**SISTEMA DE SEGURIDAD DE ACCESO PARA LAS OPCIONES DE LA
APLICACION DE CAPTACION DE LA PLATAFORMA WEB DEL BANCO AV
VILLAS**

CARLOS ANDRÉS SALAMANCA GALLO

**UNIVERSIDAD SANTO TOMÁS
DIVISIÓN DE INGENIERÍAS
FACULTAD DE INGENIERÍA ELECTRÓNICA
BOGOTÁ
2017**

**SISTEMA DE SEGURIDAD DE ACCESO PARA LAS OPCIONES DE LA
APLICACION DE CAPTACION DE LA PLATAFORMA WEB DEL BANCO AV
VILLAS**

CARLOS ANDRÉS SALAMANCA GALLO

**Proyecto de grado en la modalidad de Monografía presentado como
requisito para optar por el Título de Ingeniero Electrónico.**

Directores

**ING. FABIAN EDUARDO PEREZ GORDILLO
Universidad Santo Tomás**

**ING. DIEGO ABELARDO CRUZ ROJAS
Banco AV Villas**

**UNIVERSIDAD SANTO TOMÁS
DIVISIÓN DE INGENIERÍAS
FACULTAD DE INGENIERÍA ELECTRÓNICA
BOGOTÁ
2017**

TABLA DE CONTENIDO

INTRODUCCIÓN	6
1. PLANTEAMIENTO DEL PROBLEMA	8
2. JUSTIFICACIÓN	11
3. ANTECEDENTES	13
4. VISIÓN HUMANISTA DEL PROYECTO	15
5. OBJETIVOS	17
5.1. General	17
5.2. Específicos	17
6. FACTIBILIDAD	18
6.1. Recursos Humanos	18
6.2. Viabilidad Personal	18
6.3. Viabilidad Técnica	18
6.4. Viabilidad Temporal	19
6.5. Viabilidad Económica	19
7. MARCO TEÓRICO	20
7.1. Sistema RACF	20
7.2. Iso 27001 gestión de la seguridad de la información	21
7.3. Metodología desarrollo de software	21
7.4. Diagrama de flujo para requerimientos tecnológicos	22
7.5. Sistema operativo Z/OS	23
7.6. Relación de RACF con Z/OS	24
8. DESARROLLO Y RESULTADOS DEL SISTEMA	25
8.1. Opciones de aplicación de Captación	26
8.2. Requerimientos del Sistema	28
8.2.1. Requerimientos de las opciones de aplicación	30
8.3. Diseño del Sistema	34
8.3.1. Diseño del flujo de las opciones de aplicación	35
8.4. Implementación del Sistema	39
8.4.1. Asociación de códigos RACF	39
8.4.2. Programa Monitor	40
8.4.3. Programa Final	41

8.4.4. Programa de Validación	42
8.4.5. Documentación del desarrollo	43
8.4.6. Versionamiento de los desarrollos	44
8.5. Pruebas del Sistema	45
8.5.1. Prueba al flujo de las opciones	45
8.5.2. Prueba al sistema de seguridad de acceso	46
9. CONCLUSIONES	51
BIBLIOGRAFIA	53
ANEXOS	55
Anexo 1. Etapa de Diseño	55
Anexo 2. Etapa de Desarrollo	56
Anexo 3. Etapa de Pruebas y Producción	57

INDICE DE FIGURAS

<i>Figura.1 Grafica de Vulnerabilidad de la Información desde 1996 hasta 2015</i>	<i>8</i>
<i>Figura.2 Grafica de industrias más vulnerables respecto a la seguridad de la información.....</i>	<i>9</i>
<i>Figura.3 Validación de perfiles RACF.....</i>	<i>20</i>
<i>Figura.4 Esquema Metodología Ágil para Desarrollo de Software</i>	<i>22</i>
<i>Figura.5 Diagrama de asociación de RACF con Z/OS.....</i>	<i>24</i>
<i>Figura.6 Esquema general para la Etapa de Desarrollo.....</i>	<i>25</i>
<i>Figura.7 Modelo DAC y RACF en el Entorno Web de aplicaciones</i>	<i>26</i>
<i>Figura.8 Estructura Opciones de Aplicación.....</i>	<i>27</i>
<i>Figura.9 Diseño del sistema de seguridad de acceso.....</i>	<i>34</i>
<i>Figura.10 Flujo original opción “Desbloqueo de cuentas AFC”</i>	<i>35</i>
<i>Figura.11 Flujo modificado opción “Desbloqueo de cuentas AFC”</i>	<i>35</i>
<i>Figura.12 Flujo original opción “Fraccionamiento CDT’s”</i>	<i>36</i>
<i>Figura.13 Flujo modificado opción “Fraccionamiento CDT’s”</i>	<i>36</i>
<i>Figura.14 Flujo original opción “Bloqueo y Desbloqueo TD”</i>	<i>37</i>
<i>Figura.15 Flujo modificado opción “Bloqueo y Desbloqueo TD”</i>	<i>37</i>
<i>Figura.16 Flujo original opción “Manejo cuentas servicios públicos”.....</i>	<i>38</i>
<i>Figura.17 Flujo modificado opción “Manejo cuentas servicios públicos”</i>	<i>38</i>
<i>Figura.18 Proceso de asociación de los códigos RACF con las opciones de la aplicación de captación.....</i>	<i>39</i>
<i>Figura.19 Diagrama de flujo del programa monitor asociado a la base de datos de los códigos de transacción almacenados.....</i>	<i>40</i>
<i>Figura.20 Diagrama de flujo original y modificado del “programa final”</i>	<i>41</i>
<i>Figura.21 Diagrama de flujo del “Programa de Validación”</i>	<i>42</i>
<i>Figura.22 Plataforma de documentación del desarrollo “ClearQuest”</i>	<i>43</i>
<i>Figura.23 Árbol de versiones de los desarrollos en la plataforma “ClearCase”</i>	<i>44</i>

INTRODUCCIÓN

En la última década, la tecnología de la información se ha establecido como un concepto sólido en relación a las nuevas herramientas digitales que brindan soporte a las diferentes industrias y sectores de la economía. Para fortalecer este concepto en función de sistematizar y digitalizar la información, también han surgido adversidades propias de dicho avance y con mayor énfasis en aquellas compañías que han integrado toda la naturaleza de su negocio en plataformas digitales.

Para cuidar un recurso tan importante como lo es la información, surgen estrategias de seguridad a nivel interno y externo de una compañía, que buscan limitar el acceso para quienes se relacionan con la información¹.

Diferentes compañías, han implementado estas nuevas herramientas, y los Bancos son un claro ejemplo de adaptación a los nuevos entornos tecnológicos, puesto que las distintas operaciones y procesos que se realizan en estas compañías, en la actualidad se trabajan desde el entorno digital, ahorrando tiempo y recursos en la relación que se da entre el Banco y el Cliente.

El Banco AV Villas es una compañía financiera, miembro del grupo AVAL, que se dedica a realizar operaciones financieras con el dinero procedente de accionistas y clientes². Esta compañía se caracteriza por estar a la vanguardia de los nuevos desarrollos tecnológicos, buscando innovar y mejorar los diferentes productos y servicios que ofrece. Para ello es importante para el Banco contar con un área específica que se encargue de todos los temas relacionados a la tecnología de la información, por tal motivo se establece la Vicepresidencia de Operaciones y Tecnología, la cual se enfoca en todos aquellos proyectos de nivel tecnológico, dividiendo las temáticas de trabajo en áreas tales como la Gerencia de Desarrollo, la cual se orienta en generar desarrollos de software en función de las operaciones del negocio financiero.

Dentro de dichas operaciones está el área de Captación, la cual se dirige a todos los procesos financieros relacionados con aquellos productos y/o servicios que el Banco denomina pasivos. Estos procesos se relacionan con el dinero almacenado por el banco, el cual los clientes entregan ya sea en una cuenta de ahorros, una cuenta AFC o un CDT.

Esta área, cuenta con una dirección que trabaja en conjunto para la ejecución y soporte de aquellos proyectos tecnológicos que le brinden beneficio al negocio en las operaciones de Captación, dicho soporte es brindado por la Dirección de

¹ Banco AV Villas. SEGURIDAD INFORMACION. [En Línea]. 1a ed. Bogotá: Gerencia de Desarrollo. [Citado 13-Febrero-2017]. Disponible en internet: <http://gata/portalintranet/especiales2014/Contraloria/SeguridadInformacion/AsiManejamos.html>

² (LosBancos-Lectura. [En Línea]. [Citado 13-Febrero-2017]. Disponible en internet: <http://www.spanish.cl/Vocabulary/Notes/Bancos.htm>)

Proyectos de Captación, la cual se compone de cuatro áreas de respaldo para la operación que son³: i) El área de Bach, encargada de las operaciones tales como consolidación de movimiento y control de operaciones que se ejecutan fuera de línea, cuando el Banco finaliza sus operaciones diarias. ii) El área de Canales Virtuales que se encarga de la ejecución de proyectos de software que involucran principalmente canales electrónicos para persona natural, adicionalmente administra la relación técnica con el proveedor ATH y los proyectos afines. iii) El área de Canales que se encarga de la ejecución de proyectos que involucran principalmente canales presenciales (oficinas) y cobros. Finalmente iv) El área de Redes que se encarga de la ejecución de proyectos de software que involucran principalmente canales electrónicos para persona jurídica, ampliación de los canales electrónicos para persona natural a través de nuevas tecnologías como Transfer y CNB, Convenios y administra la relación técnica con las redes financieras como ACH, PSE, Redeban, VISA entre otros.

Este proyecto tiene como enfoque brindar apoyo a la dirección de proyectos de Captación, en el diseño e implementación de un sistema de seguridad de acceso para las opciones de la aplicación de Captación, mediante el desarrollo de software en las plataformas Z/OS y ASP.net, para ello se hace especial énfasis en las áreas relacionadas a la línea de programación.

Estos conocimientos han sido ya trabajados desde el ámbito académico en la Universidad Santo Tomás en la Facultad de Ingeniería Electrónica y el proyecto es adicionalmente una buena oportunidad para fortalecer la presencia de los ingenieros electrónicos dentro del sector financiero y para hacer énfasis en el ámbito humanista al tener como uno de los aspectos fundamentales el ahorro de recursos, evitando el desperdicio materiales e insumos en procesos de seguridad gracias a la implementación de herramientas digitales con la aplicación de la ingeniería electrónica.

³ Banco AV Villas. 1611-DIRECCIÓN PROYECTOS DE CAPTACIÓN. [En Línea]. 1a ed. Bogotá: Gerencia de Desarrollo. [Citado 13-Febrero-2017]. Disponible en internet: http://qata/portalintranet/neolntranet/SomosAVVillas/Dependencias/docs_tecnologia/GerenciaDesarrollo/1611DireccionProyectosCaptacion.pdf

1. PLANTEAMIENTO DEL PROBLEMA

La seguridad de la información es un concepto valioso para las empresas, puesto que cuidar este recurso no es una operación que se someta simplemente a controlar el acceso de información al público (clientes) respecto a datos y/o archivos, sino que también se debe contemplar el escenario interno de la compañía (colaboradores). Las opciones de la aplicación de Captación se encuentran actualmente es un alto grado de vulnerabilidad, puesto que no se ha establecido para esta área en específico un control de acceso que se encargue de gestionar quienes pueden hacer uso de estas opciones de aplicación en todo lo relacionado a procesos de Captación.

Diversas compañías brindan soporte a las entidades financieras en todos los aspectos relacionados con la seguridad de la información, como lo es el caso de IBM. Esta compañía presenta las siguientes estadísticas relacionadas con la vulnerabilidad de la información año tras año y las industrias más afectadas por este fenómeno⁴.

- La información es más vulnerable a medida que avanza la tecnología. En el año 2015 IBM reportó alrededor de 8000 casos relacionados con este tema en las compañías a las cuales brinda soporte (*Figura.1*) y la tendencia muestra que el fenómeno de la violación de datos va en aumento con el pasar del tiempo

Figura.1 Grafica de Vulnerabilidad de la Información desde 1996 hasta 2015

⁴ IBM. Estadísticas de la violación de Datos. [En Línea] [Citado 13-Febrero-2017]. Disponible en internet: <https://www.ibm.com/services/co/es/it-services/data-breach/data-breach-statistics.html>

- Las industrias con más ataques relacionados a la seguridad de la información son (*Figura.2*):

Figura.2 Grafica de industrias más vulnerables respecto a la seguridad de la información

Todos los procesos y operaciones en el Banco se manejan a través de una plataforma web, que utilizan los colaboradores de la compañía. Estos acceden con el documento de identidad y la clave de red. La plataforma cuenta con diferentes opciones de aplicación, clasificadas por áreas de operación, útil para simular procesos y conocer información bancaria. Cualquier colaborador, cuenta con acceso a la mayoría de las opciones de aplicación en la plataforma, sin embargo, esta condición se presenta como un problema, puesto que al no proteger todos los procesos, se pone en riesgo la seguridad de la información e incluso la operación financiera, generando así pérdidas significativas para la compañía.

La dirección de proyectos de Captación ha detectado como una amenaza potencial, la falta de control de acceso en las opciones de la aplicación de Captación, puesto que en dicha área se maneja todo lo que representa un pasivo para el Banco, referente al dinero que se guarda de los clientes. Las opciones van desde realizar la consulta de una cuenta, hasta modificar información y realizar bloqueos a las cuentas de los clientes; dichos procesos tienen un alto nivel de responsabilidad por lo que de igual manera el acceso a estas opciones no debería estar habilitado para cualquier colaborador, sino solamente para quienes sea de interés laboral, las operaciones del área de Captación.

Para el Banco AV Villas⁵ la información es su principal activo, por consiguiente es importante realizar una estrategia integral que vele por la seguridad de la información en diferentes niveles de la operación financiera y generar así un estándar para todos los colaboradores del Banco. Se debe proteger la información incluso de los operarios de diferentes áreas, puesto que la falta de seguridad de acceso en este tipo de información puede ocasionar incidentes, por ejemplo: fuga de información, abuso de contenido, violación de políticas corporativas y hasta robo de recursos económicos.

⁵ Banco AV Villas. Seguridad de la Información. [En Línea]. 1a ed. Bogotá: Dirección de Seguridad Informática. [Citado 13-Febrero-2017]. Disponible en internet: <http://gata/portalintranet/especiales2014/Contraloria/SeguridadInformacion/Incidentes.html#01>

2. JUSTIFICACIÓN

En la actualidad la seguridad de la información es uno de los principales temas de interés para los Bancos, puesto que el éxito operacional de estas compañías depende del cuidado que se le dé a la información a nivel interno y externo, tomado como referencia políticas de seguridad que permitan manejar la información y controlar su acceso, para brindar el soporte y la confiabilidad que los Bancos prometen a sus clientes respecto a la confidencialidad de la información.

Para ejecutar los diferentes procesos financieros, el Banco cuenta con diversos canales de interacción que incluyen aplicaciones (apps) de: seguridad, banca móvil, banca virtual, cajeros depositarios y dispensadores, centros de pago virtual (CPV); buscando de esta manera mejorar los recursos que se emplean en cualquier operación entre el Banco y el Cliente

El Banco AV Villas es una compañía que hace constante énfasis en el tema de la seguridad de la información. Para ello la Gerencia de Desarrollo, se somete a revisiones periódicas, por medio de auditorías con el fin de determinar que procesos no se están siguiendo a conformidad de las políticas propuestas. Se evidencia que el proceso en la plataforma web relacionado al área de Captación, tiene oportunidades de mejora, en aspectos puntuales como determinar el flujo apropiado para que un programa de la plataforma web se asocie a un único programa fuente, que le garantice su origen. Con ello se asegura la implementación de estrategias de control de acceso a las diferentes opciones de las aplicaciones de Captación, perfilando a los usuarios o grupos de usuario, y mediante este tipo de estrategias no apuntar solo hacia la consecución de resultados más precisos en la operación, sino que también influyen considerablemente en una disminución del riesgo informático a la que se expone el Banco en relación a todos sus productos de Captación y quien puede tener contacto con ellos.

Puesto que la información es el activo más importante para el Banco, es fundamental que el sistema de seguridad de acceso que se implemente respecto a este recurso, se desarrolle de manera integral, entendiendo todas las operaciones relacionadas al área de Captación tales como consultas, modificaciones e incluso bloqueos de aquellos productos que se relacionan con los pasivos del Banco y generar así un desarrollo capaz de brindar protección de acceso a las opciones de la aplicación relacionadas a esta área.

Las ventajas de implementar un sistema de seguridad de acceso para las opciones de la aplicación de Captación radican en los siguientes aspectos.⁶

- Minimizar riesgos operacionales al limitar el acceso del personal a las opciones de la aplicación, impidiendo la realización de modificaciones y consultas en los procesos relacionados al área de Captación.
- Evitar la destrucción o pérdida de información puesto que al perfilar a los colaboradores, las operaciones y desarrollos que se realicen en el área pueden ser monitoreados conociendo en detalle a los usuarios que intervienen en los procesos que se realicen en el área de Captación.
- Prevenir los impactos negativos de carácter financiero, legal y de imagen que pueden surgir, puesto que el Banco trabaja de manera integral en todas sus áreas y al verse comprometida en una de ellas, se puede generar pérdidas económicas que conlleve a graves consecuencias en los aspectos inicialmente mencionados.
- Optimizar el proceso relacionado a la seguridad de la información puesto que al implementar una estrategia de control preventivo, se ahorran recursos referentes a la protección de datos.
- Preservar la confidencialidad en los procesos internos del Banco, ya que al restringir el acceso en las opciones de la aplicación para quienes no es de interés el área de Captación, se previene las prácticas de manejo inadecuado de la información respecto a esta área.

Es importante que además de la implementación del sistema de seguridad de acceso, se cumpla con las políticas del Banco, en las que establece la necesidad de realizar la identificación, documentación y pruebas del sistema implementado, para verificar el éxito del proceso y así mismo, ajustar dicho sistema en beneficio de otras áreas diferentes del área de Captación que existan en el Banco.

⁶ Banco AV Villas. Ventajas de la Seguridad Informática. [En Línea]. 1a ed. Bogotá: Dirección de Seguridad Informática. [Citado 13-Febrero-2017]. Disponible en internet: <http://gata/portalintranet/especiales2014/Contraloria/SeguridadInformacion/ventajasseguridad.html#05>

3. ANTECEDENTES

El avance tecnológico y el proceso de digitalización, se han presentado como herramientas útiles para cualquier compañía, permitiendo que procesos tales como la administración y seguridad de la información se hagan de manera óptima y más eficiente.

Los Bancos han entendido esta dinámica, haciendo de las aplicaciones web y demás herramientas, sus principales aliados con respecto a las operaciones financieras. Con el avance de la tecnología, también surgen diferentes riesgos, acordes al nuevo panorama, tales como el robo de la información, así que se debe buscar proteger dicho recurso, estableciendo parámetros de seguridad de acceso respecto al manejo de la información. El Banco cuenta con determinadas políticas que son similares a las de entidades estatales como el Ministerio del Interior respecto a los sistemas de seguridad de acceso y que confrontan al sistema que actualmente está establecido en el Banco. Algunas de estas políticas son⁷:

- Proveer al Área de Desarrollo los programas fuente solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable.
- Llevar un registro actualizado de todos los programas fuente en uso, Indicando nombre del programa, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
- Administrar las distintas versiones de una aplicación.
- Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- Realizar las copias de Seguridad y pruebas de restauración de los programas fuente.

Con base en la necesidad de protección de la información el Banco AV Villas cuenta en la actualidad con un modelo de control de acceso discrecional (DAC),⁸ que se caracteriza por poseer un usuario dueño, con capacidad para establecer parámetros de seguridad o asignar los derechos a los objetos que desea, sin embargo este

⁷ Ministerio del Interior. DESARROLLO Y MANTENIMIENTO DE SISTEMAS MINISTERIO DEL INTERIOR. [En Línea]. Bogotá. MinInterior. [Citado 13-Febrero-2017]. Disponible en internet: www.mininterior.gov.co/sites/default/files/documentos/OIP-2014-PSI-Especificas-7%20Desarrollo.doc

⁸ Subinet. ¿Cuáles son los modelos de control de acceso? [En Línea]. [Citado 13-Febrero-2017]. Disponible en internet: <http://www.subinet.es/cuales-son-los-modelos-de-control-de-acceso/>

modelo, no está en armonía con las políticas de seguridad de la compañía puesto que si de alguna manera se ve comprometida la cuenta del usuario dueño, ya sea en un ataque informático por parte de un usuario anónimo, este podría tomar control sobre el usuario dueño y a su vez tomar control completo sobre el acceso, puesto que adquiere las capacidades del usuario dueño.

En adición al modelo de control de acceso actual (DAC), el Banco también tiene como característica para sus desarrollos, un modelo de flujo que se establece desde la opción en la página web, invocando un monitor el cual se dirige a un menú de submonitores desde donde se realiza la invocación del programa. Las políticas actuales no están en armonía con este tipo de flujo puesto que al poseer programas que comparten un mismo programa origen, la información puede ser interceptada y las restricciones de acceso se pueden confundir al no entender de forma exacta la dirección de invocación del programa.

En la Vicepresidencia de Operaciones y Tecnología se cuenta con un área responsable de la seguridad de acceso, la cual es el área de la Mesa de Servicios, que se encarga de gestionar todos los procesos de seguridad en diferentes categorías incluyendo el acceso. Dicha área se limita simplemente a otorgar vínculos de seguridad de acceso, pero si el vínculo tiene conflicto con el diseño de la opción de la aplicación, quien procede a solucionar este aspecto es el desarrollador encargado, puesto que la Mesa de Servicios simplemente cumple protocolos pero no realiza desarrollos de software.

Para verificar que se esté cumpliendo con lo que se establece en las políticas es indispensable llevar a cabo un proceso de auditoría que permita conocer factores como la validación de los datos de entrada, el procesamiento interno, las interfaces entre sistemas y la validación de los datos de salida.

Con la implementación del sistema de seguridad de acceso empleando RACF, es necesario cambiar el estándar de flujos que actualmente está establecido y complementar el modelo DAC, con la implementación del sistema propuesto en este proyecto.

4. VISIÓN HUMANISTA DEL PROYECTO

El desarrollo de este proyecto, se presenta como una situación oportuna para que desde el campo de la ingeniería sea posible brindar una solución creativa y ética que aporte a las necesidades de la sociedad, como se establece en la misión de la Universidad Santo Tomas⁹. Utilizando todo el conocimiento adquirido durante la formación académica para dar respaldo a una problemática del sector financiero y planteando estrategias que se direccionen al ahorro de recursos en la compañía, en función de aportar al medio ambiente.

Herbert Simon afirmaba que *“El ingeniero, y, más generalmente, el diseñador, tienen que ver con cómo deberían ser las cosas para alcanzar las metas.”* Es posible darse cuenta que en una disciplina como lo es el desarrollo de software, se tiene la capacidad de pensar en una estrategia de diseño que más allá de solucionar una necesidad tecnológica que demanda el mundo actual en el sector financiero, se piense también en que dicha solución que se plantea sea de beneficio para el ser humano que es quien desarrolla la tecnología. Pensar en el ser humano es pensar en su entorno y en todos aquellos recursos que le garanticen una buena calidad de vida. A través de la historia se evidencia que las grandes compañías hacen uso de diferentes recursos sin pensar en el impacto de sus herramientas en el ambiente.

En el caso del Banco AV Villas, que es una compañía de carácter financiero, el papel se usa como un recurso fundamental en cada una de las operaciones. A diario se utiliza gran cantidad de papel en diferentes escenarios del Banco y en muchas ocasiones sin ser necesario. El uso del papel está generando un impacto ambiental negativo y aunque se han propuesto estrategias internas como las practicas del reciclaje, la meta del Banco se enfoca en desaparecer dicho recurso de sus herramientas y hacer uso de cualquier medio tecnológico que pueda reemplazar el uso del papel, puesto que la información podría manejarse de manera digital. Por ello la importancia de implementar un sistema de seguridad de acceso a las opciones que contienen información. De esta manera se puede evitar hacer uso del papel en las operaciones del Banco, asegurando que la información se maneje de forma digital y se proteja de personal inescrupuloso.

Santo Tomás afirmaba que *“Cada hombre tiene que inventar su camino.”* Esta idea nos lleva a pensar que el Banco es el responsable de crear una conciencia ambiental en sus empleados, en todas las prácticas que se realizan en la compañía. Sin embargo cada colaborador debe ser consiente de manera personal sobre cuál es la mejor decisión que se debe tomar para las generaciones del futuro. Ser responsable con el medio ambiente es una decisión personal, pero a su vez colectiva ya que nos impacta a todos. Como ingeniero mediante el desarrollo de

⁹ (Universidad Santo Tomas.[En Línea]. 1ª ed. Bogotá: Misión Institucional. [Citado 13-Febrero-2017].Disponible en Internet: <http://www.usta.edu.co/index.php/nuestra-institucion/presentacion-1>)

software se ayuda a crear estrategias digitales en función del ahorro de recursos y se contribuye en la reducción del impacto ambiental.

Una hoja de papel requiere de 10 Litros de agua para su elaboración¹⁰. Ahora si se piensa en todo el papel que se utiliza a diario en el Banco, el gasto hídrico que se está generando es inimaginable. El enfoque de evolución de la compañía se debe orientar no solo a ser una empresa líder del sector financiero, sino también ser líder en cuanto a impacto ambiental positivo se refiere. La ingeniería es una herramienta útil ya que propone estrategias tecnológicas para lograr dicho enfoque. Es importante entender que la operación financiera involucra muchos más procesos que recibir y dar dinero. Es una operación integral que requiere de colaboradores que tengan una visión en función del beneficio humano.

¹⁰ (Huella hídrica de México en el contexto de Norteamérica. [En línea]. México [Citado 13-Febrero-2017]. Disponible en Internet: <http://www.huellahidrica.org/Reports/AgroDer,%202012.%20Huella%20h%C3%ADdrica%20en%20M%C3%A9xico.pdf>)

5. OBJETIVOS

5.1. General

- Diseñar e Implementar un sistema de seguridad de acceso para las opciones de la aplicación de Captación en la plataforma web del Banco AV Villas, empleando RACF (Resource Access Control Facility).

5.2. Específicos

- Determinar los requerimientos y parámetros de seguridad de acceso solicitados para las opciones de la aplicación de Captación del Banco AV Villas.
- Diseñar el sistema de seguridad de acceso para las opciones de la aplicación de Captación a partir de los requerimientos propuestos, siguiendo el ciclo de vida del software del Banco AV Villas.
- Implementar el sistema de seguridad de acceso con base en los requerimientos de RACF para las opciones de la aplicación de Captación del Banco AV Villas, haciendo uso de las plataformas Z/OS y ASP.net
- Realizar las pruebas de ejecución del sistema de seguridad de acceso, de acuerdo a los procedimientos establecidos por el Banco AV Villas.

6. FACTIBILIDAD

Para la implementación del sistema de seguridad de acceso en las opciones de la aplicación de Captación, se han considerado la viabilidad de recursos humanos, personales, técnicos, temporales y económicos como a continuación se evidencia.

6.1. Recursos Humanos

En cuanto a personal de apoyo involucrado, en la Dirección de Proyectos de Captación se cuenta con el Jefe de Desarrollo de Canales y Oficinas, el cual es Ingeniero de Sistemas con un trayectoria de más de diez años en el sector bancario en diferentes compañías como el Banco BBVA, el Fondo Horizonte Pensiones y actualmente el Banco AV Villas con experiencia en todos los temas relacionados a desarrollo de software. Por otra parte se cuenta con el soporte de un Ingeniero Electrónico quien actúa como tutor de la práctica por parte de la Universidad Santo Tomas, con una trayectoria de más de cuatro años en el sector educativo e industrial en diferentes compañías como EBSA, UNISANGIL, Ingeniería Strycon y actualmente la Universidad Santo Tomas con experiencia en temas relacionados al área de desarrollo de proyectos.

6.2. Viabilidad Personal

Para la realización del proyecto se cuenta con diferentes aptitudes, que se han adquirido durante la formación académica tales como, el análisis, la creatividad, la lógica de programación y conocimientos adquiridos durante la práctica empresarial tales como programación en Cobol y ASP, para dar solución a los problemas de desarrollo que se presenten durante las diferentes etapas del sistema de seguridad de acceso.

6.3. Viabilidad Técnica

Para el desarrollo del sistema de seguridad de acceso en cuanto a hardware se refiere, el Banco AV Villas cuenta con los equipos (computadores y servidores) necesarios para realizar el proyecto.

En términos de software, el Banco AV Villas cuenta con los entornos de desarrollo Z/os y ASP.net, los cuales permiten implementar el sistema RACF y establecer la interacción con las opciones de la aplicación de Captación en la página web, siguiendo el ciclo de vida del software. Adicional a esto se cuenta con diferentes manuales y herramientas de ayuda para el uso de los lenguajes informáticos que se utilizan. El Banco también proporciona información (bases de datos) que permite verificar el éxito del sistema a implementar, concediendo permisos para acceder a dicha información.

6.4. Viabilidad Temporal

El sistema de seguridad de acceso, se enfoca a diferentes opciones, por ende el resultado o sistema final, se entiende como diferentes desarrollos por cada opción. Tomando como base el ciclo de vida del software se establece un cronograma de tiempo de trabajo para cada opción en donde es posible llegar a la etapa de implementación del sistema en general.

6.5. Viabilidad Económica

La ejecución de este proyecto es posible gracias al apoyo económico brindado por parte del Banco hacia el practicante responsable del diseño e implementación del sistema, ofreciéndole las herramientas necesarias para el desarrollo del proyecto y respaldando económicamente al tutor de la compañía, el cual genera un soporte intelectual en el desarrollo del proyecto. La universidad también apoya al practicante, mediante el respaldo económico que brinda al tutor académico, el cual actúa como asesor del proyecto en términos metodológicos y académicos.

7. MARCO TEÓRICO

7.1. Sistema RACF

“Resource Access Control Facility” es un sistema de control de acceso de IBM para la plataforma Z/os, el cual establece diferentes reglas de seguridad, que se determinan en base a unas clases, las cuales se definen como un grupo de objetos, a quienes se les otorga determinado acceso a información confidencial, y a su vez si el objeto pertenece a una misma clase, se establece el mismo nivel de seguridad.

Hay dos tipos de clases: “normales” que son clases de acceso y “especiales” que son aquellas clases que se gobiernan por las clases normales, las cuales les otorgan acceso. Las clases especiales son de dos tipos: de “usuario” que se hacen cargo de la seguridad respecto al tipo de usuario y “dataset” las cuales tienen control sobre todo elemento susceptible de grabarse en disco o cinta

RACF se encarga de todo lo relacionado al sistema interno referente a procesos, subprocesos y muchas operaciones en Z/os, ejerciendo funciones como identificar y autenticar usuarios, autorizar el acceso a los usuarios a recursos privados, registro e informe de intentos de acceso no autorizado y medios de control de accesos a recursos¹¹. En la (Figura.3) se describe la verificación de perfiles de RACF.

Figura.3 Validación de perfiles RACF

¹¹ Kujaku. Seguridad en mainframe: Introducción al RACF. [En Línea]. [Citado 13-Febrero-2017] Disponible en internet: <http://www.sigt.net/software/seguridad-en-mainframe-introduccion-al-racf.html>

7.2. Iso 27001 gestión de la seguridad de la información

El Banco AV Villas se rige por la norma de seguridad ISO 27001, por lo que es pertinente hablar de la misma, definiéndola como una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa, mostrando como beneficios de su uso¹²:

- Identificar los riesgos y establecer controles para gestionarlos o eliminarlos.
- Confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información.
- Flexibilidad para adaptar los controles a todas las áreas de la empresa o solo a algunas seleccionadas.
- Conseguir que las partes interesadas y los clientes confíen en la protección de los datos.
- Demostrar conformidad y conseguir el estatus de proveedor preferente.
- Alcanzar las expectativas demostrando conformidad.

Teniendo en cuenta los beneficios anteriormente mencionados, el Banco puede certificarse para demostrar la transparencia y confiabilidad de sus operaciones.

7.3. Metodología desarrollo de software

El software se define en el glosario de IEEE Std.610¹³ como “programas, procedimientos y documentación y datos asociados, relacionados con la operación de un sistema informático”

El software está conformado por tres componentes, el primero hace referencia a los programas que son aquellas instrucciones para ejecutar determinada operación o proceso. El segundo hace referencia a los datos, que son útiles para manipular y realizar pruebas sobre el programa. El tercer componente es la documentación en la cual se especifica y registra en el proceso todo lo relacionado con el programa y los datos del software.¹⁴

El desarrollo de software se compone de diferentes etapas desde que se realiza el diseño hasta que el software elaborado debe ser reemplazado, a esto se le

¹² Bsigroup. Sistema de gestión ISO/IEC 27001 de Seguridad de la Información [En Línea]. [Citado 13-Febrero-2017] Disponible en: <https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/>

¹³ IEEE. IEEE Standard Computer Dictionary. [En Línea]. [Citado 13-Febrero-2017] Disponible en internet: <https://standards.ieee.org/findstds/standard/610-1990.html>

¹⁴ Laboratorio Nacional de Calidad del Software de INTECO. INGENIERÍA DEL SOFTWARE: METODOLOGÍAS Y CICLOS DE VIDA. [En Línea]. 1a ed. España: Inteco. [Citado 13-Febrero-2017]. Disponible en internet: http://datateca.unad.edu.co/contenidos/301569/guia_de_ingenieria_del_software.pdf

denomina ciclo de vida del software y en el Banco también se hace uso de esta metodología.

Hay diferentes modelos para los Ciclos de Vida, sin embargo el Banco emplea la Metodología Ágil para Desarrollo de Software: “Proceso Unificado Ágil (AUP)” como se muestra en la (Figura.4). En esta metodología se generan diferentes etapas como lo son la planificación, análisis de requisitos, diseño, codificación, pruebas y documentación. Esta metodología permite desempeñar un trabajo multidisciplinario con otras áreas de Banco, en función del proyecto propuesto.¹⁵

Figura.4 Esquema Metodología Ágil para Desarrollo de Software

7.4. Diagrama de flujo para requerimientos tecnológicos

Los proyectos en el Banco AV Villas, se plantean a partir de una necesidad específica de la compañía, y dependiendo de esta, se establece un diagrama de flujo para entender el ciclo de vida del software que permite abordar el proyecto desde su etapa inicial de desarrollo, hasta su etapa final de producción. Los proyectos se conforman de cuatro etapas.

La primera es la Etapa de Diseño, en la cual se plantea la necesidad o requerimiento por parte del Banco, para después evaluar su factibilidad y una vez aprobado se procede al desarrollo, asignando la jefatura correspondiente al proyecto y avanzando a la siguiente etapa. (Ver Anexo 1).

¹⁵ Metodologías Ágiles. [En Línea]. [Citado 13-Febrero-2017]. Disponible en internet: <http://blog.leanmonitor.com/es/que-son-las-metodologias-agiles/>

La segunda es la Etapa de Desarrollo, en la cual se realiza la implementación del diseño, y la programación correspondiente al requerimiento (*Ver Anexo 2*).

Finalmente las Etapas de Prueba y Producción, en las que después de tener el desarrollo correspondiente al requerimiento, se procede a la búsqueda de las posibles fallas o irregularidades de este, realizando la simulación de diferentes situaciones y procesos, para comprobar que el desarrollo sea útil y se da por hecho que cuando las pruebas realizadas tanto de ejecución como de certificación, son superadas, se procede a realiza la implementación del desarrollo. (*Ver Anexo 3*).

7.5. Sistema operativo Z/OS

El Banco AV Villas cuenta con un sistema operativo IBM Z/OS o conocido por los colaboradores de manera informal como el Z, el cual se caracteriza por ser muy seguro, escalable y abierto, proporciona un rendimiento elevado que da soporte a un entorno de ejecución de diversas aplicaciones.¹⁶

El lenguaje de programación del Z es “COBOL” (Common Business Oriented Language) que se caracteriza por ser un lenguaje estándar que puede ser compilado y ejecutado en máquinas como IBM AS/400, ordenadores personales, etc.¹⁷

Para trabajar en la plataforma de Z/OS es necesario hacer uso de un método conocido como TSO (Time Sharing Option) el cual se define como una sesión temporal de trabajo en Z, para que quien acceda cuente con un usuario y contraseña, en donde se generen los diferentes desarrollos y librerías de quien se establezca en dicha sesión

El procesamiento en el Z se puede dar de dos maneras; la primera en LINEA la cual se utiliza para procesar transacciones con poco volumen de información para obtener resultados en tiempo real, por ejemplo cuando un usuario se acerca a un cajero para solicitar un saldo. La segunda manera es en BATCH la cual se usa para procesar grandes volúmenes de datos en una sola ejecución con el fin de evitar desaprovechar los recursos del sistema.¹⁸

En el Z se manejan diferentes procesos como los Programas Batch, los programas CICS o Monitores referentes a los procesamiento en LINEA, aquí el CICS actúa como una interface entre el sistema operativo y los programas de aplicación online. Otros procesos como los Copys que son la definición de la estructura de los archivos. Por último los JCL's que son declaraciones y ordenes con las que se indica

¹⁶ IBM. z/Architecture y el sistema operativo z/OS.[En Línea]. [Citado 13-Febrero-2017]. Disponible en internet: https://www.ibm.com/support/knowledgecenter/es/SSEPEK_10.0.0/intro/src/tpc/db2z_zarchitectureandzos.htm

¹⁷ Tutorialspoint. COBOL - Descripción General. [En Línea][Citado 13-Febrero-2017]. Disponible en internet: https://www.tutorialspoint.com/es/cobol/cobol_overview.htm

¹⁸ Contact&BusinessIT. Capacitacion Cobol. [En Línea] [Citado 13-Febrero-2017]. Disponible en internet: <http://gata/portalintranet/neohtranet/GestionesAplicacion/Formacion/Manuales/PRESENTACIONCOBOL2.pdf>. p.76

al sistema operativo que tareas debe realizar y en que secuencia han de ejecutarse¹⁹

7.6. Relación de RACF con Z/OS

Un caso particular que se presenta en el Banco puede ser cuando el usuario requiere acceder a algún determinado recurso o aplicación, usando un método de acceso que puede ser TSO, y este método envía un requerimiento a RACF para ver si el usuario tiene acceso o no al recurso, así que RACF realiza la gestión en su base de datos o en los registros existentes en memoria y revisa si el perfil es apto y cumple las condiciones; con base en esta información RACF pasa el estatus de requerimientos al método de acceso y este método le concede o niega el acceso requerido al usuario. En las (Figura.5) se ilustra el proceso²⁰

Figura.5 Diagrama de asociación de RACF con Z/OS

¹⁹ Contact&BusinessIT. Capacitacion Cobol. Op. Cit., p. 78

²⁰ Erik Zepeda. Introducción a RACF [En Línea]. [Citado 13-Febrero-2017] Disponible en: <http://cryptomex.org/SlidesMainframes/IntroRACF.pdf>

8. DESARROLLO Y RESULTADOS DEL SISTEMA

En términos tecnológicos el Banco AV Villas cuenta con un área conocida como la Gerencia de Desarrollo, que se encarga de realizar la ejecución de proyectos de software que brindan soluciones informáticas a los productos y servicios de la compañía. A su vez esta área se divide en diferentes direcciones, las cuales se responsabilizan de la ejecución de proyectos de desarrollo dependiendo la operación financiera.

Una de estas direcciones, es la dirección de proyectos de Captación, que se encarga de la ejecución de todos los desarrollos de software relacionados con los productos que representan un pasivo, como lo son las cuentas de ahorro, AFC o CDT's.

La implementación del sistema de seguridad de acceso en las opciones de aplicación de Captación, se maneja como un proceso que aborda distintas operaciones financieras e información de diferente naturaleza, relacionada en un entorno web en función de las necesidades del área de Captación. Este proceso es importante para el Banco y por tal razón se busca que el acceso a las opciones de aplicación se restrinja para quienes no corresponda el uso de determinadas operaciones que se ejecutan en el área de Captación.

Para implementar el sistema de seguridad de acceso, es fundamental tener claridad sobre el proceso a trabajar en la Etapa de Desarrollo, para ello se plantea el esquema de la (Figura.6).

Figura.6 Esquema general para la Etapa de Desarrollo.

El desarrollo del proyecto se aborda por etapas y cada una de ellas corresponde a determinada opción de aplicación del área de Captación, “ETAPA 1, ETAPA 2,..., ETAPA n” sin embargo la manera de abordar la implementación cumple con un mismo esquema para las diferentes opciones. La “ETAPA DESARROLLO” finaliza una vez se han abordado las “N” opciones de aplicación. Se procede a la “ETAPA PRUEBAS” en la cual el área de pruebas del Banco verifica que los desarrollos implementados, sean acordes a los requerimientos establecidos en el desarrollo. Finalmente esta la “ETAPA PRODUCCION” que es el ambiente de trabajo para todos los colaboradores del Banco.

Las opciones de aplicación del Banco AV Villas poseen un modelo de control de acceso discrecional (DAC). Este permite el acceso al entorno web por parte de los colaboradores cuando el usuario dueño otorga los permisos. Los jefes de área del Banco son quienes pueden decidir quién de sus colaboradores a cargo puede acceder o no al entorno web. Sin embargo una vez que el colaborador tiene acceso al entorno, también posee la libertad de acceso a las diferentes opciones de aplicación. El área de Captación busca evitar el acceso a sus opciones de aplicación en específico, mediante el uso del modelo de seguridad RACF, como se muestra en la (Figura.7).

Figura.7 Modelo DAC y RACF en el Entorno Web de aplicaciones

Para dar solución al modelo que está presente en la actualidad con respecto al sistema de acceso a las opciones de aplicación, el área de Captación establece diferentes requerimientos. Estos trazan los parámetros de direccionamiento para el diseño e implementación del sistema de seguridad de acceso y permiten conocer en detalle la necesidad a solucionar para el área de Captación.

8.1. Opciones de aplicación de Captación

El Banco AV Villas cuenta con una plataforma web compuesta de diferentes aplicaciones: Captación, Convenios, Cartera, Tesorería, entre otras aplicaciones. Estas aplicaciones a su vez poseen diferentes opciones dependiendo el producto o servicio que se relacione con la aplicación. Para el caso de la aplicación de Captación, los productos y/o servicios que se relacionan con sus opciones son todos aquellos que representen un pasivo para la compañía como: las cuentas de ahorro, cuentas AFC, CDT's, entre otros. Finalmente cada opción posee una o varias

funciones que pueden ser: consulta, modificación, adición, bloqueo, desbloqueo, entre otras. (Figura.8).

Figura.8 Estructura Opciones de Aplicación

La aplicación de Captación cuenta con cuatro opciones sobre las cuales se realiza la ejecución del sistema de seguridad de acceso. Estas opciones son:

- Desbloqueo de Cuentas AFC.
- Fraccionamiento CDT's
- Bloqueo y Desbloqueo Tarjetas Débito
- Manejo Cuentas Servicios Públicos

Cada opción contiene diferentes funciones, que permiten al colaborador realizar determinadas operaciones con respecto a un producto y/o servicio del Banco. Las funciones para cada opción se muestran en la (Tabla. 1).

OPCION	FUNCIONES		
1. Desbloqueo de Cuentas AFC.	Consultar	Desbloquear	
2. Fraccionamiento CDT's	Consultar	Fraccionar	
3. Bloqueo y Desbloqueo Tarjetas Débito	Bloqueo	Desbloqueo	
4. Manejo Cuentas Servicios Públicos	Consultar	Adicionar	Modificar

Tabla 1. Funciones de las opciones de aplicación de Captación

8.2. Requerimientos del Sistema

Para la implementación del Sistema de Seguridad de Acceso, es importante cumplir con los parámetros que el Banco AV Villas establece dentro de sus requerimientos, de esta manera se estandariza el desarrollo realizado y se respetan diferentes normativas de diseño y funcionamiento. Esta dinámica es de beneficio para los desarrolladores al momento de generar soporte sobre el desarrollo o buscar la expansión del mismo. Para un proyecto de seguridad, se deben tener presentes algunos requerimientos especiales que sirven como directriz para realizar el diseño e implementación del sistema. En términos generales estos requerimientos son:

- ***El desarrollo debe ser técnico, no funcional:*** El sistema que se implementa debe ser capaz de satisfacer las necesidades de seguridad de acceso que aún no están presentes en las opciones de la aplicación de Captación. Esto se logra realizando desarrollos técnicos que permitan la ejecución del proyecto. Sin embargo la funcionalidad de las opciones no debe verse afectada, puesto que el proyecto no establece modificaciones respecto a la dinámica de funcionamiento en las opciones de la aplicación de Captación. Para validar este requerimiento se evalúa el funcionamiento de la opción antes y después de su asociación con el sistema de seguridad de acceso.
- ***El programa final no debe compartir opciones:*** Cada opción es invocada desde una página que a su vez envía un código de transacción y el nombre de un programa monitor asociado. En el programa monitor se direcciona la ruta de la opción a un programa final. Sin embargo para el sistema de seguridad de acceso se establece que el programa final no puede compartir dos opciones. Se puede presentar un caso en el que la seguridad que se establece en una opción no sea la misma seguridad que necesite la otra opción y al compartir el programa final no sería posible establecer la seguridad de manera independiente para cada opción.
- ***El programa final no debe compartir funciones:*** Una opción puede tener funciones de consulta y bloqueo, sin embargo estas funciones no deben estar en el mismo programa final. Al establecer la seguridad de acceso para un programa final, también se otorga permisos de uso a las funciones que estén presentes en dicho programa final. El sistema de seguridad de acceso también busca separar el acceso a las funciones ya que no todas las personas que realizan labores de consulta, están autorizadas para realizar labores de bloqueo. Se debe restringir el uso de las funciones dependiendo la opción y el nivel de importancia de la misma para las operaciones bancarias.

- ***El programa final no debe compartir motivos:*** Una opción puede tener funciones de consulta y bloqueo, sin embargo la función de bloqueo se puede asociar a diferentes motivos que son las razones para realizar el bloqueo. En algunas ocasiones cada motivo debe estar asociado a un programa final por separado. Dependiendo la naturaleza del motivo para realizar un bloqueo las características de seguridad de acceso y el colaborador que puede realizar esta operación varía. Así que todos los motivos no pueden estar habilitados para los mismos colaboradores en una operación de bloqueo.
- ***Asignación de códigos RACF:*** La opción debe tener asociado un código de identificación que se vincule con las personas que tienen permitido el acceso a la opción de la aplicación de Captación. Si la opción cuenta con diferentes funciones, se genera un código por cada función. De esta manera se facilita la labor de permisos con el área de mesa de servicios la cual otorga los permisos de acceso en el Banco AV Villas.

8.2.1. Requerimientos de las opciones de aplicación

Después de conocer los aspectos generales de los requerimientos del proyecto, se aborda cada opción en específico y se determinan diferentes aspectos que permiten entender las siguientes etapas del desarrollo para cada opción con base en los requerimientos mencionados anteriormente.

1. DESBLOQUEO DE CUENTAS AFC.	FUNCIONES	
	Consultar	Desbloquear

Descripción y casos de uso	
<p>La opción “Desbloqueo de cuentas AFC” utiliza como datos de entrada el número de cuenta y la fecha en que se realizó el bloqueo. Con esta información se valida la función de consulta para conocer el motivo o los motivos que generaron el bloqueo de la cuenta y se habilita la función desbloquear. La respuesta a la operación de desbloqueo habilita la cuenta o elimina los motivos por los que se generó el bloqueo.</p>	
Situación actual	Situación planteada
<p>Los motivos de desbloqueo de las cuentas AFC comparten el mismo programa final para la función de desbloqueo. Cuando se genera la operación de desbloqueo de una cuenta sin importar el motivo con el cual se esté realizando la operación se envía desde la página un código de transacción que direcciona a un único programa final para todos los motivos.</p>	<p>Se realiza un desarrollo que permita separar el flujo de los diferentes motivos, generando códigos de transacción independientes y un programa final para cada motivo. De esta manera se cumple con los requerimientos planteados y posteriormente se asocia el código RACF para definir los perfiles que tendrán acceso a la función de desbloqueo dependiendo el motivo.</p>
Plataformas	
<ul style="list-style-type: none"> • Z/os: Se genera el desarrollo correspondiente al programa final por cada motivo y se modifican códigos de transacción. 	
Tipo de novedad	
<ul style="list-style-type: none"> • Modificación de la ruta de los programas • Generación de programas nuevos 	
Casos de uso RACF	
<p>Consultar: No se asigna código RACF en la consulta, así que cualquier persona puede realizar la operación de consulta.</p>	<p>Desbloquear: se asigna código RACF a cada programa final que se vincula a un motivo. Algunos motivos son:</p> <p>-Titular fallecido/ Intento de fraude/Bloqueo por embargo/Error del cajero, etc.</p>

2. FRACCIONAMIENTO CDT'S	FUNCIONES	
	<i>Consultar</i>	<i>Fraccionar</i>

Descripción y casos de uso	
<p>La opción “Fraccionamiento CDT's” utiliza como datos de entrada los datos del Cliente, datos del certificado a fraccionar y el selector de función. Si se valida la función de consulta, la respuesta a la operación muestra el historial de fraccionamiento que existe sobre el título. En caso de validar la función fraccionar, la respuesta a la operación realiza el fraccionamiento sobre el título.</p>	
Situación actual	Situación planteada
Las funciones “Consultar” y “Fraccionar” comparten el mismo programa final. Se envía un código de transacción distinto para cada función, sin embargo ambos códigos se direccionan al mismo programa final.	Se realiza un desarrollo que permita separar el flujo de las funciones, en este caso ya hay dos códigos de transacción, por lo tanto a cada uno se debe asignar un programa final dependiendo la función.
Plataformas	
<ul style="list-style-type: none"> • Z/os: Se genera el desarrollo correspondiente al programa final por cada función y se modifican códigos de transacción. 	
Tipo de novedad	
<ul style="list-style-type: none"> • Modificación de la ruta de los programas • Generación de programas nuevos 	
Casos de uso RACF	
Consultar: se asigna código RACF al programa final que se vincula a la función.	Fraccionar: se asigna código RACF al programa final que se vincula a la función.

3. BLOQUEO Y DESBLOQUEO TARJETAS DÉBITO	FUNCIONES	
	Bloqueo	Desbloqueo

Descripción y casos de uso	
<p>La opción “Bloqueo y Desbloqueo tarjetas débito” utiliza como datos de entrada el número de la tarjeta, el selector de función y el selector de motivo. Si se valida la función de bloqueo, esta debe coincidir con los posibles motivos de bloqueo y la respuesta a la operación realiza el bloqueo, en caso de que ya exista bloqueo, la respuesta lo indica. Si se valida la función de desbloqueo, esta debe coincidir con el único motivo asociado a desbloqueo y la respuesta a la operación realiza el desbloqueo, en caso de que ya exista el desbloqueo, la respuesta indica esta condición.</p>	
Situación actual	Situación planteada
<p>Los motivos de bloqueo de las tarjetas débito comparten el mismo programa final. Cuando se procede a realizar la operación de bloqueo para una TD todos los motivos envían el mismo código de transacción y este se direcciona a un solo programa final para todos los motivos.</p>	<p>Se realiza un desarrollo que permita separar el flujo de los motivos asociados a la función de bloqueo. Se genera un programa final para cada motivo y también se asocian códigos de transacción diferentes.</p>
Plataformas	
<ul style="list-style-type: none"> • Z/os: Se genera el desarrollo correspondiente al programa final por cada motivo y se modifican códigos de transacción. 	
Tipo de novedad	
<ul style="list-style-type: none"> • Modificación de la ruta de los programas • Generación de programas nuevos 	
Casos de uso RACF	
<p>Bloqueo: se asigna código RACF a cada programa final que se vincula a un motivo. Algunos motivos son:</p> <p>-Deterioro/Robo o Pérdida/Fraude, etc.</p>	<p>Desbloqueo: se asigna código RACF al programa final que se vincula al motivo:</p> <p>-Cambio de estado.</p>

4. MANEJO CUENTAS SERVICIOS PÚBLICOS	FUNCIONES		
	Consultar	Adicionar	Modificar

Descripción y casos de uso	
<p>La opción “Manejo cuentas servicios públicos” utiliza como datos de entrada el número de cuenta, y el selector de función. Al validar la función de consulta, la respuesta a la operación muestra si la cuenta esta activa o inactiva. Si se valida la función de adición, la respuesta a la operación permite adicionar una nueva cuenta y su estado correspondiente. Si se valida la función de modificación, la respuesta a la operación permite modificar el estado de la cuenta sobre la que se está haciendo la modificación y se puede pasar de estado activo a inactivo y viceversa.</p>	
Situación actual	Situación planteada
Las funciones “Consultar”, “Adicionar” y “Modificar” comparten el mismo programa final. Se envía un código de transacción para la consulta y un código de transacción para la adición y modificación, sin embargo ambos códigos se direccionan al mismo programa final.	Se realiza un desarrollo que permita separar el flujo de las funciones, en este caso ya hay dos códigos de transacción, pero es necesario que exista un flujo por cada función. Se debe vincular un código más y también realizar la separación de las funciones en el programa final.
Plataformas	
<ul style="list-style-type: none"> • Z/os: Se genera el desarrollo correspondiente al programa final por cada motivo y se modifican códigos de transacción. 	
Tipo de novedad	
<ul style="list-style-type: none"> • Modificación de la ruta de los programas • Generación de programas nuevos 	
Casos de uso RACF	
Consultar: se asigna código RACF al programa final de esta función.	Adicionar: se asigna código RACF al programa final de esta función. Modificar: se asigna código RACF al programa final de esta función.

8.3. Diseño del Sistema

De acuerdo con los requerimientos establecidos, la etapa de diseño permite entender gráficamente la situación actual y la situación planteada de las opciones de aplicación de Captación. Para proceder a la etapa de implementación es fundamental se realice el diseño del sistema. También se analiza una estrategia que permita modificar el flujo de cada opción y el uso del protocolo RACF en el sistema, tomando como referencia los requerimientos de cada opción para la ejecución del diseño.

En la (Figura.9) se muestra el diseño del sistema de seguridad de acceso. Los datos de entrada del sistema son: a.) El registro de identificación del usuario que accede a una opción de aplicación y b.) Los códigos RACF que se asocian con cada opción de aplicación y a su vez identifican a un grupo específico de usuarios.

Con la información de entrada en el “programa de validación” se analiza si el usuario que requiere acceder a la opción tiene el permiso necesario para continuar con la operación. En caso de tener permisos, se realiza el acceso a la plataforma Z la cual suministra la información que el usuario requiere de la opción a la que accede y como respuesta a la operación se envía el resultado de la función que requiera el usuario. En caso de no tener el permiso, se restringe el acceso a la plataforma Z y la respuesta a la operación es un mensaje que indica que el usuario no tiene permiso para acceder.

Figura.9 Diseño del sistema de seguridad de acceso.

8.3.1. Diseño del flujo de las opciones de aplicación

1. DESBLOQUEO DE CUENTAS AFC.	FUNCIONES	
	Consultar	Desbloquear

En la (Figura.10) se muestra el flujo original de la opción “Desbloqueo de cuentas AFC”. Desde la página se envía la trama o llave de información, que contiene los datos de entrada de la opción y el correspondiente código de transacción asociado a cada función. En el programa monitor se realiza la asociación con la plataforma Z. Se direcciona la llave al programa final teniendo en cuenta el código de transacción e identificación del programa final. Para la función de desbloqueo se comparten los motivos de desbloqueo.

Figura.10 Flujo original opción “Desbloqueo de cuentas AFC”

En la (Figura.11) se muestra el flujo modificado de la opción “Desbloqueo de cuentas AFC”. Cuando la trama de información llega al programa monitor en la plataforma Z, se realiza la asignación un código de transacción para cada motivo y se cambia el programa final que antes se compartía para cada opción por un programa final por cada opción.

Figura.11 Flujo modificado opción “Desbloqueo de cuentas AFC”

2. FRACCIONAMIENTO CDT'S	FUNCIONES	
	Consultar	Fraccionar

En la (Figura.12) se muestra el flujo original de la opción “Fraccionamiento CDT’s”. Desde la página se envía la trama o llave de información, que contiene los datos de entrada de la opción y el correspondiente código de transacción asociado a cada función. En el programa monitor se realiza la asociación con la plataforma Z. En esta opción se presentan dos códigos de transacción para las funciones que se dirigen al mismo programa final.

Figura.12 Flujo original opción “Fraccionamiento CDT’s”

En la (Figura.13) se muestra el flujo modificado de la opción “Fraccionamiento CDT’s”. El flujo cuenta con un código de transacción para cada función, así que en el programa monitor se realiza la asociación con cada programa final y se separan las funciones.

Figura.13 Flujo modificado opción “Fraccionamiento CDT’s”

3. BLOQUEO Y DESBLOQUEO TARJETAS DÉBITO

FUNCIONES	
Bloqueo	Desbloqueo

En la (Figura.14) se muestra el flujo original de la opción “Bloqueo y Desbloqueo TD”. Desde la página se envía la trama o llave de información, que contiene los datos de entrada de la opción y el correspondiente código de transacción asociado a cada función. En el programa monitor se realiza la asociación con la plataforma Z. La función de bloqueo tiene diferentes motivos que comparten el mismo código de transacción y programa final.

Figura.14 Flujo original opción “Bloqueo y Desbloqueo TD”

En la (Figura.15) se muestra el flujo modificado de la opción “Bloqueo y Desbloqueo TD”. Se asigna un código de transacción y un programa final a cada motivo de la función de bloqueo. En el programa monitor se realiza la asignación de los códigos de transacción.

Figura.15 Flujo modificado opción “Bloqueo y Desbloqueo TD”

4. MANEJO CUENTAS SERVICIOS PÚBLICOS

FUNCIONES		
Consultar	Adicionar	Modificar

En la (Figura.16) se muestra el flujo original de la opción “Manejo cuentas servicios públicos”. Desde la página se envía la trama o llave de información, que contiene los datos de entrada de la opción y el correspondiente código de transacción asociado a cada función. En el programa monitor se realiza la asociación con la plataforma Z. En esta opción las funciones de adición y modificación comparten código de transacción, la función de consulta utiliza otro código de transacción y las tres funciones comparten programa final.

Figura.16 Flujo original opción “Manejo cuentas servicios públicos”

En la (Figura.17) se muestra el flujo modificado de la opción “Manejo cuentas servicios públicos”. Se asigna un código de transacción y un programa final para cada función. En el programa monitor se realiza la asignación de los códigos de transacción.

Figura.17 Flujo modificado opción “Manejo cuentas servicios públicos”

8.4. Implementación del Sistema

Después de entender los requerimientos establecidos para cada opción y presentar un diseño en función de las necesidades del sistema de seguridad de acceso, se procede a realizar la implementación de los diferentes programas y desarrollos que se proponen en la etapa de diseño respecto a los flujos de las opciones y del sistema en general. Se presentan diagramas de flujo de los desarrollos realizados en las opciones de la aplicación y del programa de validación. También se muestra el proceso de asociación de los códigos RACF en los programas de las opciones.

8.4.1. Asociación de códigos RACF

Para implementar el sistema de seguridad de acceso, es fundamental asociar los códigos de RACF con las opciones de la aplicación. Mediante el documento: orden de proceso “OP” como se muestra en la (Figura.18). Se presenta la información referente al desarrollo realizado y se envía al área de “Mesa de servicio” que se encarga de suministrar los códigos que se usaran para las opciones de la aplicación de Captación. Después de obtener los códigos, la “OP” se pasa al Jefe de Captación para verificar la documentación del desarrollo y matricular los códigos RACF en los programas finales que se adjuntan en la “OP”. Una vez el jefe aprueba la documentación, la “OP” pasa al director del área el cual también realiza una revisión de la documentación y finalmente asocia los usuarios que pueden tener acceso a las diferentes opciones, dependiendo las funciones y motivos que se presenten. Así se genera una base de datos “Códigos RACF” que sirve como utilitario de búsqueda para el sistema de seguridad de acceso que se implementa.

Figura.18 Proceso de asociación de los códigos RACF con las opciones de la aplicación de captación.

8.4.2. Programa Monitor

En este programa se definen los códigos de transacción que se relacionan con la página de la opción de aplicación, como se muestra en la (Figura.19). Inicialmente se recibe la llave de información en una sección del programa que se conoce como “*Linkage Section*” la cual recibe y envía información de la llave. Después de obtener la información se realiza la lectura de la llave de información que contiene los datos de interés respecto a la opción tales como la identificación del usuario, el registro de la opción, datos referentes a la opción en caso de completar o suministrar información y los códigos de transacción. Estos se almacenan en una sección del código del programa conocida como “*Working Storage Section*” la cual relaciona los códigos de transacción con un programa en la plataforma Z. Para adicionar nuevos códigos de transacción, se utiliza el espacio libre de la llave de información y se definen los códigos, también en el programa monitor se realiza el registro de dichos códigos y se relacionan con el programa que se necesita vincular.

Figura.19 Diagrama de flujo del programa monitor asociado a la base de datos de los códigos de transacción almacenados.

8.4.3. Programa Final

Cuando se realiza la modificación del flujo de las opciones, también se debe modificar la estructura del programa final. La dinámica general del programa final de las opciones, se basa en un proceso en el cual se recibe la información de la llave que viene desde la página y ha pasado por el programa monitor. Después se realiza la lectura de dicha llave de información y se valida la función o el motivo del programa al que se accede para después preguntar por el motivo o la función del que se requiere la operación y se ejecuta el proceso. Con la modificación del flujo de las opciones el programa ahora recibe la información, hace la lectura de la llave de información y ya no realiza un proceso de validación para una función o motivo, sino que realiza la validación del usuario con el sistema de seguridad de acceso y si recibe el acceso por parte del sistema ejecuta la operación de la opción. Como se muestra en la (Figura.20)

Figura.20 Diagrama de flujo original y modificado del "programa final"

8.4.4. Programa de Validación

En la (Figura.21) se muestra el diagrama de flujo referente a la implementación del programa de validación que se presenta como un componente del diseño del sistema. En este se recibe información de la identificación de los usuarios del área de Captación y en una etapa inicial se consulta si la persona que quiere acceder a la opción, pertenece al área. En caso de pertenecer se evalúa la función con la que quiere realizar la operación y mediante los códigos RACF que se relacionan con cada opción se analiza si la persona puede o no acceder a la función. En caso de que la función posea diferentes motivos, se verifica que el usuario tenga acceso al motivo y finalmente se ejecuta el enlace con el programa final de la plataforma Z, el cual gestiona la información suministrada y brinda una respuesta a determinada operación.

Figura.21 Diagrama de flujo del "Programa de Validación"

8.4.5. Documentación del desarrollo

Después de realizar los desarrollos correspondientes al sistema y al flujo de las opciones se genera la documentación técnica y de soporte, la cual sirve como herramienta de ayuda para modificaciones posteriores en los desarrollos o como guía para otros desarrolladores que aborden el proyecto.

Como se muestra en la (Figura.22) en la plataforma de CLEARQUEST se adjunta la documentación del desarrollo y las versiones que se generan de cada programa trabajado en el desarrollo. Esta información es revisada por el Jefe de Área quien avala el desarrollo y de esta manera se pasa de la etapa de desarrollo a la etapa de pruebas.

Actividad: REQPR00237520

General Otros Criterios Observaciones Objetos PermisosCC Adjuntos Información Requerimiento ClearCase UCM Matriculas Carpetas de Intercambio

Ordenes De Proceso Actividades Relacionadas Sincronización de actividades Devoluciones Despliegues Histórico Auditoria Pruebas Adjuntos Pruebas

Paso a producción Cancelada Plataformas Proveedor Análisis e Impacto Lista chequeo 110 Lista chequeo 180 Lista chequeo 640

Especifica

Nombre Actividad Separacion de programas opcion Desbloqueo cuentas AFC

General:

ID REQPR00237520

Estado 640_Desarrollo_Aprobacion

Fecha Creación 13/02/2017

Requerimiento id

CREA REQPR00237431

Creada Por : Diego Abelardo Cruz Rojas

U. Autorizador Alfredo Jose Pertuz Montenegro

Tipo Actividad Técnica

Aplicación Afc

Tipo Desarrollo Interno

Fecha Inicio Desarrollo 13/02/2017

Fecha Fin Desarrollo 17/02/2017

Definición:

Tipo Proyecto No Planeación

Prioridad Desarrollo Baja

Riesgo Operativo Bajo

Riesgo Tecnico Bajo

Horas de Esfuerzo Planeadas 62 Horas

Horas de Esfuerzo Ejecutadas 62 Horas

Documentación :

Documentación de Estructuras de datos <<Adjunte el modelo RDA si nuevas estructuras o actualizaciones>> No

Modelo Entidad - Relacion <<Entregue el modelo E-R actualizado a Arquitectura>> No

Modelo Integración (Planos E/S, aplicaciones, BD, Usuarios) <<Diligencie el formato de integración Linea-Batch y adjúntelo >> No

Modelode infraestructura (Componentes SW/HW) <<Entregue la vista física a Arquitectura>> No

Planillas JCL/BAT/DTS/ETL/Oracle <<Entregue las planillas actualizadas a mano>> No

Hoja de Seguridad - Solicitud Perfiles <<Entregue la hoja de seguridad a Seguridad de la Información>> No

Área de Prueba

Jefatura Desarrollo 16113 Jefe desarrollo captación

Responsable Pruebas

Responsable Desarrollo Carlos Andres Salamanca Gallo

Figura.22 Plataforma de documentación del desarrollo "ClearQuest"

8.4.6. Versionamiento de los desarrollos

Cuando se realiza un desarrollo ya sea sobre un programa nuevo o uno que ya existe, se debe generar una versión del mismo. Para esto se usa la plataforma CLEARCASE en la cual se maneja un árbol de versiones como se muestra en la (Figura.23). Aquí se permite gráficamente conocer el estado del desarrollo en el ciclo de vida del software del Banco y comparar el desarrollo realizado con versiones anteriores.

Inicialmente se compila la versión del programa en el ambiente de desarrollo, después de acuerdo al ciclo de vida del software se instala en el ambiente de pruebas y finalmente se instala en el área de producción en la cual todos los colaboradores del Banco realizan las operaciones referentes a los productos y/o servicios del Banco.

Figura.23 Árbol de versiones de los desarrollos en la plataforma "ClearCase"

8.5. Pruebas del Sistema

Después de la etapa de implementación se procede a realizar las pruebas del sistema con el fin de verificar la funcionalidad del desarrollo y validar que las modificaciones que se realizaron en el flujo de las opciones se basaron en desarrollos técnicos.

8.5.1. Prueba al flujo de las opciones

Para evaluar el desarrollo técnico respecto al flujo de las opciones, y verificar que la ruta se modificó de acuerdo a los requerimientos propuestos, se hace uso de “DISPLAYS” en la plataforma de Z. Estos generan un registro cuando se accede a una opción desde la página, conociendo los códigos de transacción y el nombre del programa al que se accede. La información se almacena en un archivo de información conocido como “GE280K” el cual permite visualizar la información de todos los “DISPLAYS” presentes en la plataforma Z y saber si el flujo de las opciones es acorde al desarrollo propuesto.

El “DISPLAY” se ubica en el programa de interés y se definen las variables que se quieren visualizar.

```
VIEW          DESA.AV01.CICSLIB(AFK01202) - 01.00          Columns 00001 00072
Command ==> |_____ Scroll ==> CSR
000215      *=====
000216      020-PROCESO.
000217      *=====
000218      DISPLAY '*****ENTRA A PROGRAMA AFK01202*****'
000219      DISPLAY 'RE-COD-TRANSA: ' A028-COD-TRANSA
000220      PERFORM 025-LEER-AF010K.
```

Cuando se ejecuta la operación, la información del “DISPLAY” se muestra en el registro de “GE280K”

Display	Filter	View	Print	Options	Search	Help

SDSF OUTPUT DISPLAY CICS	DESA	STC45868	DSID	113	LINE	CHARS '*****ENTRA A PRO
COMMAND INPUT ==>						SCROLL ==> CSR
W001AH65	20170209161700	*****ENTRA A PROGRAMA AFK01202*****				
W001AH65	20170209161700	RE-COD-TRANSA: 291202				

El código de transacción se envía en la trama de información junto con la identificación del usuario que accede a la opción y la fecha de acceso.

```
VIEW          DES4.DES.GE280K.INTRA.LOG00          CHARS '291202' found
Command ==> |_____ Scroll ==> CSR
000061  2017021308372705000000000622A872001 0000013872001AH190224GEK600 CICSDES
000062  2017021308373455000000000622A872001 0000013872001AH291202GEK600 CICSDES
```

8.5.2. Prueba al sistema de seguridad de acceso

Después de implementar el sistema de seguridad de acceso se realizan pruebas de las diferentes opciones utilizando información que permita validar el desarrollo realizado y verificar el funcionamiento del sistema en las opciones de aplicación del área de Captación.

Después de implementar el sistema de seguridad de acceso, en la plataforma Z se visualiza el mensaje de respuesta a la operación cuando se intenta acceder con un usuario que no está autorizado. El resultado permite identificar datos de interés como el nombre del usuario que desea acceder a la opción, el nombre del programa que se relaciona con la opción y la razón por la cual no es posible acceder

```
ICH408I USER(CASALA1 ) GROUP(AVUSERS ) NAME(CARLOS A. SALAMANCA )  
  PROD.AV00.CICSLIB CL(DATASET ) VOL(ARLIB7)  
  INSUFFICIENT ACCESS AUTHORITY  
  FROM PROD.*.CICSLIB (G)  
  ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )  
IEC150I 913-38,IFG0194E,CASALA1,IKJUSER,ISP15544,BC0B,ARLIB7,PROD.AV00.CICSLIB  
***
```

En las opciones de aplicación se realizan pruebas con datos de cada opción que se obtienen de archivos presentes en la plataforma Z. La primera prueba se realiza antes de implementar el sistema con el fin de conocer el comportamiento de las opciones de aplicación cuando un usuario tiene acceso. En la segunda prueba se realiza la misma operación de la primera prueba pero con la implementación del sistema. En este caso el usuario no debe tener acceso a las opciones que no son de su interés puesto que sus datos no están registrados en la base de datos correspondiente al acceso de la opción.

Las pruebas se realizan con el usuario: Carlos A. Salamanca y se verifica el funcionamiento de las opciones presentando la misma prueba antes y después de la implementación del sistema de seguridad de acceso. Cuando se realiza la prueba antes del sistema el resultado a la operación puede ser “Transacción OK, Transacción Correcta o un mensaje que responda a la operación”. Cuando se realiza la prueba de la opción con el sistema implementado y utilizando un usuario que no tiene acceso el mensaje de respuesta es “Usuario no existe” y en la plataforma Z se envía un registro que verifica que el acceso a la opción fue denegado.

1. DESBLOQUEO DE CUENTAS AFC.	FUNCIONES	
	Consultar	Desbloquear

- **Pruebas sin el sistema de seguridad de acceso.**

Desbloqueo de Cuentas AFC

Desarrollo Desarrollo Desarrollo Desarrollo Desarrollo

Por favor digite una Cuenta valida

Numero de Cuenta: 127041111002

Presentar desde Fecha Bloqueo: 20151021

Consultar

Desbloqueo de Cuentas AFC

Desarrollo Desarrollo Desarrollo Desarrollo Desarrollo

DESBLOQUEOS DE CUENTAS

Desbloquear	Nro Cuenta	Fecha Bloq.	Hora Bloq.	Funcionario Bloq.	Tipo Bloq.	Estado Bloq.	Motivo Bloqueo.
☒	127041111002	20151021	091437	0000053055449	PARCIAL	ACTIVO	05 INTENTO DE FRAUDE

Desbloquear

Desbloqueo de Cuentas AFC

Desarrollo Desarrollo Desarrollo Desarrollo Desarrollo

TRANSACCION OK. DESBLOQUEO REALIZADO

DESBLOQUEOS DE CUENTAS

Desbloquear	Nro Cuenta	Fecha Bloq.	Hora Bloq.	Funcionario Bloq.	Tipo Bloq.	Estado Bloq.
-------------	------------	-------------	------------	-------------------	------------	--------------

Desbloquear

- **Pruebas con el sistema de seguridad de acceso.**

Desbloqueo de Cuentas AFC

Desarrollo Desarrollo Desarrollo Desarrollo Desarrollo

Por favor digite una Cuenta valida

Numero de Cuenta: 127041111002

Presentar desde Fecha Bloqueo: 20151021

Consultar

Desbloqueo de Cuentas AFC

Desarrollo Desarrollo Desarrollo Desarrollo Desarrollo

USUARIO NO EXISTE

DESBLOQUEOS DE CUENTAS

Desbloquear	Nro Cuenta	Fecha Bloq.	Hora Bloq.	Funcionario Bloq.	Tipo Bloq.	Estado Bloq.
-------------	------------	-------------	------------	-------------------	------------	--------------

Desbloquear

2. FRACCIONAMIENTO CDT'S

FUNCIONES	
Consultar	Fraccionar

- **Pruebas sin el sistema de seguridad de acceso.**

Fraccionamiento CDTs

RC [723] - CERTIFICADO ESTA REINVERTIDO

Datos del Certificado a Fraccionar

Numero de Certificado Padre: 004061128201 En formato OOOAAMDDNNN [En donde OOO es el Cod Oficina de Radicacion, AAMDD Fecha Apertura y NNN Consecutivo del Certificado]
 004-061128-201

Numero de Fraccionamiento: 2000 ☐ Anular

Datos Cliente

Tipo Documento:
 Numero Documento: 1111111
 Nombre: pedro diaz

Tipo Persona: Tipo Apertura: Retefuente:
 Numero de Titulo: 01043072 Cuenta: Valor Total: 1000000
 Ciudad de Correspondencia: BOGOTA (BOGOTA)
 Direccion Correspondencia: av 123-456 Telefono: 2516132

- **Pruebas con el sistema de seguridad de acceso.**

Fraccionamiento CDTs

RC [99] - USUARIO NO EXISTE

Datos del Certificado a Fraccionar

Numero de Certificado Padre: 004061128201 En formato OOOAAMDDNNN [En donde OOO es el Cod Oficina de Radicacion, AAMDD Fecha Apertura y NNN Consecutivo del Certificado]
 004-061128-201

Numero de Fraccionamiento: 2000 ☐ Anular

Datos Cliente

Tipo Documento:
 Numero Documento: 1111111
 Nombre: pedro diaz

Tipo Persona: Tipo Apertura: Retefuente:
 Numero de Titulo: 01043072 Cuenta: Valor Total: 1000000
 Ciudad de Correspondencia: BOGOTA (BOGOTA)
 Direccion Correspondencia: av 123-456 Telefono: 2516132

3. BLOQUEO Y DESBLOQUEO TARJETAS DÉBITO

FUNCIONES	
Bloqueo	Desbloqueo

- *Pruebas sin el sistema de seguridad de acceso.*

Bloqueo y Cambio de Estado Tarjetas Débito

TRANSACCION CORRECTA

Tipo Operacion	Bloqueo
Número de Tarjeta	6013673333002604
Motivo Bloqueo/Desbloqueo	06 Robada/Perdida

ENVIAR

Bloqueo y Cambio de Estado Tarjetas Débito

TRANSACCION CORRECTA

Tipo Operacion	Cambio Estado
Número de Tarjeta	6013673333002604
Motivo Bloqueo/Desbloqueo	00 Normal

ENVIAR

- *Pruebas con el sistema de seguridad de acceso.*

Bloqueo y Cambio de Estado Tarjetas Débito

USUARIO NO EXISTE

Tipo Operacion	Bloqueo
Número de Tarjeta	6013673333002604
Motivo Bloqueo/Desbloqueo	05 Deteriodo

ENVIAR

4. MANEJO CUENTAS SERVICIOS PÚBLICOS

FUNCIONES		
Consultar	Adicionar	Modificar

- **Pruebas sin el sistema de seguridad de acceso.**

Manejo Cuentas Servicios Públicos

Transacción Correcta

Seleccione la acción a ejecutar: Adicionar

Red: 1-ATH

Código: 212121 Subcódigo: 1345

Código Avalnet: 54564

Estado servicio: ACTIVO

Número cuenta: 100012510

Cruzado: ☒ Maneja adicional: ☐ Comisión línea: ☐

Comentarios: Comentario

Tipo Identif.: 1 Identificación: 12312321

Convenio Bloqueado Para CB

Full Carga: ☒ Red Cerca: ☐ Claro: ☐

Tradicionales: ☐ Exito: ☐ Reval: ☐

RBM: ☐

Nombre titular: Titular

Fecha creación: Fecha estado: Usuario:

Enviar

- **Pruebas con el sistema de seguridad de acceso.**

Manejo Cuentas Servicios Públicos

USUARIO NO EXISTE

Seleccione la acción a ejecutar: Adicionar

Red: 1-ATH

Código: 212121 Subcódigo: 1345

Código Avalnet: 54564

Estado servicio: ACTIVO

Número cuenta: 100012510

Cruzado: ☐ Maneja adicional: ☐ Comisión línea: ☐

Comentarios: Comentario

Tipo Identif.: 1 Identificación: 12312321

Convenio Bloqueado Para CB

Full Carga: ☐ Red Cerca: ☐ Claro: ☐

Tradicionales: ☐ Exito: ☐ Reval: ☐

RBM: ☐

Nombre titular: Titular

Fecha creación: Fecha estado: Usuario:

Enviar

9. CONCLUSIONES

El proyecto realizado es funcional para el Banco, ya que por medio de las pruebas ejecutadas y en armonía con los requerimientos establecidos se logró diseñar e implementar un sistema que gestionara la seguridad de acceso en la plataforma web de la compañía, haciendo más seguro el uso de las opciones de aplicación relacionadas al área de Captación.

El uso de los requerimientos permitió que este proyecto se realizara de manera integral, puesto que el ingeniero brinda sus conocimientos desde el escenario de la programación para suplir soluciones tecnológicas, pero el apoyo que se presta por parte las áreas con conocimientos en las operaciones financieras permite validar la solución presentada por el desarrollador. De esta manera se busca que el producto y/o servicio tecnológico que brinda el Banco, tenga éxito en sus operaciones tanto a nivel interno como externo de la compañía.

Cuando se realiza el desarrollo de un sistema, la etapa de diseño permite establecer una conexión entre los requerimientos que se plantean y el software que se produce. Es importante conocer las variables de entrada y salida del sistema. A partir de estos componentes se analiza la mejor estrategia en el diseño. Para el sistema implementado fue importante idear una estrategia de diseño que atendiera las necesidades referentes a la seguridad de acceso, teniendo en cuenta las políticas establecidas por el Banco, desde un panorama técnico, sin afectar el panorama funcional y para lograrlo se adicionaron componentes que aportaran a la estructura original de las opciones de aplicación de Captación, en lugar de modificar los componentes, evitando de esta manera el riesgo de afectar la funcionalidad de las opciones.

El diseño que se propone para el sistema de seguridad de acceso es escalable. De esta manera se aporta a la prolongación del ciclo de vida en el software puesto que es posible adicionar opciones al sistema y gestionar la seguridad de acceso en otras áreas del Banco diferentes al área de Captación.

La implementación de un sistema, es un proceso que no solamente se entiende como desarrollo de software. Algunos procesos como la asociación de códigos RACF, la documentación y el versionamiento de diferentes componentes, también aportan a la etapa de implementación y se trabajan de manera conjunta con diferentes desarrolladores. En la academia cuando se realiza desarrollo de software, el panorama es independiente puesto que los desarrollos que se implementan pertenecen a su diseñador y la temática

a trabajar es aleatoria. En la industria el desarrollo de software es dependiente, ya que diferentes desarrolladores pueden estar implementando en función de un mismo proyecto que pertenece a la compañía y la temática a trabajar se enfoca en la naturaleza del negocio. Es importante hacer uso de las habilidades adquiridas en la formación como ingeniero tanto a nivel técnico referente a los aspectos de programación, como a nivel humano en aspectos como la habilidad de trabajar en equipo, siendo integro en la práctica de la ingeniería.

El desarrollo de software no es un proceso que finalice en la etapa de implementación, puesto que para evaluar la eficiencia y eficacia del sistema que se desarrolla, es importante realizar una etapa de pruebas que permita verificar si la implementación que se generó, es acorde con los requerimientos propuestos. Las pruebas se deben hacer antes y después del desarrollo para verificar cambios y validar el funcionamiento de la seguridad de acceso en las opciones de la aplicación. Esta etapa es importante para el desarrollo ya que dependiendo del resultado que se obtenga de las pruebas el ciclo de vida del software implementado se puede prolongar. Para el Banco esta etapa es fundamental, puesto que cualquier deficiencia o irregularidad en el sistema que no se detecte, se puede prestar como una oportunidad para vulnerar el sistema de seguridad de acceso del Banco en su plataforma Web. Por tal motivo en las labores de desarrollo de software el ingeniero posee una gran responsabilidad, generando estrategias tecnológicas de seguridad frente a la gestión de la información que se maneja en un Banco.

BIBLIOGRAFIA

- Banco AV Villas. 1611-DIRECCIÓN PROYECTOS DE CAPTACIÓN. [En Línea]. 1a ed. Bogotá: Gerencia de Desarrollo. [Citado 13-Febrero-2017]. Disponible en internet:http://gata/portalintranet/neoIntranet/SomosAVVillas/Dependencias/docs_tecnologia/GerenciaDesarroll.
- Banco AV Villas. Seguridad de la Información. [En Línea]. 1a ed. Bogotá: Dirección de Seguridad Informática. [Citado 13-Febrero-2017]. Disponible en internet: <http://gata/portalintranet/especiales2014/Contraloria/SeguridadInformacion/Incidentes.html#01>.
- Banco AV Villas. Seguridad de la Información. [En Línea]. 1a ed. Bogotá: Dirección de Seguridad Informática. [Citado 13-Febrero-2017]. Disponible en internet: http://gata/portalintranet/neoIntranet/SomosAVVillas/Dependencias/Somos_Dependencias_Operaciones.
- Banco AV Villas. Ventajas de la Seguridad Informática. [En Línea]. 1a ed. Bogotá: Dirección de Seguridad Informática. [Citado 13-Febrero-2017]. Disponible en internet: <http://gata/portalintranet/especiales2014/Contraloria/SeguridadInformacion/ventajassegu>.
- Bsigroup. Sistema de gestión ISO/IEC 27001 de Seguridad de la Información [En Línea]. [Citado 13-Febrero-2017] Disponible en: <https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/>.
- Contact&BusinessIT.Capacitacion Cobol. [En Línea] [Citado 13-Febrero-2017]. Disponible en internet: <http://gata/portalintranet/neoIntranet/GestionesAplicacion/Formacion/Manuales/PRESENTACIONCOBOL2.pdf>. Pag.76.
- Erik Zepeda. Introducción a RACF [En Línea]. [Citado 13-Febrero-2017] Disponible en: <http://cryptomex.org/SlidesMainframes/IntroRACF.pdf>.
- Huella hídrica de México en el contexto de Norteamérica. [En línea]. México [Citado 13-Febrero-2017]. Disponible en Internet: <http://www.huellahidrica.org/Reports/AgroDer,%202012.%20Huella%20h%C3%ADdrica%20en%20M%C3%A9xico.pdf>.
- IBM. z/Architecture y el sistema operativo z/OS.[En Línea]. [Citado 13-Febrero-2017]. Disponible en internet: https://www.ibm.com/support/knowledgecenter/es/SSEPEK_10.0.0/intro/src/tpc/db2z_zarchitectureandzos.htm.
- IEEE. IEEE Standard Computer Dictionary. [En Línea]. [Citado 13-Febrero-2017] Disponible en internet: <https://standards.ieee.org/findstds/standard/610-1990.html>.
- Ingeniería de Software[En Línea]. [Citado 13-Febrero-2017] Disponible en: <http://ing-sw.blogspot.com.co/2005/04/tipos-de-pruebas-de-software.html>.

- Kujaku. Seguridad en mainframe: Introducción al RACF. [En Línea]. [Citado 13-Febrero-2017] Disponible en internet: <http://www.signt.net/software/seguridad-en-mainframe-introduccion-al-racf.html>.
- Laboratorio Nacional de Calidad del Software de INTECO. INGENIERÍA DEL SOFTWARE: METODOLOGÍAS Y CICLOS DE VIDA. [En Línea]. 1a ed. España: Inteco. [Citado 13-Febrero-2017]. Disponible en internet: http://datateca.unad.edu.co/contenidos/301569/guia_de_ing.
- LosBancos-Lectura. [En Línea]. [Citado 13-Febrero-2017]. Disponible en internet: <http://www.spanish.cl/Vocabulary/Notes/Bancos.htm>.
- Ministerio del Interior. DESARROLLO Y MANTENIMIENTO DE SISTEMAS MINISTERIO DEL INTERIOR. [En Línea]. Bogotá. MinInterior. [Citado 13-Febrero-2017]. Disponible en internet: www.mininterior.gov.co/sites/default/files/documentos/OIP-2014-PSI-Especificas-7%20.
- Ministerio del Interior. DESARROLLO Y MANTENIMIENTO DE SISTEMAS MINISTERIO DEL INTERIOR. [En Línea]. Bogotá. MinInterior. [Citado 13-Febrero-2017]. Disponible en internet: www.mininterior.gov.co/sites/default/files/documentos/OIP-2014-PSI-Especificas-7%20.
- Subinet. ¿Cuáles son los modelos de control de acceso?. [En Línea]. [Citado 13-Febrero-2017]. Disponible en internet: <http://www.subinet.es/cuales-son-los-modelos-de-control-de-acceso/>.
- Tutorialspoint. COBOL - Descripción General. [En Línea] [Citado 13-Febrero-2017]. Disponible en internet: https://www.tutorialspoint.com/es/cobol/cobol_overview.htm.
- Universidad Santo Tomas.[En Línea]. 1ª ed. Bogotá: Misión Institucional. [Citado 13-Febrero-2017].Disponible en Internet: <http://www.usta.edu.co/index.php/nuestra-institucion/presentacion-1> .

ANEXOS

Anexo 1. Etapa de Diseño

Anexo 2. Etapa de Desarrollo

Anexo 3. Etapa de Pruebas y Producción