ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"ESTABLECIMIENTO DE OBJETIVOS DE CONTROL A LOS FIREWALLS DE UNA INSTITUCIÓN FINANCIERA ALINEADOS A COBIT V 4.1"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

ROSA IRENE VILLANUEVA MOROCHO

GUAYAQUIL – ECUADOR

AÑO:2015

AGRADECIMIENTO

Agradezco principalmente a Dios por bendecirme, a mis padres y hermanos ya que gracias a su apoyo he podido continuar mi carrera y llegar donde he llegado.

Agradezco a todo el cuerpo docente de la ESPOL que hizo posible mi preparación para presentar este proyecto y adquirir mi título de graduación.

DEDICATORIA

Dedico este proyecto de graduación a Dios, a mis padres por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles.

A mis hermanos que siempre han estado presente conmigo en cada momento.

A mis compañeros de trabajo que siempre han sabido aconsejarme y guiarme y brindarme su apoyo en todo momento.

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Lenin Freire

DIRECTOR MSIA

_____

Ing. Juan Carlos García

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

_____

Mgs. Karina Astudillo

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

Este trabajo contiene los resultados de una evaluación de los objetivos de control realizada a los Firewall's perimetrales, internos y de contingencia de una Institución Financiera en base a un mapeo entre la Normativa PCI DSS v 2.0 con Cobit 4.1 en referencia a los requerimientos y controles que deben de cumplir los Firewall's.

De igual forma la evaluación de los objetivos de control se apoya en el cumplimiento de las Políticas de Seguridad de la Información de la Institución Financiera.

Esta evaluación de los objetivos de control no solo pueden ser utilizados para la evaluación del/los Firewalls, si no que puede ser utilizado para evaluar cualquier componente de red de la Institución Financiera.

ÍNDICE GENERAL

ABREVIATURAS

COBIT	Control Objectives for Information and related Technology.
DMZ	Demilitarized zone.
FTP	File Transfer Protocol
NAT	Network Address Translation.
PCI-DSS	Payment Card Industry Data Security Standard.
RBAC	Role-based access control.
VPN	Virtual Private Network
URL	Localizador Uniforme de Recursos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Actualmente todas las instituciones, especialmente las financieras se enfrentan diariamente a problemas de seguridad independientemente de su tamaño.

Los Firewalls actualmente proporcionan la mayoría de las herramientas de seguridad que son necesarias para complementar la seguridad en el acceso a los recursos de la red interna y hacia la red externa de la Institución, éste aseguramiento de la red debe de complementarse con el cumplimiento de políticas y procedimientos de seguridad.

La Institución Financiera cuenta en su Arquitectura de Guayaquil con un Firewall externo y un Firewall Interno los cuales protegen toda la red, principalmente a las áreas de Servidores y las DMZ.

De igual forma se encuentra un Firewall en la ciudad de Quevedo, dentro del Plan de Continuidad del Negocio de la Institución Financiera.

Este trabajo contiene los resultados de una evaluación de controles realizada a los Firewall's perimetrales, internos y de contingencia de una Institución Financiera en base a un mapeo entre la Normativa PCI DSS v 2.0 con Cobit 4.1 en referencia a los requerimientos y controles que debe de cumplir los Firewall's.

CAPÍTULO 1

GENERALIDADES

1.1 Objetivo general del proyecto

Establecer objetivos de control a los Firewalls de una institución financiera alineados a Cobit v 4.1 que nos ayuden a mantener una adecuada gestión del servicio considerando la necesidad de la norma PCI DSS V 2.0 y las Políticas de Seguridad de la Información de la Institución Financiera.

1.2 Objetivos específicos del Proyecto

- Evaluar y mejorar los controles aplicados actualmente para la optimización de la administración de los firewalls de la institución Financiera.
- Uso eficiente de la herramienta de seguridad Firewalls.
- Asegurarnos que la configuración de los Firewalls y la configuración de las reglas cumplan los requisitos de la norma PCI DSS v 2.0 y del Negocio así como las Políticas de Seguridad de la Información de la Institución Financiera.
- Proteger la red perimetral e interna con el fin de garantizar la alta disponibilidad de la misma y sus componentes.
- Medir el desempeño de la herramienta.

1.3 Descripción del problema

Inicialmente los Firewalls cumplían un papel específico dentro de la Institución Financiera el cual era permitir o no el tráfico en la red, pero con el transcurrir del tiempo el número de dispositivos de comunicación aumenta, debido a la necesidad del Negocio que crece día a día y esto hace la Institución Financiera adquiera Firewalls de última generación

para la protección completa de la red, esto hace que su administración se torne compleja.

Una sola regla mal configurada en los Firewalls podría conllevar a un riesgo de seguridad alto en la Institución Financiera, más aún no llevar controles sobre la misma podría conllevar a incumplimientos de normativas Nacionales o Internacionales como PCI DSS.

No se tiene establecido los responsables directos de cada cumplimiento ya sea el Administrador del Sistema o el Departamento de Seguridad de la Información.

De igual manera la Institución Financiera tiene la necesidad de certificarse PCI DSS v2.0.

1.4 Solución propuesta

Por tal motivo se realizó un levantamiento de información de las actividades de Administración del Servicio de los Firewalls, donde se identificaron los procesos que actualmente se vienen realizando los cuales no tenían establecidos objetivos de control alineados a ningún Marco de trabajo.

En base a esto se ha procedido a establecer objetivos de control alineados al Marco de Trabajo Cobit v 4.1 que nos ayuden a mantener una adecuada gestión del servicio considerando la necesidad de cumplimiento de la norma PCI DSS V 2.0 y las Políticas de Seguridad de la Información de la Institución Financiera.

CAPÍTULO 2

METODOLOGÍA Y OBJETIVOS DE CONTROL

2.1 Metodología usada

La metodología o el procedimiento que se utilizó para completar el proyecto es el siguiente:

- Revisión cumplimiento PCI DSS V2.0.
- Revisión de cumplimiento Políticas de Seguridad de la Información de la Institución Financiera.
- Objetivos de Control Marco Cobit V4.1
- Evaluación de los Objetivos de Controles:
  - Establecimiento del Requerimiento
  - Establecimiento de Responsables
  - Frecuencia del Control.

- Cumplimiento del Control.

Cobit 4.1 cubre los Procesos de TI que tiene controles generales que pueden ser utilizados en base a los requisitos de las Instituciones.

PCI-DSS es estrictamente centrado en los requisitos y procedimientos de evaluación de seguridad en la Protección de datos de los Tarjetahabientes.

El Mapeo entre PCI DSS v2.0 con COBIT 4.1 busca proporcionar orientación a las Instituciones Financieras identificando y destacando las áreas de COBIT 4.1 que debe considerar la Institución Financiera.

Como se observa en la Figura 2.1 el mapeo entre los requerimientos de control PCI DSS requisito número 1 referente al Firewall y los 6 Objetivos de Control de Cobit 4.1 que debimos seguir para la elaboración de los Objetivos de control Evaluados.

Requirement Number	PCI DSS v2.0 Control Requirements	COBIT 4.1 Control Objective/Process
1	Install and maintain a firewall to protect cardholder data.	AI2.5 Configuration and implementation of acquired application software
		AI3.2 Infrastructure resource protection and availability
		DS5.5 Security testing, surveillance and monitoring
		DS5.7 Protection of security technology
		DS5.10 Network security
		DS13.3 IT infrastructure monitoring

Figura 2.1: Mapeo PCI DSS V2 con Cobit 4.1

2.1.1 PCI DSS V2.0

La Normativa de Seguridad de Datos PCI proporciona requisitos específicos en cuanto a la correcta instalación, configuración y mantenimiento de los Firewalls de seguridad que protegen los datos de los titulares de tarjetas.

Requisito 1:

[1] **"Instale y mantenga una configuración de Firewalls para proteger los datos de los titulares de tarjetas"**

Este requisito se refiere a la necesidad de que la Institución Financiera cumpla con lo siguiente:

[1] Un proceso formal para aprobar y poner a prueba todas las conexiones de red externas e internas y los cambios en las configuraciones de los Firewalls.

[1] Diagramas actualizados de cada uno de los componentes de la red con todas las conexiones que acceden a los datos de los titulares de tarjeta.

[1] Documentar una lista de servicios y puertos necesarios para el negocio.

[1] Justificación y documentación de cualquier protocolo inseguro.

[1] Garantizar la zonificación de red adecuada con el fin de proteger los sistemas de soporte de la tarjeta con los datos

[1] Revisiones periódicas de las configuraciones de los Firewalls (por lo menos cada 6 meses).

2.1.2 COBIT 4.1

Para realizar la evaluación de los Firewalls de la Institución Financiera fueron tomados los Objetivos de Control para la información y tecnologías relacionadas COBIT debido a que es un Marco de Trabajo que engloba las mejores prácticas para la gestión de la Tecnología de la Información.

COBIT incluye objetivos de control específicos entorno de la gestión de la Administración, las pruebas de seguridad proactiva, y el monitoreo de los controles internos. Estos objetivos de control son relevantes para cualquier infraestructura de TI, incluyendo Firewalls.

2.1.3 Roles y Responsabilidades del Objetivo de Control

Chief Security Officer:

Es el Responsable de coordinar y vigilar la conformidad de la Políticas y Procedimientos de la Institución Financiera referente a la confidencialidad, integridad y Disponibilidad de sus activos de información.

Departamento de Seguridad de la Información:

Es el responsable de la planeación, educación y concienciación de la Seguridad de la Información, trabaja directamente con los Gerentes de Sistemas, administradores, usuarios con el fin de desarrollar políticas y procedimientos para proteger los activos de Información de la Institución Financiera.

Controla y supervisa y revisa el acceso al activo más importante que es la información.

Administrador de Sistema

Es el responsable de Aplicar las Políticas y procedimientos de Seguridad de la Información de la Institución Financiera. Administra los componentes de red de la Institución Financiera, mantiene diagramas de red actualizados.

2.3 Controles Evaluados

Se evaluaron un total de 51 requerimientos derivados del marco de trabajo Cobit V 4.1, tomando como métrica de ponderación el cumplimiento de las normas PCI DSS v2.0 requerimiento 1 y las Políticas de Seguridad de la Información de la Institución Financiera, obteniendo los siguientes resultados como se observa en la Figura 2.2:

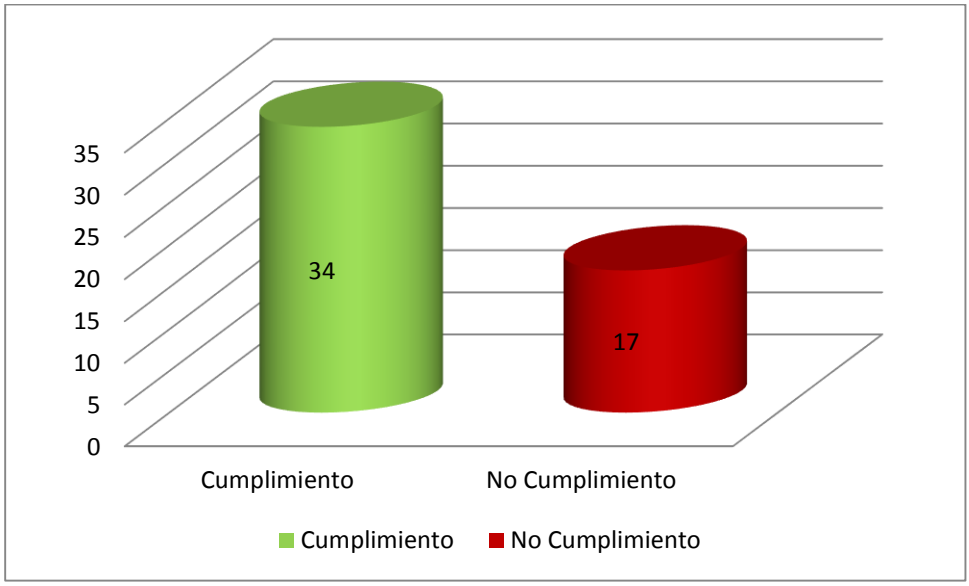

Figura 2.2 Total requerimientos evaluados (51)

CAPÍTULO 3

DETALLE DE OBJETIVOS DE CONTROL EVALUADOS

3.1 AI2.5 Configuración e Implantación de Software Aplicativo Adquirido.

Los siguientes requerimientos fueron evaluados para cumplir éste objetivo de Control como lo observamos en la Tabla 1:

TABLA 1: Objetivo de control AI2.5

Requerimiento	Frecuencia	Responsable	Cumplimiento
Análisis de Arquitectura Firewall	Bajo demanda	Administrador del sistema	☑
Implementación Firewall	Bajo demanda	Administrador del sistema	☑

Actualizaciones versión	Bajo demanda	Administrador del sistema	☑

3.2 AI3.2 Protección y Disponibilidad del Recurso de Infraestructura

Los siguientes requerimientos fueron evaluados para cumplir éste objetivo de Control como lo observamos en la Tabla 2:

TABLA 2: Objetivo de control AI3.2

Requerimiento	Frecuencia	Responsable	Cumplimiento
Procedimiento de solicitud de acceso a consola Firewall	Bajo demanda	Administrador del sistema	☒
Procedimiento de cambios configuración reglas firewall	Bajo demanda	Administrador del sistema	☑
Estándares configuración del sistema	Bajo demanda	Administrador del sistema	☒

Registro de logs administrativos	Tiempo real	Administrador del sistema	☑
Configuración de alertas	Tiempo real	Administrador del sistema	☑
Procedimiento de revisión de reglas firewall	Bajo demanda	Administrador del sistema	☑
Procedimientos backups restore	Bajo demanda	Administrador del sistema	☑
Generación de backups	Semanal	Administrador del sistema	☑
Procedimiento contingencia	Bajo demanda	Administrador del sistema	☑
Implementación contingencia	Bajo demanda	Administrador del sistema	☑

3.3 DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad

Los siguientes requerimientos fueron evaluados para cumplir éste objetivo de Control como lo observamos en la Tabla 3:

TABLA 3: Objetivo de control DS5.5

Requerimiento	Frecuencia	Responsable	Cumplimiento
Aprobar acceso a consola Firewall	Bajo demanda	Departamento Seguridad de la Información	☒
Control de acceso RBAC consola Firewall	Bajo demanda	Departamento Seguridad de la Información	☑
Habilitar acceso a consola Firewall	Bajo demanda	Administrador del sistema	☑
Aprobar cambios configuración reglas	Bajo demanda	Departamento Seguridad de la Información	☒
Revisión alertas específicas	Tiempo real	Departamento Seguridad de la Información	☒
Revisión de alertas eventos	Tiempo real	Administrador del sistema	☑
Revisión de diagrama arquitectura protección firewall	Semestral	Departamento Seguridad de la Información	☒

Revisión de reglas firewall	Semestral	Departamento Seguridad de la Información	☒
Verificación de uso de reglas y depuración	Semestral	Departamento Seguridad de la Información	☒
Revisión de tráfico autorizado/denegado	Tiempo real	Administrador del sistema	☑
Revisión de acceso usuarios consola firewall	Semestral	Departamento Seguridad de la Información	☒

3.4 DS5.7 Protección de la Tecnología de Seguridad

Los siguientes requerimientos fueron evaluados para cumplir éste objetivo de Control como lo observamos en la Tabla 4:

TABLA 4: Objetivo de control DS5.7

Requerimiento	Frecuencia	Responsable	Cumplimiento
Implementación de nat para direcciones externas	Bajo demanda	Administrador del sistema	☑

Implementación spoofing	Bajo demanda	Administrador del sistema	☑
Documentación reglas firewall	Bajo demanda	Administrador del sistema	☒
Documentar puertos, protocolos, servicios inseguros usados	Bajo demanda	Administrador del sistema	☒
No utilizar protocolo ftp para transmisión archivos con números de tarjeta	Bajo demanda	Administrador del sistema	☒
Usar reglas específicas	Bajo demanda	Administrador del sistema	☒
Implementación vpn	Bajo demanda	Administrador del sistema	☑
Excepciones de la política de administración segura de firewall	Bajo demanda	Chief Security Officer	☑

3.5 DS5.10 Seguridad de la Red

Los siguientes requerimientos fueron evaluados para cumplir éste objetivo de Control como lo observamos en la Tabla 5:

TABLA 5: Objetivo de control DS5.10

Requerimiento	Frecuencia	Responsable	Cumplimiento
Documentación diagrama de red	Bajo demanda	Administrador del sistema	☑
Actualización diagrama de red	Bajo demanda	Administrador del sistema	☑
Protección en cada conexión a Internet, entre cualquier DMZ y red interna.	Bajo demanda	Administrador del sistema	☑
Restringir conexiones con redes no confiables (externas)	Bajo demanda	Administrador del sistema	☑
Negar tráfico por defecto (block all)	Bajo demanda	Administrador del sistema	☑

Configuración servidor NTP	Bajo demanda	Administrador del sistema	☑
Restringir conexiones con redes inalámbricas	Bajo demanda	Administrador del sistema	☑
Restringir conexión a internet servidores	Bajo demanda	Administrador del sistema	☒
Implementación DMZ para tráfico entrante desde internet	Bajo demanda	Administrador del sistema	☑
Restringir conexión red interna a DMZ	Bajo demanda	Administrador del sistema	☑
Proteger red interna servidores	Bajo demanda	Administrador del sistema	☒
Filtrado de paquetes dinámico (stateful inspection)	Bajo demanda	Administrador del sistema	☑
Instalar firewall personal pcs del banco configuración no alterable	Bajo demanda	Administrador del sistema	☑

3.6 DS13.3 Monitoreo de la Infraestructura de TI

Los siguientes requerimientos fueron evaluados para cumplir éste objetivo de Control como lo observamos en la Tabla 6:

TABLA 6: Objetivo de control DS13.3

Requerimiento	Frecuencia	Responsable	Cumplimiento
Procedimiento monitoreo alertas firewall	Bajo demanda	Administrador del sistema	☑
Registro de logs tráfico	Tiempo real	Administrador del sistema	☑
Centralización de logs	Tiempo real	Administrador del sistema	☒
Bitácora registro configuración del sistema	Tiempo real	Administrador del sistema	☑
Elaboración de informe de salud	Semanal	Administrador del sistema	☑
Comunicar eventos de seguridad al departamento Seguridad de la Información	Tiempo real	Administrador del sistema	☒

CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado la elaboración de la evaluación de los controles a los Firewalls me permito presentar las siguientes conclusiones:

1. La Institución Financiera cuenta con una distribución de 2 Firewalls en Guayaquil, uno interno y uno externo.
2. En Quevedo se encuentra implementado un Firewall como parte del Plan de Continuidad del negocio.
3. Los Firewalls de Guayaquil y Quito cuentan con la última versión de la consola.
4. Existen controles para realizar adición, eliminación o cambio en las reglas de los Firewalls, mediante un formulario de permisos debidamente aprobado por la Gerencia de Sistemas.
5. Los requerimientos de cambios en el firewalls tienen un máximo 48 horas de atención.
6. Existen repositorios donde se registran todos los requerimientos aprobados para revisión de auditoría o entes externos.

7. Con la Herramienta de Firemon (Security Manager) la cual nos ayuda a entender y revisar quién tiene acceso a qué y qué controles se están concediendo.
8. De todos los controles evaluados hubo el 67% fue de cumplimiento frente al 33% de no cumplimiento.

Una vez finalizado la elaboración de la evaluación de los controles a los Firewalls me permito presentar las siguientes recomendaciones:

1. Documentar mediante bitácoras las configuraciones y reglas del Firewalls.
2. Sincronizar los últimos cambios de reglas en el Firewall de contingencia de Quevedo.
3. Eliminar todas las reglas any desde y hacia los Servidores.
4. Realizar revisiones periódicas de consumo y utilización de reglas del firewall con el fin de asegurar y depurar las mismas; conservar evidencia de ésta acción.
5. Restringir acceso a internet de servidores; para los que requieran dicho acceso limitar a las urls necesarias.
6. Limitar o eliminar el uso de reglas con permisos no definidos (any).

BIBLIOGRAFÍA

[1] PCI DSS versión 2.0 Norma de Seguridad de datos tarjetas de Pago,<https://www.pcisecuritystandards.org/documents/pci_dss_es la_v2.pdf>, fecha de consulta: Julio 2013, Julio 2015.

[2] Cobit versión 4.1 Marco de Trabajo Objetivos de control, < http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf>,fecha de consulta: Julio 2013, Julio 2015.

[3] Methodology for Firewall Reviews for PCI Compliance, < http://www.sans.org/reading-room/whitepapers/auditing/methodology-firewall-reviews-pci-compliance-34195>, fecha de consulta: Julio 2015.

[4] Mapping PCI DSS v2.0 With COBIT 4.1 http://www.isaca.org/knowledge-center/documents/mapping-pci-dss-v2.0-with-cobit-4.1.pdf>, fecha de consulta: Julio 2013, Julio 2105.

[5] Manual de Políticas y Procedimientos de Seguridad de la Información