfuerzo, dedicación y paciencia, gracias por brindarme sus conocimientos y motivarme siempre para terminar con mis estudios con éxito, a mis profesores que durante toda mi carrera me enseñaron a que cada día uno sigue aprendiendo, su aportes y sus enseñanzas han sido de gran ayuda para mi formación profesional

A toda mi familia por ser el pilar en mi vida, y a todas las personas que formaron parte de este gran proceso del cual he llegado a sentirme muy orgulloso.

ALAN MICHAEL ESPINOZA BUCHELI

Agradezco a mis padres, Marco e Isabel, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento. Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. Es por ello que soy lo que soy ahora.

Agradezco a Estefania, Isabela y Karina, por su apoyo incondicional, cada una a su manera ha sido una ayuda en las diferentes etapas de mi vida, sin ellas no podría haber llegado a cumplir las metas que me he planteado hasta el momento.

DAVID ARMANDO MONTOYA TAPIA

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El Banco Nacional de Fomento, es una entidad del gobierno, que presta varios servicios financieros a usuarios internos y externos, su Casa Matriz se encuentra en la ciudad de Quito y posee mas de 110 sucursales a nivel nacional. En los últimos años, las instituciones bancarias ecuatorianas han tenido un desarrollo organizacional, social y económico, el cual ha contribuido para la implementación de nuevos servicios a sus clientes. Actualmente el Banco Nacional de Fomento no posee un análisis de vulnerabilidades por lo que no está listo para evitar los diferentes ataques o amenazas que puedan presentarse. La metodología de Análisis de Vunerbilidades que se presenta en este proyecto se basa en la implementación de fases que servirán para determinar las brechas de seguridad existentes en la red de la institución, las mismas que la hace vulnerable. El presente análisis tendrá la información de la infraestructura tecnológica con la cuenta el BNF, las técnicas de análisis utilizadas presentarán resultados los cuales serán complementados con varias contramedidas que tienen como principal objetivo el ayudar a la entidad a mejorar su seguridad informática y mitigar las vulnerabilidades encontradas con las diferentes herramientas se fueron utilizadas para la elaboración de este análisis, como son Network Scanning (Angry IP), Port Scanning (NMAP) y Vulnerability Scanning (GFI Landguard).

PALABRAS CLAVES

- METODOLOGÍA
- ANÁLISIS
- VULNERABILIDADES
- SEGURIDAD
- NETWORK SCANNING
- PORT SCANNING
- VULNERABILITY SCANNING

ABSTRACT

The National Development Bank, is a government entity, which provides various financial services to internal and external users, its headquarters is located in the city of Quito and has more than 110 branches nationwide. In recent years, Ecuador's banking institutions have an organizational, social and economic development, which has contributed to the implementation of new services to its customers. Currently, the National Development Bank does not have a vulnerability analysis so that it is not ready to avoid the different attacks or threats that may arise. The Vunerbilidades Analysis methodology presented in this project is based on the implementation phase that will serve to identify gaps existing network security of the institution, which makes them vulnerable. This analysis will information technology infrastructure with the BNF account analysis techniques used present results which will be complemented by several countermeasures whose main objective is helping the company to improve security and mitigate vulnerabilities found with the different tools you are were used to prepare this analysis, such as Network Scanning (Angry IP), Port Scanning (NMAP) and Vulnerability Scanning (GFI Landguard) they are.

KEYWORDS

- METHODOLOGY
- ANALYSIS
- VULNERABILITIES
- SAFETY
- NETWORK SCANNING
- PORT SCANNING
- VULNERABILITY SCANNING

GENERALIDADES

1.1 Introducción

En los últimos años, las instituciones bancarias ecuatorianas han tenido un desarrollo organizacional, social y económico; el cual ha contribuido para la implementación de nuevos servicios a sus clientes, orientados principalmente en servicios web que permitan a los usuarios realizar sus transacciones en línea.

Si bien los servicios bancarios tienen varias seguridades informáticas, han ido apareciendo vulnerabilidades en las redes y en los equipos, poniendo en mayor riesgo la integridad informática de las instituciones financieras.

La seguridad de una organización es un aspecto cambiante. Una empresa puede alcanzar un nivel de protección óptimo en un momento determinado y ser totalmente sensible poco después, esto puede tener varias causas; un ejemplo podría ser, al hacer un cambio en la configuración de un servidor, o al instalar nuevos dispositivos de red, pueden aparecer vulnerabilidades que pongan en riesgo la seguridad de una entidad bancaria. Otro punto a considerar es la aparición de fallas de seguridad en software existentes, que previamente se creían seguros.

Actualmente las organizaciones tienen medidas reactivas contra los ataques, se crean trampas para el momento en que se produce un ataque y además se dispone de herramientas para capturar el tráfico que pasa por un segmento de red.

Un Análisis de Vulnerabilidad puede ser usada como medida preventiva y para ello, lo que se busca saber es cuán vulnerable son las máquinas de nuestra organización.

Se han hecho grandes esfuerzos en la comunidad informática para crear bases de datos formales donde se encuentra información crítica como: cual es vulnerabilidad, a que sistemas impacta, como se activa la vulnerabilidad, cual es el código que la activa, como se corrige la vulnerabilidad.

Una de las preocupaciones más importantes de los profesionales de la seguridad de la información es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas tecnológicos, las cuales son el blanco predilecto de herramientas de software cada vez más poderosas en su capacidad de ocasionar daños a los sistemas de información y la infraestructura que los soporta.

Lo anterior promueve a pensar que se necesita contar con una estrategia más coherente y efectiva para mitigar esta inquietante y crítica amenaza, de tal manera, que se ha recopilado una serie de actividades y recomendaciones que le ayudarán a ciertas empresas a realizar un análisis a nivel técnico de las vulnerabilidades de software, asociadas a sus activos de tecnológicos.

Una política de realización de Análisis de Vulnerabilidades periódicas, mitiga en gran medida, el riesgo asociado a un entorno en constante cambio, tal como lo representan la mayoría de los sistemas informáticos.

El Banco Nacional de Fomento, en adelante BNF, se presenta de manera individual como un banco del gobierno, mismo que a su vez presta varios servicios a usuarios internos y externos, que poseen una o varias cuentas en esta institución financieras o a su vez haciendo uso de sus Servicios, como por ejemplo Pago de Servicios Básicos, Bono de Desarrollo Humano, Transferencia interbancarias, entre otros.

BNF tiene sus oficinas principales y el centro de datos en Quito, Ecuador, en la siguiente dirección: Antonio Ante OE1-15 y Av. 10 de Agosto. Adicionalmente, cuenta con 152 sucursales a lo largo del país.

BNF cuenta con varios diagramas de red detallados que incluyen los dispositivos físicos que se encuentran en las diferentes ubicaciones dentro del edificio, como se muestra en el Anexo IV y en el Anexo Digital.

A nivel de red, BNF tienen sus oficinas principales diferentes VLANs sobre las cuales se encuentran los equipos de la red corporativa (estaciones de trabajo) y en un segmento aparte, restringido por Firewall, la red de servidores.

De acuerdo con la descripción de los procesos y la arquitectura de red actualmente el BNF incluye:

- Sede principal BNF
- Sucursales
- Servidores

Debido a que no se tiene una segmentación específica de algunos equipos en el alcance toda la red está dentro del alcance, incluyendo todas las estaciones de trabajo.

Es necesario generar un diagrama de red de alto nivel que permita identificar los diferentes sitios donde se tienen equipos de comunicación y los equipos dentro de la red, los cuales permiten controlar el tráfico y las conexiones hacia terceros.

La Gerencia de Tecnología, dentro de sus competencias, se encuentra en un proceso de mejoramiento continuo, por tal motivo el realizar un diagnóstico de red dentro de la Institución, ayudaría a minimizar los riesgos para el manejo de información de los funcionarios y clientes.

1.2 Definición del tema

El Análisis de Vulnerabilidades, se enfocará principalmente en el escaneo de redes para lo cual se tomaran en cuenta los tipos de escaneo y las diferentes herramientas que permitan acceder a información confiable para generar contramedidas que disminuyan las vulnerabilidades y mejoren la situación actual de la Institución.

Los tipos de escaneo que se realizarán en este estudio son:

- Port Scanning
- Network Scanning
- Vulnerability Scanning

Los resultados obtenidos del Análisis de Vulnerabilidad realizado, presentarán las vulnerabilidades informáticas existentes en el BNF - Edificio Santa Prisca, así como también, se generarán reportes del análisis efectuado.

1.3 Planteamiento del problema

El Banco Nacional de Fomento al momento no ha realizado un análisis de vulnerabilidades del sistema, por lo tanto no está listo para evitar diferentes amenazas o ataques informáticos que se pudieran presentar.

1.3.1 Descripción breve del escaneo de redes y la evaluación a desarrollar

El presente proyecto de tesis determina la ejecución de un plan de escaneo de la red utilizando las diferentes fases del análisis como se indica a continuación tomando en cuenta 4 partes principales que se llevarán a cabo de la siguiente manera:

En la primera parte del plan se realiza un escaneo donde se determinan puertos abiertos y cerrados, luego se muestra otras opciones que se debe tomar en cuenta para el desarrollo de los siguientes escaneos ya que con estos se puede solucionar otros problemas detectados.

Luego se realizará un escaneo de redes que en realidad determina e identifica todos los valores que nuestra red tiene y cada computador, ya que pertenecen a otro tipo de escaneo, pero a su vez como se mencionó antes, éstas herramientas permiten obtener la mayor información posible del estado del equipo escaneando.

A continuación se realizó un escaneo en busca de vulnerabilidades las cuales se ven reflejadas de igual manera en los gráficos expuestos en su implementación, al igual que los escaneos anteriores en este también se puede determinar otras funciones de escaneo que las herramientas tienen sin dejar desmerecer su primera función como es el escaneo de vulnerabilidades.

Para finalizar se presentarán diferentes contramedidas por cada técnica de escaneo.

1.4 Justificación

"El Banco Nacional de Fomento, es una entidad financiera de desarrollo, autónoma, de derecho privado y finalidad social y pública, con personería jurídica y capacidad para ejercer derechos y contraer obligaciones."

La visión del BNF es:
"Al 2017 consolidarse como la institución articuladora del desarrollo rural, mediante la provisión de servicios financieros confiables, eficientes y eficaces, que promuevan en el espacio rural el desarrollo de las familias, comunidades y sectores

productivos estratégicos para el país.”. (Ezone. (2014). Misión y Visión. 07/01/2015, De BNF Sitio web: https://www.bnf.fin.ec/index.php?option=com_content&view=article&id=1&Itemid=23&lang=es).

Como se muestra en la visión de la Institución, se busca aportar a la ejecución de objetivos del país, por tal motivo el Banco Nacional de Fomento, enfoca todos sus esfuerzos en brindar los mejores servicios tecnológicos a los Clientes Internos y Externos, pero debe tener muy claro que la Institución puede ser blanco de amenazas internas o externas, por tal motivo es muy importante la implementación de un análisis de vulnerabilidades que pueda proponer acciones o contramedidas eficaces para la mitigación de los efectos de ataques de amenazas que puedan afectar al correcto funcionamiento de los Servicios de la Institución.

Actualmente las instituciones financieras deben garantizar la seguridad de las transacciones de sus clientes, disminuyendo los riesgos de ataques de los que pueden ser víctimas, así por ejemplo:

- Se puede evitar caídas de los sistemas existentes, ya que estas perjudican a la imagen de la Institución, perdiéndose de esta manera la disponibilidad de los datos.
- Mejoramiento de la configuración de los equipos de comunicación.
- Reducir costos al adquirir solamente el hardware necesario, optimizando la red para brindar un servicio óptimo y seguro.
- Definir e implementar mejores políticas de Seguridad Informática dentro de la Institución.
- Mejorar los métodos de autenticación y procedimientos para proteger contra los riesgos de robo de claves y usuarios de los clientes a través de e-mail y otros fraudes.

- Revisar y mejorar las prácticas de protección de información confidencial de los clientes.
- Entrenar al personal interno para que puedan asesorar al cliente sobre los temas de seguridad preventiva.
- Generar un cuadro general que indica número de vulnerabilidades, nivel de impacto frente a su criticidad en una escala que va de 5 como la más alta y 3 como la más baja.
- Elaborar un informe de las vulnerabilidades encontradas que explica la amenaza, los efectos, las contramedidas y el uso de herramientas para superar tal vulnerabilidad.
- Realizar un Informe ejecutivo basado en tendencia e historial del riesgo y expresado en gráficas de impacto al negocio, de vulnerabilidades nuevas, activas, remediadas y re-abiertas/ re-incidentes).
- Reducción de los tiempos de inactividad del sistema gracias a los agentes de escaneo, expertos en labores de monitoreo y administración. Se integra con otros servicios administrados de seguridad, lo que se traduce en mejoramiento de la funcionalidad

1.5 Objetivos

1.5.1 Objetivo General

Realizar un diagnóstico de la Seguridad Informática, utilizando la metodología de Análisis de Vulnerabilidades, para determinar el estado en el cual se encuentra la red en el Edificio Santa Prisca de la Casa Matriz del Banco Nacional de Fomento, para proponer las posibles contramedidas y así, prevenir la aparición de vulnerabilidades de alto riesgo y minimizar las mismas, utilizando las técnicas de Port Scanning, Network Scanning y Vulnerability Scanning.

1.5.2 Objetivos Específicos

- Identificar la situación actual de la tecnología que utiliza el Banco Nacional de Fomento en el Área de Servicios Bancarios.
- Identificar el nivel de seguridad informática en lo referente al análisis de vulnerabilidades con el que cuenta el Banco Nacional de Fomento.
- Recomendar actualizaciones o configuraciones adicionales en los sistemas que posee el Banco Nacional de Fomento.
- Determinar los puertos abiertos y cerrados, los host y las vulnerabilidades en los PC's que posee el Banco Nacional de Fomento
- Utilizar Técnicas de Detección de Vulnerabilidades como es el Etical Hacking
- Poder determinar cuáles son las vulnerabilidades existentes en los activos de su red.
- Poder priorizar y remediar con efectividad las vulnerabilidades de los activos de su red.
- Conocer las fases a seguir al momento de realizar un análisis de vulnerabilidades
- Conocer algunas herramientas que pueden ser utilizadas para la realización de un análisis de vulnerabilidades

1.6 Alcance

Se va a monitorear todos los equipos del Banco Nacional de Fomento (700 equipos aproximadamente), con el fin de determinar vulnerabilidades y amenazas que pudieran estar afectando la seguridad informática de esta entidad.

Todos estos equipos van a ser objeto del estudio, para detectar las vulnerabilidades presentadas en la red de datos, con la información recolectada se realizará un análisis y se propondrá posibles contramedidas para mitigar las posibles y futuras amenazas en la red del Banco Nacional de Fomento.

1.6.1 Territorial

El presente proyecto se desarrollará en el Edificio Santa Prisca, donde funcionan las instalaciones de la Casa Matriz y Sucursal Quito del Banco Nacional de Fomento, ubicado en las calles Av. 10 de Agosto y Antonio Ante. En el edificio antes mencionado se procederá a realizar el análisis de vulnerabilidades a todos los equipos dentro de la red, para proponer posibles contramedidas que ayuden a mitigar riesgos y mejorar las seguridades de la red de la entidad.

1.6.2 Tecnológico

Se tomará en cuenta los diagramas de la arquitectura tecnológica con la que dispone el BNF, que servirá para delimitar y organizar el respectivo análisis como se muestra en el Diagrama 1.

La red de datos del Banco Nacional de Fomento, está dividida en Red WAN (Redes de las Sucursales), Red LAN (Red Local del Edificio Santa Prisca), la cual está dividida en VLAN's que pertenecen a los diferentes pisos que comprenden el edificio en mención.

La red Fast Ethernet, emplea cable coaxial cat. 5e, y sus protocolos ya están orientados para la automatización de oficinas, procesamiento de datos distribuido y acceso de terminales las cuales serán analizadas.

Mediante este análisis se obtendrá los resultados necesarios con los que la red de Banco Nacional de Fomento pueda mitigar ataques y asegurar la red informática, tomando en cuenta que tiene una Zona Militarizada o MZ, en la cual se encuentran los Servidores del Core Bancario, que es el Sistema Bancario Integrado con el que cuenta la Institución, también una Zona Desmilitarizada donde se encuentran los Servidores

Publicados al Internet, es decir los Servicios Externos que se ofrecen a los Clientes como por ejemplo el Servicio de Banca Electrónica.

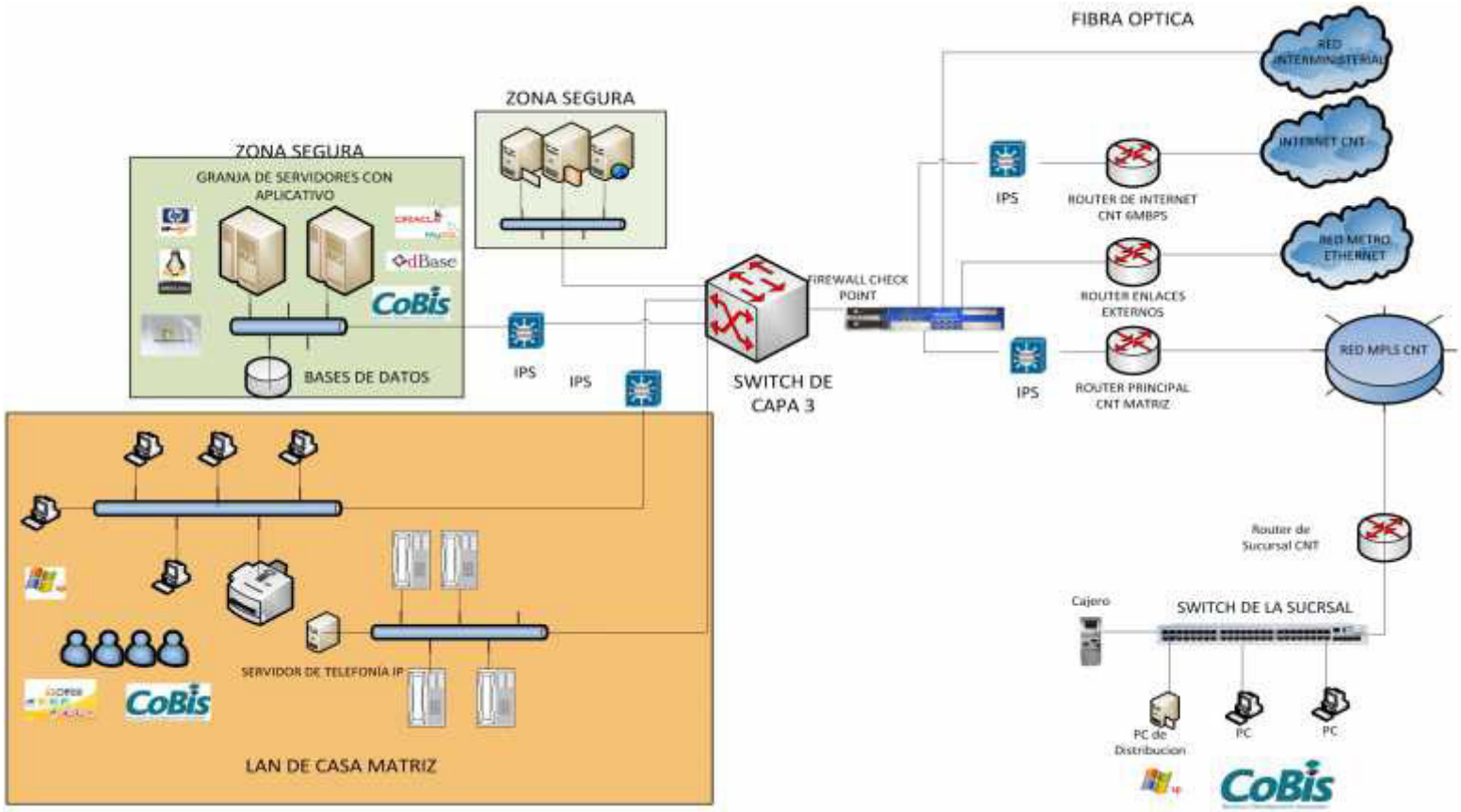

Figura 1 Diagrama de Red del BNF

1.6.3 Equipo

Talento humano: Alan Michael Espinoza Bucheli,
David Armando Montoya Tapia

Personal Administrativo e Informático del Banco Nacional de Fomento Matriz-Quito, además se necesitará la ayuda primordial de los directivos principales del Banco Nacional de Fomento para determinar los aspectos necesarios que se utilizarán para el escaneo de la red asi como su colaboración para acceder a la entidad y sus respectivos pisos donde se realice el escaneo.

1.6.4 Destinatarios

Esta investigación esta direccionada específicamente a los usuarios del Edificio Santa Prisca donde funciona la Casa Matriz del Banco Nacional de Fomento, mismos que serán beneficiarios directamente con esta investigación para su mejora en el manejo de los sistemas de seguridad informática.

También serán beneficiados de manera indirecta los clientes del banco ofreciéndoles una mayor seguridad en sus transacciones bancarias.

1.7 Factibilidad del proyecto

1.7.1 Factibilidad Técnica

En lo que se refiere a la parte de tecnología para la realización del presente plan de tesis es importante identificar cuáles son los recursos necesarios para alcanzar el objetivo planteado:

1.7.1.1 Requerimientos de hardware

Los requerimientos mínimos de hardware que deben tener los equipos a ser escaneados son:

- Procesador Intel Pentium IV o superior.
- Memoria Ram de 512 Mb ó superior.
- Disco Duro de 40 Gb o superior.
- Tarjeta de Video, Sonido.

Se utilizará dos computadoras desde las cuales se realizará el escaneo respectivo con las herramientas que se definen más adelante del presente proyecto, a su vez deben tener las siguientes características:

Computador 1

Especificaciones Técnicas

Fabricante:	HP
Modelo:	HP Compaq 6000 Pro Small Form Factor
Procesador:	Intel® Core ™ 2 Quad CPU 2.66 GHz
Memoria RAM:	2.00 GB
Tipo de Sistema:	Sistema operativo de 32 bits
Disco Duro:	320 GB
Ofimática:	Office 2010, Adobe Professional 6.0, Izarc, FileZilla
Antivirus:	Symantec EndPoint Protection / Clientes Completos
Monitor:	LCD Flat Panel 17''
Teclado:	101 Teclas Extendido en Español
Mouse:	Óptico de dos botones y botón de desplazamiento para Internet
IP:	172.16.5.82

Computador 2

Especificaciones Técnicas

Fabricante:	Dell
Modelo:	Optiplex 780
Procesador:	Intel® Core ™ 2 Duo E8400 2.99 GHz
Memoria RAM:	2.00 GB
Tipo de Sistema:	Sistema operativo de 32 bits
Disco Duro:	250 GB
Ofimática:	Office 2010, Adobe Professional 9.0, Izarc, FileZilla
Antivirus:	Symantec EndPoint Protection / Clientes Completos
Monitor:	LCD Flat Panel 17''
Teclado:	101 Teclas Extendido en Español
Mouse:	Óptico de dos botones y botón de desplazamiento para Internet
IP:	172.16.5.103

1.7.1.2 Requerimientos de software

Los requerimientos mínimos de Software de los equipos a ser escaneados son:

- Sistema Operativo Windows.

Además del sistema operativo para la realización del diagnóstico de redes, se tomará en cuenta las consideraciones y herramientas de software necesarias para el cumplimiento del presente proyecto.

Las Herramientas a utilizar para el diagnóstico de la red serán las siguientes:

i. Network Inventory Advisor
ii. Network Scanning
    - Angry IP

iii. Port Scanning
   - Nmap

iv. Vulnerability Scanning
   - Lannetscan -GFI LANGuard 2011

1.7.2 Factibilidad Económica y Financiera

1.7.2.1 Suministros de oficina

Tabla 1
Suministros de Oficina

Detalle	Cantidad	Precio unitario	Costo total
Papel Bond	1200	0.03	**$36,00**
Cartuchos (Impresora)	3 negro 3 color	30	**$180,00**
Varios			**$50,00**
		SUBTOTAL	**$286,00**

1.7.2.2 Software

Tabla 2
Software

Detalle	Cantidad	Precio unitario	Costo total
Internet	240 horas	1	**$240,00**
Herramientas	4	Software Libre y de prueba	**$0,00**
		SUBTOTAL	**$240,00**

1.7.2.3 Hardware

Tabla 3
Hardware

Detalle	Cantidad	Precio unitario	Costo total
COMPUTADOR	2	800	**$1.600,00**
Impresora	1	160	**$160,00**
		SUBTOTAL	**$1.760,00**

1.7.2.4 Talento Humano

Tabla 4
Talento Humano

Detalle	Cantidad	Precio unitario	Costo total
Personal Operativo	2	600 x 12 meses	**$14.400,00**
		SUBTOTAL	**$14.400,00**
Total general	$16.686,00		

1.7.3 Factibilidad Operativa

El Banco Nacional de Fomento proporciona a los implicados en este proyecto de Tesis la factibilidad operativa para colaborar en su desarrollo dando las facilidades necesarias para que los Sres. Alan Espinoza y David Montoya puedan ingresar en horas laborables a la institución y así, realizar un diagnóstico de vulnerabilidades de la red del BNF, siendo así que podrán utilizar las instalaciones y sus equipos para su correcto desarrollo.

Para certificar lo antes mencionado se tiene como respaldo y constancia la respectiva carta de auspicio entregado por el BNF a los Sres. integrantes del presente proyecto.

MARCO TEÓRICO

2.1 Antecedentes

Grupos de personas y organizaciones algunos de tipo “underground” están en la búsqueda de vulnerabilidades en sistemas operativos y aplicaciones informáticas, las vulnerabilidades son reportadas por estas personas y a diario ellos exponen a grandes riesgos los sistemas afectados por esas amenazas, no importa el segmento de mercado a la que pertenezca la organización afectada.

Es impresionante el crecimiento de vulnerabilidades encontradas en redes, sistemas y plataformas, dando como resultado que las organizaciones grandes o pequeñas, tengan que recurir a un analisis frecuente de vulnerabilidades que puedan afectar la infraestructura tecnológica existenete. Como resultado, es imprescindible que toda organización intente satisfacer sus necesidades de manera mas segura posible.

En el Edificio Santa Prisca se estima la existencia de 700 equipos, entre los que se encuentran PC de Escritorio o Desktops y PC Portátiles o Laptops, perteneciente a los funcionarios de la Institución.

Los equipos con los que cuenta el Banco Nacional de Fomento, son de distintos modelos con varias especificaciones técnicas, que incluyen desde equipos con procesadores Pentium III hasta Core i5, además del Software Base de la Institución el cual incluye:

Sistema Operativo:	Windows XP Service Park 3 / WIN 7 PRO
Antivirus:	Symantec EndPoint Protection
PDF:	Adobe Professional 6.0
FTP:	FileZilla
Compresor:	IZArc
Ofimática:	Microsoft Office 2007 Standart Edition

Actualmente las amenazas informáticas son enfocadas cada vez más en las personas y en los propios sistemas de la Institución, ya que se ha demostrado que son las características de nuestras redes y nuestros sistemas, los que hacen más vulnerables o no, a los incidentes de seguridad, siendo esto una realidad muy común hoy en día.

Una vulnerabilidad se presenta cuando un atacante descubre una falla en la planificación, implementación y configuración de un software o sistema operativo, y ésta es usada para violar la seguridad de un computador o de un sistema computacional.

Varias de estas vulnerabilidades pueden ser detectadas a través de la aplicación de un análisis de vulnerabilidad, el cual proporciona una vista del estado y seguridad de la red y sistemas computacionales, con el cual se obtiene como resultado un informe con las contramedidas a seguir para eliminar o reducir el punto de falla detectado, en el siguiente capítulo se muestra las diferentes contramedidas que se deben aplicar en la Institución que es el objeto de este estudio.

Un requerimiento primordial para un correcto análisis de vulnerabilidad es la capacidad de manipulación y obtención de datos e información actual, confiable y verificable de la Institución donde se aplicará la metodología.

El análisis de vulnerabilidades incluye:

- Escaneo de la red en el Banco de Fomento casa Matriz, para detectar puertos abiertos, cerrados y filtrados.
- Escaneo de las vulnerabilidades en todos los computadores o estaciones de trabajo que se encuentren conectadas a la red, asi como sus aplicaciones.
- Una vez que se realice el análisis de vulnerabilidades se presentarán los resultados obtenidos, para así determinar las respectivas contramedidas a ser tomadas en cuenta por las autoridades del BNF para tomar las respectivas acciones que el caso lo amerite.

Para el análisis de vulnerabilidades existen muchas herramientas tanto de código abierto como de código propietario. (Universidad Tecnológica de Panamá, 2014)

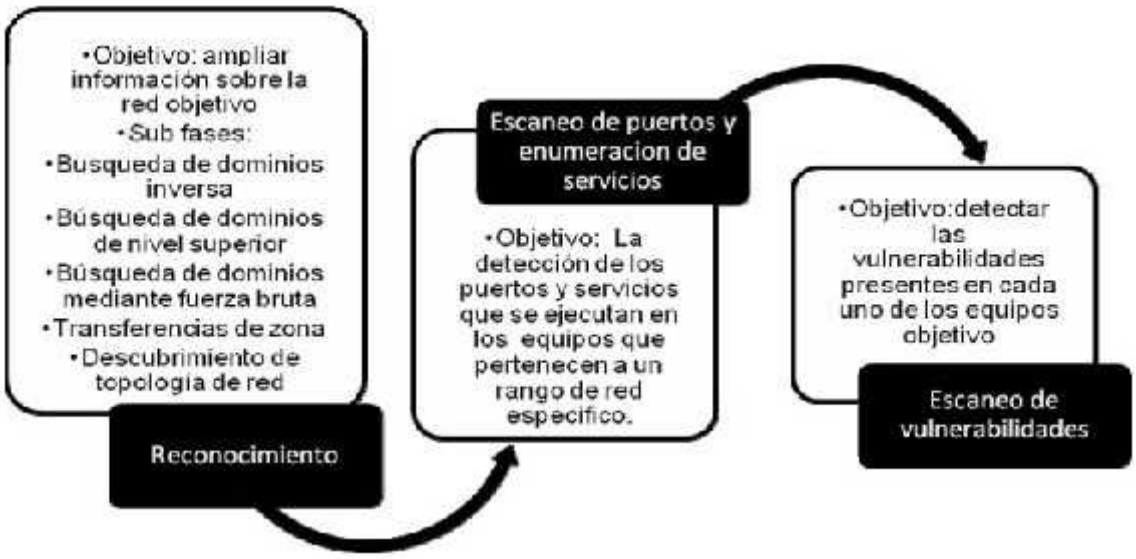

Figura 2 Esquema de la metodología para la detección de vulnerabilidades en redes de datos.
Fuente: (Franco, Perea, & Puello, 2015)

2.2 Protocolo IP

El protocolo IP (Internet Protocol) se caracteriza por ser una base primordial del Internet, identificado por llevar sus datagramas desde la fuente al destino, su nivel en la transportación de datos se inicia en el flujo de datos en datagramas que se transmite durante esta transmisión, además un datagrama puede dividirse en fragmentos que se montan nuevamente en el destino, como se puede apreciar en el Anexo I. (Universidad de Málaga, 2001)

2.2.1 Tipos de direcciones IP

2.2.1.1 Según el ámbito:

- Direcciones IP públicas.
- Direcciones IP privadas (reservadas).

2.2.1.2 Según la asignación:

- Direcciones IP estáticas (fijas).
- Direcciones IP dinámicas.

2.3 Protocolo TCP

TCP (Transmision Control Protocol) es relacionado como el protocolo mas complejo en comparación a los demás, ya que tiene como una de sus características principales que se trata de un protocolo que es orientado y vinculado siempre a conexión, esto implica que tiene consecuencias en dichas conexiones asi como: crear conexiones virtuales que se realizan por medio de sockets, los cuales permanecen activos durante toda la conexión; además es una consecuencia que se presenta se da cuando los datos se envían de forma ordenados; asi mismo esto indica un constante control de flujo de datos que viene a ser determinante el momento de descongestionar el ancho de banda del cual dispone una red, tal como se muestra en el Anexo I, para su mejor entendimiento. Bazuca. (2009). Familia de protocolos. 15 de noviembre de 2015, de Teleprocesos Sitio web:
http://rosalbauzteleprocesos.blogspot.com/

2.4 Protocolo UDP

El Protocolo de Datagramas de Usuario (UDP: User Datagram Protocol) se interpreta con la finalidad de hacer disponible la comunicación de datagramas,

intercambiando paquetes entre ordenadores dentro de un entorno de red o un conjunto interconectado de computadoras en red. (Postel; 1980, p. 10)

Los protocolos de rutas gestionan el direccionamiento de los datos y determinan el mejor medio de llegar al destino. También pueden gestionar la forma en que se dividen los mensajes extensos y se vuelven a unir en el destino. (Postel; 1980, p. 15)

Este protocolo asume que el Protocolo de Internet IP, es utilizado como un protocolo subyacente, de igual forma a este protocolo se le contribuye un procedimiento especial para que ciertos programas de aplicación puedan enviar mensajes a diferentes programas contando un mínimo de mecanismo del protocolo. Este protocolo es también orientado a transacciones, es decir, no garantiza ni la entrega ni la protección ante duplicados como se aprecia en el Anexo I. (Postel; 1980, p. 20)

Las aplicaciones que requieran de una entrega fiable y ordenada de secuencias de datos deberían utilizar el Protocolo de Control de Transmisión las cuales pueden ser observadas en el Anexo I. (Postel; 1980, p. 22)

2.5 Protocolo ICMP

2.5.1 Gestión de errores

ICMP (Protocolo de mensajes de control de Internet) se presenta como aquel que permite administrar información que está relacionada con errores de los equipos en la red, teniendo en cuenta los pocos controles que realiza el protocolo IP, ICMP no permite corregir los errores,permite notificarlos a otros protocolos de capas cercanas, tal como se muestra en el Anexo I. Es así que, el protocolo ICMP viene a ser utilizado por los routers para comunicar un error. (J. Postel - RFC 792-ISI, 1981), (Kioskea, 2015)

2.6 Vulnerabilidades.

2.6.1 Vulnerabilidad: definición y clasificación

Una vulnerabilidad se define como una debilidad de cualquier tipo misma que puede comprometer la seguridad de los sistemas informáticos y compromete su infraestructura,mismas que puden ser agrupadas en función de:
(Mifsud, MONOGRÁFICO: Introducción a las seguridad informática-Vulnerabilidades de un sistema informático, 2012)

2.6.1.1 Diseño

- Debilidad en el diseño ode los protocolos que son utilizados en la infraestructura de redes.
- Políticas de seguridad, mal establecidas por lo que llegan a ser deficientes y por lo tant inexistentes.

(Mifsud, MONOGRÁFICO: Introducción a las seguridad informática-Vulnerabilidades de un sistema informático, 2012)

2.6.1.2 Implementación

- Errores en el desarrollo de aplicaciones.
- Aparecimiento de “puertas traseras” dentro de los sistemas de carácter informáticos.
- Negligencia de los fabricantes.

(Mifsud, MONOGRÁFICO: Introducción a las seguridad informática-Vulnerabilidades de un sistema informático, 2012)

2.6.1.3 Uso

- Cuando existe una mala configuración en sistemas informáticos.

- Inexperiencia y falta de concientización de los usuarios y de los responsables de las áreas de seguridad informática.
- Disponibilidad de distintas herramientas que permiten ataques facilmente.
- Limitaciones de carácter gubernamental en procesos de seguridad tecnológica.

(Mifsud, MONOGRÁFICO: Introducción a las seguridad informática-Vulnerabilidades de un sistema informático, 2012)

2.6.1.4 Vulnerabilidad del día cero

Se establecen como las vulnerabilidades para las que no existe una solución determinada y sin conocerla, a su vez se sabe cómo explotarla. (Mifsud, OBSERVATORIO TECNOLOGICO GOBIERNO DE ESPAÑA, 2012)

Las características de las vulnerabilidades son definidas en base a varios factores que influyen en el nivel de criticidad que presentan como se muestra en el Anexo I. (Mifsud, OBSERVATORIO TECNOLOGICO GOBIERNO DE ESPAÑA, 2012)

2.7 Análisis de vulnerabilidades

"El análisis de vulnerabilidades se ha convertido en un requisito indispensable dentro del proceso de gestión de riesgos y es clave dentro del sistema de gestión de la seguridad de la información."

En la actualidad las empresas se encuentran en un mundo interconectado, todas estas tienen comunicaciones relacionadas a móviles, sucursales, clientes, proveedores, etc., lo cual genera serios riesgos de seguridad.

Las siguientes son preguntas frecuentes que cada entidad debe tomar en cuenta para mejorar la seguridad informática:

- ¿Cómo se identifica en los activos de la red, cual es configuración que tienen respecto a software, servicios, puertos abiertos, etc.?
- ¿Cómo se puede conocer las vulnerabilidades que poseen los activos de una red?
- ¿Cómo se puede categorizar y remediar vulnerabilidades encontradas en los activos de una red?
- ¿Cómo se garantiza el cumplimiento de regulaciones o auditorias enfocado al estado de vulnerabilidades de una red?

Actualmente la Seguridad de la Información se enfrenta a diversos retos, asi como, virus gusanos en internet, ataques en negación de servicios, virus en general, distintos tipos de intrusiones además de nuevos y sofisticados ataques informáticos que se generan a diario. Incluso, el aumento de las vulnerabilidades descubiertas, y la velocidad en la que son creadas estas nuevas amenazas se convierte en un mayor reto. Es importante que la medición y gestión de riesgos de una red sea un desafío para todas empresas.

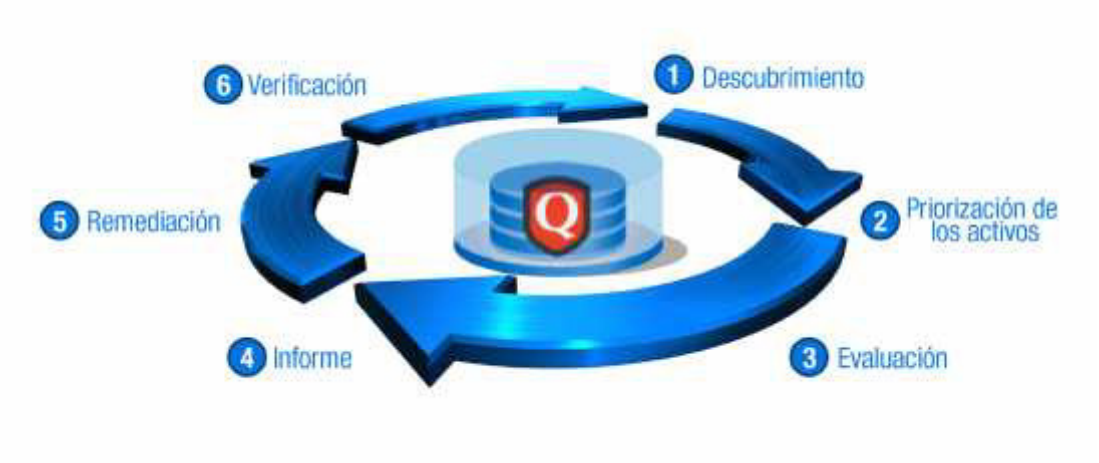

Figura 3 Análisis de Vulnerabilidades

2.8 Fases para el análisis de vulnerabilidades

- ***Fase uno:*** *Conozca sus activos.*
- ***Fase dos:*** *Clasificar sus activos.*

- ***Fase tres:*** *Crear un análisis básico de todos sus bienes.*
- ***Fase cuatro:*** *Realizar una prueba de penetración en ciertos activos.*
- ***Fase cinco:*** *Remediar las vulnerabilidades y riesgos.*
- ***Fase seis:*** *Crear una evaluación de vulnerabilidades (VA) horario.*
- ***Fase siete:*** *Crear un parche y el proceso de cambio de gestión.*
- ***Fase ocho:*** *Monitorear los nuevos riesgos para los activos.*

Cada una de las fases que sean implementadas para el análisis de vulnerabilidades son enfocadas y desarrolladas según la profundidad y priorización que sea necesario tal como se muestra en el Anexo II.

2.8.1 Fase uno: Conozca sus activos

Tabla 5
Actividades. Documente la hora de identificar los activos

Dirección IP del activo	Incluso si su organización utiliza direcciones IP asignadas dinámicamente (DHCP), no se puede analizar un sistema si no conoce la dirección IP. Además, el seguimiento de la dirección IP que se le asigna un sistema deja un rastro de auditoría buena en el caso de que un incidente debe ser investigado.
Dirección MAC del activo	Esta es la dirección física del sistema. Este es un estático 12-carácter de valor, por ejemplo, *00-0E-35-E9-98-A6-que* le permitirá asignar sistemas físicos a la dirección IP asignada.
DNS / NetBIOS Nombre del activo	Este es el nombre del sistema, normalmente el sistema de nombres de dominio (DNS) y el nombre NetBIOS será el mismo. Esta es una forma más de la estructura del sistema para la dirección IP y la dirección de Media Access Control (MAC).
Sistema operativo del activo	Aunque obvio, esto es importante para el proceso de gestión de parches. Si usted no sabe lo que sus sistemas están funcionando, es difícil, si no imposible, saber qué vulnerabilidades para monitorear y planificar las etapas de parches
Escuchando servicios	Aquel activo de los más antiguos conceptos de seguridad de la información es el de menor privilegio. Los sistemas no deberían tener servicios de escucha a los que no se están utilizando. Documentar lo que se escucha en cada sistema y lo que se necesita en cada sistema es un paso crítico.
Ubicación física del activo	Esta es la ubicación física y el departamento del activo. Esto es algo obvio del documento, ya que de vez en cuando, los recursos de TI pueden tener que acceder físicamente al sistema.
Dueño del activo	Hay dos puntos de datos para esta categoría. Usted debe saber que tanto el usuario típico del sistema, así como los que en la organización es el responsable último de ese activo, tanto de TI y un nivel de gestión.
Clasificación de los activos	Esta es la clasificación de los activos y los datos contenidos en dicho activo. Además, este es un paso importante en el proceso de gestión de vulnerabilidades entero

2.8.2 Fase dos: Clasificar sus activos

Durante esta etapa, se ordenará todos los sistemas detectados en la fase uno, para categorizarla, mismas que son basadas en la localización, importancia y criticidad entendiendose por cuan vulnerable puede ser. Puede ser útil para clasificar cada grupo de la siguiente manera:

- Ubicación geográfica 1/ Confidencial
- Ubicación geográfica 2/ Confidencial
- Ubicación geográfica 3/ Confidencial
- Localización geográfica 1/ Sólo Interno
- Localización geográfica 2/ Sólo Interno
- Localización geográfica 3/ Sólo Interno
- Localización geográfica 1/ Sin clasificar
- Localización geográfica 2/ Sin clasificar
- Localización geográfica 3/ Sin clasificar

2.8.3 Fase tres: Crear una línea de base de los activos de exploración

Una vez realizados los escaneos se debe revisar la configuración de la herramienta, asegurándose de los siguientes aspectos:

- Habilitación de un completo escaneo de puertos orientados a los protocolos TCP y UDP.
- Activaciones para la detección del sistema operativo.
- Posiblilidad de comprobación de todas las vulnerabilidades.

2.8.4 Fase cuatro: Realizar una prueba de penetración de determinados activos

Para realizar su prueba de lápiz tendrá que asegurarse de cubrir las siguientes actividades:

a) Perfil sistemas externos
b) Perfil aplicaciones externas
c) Identificar posibles debilidades arquitectónicas
d) Identificar posibles vulnerabilidades explotables
e) Explotar las debilidades y vulnerabilidades
f) Informe

En el perfil de los sistemas externos que serán documentado todo aquello que se prestará al público sobre la red dirigida al exterior, incluyendo puertos abiertos, registros DNS y registros de nombres de dominio.

2.8.5 Fase cinco: Remediar Vulnerabilidades y Riesgo

Estas son las actividades que se deberían seguir para el desarrollo de esta fase:

a) Crear un muestreo preciso de sus activos.
b) Análisis de todos los parches y los problemas de configuración en su muestreo.
c) Documentar los resultados y el documento aceptado el riesgo de cierre de sesión.
d) Continuamiento de los parches y cambios de configuración.
e) Repita la fase tres para validar despliegue.

2.8.6 Fase seis: Crear un programa de evaluaciones de vulnerabilidad

Tabla 6
Programa de muestra para la aplicación de evaluaciones de vulnerabilidad

Gatillo de lectura	Qué analizar	Al escanear	¿Qué para buscar
Proveedor libera un parche, o algún otro evento provoca cambios a gran escala	Grupos de activos no clasificados	Inmediatamente después de los análisis internos Sólo grupo de activos están completos, y de nuevo tras la rectificación completa	Analizar en busca de los proveedores liberados por parches o cuestiones que aborda el parche. Si un cambio a gran escala es el disparador, buscar todas las vulnerabilidades relacionadas con el cambio.
Una nueva amenaza se hace evidente	Grupos confidencial es de activos	Inmediatamente después del evento de disparo, y de nuevo tras la rectificación se ha completado	Analizar los sistemas operativos, aplicaciones o configuraciones que están relacionados con la nueva amenaza.
Una nueva amenaza se hace evidente	Grupos Internos único activo	Inmediatamente después de Activos Confidencial Exploraciones del Grupo están completos, y de nuevo después de la recuperación se completa	Analizar los sistemas operativos, aplicaciones o configuraciones que están relacionados con la nueva amenaza.
Una nueva amenaza se hace evidente	Grupos de activos no clasificados	Inmediatamente después de los análisis internos Sólo grupo de activos están completos, y de nuevo después de la recuperación se ha completado	Analizar los sistemas operativos, aplicaciones o configuraciones que están relacionados con la nueva amenaza.

2.8.7 Fase siete: Crear un Proceso de administración de revisiones y cambio

Se debe seguir las siguientes actividades:

a) Crear un grupo de estudio en el que se presenta una muestra de los activos de la red.
b) Documentar todo cambio propuesto con su detalle.
c) Documentar un plan de "roll-back" para deshacer el cambio de ser necesario.
d) Obtener el cierre de sesión de los propietarios de activos en el cambio planificado.
e) Implementar dicho cambio en un grupo de prueba.
f) Monitorear los efectos adversos.
g) Actualizar la información de la empresa si el grupo de prueba es exitoso.

h) Deshacer el cambio si el grupo de prueba no tiene éxito.

i) Iniciar la fase 6.

2.8.8 Fase ocho: Monitor de nuevos riesgos para los activos

La siguiente es una lista de cosas que se necesita para que su personal de seguridad de TI tome en cuenta de manera constante.

- Liberados del proveedor parches
- Debilidades de configuración
- 0 comunicados de vulnerabilidad del día
- Ataques a gran escala

2.9 Técnica de escaneo (Scanning)

El escaneo en red se define como un procedimiento para identificar los activos en una red, ya sea con el propósito de atacarlos o para que la empresa avalue el nivel de seguridad de la red. Además se sabe que algunos procedimientos de escaneo, tales como barridos de ping y escaneo de puertos, han sido utilizados para encontrar información acerca de las direcciones IP, mapas de los hosts en la red que están activos y qué servicios están ofreciendo. Otro método utilizado para un análisis es el llamado mapeo inverso, es decir que devuelven información sobre las direcciones IP, lo que permite a un atacante realizar suposiciones acerca de las direcciones viables de supuestos ataques.

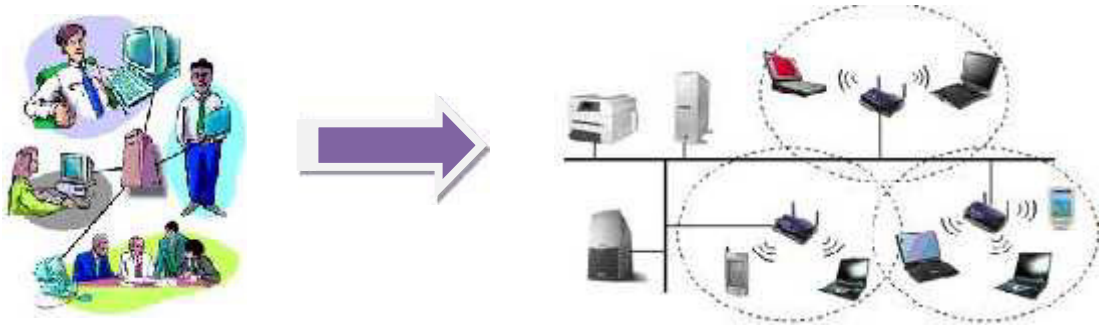

Figura 4 Escaneo de Red

La navegación ha sido ultimamente uno de los principales componentes para ejecutar la recolección de información que utilizanlos atacantes, de este modo el mismo que viene a crear un perfil dentro de la organización de manera falsa, con información del sistema de nombres del dominio (DNS) y servidores de correo electrónico donde se encuentra su rango de IPs. En la mayoría de los casos esta información se encuentra disponible en línea, obteniendo información sobre las direcciones IP específicas a las que se puede acceder simplemente a través de Internet, asi como también sus sistemas operativos, arquitectura, y los servicios que cada equipo ejecuta, para ello, el atacante recopila alguna información del usuario que está en red, nombres de grupos, tablas enrutadas y Simple Network Management Protocol (SNMP de datos).

2.9.1 Network Scanning

El escaneo de red sirve para detectar los puertos que están abiertos, utilizando las herramientas que son utilizadas por los intrusos, se analiza al detalle algunos de los sistemas que están conectados en una misma red local dentro de los rangos de direcciones IP que sean especificadas, identificando la IP, dirección MAC y velocidad de respuesta al ping, además se puede controlar los puertos TCP y los servicios SNMP.

En cierta forma se escanea los siguientes aspectos:

- Escaneo de Vulnerabilidades de Aplicaciones.
- Análisis de cada dirección IP en su red.
- Validación manual del resultado del escaneo para eliminar los resultados que son "Falsos Positivos".
- Examinación manual del contexto de la información y contenido para determinar si el resultado es apropiado para su distribución pública.
- Entrega de un reporte de Análisis de Vulnerabilidades detallado con recomendaciones y acciones (parches/service packs) para solucionar cada vulnerabilidad.

Este tipo de escaneo es de uso general y también es usado para encontrar vulnerabilidades potenciales dentro de la red en una empresa, (también se podría incluir a los escáneres de redes VoIP)

2.9.2 Port Scanning

Una actividad realizada por Port scanning es la verificación de servidores en busca de puertas vulnerables para la posterior invasión malintencionada al sistema.

El término escáner de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por cortafuegos.

Se utiliza para también para detectar a qué servicios, los mas comunesuna máquina tiene y sus posibles vulnerabilidades de seguridad tomando en cuenta los puertos abiertos. También se puede llegar a detectar qué sistema operativo está siendo ejecutadosegún estos puertos. Además puede ser usado por los administradores de sistemas para analizar posibles problemas en la seguridad, utilizado también por usuarios malintencionados que pretenden comprometer la seguridad del equipo o de la red.

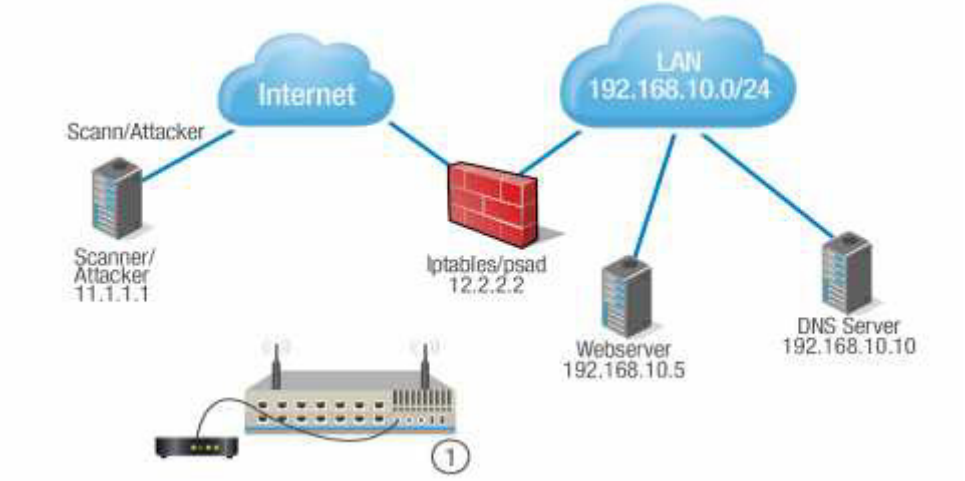

Figura 5 Port Scanning

Existen varios programas para el escaneo de puertos por la red. Uno de los más conocidos es Nmap, disponible tanto para Linux como Windows.

El escaneo de puertos es también usado simplemente para detección de hosts activos e incluso determinar qué tipo cortafuegos, sistema, etc., existe con un determinado host y para indagar si este tiene algún servidor de correo, y mas.

Se pueden escanear puertos TCP, explorar mediante envió de paquetes UDP, etc.

2.9.3 Vulnerability Scanning

En un escaneo de vulnerabilidades puede ser utilizado para llevar a cabo un simple reconocimiento de red, que normalmente se lo realiza por un atacante de manera remota que trata de obtener información o acceder a una red en la que no esté autorizada. Este reconocimiento de red es cada vez más significativo para beneficiarse de los estándares de red y los respectivos métodos automatizados de comunicación. Su objetivo es establecer qué tipos de equipos informáticos están presentes, junto con información adicional acerca de ellos, tales como el tipo y la versión del sistema operativo. Esta información puede ser analizada en busca de vulnerabilidades conocidas o recientemente descubiertas que pueden ser explotadas para acceder a redes

seguras y a las computadoras mismas. Una técnica de TCP como huella dactilar pasiva viene a ser uy ineficaz si se habla de seguridad. Hoy en día, existen numerosas herramientas para hacer el reconocimiento más fácil y eficaz.

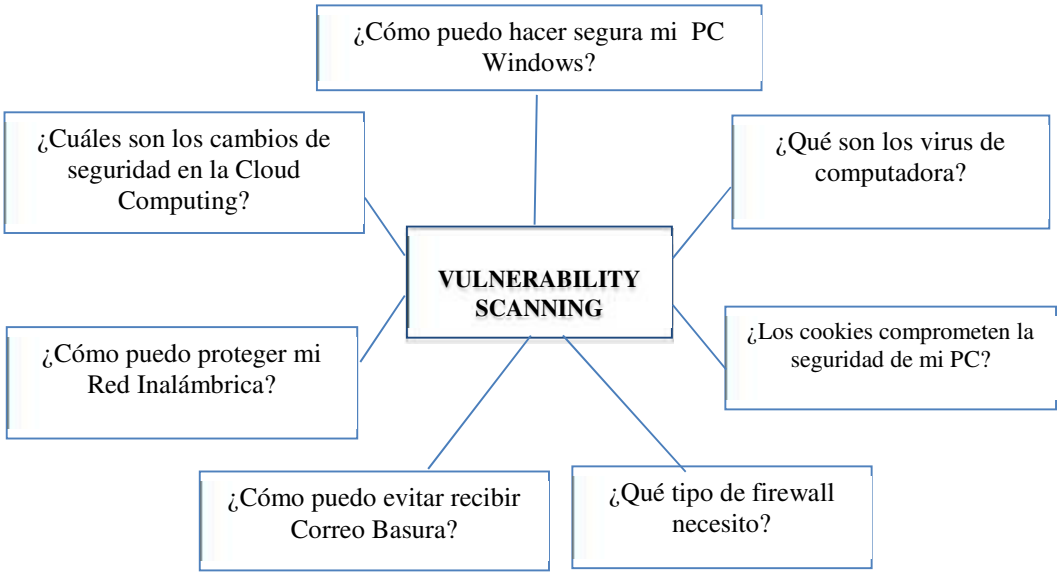

Figura 6 Vulnerability Scanning

El Análisis de vulnerabilidad utiliza un software que se encarga de buscar las fallas de seguridad basadas en una base de datos de fallas conocidas, pruebas de los sistemas en donde ocurren regularmente estas fallas y para generar informes de hallazgos que un individuo o empresa pueden utilizar para reforzar la seguridad de redes.

Además típicamente se representa a la digitalización de los sistemas que están conectados a Internet, pero también puede referirse a las auditorías de sistemas de redes internas, mismas que al no estar conectadas a Internet evalúan la amenaza de software maliciosos o empleados malintencionados en una empresa.

Por lo tanto, el Escaneo de vulnerabilidades se refiere a la automatización por medio de software especializado para la identificación de dichas fallas.

2.10 Tipos de escaneo

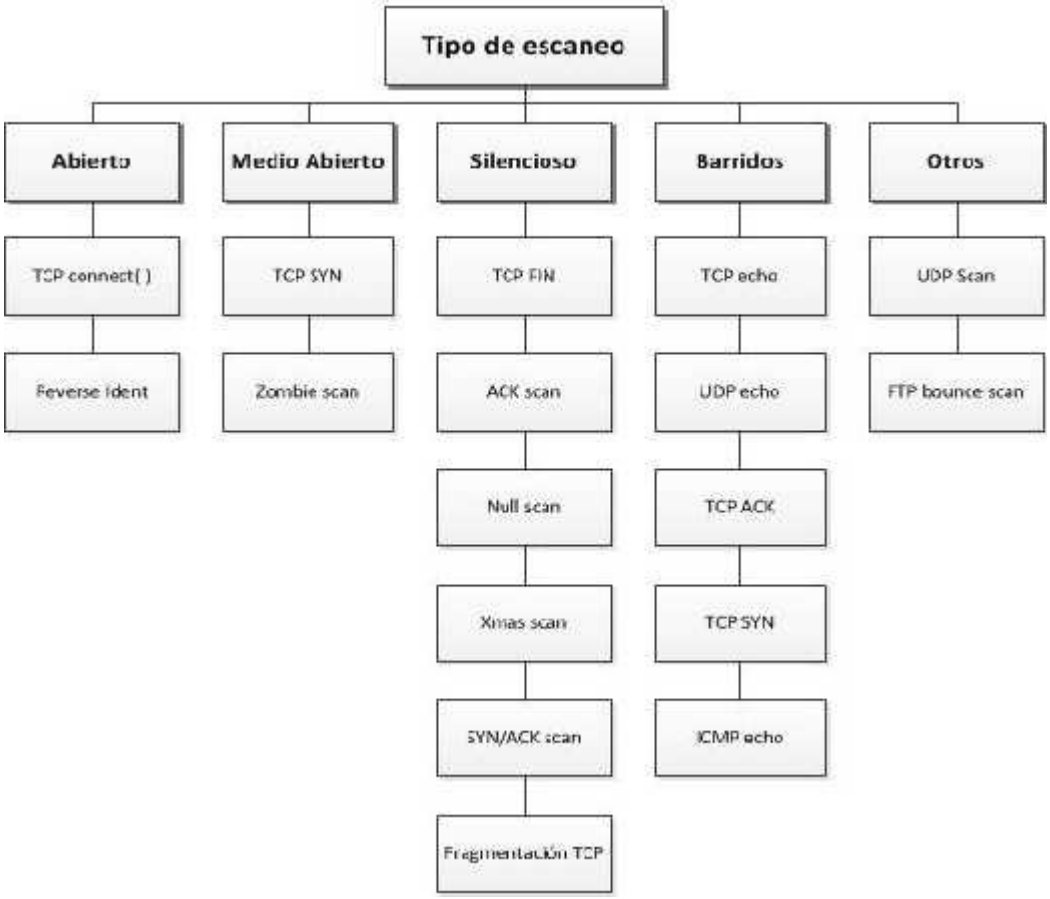

Figura 7 Tipos de Escaneo

Los tipos de escaneo descritos en el Diagrama 4 son detallados en el Anexo III

IMPLEMENTACION DEL ANÁLISIS

3.1 Metodología del análisis de vulnerabilidades

3.1.1 Identificación de vulnerabilidades

En este apartado se van a identificar todas las vulnerabilidades de la red, aplicando la técnica Scanning.

La técnica Scanning, o escaneo, se usa como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo.

La idea es recorrer (escanear) tantos puertos que respondan como sea posible y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. (Perez Salinas, 2012)

Escanear puertos implica las mismas técnicas de fuerza bruta, para implementar esta técnica, se envía una serie de paquetes para varios protocolos y se deduce que servicios están escuchando por las respuestas recibidas o no recibidas. (Esparza Morocho, 2013)

La mayor parte de las intrusiones o ataques a los sistemas que se producen actualmente se deben a la explotación de vulnerabilidades, por ello es de vital importancia poder identificar todas aquellas vulnerabilidades susceptibles de ser aprovechadas por una amenaza, para evitar que ésta llegue a materializarse. (Esparza Morocho, 2013)

Las vulnerabilidades pueden deberse a fallos de seguridad de la propia empresa o fallos de seguridad en los productos suministrados por terceras empresas, es decir proveedores de servicios a la Institución.

3.2 Implementación de las fases de un análisis de vulnerabilidades

3.2.1 Fase uno: Conozca sus activos

El edificio Santa Prisca, donde funciona la Casa Matriz y la Sucursal Quito del Banco Nacional de Fomento, posee alrededor de 700 equipos aproximadamente, por este motivo se utilizó el software Network Inventory Advisor, el cual provee toda la información necesaria que se debe levantar de los activos dentro de la red de la Institución.

Los reportes generados con Network Inventory Advisor muestran todas las VLANs de la red del Banco Nacional de Fomento, para este estudio se tomara como muestra las VLANs 2 y 10 por el impacto dentro de la Institución.

Los campos del reporte generado, para la aplicación de esta fase son los siguientes:

- Dueño
- Nombre / Host
- Dirección IP
- Dirección MAC
- Serial BIOS
- Marca
- Modelo
- Sistema Operativo
- Antivirus
- Ubicación

A continuación se muestra una parte del levantamiento de información de los activos de la VLANs 2 y 10, es decir los activos que funcionan en el Centro de Cómputo y la

Zonal Quito del Banco Nacional de Fomento respectivamente, la totalidad de la información del levantamiento de activos las Vlan 2 y 10 se los puede apreciar en el Anexo V.

3.2.1.1 Presentación de Resultados VLAN 2

Tabla 7
Levantamiento de activos de la VLAN 2

Tipo de Servidor	Dueño	Nombre	Dirección IP	Dirección MAC	Serial del BIOS	Marca	Modelo	Sistema Operativo	Antivirus
Virtual		uio001sma1	172.16.2.4			VMWare, Inc.	Linux uio001evi1 2.6.32-71.el6.x86_64 #1 SMP Wed Sep 1 01:33:01 EDT 2010 x86_64	Linux	Sin Antivirus
Físico	Windows User	UIO001LSE1	172.16.2.5	78:E7:D1:8F:7F:EE 78:E7:D1:8F:7F:F0 78:E7:D1:8F:7F:F2 78:E7:D1:8F:7F:F4	USE019N63F	HP	ProLiant DL380 G6	Microsoft® Windows Server® 2008 Standard	Symantec Endpoint Protection
Virtual		uio001sma2	172.16.2.6			VMWare, Inc.	Linux uio001sma2 2.6.18-92cp #1 SMP Wed May 25 15:04:00 IDT 2011 i686	Linux	Sin Antivirus
Físico	BNF	UIO001ADM1	172.16.2.13	00:1C:C4:6C:24:8A 00:1C:C4:6C:24:8C	USE804N1N8	HP	ProLiant DL380 G5	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	Symantec Endpoint Protection
Físico	BNF	UIO001FIL2	172.16.2.15	00:1E:0B:72:4F:CC	USE8048J93	HP	ProLiant BL460c G1	Microsoft® Windows Server® 2008 Enterprise	Symantec Endpoint Protection
Físico	Windows User	UIO001G4S1	172.16.2.16	90:B1:1C:05:4A:14	3SM7WV1	Dell Inc.	PowerEdge R720	Microsoft Windows Server 2008 R2 Standard	Symantec Endpoint Protection
Físico	BNF	UIO001WSU1	172.16.2.17	00:1E:0B:72:50:34 00:1E:0B:72:50:32	USE8048J95	HP	ProLiant BL460c G1	Microsoft Windows Server 2008 R2 Enterprise	Symantec Endpoint Protection

Continúa

Virtual	Windows User	UIO001BOX3	172.16.2.18	00:50:56:9E:3B:F9	VMware-42 1e 83 e4 64 97 81 82-1f 0c cc ba eb ee f8 86	VMWare, Inc.	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Enterprise	Symantec Endpoint Protection
Físico	Windows User	UIO001DC5	172.16.2.20	B4:B5:2F:70:C9:AC	USE246MJC1	HP	ProLiant BL460c Gen8	Microsoft Windows Server 2012 Standard	Symantec Endpoint Protection
Físico	Windows User	UIO001DC6	172.16.2.21	10:60:4B:AA:54:2C	USE246MJCC	HP	ProLiant BL460c Gen8	Microsoft Windows Server 2012 Standard	Symantec Endpoint Protection
Virtual	Windows User	UIO001BOX5	172.16.2.25	00:50:56:9E:17:8C	VMware-42 1e 1a b8 0a 9f c4 aa-10 20 ba 39 9a ae 5b 4d	VMware, Inc.	VMWare Virtual Platform	Microsoft Windows Server 2008 R2 Enterprise	Sin Antivirus
Físico	Administradores	UIO001NOM1	172.16.2.29	00:16:35:69:55:7E 00:16:35:69:55:7F	BRC616N0CT	HP	ProLiant DL380 G4	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	Symantec Endpoint Protection
Físico	Banco Nacional de Fomento	UIO001SD1	172.16.2.35	00:1E:0B:70:54:C8 00:1E:0B:70:54:C6	USE8048J96	HP	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	Symantec Endpoint Protection
Físico	Banco Nacional Fomento	UIO001BC1	172.16.2.36	00:21:5E:2F:FB:74 00:21:5E:2F:FB:72 00:21:5E:2F:FB:72	KQFXFBK	IBM	IBM eServer BladeCenter HS21 -[8853G6U]-	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	Symantec Endpoint Protection
Físico	Banco Nacional Fomento	UIO001WS1	172.16.2.37	00:1F:29:C9:C5:DC 00:1F:29:C9:C5:E0	USE829DC38	HP	ProLiant BL460c G1	Microsoft(R) Windows(R) Server 2003,	Symantec Endpoint Protection

Ver Anexo V

3.2.1.1.1 Sistemas Operativos existentes en la VLAN 2

Al finalizar la generación de Informes con la ayuda de Network Inventory Advisor, se puede presentar las siguientes estadísticas en base a toda la información recolectada.

Tabla 8
Sistemas Operativos en la VLAN 2

Sistema Operativos	Número de Activos
Linux	3
Microsoft Windows Server 2008 R2 Enterprise	20
Microsoft Windows Server 2008 R2 Standard	1
Microsoft Windows Server 2012 Standard	2
Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition	1
Microsoft(R) Windows(R) Server 2003, Enterprise Edition	39
Microsoft(R) Windows(R) Server 2003, Standard Edition	5
Microsoft® Windows Server® 2008 Enterprise	3
Microsoft® Windows Server® 2008 Standard	1
Total general	**75**

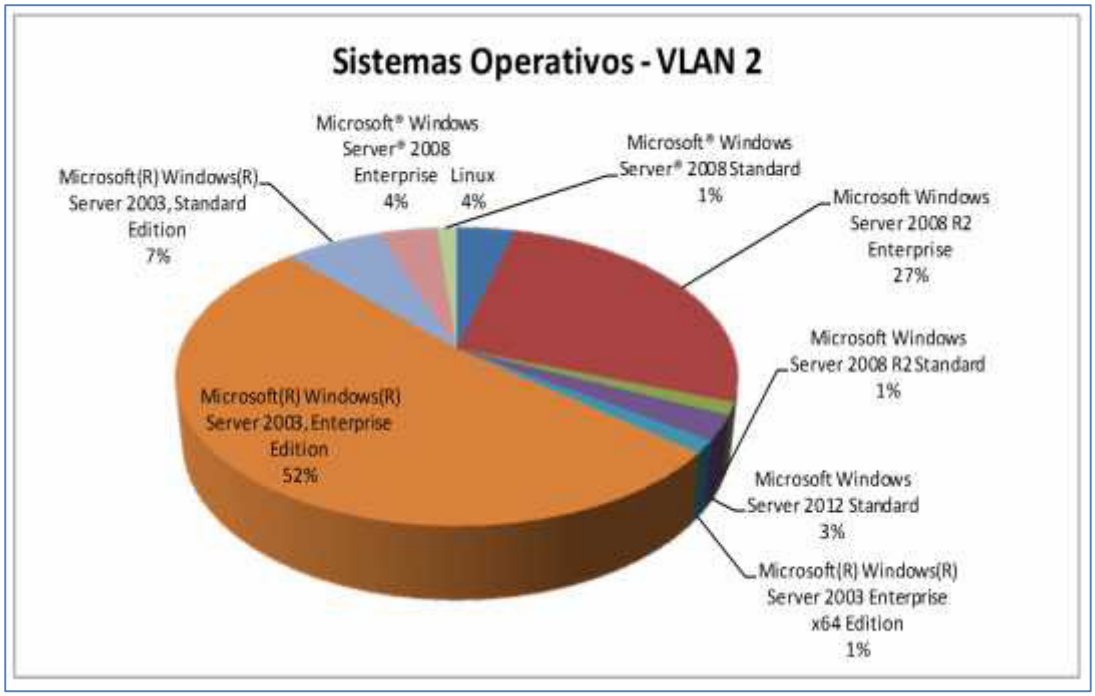

Figura 8 Sistemas Operativos en la VLAN 2

En la figura 4 se puede apreciar que existen 39 Servidores con Microsoft(R) Windows(R) Server 2003, Enterprise Edition, representando el 52% del total de los Servidores que forman parte de Centro de Computo del Banco Nacional de Fomento, los Sistemas Operativos, Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition, Microsoft Windows Server 2008 R2 Standard y Microsoft® Windows Server® 2008 Standard, representan el 3% de total de los Servidores levantados con un solo Servidor respectivamente.

3.2.1.1.2 Antivirus presentes en la VLAN 2

Tabla 9
Antivirus en la VLAN 2

Antivirus	Número de Activos
Sin Antivirus	8
Symantec Endpoint Protection	67
Total general	**75**

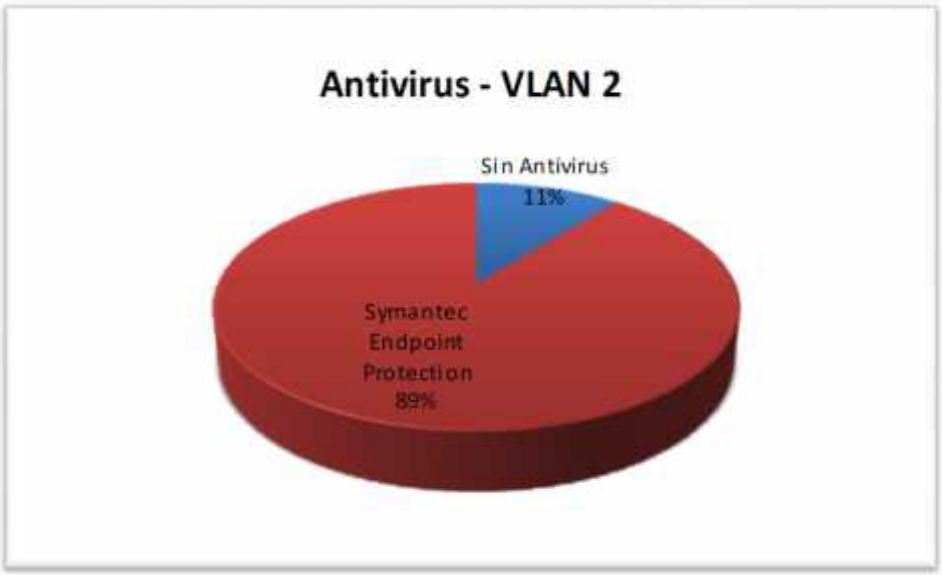

Figura 9 Antivirus en la VLAN 2

En la figura 5, se muestra un 89% de Servidores que tienen instalado el Antivirus Symantec Endpoint Protection y un 11% de Servidor no disponen de una solución Antivirus.

3.2.1.1.3 Marcas de Servidores

Tabla 10
Mapa de Servidores de la VLAN 2

Marca de Servidores	Número de Activos
Dell Inc.	2
HP	27
IBM	19
VMware, Inc.	27
Total general	**75**

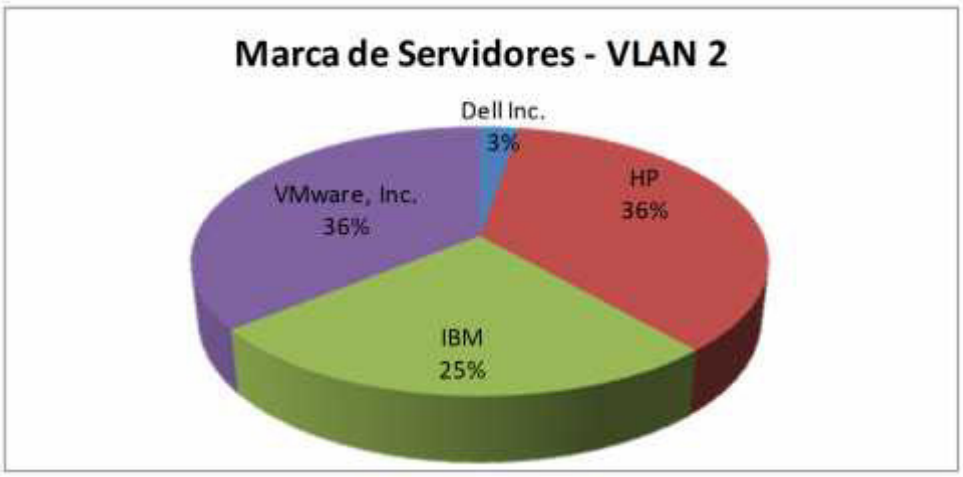

Figura 10 Mapa de Servidores de la VLAN 2

En la figura 6, se observa una presencia de Servidores de marca VMWare y Hewlett Packard con un 36%, un 25 % es representado por la marca IBM y finamente la marca Dell con un 3%.

3.2.1.1.4 Modelo de Servidores

Tabla 11
Modelos de Servidores de la VLAN 2

Modelo de Servidores	Número de Activos
IBM eServer BladeCenter HS21 -[8853G6U]-	19
Linux uio001evi1 2.6.32-71.el6.x86_64 #1 SMP	2
Linux uio001sma2 2.6.18-92cp #1 SMP	1
PowerEdge 2900	1
PowerEdge R720	1
ProLiant BL460c G1	7
ProLiant BL460c G7	8
ProLiant BL460c Gen8	2
ProLiant DL380 G4	1
ProLiant DL380 G5	8
ProLiant DL380 G6	1
VMware Virtual Platform	24
Total general	**75**

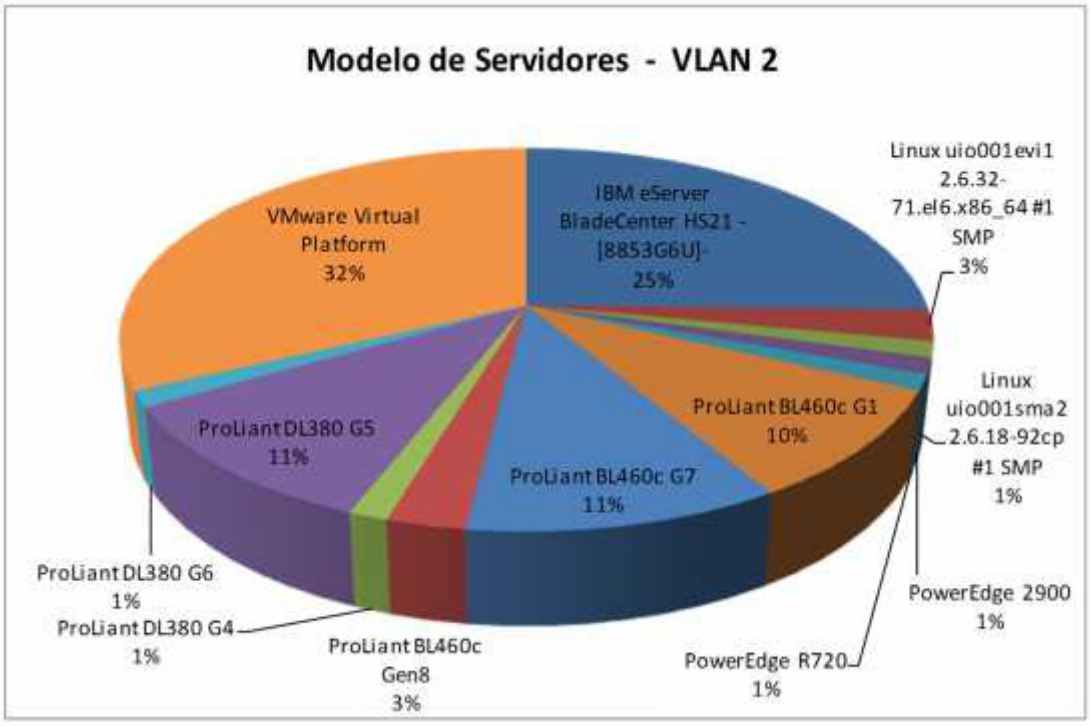

Figura 11 Modelos de Servidores de la VLAN 2

En la figura 7, se puede apreciar que el modelo VMware Virtual Platform ocupa el 32% del total de Servidores del Centro de Cómputo del BNF, el 25% es ocupado

por el modelo IBM sServer BladeCenter HS21 y con 1% se encuentran los modelos Linux, PowerEdge 2900, PowerEdge R720, ProLiant DL380 G6 y ProLiant DL380 G4.

3.2.1.1.5 Tipos de Servidores

Tabla 12
Tipos de Servidores de la VLAN 2

Tipos de Servidores	Número de Activos
Físico	48
Virtual	27
Total general	**75**

Figura 12 Tipos de Servidores de la VLAN 2

En la figura 8, se puede observar una existencia de Servidores Fisicos en un 64% y los Servidores Virtuales representan el 36% de todos los Servidores del Centro de Computo del Banco Nacional de Fomento.

3.2.1.2 Presentación de Resultados VLAN 10

Tabla 13
Levantamiento de activos de la VLAN 10

Tipo de Dispositivo	Dueño	Nombre	Dirección IP	Dirección MAC	Serial del BIOS	Marca	Modelo	Sistema Operativo	Antivirus
Impresora		NPI8C1804	172.16.10.15			Hewlett-Packard	HP Color LaserJet CM2320n MFP		
Impresora		Aficio 2035e	172.16.10.35			RICOH	RICOH Aficio 2035e		
Impresora		LD135	172.16.10.36			RICOH	LANIER LD135		
Impresora		Aficio MP 4000	172.16.10.39			RICOH	RICOH Aficio MP 4000		
Impresora		172.16.10.40	172.16.10.40			Digi Connect	Digi Connect ME		
Impresora		172.16.10.41	172.16.10.41			Digi Connect	Digi Connect ME		
Equipo de Escritorio	BNF	QTO0002QTO047	172.16.10.50		MXJ85000Z9	Hewlett-Packard	DSDT_PRJ	Microsoft Windows XP Professional	Symantec Endpoint Protection
Equipo de Escritorio	BNF	QTO0002QTO127	172.16.10.51	00:24:81:90:0E:B1	MXJ92101R8	Hewlett-Packard	HP Compaq dc5800 Small Form Factor	Microsoft Windows 7 Enterprise	Symantec Endpoint Protection
Equipo de Escritorio	BNF	QTO0001FBR410	172.16.10.53	00:1F:E2:00:51:36	OEM	OEM	OEM	Microsoft Windows 7 Enterprise	Symantec Endpoint Protection
Equipo de Escritorio	Bnf	QTO0002QTO150	172.16.10.55	B4:B5:2F:DC:1F:B9	MXL2470TN5	Hewlett-Packard	HP Compaq Pro 6300 SFF	Microsoft Windows 7 Enterprise	Symantec Endpoint Protection
Tipo de Dispositivo	**Dueño**	**Nombre**	**Dirección IP**	**Dirección MAC**	**Serial del BIOS**	**Marca**	**Modelo**	**Sistema Operativo**	**Antivirus**
Equipo de Escritorio	Javier	QTO0001FBR210	172.16.10.57	B4:B5:2F:D7:6B:53	MXL2470V10	Hewlett-Packard	HP Compaq Pro 6300 SFF	Microsoft Windows 7 Enterprise	Symantec Endpoint Protection

Continúa

Equipo de Escritorio	BNF	QTO0002QTO177	172.16.10.59	00:0F:FE:FC:39:1C	MXL0151M2P	Hewlett-Packard	HP Compaq 6000 Pro SFF PC	Microsoft Windows 7 Enterprise	Symantec Endpoint Protection
Equipo de Escritorio	Borrar	QTO0002QTO074	172.16.10.60	78:AC:C0:BF:A0:74	MXL11828PX	Hewlett-Packard	HP Compaq 8200 Elite SFF PC	Microsoft Windows 7 Enterprise	Symantec Endpoint Protection
Equipo de Escritorio	BNF	QTO0001CPC151	172.16.10.61	00:24:81:0F:CE:B8	MXJ9160583	Hewlett-Packard	HP Compaq dc5800 Small Form Factor	Microsoft Windows 7 Enterprise	Symantec Endpoint Protection
Equipo de Escritorio	BNF	QTO0001CLL001	172.16.10.62	08:2E:5F:1A:8B:64	MXL2022Q0M	Hewlett-Packard	HP Compaq 6200 Pro MT PC	Microsoft Windows XP Professional	Symantec Endpoint Protection

Ver Anexo V

3.2.1.2.1 Sistemas Operativos existentes en la VLAN 10

Tabla 14
Sistemas Operativos de la VLAN 10

Sistema Operativos	Número de Activos
Microsoft Windows 7 Enterprise	37
Microsoft Windows XP Professional	34
Sin Sistema Operativo	8
Total general	**79**

Figura 13 Sistemas Operativos de la VLAN 10

En la Figura 9, se muestran los Sistemas Operativos de los activos de la VLAN 10, siendo representados en un 47% por Microsoft Windows 7 Enterprise, Microsoft Windows XP Professional con un 43% y finalmente el 10% de los activos se refieren a las Impresoras existentes, sin un Sistema Operativo instalado.

3.2.1.2.2 Antivirus existentes en la VLAN 10

Tabla 15 Antivirus VLAN 10
Antivirus VLAN 10

Antivirus	Número de Activos
avast! Free Antivirus	1
Symantec Endpoint Protec	70
Sin Antivirus	8
Total general	**79**

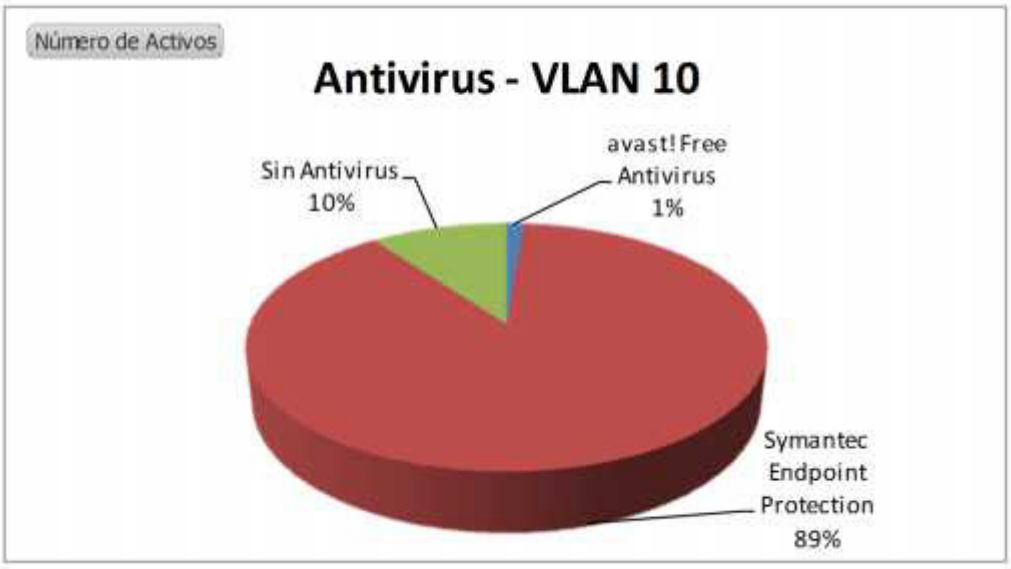

Figura 14 Antivirus VLAN 10

El antivirus Symantec Endpoint Protection se encuentra instalado en el 89% de los activos del Banco Nacional de Fomento, el antivirus avast! Free Antivirus ocupa el 1% y finalmente el 10% de los activos no posee ninguna solución Antivirus que se refiere a las Impresoras existentes en esta VLAN, esta información se encuentra representada gráficamente en la Figura 10.

3.2.1.2.3 Marca de Activos de la VLAN 10

Tabla 16
Marcas de Equipos de la VLAN 10

Marca de Activos	Número de Activos
Dell Inc.	2
Digi Connect	1
Digi Connect	1
Hewlett-Packard	61
OEM	10
RICOH	4
Total general	**79**

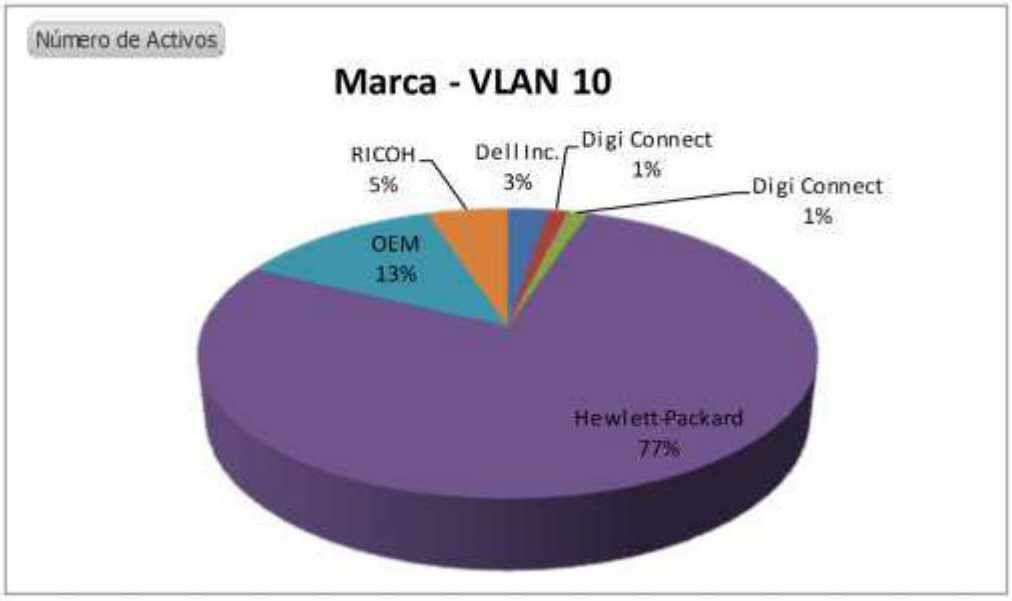

Figura 15 Marcas de Equipos de la VLAN 10

En la Figura 11, se observa que la marca Hewlett Packard representa el 77% del total de activos de la VLAN 10, el 13% lo ocupa la marca OEM (XTRATECH), la marca RICOH (Impresoras) representa el 5%, la marca DELL Inc. ocupa el 3% y finalmente el 2% es representado por las marcas Digi Connect (Impresoras).

3.2.1.2.4 Modelos de Impresoras

Tabla 17
Modelos de Impresoras y dispositivos de la VLAN 10

Modelo de Impresora	Cantidad de Activos
Digi Connect ME	2
HP Color LaserJet CM2320n MFP	1
HP ETHERNET MULTI-ENVIRONMENT	1
hp workstation xw4100	1
LANIER LD135	1
RICOH Aficio 2035e	1
RICOH Aficio MP 4000	2
Total general	**9**

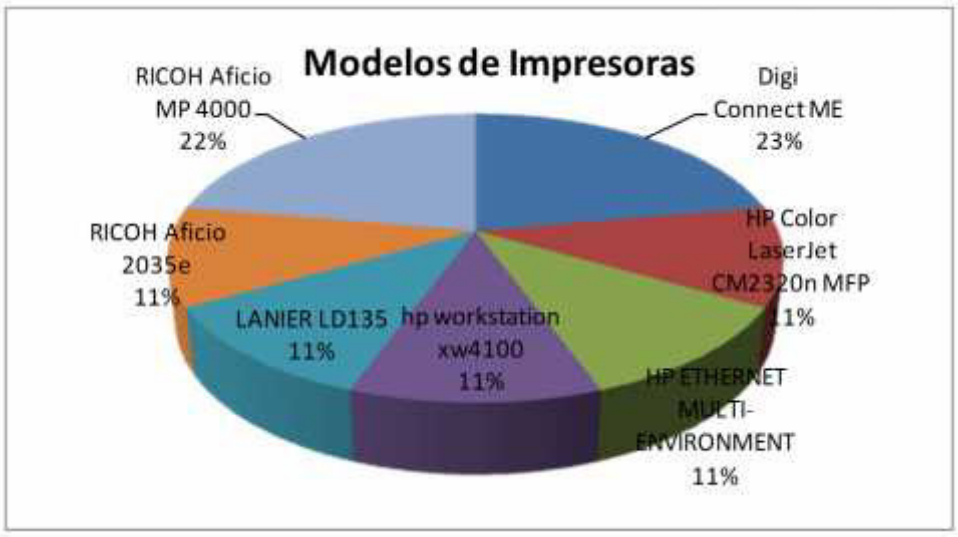

Figura 16 Modelos de Impresoras y dispositivos de la VLAN 10

Los Modelos de las Impresoras, son representadas por la marca RICOH, en un 22% por el modelo Aficio MP 4000 y un 11% por el modelo Aficio 2035e, el modelo Digi Connect ME ocupa el 23%, la marca HP es representada en un 11% con los modelos Workstation xw4100, Color LaserJet CM2320n MFP y Ethernet Multienvironment respectivamente y finalmente el modelo LANIER LD135 ocupa el 11%, esta información se muestra en la Figura 12.

3.2.1.2.5 Modelos de Equipos de Cómputo

Tabla 18
Modelos de Equipos de Cómputo Vlan 10

Modelo de Equipos de Computo	Cantidad de Activos
DSDT_PRJ	1
HP Compaq 6000 Pro SFF PC	3
HP Compaq 6200 Pro MT PC	2
HP Compaq 6710b (GB887ET#ABH)	1
HP Compaq 8100 Elite SFF PC	3
HP Compaq 8200 Elite SFF PC	9
HP Compaq dc5100 MT(ED681LA)	1
HP Compaq dc5700 Microtower	5
HP Compaq dc5700 Small Form Factor	2
HP Compaq dc5800 Microtower	1
HP Compaq dc5800 Small Form Factor	22
HP Compaq Pro 6300 SFF	7
HP d220 MT (PC641A)	1
OEM	10
OptiPlex GX520	2
Total general	**70**

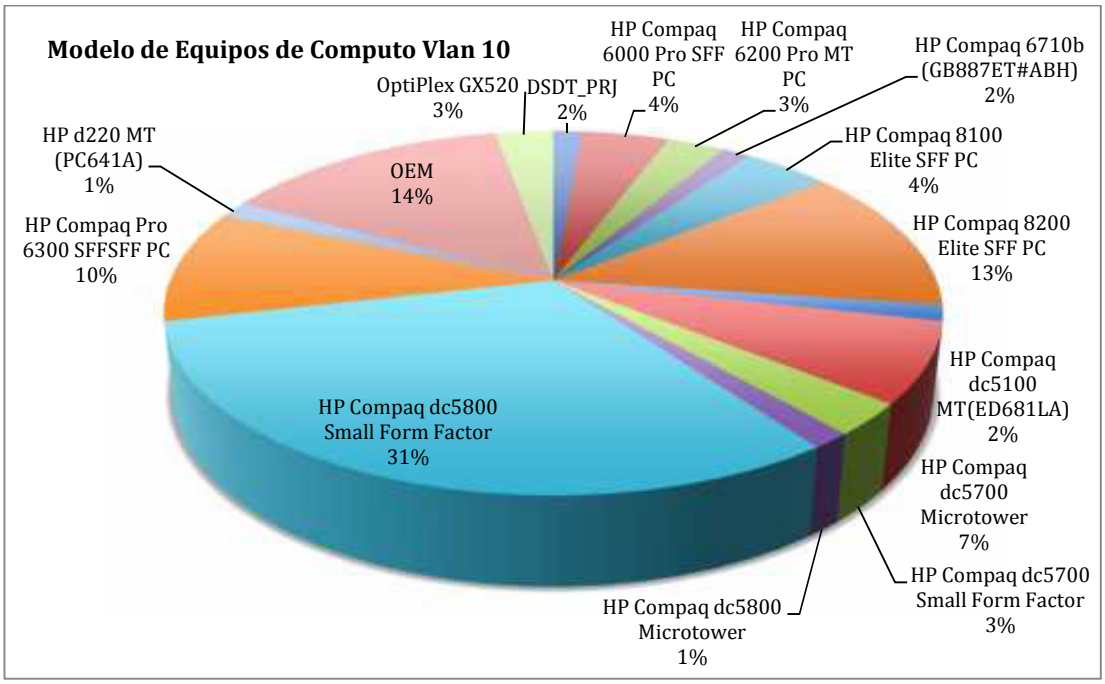

Figura 17 Modelos de Equipos de Cómputo Vlan 10

En la Figura 13 se muestra el modelo DSDT_PRJ ocupa el 2% del total de modelos existentes, la marca HP ocupa el 81%, dividida por los modelos HP Compaq 6000 Pro SFF PC con el 4%, el modelo HP Compaq 6200 Pro MT PC con el 3%, el modelo HP Compaq 6710b con el 2%, el modelo HP Compaq 8100 Elite SFF PC con el 4%, el modelo HP Compaq 8200 Elite SFF PC con el 13%, el modelo HP Compaq dc5100 MT con el 2%, el modelo HP Compaq dc5800 MT con el 1%, el modelo HP Compaq dc5800 SSF con el 31%, el modelo HP Compaq Pro 6300 SFF con el 10% y el modelo HP d220 MT con el 1%, la marca XTRATECH con el modelo OEM ocupa el 14% y finalmente la marca DELL con el modelo OptiPlex GX520 representa el 3% de los activos detectados.

3.2.1.2.6 Tipos de Activos en la VLAN 10

Tabla 19
Activos VLAN 10

Tipos de Activos	Número de Activos
Equipo de Escritorio	70
Impresora	8
Equipo Pórtatil	1
Total general	**79**

Figura 18 Tipos de Activos de la VLAN 10

En la figura 14, se puede observar que el 89% de los activos son Equipos de Escritorio, el 10% son Impresoras y 1% son Equipos Portátiles (Laptops).

Después del levantamiento de los activos del BNF, se obtuvieron los siguientes resultados:

Tabla 20 Levantamiento de activos del BNF
Levantamiento de activos del BNF

VLAN	Número de Activos (Equipos de Cómputo)	Número de Periféricos (Impresoras)	Total de Activos VLAN
2	75	0	75
5	59	1	60
10	71	8	79
15	43	1	44
20	27	2	29
30	18	4	22
32	128	5	133
40	107	7	114
60	126	8	134
70	39	2	41
80	20	3	23
Total	**713**	**41**	
		Total de Activos	**754**

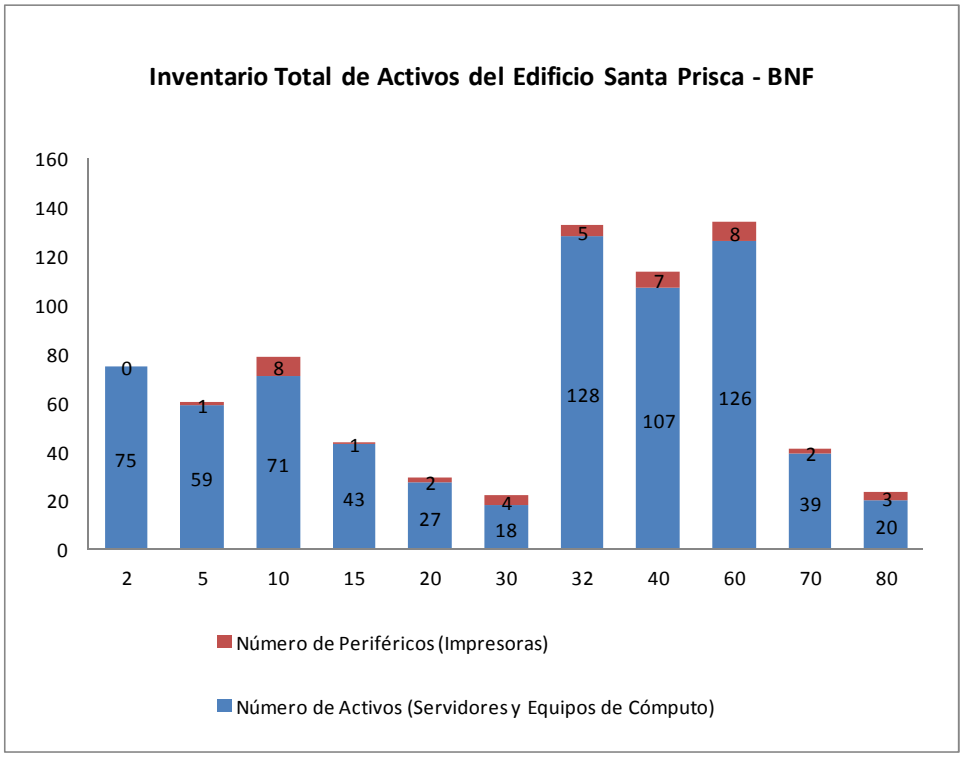

Figura 19 Inventario de activos BNF Matriz

En la figura 15, se puede apreciar que en la VLAN 32 existen 128 Equipos de Cómputo y en la VLANs 10 y 60, existen 8 Impresoras respectivamente, siendo la mayor cantidad de Activos dentro de red del Ed. Santa Prisca.

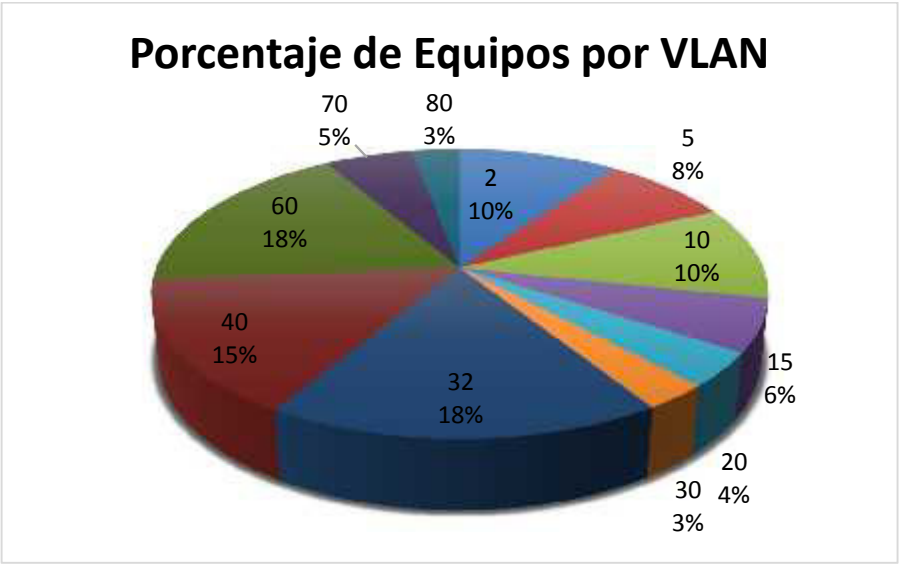

Figura 20 Porcentaje de Equipos por VLAN

En la Figura 16, se puede observar el total de activos en cada una de las VLANs, el 18% de los activos se encuentran en las VLANs 32 y 60 con la mayor cantidad de activos, mientras que las VLANs 20, 30 y 80 poseen la menor cantidad de activos.

Con esta información se demuestra que el Edificio Santa Prisca, donde funciona la Casa Matriz y la Sucursal Quito del BNF, existen 754 activos dentro de la red, como se muestra en la Tabla 20.

Esta información se la pueda apreciar en su totalidad en el anexo III

3.2.2 Fase dos: Categorizar sus activos

En esta fase, se le asignará un valor o prioridad a cada activo con el fin de organizarlos de acuerdo a la sensibilidad dentro del BNF.

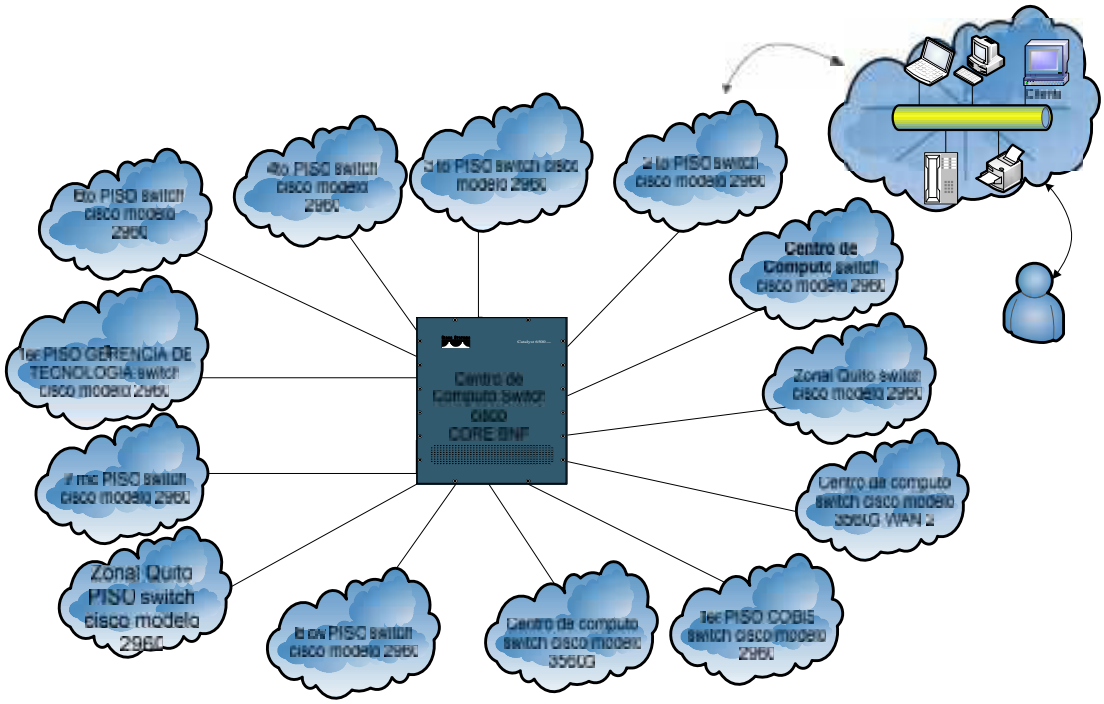

Figura 21 Edificio Matriz BNF Distribución de Pisos y Gerencias

Se asignará la prioridad por Vlan's, ya que cada una pertenece a un área específica, que tiene funciones dentro de la Institución, por tal motivo se puede determinar de manera objetiva que impacto produciría en la Institución si sufriera un ataque.

Se estableció tres prioridades, según el impacto que produciría si fuera atacada, definiéndose de la siguiente manera:

- **Alta:** Un activo se ve afectado de manera severa impidiendo su uso y afectando a actividades críticas de negocio.
- **Media:** Un activo se ve afectado impidiendo su uso pero no afectando a actividades críticas de negocio.
- **Baja:** Un activo se ve afectado pero no impide su uso.

Tabla 21
Categorización de activos segun piso del edificio matriz del BNF

PISO	IP	PRIORIDAD
Planta Baja	172.16.10.XX	ALTA
Piso 1	172.16.2.XX	ALTA
	172.16.5.XX	MEDIA
	172.16.15.XX	MEDIA
Piso 2	172.16.20.XX	BAJA
	172.16.30.XX	BAJA
Piso 3	172.16.30.XX	MEDIA
	172.16.32.XX	MEDIA
Piso 4	172.16.40.XX	BAJA
Piso 5	172.16.40.XX	BAJA
Piso 6	172.16.60.XX	MEDIA
Piso 7	172.16.60.XX	BAJA
	172.16.70.XX	MEDIA
Piso 8	172.16.80.XX	MEDIA

Como se muestra en la tabla 21, y teniendo en cuenta las prioridades antes establecidas, se asignó a cada VLAN una prioridad dependiendo la importancia del

área que utiliza dicha VLAN, dentro de la Institución y el impacto que produciría si sufriera un ataque.

Por tal motivo la VLAN 2, es utilizada por todos los servidores de la Institución donde están los diferentes servicios que ofrece el BNF y la VLAN 10, es utilizada por la Sucursal Quito, es decir funciona tanto el Área Operativa (Servicios Bancarios) como el área Comercial (Crédito, Recuperación de Cartera y Departamento Legal).

3.2.2.1 Priorización por VLANs

Tabla 22
Priorización por VLANs

Prioridad	VLANs
ALTA	2
BAJA	5
MEDIA	7
Total general	**14**

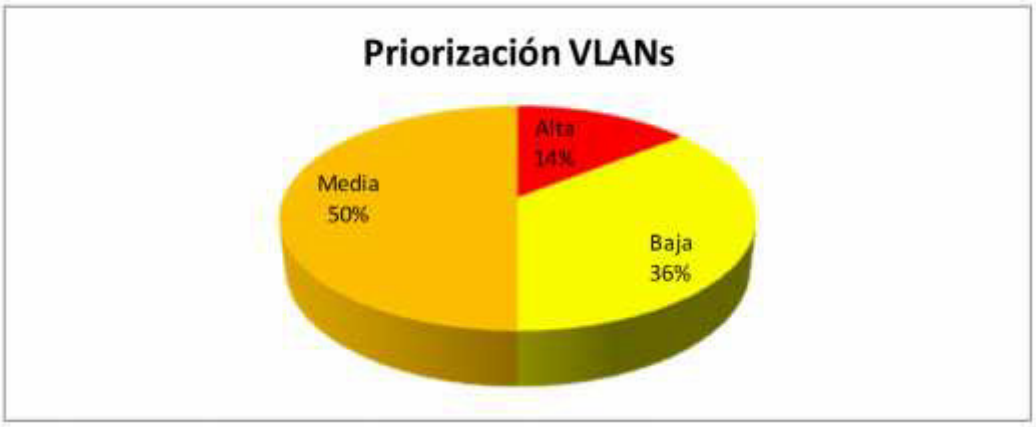

Figura 22 Nivel de Prioridad

En la figura 18, se muestra el número de redes que pertenece a cada prioridad, siendo así la prioridad Alta representa el 14% con 2 VLANs, la prioridad Media ocupa el 50% con 7 VLANs, mientras que la prioridad Baja con 5 VLANs, representa el 36%.

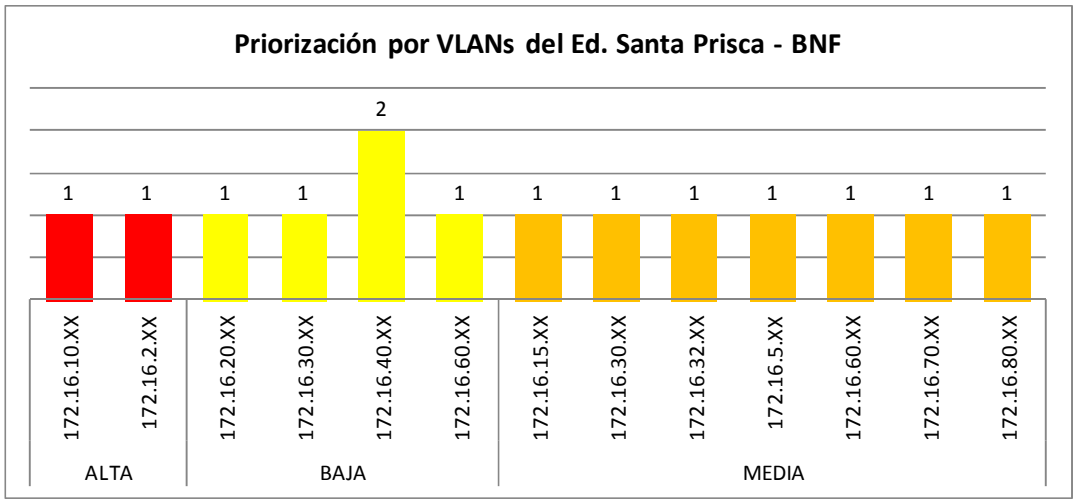

Figura 23 Priorización según VLANs

En la figura 19, se muestran cada una de las VLANs y su respectiva prioridad, teniendo que la prioridad Alta las VLANs 172.16.10 y 172.16.2, en la prioridad Media se encuentran las VLANs 172.16.20, 172.16.30, 172.16.40 y 172.16.60, finalmente las VLANs 172.16.15, 172.16.30, 172.16.32, 172.16.70 y 172.16.80, tienen una prioridad Baja.

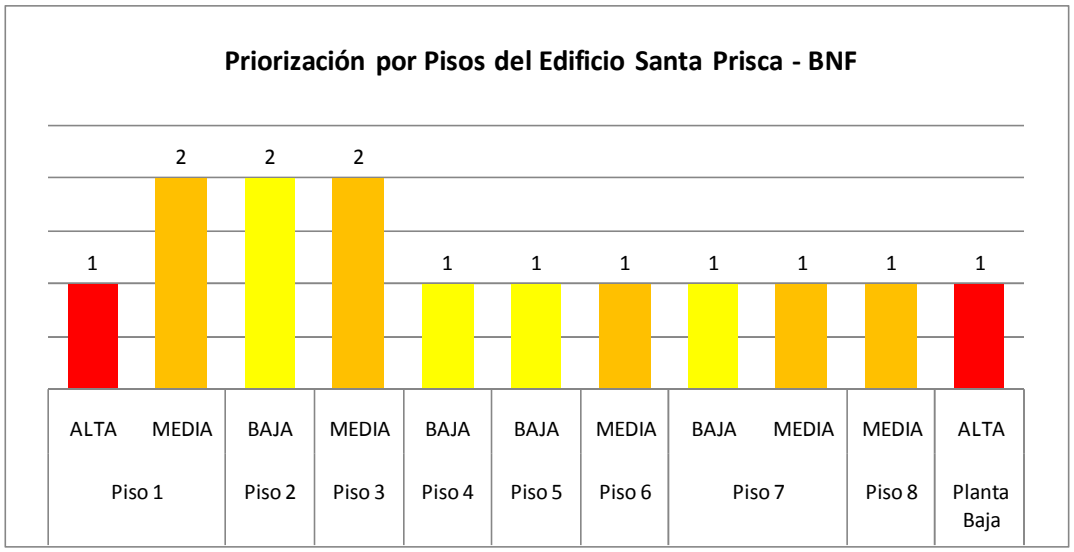

Figura 24 Priorización por pisos

En la figura 20, se muestra la prioridad en cada uno de los pisos del Edificio Santa Prisca, como se puede apreciar la prioridad Alta se encuentra en la Planta Baja

y el Piso 1, la prioridad Media está presente en los pisos 8, 7, 6, 3 y 1, mientras la prioridad Baja se encuentra en los pisos 2, 4, 5 y 7.

3.2.3 Fase tres: Crear una línea de base de los activos de exploración

En esta fase se realizará un análisis inicial, de todos los activos de la red del Edificio Santa Prisca, usando los siguientes procedimientos de escaneo:

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Para ejecutar los procedimientos de escaneo se utilizara varias herramientas, aprovechando todas las bondades que ofrecen los mismos, para obtener información precisa y fiable, que se pueda utilizar para la elaboración del presente estudio.

Los procedimientos de escaneo, tales como barridos de ping y escaneo de puertos, devuelven información acerca del mapa de direcciones IP y la información de cada uno de los hosts que están activos en Internet y cuáles son los servicios que ofrecen.

Otro método de exploración es el mapeo inverso, devuelve información de las direcciones IP que no responden; esto permite a un atacante hacer suposiciones acerca de las direcciones viables. (Lyon, 2013)

3.2.3.1 Network Scanning

Para la aplicación de este procedimiento, se contará con la ayuda de la herramienta **Angry IP Scanner.**

Tabla 23
Angry Ip

VLAN	Host activos	Host inactivos
		[n/s] [n/a]
2	68	141
5	47	133
10	47	86
15	33	137
20	22	90
30	12	206
32	78	124
40	68	137
60	87	115
70	11	60
80	17	52
Total	**490**	**1281**

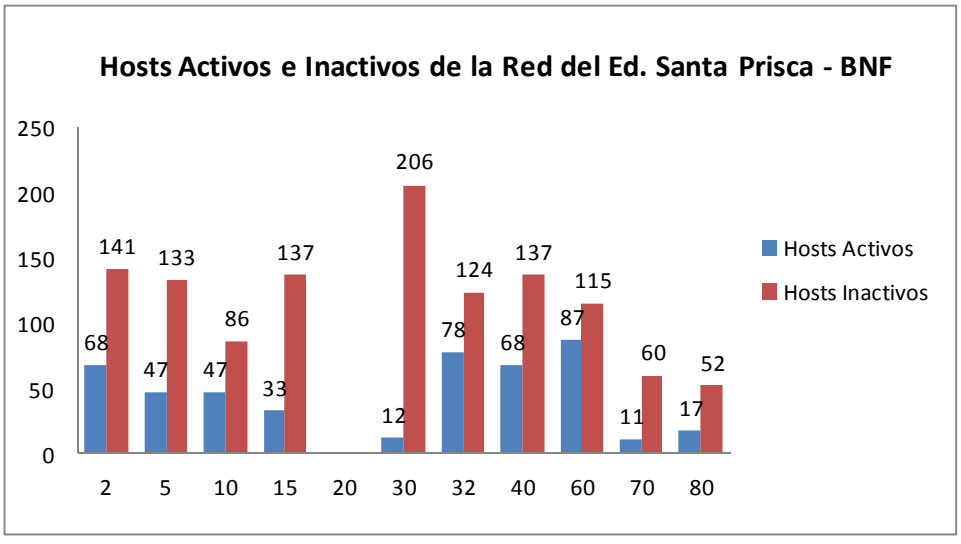

Figura 25 Host activos e inactivos del BNF ed. Matriz

En la figura 21, después de realizar el escaneo de cada VLAN, se puede obtener la cantidad de hosts activos e inactivos.

Como se muestra en la VLAN 32 donde funciona la Gerencia de Operaciones Centrales, existe mayor cantidad de host activos (78) y en la VLAN 30 donde funciona parte de la Gerencia de Talento Humano aparece la menor cantidad de hosts activos (12).

Los host activos, son los hosts que al momento de establecer conexión muestran una respuesta en milisegundos (ms), el tiempo de respuesta varias de un host a otro.

Los host inactivos, se muestran según las siguientes definiciones:

- **Desconocido:** El valor actual no fue escaneado. Etiqueta por defecto: [n/s]
- **Sin Resultados:** El valor no está disponible. Etiqueta predeterminada: [n/a]

Finalmente, se obtienen 468 host activos y 1191 host inactivos, después del escaneo realizado, se debe tener en cuenta que en la primera fase, se obtuvo 780 activos, entonces existe un desfase de 312 activos, los cuales no reportaron por varios motivos que pueden ser:

- Equipo apagado al momento del escaneo
- Firewall de Windows activado
- Problemas con los DNS (*Domain Name System*).

La informacion completa del escaneo por angry ip se encuentra en el Anexo Digital.

3.2.3.2 Port Scanning

Para la aplicación del procedimiento Port Scanning, se utilizará la herramienta **NMAP**, por todas las facilidades que ofrece.

Los resultados obtenidos de la aplicación de la técnica Port Scanning, realizada con la herramienta NMAP son los siguientes:

Tabla 24
Resultados Port Scanning

Puerto	Estado	Servicio	VLAN	
			2	10
1028/tcp	open	unknown	X	
7920/tcp	open	unknown	X	
8093/tcp	open	unknown	X	
8099/tcp	open	unknown	X	
8222/tcp	open	unknown	X	
9081/tcp	open	unknown	X	
34571/tcp	open	unknown	X	
34572/tcp	open	unknown	X	
49152/tcp	open	unknown	X	X
49153/tcp	open	unknown	X	X
49154/tcp	open	unknown	X	X
49155/tcp	open	unknown	X	X
49156/tcp	open	unknown	X	
49157/tcp	open	unknown	X	
49158/tcp	open	unknown	X	
49159/tcp	open	unknown	X	X
49163/tcp	open	unknown	X	
49175/tcp	open	unknown	X	X
49176/tcp	open	unknown		X
50001/tcp	open	unknown	X	

En la Tabla 24, se puede visualizar la presencia de los puertos 49152, 49153, 49154, 49155, 49159 y 49175 tanto en la VLAN 2 como en la VLAN 10, lo cual alerta

que estos puertos pueden ser utilizados por atacantes para vulnerar la red, por lo tanto se debe prestar mucha atención a su comportamiento, para evitar futuros ataques.

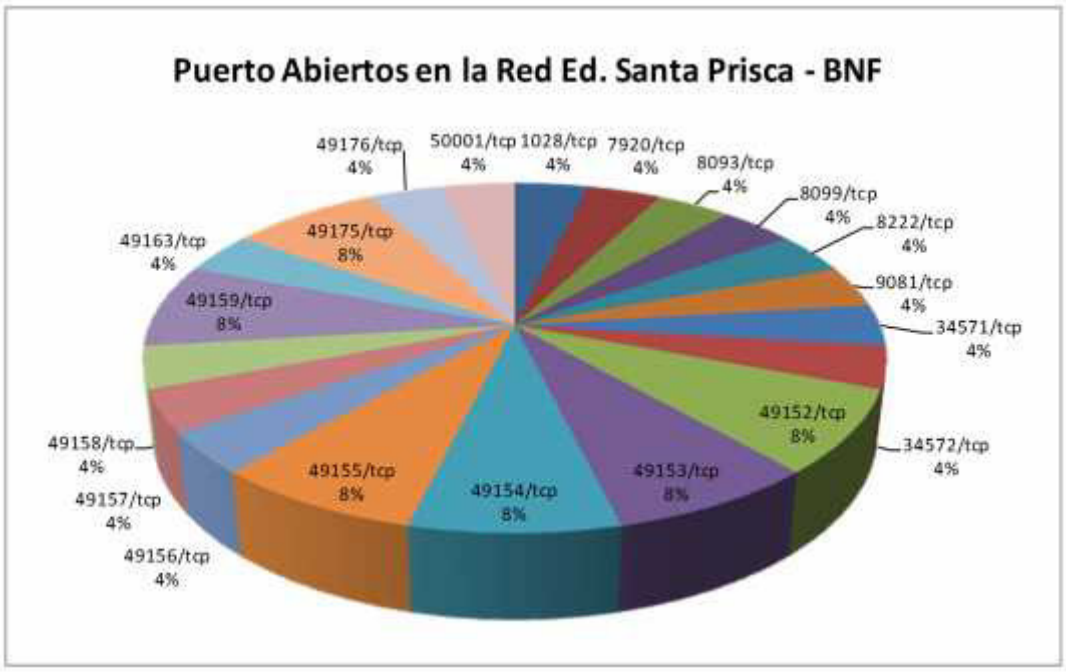

Figura 26 Puertos abiertos encontrados

En la figura 22, se muestran los puertos abiertos, a los que pertenecen los servicios desconocidos (unknown), presentes en las VLANs 2 y 10, ya que en la fase de categorización de activos, se definen como las Áreas más críticas dentro de la red del Banco Nacional de Fomento, por tal motivo la afectación de dichas VLANs produciría un fuerte impacto en el negocio de la Institución.

Dichas VLAN deben tener la mayor disponibilidad posible o si enfrentar un ataque, deberían reestablecerse en el menor tiempo posible.

A continuación se muestra un detalle de cada uno de los puertos antes mencionados, sus asignaciones y vulnerabilidades.

Tabla 25
Puerto 1028

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
1028	Tcp	trojan	DataSpy Network X, Dosh, Gibbon, KiLo, KWM, Litmus, Paltalk, SubSARI	Trojans
1028	Udp	trojan	KiLo, SubSARI	Trojans
1028	tcp,udp		Desaprobado en Febrero 2004	IANA
1028	Udp	ms-lsa	ms-lsa	Nmap
1025-1029	tcp,udp	NFS, IIS, etc.	Puertos > 1024 se designan por la asignación dinámica de Windows. Cuando los programas solicitan "disposición próxima", por lo general son los puertos secuenciales a partir de 1025. Puertos 1026/udp - 1027/udp suelen ser utilizados por el Mensajero emergente de Spam.	SG

Fuente: (Speeg Guide, 2015)

Tabla 26
Puerto 8222

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
8222	Tcp	applications	VMWare, Y-cam Wireless IP Camera	SG
8222	tcp,udp		VMware Server Management User Interface (insecure Web interface). Ver también el puerto 8333 (no oficial)	Wikipedia
8209-8229	tcp,udp		Sin asignar	IANA
8150-8350	tcp,udp	applications	Y-cam Wireless IP Camera	Portforward

Fuente: (Speeg Guide, 2015)

Tabla 27
Puerto 9081

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
9081	tcp,udp	applications	Puede ser usado por el Portal IBM WebSphere	SG
9081-9083	tcp,udp		Sin asignar	IANA

Fuente: (Speeg Guide, 2015)

Tabla 28
Puerto 34571

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
34571	Tcp	serveraid	ServeRAID Manager Cisco Unity en los servidores IBM se suministra con los ajustes que deberían haber sido inhabilitados por el fabricante, que permite a atacantes locales o remotos realizar actividades no autorizadas a través de una cuenta de usuario local "bubba", un puerto TCP abierto 34571, o cuando un servidor DHCP local por defecto no está disponible, un servidor DHCP en la red de prueba del fabricante. Referencia: [CVE-2003-0983]	SG
34380 - 34961	tcp,udp		Sin asignar	IANA

Fuente: (Speeg Guide, 2015)

Tabla 29
Puerto 34572

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
34572	Tcp	applications	ServeRAID Manager IBM Director 5.10	SG
34380 - 34961	tcp,udp		Sin asignar	IANA

Fuente: (Speeg Guide, 2015)

Tabla 30
Puerto 49152

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
49152	tcp,udp	applications	Como el primer puerto del rango dinámico / privada (49.152-65.535), este puerto es comúnmente utilizado por las aplicaciones que utilizan un puerto dinámico / random / configurable. uTorrent, Azureus y / Vuze p2p torrents clientes a menudo utilizan este puerto.	SG

Continúa

			De Apple Xsan Filesystem Access utiliza también el rango dinámico / privado 49152 a 65535.	
42800-49152-49172-49272-49292	Udp	applications	Titan Quest	Portforward

Fuente: (Speeg Guide, 2015)

Tabla 31
Puerto 49153

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
49153	Tcp	applications	ANTLR, ANother Tool for Language Recognition, (formerly PCCTS) - un generador de analizadores sintácticos para el reconocimiento de las lenguas	SG

Fuente: (Speeg Guide, 2015)

Tabla 32
Puerto 49154

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
49154	Tcp	applications	Xsan Filesystem Access	SG

Fuente: (Speeg Guide, 2015)

Tabla 33
Puerto 49156

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
49156	tcp,udp	applications	Azureus	SG

Fuente: (Speeg Guide, 2015)

Tabla 34
Puerto 49159

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
49159	tcp,udp	applications	Bonjour for Windows - contratados por iTunes e iChat para compartir archivos entre Windows y Mac OS.	SG

Fuente: (Speeg Guide, 2015)

Tabla 35
Puerto 50001

Puerto(s)	Protocolo	Servicio	Detalles	Fuente
50001	tcp,udp	applications	Java Remote Shell Server, Zotero, IBM DB2 La interfaz de administración en la puerta de enlace 2Wire 1700HG, 1701HG, 1800HW, 2071, 2700HG y 2701HG-T, con el software antes de 5.29.52, permite a atacantes remotos provocar una denegación de servicio (reinicio) a través de una secuencia 0d% 0a% en el parámetro de página al programa xslt en el puerto TCP 50001. Referencia: [CVE-2009-3962]	*SG*
50000-50004	Udp	applications	Serv-U	Portforward

Fuente: (Speeg Guide, 2015)

La informacion completa del escaneo por nmap se encuentra en el Anexo Digital.

3.2.3.3 Vulnerability Scanning

La aplicación de este procedimiento, se desarrollará con la ayuda de la herramienta **GFI LANguard.**

El procedimiento Vulnerability Scanning, generó los siguientes resultados:

Tabla 36
Resultados de Vulnerability Scanning - GFI Languard

ID	DESCRIPCION	Vlan 2	Vlan 10
	AutoRun is enabled	X	
OVAL:13205	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors related to a constructor for an unspecified ActionScript3 object and improper type checking, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574,CVE-2011-0607, and CVE-2011-0608.	X	X
OVAL:13294	Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris and 10.1.95.1 on Android, and authplay.dll (aka AuthPlayLib.bundle or libauthplay.so.0.0.0) in Adobe. Reader and Acrobat 9.x through 9.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted SWF content, as exploited in the wild in October 2010.	X	X
OVAL:13429	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0561, CVE-2011-0571.	X	X
OVAL:13809	Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to execute arbitrary code via crafted streaming media, related to a "logic error vulnerability."	X	X
OVAL:13901	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different	X	X
OVAL:13904	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial.	X	X

Continúa

OVAL:13914	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash.	X	X
OVAL:13924	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different	X	X
OVAL:13940	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to	X	X
OVAL:13945	Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows attackers to execute arbitrary code or cause a denial of service (browser crash) via unspecified vectors, related to	X	X
OVAL:13961	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial	X	X
OVAL:13979	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to	X	X
OVAL:13988	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561	X	X
OVAL:13994	Integer overflow in Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code via ActionScript that improperly handles a long array	X	X
OVAL:14003	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial	X	X

Continúa

OVAL:14014	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, when Internet Explorer is used, allows remote attackers to	X	X
OVAL:14015	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary	X	X
OVAL:14016	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary	X	X
OVAL:14021	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561	X	X
OVAL:14036	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different	X	X
OVAL:14043	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to	X	X
OVAL:14056	Integer overflow in Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code via a large array length value in the ActionScript method of the Function class.	X	X
OVAL:14066	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561	X	X
OVAL:14070	Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component in Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to execute	X	X

Continúa

OVAL:14073	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary	X	X
OVAL:14074	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary	X	X
OVAL:14077	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different	X	X
OVAL:14085	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to	X	X
OVAL:14088	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a	X	X
OVAL:14091	Adobe Flash Player before 10.3.181.26 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.23 and earlier on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified	X	X
OVAL:14111	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to	X	X
OVAL:14113	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a	X	X
OVAL:14115	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561	X	X

Continúa

OVAL:14125	Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component in Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows attackers to execute arbitrary	X	X
OVAL:14132	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to	X	X
OVAL:14137	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561	X	X
OVAL:14147	Unspecified vulnerability in Adobe Flash Player 10.2.154.13 and earlier on Windows, Mac OS X, Linux, and Solaris; 10.1.106.16 and earlier on Android; Adobe AIR 2.5.1 and earlier; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader	X	X
OVAL:14160	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a	X	X
OVAL:14164	Unspecified vulnerability in Adobe Flash Player before 10.2.152.26 allows remote attackers to execute arbitrary code via a crafted font.	X	X
OVAL:14165	Stack-based buffer overflow in Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute	X	X
OVAL:14169	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0571	X	X
OVAL:14172	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561	X	X

Continúa

OVAL:14175	Adobe Flash Player before 10.2.154.27 on Windows, Mac OS X, Linux, and Solaris and 10.2.156.12 and earlier on Android; Adobe AIR before 2.6.19140; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader 9.x before 9.4.4 and 10.x	X	X
OVAL:14189	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial	X	X
OVAL:14194	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to	X	X
OVAL:14199	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows remote attackers to execute	X	X
OVAL:14215	Buffer overflow in Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code	X	X
OVAL:14231	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial	X	X
OVAL:14260	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial	X	X
OVAL:14312	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial	X	X
OVAL:14507	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial	X	X

Continúa

OVAL:14510	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial	X	X
OVAL:14654	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or	X	X
OVAL:14731	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to bypass intended access	X	X
OVAL:14795	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or	X	X
OVAL:14881	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to bypass intended access	X	X
OVAL:14985	The ActiveX control in Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	X	X
OVAL:15030	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or	X	X
OVAL:15993:	Use-after-free vulnerability in the XPCWrappedNative::Mark function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service		X
OVAL:16171:	The nsSVGPathElement::GetPathLengthScale function in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and		X

Continúa

OVAL:16189:	Use-after-free vulnerability in the ~nsHTMLEditRules implementation in Mozilla Firefox before 18.0,Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before..		X
OVAL:16199:	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.1, and		X
OVAL:16288	Use-after-free vulnerability in the imgRequest::OnStopFrame function in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before		X
OVAL:16336:	Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving the setting of Cascading Style Sheets		X
OVAL:16383:	Use-after-free vulnerability in the nsOverflowContinuationTracker::Finish function in Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16		X
OVAL:16407	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe	X	X
OVAL:16570:	Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 do not properly implement quickstubs		X
OVAL:16573:	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allow remote attackers to		X
OVAL:16595:	Unspecified vulnerability in the browser engine in Mozilla Firefox before 20.0 on Android allows remote attackers to cause a denial of service (stack memory corruption and application crash) or possibly execute arbitrary code via unknown		X

Continúa

OVAL:16603	Integer overflow in the WebGL subsystem in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary		X
OVAL:16619:	The ClusterIterator::NextCluster function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via		X
OVAL:16690:	Use-after-free vulnerability in the nsPlaintextEditor::FireClipboardEvent function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14		X
OVAL:16694:	Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to execute arbitrary code or cause a denial of service		X
OVAL:16715:	The nsSOCKSSocketInfo::ConnectToProxy function in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 does not ensure thread safety for SSL		X
OVAL:16737:	Use-after-free vulnerability in the nsEditor::IsPreformatted function in editor/libeditor/base/nsEditor.cpp in Mozilla Firefox before 19.0.2, Firefox ESR 17.x before 17.0.4, Thunderbird before 17.0.4, Thunderbird ESR 17.x before 17.0.4		X
OVAL:16739:	Heap-based buffer overflow in the image::RasterImage::DrawFrameTo function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows		X
OVAL:16747	The nsCodingStateMachine::NextState function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via		X
OVAL:16748	The texImage2D implementation in the WebGL subsystem in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 does not properly interact with...		X

Continúa

OVAL:16761	Use-after-free vulnerability in the nsEditor::FindNextLeafNode function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service		X
OVAL:16812:	Use-after-free vulnerability in the ListenerManager implementation in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before...		X
OVAL:16813:	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Thunderbird before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to cause a denial of service (memory corruption and application crash)…		X
OVAL:16832	Use-after-free vulnerability in the mozilla::TrackUnionStream::EndTrack implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before...		X
OVAL:16833	The Style Inspector in Mozilla Firefox before 17.0 and Firefox ESR 10.x before 10.0.11 does not properly restrict the context of HTML markup and Cascading Style Sheets (CSS) token sequences, which allows user-assisted remote attackers to...		X
OVAL:16839	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allow remote attackers to cause a denial of service (memory corruption and application crash)...		X
OVAL:16846	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:16849	Heap-based buffer overflow in the nsWindow::OnExposeEvent function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote…		X
OVAL:16861	The Chrome Object Wrapper (COW) and System Only Wrapper (SOW) implementations in Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 do not...		X

Continúa

OVAL:16896	The copyTexImage2D implementation in the WebGL subsystem in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption...		X
OVAL:16897	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:16902	Use-after-free vulnerability in the gfxFont::GetFontEntry function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows remote...		X
OVAL:16904	Use-after-free vulnerability in the nsTextEditorState::PrepareEditor function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before 2.14 allows...		X
OVAL:16906	Heap-based buffer overflow in the nsSaveAsCharseterbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code via unspecified vectors.		X
OVAL:16913	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:16921	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:16932	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:16934	Use-after-free vulnerability in the nsPrintEngine::CommonPrint function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of service...		X

Continúa

OVAL:16939	The Chrome Object Wrapper (COW) implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 does not prevent modifications to the...		X
OVAL:16950	Use-after-free vulnerability in the nsImageLoadingContent::OnStopContainer function in Mozilla Firefox before 19.0, Firefox ESR 17.x before 17.0.3, Thunderbird before 17.0.3, Thunderbird ESR 17.x before 17.0.3, and SeaMonkey before 2.16…		X
OVAL:16953	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allow remote attackers to...		X
OVAL:16957	Integer overflow in the JavaScript implementation in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and...		X
OVAL:16958	Use-after-free vulnerability in the nsViewManager::ProcessPendingUpdates function in Mozilla Firefox before 17.0, Thunderbird before 17.0, and SeaMonkey before 2.14 allows remote attackers to execute arbitrary code or cause a denial of…		X
OVAL:16968	Heap-based buffer overflow in the gfxShapedWord::CompressedGlyph::IsClusterStart function in Mozilla Firefox before 17.0, Firefox ESR 10.x before 10.0.11, Thunderbird before 17.0, Thunderbird ESR 10.x before 10.0.11, and SeaMonkey before…		X
OVAL:16969	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:16977:	Use-after-free vulnerability in the nsDisplayBoxShadowOuter::Paint function in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allows remote attackers to execute arbitrary code or cause a denial of…		X
OVAL:16990:	Stack-based buffer overflow in the Canvas implementation in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to...		X

Continúa

OVAL:16995	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:17007:	Use-after-free vulnerability in the TableBackgroundPainter::TableBackgroundData::Destroy function in Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x...		X
OVAL:17019:	Heap-based buffer overflow in the gfxTextRun::ShrinkToLigatureBoundaries function in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15...		X
OVAL:17030	Adobe Flash Player before 10.3.183.90 and 11.x before 11.7.700.224 on Windows; Adobe AIR before 3.7.0.2090 on Windows; and Adobe AIR SDK and Compiler before 3.7.0.2090 on Windows allow attackers to execute arbitrary code or cause a…	X	X
OVAL:17050	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:17083	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:17086	Buffer overflow in the CharDistributionAnalysis::HandleOneChar function in Mozilla Firefox before 18.0, Thunderbird before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code via a crafted document.		X
OVAL:17087:	Mozilla Firefox before 18.0, Firefox ESR 10.x before 10.0.12 and 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 10.x before 10.0.12 and 17.x before 17.0.2, and SeaMonkey before 2.15 allow remote attackers to execute...		X
OVAL:17101:	Use-after-free vulnerability in the obj_toSource function in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.2, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.2, and SeaMonkey before 2.15 allows remote attackers to...		X

Continúa

OVAL:17107:	Use-after-free vulnerability in Mozilla Firefox before 18.0, Firefox ESR 17.x before 17.0.1, Thunderbird before 17.0.2, Thunderbird ESR 17.x before 17.0.1, and SeaMonkey before 2.15 allows remote attackers to execute arbitrary code or...		X
OVAL:17118	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:17119	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 19.0, Thunderbird before 17.0.3, and SeaMonkey before 2.16 allow remote attackers to cause a denial of service (memory corruption and application crash)...		X
OVAL:17141	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe…	X	X
OVAL:6660	Adobe Flash Player and AIR Loader Object Heap Memory Corruption Vulnerability	X	X
OVAL:6865	Adobe Flash Player and AIR URI Parsing Heap Buffer Overflow Vulnerability	X	X
OVAL:6998	Adobe Flash Player and AIR 'intf_count' Integer Overflow Vulnerability	X	X
OVAL:7011	Adobe Flash Player and AIR NULL Pointer Exception Remote Code Execution Vulnerability	X	X
OVAL:12566	Microsoft Windows Human Interface Device (HID) driver is prone to security bypass ulnerability.	X	X
	AutoShareServer	X	X
	AutoShareWKS	X	X
	Cached Logon Credentials	X	X
	Service running: HTTP	X	X
	Shutdown without logon		X

Fuente: (GFI LanGuard, 2011)

Figura 27 Escaneo de la Vlan 2

Figura 28 Escaneo de la Vlan 10

Esta clasificación depende principalmente del impacto que genera la vulnerabilidad detectada en el equipo.

Para este estudio han sido seleccionadas las vulnerabilidades de nivel Alto (High), ya que son las de mayor impacto dentro de la Institución.

Tabla 37
Incidencia de las Vulnerabilidades detectadas

Aplicativo / Servicio	Incidencia
Adobe Acrobat Reader	2
Adobe Flash Player	123
Adobe Flash Player / Acrobat Reader	1
Adobe Flash Player / Adobe AIR	10
Adobe Shockwave Player	43
Apple Quicktime	57
Fax Cover Page	1
Internet Information Services	2
Java Runtime Environment (JRE)	1
JavaFX	2
Microsoft Office PowerPoint 2007	2
Microsoft Windows Internet Communication Settings on Windows XP SP3 and Windows XP SP2	1
Microsoft Windows Progman Group Converter	2
Mozilla Firefox	163
SQL	1
Thunderbird ESR / SeaMonkey	1
Vmware	1
VMware Workstation	3
Win32k	1
Wireshark	4
AutoRun	1
ActiveX Objec	1

La tabla 37, muestra los Aplicativos y Servicios que son utilizados por atacantes para abrir brechas de seguridad y producir amenazas, además se aprecia la

incidencia presentada en cada Aplicativo o Servicio, de cada vulnerabilidad detectada, según el informe generado por el análisis realizado por la herramienta GFI LANguard.

Teniendo en cuenta estos Aplicativos y Servicios, se puede definir contramedidas para minimizar los posibles riesgos que se pueden presentar al momento de utilizar dichas herramientas.

CONTRAMEDIDAS

Acontinuación se presentan las vulnerabilidades más comunes que se pueden presentar dentro de una Institución, en este caso el Banco Nacional de Fomento y su situación actual, es decir, la contramedida (cuya definición y clasificación se puede apreciar en el Anexo I), aplicada o la proyección como Institución para minimizar el impacto que podría producir la misma.

Tabla 38
Vulnerabilidades comunes y situación actual en el BNF

Vulnerabilidad	Situación actual del Banco Nacional de Fomento
Instalación de sistemas operativos y aplicaciones, dejando sus valores por defecto. **Es importante revisar todas las configuraciones de los equipos, antes de la máquina pueda acceder a la red.**	El Área de Mesa de Ayuda de la Gerencia de Tecnología del Banco Nacional de Fomento, ha definido un proceso de Instalación, Mantenimiento, Actualización y Configuración (IMAC), para todo el campo computacional existente, en el cual están definidas todas las configuraciones básicas que debe tener un equipo para funcionar correctamente dentro de la red de la Institución.
Cuentas sin contraseñas o con contraseñas débiles. **Muchos sistemas disponen de una única línea de defensa: la contraseña del usuario. No se debe colocar contraseñas tan obvias**	El Área de Seguridad de la Información de la Gerencia de Riesgos, ha definido una política de Seguridad a nivel de contraseña de acceso, por medio del Directorio Activo (Active Directory), además de campañas de concientización para el correcto uso de contraseñas, con lo cual se trata de minimizar las brechas de seguridad existentes con el manejo de contraseñas.
Copias de seguridad inexistentes o incompletas. **No hay nada más inútil que una copia de seguridad que no pueda ser restaurada o cuyo contenido no sirva.**	El Banco Nacional de Fomento, cuenta con una herramienta especializada en generación de copias de seguridad, se encuentra en la fase de pruebas e implementación, teniendo como primera fase, la generación de copias de seguridad de los funcionarios de nivel Jerárquico Superior (Gerentes y Asesores), por la importancia de la información que manejan dichos funcionarios.
Gran cantidad de puertos abiertos. **Cuanto más puertos abiertos hayan, más posibilidades existen que algún intruso pueda conectase. Por tanto, es importante que sólo estén abiertos aquellos puertos realmente necesarios para el normal funcionamiento del sistema.**	Actualmente no se cuenta con un registro formal sobre el estado de los puertos que son utilizados por los servicios y aplicaciones del Banco Nacional de Fomento. Por lo tanto, es importante mantener abiertos sólo los puertos imprescindibles para que el

Continúa

	sistema funcione correctamente. El resto de los puertos deben ser cerrados. En este estudio se brindará apoyo en este tema, indicando los controles que deben ser aplicados en los puertos utilizados en la Institución.
No realizar correctamente el filtrado de las direcciones entrantes y salientes. **La suplantación de direcciones IP es un método frecuentemente utilizado por los atacantes como medida de ocultación.** **Por tanto, deben aplicarse las medidas necesarias para impedir la entrada y/o salida de direcciones IP incorrectas, inesperadas o no válidas.**	El Banco Nacional de Fomento, administra el filtrado de tráfico de la red, mediante un firewall institucional, estableciendo controles de acceso o restricción dentro de la red, para minimizar los posibles riesgos que podrían presentarse. Se debe utilizar un mecanismo de filtrado sobre el tráfico que entra en la red (ingress filtering) y el que sale (egress filtering) le ayudará a lograr un alto nivel de protección, lo cual es un proyecto pendiente dentro de la Institución.
Registro de eventos (logging) inexistente o incompleto **La prevención de incidentes de seguridad es importante, pero mucho más valioso es poder detectarlos lo antes posible.** **Por ello es importante registrar la mayor cantidad de información posible sobre la actividad del sistema, aplicando las medidas necesarias para el análisis de los registros.**	El Banco Nacional de Fomento, no posee un registro de las novedades presentadas en los sistemas clave de la entidad, por tal motivo se recomienda que el registro debe ser realizado periódicamente. Los registros proporcionan los detalles de lo que está ocurriendo, qué sistemas se encuentran bajo ataque y qué sistemas han sido comprometidos. El registro debe ser realizado de forma regular y debe ser archivado y respaldado, porque nunca se sabe cuándo puede ser necesario. Lo recomendable es almacenar los registros en un recolector central que escribe la información en un soporte que sólo admita una escritura, con el fin de que el atacante no pueda sobrescribir los registros para evitar la detección.
Programas de CGI (Common Gateway Interface) vulnerables. **La mayoría de servidores Web permiten utilizar programas CGI para acceder a información, recoger datos, identificar usuarios, entre otros.**	Actualmente, no se dispone de una protección adecuada de los programas CGI ya que la mayoría de servidores web vienen con programas CGI de ejemplo preinstalados, usados por intrusos para realizar ataques. Como regla general, se propone que los programas de ejemplo deben ser siempre eliminados de los sistemas de producción, para que sean objeto de ataques externos.
Vulnerabilidad de Unicode (Web Server Folder Traversal). **Las versiones de IIS (Internet Information Server), son vulnerables a un ataque consistente en ocultar URL ilegales (como el acceso a directorios del sistema) mediante la**	El Banco Nacional de Fomento, no tiene implementada ninguna medida de seguridad para evitar ataques de saltos de directorio (Directory Traversal Attack), utilizados por los atacantes para entrar y salir de los directorios de los servidores y ejecutar scripts de forma arbitraria.

Continúa

representación de diversos caracteres en formato Unicode.	Se debe implementar medidas de seguridad para evitar esta clase de ataques que ocasionan graves problemas a la infraestructura de la Institución.
Desbordamiento de búfer en extensiones ISAPI. **Cuando se instala IIS, también se instalan automáticamente diversas extensiones ISAPI (Interfaz de Programación de Aplicaciones para Servicios de Internet).** **Existen diversos problemas de desbordamiento de memoria intermedia en estas extensiones que pueden ser utilizadas por un atacante para obtener el control completo del sistema.**	Al instalarse las extensiones ISAPI, permite que los programadores puedan extender las capacidades de un servidor mediante el uso de DLLs, pero varias de las DLLs, como idq.dll, contienen errores de programación que causan que éstas realicen un chequeo incorrecto de límites. En particular no bloquean entradas inaceptablemente largas.Los atacantes pueden enviar información a estas DLLs, en lo que se conoce como un ataque por desbordamiento de buffer, y tomar control de un servidor IIS.Se recomienda bloquear las entradas inaceptablemente largas, para evitar que puedan ser usadas para tomar control de los servidores de la entidad.
Exploits para RDS (Microsoft Remote Data Services) del IIS (Microsoft Internet Information Server). **Existen diversas vulnerabilidades en el componente RDS (Remote Data Services) de IIS que pueden ser utilizadas por un atacante remoto para la ejecución de comandos del sistema con privilegios de administrador.**	Los atacantes pueden explotar fallos de programación en los servicios RDS de IIS con el fin de ejecutar comandos remotos y abrir brechas de seguridad en la infraestructura tecnológica de la Institución. Habitualmente resultan afectados los sistemas Microsoft Windows NT 4.0 con Internet Information Server que tengan el directorio virtual /msadc asociado. No se cuenta con políticas de seguridad en cuanto a los Exploits para RDS del IIS, se debe implementar medidas para asegurar dichas brechas de seguridad.
NETBIOS - recursos sin protección, compartidos en redes bajo Windows. **Algunos protocolos de red incluidos en el sistema operativo Windows no ofrecen mecanismos de protección adecuados, por lo que un atacante remoto puede obtener acceso a información almacenada en los computadores.**	El Banco Nacional de Fomento, no tiene un control apropiado de las carpetas compartidas dentro de la red, ya que al momento de habilitar la propiedad de compartir archivos en máquinas Windows las hace vulnerables tanto al robo de información como a ciertos tipos de virus que se propagan con rapidez. Las máquinas Macintosh y UNIX son también vulnerables a ataques de este tipo si los usuarios habilitan la compartición de archivos. Los mecanismos SMB que permiten el compartir archivos en Windows pueden ser también utilizados por posibles atacantes para obtener información sensible acerca de dichos sistemas. A través de conexiones de tipo "sesión nula" ("null session") con el servicio de sesión de NetBIOS es posible obtener información sobre usuarios y grupos (nombres de usuario, fecha de la última sesión, política de contraseñas, información de acceso remoto RAS), sobre el

Continúa

	sistema, y ciertas claves del registro. Toda esta información es útil para los crackers porque les ayuda a preparar un ataque contra el sistema consistente en la predicción de posibles contraseñas o simplemente la averiguación de las mismas por la fuerza bruta. Se debe deshabilitar la opción de compartir carpetas dentro de la red de la Institución, se puede plantear opciones más seguras para que la información que se necesita compartir entre funcionarios y áreas de la Institución.
Fuga de información a través de conexiones anónimas (NULL). **Si el sistema Windows permite la conexión de usuarios anónimos (usuarios sin contraseña), un atacante remoto puede obtener información, accediendo a los recursos de red y a cuentas de usuarios definidas en el sistema.**	Los equipos existentes en el Banco Nacional de Fomento, no permiten el acceso con conexiones anónimas, ya que se tiene un control de los usuarios locales, así como los usuarios del dominio. Los usuarios locales, son únicamente utilizados para activación de permisos temporales, instalaciones y demás actividades de soporte, que necesitan privilegios adicionales a los establecidos inicialmente para su correcto funcionamiento.
Contraseñas Débiles. **Con el objetivo de ofrecer compatibilidad descendente, tanto Windows NT, como Windows 2000 almacenan por omisión las contraseñas utilizando un método de cifrado de escasa calidad.** **Esta contraseña cifrada puede ser develada mediante ataques de fuerza bruta, con muy poco esfuerzo.**	El Área de Seguridad de la Información de la Gerencia de Riesgos, ha definido una política de Seguridad a nivel de contraseña de acceso, por medio del Directorio Activo (Active Directory), además de campañas de concientización para el correcto uso de contraseñas, con lo cual se trata de minimizar las brechas de seguridad existentes con el manejo de contraseñas.
Desbordamientos de memoria intermedia en servicios RPC. **Los servicios RPC permiten que un computador ejecute un programa en otro computador.** **Existen múltiples vulnerabilidades por desbordamiento de memoria intermedia en estos servicios que permiten a un intruso la realización de ataques de denegación de servicio o la obtención de privilegios de administrador.**	El Área de Infraestructura de la Gerencia de Tecnología, Las llamadas a procedimiento remoto (RPCs) hacen posible que programas que se encuentran ejecutándose en un sistema ejecuten a su vez otros programas en un segundo sistema. Este tipo se servicios son ampliamente utilizados para acceder a servicios de red tales como el compartir archivos a través de NFS o NIS. Un gran número de vulnerabilidades causadas por defectos en los RPC han sido activamente explotadas.
Vulnerabilidades en Sendmail. **Sendmail es un programa utilizado para envío, redirección y enrutamiento de e-mail.**	El Banco Nacional de Fomento, utiliza la consola de Symantec Endpoint Protection, para la verificación de correo malicioso o de dudosa procedencia, para evitar ataques por medio del

Continúa

Las versiones antiguas de este programa tienen un gran número de problemas y vulnerabilidades que permiten al intruso obtener acceso al sistema.	envío de correos electrónicos de atacantes externos que intentar vulnerar la seguridad de la red.
Vulnerabilidades en BIND (Berkeley Internet Name Domain) **El programa BIND es habitualmente utilizado para actuar como servidor de nombres de dominio (DNS).** **Algunas versiones del mismo pueden ser utilizadas para obtener acceso al sistema con privilegios de administrador.**	El Banco Nacional de Fomento, no utiliza el programa BIND para la implementación de DNS, por los varios problemas de seguridad que presenta este programa.
Comandos "R" **La familia de comandos "R" permiten a un usuario autenticado de forma local ejecutar comandos o acceder a sistemas remotos sin necesidad de volver a autenticarse.** **Las empresas habitualmente asignan a un único administrador la responsabilidad sobre docenas o incluso centenares de sistemas. Los administradores a menudo utilizan relaciones de confianza a través del uso de los comandos "r" para poder saltar de sistema en sistema convenientemente.** **Si un atacante consigue el control de cualquier máquina en la red, esta falla le permitiría acceder libremente al resto del sistema.**	El Banco Nacional de Fomento, cuenta con varios analistas que controlan los sistemas de existentes, pero no se cuenta con una normativa formal como Gerencia de Tecnología, del uso de los comandos para la administración de los sistemas para evitar ataques externos. Se debe determinar los comandos seguros que deben usar los administradores de los sistemas de la Institución, para que no sean utilizados por atacantes externos y puedan tomar control de la red.
"Daemon" del protocolo de impresión remota (LPD) **Existe una vulnerabilidad de desbordamiento de memoria intermedia en diversas versiones del "demonio de impresión" (conocido como: "daemon lpd") que puede ser utilizada por un atacante para ejecutar código arbitrario en el sistema.**	Actualmente, no se tiene ninguna contramedida implementada para contrarrestar los ataques del Demonio del protocolo de impresión remota (LPD). Se debe tener en cuenta que, sS el demonio recibe demasiados trabajos de impresión en un corto intervalo de tiempo, éste morirá o permitirá la ejecución de código arbitrario con privilegios elevados, minimizando la amenaza existente.
Sadmind y Mountd **Sadmind es un programa para administrar sistemas Solaris; Mountd, por su parte, facilita el acceso a los directorios del sistema.** **Ambos programas tienen diversos problemas de desbordamiento de memoria intermedia**	El Banco Nacional de Fomento, no cuenta con medidas de seguridad para mitigar esta vulnerabilidad. Se debe limitar la utilización de estos programas para que no puedan ser aprovechados por atacantes.

Continúa

que permiten a un atacante remoto obtener privilegios de administrador.	
Valores de SNMP por omisión. **El protocolo SNMP, es ampliamente utilizado para administrar cualquier dispositivo existente en una red, tiene mecanismos de seguridad muy débiles, siendo posible modificar fácilmente la configuración de los dispositivos conectados en red.**	Actualmente, el protocolo SNMP, es utilizado por los administradores de la red del Banco Nacional de Fomento, el cual presenta varios problemas de seguridad, por tal motivo se recomienda que se utilice otro protocolo más robusto y seguro que permita de manera adecuada la red de la Institución.

La tabla 38 muestra las vulnerabilidades más comunes, cabe indicar que al solucionarlas no se garantiza una seguridad total en la infraestructura tecnológica, pero si brindará una notable ayuda para protegerla de muchos incidentes masivos y atacantes con bajo nivel de preparación, conocidos como "script kiddies".

Las vulnerabilidades que se detallaron anteriormente, no fueron detectadas en el análisis realizado para la elaboración de este proyecto, ya que como se indicó el Banco Nacional de Fomento, ha implementado varias medidas para asegurar su infraestructura, pese a esto, existen varias vulnerabilidades todavía latentes que se pueden mitigar, siendo este el principal objetivo de este estudio.

A continuación se plantearán las diferentes contramedidas, después del escaneo realizado en el edificio Santa Prisca, donde funcionan la Casa Matriz y Sucursal Quito del Banco Nacional de Fomento.

Las contramedidas que se plantearán son para cada una de los procedimientos de escaneo que se utilizaron para realizar el presente estudio, son las siguientes:

4.1 Contramedidas para la Técnica Network Scanning

El procedimiento Network Scanning, tiene como principal objetivo, el identificar los hosts activos e inactivos dentro de una red, para que estos no sean utilizados como posibles puertas para la realización de ataques internos o externos.

Teniendo esto presente el Banco Nacional de Fomento, debe aplicar las contramedidas necesarias para minimizar los riesgos presentes.

Para lo cual se debe elaborar un inventario periódico de los activos existentes, para determinar la disminución o incremento de los activos dentro de la red del Banco Nacional de Fomento, actualmente se cuenta con una herramienta propia de la Institución, CA IT Client.

CA IT Client, es una herramienta que ofrece una visión completa de toda la base de activos de TI, utiliza una automatización completa, además posee capacidades de administración de clientes remotos para la gestión de equipos de usuarios finales, ya sean físicos o virtuales.

No importa la complejidad del entorno de TI existente, la herramienta permite agilizar las tareas operativas diarias de la organización de TI, ayudando a ejecutarlas de manera más eficiente y rentable que nunca.

Esta solución de gestión de clientes permite aumentar la eficiencia y la seguridad de los equipos de sobremesa, portátiles y servidores, la automatización de clientes basada en políticas y análisis robustos.

También unifica la administración de su entorno físico y virtual con el fin de reducir la complejidad de la gestión y mejorar la prestación de servicios.

Los principales beneficios de esta herramienta son:

- Mejorar la eficiencia mediante la automatización de los procesos operativos diarios.
- Mitigar el riesgo de mantener y asegurar los dispositivos cliente.
- Unificar la gestión de su entorno de cliente físico y virtual.

- Agilizar las iniciativas de cambio de PC, incluyendo la migración a otros sistemas operativos.
- Gestionar de forma coherente tanto sus dispositivos corporativos de propiedad, así como de propiedad del usuario. (Technologies, CA, 2015)

La herramienta CA IT Client, tiene muchos beneficios dentro de una organización, en este caso el Banco Nacional de Fomento, por tal motivo puede ser usada para la ejecución de la contramedida planteada en este estudio.

Se plantea el generar un inventario de todos los activos de la red, cada 15 días, para tener un control adecuado del incremento o disminución del campo computacional que existe en el Banco Nacional de Fomento, para realizar esta actividad, el Área de Mesa de Servicios se ayudará con la tabla, que recopila la siguiente información:

- Tipo de activo
- Usuario asignado
- Dependencia
- Nombre de equipo
- Dirección IP
- Dirección MAC
- Serial de BIOS
- Marca
- Modelo
- Sistema Operativo
- Antivirus

Tabla 39
Formato de Inventario.

Tipo de Activo	Usuario asignado	Dependencia	Nombre De Equipo	Dirección IP	Dirección MAC	Serial BIOS	Marca	Modelo	Sistema Operativo	Antivirus

Con esta información, la Gerencia de Tecnologías, estará en la capacidad de tomar decisiones adecuadas sobre aprovisionamiento de equipos de cómputo, así como implementación de nuevas y mejores políticas, que beneficien al cumplimento de los objetivos institucionales de la entidad.

4.2 Contramedidas para la Técnica Port Scanning

El procedimiento Port Scanning, permitirá obtener en primer lugar información básica acerca de qué servicios están ejecutándose en los equipos de la Institución, adicionalmente, otros detalles del entorno como qué sistema operativo está instalado en cada host o ciertas características de la arquitectura de la red.

Analizando qué puertos están abiertos en un sistema, el atacante puede buscar agujeros en cada uno de los servicios ofrecidos, cada puerto abierto en un equipo, es una potencial puerta de entrada a la misma. (Villalón Huerta, 2002).

Después del estudio realizado se detectó los siguientes puertos abiertos asociados a un servicio desconocido (Unknown), los mismos pueden ser usados por un atacante para vulnerar la seguridad de la infraestructura de la institución, por tal motivo la contramedida que se propone en este estudio es el cierre de los siguientes puertos:

Tabla 40
Contramedidas Port Scanning

Puerto	Estado	Servicio	VLAN	
			2	10
1028/tcp	Open	Unknown	X	
7920/tcp	Open	Unknown	X	
8093/tcp	Open	Unknown	X	
8099/tcp	Open	Unknown	X	
8222/tcp	Open	Unknown	X	
9081/tcp	Open	Unknown	X	
34571/tcp	Open	Unknown	X	
34572/tcp	Open	Unknown	X	
49152/tcp	Open	Unknown	X	X
49153/tcp	Open	Unknown	X	X
49154/tcp	Open	Unknown	X	X
49155/tcp	Open	Unknown	X	X
49156/tcp	Open	Unknown	X	
49157/tcp	Open	Unknown	X	
49158/tcp	Open	Unknown	X	
49159/tcp	Open	Unknown	X	X
49163/tcp	Open	Unknown	X	
49175/tcp	Open	Unknown	X	X
49176/tcp	Open	Unknown		X
50001/tcp	Open	Unknown	X	

Al aplicar esta contramedida, se puede tener un control adecuado de los puertos que utilizan las aplicaciones institucionales, con lo cual se puede minimizar los intentos para vulnerar la seguridad de la entidad, utilizando dichos puertos, mejorando así la seguridad de la red del Banco Nacional de Fomento.

4.3 Contramedidas para la Técnica Vulnerability Scanning

En la actualidad ningún sistema operativo existente es totalmente seguro y varias de estas vulnerabilidades son utilizadas por atacantes y programas maliciosos para tener acceso a los equipos de una entidad, con el fin de robar información o datos importantes, e inclusive producir fallos en los sistemas operativos.

Los fabricantes de sistemas operativos constantemente liberan actualizaciones o parches, para solucionar estos riesgos o vulnerabilidades, permitiendo a los usuarios aumentar el nivel de seguridad de los mismos.

En el capítulo anterior se detectaron varias vulnerabilidades en los sistemas operativos de los equipos de cómputo del Banco Nacional de Fomento, a continuación se detalla cada una de las contramedidas para las vulnerabilidades detectadas anteriormente.

Cada contramedida propuesta en el presente análisis se la divide en 5 partes principales, mismas que se detallan de la siguiente manera:

- ID de la vulnerabilidad identificada por el sistema GFI Languard
- Título de la vulnerabilidad
- Descripción de la vulnerabilidad
- Plataformas en donde se presenta la vulnerabilidad
- Flujo de contramedida
- Contramedida propuesta

Información tomada de http://www.security-database.com/about.php?type=about

4.3.1 Vulnerabilidad Oval:12209

4.3.1.1 Título

Vulnerabilidad de la ruta de búsqueda no fiable en Microsoft Windows Progman Group Converter

4.3.1.2 Descripción

La vulnerabilidad de la ruta de búsqueda no fiable en Microsoft Windows Progman Group Converter (grpconv.exe), permite a los usuarios locales y posiblemente atacantes remotos, ejecutar arbitrariamente código y llevar a cabo ataques de secuestro de DLL a través de un imm.dll (caballo de Troya), que se encuentra en la misma carpeta como un archivo .grp.

4.3.1.3 Plataforma

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows XP

4.3.1.4 Flujo de la Contramedida

- grpconv.exe en Microsoft Windows XP SP3
    - Microsoft Windows XP (x86) SP3 está instalado
    - Y Verificar SI la versión de grpconv.exe en Microsoft Windows XP SP3 es menor o igual a 5.1.2600.5512
- OR grpconv.exe en Microsoft Windows XP SP2
    - Microsoft Windows XP (x86) SP2 está instalado
    - Y Verificar SI la versión de grpconv.exe en Microsoft Windows XP SP2 es menor o igual a 5.1.2600.2180
- OR grpconv.exe en Microsoft Windows 2000 SP4
    - Microsoft Windows 2000 SP4 o posterior está instalado
    - Y Verificar SI la versión de grpconv.exe en Microsoft Windows 2000 SP4 es menor o igual a 5.0.2134.1
- OR grpconv.exe en Microsoft Windows server 2003 SP2
    - Microsoft Windows Server 2003 SP2 (x86) está instalado

- Y Verificar SI la versión de grpconv.exe en Microsoft Windows server 2003 SP2 es menor o igual a 5.2.3790.3959

- OR grpconv.exe en Microsoft Windows Server 2003 SP1
  - Microsoft Windows Server 2003 SP1 (x86) está instalado
  - Y Verificar SI la versión de grpconv.exe in Microsoft Windows Server 2003 SP1 es menor o igual a 5.2.3790.1830

4.3.1.5 Solución Propuesta (Código Fuente)

OR

AND grpconv.exe in Microsoft Windows XP SP3

Extended Definition oval:org.mitre.oval:def:5631

Microsoft Windows XP (x86) SP3 is installed

Criterion: Check if the version of grpconv.exe in Microsoft Windows XP SP3 is less than or equal to 5.1.2600.5512

file_test (oval:org.mitre.oval:tst:41692) check_existence = at_least_one_exists, check = all

file_object oval:org.mitre.oval:obj:307

path var_ref= oval:org.mitre.oval:var:200 | var_check=all |

filename grpconv.exe

file_state oval:org.mitre.oval:ste:11851

version datatype=version | operation=less than or equal | value=5.1.2600.5512

AND grpconv.exe in Microsoft Windows XP SP2

Extended Definition oval:org.mitre.oval:def:754

Microsoft Windows XP (x86) SP2 is installed

Criterion: Check if the version of grpconv.exe in Microsoft Windows XP SP2 is less than or equal to 5.1.2600.2180

file_test (oval:org.mitre.oval:tst:41681) check_existence = at_least_one_exists, check = all

file_object oval:org.mitre.oval:obj:307

path var_ref= oval:org.mitre.oval:var:200 | var_check=all |

filename grpconv.exe

file_state oval:org.mitre.oval:ste:11203

version datatype=version | operation=less than or equal | value=5.1.2600.2180

AND grpconv.exe in Microsoft Windows 2000 SP4

Extended Definition oval:org.mitre.oval:def:229

Microsoft Windows 2000 SP4 or later is installed

Criterion: Check if the version of grpconv.exe in Microsoft Windows 2000 SP4 is less than or equal to 5.0.2134.1

file_test (oval:org.mitre.oval:tst:41132) check_existence = at_least_one_exists, check = all

file_object oval:org.mitre.oval:obj:307

path var_ref= oval:org.mitre.oval:var:200 | var_check=all |

filename grpconv.exe

file_state oval:org.mitre.oval:ste:11007

version datatype=version | operation=less than or equal | value=5.0.2134.1

AND grpconv.exe in Microsoft Windows server 2003 SP2

Extended Definition oval:org.mitre.oval:def:1935

Microsoft Windows Server 2003 SP2 (x86) is installed

Criterion: Check if the version of grpconv.exe in Microsoft Windows server 2003 SP2 is less than or equal to 5.2.3790.3959

Windows : File

[[value of ${{windows:registry_object:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion : SystemRoot}}]]\System32\grpconv**.exe**

4.3.2 Vulnerabilidad Oval:12215

4.3.2.1 Título

Vulnerabilidad de recuento de la referencia Win32k

4.3.2.2 Descripción

La vulnerabilidad se presenta en los controladores en modo kernel de Microsoft Windows Vista SP1 y SP2 y Server 2008 SP2 Gold y permite a usuarios locales conseguir privilegios o causar una denegación de servicio (caída del sistema), mediante el uso de un gran número de llamadas a la función NtUserCheckAccessForIntegrityLevel para desencadenar un fallo en el Función LockProcessByClientId , dando lugar a la eliminación de un objeto de proceso en uso, también conocido como " Vulnerabilidad de recuento de la referencia Win32k".

4.3.2.3 Plataforma

- Microsoft Windows Vista
- Microsoft Windows Server 2008

4.3.2.4 Flujo de la Contramedida

- Sistema Operativo Vulnerable Microsoft Windows Vista SP1 x86/x64, Server 2008 32bit/x64/ia64
    - Microsoft Windows Vista SP1 x86/x64, Server 2008 32bit/x64/ia64
        - Microsoft Windows Vista (32-bit) Service Pack 1 está instalado
        - Y Microsoft Windows Server 2008 (32-bit) está instalado
        - Y Microsoft Windows Vista x64 Edition Service Pack 1 está instalado

        - Y Microsoft Windows Server 2008 (64-bit) está instalado
        - Y Microsoft Windows Server 2008 (ia-64) está instalado
    - Y Tipo de Servicio GDR o LDR
        - la versión de win32k.sys es menor que 6.0.6001.18523
        - O LDR
            - la versión de win32k.sys es menor que 6.0.6001.22754
            - Y la versión de win32k.sys es mayor que 6.0.6001.22000
- **O** Sistema Operativo Vulnerable Microsoft Windows Vista SP2 x86/x64, Server 2008 SP2 32bit/x64/ia64
    - Windows Vista SP2 x86/x64, Server 2008 SP2 32bit/x64/ia64
        - Microsoft Windows Vista (32-bit) Service Pack 2 está instalado
        - Y Microsoft Windows Server 2008 x64 Edition Service Pack 2 está instalado
        - Y Microsoft Windows Server 2008 (32-bit) Service Pack 2 está instalado
        - Y Microsoft Windows Vista x64 Edition Service Pack 2 está instalado
        - Y Microsoft Windows Server 2008 Itanium-Based Edition Service Pack 2 está instalado
    - Y Tipo de Servicio GDR or LDR
        - la versión de win32k.sys es menor que 6.0.6002.18305
        - O LDR
            - la versión de win32k.sys es menor que 6.0.6002.22478
            - Y la versión de win32k.sys es mayor que 6.0.6002.22000

4.3.2.5 Solucion propuesta (Código fuente)

OR

AND Vulnerable Microsoft Windows Vista SP1 x86/x64, Server 2008 32bit/x64/ia64

OR Microsoft Windows Vista SP1 x86/x64, Server 2008 32bit/x64/ia64

Extended Definition oval:org.mitre.oval:def:4873

Microsoft Windows Vista (32-bit) Service Pack 1 is installed

Extended Definition oval:org.mitre.oval:def:4870

Microsoft Windows Server 2008 (32-bit) is installed

Extended Definition oval:org.mitre.oval:def:5254

Microsoft Windows Vista x64 Edition Service Pack 1 is installed

Extended Definition oval:org.mitre.oval:def:5356

Microsoft Windows Server 2008 (64-bit) is installed

Extended Definition oval:org.mitre.oval:def:5667

Microsoft Windows Server 2008 (ia-64) is installed

OR GDR or LDR Service branch

Criterion: the version of win32k.sys is less than 6.0.6001.18523

file_test (oval:org.mitre.oval:tst:11810) check_existence = at_least_one_exists, check = at least one

file_object oval:org.mitre.oval:obj:570

path var_ref= oval:org.mitre.oval:var:200 | var_check=all |

filename win32k.sys

file_state oval:org.mitre.oval:ste:7411

version datatype=version | operation=less than | value=6.0.6001.18523

AND LDR

Criterion: the version of win32k.sys is less than 6.0.6001.22754

file_test (oval:org.mitre.oval:tst:11488) check_existence = at_least_one_exists, check = at least one

file_object oval:org.mitre.oval:obj:570

path var_ref= oval:org.mitre.oval:var:200 | var_check=all |

filename win32k.sys

file_state oval:org.mitre.oval:ste:7224

version datatype=version | operation=less than | value=6.0.6001.22754

Criterion: the version of win32k.sys is greater than 6.0.6001.22000

file_test (oval:org.mitre.oval:tst:10142) check_existence = at_least_one_exists, check = at least one

file_object oval:org.mitre.oval:obj:570

path var_ref= oval:org.mitre.oval:var:200 | var_check=all |

filename win32k.sys

file_state oval:org.mitre.oval:ste:4525

version datatype=version | operation=greater than or equal | value=6.0.6001.22000

AND Vulnerable Microsoft Windows Vista SP2 x86/x64, Server 2008 SP2 32bit/x64/ia64

OR Windows Vista SP2 x86/x64, Server 2008 SP2 32bit/x64/ia64

4.3.3 Vulnerabilidad oval:12219

4.3.3.1 Título

Vulnerabilidad de la ruta de búsqueda no fiable en Microsoft Windows Office PowerPoint 2007

4.3.3.2 Descripción

Permite a los usuarios locales y posiblemente atacantes remotos ejecutar código arbitrario y llevar a cabo ataques de secuestro de DLLs a través de un

Rpawinet.dll (caballo de Troya) que se encuentra en la misma carpeta que un archivo con extensión .odp, .pothtml, .potm, .potx , .ppa, .ppam, .pps, .ppt, .ppthtml, .pptm, .pptxml, .pwz, .sldm, .sldx y .thmx.

4.3.3.3 Plataforma

- Microsoft Windows 2000
- Microsoft Windows 7
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows XP

4.3.3.4 Flujo de la Contramedida

- PowerPoint 2007 está instalado
- Y la versión de powerpnt.exe es mayor o igual al 12.0.0.0
- Y la versión de powerpnt.exe es menor a 13.0.0.0

4.3.3.5 Solución Propuesta (Código Fuente)

AND

Extended Definition oval:org.mitre.oval:def:5937

Microsoft PowerPoint 2007 is installed

4.3.4 Vulnerabilidad oval12689

4.3.4.1 Título

Vulnerabilidad en portada de fax Windows Page Editor

4.3.4.2 Descripción

Desbordamiento de búfer de la pila basado en la función en CDrawPoly. Al serializar la función fxscover.exe en Microsoft Windows Servicio de Editor de portadas de fax 5.2 r2 en Windows XP Professional SP3, Server 2003 R2 Enterprise Edition SP2 y Windows 7 Professional, permite a atacantes remotos ejecutar código arbitrario a través de un largo historial en un archivo (.cov) de portadas de fax.

Las vulnerabilidades podrían permitir la ejecución remota de código si un usuario abre un archivo de portada de fax especialmente diseñado (.cov) utilizando el Editor de portadas de fax de Windows. Un atacante que aprovechara cualquiera de estas vulnerabilidades podría conseguir el mismo nivel de derechos de usuario que el usuario ha iniciado la sesión. Los usuarios cuyas cuentas estén configuradas con pocos derechos de usuario en el sistema correrían un riesgo menor que aquellos que cuenten con derechos de usuario administrativos.

NOTA: Algunos de estos detalles han sido obtenidos de información de terceros.

4.3.4.3 Plataforma

- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows Vista
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows 7

4.3.4.4 Flujo de la Contramedida

- Sistema Operativo Vulnerable Microsoft Windows XP (x86) SP3
    - Microsoft Windows XP (x86) SP3 está instalado
    - Y Mfc42.dll o Fxscover.exe
        - la versión de Mfc42.dll es menor a 6.2.8081.0
        - Y la versión de Fxscover.exe es menor a 5.2.2600.6078
- O Sistema Operativo Vulnerable Microsoft Windows XP x64 SP2, Server 2003 x64/ia64 SP2
    - Sistema Operativo Vulnerable Microsoft Windows XP x64 SP2, Server 2003 x64/ia64 SP2
        - Microsoft Windows XP x64 Edition SP2 está instalado
        - Y Microsoft Windows Server 2003 SP2 (x64) está instalado
        - Y Microsoft Windows Server 2003 (ia64) SP2 está instalado
    - Y Mfc42.dll o Fxscover.exe
        - la versión de Mfc42.dll es menor a 6.5.9151.0
        - Y la versión de Fxscover.exe es menor a 5.2.3790.4829
- O Sistema Operativo Vulnerable Microsoft Server 2003 x86 SP2
    - Microsoft Windows Server 2003 SP2 (x86) está instalado
    - Y Mfc42.dll o Fxscover.exe
        - la versión de Mfc42.dll es menor a 6.6.8064.0
        - Y la versión de Fxscover.exe es menor a 5.2.3790.4829
- O Sistema Operativo Vulnerable Microsoft Windows Vista SP1 x86/x64, Server 2008 32bit/x64/ia64
    - Sistema Operativo Vulnerable Microsoft Windows Vista SP1 x86/x64, Server 2008 32bit/x64/ia64
        - Microsoft Windows Vista (32-bit) Service Pack 1 está instalado
        - Y Microsoft Windows Vista x64 Edition Service Pack 1 está instalado
        - Y Microsoft Windows Server 2008 (32-bit) está instalado

        - Y Microsoft Windows Server 2008 (64-bit) está instalado
        - Y Microsoft Windows Server 2008 (ia-64) está instalado
    - Y Tipo de servicio Mfc42.dll o Fxscover.exe - GDR o LDR
        - la versión de Fxscover.exe es menor a 6.0.6001.18597
        - O LDR
            - la versión de Fxscover.exe es mayor o igual a 6.0.6001.22000
            - Y la versión de Fxscover.exe es menor a 6.0.6001.22852
        - Y la versión de Mfc42.dll es menor a 6.6.8064.0
- O Sistema Operativo Vulnerable Microsoft Windows Vista SP2 x86/x64, Server 2008 SP2 32bit/x64/ia64
    - Sistema Operativo Vulnerable Microsoft Windows Vista SP2 x86/x64, Server 2008 SP2 32bit/x64/ia64
        - Microsoft Windows Vista (32-bit) Service Pack 2 está instalado
        - Y Microsoft Windows Vista x64 Edition Service Pack 2 está instalado
        - Y Microsoft Windows Server 2008 (32-bit) Service Pack 2 está instalado
        - Y Microsoft Windows Server 2008 x64 Edition Service Pack 2 está instalado
        - Y Microsoft Windows Server 2008 Itanium-Based Edition Service Pack 2 está instalado
    - Y Tipo de servicio Mfc42.dll o Fxscover.exe - GDR o LDR
        - la versión de Fxscover.exe es menor a 6.0.6002.18403
        - O LDR
            - la versión de Fxscover.exe es mayor o igual a 6.0.6002.22000

        - Y la versión de Fxscover.exe es menor a 6.0.6002.22586
    - Y la versión de Mfc42.dll es menor a 6.6.8064.0
- O Sistema Operativo Vulnerable Microsoft Windows 7 x86/x64, Windows Server 2008 R2 x86/x64/ia64
    - Sistema Operativo Vulnerable Microsoft Windows 7 x86/x64, Windows Server 2008 R2 x86/x64/ia64
        - Microsoft Windows 7 (32-bit) está instalado
        - Y Microsoft Windows 7 x64 Edition está instalado
        - Y Microsoft Windows Server 2008 R2 x64 Edition está instalado
        - Y Microsoft Windows Server 2008 R2 Itanium-Based Edition está instalado
    - Y Tipo de servicio Mfc42.dll o Fxscover.exe - GDR o LDR
        - la versión de Fxscover.exe es menor a 6.1.7600.16759
        - O LDR
            - la versión de Fxscover.exe es mayor o igual a 6.1.7600.20000
            - Y la versión de Fxscover.exe es menor a 6.1.7600.20900
        - Y la versión de Mfc42.dll es menor a 6.6.8064.0
- O Sistema Operativo Vulnerable Microsoft Windows 7 x86/x64 SP1, Windows Server 2008 R2 x64 SP1
    - Sistema Operativo Vulnerable Microsoft Windows 7 x86/x64 SP1, Windows Server 2008 R2 x64 SP1
        - Microsoft Windows 7 (32-bit) Service Pack 1 está instalado
        - Y Microsoft Windows 7 x64 Service Pack 1 está instalado
        - Y Microsoft Windows Server 2008 R2 x64 Service Pack 1 está instalado

- Y Microsoft Windows Server 2008 R2 Itanium-Based Edition Service Pack 1 está instalado
  - Y Tipo de servicio Mfc42.dll o Fxscover.exe - GDR o LDR
    - la versión de Fxscover.exe es menor a 6.1.7601.17559
    - O LDR
      - la versión de Fxscover.exe es mayor o igual a 6.1.7601.21000
      - Y la versión de Fxscover.exe es menor a 6.1.7601.21659
    - Y la versión de Mfc42.dll es menor a 6.6.8064.0

4.3.4.5 Solución Propuesta (Código Fuente)

OR

AND Vulnerable Microsoft Windows XP (x86) SP3

Extended Definition oval:org.mitre.oval:def:5631

Microsoft Windows XP (x86) SP3 is installed

OR Mfc42.dll or Fxscover.exe

Criterion: the version of Mfc42.dll is less than 6.2.8081.0

file_test (oval:org.mitre.oval:tst:42290) check_existence = at_least_one_exists, check = at least one

file_object oval:org.mitre.oval:obj:15905

path var_ref= oval:org.mitre.oval:var:200 | var_check=all |

filename Mfc42.dll

file_state oval:org.mitre.oval:ste:11870

version datatype=version | operation=less than | value=6.2.8081.0

Criterion: the version of Fxscover.exe is less than 5.2.2600.6078

file_test (oval:org.mitre.oval:tst:42169) check_existence = at_least_one_exists, check = at least one

file_object oval:org.mitre.oval:obj:15173
path var_ref= oval:org.mitre.oval:var:200 | var_check=all |
filename Fxscover.exe
file_state oval:org.mitre.oval:ste:12454
version datatype=version | operation=less than | value=5.2.2600.6078

AND Vulnerable Microsoft Windows XP x64 SP2, Server 2003 x64/ia64 SP2

OR Vulnerable Microsoft Windows XP x64 SP2, Server 2003 x64/ia64 SP2

Extended Definition oval:org.mitre.oval:def:4193
Microsoft Windows XP x64 Edition SP2 is installed

Extended Definition oval:org.mitre.oval:def:2161
Microsoft Windows Server 2003 SP2 (x64) is installed

Extended Definition oval:org.mitre.oval:def:1442
Microsoft Windows Server 2003 (ia64) SP2 is installed

OR Mfc42.dll or Fxscover.exe

Criterion: the version of Mfc42.dll is less than 6.5.9151.0
file_test (oval:org.mitre.oval:tst:42593) check_existence = at_least_one_exists, check = at least one

file_object oval:org.mitre.oval:obj:15905

4.3.5 Vulnerabilidad oval:13205

4.3.5.1 Título

Las versiones posteriores a 10.2.152.26 de Adobe Flash Player, permite a los atacantes ejecutar código arbitrario o causar una denegación de servicio (corrupción de memoria) a través de vectores no especificados, relacionados con un constructor de un objeto ActionScript3 no especificado y comprobación de tipos inadecuada, una vulnerabilidad diferente a CVE - 2011-0559, CVE - 2011-0560, CVE - 2011-0561, CVE - 2011-0571, CVE - 2011-0572, CVE - 2011-0573, CVE - 2011-0574, CVE - 2011-0607 y CVE - 2011 a 0608.

4.3.5.2 Descripción

Las versiones posteriores a 10.2.152.26 de Adobe Flash Player, permite a los atacantes ejecutar código arbitrario o causar una denegación de servicio (corrupción de memoria) a través de vectores no especificados, relacionados con un constructor de un objeto ActionScript3 no especificado y comprobación de tipos inadecuada, una vulnerabilidad diferente a CVE - 2011-0559, CVE - 2011-0560, CVE - 2011-0561, CVE - 2011-0571, CVE - 2011-0572, CVE - 2011-0573, CVE - 2011-0574, CVE - 2011-0607 y CVE - 2011 a 0608.

4.3.5.3 Plataforma

- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows Server 2003
- Microsoft Windows XP
- Microsoft Windows 2000

4.3.5.4 Flujo de la Contramedida

- Determine **SI** la versión de Adobe Flash Player es menor o igual a 9.125.0
    - Adobe Flash Player 9 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0
- O Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
- O Determine SI la versión de Adobe Flash Player es menor o igual a 10.2.152
    - Adobe Flash Player 10 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 10.2.152
- O Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
- O Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
- Y Determine SI la versión deFlash.ocx es menor o igual a 9.125.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 7.2
- Y Determine SI la versión deFlash.ocx es menor o igual a 10.2.152
- Y Determine SI la versión deFlash.ocx es menor o igual a 8.0.42.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 6.0.79

4.3.5.5 Solución Propuesta (Código Fuente)

OR

AND Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

Extended Definition oval:org.mitre.oval:def:7402

Adobe Flash Player 9 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

registry_test (oval:org.mitre.oval:tst:77132) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174

oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18021

value datatype=version | operation=less than or equal | value=9.125.0

AND Determine if the version of Adobe Flash Player is less than or equal to 7.2

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 7.2

registry_test (oval:org.mitre.oval:tst:77458) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174

oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17714

value datatype=version | operation=less than or equal | value=7.2

AND Determine if the version of Adobe Flash Player is less than or equal to 10.2.152

Extended Definition oval:org.mitre.oval:def:7610

Adobe Flash Player 10 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 10.2.152

registry_test (oval:org.mitre.oval:tst:77543) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174

oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18042

value datatype=version | operation=less than or equal | value=10.2.152

AND Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

registry_test (oval:org.mitre.oval:tst:77303) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174

oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17719

value datatype=version | operation=less than or equal | value=8.0.42.0

AND Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

registry_test (oval:org.mitre.oval:tst:77137) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174

oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18154

value datatype=version | operation=less than or equal | value=6.0.79

4.3.6 Vulnerabilidad oval:13294

4.3.6.1 Título

La versión 9.0.289.0 y anteriores a la versión 10.x y 10.1.102.64 de Adobe Flash Player en Windows, Mac OS X, Linux, Solaris y 10.1.95.1 en Android y authplay.dll (alias AuthPlayLib.bundle o libauthplay.so.0.0.0) en Adobe Reader y Acrobat 9.x y 9.4, permiten a atacantes remotos ejecutar código arbitrario o causar una denegación de servicio (corrupción de memoria y caída de aplicación) a través de contenido SWF diseñado, fueron explotados en octubre de 2010.

4.3.6.2 Descripción

La versión 9.0.289.0 y anteriores a la versión 10.x y 10.1.102.64 de Adobe Flash Player en Windows, Mac OS X, Linux y Solaris y 10.1.95.1 en Android, y authplay.dll (alias AuthPlayLib.bundle o libauthplay.so.0.0.0) en Adobe Reader y Acrobat 9.x y 9.4, permiten a atacantes remotos ejecutar código arbitrario o causar una denegación de servicio (corrupción de memoria y caída de aplicación) a través de contenido SWF diseñado, fueron explotados en octubre de 2010.

4.3.6.3 Plataforma

- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows Server 2003
- Microsoft Windows XP
- Microsoft Windows 2000

4.3.6.4 Flujo de la Contramedida

- Determine **SI** la versión de Adobe Flash Player es menor o igual a 9.125.0 **Y** es mayor o igual a 9.0.16
    - Adobe Flash Player 9 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0
    - Y Determine SI la versión de Adobe Flash Player es mayor o igual a 9.0.16
- O Determine SI la versión de Adobe Flash Player es menor o igual a 10.1.95.2 Y es mayor o igual a 10.0.0.584
    - Adobe Flash Player 10 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 10.1.95.2
    - Y Determine SI la versión de Adobe Flash Player es mayor o igual a 10.0.0.584
- O Determine SI la versión de Adobe Acrobat es menor o igual a 9.4 Y es mayor o igual a 9.0
    - Adobe Acrobat 9 Series está instalado
    - Y Determine SI la versión de Adobe Acrobat es menor o igual a 9.4
    - Y Determine SI la versión de Adobe Acrobat es mayor o igual a 9.0

- O Determine SI la versión de Adobe Flash Player es menor o igual a 7.2 Y es mayor o igual a 7.0.1
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
    - Y Determine SI la versión de Adobe Flash Player es mayor o igual a 7.0.1
- O Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0 Y es mayor o igual a 8.0.22.0
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
    - Y Determine SI la versión de Adobe Flash Player es mayor o igual a 8.0.22.0
- O Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79 Y es mayor o igual a 6.0.21.0
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
    - Y Determine SI la versión de Adobe Flash Player es mayor o igual a 6.0.21.0
- O Determine SI la versión de Adobe Reader es menor o igual a 9.4 Y es mayor o igual a 9.0
    - Adobe Reader 9 Series está instalado
    - Y Determine SI la versión de Adobe Reader es menor o igual a 9.4
    - Y Determine SI la versión de Adobe Reader es mayor o igual a 9.0
- O Sección Flash.ocx 9
    - Determine SI la versión deFlash.ocx es menor o igual a 9.125.0
    - Y Determine SI la versión deFlash.ocx es mayor o igual a 9.0.16
- O Sección Flash.ocx 10

- Determine SI la versión deFlash.ocx es menor o igual a 10.1.95.2
- Y Determine SI la versión deFlash.ocx es mayor o igual a 10.0.0.584

- O Sección Flash.ocx 7
  - Determine SI la versión deFlash.ocx es menor o igual a 7.2
  - Y Determine SI la versión deFlash.ocx es mayor o igual a 7.0.1
- O Sección Flash.ocx 8
  - Determine SI la versión deFlash.ocx es menor o igual a 8.0.42.0
  - Y Determine SI la versión deFlash.ocx es mayor o igual a 8.0.22.0
- O Sección Flash.ocx 6
  - Determine SI la versión deFlash.ocx es menor o igual a 6.0.79
  - Y Determine SI la versión deFlash.ocx es mayor o igual a 6.0.21.0

4.3.6.5 Solución Propuesta (Código Fuente)

OR

AND Determine if the version of Adobe Flash Player is less than or equal to 9.125.0 and is greater than or equal to 9.0.16

Extended Definition oval:org.mitre.oval:def:7402

Adobe Flash Player 9 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

registry_test (oval:org.mitre.oval:tst:77132) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18021

value datatype=version | operation=less than or equal | value=9.125.0

Criterion: Determine if the version of Adobe Flash Player is greater than or equal to 9.0.16

registry_test (oval:org.mitre.oval:tst:76670) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18231

value datatype=version | operation=greater than or equal | value=9.0.16

AND Determine if the version of Adobe Flash Player is less than or equal to 10.1.95.2 and is greater than or equal to 10.0.0.584

Extended Definition oval:org.mitre.oval:def:7610

Adobe Flash Player 10 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 10.1.95.2

registry_test (oval:org.mitre.oval:tst:77607) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18192

value datatype=version | operation=less than or equal | value=10.1.95.2

Criterion: Determine if the version of Adobe Flash Player is greater than or equal to 10.0.0.584

registry_test (oval:org.mitre.oval:tst:77490) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17448

value datatype=version | operation=greater than or equal | value=10.0.0.584

AND Determine if the version of Adobe Acrobat is less than or equal to 9.4 and is greater than or equal to 9.0

Extended Definition oval:org.mitre.oval:def:6013

Adobe Acrobat 9 Series is installed

Criterion: Determine if the version of Adobe Acrobat is less than or equal to 9.4

registry_test (oval:org.mitre.oval:tst:77227) check_existence = at_least_one_exists, check = all

registry_object oval:org.mitre.oval:obj:7189

behaviors windows_view=32_bit |

4.3.7 Vulnerabilidad oval:13429

4.3.7.1 Título

La versiones anteriores a 10.2.152.26 de Adobe Flash Player, permiten a los atacantes ejecutar código arbitrario o causar una denegación de servicio (corrupción de memoria) a través de vectores no especificados, una diferente vulnerabilidad a CVE - 2011-0559, CVE - 2011-0561, CVE - 2011-0571, CVE - 2011-0572, CVE - 2011-0573, CVE - 2011-0574, CVE - 2011-0578, CVE - 2011-0607 y CVE - 2011-0608.

4.3.7.2 Descripción

La versiones anteriores a 10.2.152.26 de Adobe Flash Player, permiten a los atacantes ejecutar código arbitrario o causar una denegación de servicio (corrupción de memoria) a través de vectores no especificados, una diferente vulnerabilidad a CVE

- 2011-0559, CVE - 2011-0561, CVE - 2011-0571, CVE - 2011-0572, CVE - 2011-0573, CVE - 2011-0574, CVE - 2011-0578, CVE - 2011-0607 y CVE - 2011-0608.

4.3.7.3 Plataforma

- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows Server 2003
- Microsoft Windows XP
- Microsoft Windows 2000

4.3.7.4 Flijo de la Contramedida

- Determine **SI** la versión de Adobe Flash Player es menor o igual a 9.125.0
    - Adobe Flash Player 9 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0
- O Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
- O Determine SI la versión de Adobe Flash Player es menor o igual a 10.2.152
    - Adobe Flash Player 10 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 10.2.152
- O Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0

- O Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
- Y Determine SI la versión deFlash.ocx es menor o igual a 9.125.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 7.2
- Y Determine SI la versión deFlash.ocx es menor o igual a 10.2.152
- Y Determine SI la versión deFlash.ocx es menor o igual a 8.0.42.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 6.0.79

4.3.7.5 Solución Propuesta (Código Fuente)

OR

AND Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

Extended Definition oval:org.mitre.oval:def:7402

Adobe Flash Player 9 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

registry_test (oval:org.mitre.oval:tst:77132) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18021

value datatype=version | operation=less than or equal | value=9.125.0

AND Determine if the version of Adobe Flash Player is less than or equal to 7.2

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 7.2

registry_test (oval:org.mitre.oval:tst:77458) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17714

value datatype=version | operation=less than or equal | value=7.2

AND Determine if the version of Adobe Flash Player is less than or equal to 10.2.152

Extended Definition oval:org.mitre.oval:def:7610

Adobe Flash Player 10 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 10.2.152

registry_test (oval:org.mitre.oval:tst:77543) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18042

value datatype=version | operation=less than or equal | value=10.2.152

AND Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

registry_test (oval:org.mitre.oval:tst:77303) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17719

value datatype=version | operation=less than or equal | value=8.0.42.0

AND Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

registry_test (oval:org.mitre.oval:tst:77137) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18154

value datatype=version | operation=less than or equal | value=6.0.79

4.3.8 Vulnerabilidad oval:13809

4.3.8.1 Título

La versiones anteriores a 10.3.183.10 de Adobe Flash Player en Windows, Mac OS X, Linux y Solaris y anteriores a 10.3.186.7 en Android, permiten a atacantes

remotos ejecutar código arbitrario a través de streaming media manipulada, relacionado con una "vulnerabilidad de error lógico".

4.3.8.2 Descripción

La versiones anteriores a 10.3.183.10 de Adobe Flash Player en Windows, Mac OS X, Linux y Solaris y anteriores a 10.3.186.7 en Android, permiten a atacantes remotos ejecutar código arbitrario a través de streaming media manipulada, relacionado con una "vulnerabilidad de error lógico".

4.3.8.3 Plataforma

- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows Server 2003
- Microsoft Windows XP
- Microsoft Windows 2000

4.3.8.4 Flujo de la Contramedida

- Determine **SI** la versión de Adobe Flash Player en Windows es menor o igual a 10.3.183.7
    - Adobe Flash Player 10 está instalado
    - Y Determine SI la versión de Adobe Flash Player en Windows es menor o igual a 10.3.183.7
- O Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0
    - Adobe Flash Player 9 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0

- O Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
- O Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
- O Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 10.3.183.7
- Y Determine SI la versión deFlash.ocx es menor o igual a 9.125.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 7.2
- Y Determine SI la versión deFlash.ocx es menor o igual a 6.0.79
- Y Determine SI la versión deFlash.ocx es menor o igual a 8.0.42.0

4.3.8.5 Solución Propuesta (Código Fuente)

OR

AND Determine if the version of Adobe Flash Player on Windows is less than or equal to 10.3.183.7

Extended Definition oval:org.mitre.oval:def:7610

Adobe Flash Player 10 is installed

Criterion: Determine if the version of Adobe Flash Player on Windows is less than or equal to 10.3.183.7

registry_test (oval:org.mitre.oval:tst:77559) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17833

value datatype=version | operation=less than or equal | value=10.3.183.7

AND Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

Extended Definition oval:org.mitre.oval:def:7402

Adobe Flash Player 9 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

registry_test (oval:org.mitre.oval:tst:77132) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18021

value datatype=version | operation=less than or equal | value=9.125.0

AND Determine if the version of Adobe Flash Player is less than or equal to 7.2

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 7.2

registry_test (oval:org.mitre.oval:tst:77458) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17714

value datatype=version | operation=less than or equal | value=7.2

AND Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

registry_test (oval:org.mitre.oval:tst:77137) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18154

value datatype=version | operation=less than or equal | value=6.0.79

AND Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

Extended Definition oval:org.mitre.oval:def:6700

4.3.9 Vulnerabilidad oval:13832

4.3.9.1 Título

Las versiones anteriores a 10.3.181.14 de Adobe Flash Player en Windows, Mac OS X, Linux y Solaris y versiones anteriores a 10.3.185.21 en Android, permiten a los atacantes ejecutar código arbitrario o causar una denegación de servicio (corrupción de memoria) a través de vectores no especificados, una vulnerabilidad diferente de CVE -2011-0619, CVE - 2011-0621 y CVE - 2011-0.622.

4.3.9.2 Descripción

Las versiones anteriores a 10.3.181.14 de Adobe Flash Player en Windows, Mac OS X, Linux y Solaris y versiones anteriores a 10.3.185.21 en Android, permiten a los atacantes ejecutar código arbitrario o causar una denegación de servicio (corrupción de memoria) a través de vectores no especificados, una vulnerabilidad diferente de CVE -2011-0619, CVE - 2011-0621 y CVE - 2011-0.622.

4.3.9.3 Plataforma

- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows Server 2003
- Microsoft Windows XP
- Microsoft Windows 2000

4.3.9.4 Flujo de la Contramedida

- Determine **SI** la versión de Adobe Flash Player es menor o igual a 10.2.159.1
    - Adobe Flash Player 10 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 10.2.159.1
- O Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0
    - Adobe Flash Player 9 está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0
- O Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 7.2

- O Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
- O Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
- Y Determine SI la versión deFlash.ocx es menor o igual a 10.2.159.1
- Y Determine SI la versión deFlash.ocx es menor o igual a 9.125.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 7.2
- Y Determine SI la versión deFlash.ocx es menor o igual a 8.0.42.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 6.0.79

4.3.9.5 Solución Propuesta (Código Fuente)

OR

AND Determine if the version of Adobe Flash Player is less than or equal to 10.2.159.1

Extended Definition oval:org.mitre.oval:def:7610

Adobe Flash Player 10 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 10.2.159.1

registry_test (oval:org.mitre.oval:tst:76904) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17734

value datatype=version | operation=less than or equal | value=10.2.159.1

AND Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

Extended Definition oval:org.mitre.oval:def:7402

Adobe Flash Player 9 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

registry_test (oval:org.mitre.oval:tst:77132) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18021

value datatype=version | operation=less than or equal | value=9.125.0

AND Determine if the version of Adobe Flash Player is less than or equal to 7.2

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 7.2

registry_test (oval:org.mitre.oval:tst:77458) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17714

value datatype=version | operation=less than or equal | value=7.2

AND Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

registry_test (oval:org.mitre.oval:tst:77303) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17719

value datatype=version | operation=less than or equal | value=8.0.42.0

AND Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

Extended Definition oval:org.mitre.oval:def:6700

4.3.10 Vulnerabilidad oval:13901

4.3.10.1 Título

Las versiones anteriores a 10.3.181.14 de Adobe Flash Player en Windows, Mac OS X, Linux y Solaris y versiones anteriores a 10.3.185.21 en Android, permiten a los atacantes ejecutar código arbitrario a través de vectores no especificados, relacionados con un problema de "comprobación de límites", una vulnerabilidad diferente a CVE- 2011-0624, CVE - 2011-0625 y CVE - 2011-0626.

4.3.10.2 Descripción

Las versiones anteriores a 10.3.181.14 de Adobe Flash Player en Windows, Mac OS X, Linux y Solaris y versiones anteriores a 10.3.185.21 en Android, permiten

a los atacantes ejecutar código arbitrario a través de vectores no especificados, relacionados con un problema de "comprobación de límites", una vulnerabilidad diferente a CVE- 2011-0624, CVE - 2011-0625 y CVE - 2011-0626.

4.3.10.3 Plataforma

- Microsoft Windows 7
- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows Server 2003
- Microsoft Windows XP
- Microsoft Windows 2000

4.3.10.4 Flujo de la Contramedida

- Determine **SI** la versión de Adobe Flash Player es menor o igual a 10.2.159.1
  - Adobe Flash Player 10 está instalado
  - Y Determine SI la versión de Adobe Flash Player es menor o igual a 10.2.159.1
- O Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0
  - Adobe Flash Player 9 está instalado
  - Y Determine SI la versión de Adobe Flash Player es menor o igual a 9.125.0
- O Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
  - Adobe Flash Player está instalado
  - Y Determine SI la versión de Adobe Flash Player es menor o igual a 7.2
- O Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
  - Adobe Flash Player está instalado

    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 8.0.42.0
- O Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
    - Adobe Flash Player está instalado
    - Y Determine SI la versión de Adobe Flash Player es menor o igual a 6.0.79
- Y Determine SI la versión deFlash.ocx es menor o igual a 10.2.159.1
- Y Determine SI la versión deFlash.ocx es menor o igual a 9.125.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 7.2
- Y Determine SI la versión deFlash.ocx es menor o igual a 8.0.42.0
- Y Determine SI la versión deFlash.ocx es menor o igual a 6.0.79

4.3.10.5 Solución Propuesta (Código Fuente)

OR

AND Determine if the version of Adobe Flash Player is less than or equal to 10.2.159.1

Extended Definition oval:org.mitre.oval:def:7610

Adobe Flash Player 10 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 10.2.159.1

registry_test (oval:org.mitre.oval:tst:76904) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 | value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17734

value datatype=version | operation=less than or equal | value=10.2.159.1

AND Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

Extended Definition oval:org.mitre.oval:def:7402

Adobe Flash Player 9 is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 9.125.0

registry_test (oval:org.mitre.oval:tst:77132) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18021

value datatype=version | operation=less than or equal | value=9.125.0

AND Determine if the version of Adobe Flash Player is less than or equal to 7.2

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 7.2

registry_test (oval:org.mitre.oval:tst:77458) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17714

value datatype=version | operation=less than or equal | value=7.2

AND Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 8.0.42.0

registry_test (oval:org.mitre.oval:tst:77303) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:17719

value datatype=version | operation=less than or equal | value=8.0.42.0

AND Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

Extended Definition oval:org.mitre.oval:def:6700

Adobe Flash Player is installed

Criterion: Determine if the version of Adobe Flash Player is less than or equal to 6.0.79

registry_test (oval:org.mitre.oval:tst:77137) check_existence = at_least_one_exists, check = at least one

registry_object oval:org.mitre.oval:obj:7290

set xmlns=http://oval.mitre.org/XMLSchema/oval-definitions-5 |

value=oval:org.mitre.oval:obj:27479oval:org.mitre.oval:obj:27174 oval:org.mitre.oval:obj:27426

registry_state oval:org.mitre.oval:ste:18154

value datatype=version | operation=less than or equal | value=6.0.79

Se detectaron varias vulnerabilidades en el capítulo III y se plantean contramedidas para solucionar las mismas, las cuales se muestran en el Anexo VI

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones.

- El estudio realizado ha dado un panorama bastante claro de la situación actual del Banco Nacional de Fomento, con lo cual se debe implementar varias medidas de seguridad en la red de la Institución, las mismas ayudaran a estabilizarla de manera adecuada.
- Existen una gran cantidad de motivos por los cuales un usuario se puede ver afectado dentro de la red, en este caso el acceso a la misma desde un externo proporciona las facilidades para que un atacante pueda acceder a la información de la empresa, tanto a los servicios que el Banco Nacional de Fomento presta interna y externamente, siendo riesgos críticos determinados en base a la continuidad del negocio más no en un cierto servicio, también en la experiencia de las personas que están al contacto de los usuarios finales y por la probabilidad de ocurrencia de los riesgos.
- Al aplicar la técnica Network Scanning, se detecto el registro de varios hosts que en algún momento ingresaron a la red del Banco Nacional de Fomento, muchos de estos hosts aún estan registrados en los equipos de la Institución es decir en el servidor DHCP, lo que indica que no se esta realizando un mantenimiento periódico de este servidor, ya que el servidor tiene muchos registros de información basura.
- Al ejecutar la técnica Port Scanning, se encontró varios puertos abiertos asociados a servicios desconocidos, lo cual puede ser una evidencia de una intrusión o un intento de ataque utilizando dichos puertos, lo cual hace notar lo frágil que puede llegar a ser una infraestructura sin la implementación de políticas de seguridad.
- Después de la ejecución de la tecnica Vulnerability Scanning, se encontraron muchas brechas de seguridad en los aplicativos que utilizan los funcionarios

del Banco Nacional de Fomento, cada una de estas brechas podrían ser usadas por atacantes que podrían ingresar a la red de la Institución y tener control de la misma, afectando directamente a los servicios que la entidad ofrece.

- El personal del Banco Nacional de Fomento, no cuenta con conocimientos básicos sobre las amenazas y las vulnerabilidades actuales, a los que podrían enfrentarse los sistemas de la Institución, por lo tanto podría contribuir a un ataque y peor aún no tener el conocimiento suficiente para poder enfrentarlo en un determinado momento, afectando de manera significativa a los servicios que posee el Banco Nacional de Fomento.
- Es pertinente que las respectivas autoridades del Banco Nacional de Fomento, conozcan la realidad latente de la falta de concientización por parte de los usuarios y los problemas que se están ocasionando, con esto se puede obtener que las autoridades puedan tomar decisiones acertadas y oportunas en lo que se refiere a procesos de seguridad mas rápidamente.
- Es asi que tomando en cuenta que el BNF no maneja una red inalámbrica, se maneja un concepto de seguridad de alto nivel en lo que se refiere a posibles ataques por tener una red cableada en todo el banco.
- Las técnicas, procesos y herramientas utilizadas fueron de suma importancia el momento de realizar el análisis respectivo, desde la recopilación de información hasta la obtención de resultados, el software utilizado fue gratuito en un caso y licenciado en otro siendo utilizable las versiones de prueba pertinentes con las que se logró identificar las vulnerabilidades que aun no se habías tomado en cuenta en el BNF,

5.2 Recomendaciones.

- Tomar contramedidas para combatir las vulnerabilidades encontradas.
- Concientizar a todos los usuarios que tienen un computador con una conexión de red, y se entregue conocimientos básicos sobre las amenazas actuales y las vulnerabilidades a los que podría enfrentarse en el caso de que sufra algún ataque, para ello se pretende que el usuario esté preparado en caso de existir algún riesgo que pueda afectar el normal desempeño y evitar intrusiones maliciosas o incluso robos de información.
- Concientizar a usuarios finales para mitigar el gran porcentaje de problemas encontrados, siendo el usuario final el principal protagonista, además es recomendable proporcionar capacitaciones periódicas enfocadas al factor humano con el tema de seguridad de la información para que estos puedan protegerse de posibles ataques.
- Se recomienda a otras instituciones públicas y bancarias realizar este tipo de Análisis que les permitan detectar sus vulnerabilidades y tomar acciones correctivas al respecto.
- Se recomienda tomar las acciones correctivas necesarias para usuarios que ingresan al BNF por medio de Internet, ya que muchos ataques pueden venir por este medio.
- Se recomienda que el BNF realice un análisis mas a fondo de las vulnerabilidades encontradas para poder tomar decisiones acerca de la estrategia que se puede o se piense aplicar sean estas de corto, mediano o largo plazo dependiendo del tipo
- Incrementar políticas que obliguen a los usuarios del BNF a tener claves de mayor complejidad que sean difíciles de adivinar, mientras que se crea un nivel de conciencia para que los usuarios ayuden a difundir estas prácticas.
- Considerar la adquisición de algún software que pueda detectar de manera oportuna cualquier vulnerabilidad que podrían afectar a la información a la que se tiene acceso

- Priorizar la utilización de herramientas, técnicas y procedimientos que permitan evitar, detectar o corregir las vulnerabilidades encontradas, para asi actuar de forma pro activa ante ataques informáticos ya que todos los procesos, tecnología y servicios a implementar en la red de LAN sean para el uso de los usuarios finales y se provea de un proceso de análisis de vulnerabilidades mismo que se proyecte para un ambiente de pruebas y que este pueda evitar la interrupción del servicio en producción del banco.
- Implementar un plan de acción fundamental sobre las vulnerabilidades encontradas para que sea aplicado por las personas encargadas de la gestión de seguridad de la información del BNF
- Implementar un IDS/IPS para todos los segmentos de la red enfocados a los usuarios finales garantizando la seguridad.
- Capacitar constantemente a los usuarios que se encargan de la seguridad informática en el banco, sobre herramientas de seguridad disponibles debido a que las vulnerabilidades y amenazas están en constante cambio y aumento y se debe monitorear de forma continua y con un plan de seguridad preestablecido.
- Exigir el cumplimiento de las políticas de seguridad con las que actualmente consta el BNF, como parches de las aplicaciones que son las mas encontradas analizando el nivel de cumplimiento de las mismas.
- Capacitar y Asesorar constantemente el recurso humano que integra el grupo de seguridad, y llevar un seguimiento total o un ethical hacking de la seguridad implementada, generando un informe de las vulnerabilidades encontradas y las correcciones correctivas.

BIBLIOGRAFIA

Alvarado, I., Galecio, M., & Ruiz, J. (2013). *Ataque de Denegación de Servicio.* Obtenido de Deber de Seguridades de redes y computadores: http://docs.universidadecotec.edu.ec/tareas/2013E/COM407/alum/2013290345_3873_2013E_COM407_Bloqueo_de_Puertos_con_taller.docx.

España, U. d. (21 de 12 de 2007). *Protocolos de Comunicación*. Obtenido de http://neo.lcc.uma.es/evirtual/cdd/tutorial/Indice.html

Esparza Morocho, J. P. (06 de 03 de 2013). *Repositorio Digital EPN.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/6056/1/CD-4785.pdf

Franco, D. A., Perea, J. L., & Puello, P. (7 de Enero de 2015). Obtenido de www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

GFI LanGuard. (12 de Agosto de 2011). Obtenido de http://www.gfi.com

GFI Software Ltda. (09 de 05 de 2014). *Manual de Administrador.* Obtenido de GFI Languard: http://www.gfi.com/lanss/lanscan2014manual_es.pdf

Information Sciences Institute RFC -793. (Septiembre de 1981). *TRANSMISSION CONTROL PROTOCOL.* Obtenido de http://www.ietf.org/rfc/rfc793.txt

J. Postel - RFC 792-ISI. (Septiembre de 1981). *INTERNET CONTROL MESSAGE PROTOCOL.* Obtenido de http://www.ietf.org/rfc/rfc792.txt

Kioskea. (Febrero de 2015). *El protocolo ICMP*. Obtenido de http://es.kioskea.net/contents/265-el-protocolo-icmp

Lyon, G. (2013). *Nmap Network Scanning*. Obtenido de Descubiendo sistemas: http://nmap.org/man/es/man-host-discovery.html

Mifsud, E. (26 de 03 de 2012). *Introducción a la seguridad informática*. Obtenido de http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

Mifsud, E. (26 de Marzo de 2012). *MONOGRÁFICO: Introducción a las seguridad informática- Vulnerabilidades de un sistema informático*. Obtenido de http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3

Mifsud, E. (26 de Marzo de 2012). *OBSERVATORIO TECNOLOGICO GOBIERNO DE ESPAÑA*. Obtenido de http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

Perez Salinas, M. M. (1 de 10 de 2012). *SEGURIDAD INFORMATICA*. Obtenido de SCANNING: http://seguridadinformatica5e.blogspot.com/2012/10/scannig.html

Postel, J.-RFC 768 - ISI. (28 de Agosto de 1980). *User Datagram Protocol.* Obtenido de http://www.ietf.org/rfc/rfc768.txt

Rios, J. (22 de 09 de 2010). *Seguridad Informática*. Obtenido de http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml

Speeg Guide. (Enero de 2015). *Speed Guide.* Obtenido de http://www.speedguide.net/ports.php?filter=&sort=&p=26

Technologies, CA. (01 de 2015). *CA Client Automation*. Obtenido de http://www.ca.com/us/opscenter/ca-client-automation.aspx

The SANS Institute. (17 de 09 de 2002). *Las 20 vulnerabilidades más críticas del Internet*. Obtenido de http://www.vsantivirus.com/20vul.htm

Universidad de Málaga. (21 de 12 de 2001). *Protocolos de Comunicación*. Obtenido de El Protocolo IP: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/ip.html

Universidad Tecnológica de Panamá. (14 de 03 de 2014). *Análisis de Vulnerabilidad.* Obtenido de http://www.utp.ac.pa/analisis-de-vulnerabilidad

Villalón Huerta, A. (2002). *Escaneos de puertos*. Obtenido de http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node273.html

ANEXOS

ANEXO I: Conceptos Y Definiciones

ANEXO II: Fases para el análisis de vulnerabilidades

ANEXO III: Tipos de escaneo NMAP

ANEXO IV: Diagramas de red y vlans del bnf

ANEXO V: Inventario De Red Con Network Inventory

ANEXO VI: Contramedidas