Auditoría Seguridad Perimetral Para una Entidad Financiera

Juan Nicolás Mayorga Díaz.
Junio 2018.

Universidad Politécnico Grancolombiano.
Bogotá D.C.
Práctica Empresarial

Dedicatoria

Esta dedicatoria va dirigida a mi familia que ha sido todo mi apoyo incondicional, siempre han estado ahí para darme mucho valor y resistencia, para superar cada etapa y proyecto de mi vida.

Agradecimientos

Gracias a Dios, mi familia, amigos y compañeros, que han aportado en mí, su sabiduría y toda fortaleza para el cumplimiento de este proyecto, como a cada profesor e integrante de la universidad Politécnico Grancolombiano que han dejado en mí una gran huella de conocimiento

Abstract

The project is about a Perimeter Security audit that is defined as the set of policies, security elements and computer systems aimed at protecting the frontier of the Network in an organization.
The present audit must be the first barrier of computer defense, to control and avoid all types of frauds and risks that may be generated such as: Loss of information, cyber-attacks and electronic fraud. For this type of threats, measures implemented by controls that mitigate each one of the risks will be carried out.

Tabla de Contenidos

Lista De Tablas

Lista De Gráficas

Capítulo 1

Introducción y Planteamiento del Problema.

Introducción

La auditoría de seguridad perimetral tiene como objetivo evaluar los controles establecidos por la entidad para proteger el perímetro de la Red interna por medio del cumplimiento de políticas y procedimientos orientados a la configuración, disponibilidad y monitoreo de herramientas tecnológicas de seguridad perimetral.

Para esto se va a llevar a cabo una serie de procedimientos dentro de la auditoría que entran a evaluar los componentes tecnológicos de seguridad de una entidad financiera, partiendo de la información encontrada y verificando sus respectivas vulnerabilidades y riesgos, que para estos se tomaran controles específicos, que mitigaran los riesgos y ayudara para fortalecer la seguridad en la entidad bancaria. Las conclusiones son de vital importancia, porque es parte del resultado de la auditoría donde se tiene previsto aplicar todas las medidas que ayuden a corregir, prevenir o asignar medidas para mitigar los riesgos.

Planteamiento del Problema

¿Una entidad financiera que medidas de seguridad perimetral puede llegar a necesitar?

Capítulo 2

Objetivo General y Objetivos Específicos.

Objetivo General

Realizar una auditoría de seguridad perimetral donde se permita recopilar información de los activos, identificar vulnerabilidades y riesgos, evaluando controles que mitiguen los riesgos encontrados para proteger el perímetro de la Red interna del Banco.

Objetivos Específicos

Los objetivos específicos realizados para la auditoría son los siguientes:

- Recolectar información de las redes, topologías y protocolos del banco.
- Documentar la verificación del Cumplimiento de los estándares internacionales ISO, que aplican para la auditoría de seguridad perimetral.
- Identificar los sistemas operativos instalados en equipos y servidores del banco.
- Elaborar análisis de servicios y aplicaciones que usa el banco.
- Realizar la evaluación de vulnerabilidades y riesgos encontrados dentro de la auditoría.
- Elaborar cuadro de controles para mitigar los riesgos encontrados en el anterior objetivo.
- Plantear y hacer conclusiones que sirvan como medidas preventivas, para dar solución a los problemas expuestos.

Capítulo 3

Marco Teórico y Cronograma.

Marco Teórico

La seguridad perimetral se define como la integración de elementos y sistemas informáticos destinados a la protección de la frontera de la Red de una organización, realizando tareas de detección y defensa ante intrusos (hackers, virus, personal externo no autorizado). Se trata de la primera línea de defensa informática, la cual reduce el riesgo de fraude o pérdida de información como: Ataques cibernéticos, fraude electrónico e impacto reputacional.

Un modelo de seguridad robusto implementado en el perímetro de la Red garantiza la integridad, confidencialidad y disponibilidad de la información y el control de accesos como protección de los servicios informáticos.

La mejor manera de proteger el perímetro de red de una organización es por medio de la implementación de herramientas y medidas de seguridad que ofrezcan solución ante una amenaza, es por ello que el Banco cuenta con los siguientes mecanismos tecnológicos:

Firewall Perimetral
El firewall perimetral de la red del Banco en Colombia es una herramienta que define la política de accesos de red desde y a hacia Internet, el tipo de tráfico que se permite o se deniega, el nivel de protección contra ataques externos, la generación de canales de comunicación cifrados con terceros, conexiones remotas a equipos de administración.

Sistemas de Detección y Prevención de Intrusos (IDS/IPS)
Estos dispositivos monitorean, generan alarmas cuando hay eventos de seguridad y detienen las acciones realizadas por intrusos, actualmente se tiene configurado el módulo de IPS en el firewall perimetral del Banco.

Redes privadas virtuales (VPN)
Configuradas por medio de reglas en el firewall perimetral, las VPN proporcionan un canal de comunicación cifrado entre terceros y la red interna del Banco, por medio de ellas se gestiona de manera segura y controlada el intercambio de información con estas entidades.

Gestión de navegación a internet (Proxy)
En el proxy se define la política de navegación desde la red interna hacia internet, controlando de esta manera el ingreso a páginas con contenido malicioso y previniendo la fuga de información por medio del acceso a páginas web de almacenamiento en la nube.

Antivirus
El antivirus corporativo es de la marca TrendMicro, éste realiza la protección ante virus y software malicioso cubriendo los servidores físicos y virtuales, equipos de trabajo y de oficina. Adicionalmente gestiona el uso de dispositivos USB externos, impidiendo de esta manera infecciones por este medio.

Prevención de ciber-ataques
El sistema FireEye, Web Malware Protection System (MPS), ofrece protección avanzada contra ciber-ataques, y software malicioso que no ha sido catalogado como virus, trabaja verificando el comportamiento de los programas y detectando patrones sospechosos. Esta solución es instalada en los portátiles del Banco.

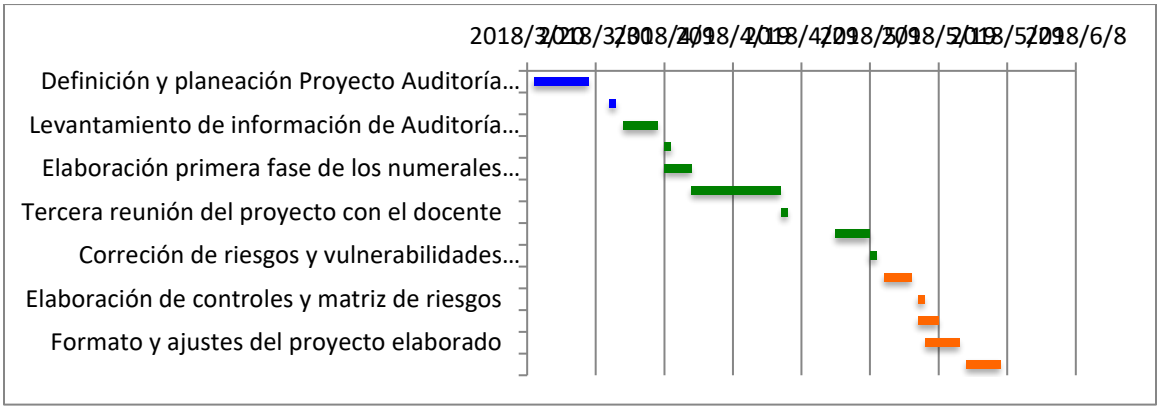
Principales Riesgos:

- Pérdida de confidencialidad, integridad y disponibilidad de la información por accesos de personas externas por medio de la ejecución de ataques informáticos (virus - hackers - etc.).
- Indisponibilidad de los servicios tecnológicos del Banco ocasionados por ataques informáticos realizados por terceros (hackers).
- Fraude externo originado por intrusiones realizadas por atacantes informáticos a la Red interna del Banco.
- Fuga de información por acceso de personal interno a páginas web de almacenamiento externo (dropbox, google drive, one drive, etc…).
- Indisponibilidad en la comunicación entre el Banco con terceros por fallas en las herramientas de seguridad perimetral que soportan el flujo de información.

Cronograma

Tareas	Responsable	Fecha de inicio	Fecha final	Días	Estado
Definición y planeación Proyecto Auditoría Seguridad Perimetral	J. Nicolás Mayorga	2018/3/21	2018/3/29	8	Completado
Reunión de Inicio y elaboración del proyecto con el docente	J. Nicolás Mayorga	2018/4/1	2018/4/2	1	Completado

Levantamiento de información de Auditoría Seguridad Perimetral	J. Nicolás Mayorga	2018/4/3	2018/4/8	5	**Completado**
Segunda reunión del proyecto con el docente	J. Nicolás Mayorga	2018/4/9	2018/4/10	1	**Completado**
Elaboración primera fase de los numerales 1,2 y 3 del proyecto	J. Nicolás Mayorga	2018/4/9	2018/4/13	4	**Completado**
Elaboración segunda fase de los numerales 2,3 y 4 del proyecto	J. Nicolás Mayorga	2018/4/13	2018/4/26	13	**Completado**
Tercera reunión del proyecto con el docente	J. Nicolás Mayorga	2018/4/26	2018/4/27	1	**Completado**
Elaboración tercera fase sobre riesgos y vulnerabilidades	J. Nicolás Mayorga	2018/5/4	2018/5/9	5	**Completado**
Corrección de riesgos y vulnerabilidades mencionadas por el docente	J. Nicolás Mayorga	2018/5/9	2018/5/10	1	**Completado**
Desarrollo de corrección de riesgos y vulnerabilidades encontradas	J. Nicolás Mayorga	2018/5/11	2018/5/15	4	**Completado**
Elaboración de controles y matriz de riesgos	J. Nicolás Mayorga	2018/5/16	2018/5/17	1	**Completado**
Conclusiones del desarrollo de la auditoría	J. Nicolás Mayorga	2018/5/16	2018/5/19	3	**Completado**
Formato y ajustes del proyecto elaborado	J. Nicolás Mayorga	2018/5/17	2018/5/22	5	**Completado**
Finalización del proyecto, ajustando: Introducción, objetivos, abstract, etc…	J. Nicolás Mayorga	2018/5/23	2018/5/28	5	**Completado**
TOTAL				57	



Capítulo 4

Desarrollo del Trabajo.

Contenido

1. Enumeración de redes, topologías y protocolos

Realizando un levantamiento de información para esta auditoría de seguridad perimetral, se identificaron los siguientes protocolos que emplea la empresa para transferencia de información con terceros:

Tabla 1 Protocolos

Protocolos	Cantidad Total Por Protocolos De Servicio	Protocolos Identificados En Uso
TCP	372	7
UDP	93	3

TCP: Por TCP se estima que aproximadamente hay unos 7 servicios asignados con las VPN de cada proveedor de servicios con los que interactúa la entidad financiera, para que el banco pueda acceder de forma fácil y segura a toda información brindada por el tercero.
UDP: Se estima que aproximadamente hay 3 servicios UDP a nivel interno de la entidad financiera, que facilita todo tipo de transacciones a dentro de la compañía y además 90 servicios independientes que corresponden a monitoreos en diferentes áreas.
Siguiendo el modelo OSI, estos protocolos de servicio operan en la capa de transporte.

Tabla 2 Protocolos

Protocolos	Cantidad Total Por Protocolos De Servicio	Protocolos Identificados En Uso
ICMP	56	5

ICMP: En ICMP existen 5 servicios de la entidad bancaria. Este protocolo determina si un host o router no logra ser localizado, enviando un mensaje de error. Siguiendo el modelo OSI, este protocolo de servicio opera en la capa de red.

Tabla 3 Protocolos

Protocolos	Cantidad Total Por Protocolos De Servicio	Protocolos Identificados En Uso
HTTP	404	155
SSH	123	63
FTP	74	34
RDP	32	9
SMTP	6	6
POP3	4	4
IMAP	4	4

HTTP: Existen 155 servicios HTTP que permiten el acceso desde la entidad financiera a las páginas web de los diferentes terceros y proveedores.

SSH: Para SSH se detectan 63 servicios para la conexión entre terceros y diferentes dependencias de la entidad bancaria. Este se utiliza para realizar una comunicación segura teniendo en cuenta que encripta la sesión de conexión y utiliza una arquitectura cliente/servidor.

FTP: Para FTP se detectan 34 servicios para la comunicación con terceros y uso interno. Estos son utilizados normalmente para la transferencia de archivos o información, también se puede identificar sus servidores ftp para la accesibilidad con terceros.

RDP: Se identifican 9 servicios para RDP, que tienen relación con varias dependencias internas de la entidad bancaria. Permitiendo la comunicación en plena ejecución de una aplicación del terminal, tomando la información que es suministrada por el servidor.

SMTP: Es utilizado para la transferencia de mensajes por correo electrónico.

POP3: Es utilizado para clientes locales de correo de la misma entidad financiera, descargando los mensajes para ser visualizados.
IMAP: Es utilizado para tener accesibilidad al servicio de correo desde cualquier dispositivo con conexión a internet; siendo la mejor opción por permitir visualizar los mensajes de manera remota.
Siguiendo el modelo OSI, estos protocolos de servicio operan en la capa de aplicación.

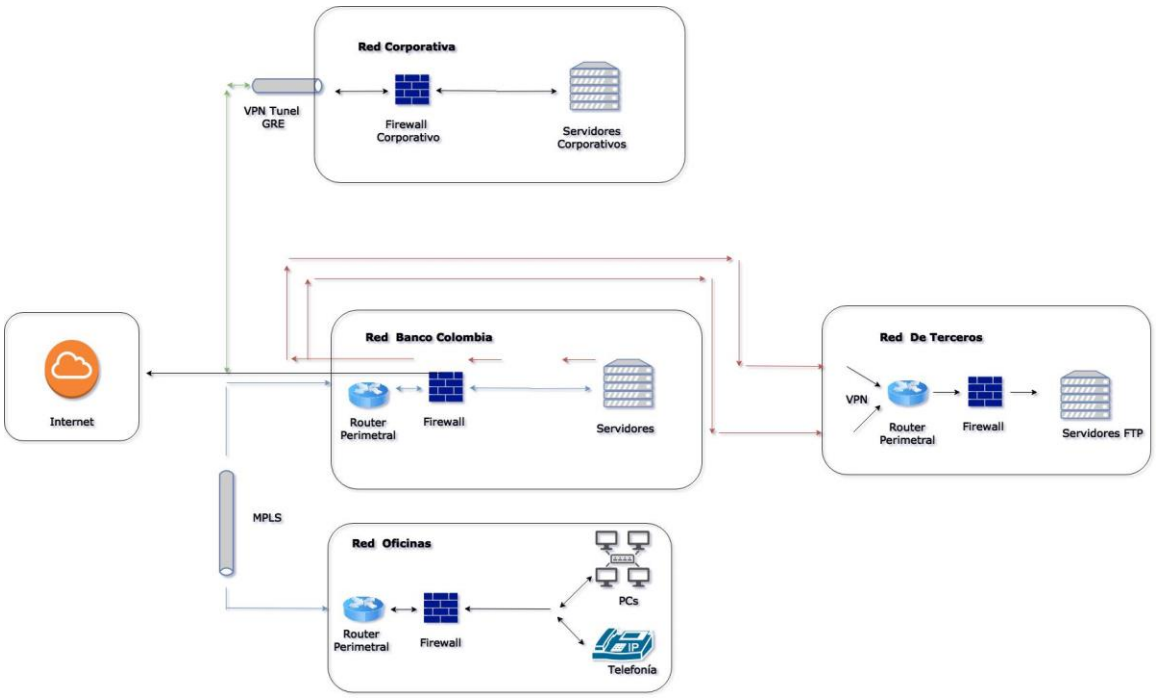
Para esta auditoría, la entidad bancaria está conformada por 4 redes que son:

- Red Banco Colombia
- Red de oficinas
- Red de terceros

- Red corporativa

Con las anteriores descripciones de protocolos y redes se realizó un diagrama de red, el cuál describe la comunicación y el funcionamiento de estas redes:

Gráfica 1 Diagrama de red



2. Verificación del Cumplimiento de los estándares internacionales ISO

En el área de auditoría se toma como referencia la norma ISO 27002:2013, esta cuenta con 14 dominios y 114 controles. Que resume los dominios en que trabaja la auditoría de seguridad perimetral y de ahí se hallará un resultado.
En las observaciones del resultado se estableció variables SI/NO y N/A, que nos indicará si la norma se cumple o no se cumple actualmente. Las definiciones nos ayudarán a identificar por medio de las normas si es una amenaza persistente, y si es mitigable o no mitigable por completo, ya que son procesos que cambian constantemente en la entidad financiera.

Tabla 4 Normas ISO

Dominio de control	Prueba	Resultado
5. POLITICAS DE SEGURIDAD	En la entidad financiera ya se encuentra estipulado un documento o reporte formal sobre las políticas y recomendaciones de seguridad que se deben de llevar a cabo en los procedimientos con respecto a la información y sistemas del banco, asignado por el área de seguridad de la información	SI
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	En el documento o reporte de políticas de seguridad del banco se encuentran claras y bien definidas sus políticas, sobre el manejo y el buen uso que se le debe dar a la información, como la disposición sobre el uso de los dispositivos que se encuentran dentro de la entidad bancaria	SI
9. CONTROL DE ACCESOS	La entidad financiera tiene estipulados para la seguridad perimetral de la misma el apoyo de controles como lo son las VPN configuradas dentro de los respectivos firewall, que dan una capa de seguridad más, con respecto a la penetración de alguna amenaza externa, al igual el manejo de controles activos y pasivos de seguridad, que compromete a tener por el lado de los activos, contraseñas fuertes, software de antivirus actualizado, últimos parches de seguridad del S.O, backup de la información, denegación al acceso de dispositivos extraíbles y en la parte de los pasivos, identificar que el antivirus realice escaneos de seguridad periódicamente, que los dispositivos tengan restringidos algunos accesos a cierta información confidencial o vulnerable para la entidad.	SI

12. SEGURIDAD EN LA OPERACION	Es importante que haya un respaldo de la información y bases de datos que tienen las aplicaciones y demás sistemas ejecutados, como los debidos permisos o autorizaciones que se deben de cumplir con respecto a la instalación de alguna aplicación o software de tercero no estipulada por la entidad bancaria	SI
13. SEGURIDAD EN LAS TELECOMUNICACIONES	La entidad bancaria tiene establecido en sus datacenter, toda la infraestructura correspondiente para la operación de los dispositivos de telecomunicaciones, además tienen establecido controles de monitoreo para los servicios de redes proporcionados, llevando una gestión eficiente en los mecanismos de seguridad que van asociados a las redes de la entidad financiera	SI
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	La entidad financiera debe verificar si es necesario contemplar la adquisición de dispositivos informáticos como respaldo ante alguna contingencia o eventualidad que suceda y no afecte la continuidad del negocio	N/A.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	Pueden suceder uno o varios eventos de seguridad no deseados, los cuales pueden comprometer la información de la entidad financiera, por lo que esta misma lleva un gestionamiento de seguridad tanto en equipos físicos como firewall, también un software especializado para contrarrestar todo tipo de ataques inesperados que puedan ocurrir contando con antivirus, agentes de protección ante malware y controles en el gestionamiento de las reglas en el proxy.	SI

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Los aspectos a evaluar con respecto a las políticas de seguridad de la información de la entidad financiera, será planificar, implementar y verificar el gestionamiento de los elementos de seguridad que actúan en contra de las amenazas o vulnerabilidades que pueden llegarse hallar, para que trabajen de forma óptima y que así mismo todos los dispositivos y equipos del banco, no representen un riesgo o comprometan la información almacenada en los mismos.	N/A.

Fuente 5. (http://iso27000.es/iso27002.html)

3. Identificación de los sistemas operativos instalados

Los sistemas operativos instalados están en equipos y servidores físicos, que actualmente trabaja toda la infraestructura de la entidad bancaria, que se registran a continuación:

Se describen los resultados de la base de datos para encontrar los dispositivos y equipos que cuentan con sistema operativo.

Tabla 5 Sistemas operativos (equipos)

Usabilidad	(Todas)

Etiquetas de fila	Cuenta de Total OS
Windows 10 Pro	175
Windows 7 Professional	1858
Windows XP Professional	5
Total general	**2038**

Se analiza que la mayoría de equipos, que es aproximadamente del 91%, maneja Windows 7 Professional, con un 9% que utiliza Windows 10 Pro y con un 1% que restan utilizando Windows XP Professional.

Los servidores físicos con los que cuenta la entidad financiera se describen a continuación, detallando cada uno por su respectiva marca y el S.O que maneja actualmente.

Tabla 6 Sistemas operativos (servidores)

Sede	(Todas)

Etiquetas de fila	Cuenta de S.O
2008	**7**
HP	2
IBM	5
2008 R2	**10**
HP	1
IBM	9
2008 sp1	**2**
IBM	2
AS-400	**1**
IBM	1
DISPONIBLE	**1**
IBM	1
Integrity	**1**
HP	1
LINUX	**1**
HITACHI	1
Linux red Hat	**4**
HP	1
IBM	3
oracle linux 5	**15**
AVAYA - HP	2
IBM	13
OS400	**4**
IBM	4
VMS 8.4	**3**
HP	3
Vmware 5.5	**39**
HP	39
VMWARE 6.0	**3**
IBM	3
WS 2003 R2 STD	**2**
HP	2

WS 2008 R2 ENT	**3**
HP	3
WS 2008 R2 STD	**15**
HP	1
IBM	14
WS 2012 R2 STD	**3**
DELL	1
HITACHI	1
HP	1
Total general	**114**

Se analiza que la mayoría de servidores corresponden al 34% de marca HP, y teniendo el 66% restante de diferentes marcas, que la mayoría de los servidores usan Windows Server 2008, Vmware 5.5 y Oracle Linux 5.

4. Análisis de servicios y aplicaciones.

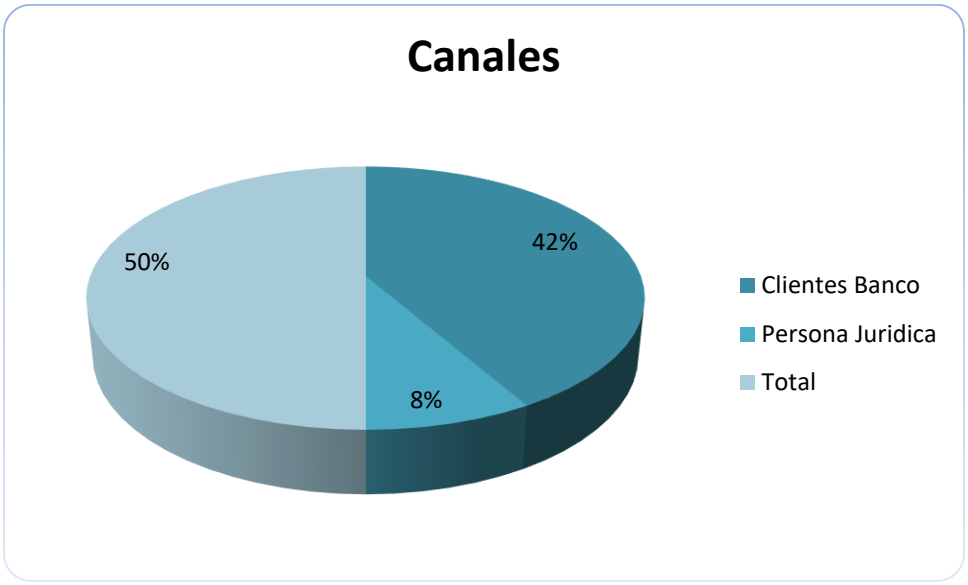
El objetivo es identificar los servicios y aplicaciones usados por el banco, en el que se determinará por medio de la metodología de arquitectura de empresa (TOGAF), un resumen que ayudará con la identificación y segmentación de los aplicativos.

En los siguientes cuadros, se expone la cantidad de canales de servicio como aplicativos, usados por la entidad financiera:

Tabla 7 Canales de servicio

	Clientes Banco	Persona Jurídica	Total
Canales	5	1	6

Gráfica 2 Canales de servicio



En la anterior gráfica, se verificó la cantidad de canales de servicio presentados por el banco, representado por un 42% donde estas son aplicaciones web que usan los clientes del banco continuamente tanto para persona natural y 8% para persona jurídica como:

- Pagos por PSE
- IVR (Respuesta de Voz Interactiva)
- Aplicación web usada en los kioscos de las oficinas de los bancos
- Omnichannel: Página web (página pública), aplicación mobile, acceso a la página web desde el navegador de un celular)
- Portal Empresarial

Donde omnichannel se divide en desktop y mobile:
Desktop: Comunica desde la página web, a través de "banca en línea" para ingresar a la página pública de la entidad bancaria desde un computador
Mobile: Es usada para acceder a "banca en línea" por medio de un móvil a la página web del banco, a través del navegador del dispositivo.
También omnichannel realiza comunicación con la aplicación dedicada para smartphones del banco.

Tabla 8 Aplicaciones internas

	Usuarios Banco
Aplicaciones Internas	29

Se identificaron 29 aplicaciones que son usadas por los funcionarios de la entidad bancaria, que se componen de aplicaciones como aplicaciones web; algunas de ellas son:

- Aplicación de ingreso de personal
- Aplicación web de aprobaciones de producto
- Aplicación de inventarios
- Aplicación de registro de ventas, transacciones y procesos
- Aplicación de biometria
- Aplicación de retenciones
- Aplicación para validaciones de cuenta
- Aplicación de pagos
- Aplicación web de extractos
- Aplicación web de bloqueos
- Aplicación de comisiones

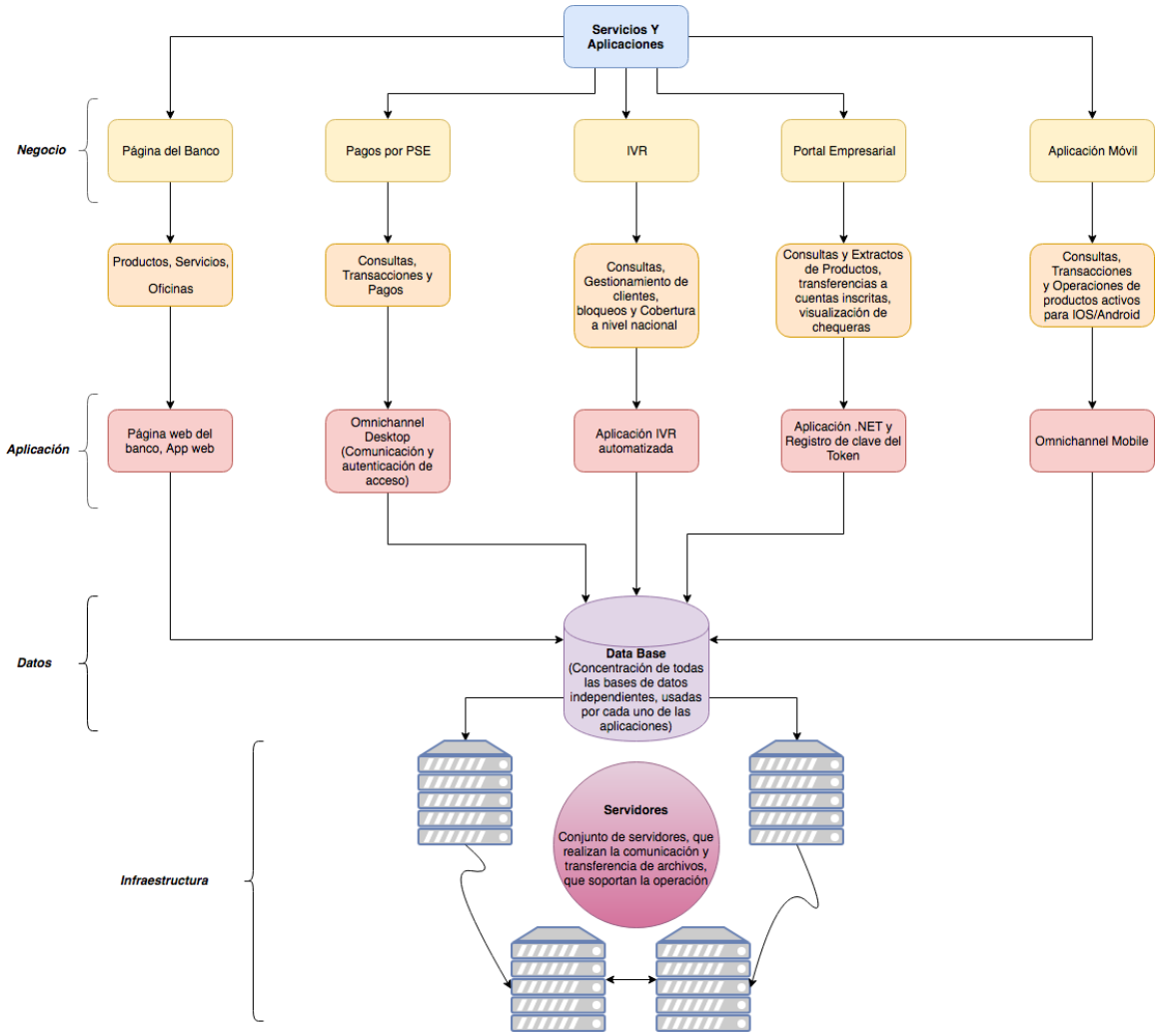
La realización del diagrama se planteo definiendo los siguientes criterios:

Tabla 9 TOGAF

S E G U R I D A D	Negocio
	Aplicación
	Datos
	Infraestructura

- **Negocio:** Se refiere a todas las aplicaciones y aplicaciones web que maneja el banco y son usadas por los clientes.
- **Aplicación:** Son las aplicaciones que logran la comunicación y autenticidad de acceso al cliente a las diferentes plataformas de la entidad financiera, dando soporte al buen funcionamiento del sistema.
- **Datos:** Son todas las bases de datos con relación a las aplicaciones asociadas y contempla toda la información proporcionada por proveedores y terceros a la entidad financiera.
- **Infraestructura:** Es todo el hardware y dispositivos que hacen sostenible la operación del sistema en la entidad bancaria.

Gráfica 3 Diagrama de flujo TOGAF



5. Detección, comprobación y evaluación de vulnerabilidades

Se desarrollo la comprobación y evaluación de las vulnerabilidades, según la tabla de puntaje a continuación:

Tabla 10 Evaluación

BAJO	0-34
MEDIO	35-69
ALTO	70-100

Tabla 11 Vulnerabilidades y riesgos

ID	ACTIVO	DESCRIPCIÓN VULNERABILIDAD	AMENAZA	RIESGO	PRINCIPIO AFECTADO	PROBABILIDAD	IMPACTO	RESULTADO
V1	Servidores de seguridad	Fallas por no establecer controles periodicos adecuados en el mantenimiento de los sistemas en los servidores que soportan la seguridad, mediante la ejecución de agentes antimalware y ciber-ataques.	Personas Externas, que ejecuten ataques informaticos	Perdida de confidencialidad, integridad y disponibilidad de la información, generada por personas externas a la empresa, realizando la ejecución de ataques informaticos como: Virus, Malware, spyware, denegación de servicios, etc...	Confidencialidad	BAJO	ALTO	MEDIO
V2	Información De La Entidad Bancaria	Falta de aplicación de controles de acceso seguro para el personal interno, que en el momento no cuenta con roles autorizados para navegación libre.	Personal Interno, que utiliza almacenamiento externo, para guardar información en la nube	Fuga de información por acceso de personal interno a páginas web de servicio de almacenamiento externo de archivos en la nube y sincronización de estos con otros dispositivos (dropbox, google drive, icloud y MEGA).	Confidencialidad	BAJO	MEDIO	MEDIO
V3	IDS	Falencia en la supervisión de sistemas IDS que respaldan la comunicación, al no generar un mantenimiento adecuado en los O.S. donde estas herramientas de seguridad son ejecutadas	Fallas en la comunicación con las herramientas de seguridad perimetral	Indisponibilidad en el IDS que verifica y respalda la información que comunica el Banco con terceros, por fallas en las herramientas de seguridad perimetral que soportan	Disponibilidad	BAJO	ALTO	MEDIO

				el flujo de la información.				
V4	Información De La Entidad Bancaria	Fallas en el cifrado de la información y uso de protocolos de comunicación inseguros	Uso de herramientas de scaneo y penetración de red	Pérdida de confidencialidad, integridad y disponibilidad de información por fallas en el cifrado por protocolos de comunicación inseguros entre la Red de oficinas y la Red interna.	Confidencialidad	MEDIO	ALTO	ALTO
V5	Antivirus y agente de seguridad	Falla en la revisión sobre la actualización de la base de datos de firmas del antivirus y agente de seguridad, para mitigar el software malicioso que se encuentre en los equipos.	software malicioso	Pérdida de confidencialidad, integridad y disponibilidad de la información por infecciones de software malicioso en los equipos de oficinas.	Confidencialidad - Integridad - Disponibilidad	MEDIO	MEDIO	MEDIO
V6	Infraestructura de red	Problema por la inexistencia de canales redundantes, ya que se puede sufrir perdidas de comunicación entre la red interna a la red corporativa	Baja adminstración de infraestructura	indisponibilidad de las plataformas de seguridad perimetral que interactuan en la comunicación con la red interna a la red corporativa	Disponibilidad	MEDIO	MEDIO	MEDIO
V7	red	Falla en la segmentación y cifrado en la red interna, al no tener un módulo de acceso web cifrado, para usuarios externos, no pertenecientes a la empresa.	Terceros no autorizados con acceso a la red interna	Acceso no autorizado por parte de terceros puedan conectarse a la Red interna del Banco originado por inadecuada segmentación de Red.	Confidencialidad	MEDIO	ALTO	MEDIO
V8	Infraestructura	Falla al no tener y operar el control	Infraestructura	Posible perdida, disponibilida	Confidenci	MEDIO	ALTO	MEDIO

		total de la infraestructura, exponiendo información y su tratamiento confidencial ante personas no autorizadas	implementada con terceros	d y confidencialidad de la información, al no tener el control de la infraestructura y todo los filtros por donde la información tiene que pasar, ya que la privacidad se vería afectada.	alidad			
V9	sistemas de seguridad perimetral	Fallas de los sistemas de seguridad perimetral, como verificación de los últimos parches de seguridad y a nivel general la no implementación de test o simulacros de intrusión en la red interna	Atacantes Informaticos	Que exista un Fraude externo ocasionado por intrusiones realizadas por atacantes informáticos a la Red interna del Banco.	Confidencialidad - Integridad	MEDIO	ALTO	ALTO
V10	Información De La Entidad Bancaria	Falla al no realizar un monitoreo preventivo de las actividades inusuales, que generan los intrusos por medio de ataques informaticos que se deben de reportar a través de registros	Atacantes informaticos (Hackers)	Indisponibilidad de los servicios tecnológicos del Banco ocasionados por ataques informáticos realizados por terceros, ejemplo: (hackers).	Disponibilidad	ALTO	ALTO	ALTO
V11	Enrutadores perimetrales	Posible falla en los enrutadores perimetrales al no haber un cambio prudencial o de actualización del hardware por su uso máximo de vida.	Terceros no autorizados con acceso a la red del banco que extraen información de la entidad	Fuga de información por acceso de personas no autorizadas a la Red del Banco, afectando la comunicación con terceros	Confidencialidad	MEDIO	ALTO	MEDIO
V12	Información De La	Falla en reglas de contingencia para las plataformas de seguridad	Ausencia de reglas de	Indisponibilidad de acceso a información financiera de	Disponibilidad	BAJO	MEDIO	MEDIO

	Entidad Bancaria	perimetral, que soportan el flujo de información con la Red interna del Banco.	contingencia	clientes en las oficinas del banco				
V13	Firewalls Perimetrales	Fallas en la comunicación de la red interna y la red corporativa del banco por no preveer manteniemto a firewalls perimetrales	Fallos en los firewall perimetrales	Pérdida de confidencialidad, integridad y disponibilidad de información debido a fallas en los firewall de la Red interna y la Red corporativa.	Confidencialidad - Integridad - Disponibilidad	MEDIO	ALTO	MEDIO
V14	Software de seguridad	Falla en la revisión y mantenimiento periodica de software de seguridad para los equipos internos	Atacantes Informaticos	Algunos equipos de la red interna del banco como portatiles y de escritorio tienen instalado su antivirus y agente, pero estos no estan habilitados en los equipos, por lo que compromete la confidencialidad de la información de la entidad.	Confidencialidad	BAJO	MEDIO	BAJO

Realizando la matriz de riesgos, se procede a hacer un análisis cualitativo:

Tabla 12 Matriz de riesgos

		PROBABILIDAD		
		Poco Probable	Posible	Muy Probable
CONSECUENCIAS O IMPACTO	Menores	**V14**		
	Moderadas	**V2, V12**	**V5, V6, V11, V13**	**V7, V8**
	Mayores	**V1, V3**	**V4, V10**	**V9**

Tabla 13 Clasificación de riesgos

	BAJO
	MEDIO
	ALTO

Se puede determinar que para esta auditoría se encontraron en la matriz de riesgos vulnerabilidades como riesgos principales en categoría entre medio – alto. Porque los temas que son tratados en seguridad perimetral conllevan a exponer tanto información como infraestructura valiosa para la entidad; ya que estos activos son parte principal para su funcionamiento.

6. Medidas específicas de corrección

Para cada vulnerabilidad como riesgo encontrado, se toma una serie de controles, que ayudan a mitigar cualquier riesgo presentado, minimizando todo tipo de alertas que pueden ser críticas, ayudando a mejorar la seguridad de la información de la entidad. Colocando las de mayor importancia primero; ya que deben ser tratadas con una prioridad mayor, hasta llegar a las de menor prioridad.

Tabla 14 Controles de riesgos

ID	CONTROLES	PRIORIDAD
V9	Para mitigar el riesgo como la vulnerabilidad de posibles intrusiones, se recomienda elaborar un plan estratégico para realizar un test de intrusión en el que un auditor empleará las mismas técnicas que utilizaría un atacante malintencionado que quisiera acceder al sistema para robar información o realizar cualquier otra acción ilegítima y así reforzar las debilidades ante el riesgo presentado.	ALTA
V4	Se debe de verificar la implementación de protocolos seguros en la red como lo es un protocolo IPsec, que actúa en la capa 3 de red, brindando cifrado en la comunicación	ALTA
V10	Realizar monitoreos preventivos diariamente, llevando un registro organizado del día de eventos inusuales presentados en la red, por lo que se optimizará, analizando que casos de ataques son más frecuentes y así generando un plan de acción para mitigarlos a corto plazo, como para desvanecer la presencia de ataques futuros.	ALTA
V7	Se identifica que es necesario para respaldar la información de la empresa, implementar un servicio de acceso web cifrado, para que las personas externas, puedan conectarse a la red interna, por medio	MEDIA

	de un control establecido de usuario y contraseña, apra fortalecer aún mas la seguridad.	
V8	La entidad podría plantear una reunión de gerencia, para decidir de una forma acorde a las políticas preestablecidas del banco, si existe alguna posibilidad de implementar una infraestructura propia en los procesos que son manejados por terceros, para equipos y dispositivos de telecomunicaciones.	**MEDIA**
V5	Implementar revisión periódica para actualizar la base de datos de la firma del antivirus, como un control con respecto al agente de seguridad adicional, manejado en los equipos de oficina de la empresa.	**MEDIA**
V6	Implementar canales secundarios o de respaldo para no afectar la comunicación entre la red interna a la red corporativa, como la implementación de routers permitrales adicionales para que la comunicación no vaya por una sola vía.	**MEDIA**
V11	Verificar la implementación y renovación del hardware en la red perimetral con terceros, para evitar la fuga de la información que hacen terceros.	**MEDIA**

V13	Realizar un diagnóstico y mantenimiento a los firewalls de Perímetro dedicados en cada una de las dos Redes	**MEDIA**
V1	Organizar controles preventivos en el mantenimiento de los sistemas de seguridad que tienen los servidores para mitigar los ataques externos.	**MEDIA**
	Implementar Servidores de respaldo, que cumplan las políticas establecidas por la entidad, en caso de mal funcionamiento de los servidores principales que establecen la seguridad mediante agentes.	
V3	Realizar seguimiento del módulo IDS, que debe ser verificado diariamente, para no desproteger la información que se revive de terceros. Se recomienda Implementar un sistema IDS de respaldo para proteger la comunicación con terceros, en caso de que suceda un problema de infraestructura y deje de operar el IDS principal	**MEDIA**
V2	Se debe de generar un plan de acción para establecer políticas de acceso y restringir la navegación libre a determinados roles o cargos que no lo requieran.	**MEDIA**

V12	Implementar reglas o políticas de contingencia, para la plataforma e infraestructura de seguridad perimetral y así tener alta disponibilidad de la información financiera de clientes en las oficinas del banco	**MEDIA**
V14	Se requiere implementar una actividad de recorrido en los equipos con falencia de software de antivirus y agente de seguridad, para que se reporte y agregue en el informe de auditoría de seguridad perimetral, y así informar al área de seguridad de la información para que tome el control y mitigue dicho riesgo	**BAJA**

Capítulo 5

Conclusiones

Conclusiones

- Se observó durante la auditoría, que el proceso cuenta con herramientas de seguridad perimetral que mitigan algunos riesgos ocasionados por ataques externos.
- Se debe preveer mantenimientos mas efectivos a nivel general, para que no se convierta en una vulnerabilidad de las anteriores halladas, como en V1.
- Se encontraron 3 vulnerabilidades en “ALTO”, siendo: (V4,V9,V10); a cada una se ha asignado un control para mitigar su riesgo, como ocurrencia.
- Las vulnerabilidades (V4,V9,V10), se clasificaron como relevantes dando una prioridad alta y dejando especificados sus controles para que se apliquen .
- Existe protección por antivirus y agentes de seguridad para la eliminación de virus, escaneo programado a los equipos tecnológicos del banco y conexión de dispositivos USB en los equipos de trabajo, impidiendo de esta forma afectaciones en la integridad de la información, su disponibilidad y confidencialidad.
- La plataforma de seguridad que tiene implementada la entidad, debe ser monitoreada y llevar controles de mantenimiento para minimizar toda falla ocasional que pueda presentar.
- Para la infraestructura de las oficinas deberían de implementarse algunos firewalls que controlen la entrada y salida del trafico para mejorar su seguridad.
- Se estima la revisión de equipos que no tienen antivirus, realizando un diagnostico presencial a los que se encuentran ubicados en la red interna.
- Se evidenció que algunos equipos del banco no cuentan con antivirus instalado, para la red interna falta el 23% (87 equipos) y para la red de oficinas un 13% (201 equipos).
- La entidad debe preveer a mediano y largo plazo de proveer su propia infraestructura para ejecutar sus procesos.
- Se evidencia que la entidad financiera tiene controles de medidas de seguridad ante la comunicación con terceros, que mitigan algunos riesgos.
- Se tiene buen alcance en la seguridad perimetral de la entidad, al tener destinado en cada red un firewall perimetral que genera una protección a la entrada y salida de la información.
- Cada empleado perteneciente a la entidad, tiene creado un usuario y una contraseña, esta es actualmente programada para que se cambie cada 2 meses, así

respaldando con un mayor criterio la seguridad que es almacenada en cada equipo de los usuarios.

- No se tiene configurado el bloqueo de IP externas que generen ataques informáticos hacia la Red del Banco, actualmente solo se tiene habilitado el monitoreo de actividad inusual proveniente de redes externas.
- Se identificaron diferentes tipos de riesgo dentro de la auditoría, siendo el mas relevante el V10, porque genera una indisponibilidad de los servicios tecnologicos.

Bibliografía

1. Marcelo Wladimir León Gudiño. (2017). Auditoría de seguridad informática en la red interna de la universidad técnica del norte según la metodología offensive security professional training and tools for security specialists y planteamiento de políticas de seguridad basadas en la norma iso/iec 27001. http://repositorio.utn.edu.ec/bitstream/123456789/6975/1/04%20RED%20162%20TRABAJO%20DE%20GRADO.pdf.

2. Rubén Díaz Pérez. Junio (2016). Auditoria de sistemes i serveis de ciberseguretat a una empresa d´assegurances. https://upcommons.upc.edu/bitstream/handle/2117/90108/Memoria_PFC_RDP.pdf?sequence=1&isAllowed=y.

3. Carlos Marcelo Ruales Casal. (2016). Auditoria de seguridad perimetral en dispositivos de capa 3 para entornos empresariales utilizando la herramienta kali linux. Página principal (http://repositorio.ug.edu.ec/handle/redug/11919). http://repositorio.ug.edu.ec/bitstream/redug/11919/1/B-CINT-PTG-N.73%20RUALES%20CASAL%20CARLOS%20MARCELO.pdf.

4. José Edwin González Retamozo. (2017). Auditoria de seguridad informática para la institución educativa departamental Luis Carlos Galán - municipio de Yacopí Cundinamarca. https://repository.unad.edu.co/bitstream/10596/17390/1/10188295.pdf

5. Versión ISO/IEC 27002:2013. http://iso27000.es/iso27002.html