“Metodología para el Análisis y Recomendaciones de Puntos de Control,

En la Aplicación de Administración de Token´s”

Edgar Isauro Corredor Morales y Cesar Augusto Herrera Agudelo

Universidad Católica de Colombia

Notas del autor

Edgar Isauro Corredor Morales y Cesar Augusto Herrera Agudelo, Facultad de posgrados de Ingeniería, Universidad Católica de Colombia

Este proyecto ha sido financiado por los propios alumnos

Universidad Católica de Colombia, Avenida Caracas # 46 -72 sede el Claustro

Contactos: edgarcorredor@gmail.com, caherrera23@ucatolica.edu.co

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS.

1 INTRODUCCIÒN

La Superintendencia Financiera de Colombia como organismo regulador de las entidades financieras colombianas, mediante la circular externa 052 de Octubre de 2007 ordenó la implementación y uso de los sistemas de seguridad de autenticación, motivo por el que las entidades financieras iniciaron con la implementación y uso de los TOKENS, en aplicaciones y sitios WEB "ONE TIME PASSWORDS", que consiste en la utilización de diferente contraseña cada vez que se requiera ingresar a la aplicación y realizar transacciones bancarias; mediante la ayuda del dispositivo físico o electrónico el banco genera esta contraseña diferente cada cierta cantidad de segundos.

El diario Portafolio en la página 36 de octubre 24 de 2011 advirtió que: "Los criminales cibernéticos (Hankers) no atacan los sistemas bancarios, sino la PC de los clientes", (Superintendencia Financiera de Colombia, s.f.); es decir que atacan la vulnerabilidad de los clientes; tratando de robar la identidad de los mismos, Usuario de acceso al sistema electrónico, contraseña, pin de seguridad. Lo hacen a través de correos que se finge ser enviados por el banco al cliente, el cliente la accede y este es direccionado a las páginas de los ladrones, quienes aprovechan para acceder a la información del cliente ya sea con la inocencia de éste, o la información que proporciona al PC en ese momento. Una medida de seguridad obligatoria es que el ladrón financiero además de robar sus claves en forma virtual tenga que robar algo físico para poder completar los requisitos de acceso a las cuentas del cliente, y para esto se ha provisto de Tokens a los clientes que usan sistemas de banca electrónica, dispositivos que permiten realizar acciones físicas que comprometen al cliente

aún más con la seguridad de sus transacciones financieras.

La Banca Colombiana en publicación del diario El Colombiano del 12 de abril de 2018 en el informe anual de Symantec (Empresa Norteamericana que desarrolla sistemas de seguridad y antivirus) que analiza a 157 países, reveló que en 2017 Colombia fue el sexto país de Latinoamérica con el mayor número de ataques cibernéticos. Los tres primeros lugares los ocupan Argentina, Chile y Brasil.

De acuerdo con el informe, Colombia sufrió el 0,36% de las amenazas que se reportaron en América Latina durante el 2017. Con respecto al Phishing (método que se usa para el jaqueo de contraseñas o datos de cuentas bancarias), Daryan Reinoso Ingeniero senior de seguridad de Symantec afirma que éste ataca en Colombia en uno de cada 11.770 casos.

"Uno de los delitos más comunes es el robo de la información de los clientes bancarios, y se conoce como 'troyanos financieros', esta es una de las amenazas que viene en aumento", indicó Reinoso y añadió que el cibercrimen mueve anualmente cerca de 10.000 billones de dólares en el mundo.

Por todas estas innumerables razones que dan exigente importancia al tema de la seguridad bancaria es que se deben atender con especial cuidado los temas de accesos seguros a las plataformas financieras web, para garantizar la confidencialidad de la información compartida por los sistemas bancarios; la integridad de los datos mediante registro de auditoría del cambio de información generado en los proceso y la disponibilidad del servicio para no afectar las operaciones que realizan los clientes.

Por todo lo anterior, se propone concebir una metodología para el análisis de puntos de control y establecer recomendaciones, en la aplicación de Administración de Tokens. Esta metodología abarca los procesos puntuales de cargue, administración de creación, asignación, entrega y bloqueos del Token, cubriendo ciclo de vida de los Tokens haciendo

un énfasis especial en los Token s físicos, debido al tiempo de vida del dispositivo.

Nos centramos en identificar una metodología de auditoria con base en buenas prácticas apoyadas en los dominios de la Norma ISO27002, por lo que el foco principal está en las tecnologías de información, los controles y las recomendaciones en cada uno de los procesos principales anteriormente listados con el objetivo de poder asegurar un proceso transparente, seguro y controlado en el sector bancario. Se han elegido los pilares de ISO 27002 porque es una norma aceptada como una buena práctica para el control y seguridad de la información.

Dada la evolución que surge en los procesos de los distintos sectores, abordaremos el tema de la seguridad en los procesos y controles de las transacciones bancarias de clientes tanto naturales como corporativos, teniendo como referencia aspectos de la norma internacional ISO 27002 según los dominios de y control de accesos y cifrado de información aplicado en varios procesos.

Anteriormente, bastaba con digitar una clave asignada para aprobar la realización de transacciones bancarias en un ambiente virtual, sin embargo, con el pasar del tiempo, la seguridad se vio comprometida con el creciente aumento de transacciones fraudulentas, afectando la economía de los clientes de los bancos así como la confiablidad del mismo banco al permitir los desembolsos no realizados por los titulares de las cuentas, debido a esto en Colombia en el año 2010 la Superintendencia Financiera Colombiana decretó la implementación de una segunda clave para los usuarios a la hora de realizar transacciones, en busca de brindar un mayor grado de seguridad.

Inicialmente, esta segunda clave fue también estática y con el transcurrir del tiempo y el incremento de fraudes, llegó finalmente a convertirse en dinámica con la ayuda de las tecnologías de software y hardware, es así como hoy en día este código dinámico es producido por demanda cada cierta cantidad de tiempo. Generando así que muchos clientes

bancarios sintieran una mayor confianza para realizar transacciones a través de la banca virtual y dejar de ir a las sucursales físicas, agilizando sus pagos, transacciones, evitando largas filas e incrementando el comercio web, de ahí el creciente número de tiendas web y servicios de todo tipo transando desde la comodidad del hogar u oficina.

Teniendo en cuenta la importancia del papel que juega la tecnología en los sectores productivos del país, y la necesidad de hacer uso de ella para el mejoramiento continuo de los procesos financieros, se centrara la atención en el sector que se considera tiene como base la seguridad y autenticación de los clientes, en el sector Bancario cuando se usa la internet como medio seguro para realizar transacciones sin necesidad de salir de casa. Y entiéndase como casa, las mismas oficinas de gestión administrativa, financiera de las empresas.

Partiendo de ese punto, se enfocará la auditoría de los procesos que conciernen al control en todo momento del cargue y administración de semillas en las aplicaciones bancarias para tal fin. Por tal motivo, el nombre planteado para el proyecto es:

*"*METODOLOGIA PARA EL ANÁLISIS Y RECOMENDACIONES DE LOS PUNTOS DE CONTROL, EN LA APLICACIÓN DE ADMINISTRACIÓN DE TOKENS FÍSICOS, PARA EL SECTOR BANCARIO*"*

1.1 Línea de Investigación

El proyecto se enmarca en el diseño de software inteligente y de convergencia tecnológica.

Esta investigación es de tipo evaluativa, por lo que se desea realizar una auditoría, evaluar, cotejar y dar juicio sobre los diferentes procesos involucrados en el otorgamiento del Token bancario.

Con un enfoque cuantitativo toda vez que lo que se pretende es recolectar datos, basados en la observación, análisis y evaluación sin buscar una medida numérica para establecer los

puntos de control de la aplicación.

1.2 Planteamiento del Problema

Dado el gran crecimiento de los usuarios del sistema financiero, por la continua búsqueda de la bancarización de la sociedad (Figura 1), se creó la necesidad de brindarles a estos usuarios instrumentos de seguridad para el uso de sus cuentas bancarias.

Cuando la Superintentendencia Financiera de Colombia obligó a las entidades financieras para que fijaran instrumentos de seguridad para sus clientes, estas entidades iniciaron con la búsqueda de la mejor herramienta para lograr brindarles la mayor seguridad a sus usuarios. Logrando así que muchos de los bancos se decantaron por el Token, por la confiablidad que generaba. Por lo que iniciaron su proceso de adopción y socialización a sus clientes sobre esta herramienta.

Como la Superintendencia Financiera no daba un lineamiento rígido sobre lo que debían hacer las entidades financieras para lograr la seguridad de sus clientes, cada entidad podía escoger la forma en que resguardaría el dinero de sus usuarios. Esto genero para el caso del Token que el proceso al interior de cada entidad fuera asimilado de forma diferente, pero con similitudes en su accionar, sus procesos, asociación, y trazabilidad interna. Y como cada entidad lo hacía según sus recursos disponibles, en los procesos que intervenían en la consecución, solicitud y entrega del Token existen vacíos de seguridad, y riesgos no cubiertos

o que no están siendo identificados.

El Token al ser un elemento implementado para lograr una mayor seguridad en las transacciones bancarias, resultaría contradictorio que, en su ciclo de generación, cargue, solicitud y asignación al interior del banco, no presente la suficiente seguridad en sus procesos.

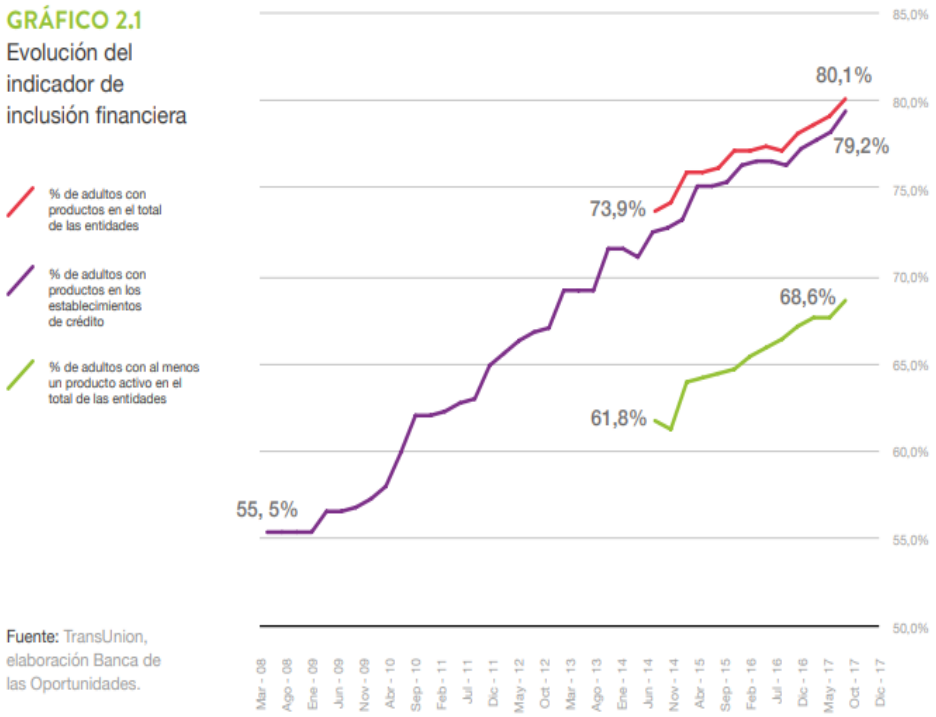


Figura *1*. Evolución del indicador de inclusión financiera

.Referencia: Tomado de: (Superintendencia Financiera de Colombia, 2017) "Reporte de inclusión financiera año 2017". Consultado el 20 de agosto del 2018. Disponible en URL: https://www.superfinanciera.gov.co/inicio/informes-y-cifras/informes/10085394

1.3 Antecedentes del problema

Comúnmente los sistemas desarrollados y puestos en ambientes de producción no son controlados ciento por ciento y tampoco son perfectos, lo que conlleva a la existencia de un

periodo de estabilización, afinamiento y control de cambios. Es por eso la importancia de la auditoría y del auditor, puesto que permite al ser involucrado en el ciclo de vida de los desarrollos y/o posteriormente en la revisión, que genere un valor agregado que facilite y permita asegurar que la información que se genera proporciona confiabilidad del sistema a los usuarios.

En el sector bancario es grave que se operen aplicaciones con defectos, siempre la seguridad, disponibilidad, la integridad de la información y procesos debe ser lo primordial. En donde operar, afinar y mantener el sistema puede ser costoso, sin embargo, para este sector, el prestigio y buen nombre vale más, por lo que siempre se propone hacer que sus clientes al utilizar los sistemas bancarios se sientan confiados de que su información está siendo protegida al máximo por la entidad, la cual debe garantizar las buenas prácticas en el cumplimiento de las normas legales y técnicas de las entidades que los supervisan.

En enero (Revista Dinero, 2017) o publicó un artículo en donde hace ver que el cibercrimen ha crecido tanto en todo el mundo, que ya no se trata de experiencias individuales de hackers si no bandas internacionales organizadas y muy poderosas. Pero también resalta que, aunque existe mucha tecnología de protección el talón de Aquiles esta en los usuarios y sus malos hábitos en la línea. Resalta el desconocimiento de los usuarios en los ataques a sus cuentas bancarias y la inocencia de estos. Ataques que se llevan a cabo en las páginas financieras, en los cajeros automáticos y en la banca móvil.

Y muchas veces por el desconocimiento de la existencia del cibercrimen y por el no acatamiento a las medidas de seguridad que proporcionan las entidades financieras.

Kaspersky (proveedor de desarrollos antivirus) indica que los ataques con malware para robar información financiera se han venido incrementando en un 22,4%, en tanto que RSA calcula en 9.100 millones de dólares al año las pérdidas por phishing y el FBI estima en 2.300

millones de dólares en los últimos 3 años solo por ramsonware, versión digital de secuestro que se libera con el pago de un rescate.

Estudios de la compañía Kaspersky informan que más de 550 colombianos han sido víctimas de operaciones de ramsonware originadas en México y que han cobrado más de 120.000 víctimas desde que fue lanzada en 2009.

Muy importante es que la mayoría de las personas (86%), que utilizan el celular entre los 25 y 35 años, utilizan la Banca en línea. Y claro, nadie quiere hacer cola en los bancos y desperdiciar tiempo, muchos comparten usuarios y claves, y muchos acceden a los sitios financieros desde puntos públicos, y todo esto son malos hábitos de los clientes que son aprovechados por los cibercriminales.

En el 2017 el Sistema Financiero Colombiano realizó más de 5.400 millones de operaciones con un incremento del 11% respecto del año anterior. El año pasado el canal de Internet fue el de más auge en las operaciones bancarias.

Número de Operaciones (monetarias y no monetarias)				
Canal	**2014**	**2015**	**2016**	**2017**
Internet	1.376.646.150	1.905.341.076	2.295.131.790	2.576.621.515
Datáfonos	413.158.092	460.510.198	516.618.932	568.531.271
Oficinas	700.644.424	664.830.147	655.514.932	615.188.401
Cajeros Automáticos	705.493.171	732.473.320	760.247.270	801.598.435
Telefonía Móvil	119.014.902	132.811.894	197.331.398	330.352.155
Corresponsales Bancarios	118.495.575	147.531.436	184.076.395	235.455.467
Audio Respuesta	94.456.040	93.280.629	98.449.892	112.688.908
ACH	96.256.151	101.734.031	111.933.940	112.047.587
Pagos Automáticos	92.616.193	94.672.878	106.835.895	109.622.735
Total	**3.716.780.698**	**4.333.185.609**	**4.926.140.444**	**5.462.106.474**

Figura 2. Número de operaciones (Monetarias y no monetarias)

Nota: Numero de Operaciones (Monetarias y no monetarias)

La Banca Móvil ha venido creciendo en participación de las operaciones financieras, de las cuales redunda en importancia del porqué hay que ponerle mérito al tema del afinamiento del uso del Token y de su administración. He aquí las cifras hasta el 2017.

Número de Operaciones (monetarias y no monetarias)				
Canal	2014	2015	2016	2017
Internet	1.376.646.150	1.905.341.076	2.295.131.790	2.576.621.515
Datáfonos	413.158.092	460.510.198	516.618.932	568.531.271
Oficinas	700.644.424	664.830.147	655.514.932	615.188.401
Cajeros Automáticos	705.493.171	732.473.320	760.247.270	801.598.435
Telefonía Móvil	119.014.902	132.811.894	197.331.398	330.352.155
Corresponsales Bancarios	118.495.575	147.531.436	184.076.395	235.455.467
Audio Respuesta	94.456.040	93.280.629	98.449.892	112.688.908
ACH	96.256.151	101.734.031	111.933.940	112.047.587
Pagos Automáticos	92.616.193	94.672.878	106.835.895	109.622.735
Total	3.716.780.698	4.333.185.609	4.926.140.444	5.462.106.474

Figura 3. Número de operaciones (Monetarias y no monetarias).

Fuente: Tomado de: (Revista Dinero, 2018). URL:

https://www.dinero.com/economia/articulo/operaciones-financieras-en-colombia-en-2017/256283

1.4 Pregunta de investigación

¿El desarrollar una metodología que inspeccione y estructure los puntos de control para el sistema de administración de Tokens, puede asegurar la confidencialidad y disponibilidad de los procesos que apoyan su uso en el sector bancario como norma de autenticación?

1.5 Variables del Problema

En el capítulo de Monitoreo y Control y bajo las buenas prácticas de COBIT 5 se reconocen, identifican y diagnostican los procesos dentro de los módulos de desarrollo de software; que aplicados al módulo de Administración de Tokens contemplan temas de gran importancia para el aseguramiento de la calidad de los controles. Así mismo el dominio 6

de la Norma ISO27002 que habla sobre los aspectos organizativos de la seguridad de la información

Variables internas:

Conocer la situación actual de la Aplicación. (Recopilación de la documentación e información). Cualitativa).

Establecer los momentos, y proponer puntos de control para aumentar la seguridad de la aplicación. (Cualitativa).

Logs que aseguren la trazabilidad en cualquier momento, para dar soporte a situaciones que se presenten. (Cualitativa).

Confiabilidad de la información. (Garantizar la completitud efectiva de los procesos). (Cualitativa).

Variables externas:

Análisis de los momentos de violación de la información que podría estar sucediendo en la aplicación de Tokens bancario. (Segmentación de usuarios, continuidad, disponibilidad y recuperación). (Cualitativa).

Confiabilidad de la información. (Garantizar la completitud efectiva de los procesos). (Cualitativa).

Adaptabilidad tecnológica al cambio. (Token físico a Token virtual). (Cualitativa).

Comparación de COBIT 5, ITIL e ISO 27002 para tomar como herramienta de apoyo para la elaboración de la metodología una extracción de los puntos que contemplan los dominios

que se acomodan a la Administración de Tokens bancarios.

ÁREA	CobiT	ITIL	ISO 27002
Funciones	Mapeo de procesos IT	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de referencia de seguridad de la Información
Áreas	4 Procesos y 34 Dominios	9 Procesos	14 Dominios
Creador	ISACA	OGC	ISO International Organization for Standardization
¿Para que se Implementa?	Auditoria de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad
¿Quienes lo evalúan?	Compañias de contabilidad, Compañias de consultoria en IT	Compañias de Consultoria en IT	Compañias de Consultoria en IT, Empresas de Seguridad, Consultores de seguridad en redes

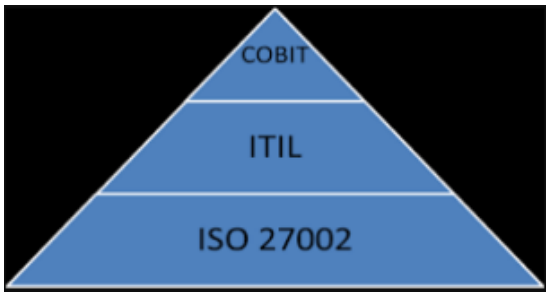


Figura 4. Cuadro comparativo COBIT, ITIL, ISO 27002, 2018

Fuente: Tomado de: (Aranda Software, 2012) Consultado el 26 de agosto del 2018. Disponible en URL: https://arandasoft.com/itil-y-cobit-algunas-diferencias/

Contenidos de COBIT 5: Se resalta el capítulo de Monitoreo y Evaluación.

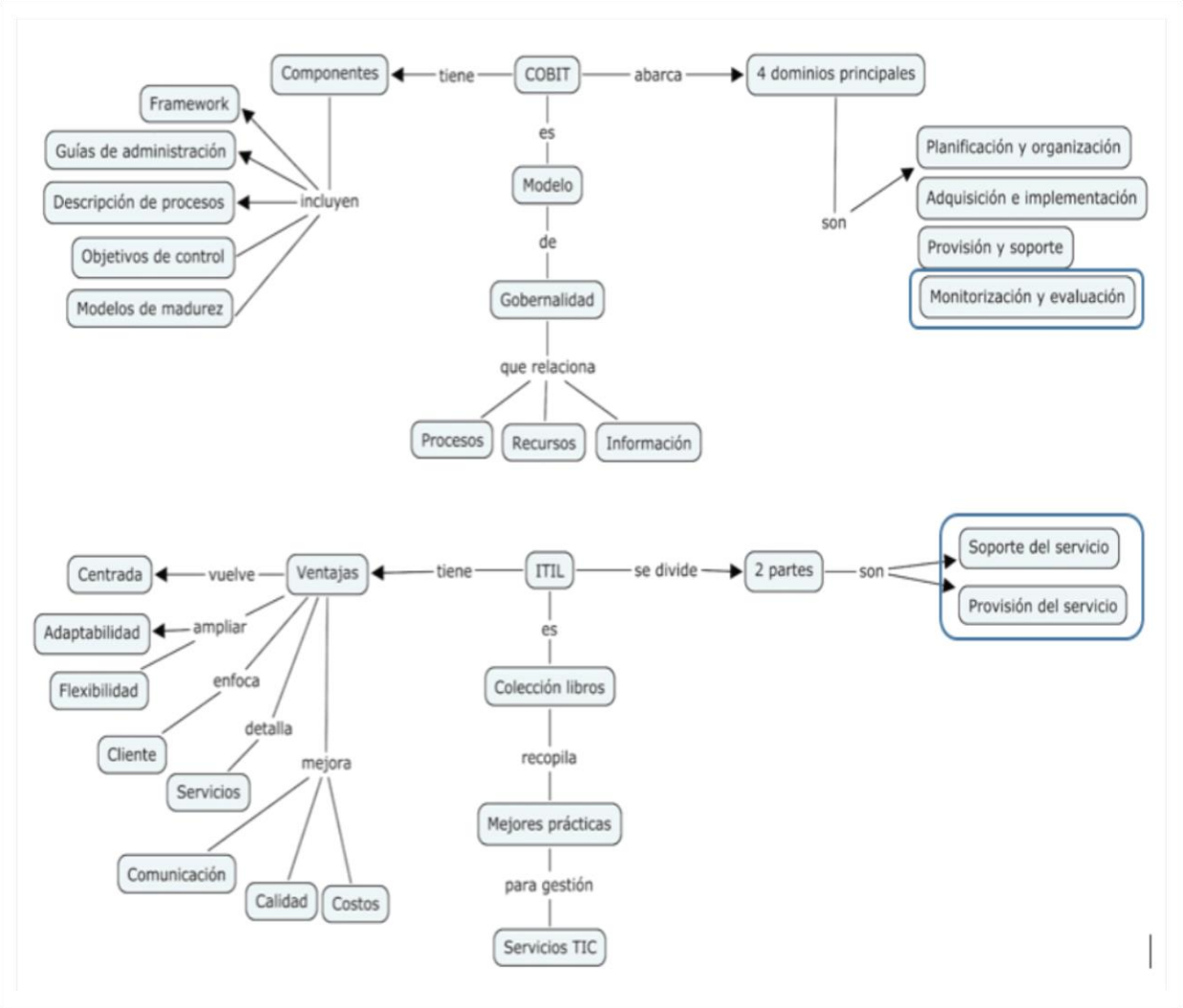


Figura 5. Cuadro mapa conceptual COBIT e ITIL

Fuente: Tomado de: Mapas Conceptuales COBIT e ITIL Consultado el 2 de septiembre del 2018. Disponible en: URL:http://3.bp.blogspot.com/-tVTYOsnHw0s/T75uckZIcxI/AAAAAAAAACw/taQ-ICFHAEo/s1600/AFI+MC11+-+COBIT+e+ITIL.jpg

Esta información de comparación entre los dos Modelos de Gobierno resalta que el punto importante acomodado a nuestro desarrollo es el Monitoreo y Control que destaca COBIT 5. En ITIL podemos visualizar que, siendo un modelo de servicios de grandes ventajas ayuda

el capítulo de Soporte y Provisión del Servicio, puesto que contempla servicios para clientes internos como externos a la organización.

Finalmente destacamos el Modelo a referenciar en este proyecto y nos lo ofrece la Norma **ISO 27002**. Que establece directrices y principios generales, para el comienzo, la implementación, el mantenimiento y la mejora de la gestión de la seguridad de la información en una organización, siendo un catálogo de buenas prácticas, obtenido a partir de la experiencia y colaboración de todos los participantes; los cuales han alcanzado un conceso a cerca de los objetivos comúnmente aceptados para la gestión de la seguridad de la información.

De aquí destacamos aún más los objetivos para los controles recomendados que hay que tener en cuenta en el desarrollo, implementación y puesta en marcha de las aplicaciones que se montan para dar soporte en colaboración de la integración con otros aplicativos. Cabe destacar que con la Norma 27002 estamos ajustando todos los ciclos del PHVA (Planear, Hacer, Verificar y Actuar).

De los múltiples Dominios que contempla La ISO 27002 destacamos los siguientes, y son los que nos apoyan en el control del tema de la Administración de Tokens:

Figura 6. Cuadro PHVA para gestionar la seguridad de la información.

Fuente: Tomado de: (Welive Security, 2017) Cambios en la norma para gestionar la seguridad de la información. Consultado el 2 de septiembre del 2018. Disponible en URL: https://www.welivesecurity.com/wp-content/uploads/es-la/2013/10/1.jpg

Dominios que establece la Norma ISO 27002:

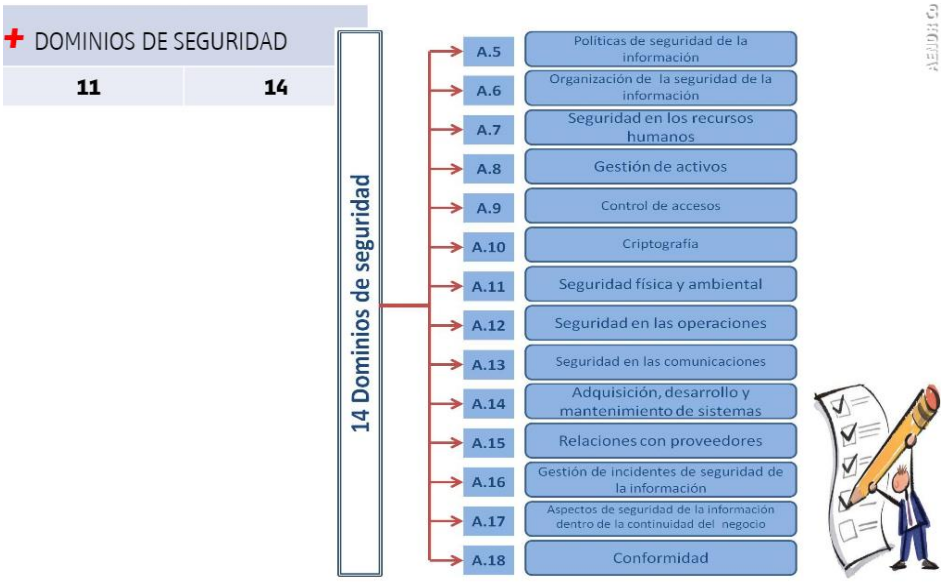


Figura 7. Cuadro Dominios ISO 27002

Fuente: Autor, septiembre 2018

De los cuales tomamos los siguientes para la evaluación de la Administración de Tokens y que ayuda con los principios de gestión, como la orientación al cliente, el liderazgo, enfoque de sistemas de gestión, mejora continua, etc:

NORMAS PARA ADOPTAR EN EL PROYECTO			
NORMAS	**ISO27002**		
DOMINIOS	5-POLÍTICAS DE SEGURIDAD..		
		5.1 Directrices de la Dirección en seguridad de la información	
			5.1.1 Conjunto de políticas para la seguridad de la información.
			5.1.2 Revisión de las políticas para la seguridad de la información.
	6-ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.		
		6.1 Organización interna.	
			6.1.1 Asignación de responsabilidades para la seguridad de la información.
			6.1.2 Segregación de tareas
			6.1.3 Contacto con las autoridades.
	9-CONTROL DE ACCESOS.		
		9.2 Gestión de acceso de usuario.	
			9.2.2 Gestión de los derechos de acceso asignados a usuarios.
	10-CIFRADO.		
		10.1 Controles criptográficos.	
			10.1.1 Política de uso de los controles criptográficos.
			10.1.2 Gestión de claves.
	12. SEGURIDAD EN LA OPERATIVA.		
		12.1 Responsabilidades y procedimientos de operación.	
			12.1.1 Documentación de procedimientos de operación.
		12.4 Registro de actividad y supervisión.	
			12.4.1 Registro y gestión de eventos de actividad.
	13. SEGURIDAD EN LAS TELECOMUNICACIONES.		
		13.1 Gestión de la seguridad en las redes.	
			13.1.2 Mecanismos de seguridad asociados a servicios en red.
	17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.		
		17.1 Continuidad de la seguridad de la información	
			17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Figura 7.1 Cuadro Dominios ISO 27002

Fuente: Autor, septiembre 2018

Por esta variable de aplicabilidad de las Normas es que hacemos la comparación viendo que aplicando la Norma 27002 exponemos el aplicativo a una dinámica que absorbe los

aspectos que deben tener en cuenta a la hora de obtener un producto de manejo del sistema de información excelente, aplicando laboriosidad, seguridad, trazabilidad y efectividad.

COMPARATIVO PERSONAL DE LA ELECCIÓN DE LA NORMA			
NORMAS	**COBIT 5**	**ITIL**	**ISO27002**
DOMINIOS	**MEA02:** Supervisar, Evaluar y Valorar el Sistema de Control Interno..		
		Soporte y Provisión del Servicio	
			5-Políticas de Seguridad de la Información.
			6-Aspectos organizativos de la Seguridad de la información.
			9-Control de Accesos
			10-Cifrado
			17-Aspectos de seguridad de la información en la gestión de Continuidad del Negocio.

Figura 8. Cuadro comparativo COBIT 5, ITIL, ISO 27002

Fuente: Autor, septiembre 2018

1.6 Justificación

De acuerdo a lo dispuesto en la introducción, y al planteamiento del problema, es viable la realización de este proyecto ya que permite la creación de una metodología que evalué, analice, y permita identificar los puntos de control de los tres módulos del sistema de Tokens, determinando los puntos auditables.

La Metodología generada podrá ayudar a otras instituciones financieras a realizar implementaciones o mejorar las existentes en materia de controles y monitoreo.

Desde el punto de visto social a los empleados y usuarios del sistema financiero se crea un ambiente de negocios mucho más confiable debido a que se le da un control efectivo a las actividades que interfieren en la solicitud, creación y asignación del Token, logrando un beneficio social respecto al manejo de la confidencialidad, e integridad de la información, los activos y posterior mejoramiento de los servicios prestados por la entidad bancaria hacia los usuarios. Lo anterior toma más fuerza teniendo en cuenta que las transacciones

financieras por internet registraron un crecimiento de 38,4 % en 2015 con un total de 1,905 millones de pesos, convirtiéndose en el canal que mueve más dinero por su uso 24 horas. Algunos datos para tener en cuenta en cuanto a la seguridad de las transacciones electrónicas;

Colombia sufrió el 0.36% de todas las amenazas que se reportaron en América Latina durante el 2017.

Colombia, sexto país en Latino América con mayor número de Ciberataques.

12 Ciberataques de programas maliciosos Malware cada segundo que provienen de piratas de Rusia y Estados Unidos.

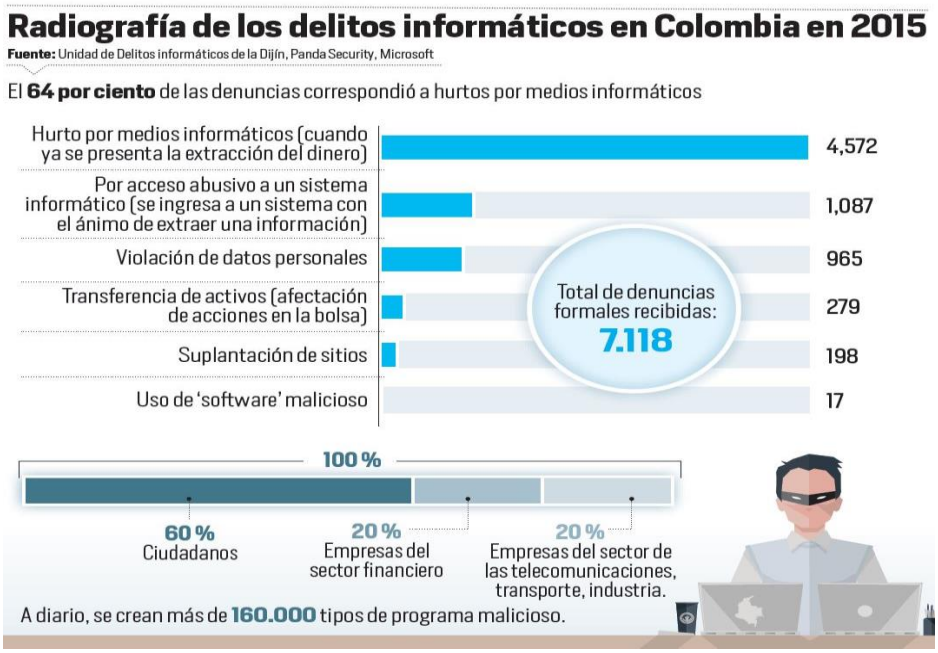


Figura 9. Imagen Radiografía de delitos informáticos en Colombia en 2015

Fuente: Tomado de: (Periodico el Colombiano, 2018). Consultado el 2 de junio del 2018. Disponible en URL: http://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174

1.7 Objetivos

1.7.1 Objetivo general

- Desarrollar una Metodología para definir e inspeccionar la estructura de los puntos de control en las aplicaciones de Administración de Tokens Bancario.

1.7.2 Objetivos específicos

- Identificar los puntos de control auditables, contemplados en los módulos de cargue de semillas, creación de la Solicitud y asignación del Token para asegurar la confiabilidad de la aplicación y generar la matriz de riesgos.
- Realizar la auditoría a los módulos del sistema para verificar la metodología y asegurar que los procesos estén vigilados.
- Evaluar la metodología propuesta del sistema para mitigar las vulnerabilidades encontradas en el sistema de administración de Token.

2 MARCOS DE REFERENCIA

2.1 Marco Conceptual

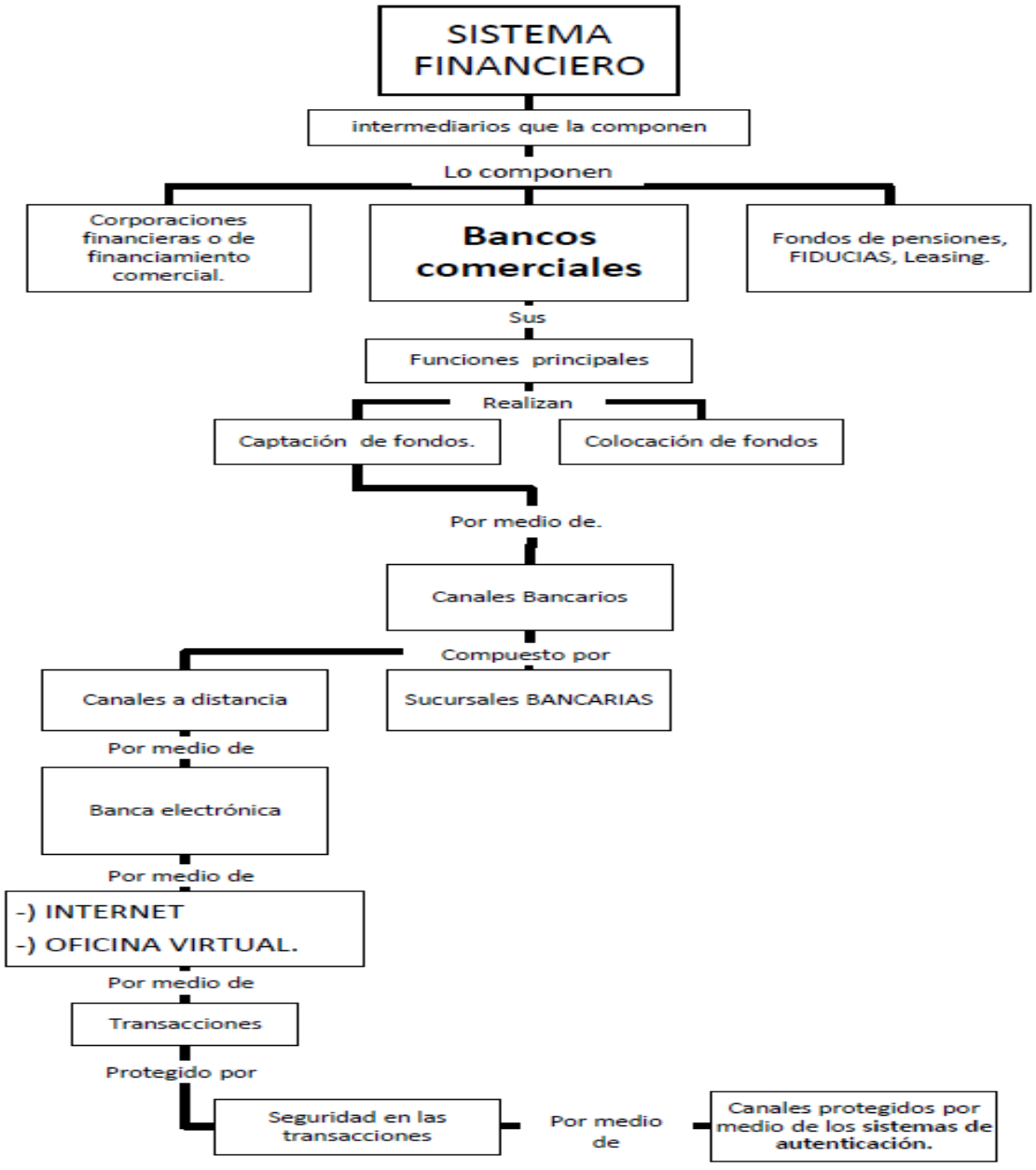


Figura 10. Cuadro Mapa conceptual

Fuente: Autor, septiembre 2018

Banco Comercial:

> "Institución financiera de intermediación que recibe fondos en forma de depósito de las personas que poseen excedentes de liquidez, utilizándolos posteriormente para operaciones de préstamo a personas con necesidades de financiación, o para inversiones propias. Presta también servicios de todo tipo relacionados con cualquier actividad realizada en el marco de actuación de un sistema financiero." Afirma (Superintendencia Financiera de Colombia, 2018)
>
> "Un banco comercial es una institución financiera que actúa como intermediario en el juego de la oferta y la demanda entre compradores y vendedores de recursos financieros; esta denominación sirve para distinguirla de los llamados bancos industriales, que igualmente prestan fondos a empresas, pero también adquieren acciones de dichas empresas. Su función principal es recibir y canalizar el ahorro de particulares y empresas mediante depósitos, plazos fijos, etc. (operaciones de pasivo) y a su vez otorgar préstamos y créditos a otros particulares y empresas que necesitan financiación (operaciones de activo). Los bancos comerciales también realizan otros servicios como el cobro de impuestos o el cambio de monedas y billetes. Todas las operaciones de activo y pasivo que realiza un banco comercial están reguladas mediante la normativa vigente correspondiente en cada país y el Banco Central del país." (MyTripleA, 2018)

Banca virtual La banca electrónica: puede definirse como la provisión de servicios financieros por medio del intercambio de datos electrónicos entre un cliente y una institución financiera. (El Tiempo, 2002)

> "También llamada banca virtual o online, es un servicio prestado por las entidades

financieras que tiene como misión permitir a sus clientes realizar operaciones y transacciones con sus productos de forma autónoma, independiente, segura y rápida a través de Internet. Entre las transacciones más típicas que se pueden realizar a través de este servicio de banca electrónica están las transferencias, el envío y recepción de ficheros o cuadernos de gestión y la consulta de los movimientos de las cuentas" Informa (Economia Simple.Net, 2018)

C.F.C. Compañías de financiamiento comercial:

"Son C.F.C. las instituciones que tienen por función principal captar recursos a término, con el objeto primordial de realizar operaciones activas de crédito para facilitar la comercialización de bienes y servicios, y realizar operaciones de arrendamiento financiero o leasing", (ASOBANCARIA, 2016)."

Canales de distribución bancaria: Es la forma en que las entidades financieras le ofrecen a sus diferentes clientes actuales sus productos o servicios. Un canal es el medio que utilizan las entidades financieras para prestar sus servicios a los clientes y/o usuarios. (ASOBANCARIA, 2018) (Canales y seguridad) consultado el 16 de septiembre de 2018, http://www.asobancaria.com/sabermassermas/home/consumidor-informado/mas-acerca-de-los-bancos/canales-y-seguridad/.

Tradicionalmente, el canal de distribución bancaria ha sido la oficina o sucursal antes de la incursión de la tecnología para ofrecer estos servicios: El Banco prestaba sus servicios a sus clientes, requiriéndose una presencia física de ambas partes tanto para realizar operaciones bancarias, como para formalizar contratos o simplemente para solicitar información. Esto ha ido modificándose con los años, abriéndose el paso los canales electrónicos dando variadas oportunidades de negocio, pero también abriendo la puerta a

numerosos riesgos por el uso de este tipo de canales.

Captación de fondos: La superintendencia financiera de Colombia en su Concepto No. 2000048692-1. junio 30 de 2000 realiza una síntesis de las características de intermediación financiera. (El proceso de captación de fondos se entiende como la acción de atraer el dinero de las personas para realizar la administración de este y generar una utilidad, también conocido en el ámbito económico como fundraising, supone la recolección de recursos económicos por parte de una persona u organización para, posteriormente, destinar dichos fondos reunidos a un objetivo ajeno al lucro personal o empresarial.

Colocación de fondos: La SFC en su Concepto No. 2000048692-1. Junio 30 de 2000. realiza una síntesis de las características de intermediación financiera, en la que habla de la colocación y que esta permite la puesta de dinero en circulación en la economía, es decir, la banca genera un nuevo dinero del capital o los recursos que obtiene a través de la captación y, con estos recursos, se otorgan créditos a las personas, empresas u organizaciones que los soliciten. Por dar estos préstamos el banco cobra unas cantidades de dinero que se llaman intereses, o intereses de colocación, y comisiones.

Fiduciarias: Fiduciarias son entidades financieras, con profesionales en la gestión de negocios, transacciones u operaciones por cuenta de terceros. Que reciben mandatos de, los cuales se desarrollan con el objeto de cumplir una finalidad específica, administración, compra, venta, comodato. “Citibank (2018) Que son las sociedades fiduciarias?, consultado el 2018/09/07 (CITIBANK, 2018)”

Leasing:

> “figura que usa una entidad financiera, adquiriendo un bien a nombre propio, para arrendarlo a mediano o largo plazo al locatario, teniendo como beneficio el canon de arrendamiento que cancela según lo pactado en el contrato leasing. Al finalizar el

tiempo del contrato de arriendo, el usuario decide si compra el bien, si renueva el contrato o por el contrario se lo devuelve a la entidad financiera.” “ (ASOBANCARIA, 2016) Que es leasing?, consultado el 2018/09/07, http://www.asobancaria.com/sabermassermas/que-es-leasing/”

Sistema financiero:

“Es un sistema conformado por un conjunto de instituciones, medio y mercado, cuyo objetivo principal es canalizar el ahorro que generan los prestamistas o unidades de gasto con superávit hacia los prestatarios. Este sistema también medio entre aquellas personas que no gastan todo su ingreso (tienen excedentes de dinero) y los que gastan más de lo que tienen (necesitan esos recursos para financiar sus actividades de consumo o inversión como abrir un negocio, comprar casa propia, etc.).

El sistema financiero permite que el dinero circule en la economía, que pase por muchas personas y que se realicen transacciones con él, lo cual incentiva un sin número de actividades, como la inversión en proyectos que, sin una cantidad mínima de recursos, no se podrían realizar, siendo esta la manera en que se alienta toda la economía. “

(Superintendencia Financiera de Colombia, 2018) (Conformación del Sistema Financiero Colombiano, consultado el 16 de septiembre de 2018, , URL https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=11268&dPrint=1

Sociedades Administradoras de Fondos de Pensiones y Cesantías: Instituciones financieras privadas de carácter previsional encarga das de administrar eficientemente los fondos y planes de pensiones del Régimen de ahorro individual y de los fondos de cesantías en Colombia. “ (FONCEP Fondo de prestaciones economicas, cesantias y pensiones., 2016)

Glosario AFP, consultado el 2018/09/07, http://www.foncep.gov.co/index.php/glosario"

Sucursal bancaria: La oficina o sucursal bancaria es la dependencia que establece una entidad financiera como principal canal de distribución de sus productos. (Superintendencia Financiera de Colombia, 2018)

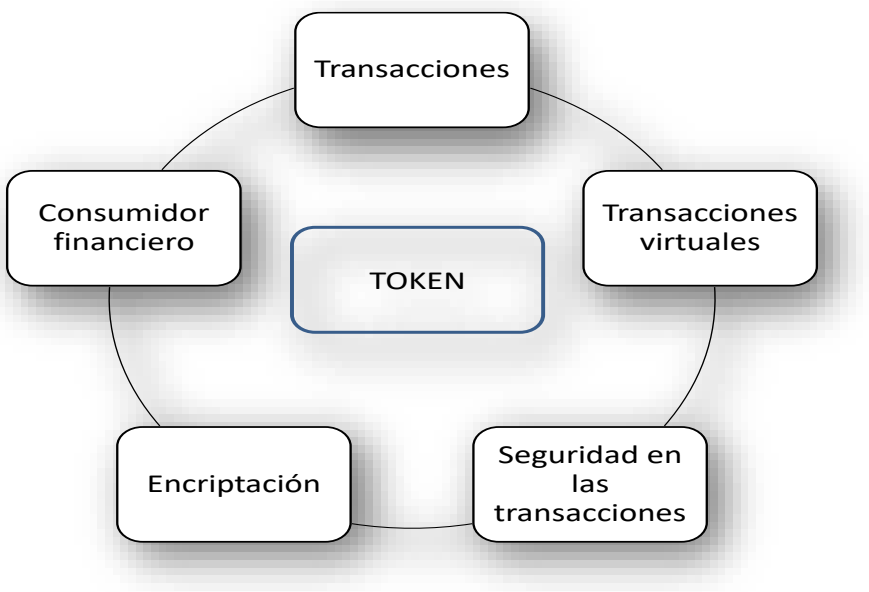


Figura 11. Cuadro Mapa conceptual transacciones

Fuente: Autor, septiembre 2018

Consumidor financiero: Es todo cliente, usuario o cliente potencial de los productos o servicios ofrecidos por las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera, así como todo aquel que determine la Ley o el Gobierno Nacional. (Ley 1328 de 2009). Detalle los conceptos (Ley 1328 del 15 de julio de 2009, Título I, Capítulo I, Artículo2.

Encriptación: Es la forma de cifrar la información de especial importancia, como técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Para autores como Galende Díaz (1995: 15), la actividad de criptoanálisis puede

denominarse de dos formas, dependiendo si el que realiza la actividad es un destinatario legítimo o no; la primera sería el destinatario que de forma legítima hace el criptoanálisis, en donde el proceso a realizar se denominaría "descifrar"; y la segunda que correspondería a un ataque o intrusión por parte de un usuario no autorizado, en este caso se denomina "desencriptar". (Pabón Cadavid, 2018) La criptografía y la protección a la información digital. Revista Universidad externado. Consultado el 16 de septiembre de 2018, https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636.

Seguridad en las transacciones:

"El comercio electrónico necesita garantizar una seguridad técnica y jurídica que impida un anormal funcionamiento del negocio o una desconfianza en el medio utilizado para comerciar. En este sentido se han aportado una serie de soluciones, propuestas por los organismos de normalización, para evitar los posibles peligros u operaciones ilegales a los que puede estar sometida Internet.

Básicamente se trataría de garantizar cuatro principios.

1. Principio de autenticidad: que la persona o empresa que dice estar al otro lado de la red es quién dice ser.

2. Principio de integridad: que lo transmitido a través de la red no haya sido modificado.

3. Principio de intimidad: que los datos transmitidos no hayan sido vistos durante el trasiego telemático.

4. Principio de no repudio: que lo transmitido no pueda ser repudiado o rechazado."

(XARXA AFIC El portal del Comerciante, 2018) la seguridad transaccional, consultado el 7 de septiembre de 2018,

https://www.portaldelcomerciante.com/es/articulo/la-seguridad-transacciones

Transacciones: Termino empleado en el uso de dinero para sufragar el costo de un servicio o bien comprado. Uno de los aspectos que más caracteriza a la transacción es que hay una idea común entre las partes que realizan la operación. Para que se realice es preciso disponer de un capital y que alguien proporcione un servicio o bien que se ajuste a la cantidad reclamada. (Economia Simple.Net, 2018), Consultado el 16 de septiembre de 2018, https://www.economiasimple.net/glosario/transaccion

Transacciones electrónicas: El término "transferencia electrónica" (o "giro electrónico") se refiere a cierto método de transferir los fondos; es decir, la transferencia de fondos que generalmente realiza un usuario por medio de una institución bancaria, por lo que se denomina más propiamente transferencia electrónica. (Bocanegra Requena & Bocanegra Gil, 2011)

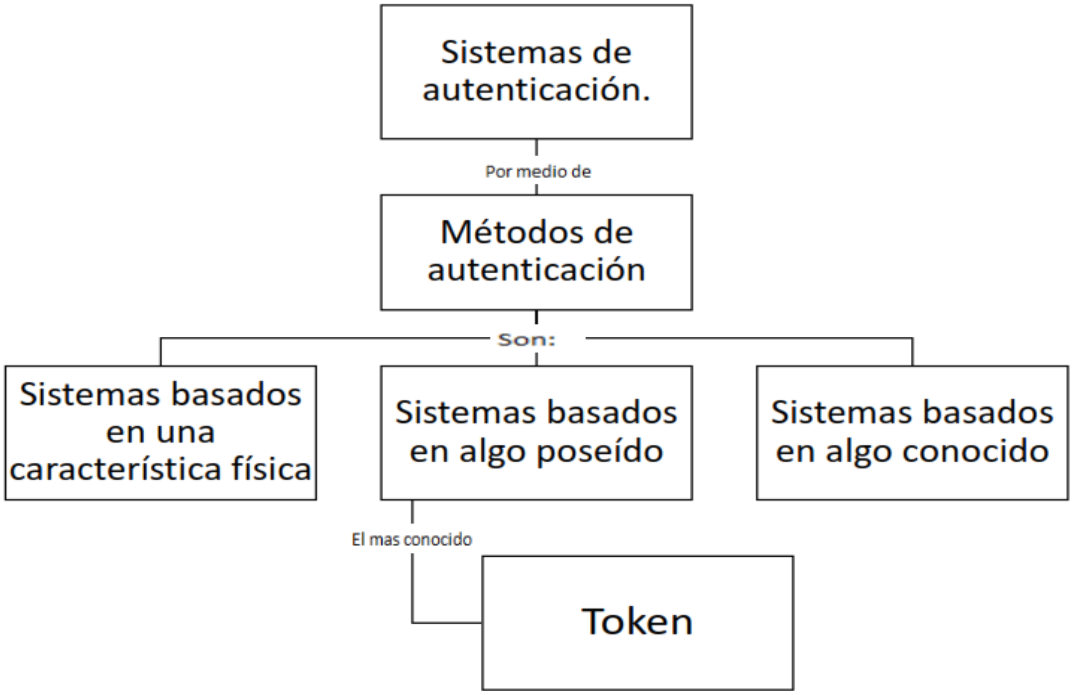


Figura 12. Cuadro Mapa conceptual Sistemas de autenticación

Fuente: Autor, septiembre 2018

Autenticación: es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación (decirle al sistema quién es) y autenticación (demostrar que el usuario es quien dice ser). (Pabón Cadavid, 2018)

Métodos de autenticación:

"Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en tres categorías:

- Sistemas basados en algo conocido. Ejemplo, un password (Unix) o passphrase (PGP).
- Sistemas basados en algo poseído. Ejemplo, dispositivo usb tipo epass token.
- Sistemas basados en una característica física: Ejemplo, verificación de voz, de huellas, de patrones oculares."

(seguridadensistemascomputacionales.zonalibre.org, 2011)

Token: Token de Seguridad es un doble factor de autenticación que genera códigos de seguridad de # dígitos que cambian constantemente. Estos, nos permiten identificarte como Cliente al momento de realizar tus operaciones en el banco, ofreciéndote un nivel adicional de seguridad. (GRUPO SANTANDER S.A., 2018)

2.2 Marco teórico

Este aparte constituye en gran parte los temas del proyecto y abarca en su contenido los antecedentes vistos y evaluados en esa área, el cómo las cifras de ataques y vulnerabilidades y que año por año han venido incrementado con indicadores altamente preocupantes que llevan a definir que debe aumentarse la seguridad en las transacciones en línea de tal manera que los índices que van en aumento logren bajar, para que así mismo baje la preocupación

que existe al respecto.

El marco teórico toca temas como la misma definición del problema, la hipótesis, el objetivo general y los particulares, las áreas de estudio y sus unidades y la misma metodología usada para definir la solución que persigue este compendio.

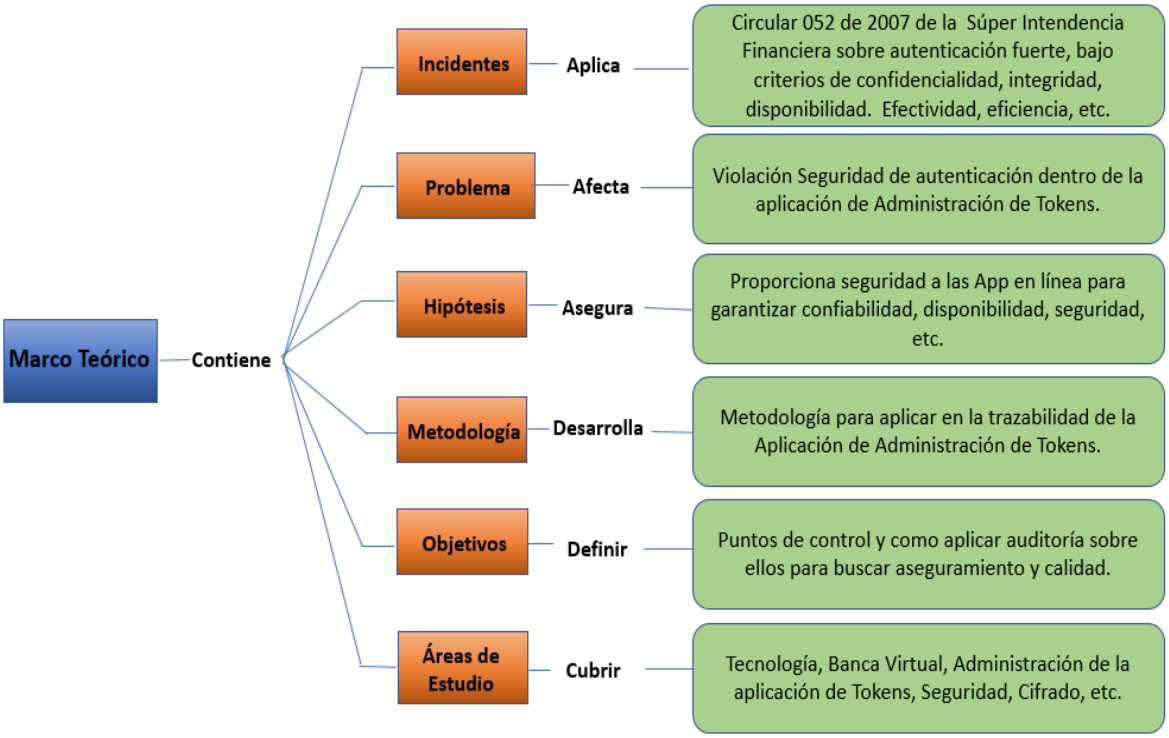


Figura 13. cuadro marco teórico

Fuente: Autor, septiembre 2018

Con el fin de tener un sustento teórico para proponer una metodología que, para definir, inspeccionar y estructurar los puntos de control, en las aplicaciones de Administración de Tokens Bancario, este marco toma los aspectos más destacados de la literatura relacionada con seguridad transaccional, encriptación, y confianza en transacciones electrónicas. Esta parte del trabajo hace hincapié en el estudio de un modelo de confianza interpersonal, que es el punto de inicio y la base principal del presente proyecto.

Transacciones electrónicas: Desde el bum del internet a finales de los años 90, varias de

las tradiciones económicas han cambiado a un ambiente netamente virtual, un ejemplo claro son los millones de transacciones que se realizan diariamente sea por grandes compañías, o personas del común. Hace poco más de una década la única forma de realizar transacciones era por intermedio de un papel, que, aunque relativamente seguro consumía tiempo y si era urgente o para el mismo día era imposible. Con el ingreso del internet a nuestras vidas estas transacciones empezaron hacerse de forma virtud beneficiando en primera medida el tiempo que el usuario destinaba a dicha actividad. En detalle una transacción electrónica es cualquier movimiento que implique la transferencia de información digital para propósitos específicos. Pero en el trasfondo conserva su esencia conservando reglas y procedimientos que las rigen. (Ayala , 2010)

El comercio electrónico es el origen del principal tipo de transacción que hay en internet "El comercio electrónico (e-commerce), como su nombre lo indica significa la comercialización electrónica de bienes tangibles, intangibles e información" y el intercambio automático de información entre unidades de negocios que residen en organizaciones diferentes (TIMMERS & VEER, 1999). El comercio electrónico es fundamentalmente diferente de los mecanismos tradicionales en transacciones de información. En una transacción de negocios tradicional, los individuos participantes han estado en contacto directo, personalmente o a través del teléfono o el sistema postal, y

estos individuos actúan en base a la información intercambiada.

Tipos de transacciones electrónicas:

Bussines to consumers – entre empresa y consumidor.

Entre consumidor y consumidor.

Consumidor y gobierno.

Entre empresa y gobierno.

Como se mencionó diariamente se están realizando millones de transacciones, y están solo serían posibles con los niveles de seguridad suficientes para brindar la confianza de los usuarios.

Tipos de seguridad electrónica: Se puede enmarcar la seguridad electrónica o informática en dos tipos diferentes de criterios, que pueden ser a su vez complementarios entre sí:

Seguridad Física y seguridad lógica:

> "La seguridad física hace referencia a la protección de los elementos físicos de posibles desastres naturales (incendios, terremotos o inundaciones) o amenazas externas como robo, problemas eléctricos.
>
> Y la seguridad Lógica, es la protección de todo lo relacionado al Software o la información que contienen los equipos mediante el uso de antivirus, encriptación de la información, ataques de hackers externos." (Yañez, 2017) Planeta formación universidades consultado el 2018/09/21, de la URL https://www.ceac.es/blog/tipos-de-seguridad-informatica
>
> Seguridad de Hardware, Seguridad de Software y Seguridad de red:
>
> • Hablamos de seguridad de Hardware cuando tomamos las medidas para proteger nuestros equipos físicos, como una UPS, sistemas de alimentación ininterrumpida, u

otras medidas de protección para cambios de tensión eléctrica.

• La seguridad en Software, es cuando tomamos las medidas necesarias para proteger el software como los mecanismos de protección contra virus, hackers y robo de información sensible.

• La seguridad de red, es la toma de medidas para la protección de las redes corporativas o domesticas "Es esta seguridad quizás la más compleja de gestionar ya que un ataque a un equipo conectado a la red, fácilmente se propagará por la misma a otros equipos si no ponemos los medios necesarios" (Yañez, 2017) Planeta formación universidades, consultado el 2018/09/21, de la URL https://www.ceac.es/blog/tipos-de-seguridad-informatica

Seguridad en las transacciones:

"La seguridad en la red, que, a su vez, forma parte del concepto de seguridad en sí incluye confidencialidad, integridad, disponibilidad, y no repudio (es decir, el no rechazo de operaciones). Es un tema de muy amplio debate y actual, dada la movilidad que estamos teniendo en la multitud de servicios que manejamos.

Para hablar de seguridad de las transacciones electrónicas, vamos a definir el término transacciones electrónicas, el cuál abarca las realizadas en diferentes canales digitales, tales como las compras en el comercio en general utilizando puntos de ventas (PDV); o en compra en línea en tiendas virtuales como Amazon o eBay; también incluyen las transferencias bancarias entre cuentas propias o a terceros a través de internet banking, ibanking o banca en línea; entre otras. Si nos enfocamos en las transacciones realizadas en la web, requerimos el uso de una aplicación que opera utilizando nuestro navegador web. Estos navegadores web pueden estar tanto en un computador de escritorio o portátil de línea fija; como un dispositivo móvil." (Mercado, 2018) "seguridad en las transacciones electrónicas" internet society, 2018.

de la URL https://isoc-rd.org.do/publicaciones/recursos/seguridad-de-las-transacciones-electronicas/

Riesgo en las transacciones electrónicas: Dada las condiciones del ambiente en línea, siendo este distante e impersonal se genera una incertidumbre aún mayor en los usuarios el tener que usar plataformas abiertas y globales, que, aunque para ciertos espectros de la población mundial es conocida, no lo es para la mayoría de las personas.

Según (Pavlou, 2003) existen dos tipos de situaciones en las transacciones electrónicas que generan nerviosismo la incertidumbre ambiental y la incertidumbre conductual. La incertidumbre conductual, esta consiste en que el sujeto (sea persona o empresa) que usa los medios electrónicos para la comercialización de sus productos o servicios, pueda aprovecharse de la relación virtual (no física), y del poco control institucional que se ejerce en el monitoreo de estas transacciones. Este tipo de incertidumbre crea riesgos financieros, personales, y riesgos en su privacidad. En cuanto a la incertidumbre ambiental (Pavlou, 2003) dice que es lo inherente al uso de esta plataforma de comercio global, y lo impredecible que puede ser internet, que por ende no puede ser controlada pese a que el vendedor implemente medidas de seguridad (Firewall, encriptación, métodos de autenticación, etc..) este tipo de incertidumbre crea riesgos de financieros y de privacidad.

Riesgo: "Efecto de la incertidumbre sobre los objetivos" ISO (31000, 2011) conceptos. Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Los objetivos pueden tener diferentes aspectos y categorías y pueden aplicar a diferentes niveles. Con frecuencia el riesgo se expresa en términos de fuentes de riesgo, eventos, potenciales, sus consecuencias y sus probabilidades.

Existen varias teorías acerca de los riesgos y muchas de ellas no resultan ser compatibles

en cuanto a la eliminación total del riesgo, o sola la posibilidad de mitigación de este.

Tomamos la definición dada por la ISO 31000, para dar contexto a nuestro proyecto de grado, abordándolo desde el riesgo en la seguridad de la información que en su concepto esta es: “Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. NOTA Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.” Riesgo en la seguridad de la información –ISO/IEC (27005, 2009).

Encriptación y protección de información digita: La criptografía es una técnica utilizada para cifrar mensajes que suelen contener información privada. La palabra Criptografía proviene del griego Kryptos y Graphein, que significan "escondido" y "escritura".

Según la RAE es el “Arte de escribir con clave secreta o de un modo enigmático”.

Viéndolo desde las transacciones comerciales la encriptación se ha convertido en un basteon y un método de seguridad indispensable para la comercialización de producto y servicios, con el que se busca la eliminación de riesgos e incertidumbre por parte de los usuarios. Los bancos en su mayoría optan por estas medidas de seguridad (Encriptación) para él envió de información interna y externa, manejo de recursos, Hasta el surgimiento de los ordenadores modernos y del uso de sistemas binarios para las telecomunicaciones, la criptografía se basaba en una matemática relativamente elemental, en el conocimiento de alfabetos y sistemas de comunicación lo más seguros posibles, pero esta seguridad en los sistemas de comunicación, más que el desarrollo tecnológico de éstos buscaba ardides para ocultar los mensajes. Ahora, la relación de la criptografía con múltiples áreas del conocimiento, como la teoría de la información5, teoría de conjuntos, informática, la importancia de los números primos, las telecomunicaciones, hace que sea necesario para el

desarrollo de criptosistemas robustos un estudio interdisciplinario, que más que nada necesita capital humano para su desarrollo, tanto para el criptoanálisis como para la criptografía. (Pabón Cadavid, 2018) La criptografía y la protección a la información digital. Revista UExternado. Consultado el 16 de Septiembre de 2018, de la base de datos https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

Tipos de encriptación: Toda encriptación está basada en un algoritmo, que codifica la información para que no pueda ser vista. La función de este algoritmo es transformar la información original en otra forma difícil de descifrar, y luego cuando llegue al destino final volver a transformar la información en su estado inicial. (Pabón Cadavid, 2018)

Existen dos tipos de encriptación, la clase simétrica y la de clave asimétrica:

Encriptación simétrica: Es aquella en donde cada usuario que participan en el intercambio de información tiene una clave secreta, solo conocida por ambos que se encarga de cifrar y descifrar la información, usando la misma clave.

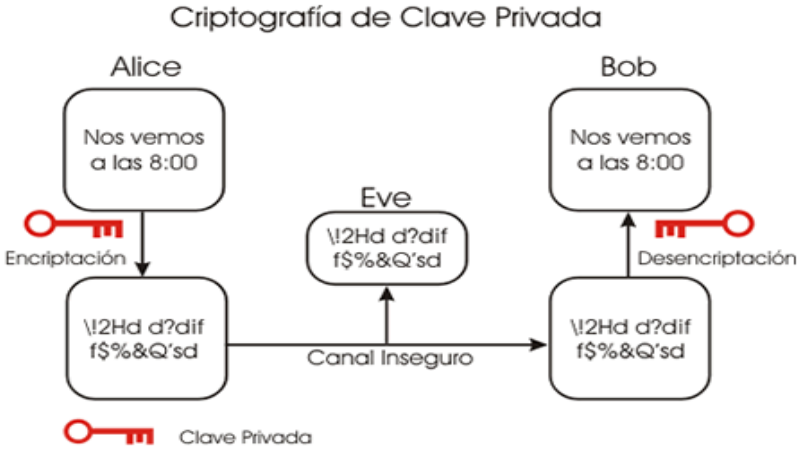


Figura 14. Criptografía clave privada.

Fuente: (Textos Cientificos, 2006) Consultado el 21 de septiembre del 2018. Disponible

en URL: https://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptacion.

Encriptación de clave pública asimétrica: se basa en el uso de dos claves diferentes, una para encriptar y otra para desencriptar. Estas claves se generan al tiempo estando ligadas, y son designadas por el algoritmo, y no por los usuarios del mensaje.

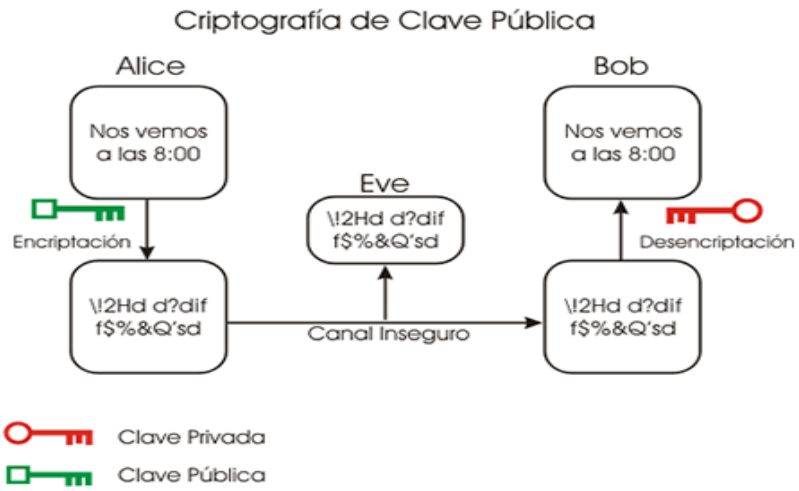


Figura 15. Criptografia clave pública

Fuente: Tomado de (Textos Cientificos, 2006). Consultado el 21 de septiembre del 2018. Disponible en URL: https://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptacion.

CONFIANZA:

(BOON & HOLMES, 1991) definen la confianza como "estado que involucra expectativas confiadas positivas acerca de los motivos de otro hacia situaciones que conlleven riesgo para uno mismo" en cuanto al concepto como tal la (RAE (Real Academia Española), 2018) tiene varias definiciones cortas como "Esperanza firme que se tiene de alguien o algo", "Seguridad que alguien tiene en sí mismo.", en algún sentido las palabras como seguridad, riesgo, o firmeza tienden a expresarse en cada concepto que llegamos a encontrar de confianza. Y dada sus variados significados la mayoría de los investigadores y publicaciones coinciden en ver la confianza como un término fuertemente relacionado con

credibilidad, vulnerabilidad, expectativa segura o creencia positiva.

Pero los beneficios que lleva consigo la confianza es inimaginable, en términos comerciales la confianza es el eje principal de la relación económica. (Ratnasingam, 2005) aseguran que la confianza es clave porque acrecienta las relaciones de intercambio a largo plazo y contribuye a la colaboración entre las partes, obteniendo así beneficios estratégicos.

2.3 Marco jurídico

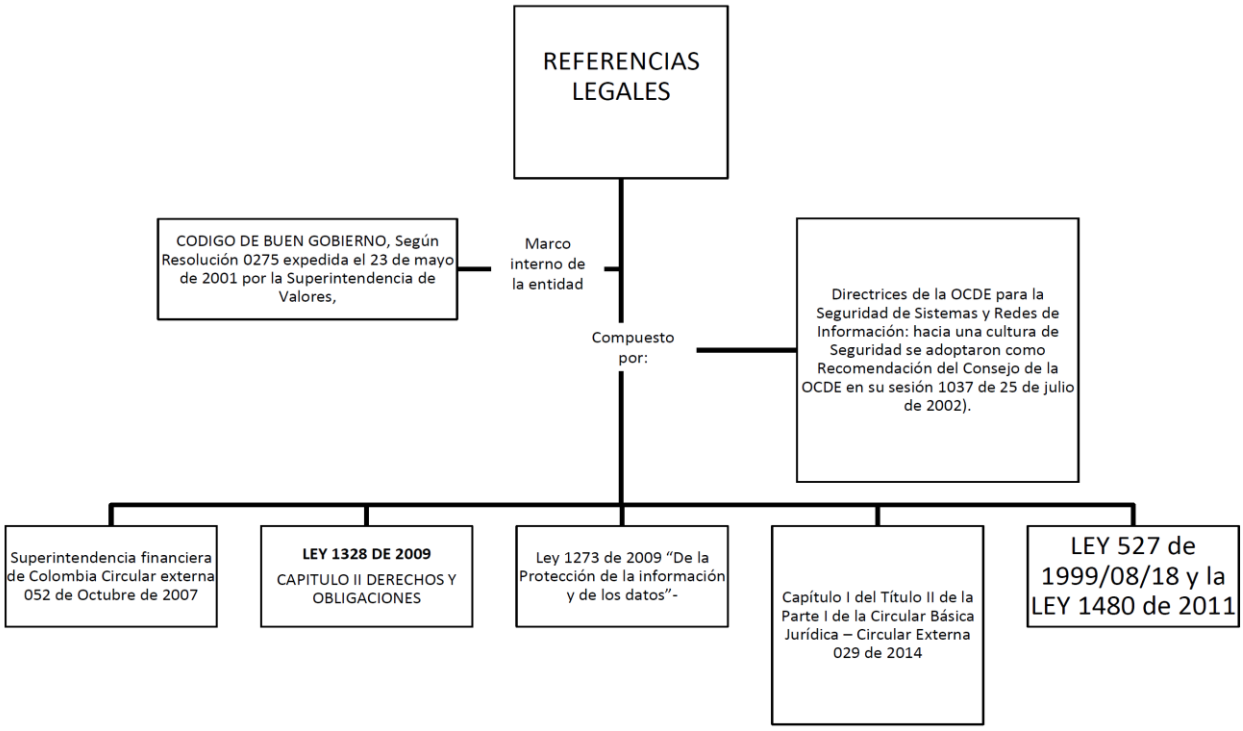


Figura 16. Cuadro Marco jurídico – Referencias legales

Fuente: Autor, septiembre 2018

Ley 527 del 199/08/18: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.

Resolución 0275 expedida el 23 de mayo de 2001 por la Superintendencia de Valores:

> En Colombia se empezó a hablar de prácticas de buen gobierno desde el año 2001 con la resolución 275 del 2001, que establecía la adopción de un código de gobierno corporativo para quienes desearan que sus valores fueran adquiridos o financiados por fondos de inversión.
>
> "El gobierno corporativo es el conjunto de instancias y prácticas institucionales en el proceso de toma de decisiones de la empresa que contribuyen a la creación sustentable de valor en un marco de transparencia, ética y responsabilidad empresarial, alineando intereses y promoviendo el respeto a los derechos de todos los accionistas y grupos de interés que participan directa o indirectamente en la empresa" (Fuente: El Centro para el Gobierno de la Empresa, "Principios Generales de Gobierno Societario para las Empresas Chilenas").
>
> Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad se adoptaron como Recomendación del Consejo de la OCDE en su sesión 1037 de 25 de julio de 2002): Los paises y organizaciones en todo el mundo se dieron cuenta de la necesidad creada por la evolucion de las tecnologias y las comunicaciones de crear una legislación sobre los delitos informaticos dados todos los daños y perjuicios que ha causado a la humanidad en el contexto interenacional. Dando como resultado el agrupamiento de paises para definir los terminos ciberneticos que permitieron la unificación de criterios en esta materia, que por parte de OCDE inicio con

la emision del informer llamado “Delitos de informatica: analisis de la normativa jurídica” en donde se recomendaba y se daban ejemplos de paises con la tecnificación de estos delitos, y leyes ya aprobadas para el tratamiento de ellos.

Luego en la directriz 25 del 25 de julio de 2002, en su parrafo I (Hacia una cultura de seguridad) informaba lo siguiente “Estas Directrices pretenden dar respuesta a un ambiente de seguridad cada vez más cambiante, a través de la promoción del desarrollo de una cultura de seguridad – esto es, centrándose en la seguridad del desarrollo de sistemas y redes de información, así como en la adopción de nuevas formas de pensamiento y comportamiento en el uso e interconexión de sistemas y redes de información. Estas Directrices marcan una clara ruptura con un tiempo en el que los aspectos de seguridad y el uso de redes y sistemas se consideraban con frecuencia como elementos a posteriori. Los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada vez más dependientes de éstos. Sólo un enfoque que tome en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines puede proporcionar una seguridad efectiva.” Lo anterior toma mayor relevancia al conocerse el pasado 25 de Mayo que Colombia fue admitido como el país número 37 de la Organización para la Cooperación y el Desarrollo Económico (OCDE), una de las metas de política internacional que más perseguía el gobierno Santos y un proceso que le tomó al país más de cinco años en llevar a buen término.

Superintendencia financiera de Colombia Circular externa 052 de Octubre de 2007: Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios. En efecto, la Circular Externa 052 de 2007, la cual adicionó el Capítulo

Décimo Segundo al Título Primero de la Circular Básica Jurídica (Circular Externa 007 de 1996), impartió algunos *"(r)equerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios*", sin embargo, dicho instructivo fue objeto de reforma por parte de la Circular Externa 042 de octubre 4 de 2012, mediante la cual se realizaron algunas modificaciones al referido capítulo en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones; cambios que responden precisamente a distintos factores como la masificación del uso de los dispositivos móviles, la disminución de la brecha digital, la irrupción de las tecnologías de la información en las facetas cotidianas de la vida, entre otros motivos.

Dentro de las reformas introducidas, destaca aquellas relacionadas con la inclusión de la Banca Móvil como un canal adicional de distribución de servicios financieros, y la definición de los "dispositivos móviles" como instrumentos que permiten impartir "las órdenes para la realización de operaciones a través de los canales de distribución (…)".

LEY 1480 de 2011: Esta ley se crea con la intencion de proteger, promover y garantizar la efectividad y el libre ejercicio de los derechos de los consumidores, tambien el amparar el respeto de su dignidad y a sus intereses económicos, en referencia a:

El acceso de los consumidores a una información adecuada.

La educación del consumidor.

La libertad de constituir organizaciones de consumidores y la oportunidad para esas organizaciones de hacer oír sus opiniones en los procesos de adopción de decisiones

que las afecten.

La protección especial a los niños, niñas y adolescentes.

Capítulo I del Título II de la Parte I de la Circular Básica Jurídica – Circular Externa 029 de 2014: define la Banca Móvil como un canal de banca electrónica en el cual "el dispositivo móvil es utilizado para realizar operaciones y su número de línea es asociado al servicio". Esta conceptualización contiene un elemento importante en la medida en que trazó una distinción fundamental, y es que los servicios a los que el consumidor financiero acceda utilizando un dispositivo móvil, pero a través de un navegador web y sin que haya asociación del servicio a la línea móvil, son considerados por la circular como banca por internet para todos los efectos.

"La prestación de servicios a través de banca móvil debe cumplir con los siguientes requerimientos:

2.3.4.11.1. Contar con mecanismos de autenticación de 2 factores para la realización de operaciones monetarias y no monetarias.

2.3.4.11.2. Para operaciones monetarias individuales o que acumuladas mensualmente por cliente superen 2 SMMLV, implementar mecanismos de cifrado fuerte de extremo a extremo para el envío y recepción de información confidencial de las operaciones realizadas, tal como: clave, número de cuenta, número de tarjeta, etc. Esta información, en ningún caso, puede ser conocida por los proveedores de redes y servicios de telecomunicaciones ni por cualquier otra entidad diferente a la entidad financiera que preste el servicio a través de este canal. Dicha información tampoco puede ser almacenada en el teléfono móvil.

2.3.4.11.3. Cualquier comunicación que se envíe al teléfono móvil como parte del servicio de alertas o notificación de operaciones no requiere ser cifrada, salvo que incluya

información confidencial.

2.3.4.11.4. Para las operaciones monetarias individuales o que acumuladas mensualmente por cliente sean inferiores a 2 SMMLV y que no cifren la información de extremo a extremo, la entidad debe adoptar las medidas necesarias para mitigar el riesgo asociado a esta forma de operar, el cual debe considerar los mecanismos de seguridad en donde la información no se encuentre cifrada. La SFC puede suspender el uso del canal cuando se advierta que existen fallas que afecten la seguridad de la información.

2.3.4.11.5. Contar con medidas que garanticen la atomicidad de las operaciones y eviten su duplicidad debido a fallas en la comunicación ocasionadas por la calidad de la señal, el traslado entre celdas, entre otras.

2.3.4.11.6. Los servicios que se presten para la realización de operaciones a través de Internet, en sesiones originadas desde el dispositivo móvil, deben cumplir con los requerimientos establecidos en el subnumeral 2.3.4.9. de Internet".

Referencia: Tomado de: (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2016). Consultado el 03 de septiembre del 2018. Disponible en URL:https://www.superfinanciera.gov.co/publicacion/10087124

Ley 1273 de 2009: *"De la Protección de la información y de los datos"*, Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. Tomado de: (Dacchan T., 2018). Consultado el 03 de septiembre del 2018. Disponible en URL: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Ley 1328 de 2009 CAPITULO II DERECHOS Y OBLIGACIONES: tiene por objeto establecer los principios y reglas que rigen la protección de los consumidores financieros en

las relaciones entre estos y las entidades vigiladas por la Superintendencia Financiera de Colombia, sin perjuicio de otras disposiciones que contemplen medidas e instrumentos especiales de protección.

Normas reglamentarias sobre Protección al Consumidor Financiero:

Decreto 2555 de 2010 Título 2 Artículos 2.34.2.1.1 al 2.34.2.1.9 (deroga al Decreto 2281 de 2010 por el cual se reglamenta la Defensoría del Consumidor Financiero).

Circular Externa 018 de 2010 modifica los términos establecidos para la Transmisión de novedades con el trámite de posesiones.

Circular Externa 016 de 2010 imparte las instrucciones respecto Posesión y Registro de Defensores del Consumidor Financiero.

Circular Externa 015 de 2010 imparte las instrucciones respecto del Sistema de Atención al Consumidor Financiero SAC.

Circular Externa 038 de 2011 Imparte instrucciones relacionadas con la información a los consumidores financieros.

Circular Externa 039 de 2011 Imparte instrucciones relacionadas con la información a los consumidores financieros.

Referencia: Tomado de: (SUPERINTENDENCIA FINANCIERA DE COLOMBIA , 2009) Consultado el 03 de septiembre del 2018. Disponible en URL: https://www.superfinanciera.gov.co/SFCant/ConsumidorFinanciero/reformafinanciera.html

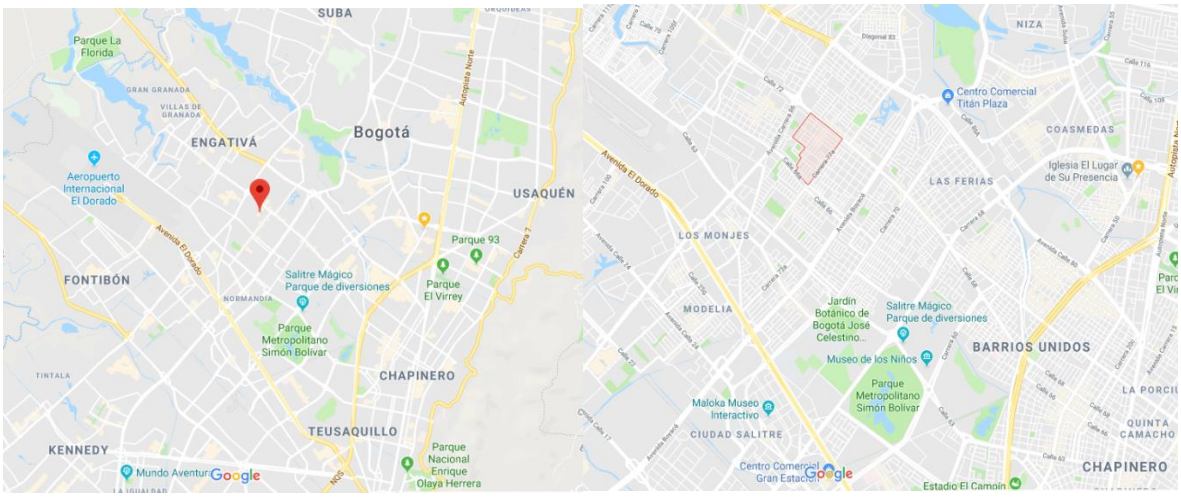
2.4 Marco geográfico

El impacto del proyecto tiene un alcance nacional, debido a que toda persona que tenga acceso a internet podrá conectarse a la red bancaria de su entidad financiera y realizar los

trámites que le sean necesarios.

El trabajo de proyecto de trabajo de grado se realiza en la ciudad de Bogotá en el marco del edificio central del Banco Gran Colombiano creado especialmente para este proyecto. Y cuyos estamentos cercanos apoyan la gestión que simuladamente se va a realizar, situado en la localidad de Engativá, barrio Santa Helenita, ubicado en el Noroccidente de la ciudad de BOGOTA.

Mapas de micro Localización



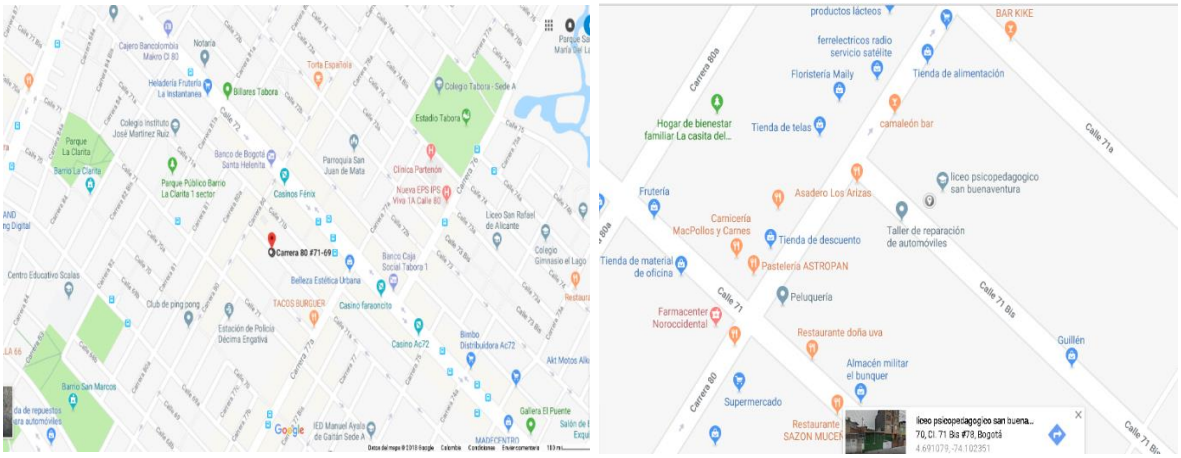


Figura 17. Microlocalización en Mapas

Fuente, Google maps

Departamento: Cundinamarca.

Ciudad: Bogotá.

Localidad: Engativá

Barrio: Santa Helenita (Noroccidente)

Lugar: Instalaciones del Banco GranColombiano. Creado para realizar el seguimiento de la trazabilidad de la operación de Tokens.

Carácter: Privado.

2.5 Marco demográfico

El presente proyecto beneficia directa o indirectamente a una población mayor de edad que según proyecciones del DANE a 2018 en Colombia asciende a 34.379.607 de personas, o aquellos menores con autorización para el manejo de cualquier producto financiero, hombre o mujer, con estudios iguales o superiores de básica primaria. El proyecto está dado para que las personas de todos los estratos socioeconómicos se vean directa o indirectamente afectados en la finalidad del proyecto, pero según

estimaciones realizadas por el la ASOBANCARIA en 2015, 3 de cada 10 colombianos no usan ningún tipo de producto financiero en donde la mayoría de estas personas son de estratos inferiores al 3, y en el caso del estrato 1 solo el 24% tiene al menos una cuenta de ahorro, mientras que el estrato 6 la cifra aumenta hasta el 74%. Viendo las condiciones expuestas anteriormente el proyecto tendrá mayor impacto en la población de estrato 3 en adelante.

(Avila Forero, 2018) 13 de agosto de 2018, ¿Bancarizar o no bancarizar? https://www.dinero.com/Item/ArticleAsync/260869

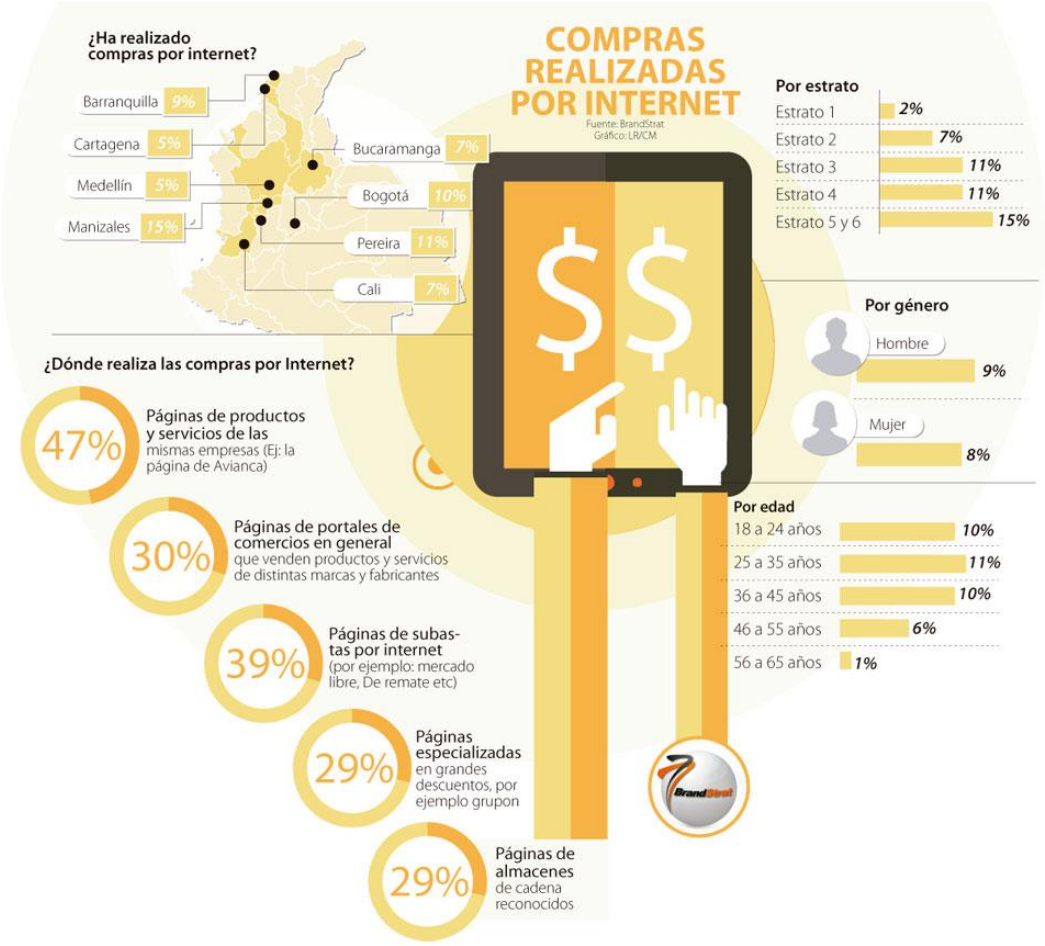


Figura 18. Estudio socioeconómico de compras por internet

Fuente: Tomado de: (Ramirez, 2015). Consultado el 16 de septiembre del 2018.

Disponible en URL: https://www.larepublica.co/consumo/pereira-y-manizales-las-ciudades-que-mas-compran-online-2231601.

En 2015 la ASOBANCARIA informo que, de la población apta para estar vinculada al sistema financiero, el 75% contaba con al menos un producto financiero y que para el año 2018 esperaban contar con un 85% de inclusión financiera en todo el tipo de población colombiana Sin importar la ubicación, tipo de raza o nivel económico. Esto y teniendo en cuenta la introducción de la bancarización a los diferentes estratos económicos en Colombia se impactará con mayor relevancia a los estratos 3, 4, 5 y 6 que representan el 55.2% de la población. Según la siguiente figura.

Figura 19. Composición de la población en Colombia por estratos

Referencia: Tomado de: (Portafolio, 2015). Consultado el 16 de septiembre del 2018. Disponible en URL: https://www.portafolio.co/tendencias/distribuidos-colombianos-

estratos-sociales-57300

Como referencia internacional podemos observar un estudio de Gemalto, realizado en Estados Unidos, Reino Unido, Brasil, México y Singapur, encontró que 38% de las personas entre 16 y 24 años de edad, utilizan su teléfono durante cinco horas diarias, y la mitad de ellos realiza sus pagos y transacciones bancarias exclusivamente desde el celular.

Pero el dato más sorprendente del estudio es que 37% de los encuestados cambiaría de banco si no pudiera realizar sus operaciones financieras desde el teléfono móvil.

"Ninguna organización con visión de futuro puede desechar hoy la movilidad como factor fundamental de su estrategia", afirma Daniel Cuéllar, vicepresidente regional de Gemalto, compañía especializada en seguridad digital. Tomado de (Revista Dinero, 2016) "Bancos se preparan para la nueva era de transacciones móviles" URL https://www.dinero.com/edicion-impresa/tecnologia/articulo/bancos-se-preparan-para-la-nueva-era-de-transacciones-moviles/225415,

3 METODOLOGÍA

Los objetivos del proyecto se ven encaminados hacia un resultado que debe ser obtenido de acuerdo con una serie de pasos sistemáticos que poco a poco van iluminando la perspectiva de todos los temas que existen alrededor del problema. Los pasos en el desarrollo llevan a que el proyecto encuentre el horizonte deseado; y para ello utiliza una metódica incremental de gestión; Ella va desde la gestión de los recursos evaluados en el presupuesto del proyecto, sigue con la obtención de la información, continua con el análisis de la misma y finalmente concluye con la metodología que se requiere para aplicar a los desarrollos para control de la aplicación de Administración de Tokens.

La metodología tiene 2 tipos esenciales que califican la calidad de la información que se levanta en los proyectos. Tipo cualitativo y cuantitativo, pero la que se destaca para este tipo de información es la cualitativa, porque depende de la observación directa.

La de Tipo Cualitativo, es aquella información obtenida de la observación y arroja conceptos que no son medibles con exactitud, si no que se obtienen directamente afinando la seguridad de la información.

Para el caso de estudio, se toma la trazabilidad del proceso en sus diferentes etapas y se da un veredicto que lleva a definir los pasos del mismo, los actores involucrados, las herramientas utilizadas, los resultados obtenidos, los interesados en el proceso, los insumos de uso, las instalaciones donde se lleva a cabo el proceso y la seguridad física que lo rodea, etc.

3.1 Fases del Proyecto

El proyecto se desarrolla en 4 grandes fases:

Conocer la realidad, elaborar el diagnóstico, destacar las acciones a realizar y se finaliza

con la entrega de los resultados.

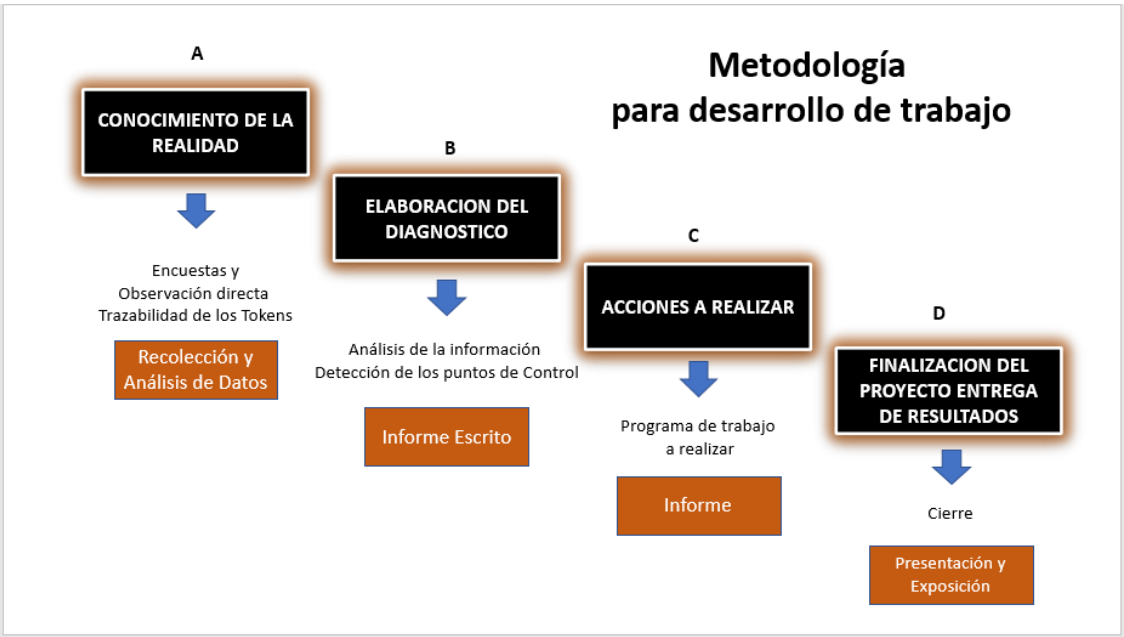


Figura 20. metodología para desarrollo de Trabajo de Investigación

Fuente: Autor, septiembre 2018

La entrega del proyecto contiene un informe detallado del recorrido de la aplicación diciendo en cada punto de control los temas cubiertos con base en los objetivos planteados y los resultados esperados al finalizar el mismo. Los resultados son obtenidos en diferentes momentos en la consecución paso a paso del proyecto de los cuales se destacan:

La aplicación del Dominio 10 de la Norma ISO 207002 que habla sobre cifrado de toda la información que se comparta entre diferentes ambientes o que tenga que viajar a través de las redes.

Todos los registros de información que manejen datos deben consignar fecha, hora, y usuario responsable del momento en que fue creado, modificado y eliminado del sistema.

Aplicación del Dominio 11 ISO 27002 que habla sobre Control de acceso a las aplicaciones. Debe haber perfilamiento en la aplicación con roles definidos, tareas asignadas

por roll y administración de las asignaciones a usuarios de los roles de la aplicación.

Aplicación de los temas de la Norma en términos de políticas de apoyo estratégico aplicando políticas de seguridad organizativa, seguridad lógica, seguridad física y apoyo de seguridad legal.

Esta figura muestra algunos de los dominios de ISO 27002 contemplados:

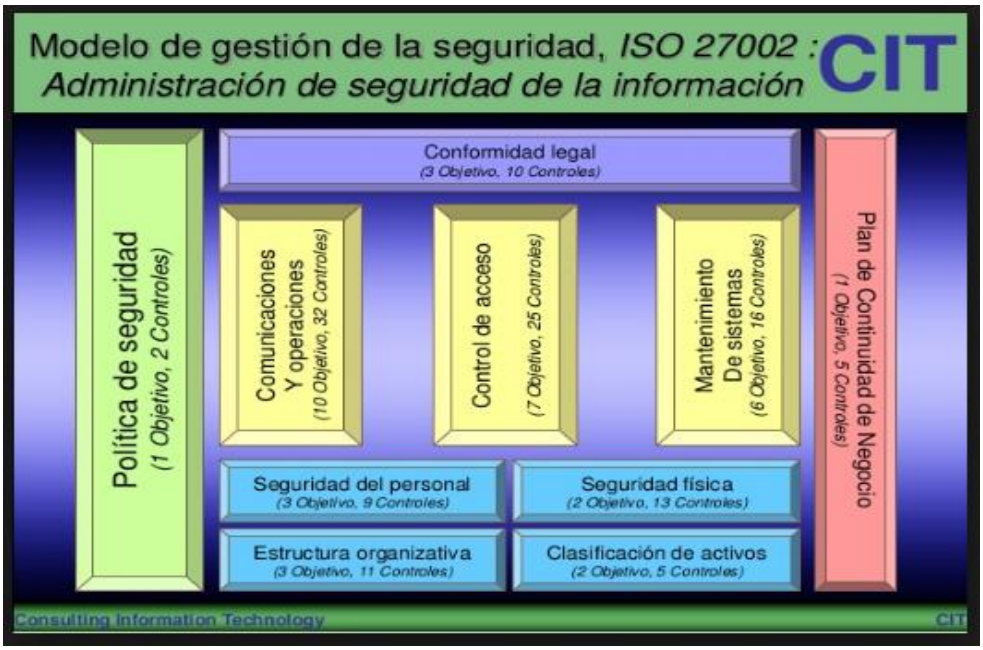


Figura 21. Dominios ISO 27002 tomados en cuenta.

Referencia: Tomado del Estándar iso iec 27002 2005 (Bonilla, 2013). Consultado el 2 de octubre de 2018 e URL: https://es.slideshare.net/cirobonilla/estndar-iso-iec-27002-2005

3.2 Instrumentos o herramientas utilizadas

3.2.1 Cuestionarios.

Los cuestionarios a ser aplicados van dirigidos a todos los interesados que hacen parte de la trazabilidad o proceso de la aplicación:

El administrador del servidor de Tokens, El director del área de tarjetas, los gestores de la aplicación, el autorizador de asignaciones y los gestores de servicio. al Cliente y monitoreo.

Ver Anexo cuestionarios.

3.2.2 Observación.

La Observación directa se realiza con varias visitas al proceso. El proceso se divide en varios tramos:

- Compra del Lote de Tokens al Proveedor Vasco.
- Recepción de los Tokens en el Banco e ingreso a cadena de custodia tanto física como lógica.
- Cargue de las semillas en el servidor de Tokens Vasco en el Banco.
- Producción del archivo de cargue del inventario de Tokens en el inventario de control del banco.
- Envío del archivo para cargue de inventario en el AS400.
- Cargue del archivo al inventario de Tokens. Las semillas se cargan para iniciar su proceso de trazabilidad de los Tokens. Los Tokens se cargan en estado N=Nuevos.
- Producción de la Solicitud de Tokens en la página de la Banca Virtual desde la creación de la BV de un Cliente, o por pérdida del token, o por deterioro del mismo.
- Atención de la Solicitud de Tokens asignando los Tokens al requerimiento.
- Inicio del proceso que llevará el Token a su destino y su uso final
- Asignación del Token a la Solicitud
- Paso para aprobación de la solicitud por parte de la administración.
- Solicitud aprobada.
- Armado del lote diario en donde se va la solicitud a su destino.
- Generación del archivo plano para envío a Domesa que es el proveedor Courrier

del banco.

- Lote por envío, o sea en ese envío al Courrier solo se va un lote junto.
- El proveedor Courrier hace la recepción del envío custodiado.
- Sube el archivo plano en su base de datos y arma sus rutas de entrega con custodia.
- El Token es entregado al cliente y Domesa informa al Banco que el Cliente ya tiene acuso de recibo del Token.
- El Cliente recibe instrucción de llamar al Banco para que el Token le sea activado y pueda ingresar a la Banca Virtual sin problema.
- El Cliente llama a Servicio al Cliente del Banco y luego de pasar el evidente de verificación de que el cliente si es quien dice ser, le activa el Token.

3.3 Población y Muestra.

La información es de tipo cualitativo y se consigue en forma explícita a través de la observación directa. En realidad, se obtiene del 100% de la población que acompaña el proceso; y se hace siguiendo la trazabilidad, e indagando a través de cuestionarios que se aplican a los interesados.

A continuación, se muestra la temática de los modelos probabilísticos y no probabilísticos, pero este modelo es clasificado como modelo no probabilístico y de tipo Casual o incidental. Del cual se hace una reseña en este momento:

Modelo No Probabilístico de Tipo Casual o Incidental:

> En el muestreo incidental el investigador determina deliberadamente qué individuos formaran parte de la muestra, tratando de escoger a los casos considerados

típicamente representativos de la población.

Es una modalidad del muestreo determinístico y ocurre cuando el investigador selecciona directa e intencionadamente a los individuos de la población o los selecciona todos, o sea población total igual a muestra.

Muestreo para Modelo de Administración de Tokens:

Es una herramienta de la investigación científica. Su función básica es determinar que parte de una realidad en estudio (población o universo) debe examinarse con la finalidad de poder hacer inferencias sobre la población.

Terminología:

Población objeto: Conjunto de individuos de los que se desea obtener una información.

Unidades de muestreo: Número de elementos de la población.

Unidades de análisis: Objeto o individuo del que hay que obtener la información.

Marco muestral: lista de unidades o elementos de muestreo.

Muestra: conjunto de unidades o elementos de análisis sacados del marco.

Tamaño de la población conocido: Tamaño de la muestra $n = (N \cdot Z^2 \cdot p \cdot q)/(e^2(N-1) + (Z^2 \cdot p \cdot q))$

Fórmula para hallar el valor de la muestra tanto en una población finita como infinita.

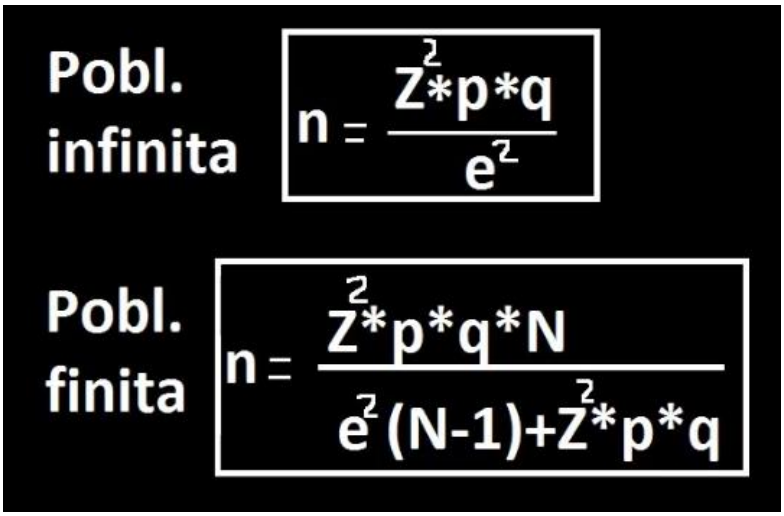


Figura 22. Fórmula para establecer la muestra

Fuente: Autor, septiembre 2018

Aplicado al caso de la población:

N = Población total involucrada de los interesados. Nivel de confianza.

e = Margen de error de la muestra.

Z = Nivel de confianza.

P = Probabilidad a favor.

q = Probabilidad en contra.

n = Muestra.

Cálculo de la muestra poblacional: Calcular la muestra para una población de 32 personas con un nivel de confianza del 95 % y un margen de error del 6%.

N ➔ 32 personas en las áreas.

e = 0.06 ➔ sale de volver número el porcentaje dividiéndolo entre 100.

Z = 1.96 ➔ sale del nivel de confianza de las tablas estadísticas, de acuerdo con el

P = 0,5 ➔valor estimado de probabilidad a favor

q = 1 – p ➔ 1 -0,5 = 0,5 probabilidad en contra.

Reemplazamos en la fórmula:

$n = (N \cdot Z^2 \cdot p \cdot q)/(e^2(N-1) + (Z^2 \cdot p \cdot q))$

$n = (32 * 1{,}96^2 * 0{,}5 * 0{,}5) / (0{,}06^2(32-1) + (1{,}96^2 \cdot 0{,}5 \cdot 0{,}5))$

$n = (32 * 3{,}8416 * 0{,}25) / (0{,}0036(32-1) + (3{,}8416 \cdot 0{,}25))$

$n = (32 * 0{,}9604)/(0{,}01152 – 0{,}0036) + 0{,}9604)$

$n = (31)/(1{,}0116 + 0{,}9604)$

$n = (31)/(1{,}972)$

n = 16 Tamaño de la muestra del proceso…

Este es el número de personas con las que vamos a trabajar para el levantamiento, análisis y realización de la metodología de la aplicación. Las personas, son miembros de diferentes áreas por las cuales se va haciendo real la utilización del token en las aplicaciones electrónicas.

Modelos Probabilísticos: Existen los métodos discretos (Ensayos de Bernoulli y las distribuciones geométrica y binomial) y Continuos (La distribución normal y distribuciones relacionadas).

He aquí la clasificación del muestreo poblacional que sirve como base para los temas de

investigación:

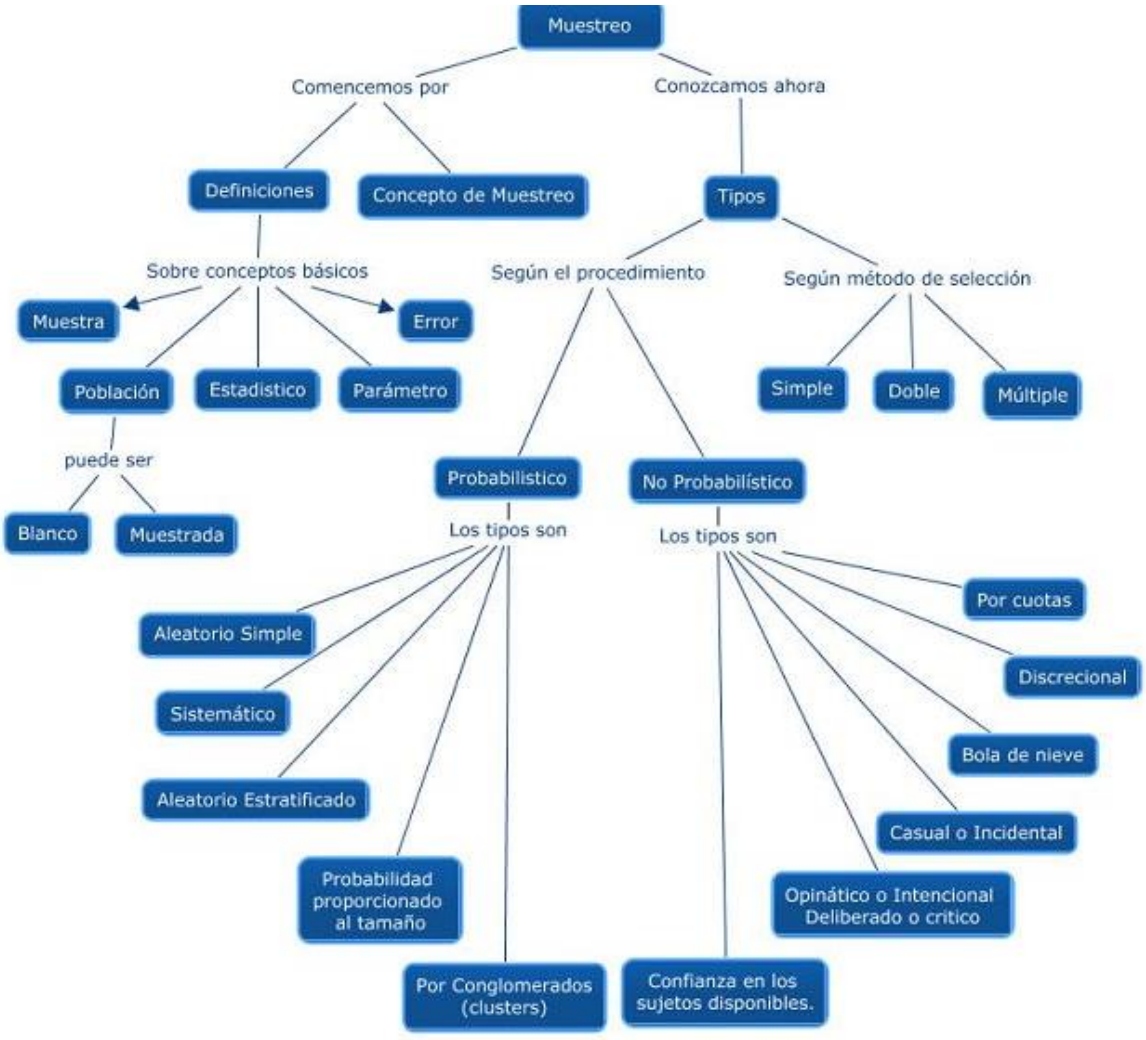


Figura 23. Clasificación de la obtención de la información.

Fuente: Tomado (Webscolar, 2018), consultado el 2018/09/14 tomado de URL:

http://www.webscolar.com/metodo-de-muestreo

Muestreo Aleatorio Simple. Muestreo en el que todas las muestras tienen la misma probabilidad de ser seleccionadas y en el que las unidades obtenidas a lo largo del muestreo se devuelven a la población. Muestreo en el que la muestra aleatoria está formada por n variables aleatorias independientes e idénticamente distribuidas a la variable aleatoria

poblacional. Sinónimo de Muestreo aleatorio con reemplazamiento.

Muestreo Sistemático: Conjunto parcial de datos escogidos al azar (muestra aleatoria) de cuyo análisis se pretende obtener conclusiones aproximadamente validad en relación al todo o universo de donde se obtuvo. Existe una relación directa entre el tamaño de la muestra y la exactitud de las conclusiones.

Muestreo Estratificado: Muestreo en el que la población se divide previamente en un número de subpoblaciones o estratos, prefijado de antemano. Dentro de cada estrato se realiza un muestreo aleatorio simple.

Muestreo Doble: Muestreo que consta de dos fases; en la primera, de las cuales se toma una muestra muy amplia a la que se analiza algún aspecto que es fundamental para la segunda fase; esta segunda fase, la constituye un muestreo cualquiera de la primera.

Muestreo Polifásico o Múltiple: El procedimiento bajo este método es similar al expuesto en el muestreo doble, excepto que el número de muestras sucesivas requerido para llegar a una decisión es más de dos muestras. Métodos de muestreo clasificados de acuerdo con las maneras usadas en seleccionar los elementos de una muestra. (webscolar, 2018) tomado de URL: http://www.webscolar.com/metodo-de-muestreo

Muestreo no probabilístico:

Muestreo por conveniencia: El muestreo por conveniencia es probablemente la técnica de muestreo más común. En el muestreo por conveniencia, las muestras son seleccionadas porque son accesibles para el investigador. Los sujetos son elegidos simplemente porque son fáciles de reclutar. Esta técnica es considerada la más fácil, la más barata y la que menos tiempo lleva.

Muestreo Consecutivo: El muestreo consecutivo es muy similar al muestreo por conveniencia, excepto que intenta incluir a TODOS los sujetos accesibles como parte de la

muestra. Esta técnica de muestreo no probabilístico puede ser considerada la mejor muestra no probabilística, ya que incluye a todos los sujetos que están disponibles, lo que hace que la muestra represente mejor a toda la población. Fuente: Tomado de RRL: https://explorable.com/es/muestreo-no-probabilistico

Formulación para cálculo muestral:

FÓRMULAS DE CÁLCULO PARA n

SITUACIÓN N	PARA ESTIMAR LA MEDIA POBLACIONAL (μ)	PARA ESTIMAR LA PROPORCIÓN POBLACIONAL (P)
N es infinita	Donde: $n = \left(\frac{Z_{\alpha/2}\sigma}{e}\right)^2$ $Z_{\alpha/2}$ = se define según el N.C. σ = Desviación estándar e = Error máximo tolerable	Donde: $n = \frac{Z^2_{\alpha/2}pq}{e^2}$ $Z_{\alpha/2}$ = se define según el N.C. p = Proporción de elementos que poseen la característica de interés e = Error máximo tolerable
N es finita (conocida)	$n = \frac{Z^2_{\alpha/2}N\sigma^2}{\sigma^2 Z^2_{\alpha/2} + (N-1)e^2}$ Donde: N = Tamaño dela población. Las demás especificaciones, son las mismas	$n = \frac{Z^2_{\alpha/2}Npq}{pqZ^2_{\alpha/2} + (N-1)e^2}$ Donde: N = Tamaño de la población. Se mantienen las demás especificaciones

Figura 24. Formulación Muestreo simple.

Fuente: Tomado del (Navarro, 2010). Consultado el 2018/10/02 URL: https://es.slideshare.net/milit/muestreo-aleatorio-simple

3.4 Población y Segmentación.

Así como la dirección del marco demográfico sectoriza la población apta para obtener los beneficios de poder tener una vinculación bancaria, entonces quienes se benefician del tema de la Administración de Tokens son las personas que teniendo productos bancarios asumen

canales electrónicos que los llevan al uso obligatorio de ellos para resguardar con seguridad compartida los accesos a sus productos financieros.

La siguiente gráfica muestra la participación año por año de los diferentes canales virtuales a los cuales se les asigna Tokens como mecanismo de autenticación fuerte.

Los canales de Internet, ACH, Telefonía móvil, etc. usan dispositivos de seguridad fuerte, por lo tanto la importancia que merecen es de carácter especial. El porcentaje ha venido incrementándose año por año, haciendo de los canales virtuales, los de mayor sintonía. Y es que es muy atractivo dejar de hacer colas en las entidades financieras, evitarse el transportarse hasta las instalaciones de los bancos, y las congestiones callejeras, además de exponerse a la inseguridad de las ciudades.

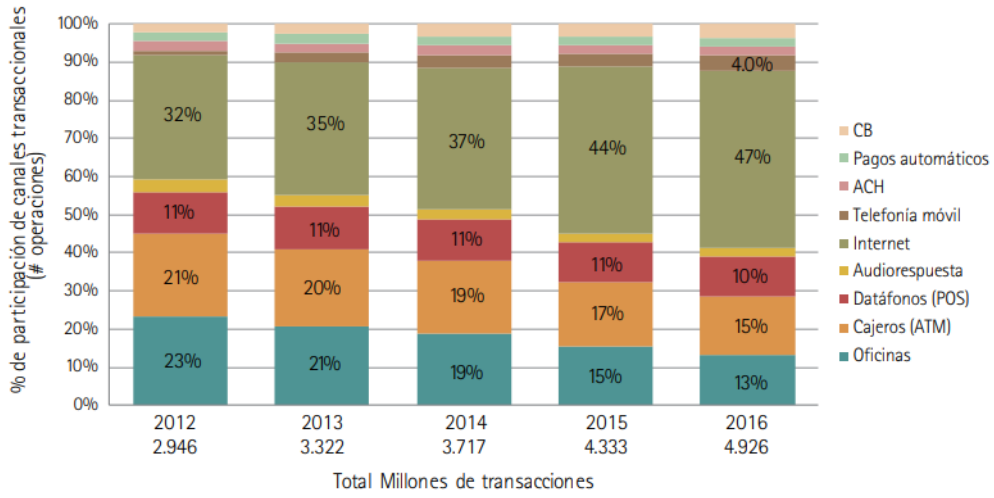


Figura 25. Participación de canales transaccionales. Número total de transacciones.
Fuente: Tomado de (Superintendencia Financiera de Colombia, 2017) consultado el 02 de octubre de 2018. URL:

http://bancadelasoportunidades.gov.co/sites/default/files/2017-07/RIF%202016-%20final.pdf

Los porcentajes de canales virtuales se incrementan, el renglón del uso de participación

de los Smart Phones y las aplicaciones que se desarrollan a la medida para acceder a las transacciones bancarias también. Todo esto justifica que se tenga una buena causa para tener en cuenta la importancia del uso de los Tokens y por ende su administración. La siguiente gráfica muestra como la Banca Móvil va ganando terreno en el tema de servir como medio de un canal virtual para apoyar la transaccionalidad financiera usada por los clientes de los bancos.

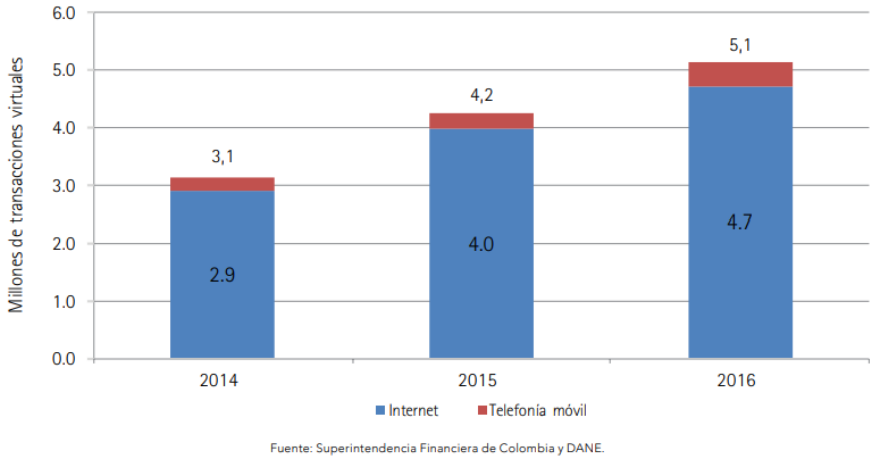


Figura 26. Número de transacciones virtuales por cada 100.000 personas

Fuente: Tomado del (Superintendencia Financiera de Colombia, 2017) consultado el 02 de octubre de 2018. URL: http://bancadelasoportunidades.gov.co/sites/default/files/2017-07/RIF%202016-%20final.pdf

Se puede también observar la participación de todos los Bancos en Colombia tanto en Nro. de operaciones como en valores de las mismas, monetarias y no monetarias; estas, año por año van incrementándose dando mayor importancia al uso de los Tokens en todo sentido.

Los Tokens son una autenticación fuerte, y por lo tanto dan seguridad transaccional a las operaciones bancarias para dar gran seguridad a las operaciones. El uso de los Tokens ya superó la década, lo que quiere decir que han sido efectivos a la hora de apoyar las

autenticaciones de los clientes en los canales virtuales.

Montos en millones de pesos

Nº	Nombre de la Entidad	Número de Operaciones Monetarias	Número de Operaciones no Monetarias	Número Total de Operaciones	Monto de Operaciones
1	Bancolombia	463.726.155	831.039.513	1.294.765.668	945.238.300
2	Banco Davivienda	177.137.453	81.592.786	258.730.239	483.230.106
3	Banco de Bogotá	140.230.401	94.432.137	234.662.538	717.890.475
4	BBVA Colombia	122.080.856	48.597.519	170.678.375	272.818.445
5	Banco AV Villas	62.154.640	20.108.443	82.263.083	58.692.629
6	Banco Colpatria	48.866.201	13.993.158	62.859.359	74.840.436
7	Banco Caja Social BCS	45.957.486	12.477.081	58.434.567	58.831.674
8	Banco Agrario	37.556.443	22.311.039	59.867.482	54.661.324
9	Banco Popular	37.500.884	10.166.129	47.667.013	81.094.998
10	Banco de Occidente	35.056.787	8.809.283	43.866.070	293.323.462
11	Citibank	34.097.730	34.267.814	68.365.544	190.641.629
12	Tuya	20.609.767	4.230.565	24.840.332	5.687.360
13	Banco Corpbanca	20.190.137	9.318.432	29.508.569	119.340.616
14	Banco Falabella	17.577.470	6.668.626	24.246.096	6.159.328
15	Banco GNB Sudameris	15.239.249	4.779.757	20.019.006	72.861.726
16	Bancoomeva	5.887.027	1.804.522	7.691.549	7.693.152
17	Giros & Finanzas	5.335.722	362.234	5.697.956	3.170.605
18	Serfinansa	5.226.305	3.447.815	8.674.120	2.082.907
19	Banco Pichincha	4.655.203	1.014.801	5.670.004	8.022.746
20	Banco WWB.	3.377.585	1.169	3.378.754	1.565.308
Total		**1.302.463.501**	**1.209.422.823**	**2.511.886.324**	**$3.457.847.226**

Figura 27. Volumen de Operaciones en el segundo semestre 2016

Fuente: Tomado (Superintendencia Financiera de Colombia, 2017) Consultado el 04 de octubre de 2018. URL: https://www.superfinanciera.gov.co/jsp/10082624

3.5 Recolección de datos

La recolección de la información que va apoyar el desglose metodológico de la traza del proceso, que para este caso se hace a través de la observación directa del punto: 'Observación', con los cuestionamientos directos y sin entregar las encuestas a los interesados. Se hace puesto por puesto siguiendo el camino que la consecución de los pasos indica. Y observando lo que se hace en cada punto de la transformación de la información.

Se deben recoger todas las evidencias paso a paso, los reportes generados y establecer lo

que se hace y lo que se debería hacer según la aplicación de las normas de los dominios de estudio.

El Proceso de Cargue de semillas es como sigue, según la observación que se realiza de antemano, en donde muestra paso a paso como se observa en la gráfica del cargue de los nuevos Tokens comprados tanto en la consola servidor de Tokens, como en el inventario que se va a administrar. Los otros 2 procesos de estudio los detallaremos en el desarrollo del proyecto más adelante.

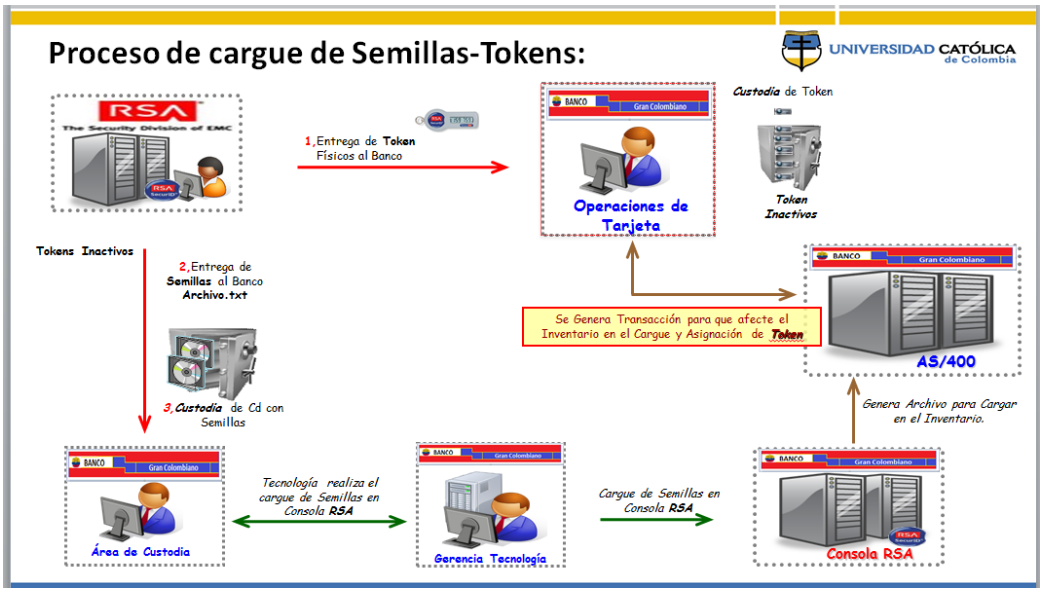


Figura 28. Primer proceso. Trazabilidad del proceso de obtención de semillas y cargue a los inventarios.

Referencia: Desarrollo con base en la observación del Banco de Estudio.

3.6 Diagnóstico de la Muestra.

La muestra generalizada evidencia punto por punto la revisión de las fallas que pueden presentarse, los riesgos a que está expuesto y los controles que deberán aplicarse en el desarrollo del software para recomendar como podría ser más seguro tanto para la entidad

financiera como para el cliente.

El nivel de significación de una prueba estadística es un concepto estadístico asociado a la verificación de una hipótesis. En pocas palabras, se define como la probabilidad de tomar la decisión de rechazar la hipótesis nula cuando ésta es verdadera (decisión conocida como error de tipo I, o "falso positivo").

Si el valor de (P) Probabilidad (generalmente 0,05) está por debajo de un nivel de significancia especificado, se puede decir que la diferencia es estadísticamente significativa y rechaza la hipótesis nula de la prueba. A penas se menciona, pero el trabajo no tiene media poblacional dentro del banco, luego la medida de significancia no sería necesario encontrarla.

Si se generaliza a todos los Bancos la población que administra los tokens es muy similar a la del Banco de estudio. Y la calidad de clientes fue explicada en los puntos de los marcos vistos en el punto 2.

3.7 Resumen final de la Metodología.

Para resumir la Metodología, la exponemos en 4 grandes etapas:

INICIO

- Definición del Proyecto.
- Definición del alcance.

PLANEACION

- Construcción proyecto previo.

EJECUCION y MONITOREO

- Ejecución del Proyecto
- Análisis de resultados.

CIERRE DEL PROYECTO.

- Presentación del Proyecto.

Los detalles los encontramos en la siguiente Figura:

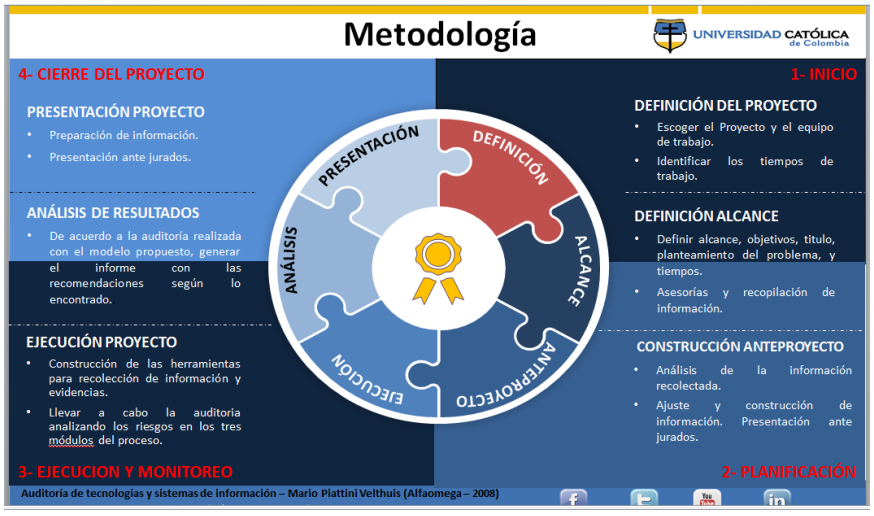


Figura 29. Resumen de la Metodología definida para el Proyecto.

Referencia: Auditoría de tecnologías y sistemas de información – Mario Piattini Velthuis (Alfaomega–2008). Extracción y mezcla propia para aplicar el desarrollo.

4 DESARROLLO DE LA PROPUESTA

Para el desarrollo de la propuesta de trabajo se aprovecha la trazabilidad de las operaciones. Se va paso a paso dentro de la dinámica de programas, mostrando los detalles de cada uno de los ítems y revisando la aplicación de normas y estándares reconocidos; normas que se han investigado y que deben aplicarse, entre ellas: las de temas de calidad, de servicio, de seguridad y la parte procedimental del ejercicio, que va dando cuerpo al desarrollo del programa.

Se comienza por la configuración del sistema donde corren las aplicaciones que rodean todo el proceso.

Área de la plataforma:

Hardware: El proceso funciona segmentado en dos grandes partes:

Interna: La administración de Tokens:

La Base de datos para la administración de Tokens en un Banco funciona en un entorno:

Tabla 1

Entorno

Componente	Descripción
Base de Datos	DB2 AS400 de IBM

Datos obtenidos en em campo (Elaboración propia)

Tabla 1. Descripción Servidor de Aplicaciones Interno

Externa (hacia el cliente) Aplicación para clientes:

Los clientes de la Aplicación funcionan en un entorno con la siguiente descripción:

Componente	Descripción
Servidor	Power 770+ (LPART-Banca Virtual)
CPU	1.1 Core de procesamiento
Memoria Ram	6,5 GB
Disco Duro	5 TB

Descripción Servidor de Aplicaciones del cliente

Software: El sistema funciona con los siguientes:

Software	Descripción
SuSe Linux 11 SP3	Sistema operativo Servidores
Java 8	Java de la aplicación
McAfee	Antivirus
Genexus	Para desarrollo y administración la Base de Datos
Windows 10	Sistema Operativo Clientes
Antispam	Protección Anti Spam
Apache	2.2.14

Redes:

Componente	Descripción
Firewall	Fortinent 1200
Firewall para redundancia	Juniper
Proveedor de Internet	ETB
Proveedor alterno de internet	Telefónica
Routers	SISCO
Switches	Huawei
Tomcat	8.5.6

Módulos

Cargue de semillas Tokens

Creación solicitud Tokens

Asignación de Token a la solicitud

Documentación: Se tienen los siguientes documentos sobre el aplicativo:

Diccionario de Datos

Inventario de objetos de la Base de datos

Modelo Entidad Relación

Diagramas de flujo de los procesos

Normas internas del banco que rigen los suministros y procesos de la aplicación

4.1 Levantamiento de información operativa y de seguridad

Con el fin de iniciar con la fase de desarrollo del proyecto iniciamos el levantamiento de la información de los 3 módulos del sistema de Token´s.

4.2 Cargue de semillas de Token. (Proceso número uno).

Flujo de la Operación de Administración de Semillas: Opera desde que se inyectan las Semillas en el Inventario y en la consola, se sincronizan y se hace la asignación a los clientes entregándoles los Tokens y luego inicializárselos a estado Activo.

El gráfico muestra a través de las flechas el camino del Token al inventario de semillas y al inventario de administración de Tokens en el AS400, cuya alimentación inicia los

procesos de vida de los mismos:

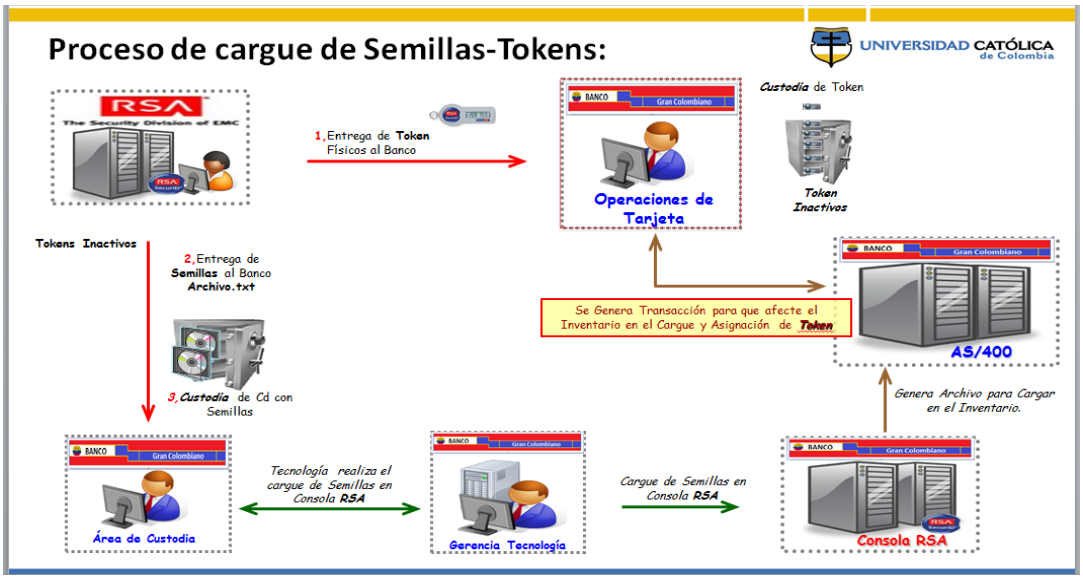


Figura 30. Proceso cargue de semillas de Token´s

Autenticación del Cliente en Banca Virtual: Este es el proceso a través del cual cada uno de los clientes ya sea de empresas como de personas usa el Token como método de autenticación fuerte y se verifica frente a la aplicación de Banca Virtual usando Usuario, Clave y Token como validadores de su identidad real ante el Banco.

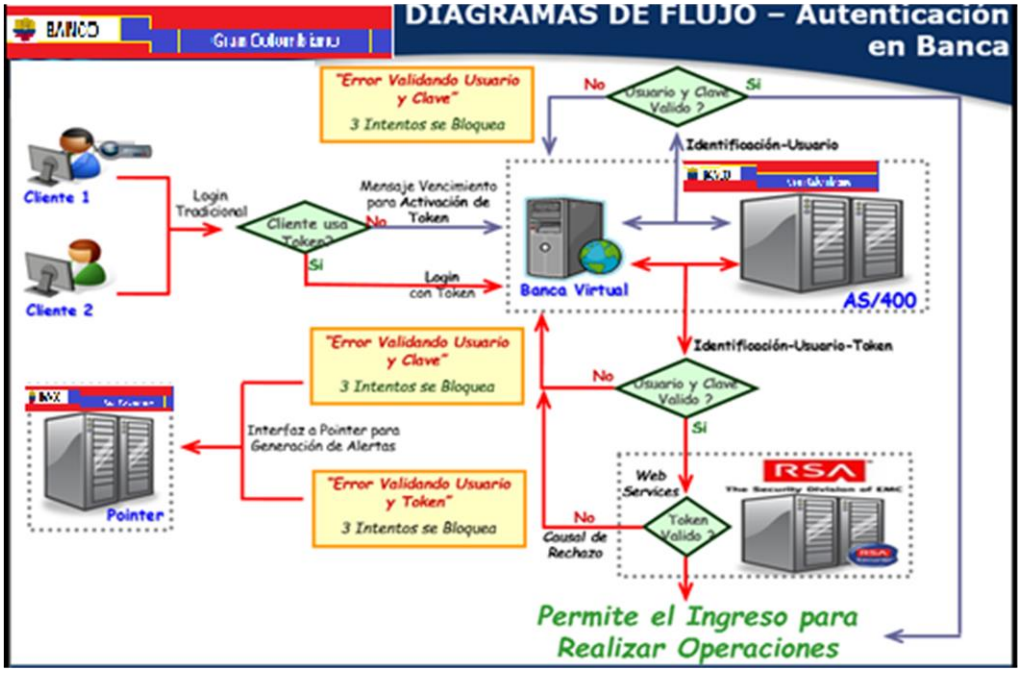


Figura 31. Diagrama de flujo, Autenticación en Banca

Entradas:

Archivo de texto (secreto) generado por el DBA en el servidor de Tokens Vasco.

Ventana de cargue de semillas del usuario administrador en la aplicación de Tokens.

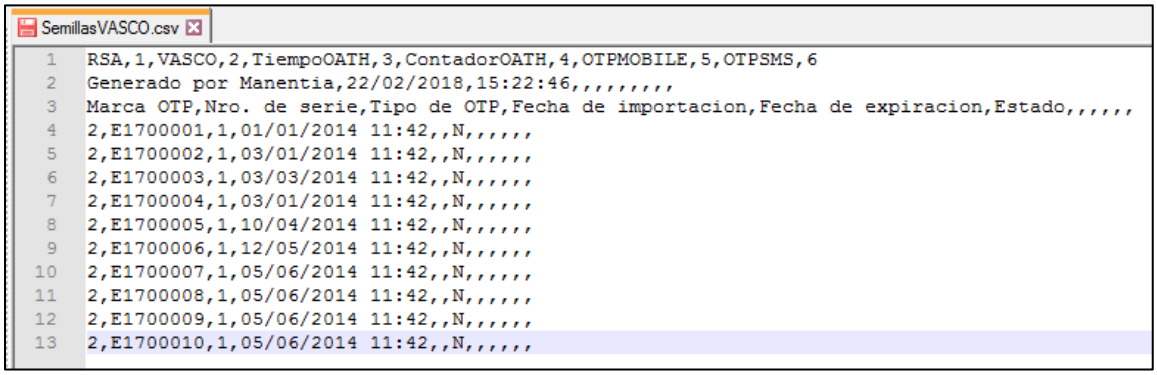


Figura 32. Ventana de cargue de semillas

La pantalla siguiente muestra el inventario cargado en la tabla BDOD14 y que es el mundo de tokens que se van a utilizar para entregarlos a los clientes. La identificación del Token es un número de serial que se encuentra atrás de cada token físico y que servirá para atar a las identificaciones de los clientes con el serial del token.

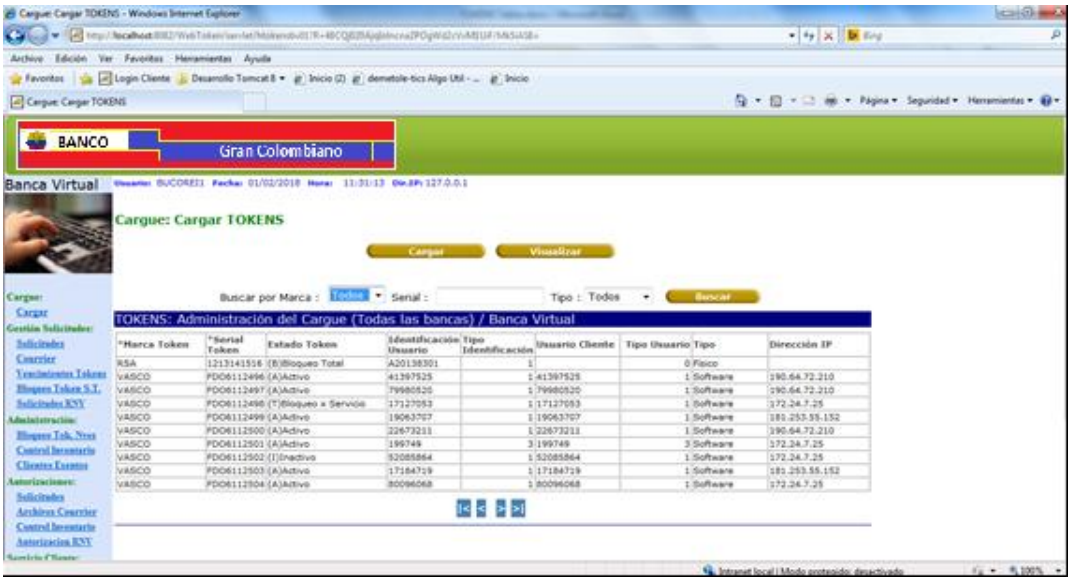


Figura 33. inventario cargado en la tabla BDOD14

Información del usuario logueado en la aplicación que realizará el cargue.

Figura 34. Información del usuario logueado en la aplicación que realizará el cargue

Procesos:

El usuario con perfil administrador del aplicativo ubicado en la ventana de CARGAR TOKENS selecciona la opción CARGAR ARCHIVO PLANO y selecciona el archivo en la ruta del sistema donde lo haya descargado el correo recibido y lo escoge para cargarlo, una vez aparece en la pantalla el archivo seleccionado, elige la opción ‘cargar’ para procesar el archivo plano que ha recibido por correo el director de operaciones de tarjetas

del área de seguridad informática.

Aquí, desde el inventario escogemos con el botón ‘cargar archivo plano’ el archivo a ser cargado.

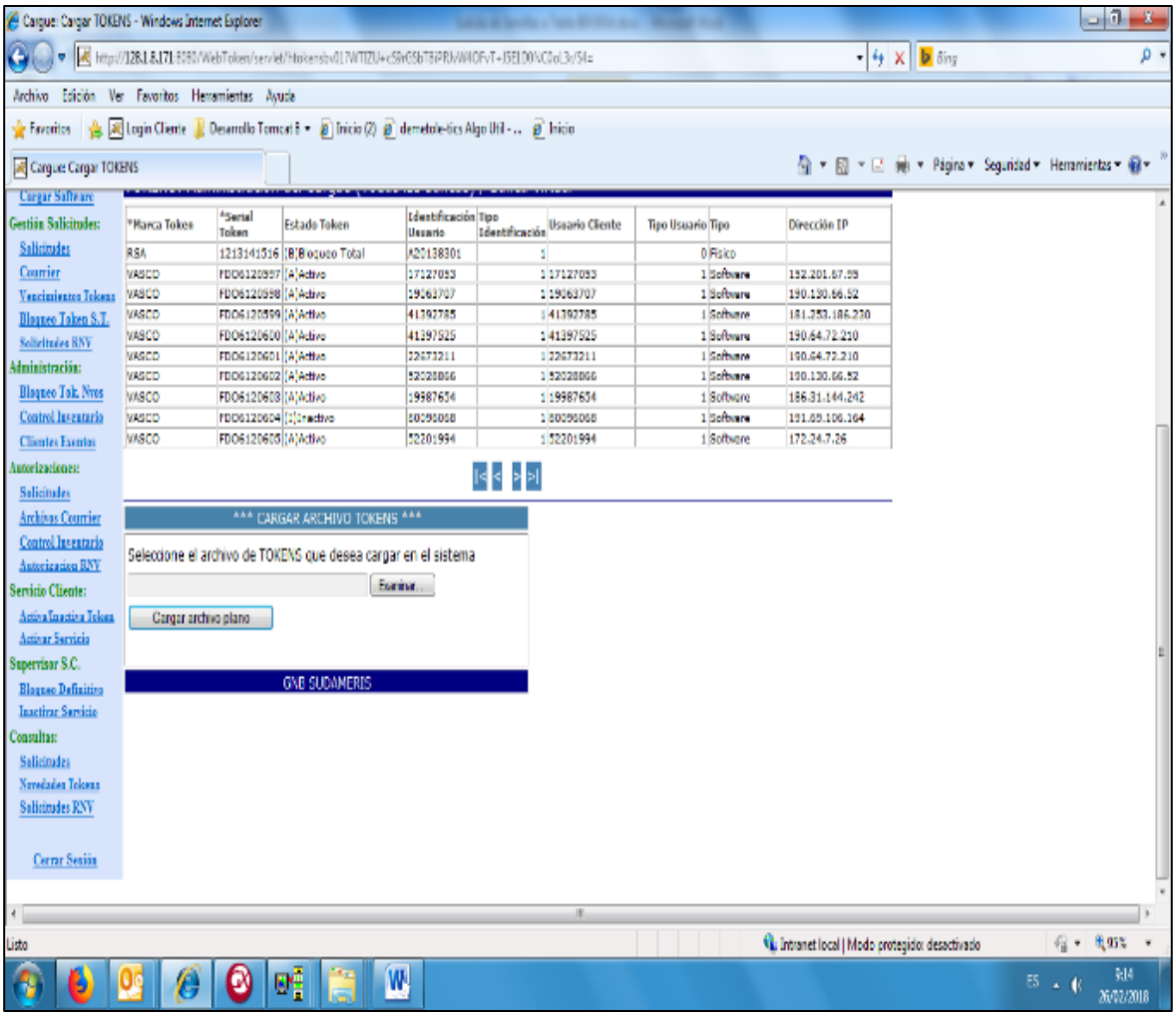


Figura 35. Ventana para cargar archivo plano

Aquí muestra el archivo plano a ser subido al inventario y que debe seleccionarse para realizar el cargue.

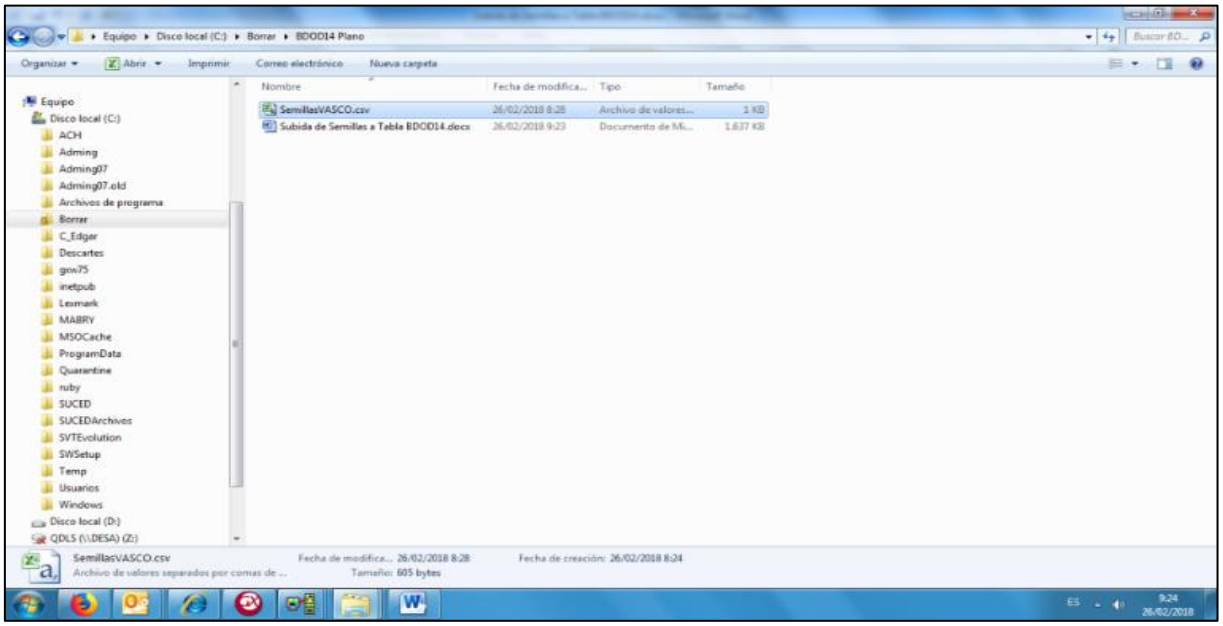


Figura 36. Ubicación archivo plano

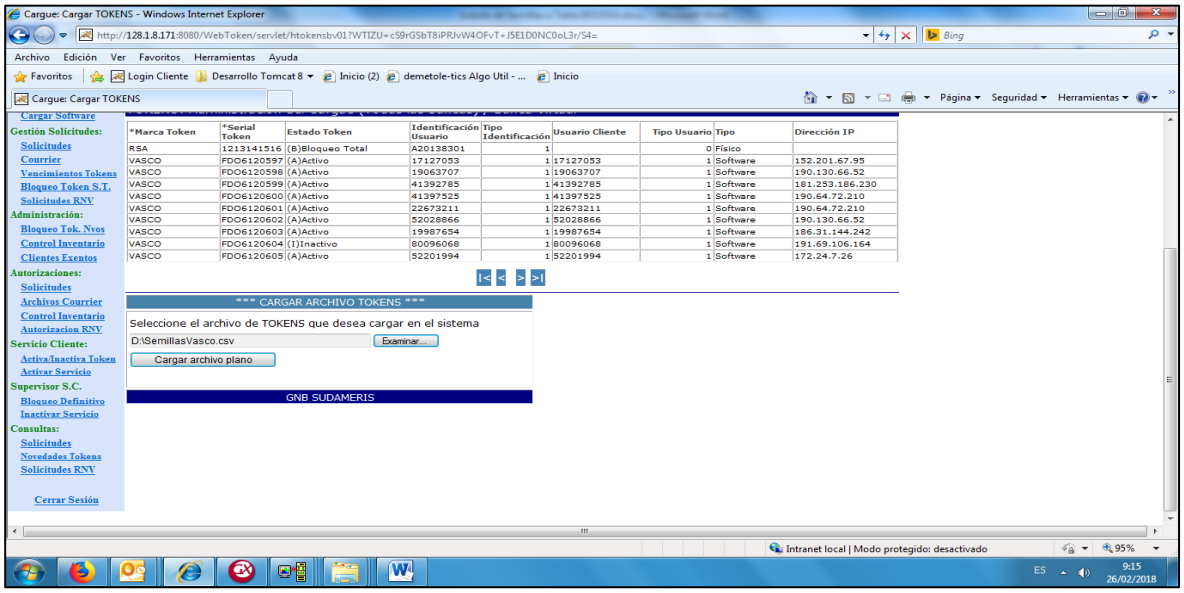


Figura 37. Ruta para el cargue del archivo

Aquí ya muestra la ruta tomada para cargar el archivo, y se le dice que ‘cargar el archivo plano’.

El sistema internamente comienza a procesar registro a registro contenido en el archivo obteniendo de cada campo la información y validando el formato.

A cada registro procesado le asigna del estado “N” el cual significa que se encuentra en el inventario y es nuevo o disponible.

El avance en el procesamiento de los registros a nivel del sistema se refleja en la ventana de estado la cual Informa el total de registros en el archivo y el total de registros cargados al sistema los cuales deben coincidir.

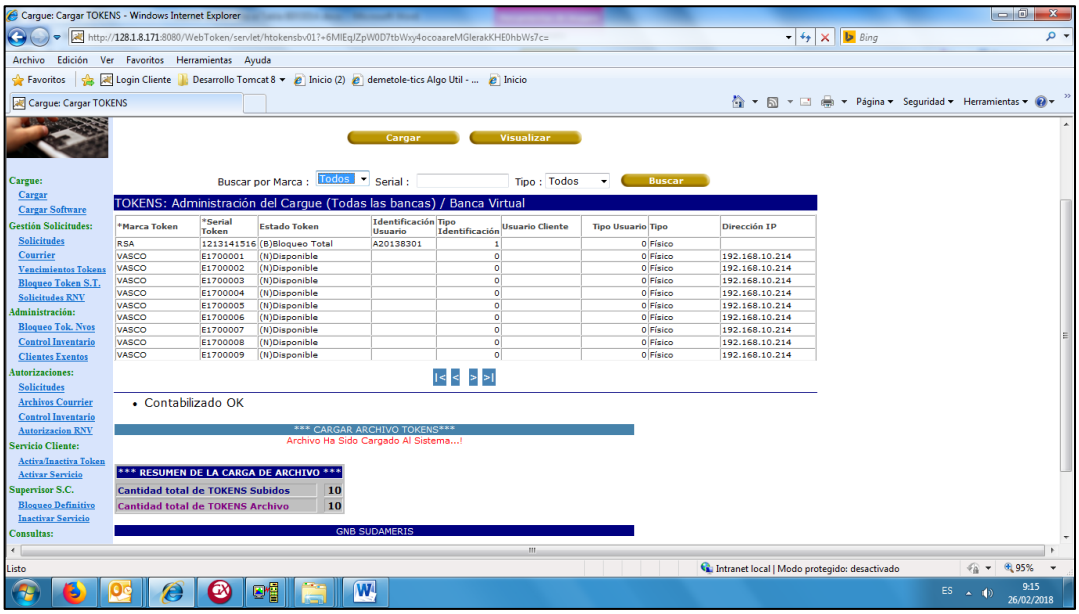


*Figura 38. T*otal de registros en el archivo y el total de registros cargados

Si algunos de los registros han sido procesados previamente, ya no hay forma de eliminar registros en el sistema. Adicionalmente, si algún registro llega a fallar y no es cargado el sistema y si por alguna razón se vuelve a enviar el archivo con más registros de los cuales cierta cantidad ya están cargados al sistema y otros son nuevos aunque se procese todos los registros en las validaciones el sistema informa que sólo se procesarán x cantidad correspondiente a los nuevos registros de un total de registros en el sistema en que los otros

ya están cargados al sistema y no informa el rechazo de estos registros en el archivo.

La tabla de inventario tiene como condición que sea llave única la marca y serial del dispositivo Token, con el fin de no permitir duplicar registros al momento de cargarlos.

Salidas:

Registro de Tokens provenientes del cargue a la tabla de inventario (BDOD14)

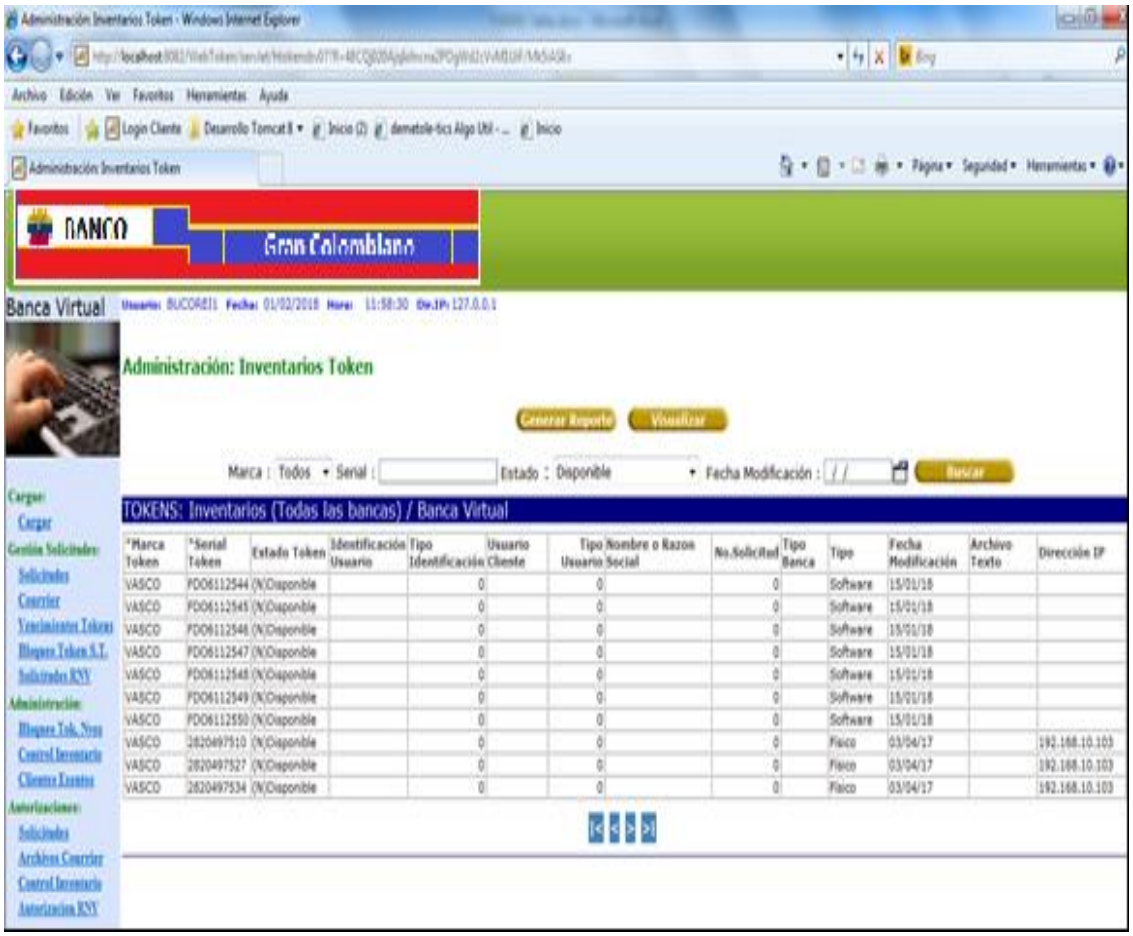


Figura 39. Registro de Tokens provenientes del cargue a la tabla de inventario

Consulta a la tabla de la base de datos DB2 donde se cargaron 10 Semillas en estado N =

Nuevo de fecha de cargue = ‘20180226’

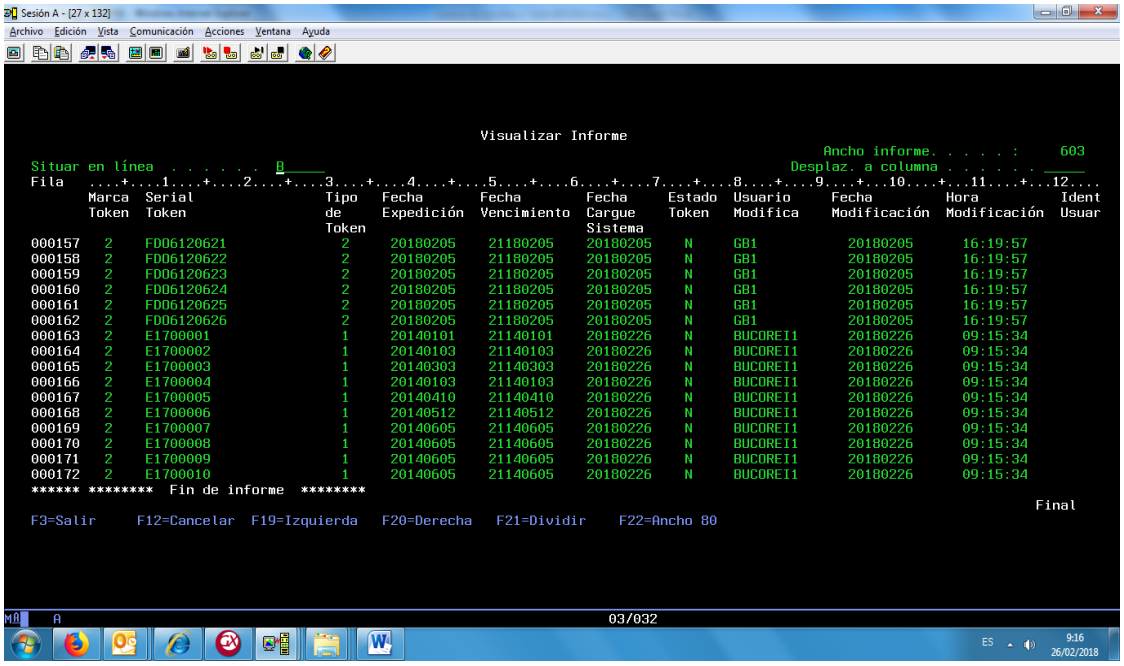


Figura 40. Registro de auditoria proveniente del cargue de Tokens a la tabla de inventario

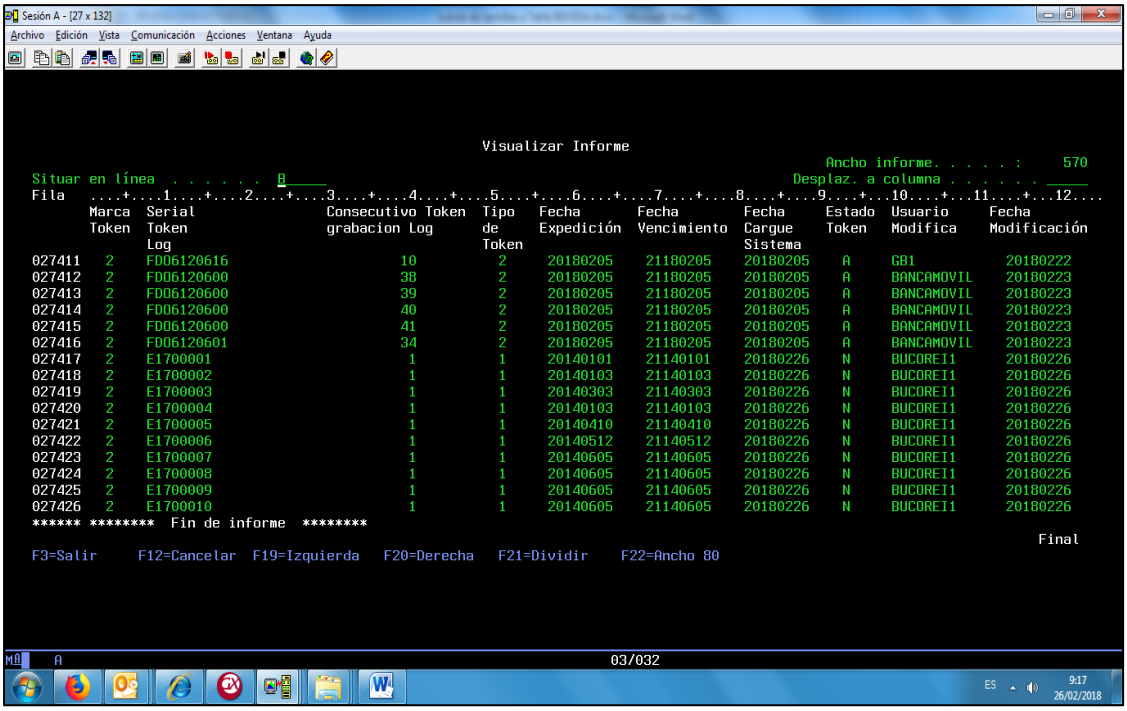


Figura 41. Registro en la contabilidad de la creación del Tokens tabla FSD016

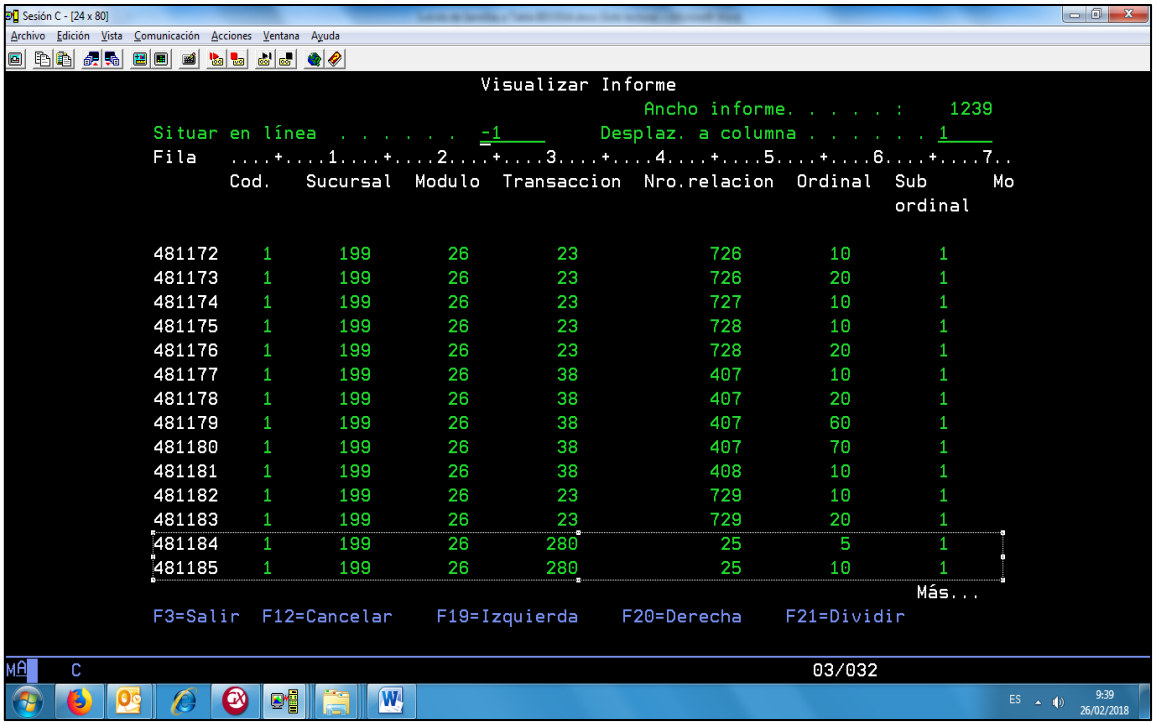


Figura 41. Registro en la contabilidad de la creación del Tokens tabla FSD016.

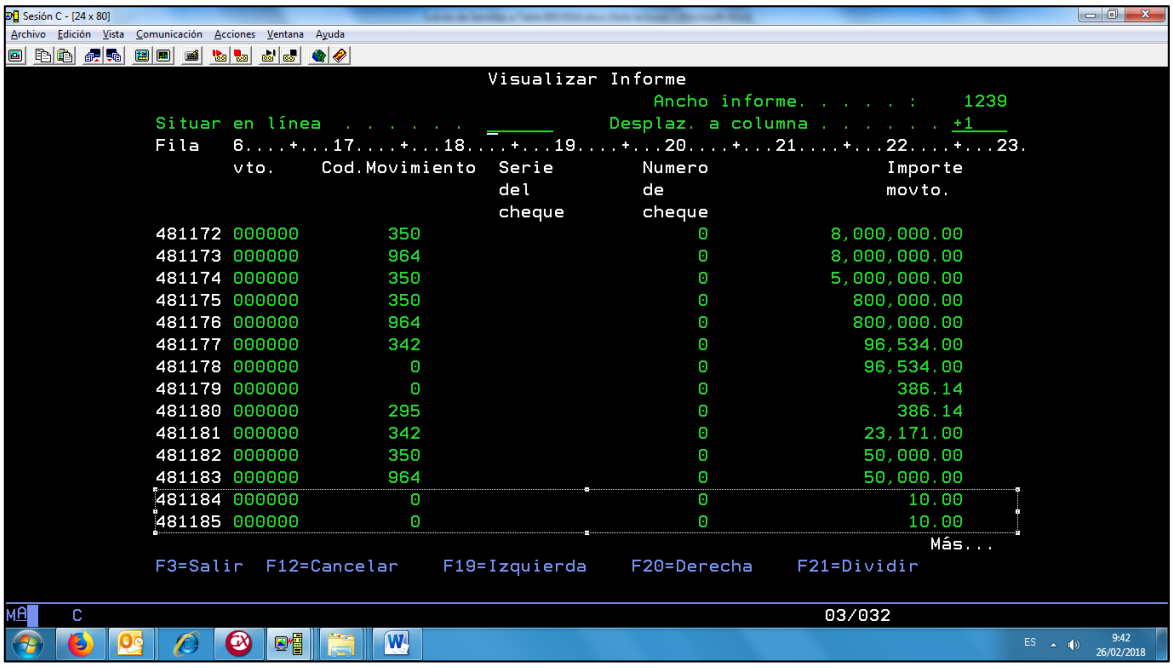


Figura 42. Registro de auditoria proveniente del cargue de Tokens

Registro de auditoria proveniente del cargue de Tokens a la tabla de inventario (BDOD16)

contiene información llave y registra secuencia de cambio, fecha, usuario, hora de quien realiza un cambio sobre registros del inventario. Se contabilizó por los Rubros de Inventarios. 10 pesos porque los Tokens entran y salen del inventario a 1 peso cada uno.

Guías de Auditoría

Guías de Auditoría utilizadas:

Durante la elaboración del trabajo usamos como apoyo guías de auditoría tomadas como sigue:

El enfoque metodológico de las guías de auditoría es basado en el marco de ISACA (Systems Audit and Control Association), con cambios para agilizarlo. Las planillas de diseño, ejecución de pruebas y documentación de hallazgos son basados en algunos modelos del ISAF (órgano autónomo encargado de revisar y fiscalizar los estados financieros, cuentas públicas estatal y municipales, de fiscalizar los ingresos y egresos) y la matriz de riesgos y controles basada en COBIT (Control Objectives for Information and related Technology) y COSO (Committee of Sponsoring Organizations of the Treadway) con algunos cambios de nuevo para hacerla más práctica. Esto quiere decir que se han incluido diferentes apartes de marcos de referencia para estandarizar una metodología y lograr más efectividad y resumen a la hora de lo que se quiere lograr con las pruebas buscando resultados para apoyar los procedimientos metodológicos.

4.3 Guía de auditoria Cargue de semillas Tokens

AUDITORÍA SISTEMAS ADMINISTRACION DE TOKENS EN UN BANCO		
PROGRAMA DE AUDITORÍA		
DEPENDENCIA:	FECHA:	
PROCESO: Cargue de semillas Tokens	ELABORADO	
PROCEDIMIENTO DE AUDITORÍA	REF. P/T	POR
OBJETIVOS: Evaluar todos los controles que se encuentran en las entradas, procesos y salidas del aplicativo para el proceso de cargue de semillas de Tokens.		
NORMATIVA APLICABLE: Norma interna del Banco para la confidencialidad de semillas entregadas por VASCO y Norma interna de auditoria para el procesamiento de semillas en el ambiente productivo de la banca Virtual.		
1. ENTRADA Y CAPTURA DE DATOS		
1.1 Verifique con el jefe de Tarjetas, que, en los últimos 10 correos enviados a éste por el DBA de la consola de VASCO, existe un único destinatario, nadie más en destinatario o con copia o copia oculta.		
1.2 Tome el ultimo archivo de semillas y constate que tiene extensión csv y que cumple con: Numero de campos establecidos Separadores “,”		
1.3 Tome una muestra de 30 registro del archivo a cargar de semillas y verifique que cada registro tiene el número correcto de campos y que la información de cada campo contiene el formato esperado ya sea caracter, numérico o fecha.		

	1.4 Verifique el jefe de Tarjetas esté supervisado por el auditor y el experto de Sistemas para realizar el proceso de cargue de semillas, observe que el jefe de tarjetas se loguea en el servidor de aplicaciones exitosamente.		
	1.5 Observe que el Jefe de tarjetas: Accede a la aplicación de tokens con usuario y contraseña en el servidor de aplicaciones. Se registran los datos del usuario en la aplicación los cuales corresponden al log auditoría que se registrará en las acciones que realice el usuario en la aplicación. El usuario tiene activo el menú para cargues de semillas. Se presenta la ventana para cargue de semillas de Tokens. Selecciona el archivo de semillas a cargar.		
	2. PROCESAMIENTO		
	2.1 Cerciórese que el usuario realiza el proceso de cargue: Selecciona la opción de cargar el archivo Se inicia el proceso de validación y registro de semillas en el sistema el cual es informado mediante la ventana de estado de la ejecución.		
	2.2 Verifique que el proceso inicia a generar un archivo de log nuevo, en la ruta de log de procesos del servidor de aplicaciones, para la carpeta de Banca virtual, el cual se nombra con el prefijo de seedLoad, seguido de él la fecha y hora en que inició el proceso de cargue de semillas con el formato YYYYMMDDhhmmss.		

2.3 Verifique que durante el proceso la base de datos presenta actividad para el registro de las semillas.		
2.4 Observe que terminado el proceso de cargue la ventana de estado presenta el número de semillas registradas en el sistema y que concuerda con el número de registros en el archivo.		
2.5 Determine que, una vez terminado el procesamiento según lo informado por la aplicación, ya no existe actividad en la Base de Datos.		
3. SALIDAS QUE GENERA LA APLICACION		
3.1 Verifique el cargue de las semillas en la tabla BDOD14		
3.2 Verifique el registro de creación de las semillas en la tabla de log BDO16		
3.3 Verifique a través de la aplicación que se visualizan una muestra de 5 semillas de las recién cargadas con estado “N” Nuevo		
3.4 Verifique se registra en la contabilidad el cargue de las nuevas semillas de Tokens disponibles		
3.5 Verifique el total de semillas cargadas en la última hora por el usuario administrador del jefe de tarjetas.		
4. PISTAS DE AUDITORIA		
4.1 Verifique el registro de creación de las semillas en la tabla de log BDO16 para las semillas que estaban contenidas en el archivo recién cargado		
4.2 Verifique que en la tabla de log BDOD16 cada Token nuevo del archivo se encuentra una única vez y que la secuencia de registro es 1.		

4.3 Verifique en el archivo de log para el proceso que no se presentó ninguna falla durante la ejecución del cargue de semillas.		
4.4 Verifique que se han registrado en la contabilidad el total se semillas que generan un costo para la banca.		
4.5 Verifique que se registra en la minuta de cargue de semillas el nombre del archivo cargado, cantidad de registro, veedores, fecha y hora, nombre y usuario que realiza el cargue.		

Diseño y ejecución de pruebas:

Prueba 1. Cargue de semillas Tokens (Entrada)

Medición de la prueba: Esta prueba mide la aplicación de los términos de seguridad explícitos en el dominio 10 de la Norma 27002 que conduce a saber si se tiene seguridad en el envío y recepción de archivos, que por efectos del proceso deben compartirse aplicando el detalle:

"**10. Cifrado:** El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas." Y aplica todo el

dominio y sus ítems.

"***9. Control de Accesos:*** El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento." Aplica en todos los módulos, y en el perfilamiento de la aplicación para definir autoridad y responsabilidad y dividir el trabajo para saber qué es lo que se hace en cada uno de los pasos de cada módulo.

Prueba:

Se toma un archivo de semillas y se constata en el contenido el formato de la

información de campo, campos obligatorios y el separador de campos:

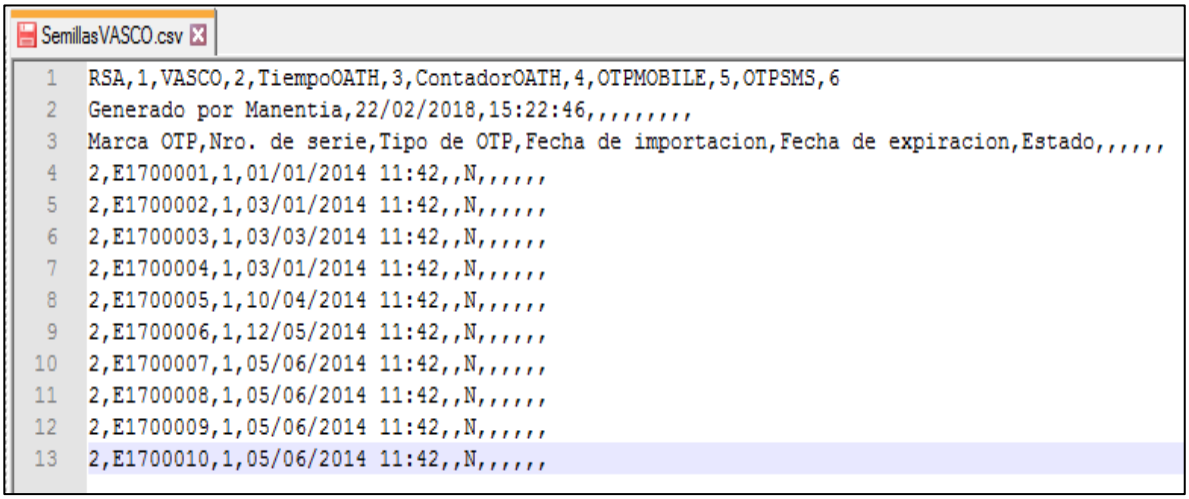


Figura 43. Archivo de semillas verificación de información

Primera línea del archivo es la información del generador, fijo:

RSA,1,VASCO,2,TiempoOATH,3,ContadorOATH,4,OTPMOBILE,5,OTPSMS,6

La segunda línea del archivo corresponde al usuario generador y fecha de generación.

El primer campo indica el proveedor, 1 - , 2- VASCO

El segundo campo es una secuencia de texto corresponde al número de serie del Token

El tercer campo indica el Tipo del Token 1- Fisico, 2- Virtual

El cuarto campos es la fecha de creacion para las semillas debe ir en formato

dd/mm/yyyy 24hh:mm

El Quinto campo debe ir nulo

El sexto campo es el estado inicial de la semilla “N” Nuevo

Los siguientes 5 campos deberá ser nulos.

Prueba 2. Cargue de semillas Tokens (Salida)

Se valida en la tabla de inventario el registro único para las semillas nuevas estado “N”

para cada una de ellas y usuario creador el del jefe fe Tarjetas.

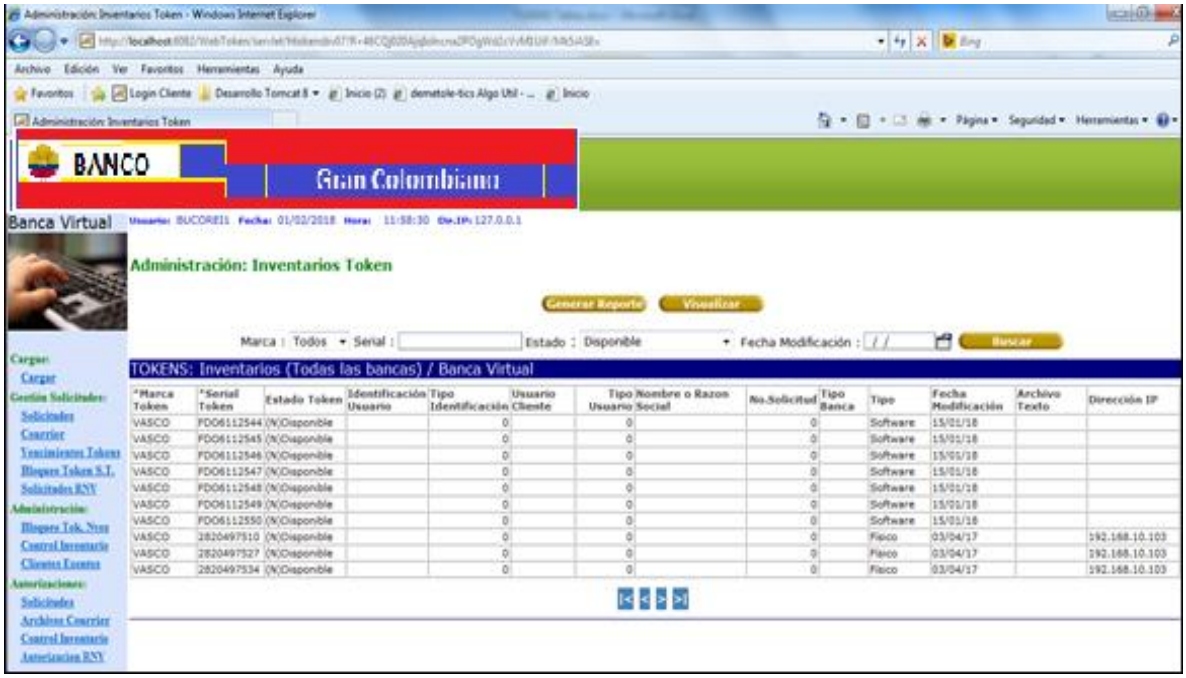


Figura 44. Tabla de inventario, registro único

nivel del aplicativo: Lo verificamos en la Pantalla del AS400: Tabla: BDOD14

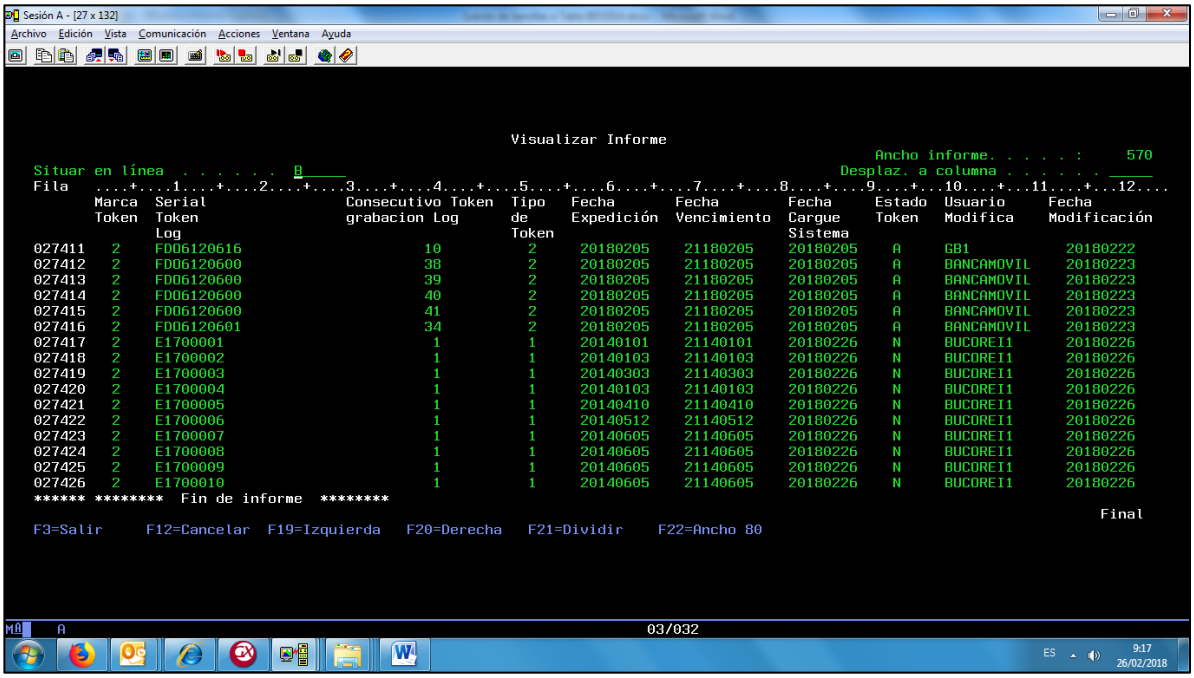


Figura 45. Pantalla del AS400, evidencia cargue

Evidencian las secuencias recién cargadas, el tipo de token, el proveedor, fecha de

expedición, fecha de vencimiento, el estado del Token y el registro del usuario que cargó la información, fecha y hora.

4.4 Creación de la Solicitud de Tokens. (Proceso número dos).

Esta sección muestra la creación de la Solicitud de Tokens desde la Banca Virtual, único sitio después de que se autentique el usuario, o desde fuera, pero con sus credenciales de cliente. El sistema le crea la solicitud al cliente tomando los datos de la (BUC) Base única de Clientes; estos datos son mostrados desde cuando fueron originados al momento de la creación del cliente. Igual están editables, por si el cliente ha cambiado de domicilio para que el token le llegue directamente a sus manos. Aquí nace el uso del token por el cliente; con el requerimiento.

Entradas:

Pedido del Token – Creación Solicitud de Token: Ingresa a la página del Banco y hace la Solicitud del Token por el ícono de: Regístrese

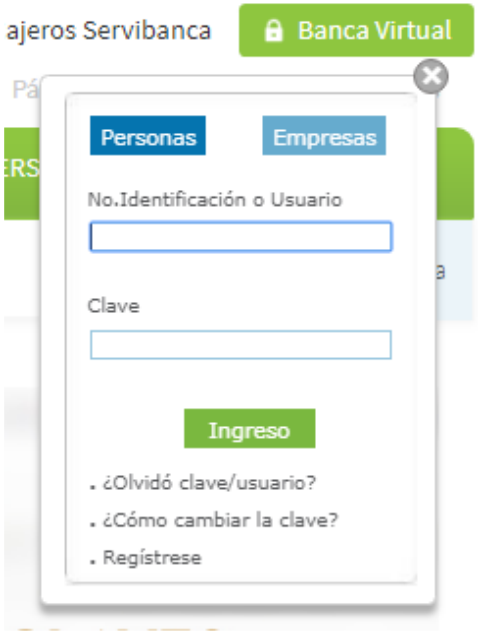


Figura 47. Pantalla Solicitud Nuevo Token

Se asegura que sea el mismo cliente que ingresó el que está aprobando la Solicitud del nuevo Token y vuelve a solicitar los datos del usuario:

Figura 48. Pantalla Solicitud Nuevo Token

Se traen los datos que se crearon inicialmente por la Base Única de Clientes (BUC), de cuando se creó el cliente por primera vez y si se modificó en otras oportunidades.

Si el cliente ha cambiado alguno de los datos, esta es la oportunidad de que los modifique para que el token llegue a su destino y asegurarse que sea recibido por el cliente. El manejo de esta base para el manejo de la información del cliente es importante debido a que cada actualización que se le realice al cliente por cambio de dirección de habitación, número de teléfono, contactos personales y laborales, siempre los realizan en este aplicativo, configurando así la base más actualizada y disponible para el apoyo de otros procesos dentro

del banco, como lo son los Token’s.

Figura 49. Pantalla Solicitud servicio de reposición

Proceso y Salidas: Finalmente, la Solicitud llega a la tabla: BBVD87 de Solicitudes de Token con toda la información para ser procesada. El estado de la solicitud nace en estado ‘P’ pendiente de procesar. Y comienza su trazabilidad hasta que el token sea entregado al cliente por el courrier.

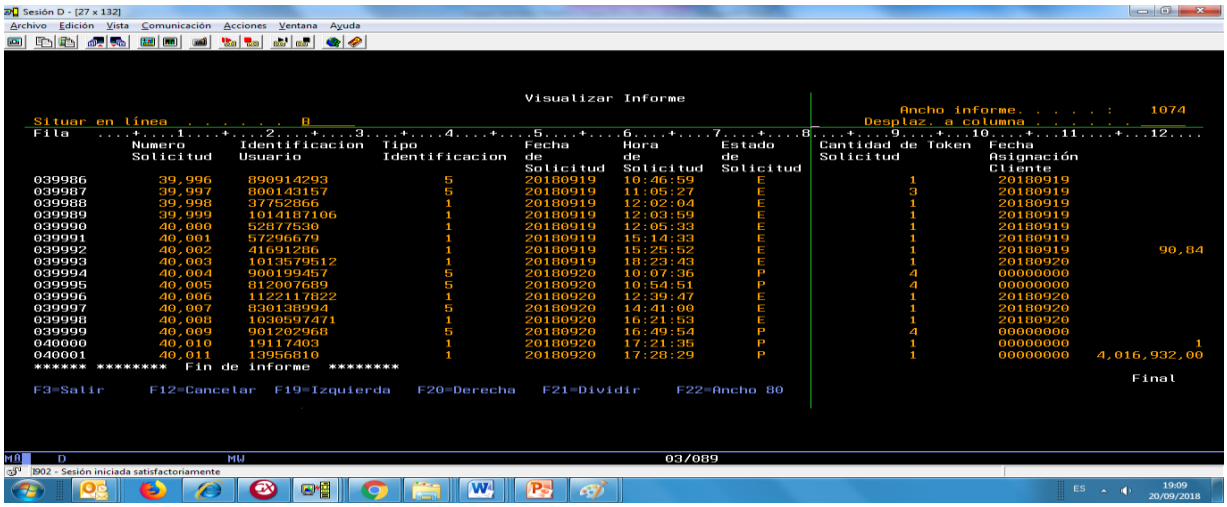


Figura 50. Tabla BBVD87 Información para ser procesada

4.5 Guía de auditoria Creación solicitud Tokens

AUDITORÍA SISTEMAS ADMINISTRACION DE TOKENS EN UN BANCO		
PROGRAMA DE AUDITORÍA		
DEPENDENCIA:	FECHA:	
PROCESO: Creación de solicitud de Tokens	ELABORADO	
PROCEDIMIENTO DE AUDITORÍA	REF. P/T	POR
OBJETIVOS: Evaluar todos los controles que se encuentran en las entradas, procesos y salidas del aplicativo para el proceso de creación de solicitud de token.		
NORMATIVA APLICABLE: Norma interna del Banco para la confidencialidad y trato de la información en la creación de la solicitud del token y norma interna de auditoria para el procesamiento de trato de la información en el ambiente productivo de la banca Virtual, al igual de la norma que solo se permite una solicitud de token activa.		
1. ENTRADA Y CAPTURA DE DATOS		
1.1 Verifique con el jefe de Tarjetas, que, en los últimos 10 correos enviados a éste por el DBA de la consola de VASCO, existe un único destinatario, nadie más en destinatario o con copia o copia oculta.		
1.2 Tome el ultimo archivo de semillas y constate que tiene extensión csv y que cumple con: Numero de campos establecido		

	Separador es “,”		
	1.3 Tome una muestra de 30 registro del archivo a cargar de semillas y verifique que cada registro tiene el número correcto de campos y que la información de cada campo contiene el formato esperado y a sea carácter, numérico o fecha.		
	1.4 Verifique el jefe de Tarjetas esté supervisado por el auditor y el experto de Sistemas para realizar el proceso de cargue de semillas, observe que el jefe de tarjetas se loguea en el servidor de aplicaciones exitosamente.		
	1.5 Observe que el jefe de tarjetas: Accede a la aplicación de tokens con usuario y contraseña en el servidor de aplicaciones Se registran los datos del usuario en la aplicación los cuales corresponden al log auditoría que se registrará en las acciones que realice el usuario en la aplicación. El usuario tiene activo el menú para cargues de semillas. Se presenta la ventana para cargue de semillas de Tokens. Selecciona el archivo de semillas a cargar.		
	2. PROCESAMIENTO		
	2.1 Cerciórese que el usuario realiza el proceso de cargue: Selecciona la opción de cargar el archivo Se inicia el proceso de validación y registro de semillas en el sistema el cual es informado mediante la ventana de estado de la ejecución.		
	2.2 Verifique que el proceso inicia a generar un		

archivo de log nuevo, en la ruta de log de procesos del servidor de aplicaciones, para la carpeta de Banca virtual, el cual se nombra con el prefijo de seedLoad, seguido de el la fecha y hora en que inició el proceso de cargue de semillas con el formato YYYYMMDDhhmmss.		
2.3 Verifique que durante el proceso la base de datos presenta actividad para el registro de las semillas.		
2.4 Observe que terminado el proceso de cargue la ventana de estado presenta el número de semillas registradas en el sistema y que concuerda con el número de registros en el archivo.		
2.5 Determine que, una vez terminado el procesamiento según lo informado por la aplicación, ya no existe actividad en la Base de Datos.		
3. SALIDAS QUE GENERA LA APLICACION		
3.1 Verifique el cargue de las semillas en la tabla BDOD14		
3.2 Verifique el registro de creación de las semillas en la tabla de log BDO16		
3.3 Verifique a través de la aplicación que se visualizan una muestra de 5 semillas de las recién cargadas con estado “N” Nuevo		
3.4 Verifique se registra en la contabilidad el cargue de las nuevas semillas de Tokens disponibles.		
3.5 Verifique el total de semillas cargadas en la última hora por el usuario administrador del jefe de tarjetas.		

4. PISTAS DE AUDITORIA		
4.1 Verifique el registro de creación de las semillas en la tabla de log BDO16 para las semillas que estaban contenidas en el archivo recién cargado		
4.2 Verifique que en la tabla de log BDOD16 cada Token nuevo del archivo se encuentra una única vez y que la secuencia de registro es 1.		
4.3 Verifique en el archivo de log para el proceso que no se presentó ninguna falla durante la ejecución del cargue de semillas.		
4.4 Verifique que se han registrado en la contabilidad el total se semillas que generan un costo para la banca.		
4.5 Verifique que se registra en la minuta de cargue de semillas el nombre del archivo cargado, cantidad de registro, veedores, fecha y hora, nombre y usuario que realiza el cargue.		

Prueba 1. Creación solicitud Tokens “Nueva solicitud por perdida o hurto”

Se toma una solicitud de token por pérdida, de las ingresadas por la página https://servicios.sudameris.com.co/Colombia9.2/servlet/hcolsolservtokenpers800, y se verifica en primera instancia la creación automática de la tabla (BBVD87), luego verificamos que la información registrada en todos los campos corresponda a la más actualizada que se puedan tomar, se verifica la última actualización de los datos personales en la última tabla del token asignado y se constata con la información de la BUC “Base única de clientes”.

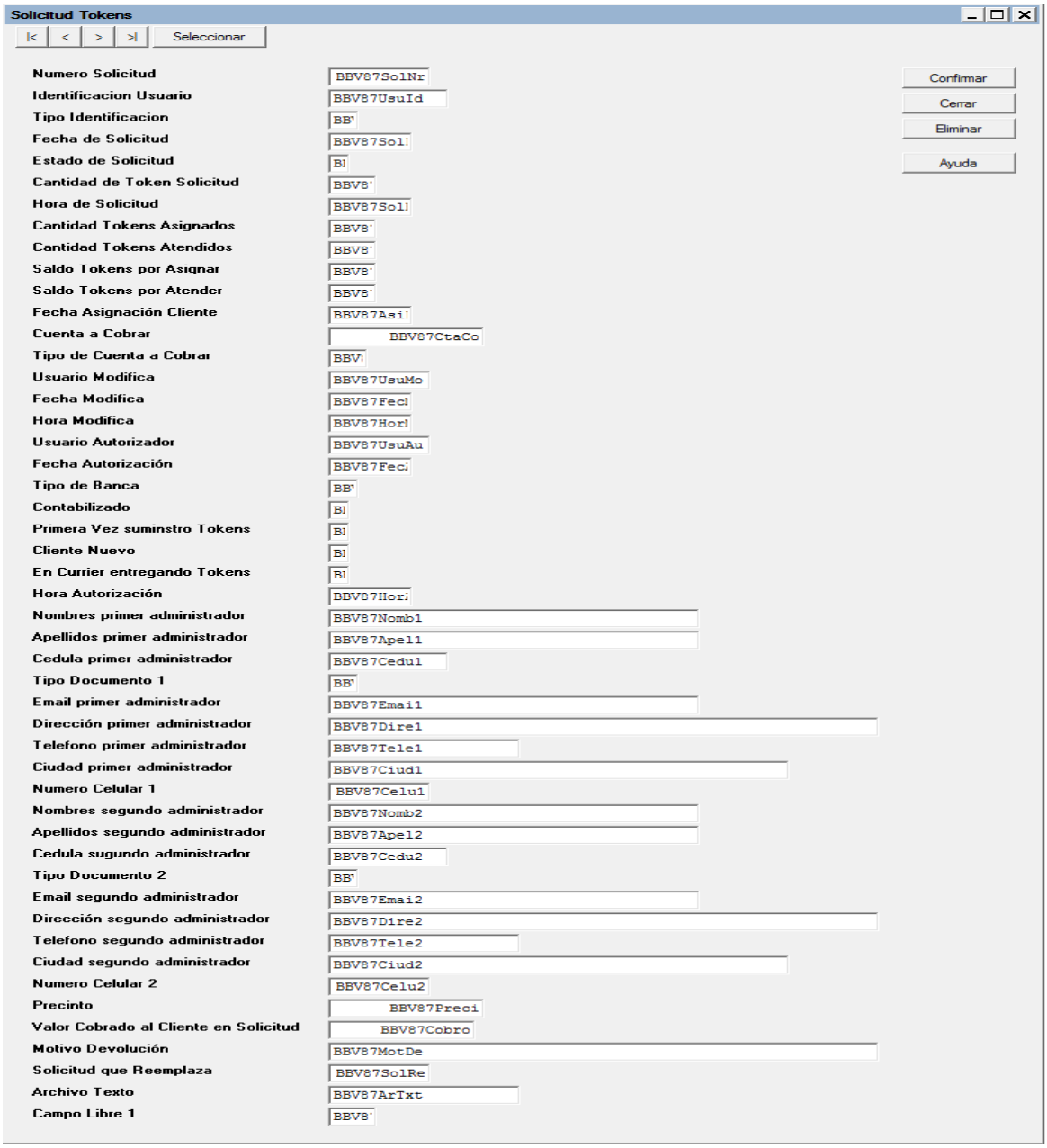


Figura 51. creación automática de la tabla (BBVD87)

Prueba 2. Creación solicitud Tokens “Nueva solicitud por daño”.

La prueba 2 en la creación de la solicitud de token, se realizó sobre el proceso una vez se entregó el token por parte del cliente en la oficina por daño en el físico, lo primero que se constata visualmente es el recibo del token actual y la suspensión en el aplicativo del mismo.

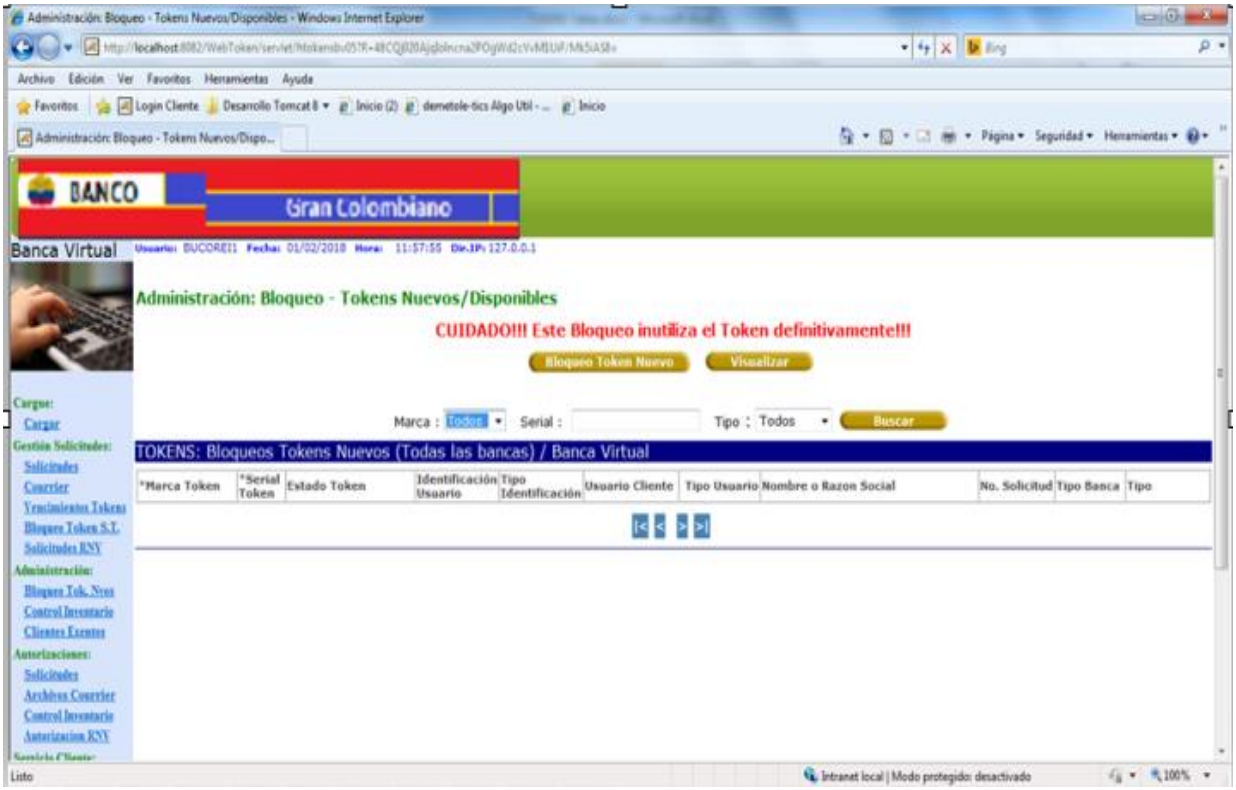


Figura 52. Pantalla administración bloqueo.

Luego se realiza la validación de la creación de la nueva tabla (BBVD87) en la que se valida que la información que está dentro de la tabla sea la más actualizada y que la banca virtual este suspendida por el cambio del token. Desde la Página de la Banca Virtual:

4.6 Asignación de los Tokens a la Solicitud. (Proceso número tres).

Luego de que se ha creado la Solicitud de Tokens por medio del ingreso del cliente a la Banca Virtuak, esta llega al área de Tarjetas en donde es gestionada por la encargada de gestión de las asignaciones de Tokens; el proceso comienza viendo en la bandeja de

Solicitudes las que estén en estado P, pendiente. Las solicitudes pueden venir de personas o de empresas. Cuando se crea el cliente en la banca Virtual, automáticamente se crea la Solicitud de Tokens puesto que la Banca necesita de Token obligatorio para ser usado por el cliente.

Entradas:

Creación de la Solicitud de Tokens nueva en estado P= Pendiente.

Figura 53. Creación solicitud de tokens.

Aparece la Solicitud en estado Pendiente y sin Tokens cargados, para este caso el Cliente que es de Personas solicitó un Token.

Figura 54. Creación solicitud de tokens.

El Cliente muestra toda la información del Pedido en donde debe estipular donde quiere

que se le entregue el Token. Dirección, teléfonos, ciudad, etc.

Para que el Courrier le haga el envío.

Pantalla para hacer el proceso desde donde parte la asignación de Tokens a la Solicitud.

Figura 55. Pantalla proceso inicial asignación Token

Inventario de Tokens disponible: Tabla BDOD14:

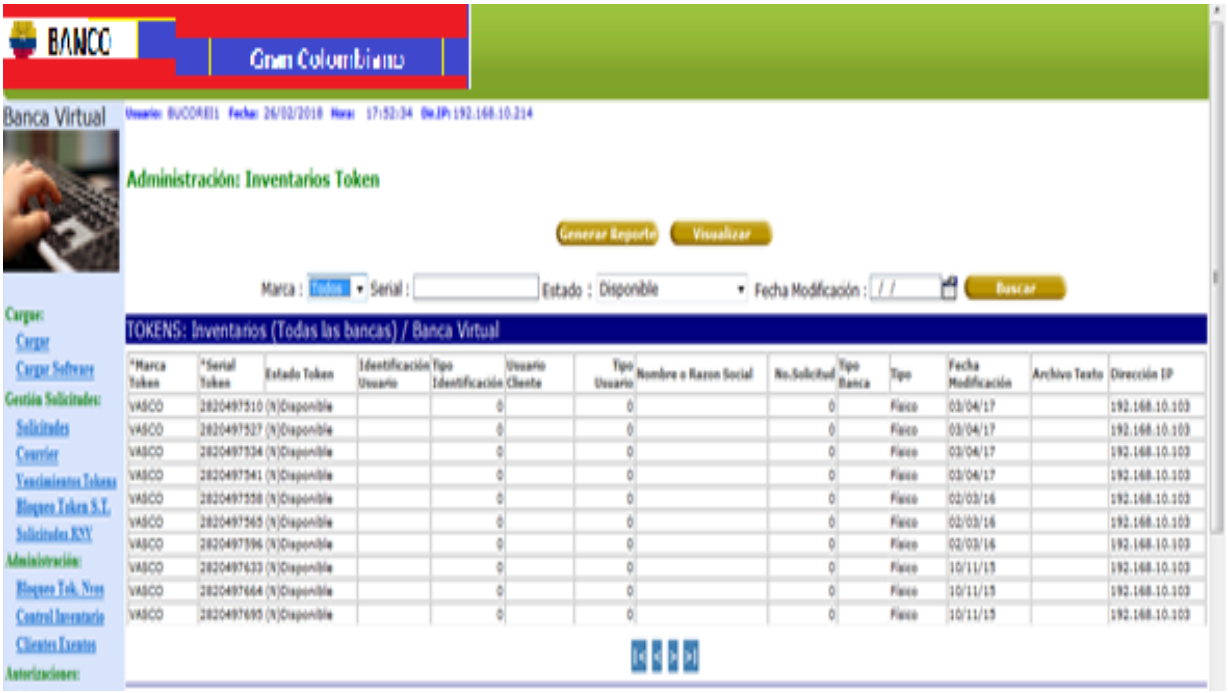


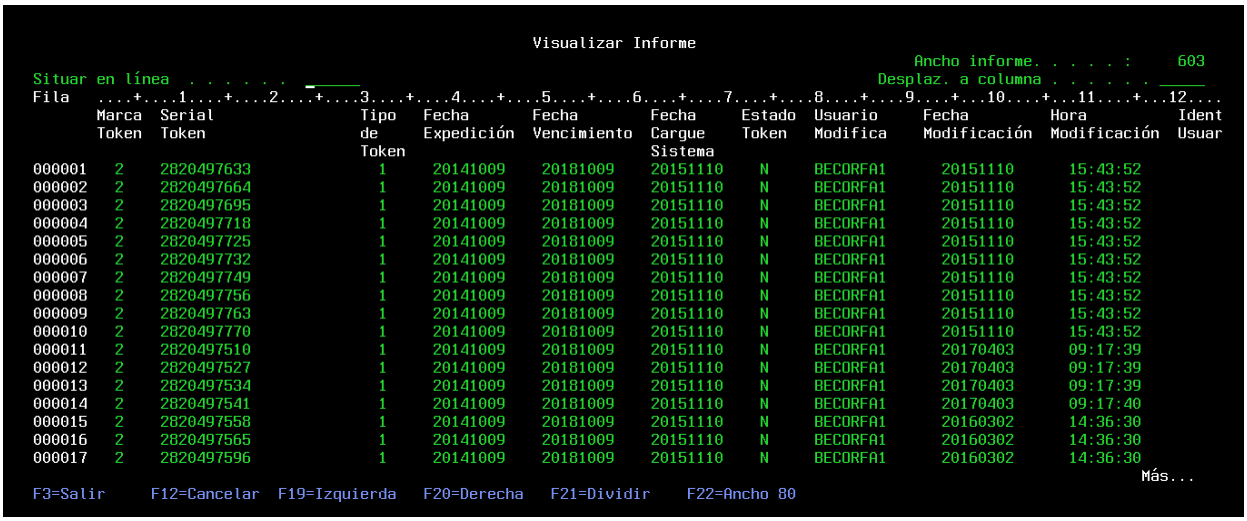
Figura 56. Inventario de Tokens disponible: Tabla BDOD14

Pantalla de Asignación individual de Tokens a la Solicitud:

Figura 57. Pantalla de Asignación individual de Tokens a la Solicitud

Inventario de Tokens: Tabla: BDOD14:

Figura 58. Inventario de Tokens: Tabla: BDOD14



Visualizar Informe

Ancho informe. . . . . : 603

Situar en línea . . . . . Desplaz. a columna . . . . .

Fila ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12....

	Marca Token	Serial Token	Tipo de Token	Fecha Expedición	Fecha Vencimiento	Fecha Cargue Sistema	Estado Token	Usuario Modifica	Fecha Modificación	Hora Modificación	Ident Usuar
000001	2	2820497633	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000002	2	2820497664	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000003	2	2820497695	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000004	2	2820497718	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000005	2	2820497725	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000006	2	2820497732	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000007	2	2820497749	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000008	2	2820497756	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000009	2	2820497763	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000010	2	2820497770	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000011	2	2820497510	1	20141009	20181009	20151110	N	BECORFA1	20170403	09:17:39	
000012	2	2820497527	1	20141009	20181009	20151110	N	BECORFA1	20170403	09:17:39	
000013	2	2820497534	1	20141009	20181009	20151110	N	BECORFA1	20170403	09:17:39	
000014	2	2820497541	1	20141009	20181009	20151110	N	BECORFA1	20170403	09:17:40	
000015	2	2820497558	1	20141009	20181009	20151110	N	BECORFA1	20160302	14:36:30	
000016	2	2820497565	1	20141009	20181009	20151110	N	BECORFA1	20160302	14:36:30	
000017	2	2820497596	1	20141009	20181009	20151110	N	BECORFA1	20160302	14:36:30	

Más...

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80

Figura 59. Rutinas de Tratamiento especial

RTE Rutinas de Tratamiento especial. Estas son como los Trigers que se corren dentro de la Parametrización al correr los programas y que llenan datos en otras tablas.

Proceso:

El usuario con perfil de Gestor de la Aplicación. Aplica la asignación de Tokens por la pantalla siguiente, con el botón asignar:

Figura 60. Pantalla asignación de Tokens – Usuario -

El Proceso lo que hace es ir a la tabla BDOD14, ordenarla por el Nro. del Serial y extraer

el serial que se va a asignar a la Solicitud. antes evalúa que el Cliente no tenga más seriales asignados y en funcionamiento, porque el cliente de personas solo puede tener un Token nada más, igual la consola que administra las semillas lógicas solo puede tener un token para cada identificación. El proceso consiste en realidad en marcar la semilla en el inventario **BDOD14** con la identificación en el campo: **BDO14USUID** y el tipo de identificación en el campo **BDO14TPIDC**. Además hay que cambiar el estado de 'N'=Nuevo a 'X'=Asignado y por autorizar. Debe también registrarse el log de modificación en los campos. De Usuario, Fecha, y hora. Debe registrarse también la fecha de asignación de Token.

Visualizar Informe

Ancho informe. . . . . : 603
Situar en línea 8
Desplaz. a columna . . . . . _____

Fila ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12....

	Marca Token	Serial Token	Tipo de Token	Fecha Expedición	Fecha Vencimiento	Fecha Cargue Sistema	Estado Token	Usuario Modifica	Fecha Modificación	Hora Modificación	Ident Usuar
094548	2	3560658568	1	20160805	20200805	20160812	E	MSL	20180221	16:18:59	9000
094549	2	3560658575	1	20160805	20200805	20160812	A	BECRUDO1	20180226	13:35:02	5204
094550	2	3560658582	1	20160805	20200805	20160812	E	MSL	20180222	16:02:40	6758
094551	2	3560658599	1	20160805	20200805	20160812	A	BECRUDO1	20180227	15:11:36	5164
094552	2	3560658605	1	20160805	20200805	20160812	A	BECRUDO1	20180227	15:23:36	1934
094553	2	3560658612	1	20160805	20200805	20160812	E	MSL	20180222	16:02:27	1010
094554	2	3560658629	1	20160805	20200805	20160812	E	MSL	20180222	16:02:34	1009
094555	2	3560658636	1	20160805	20200805	20160812	A	BECRUDO1	20180226	13:37:41	D121
094556	2	3560658643	1	20160805	20200805	20160812	E	MSL	20180222	16:02:52	4207
094557	2	3560658650	1	20160805	20200805	20160812	E	MSL	20180222	16:03:05	7765
094558	2	3560658667	1	20160805	20200805	20160812	E	MSL	20180222	16:01:58	9004
094559	2	3560658674	1	20160805	20200805	20160812	E	MSL	20180222	16:01:58	9004
094560	2	3560658681	1	20160805	20200805	20160812	E	MSL	20180222	16:01:58	9004
094561	2	3560658698	1	20160805	20200805	20160812	E	MSL	20180222	16:01:58	9004
094562	2	3560658704	1	20160805	20200805	20160812	L	BERUIMA1	20180227	11:22:31	8020
094563	2	3560658711	1	20160805	20200805	20160812	L	BERUIMA1	20180227	11:22:31	8020
094564	2	3560658728	1	20160805	20200805	20160812	L	BERUIMA1	20180227	11:22:31	8020

Más...

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80

Visualizar Informe

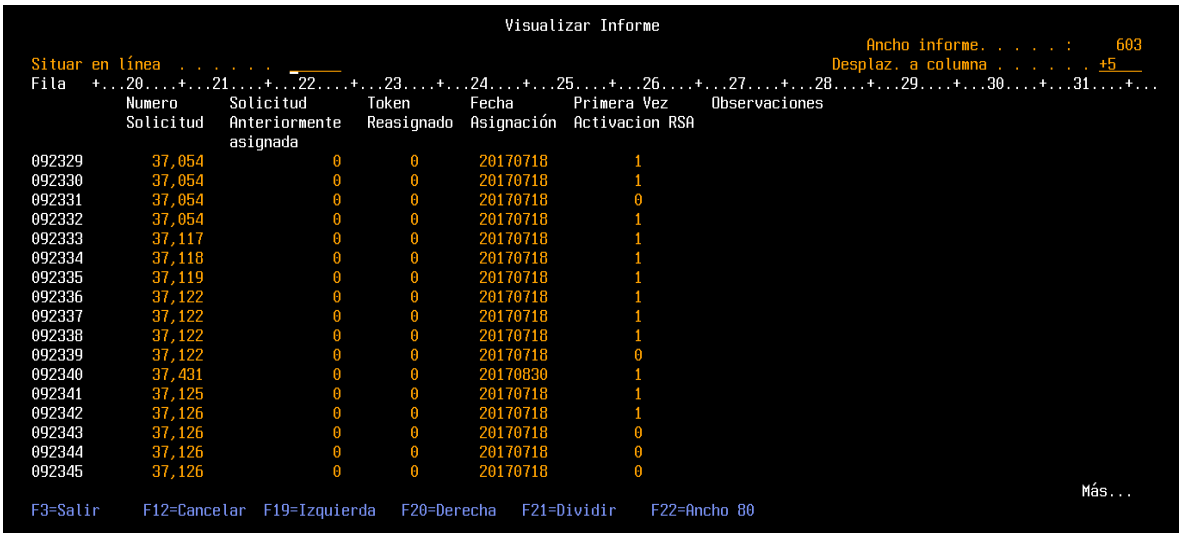
Ancho informe. . . . . : 603
Situar en línea . . . . . _____
Desplaz. a columna . . . . . +5

Fila ....+....8....+....9....+...10....+...11....+...12....+...13....+...14....+...15....+...16....+...17....+...18....+...19....

	Estado Token	Usuario Modifica	Fecha Modificación	Hora Modificación	Identificación Usuario	Tipo Identificación	Usuario Cliente	Tipo Usuario	Fecha Ultimo Ingreso	Intentos Fallidos
092329	A	ADMINIST1	20171128	11:41:33	830019543	5	ADMINIST1	1	00000000	0
092330	A	ADMINIST2	20171128	11:42:59	830019543	5	ADMINIST2	1	00000000	0
092331	B	ADMINIST1	20170802	08:55:50	830019543	5		0	00000000	0
092332	A	TESORERIA	20180227	16:31:52	830019543	5	TESORERIA	1	00000000	0
092333	A	80243671	20180222	09:09:00	80243671	1	80243671	1	00000000	0
092334	A	71702235	20180216	17:55:23	71702235	1	71702235	1	00000000	0
092335	A	1050954656	20180227	14:16:26	1050954656	1	1050954656	1	00000000	0
092336	A	ADMINIST1	20180212	09:20:33	900666467	5	ADMINIST1	1	00000000	0
092337	A	ADMINIST2	20180212	08:28:27	900666467	5	ADMINIST2	1	00000000	0
092338	A	ALTO	20180227	06:14:56	900666467	5	ALTO	1	00000000	0
092339	L	BERUIMA1	20170724	09:10:24	900666467	5		0	00000000	0
092340	A	423222	20180219	16:40:59	423222	3	423222	3	00000000	0
092341	A	79103167	20170822	21:14:38	79103167	1	79103167	1	00000000	0
092342	A	CONLNATAGA	20180213	08:09:15	800142383	5	CONLNATAGAR	1	00000000	0
092343	L	BERUIMA1	20170726	11:12:00	800142383	5		0	00000000	0
092344	L	BERUIMA1	20170726	11:12:00	800142383	5		0	00000000	0
092345	L	BERUIMA1	20170726	11:12:00	800142383	5		0	00000000	0

Más...

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80



Visualizar Informe

Ancho informe. . . . . : 603

Situar en línea . . . . . _____ Desplaz. a columna . . . . . +5___

Fila +...20....+...21....+...22....+...23....+...24....+...25....+...26....+...27....+...28....+...29....+...30....+...31....+...

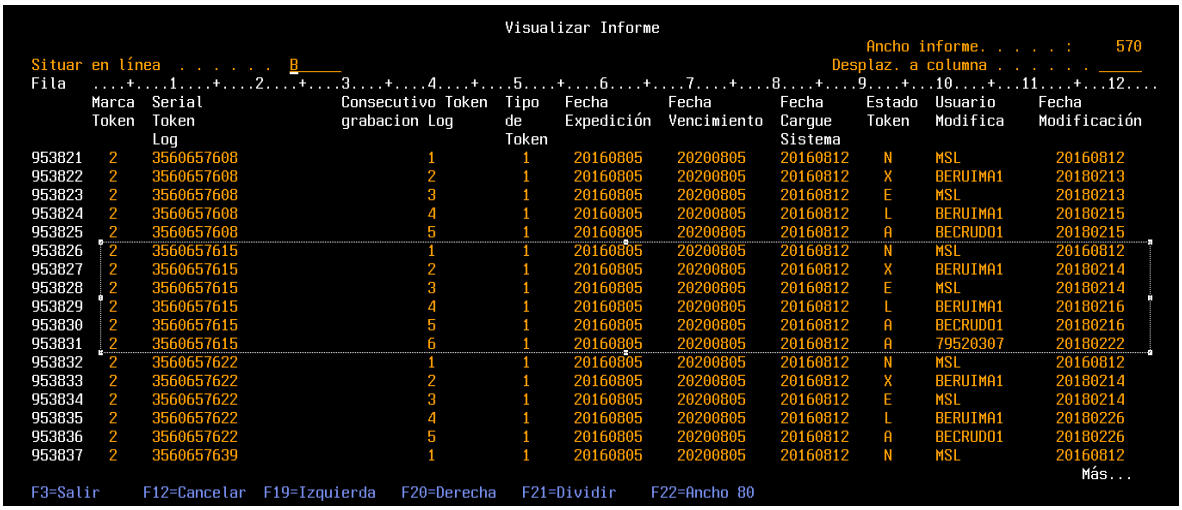
	Numero Solicitud	Solicitud Anteriormente asignada	Token Reasignado	Fecha Asignación	Primera Vez Activacion RSA	Observaciones
092329	37,054	0	0	20170718	1	
092330	37,054	0	0	20170718	1	
092331	37,054	0	0	20170718	0	
092332	37,054	0	0	20170718	1	
092333	37,117	0	0	20170718	1	
092334	37,118	0	0	20170718	1	
092335	37,119	0	0	20170718	1	
092336	37,122	0	0	20170718	1	
092337	37,122	0	0	20170718	1	
092338	37,122	0	0	20170718	1	
092339	37,122	0	0	20170718	0	
092340	37,431	0	0	20170830	1	
092341	37,125	0	0	20170718	1	
092342	37,126	0	0	20170718	1	
092343	37,126	0	0	20170718	0	
092344	37,126	0	0	20170718	0	
092345	37,126	0	0	20170718	0	

Más...

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80

Figura 61. Pantallas proceso de marcación de semilla

Se registra también en el Log de Tokens Tabla: **BDOD16** el registro que guarda la trazabilidad del Token a medida que va siendo afectado se guardan los momentos en los cuales se afectó y lo que sucedió en él.



Visualizar Informe

Ancho informe. . . . . : 570

Situar en línea . . . . . 8_____ Desplaz. a columna . . . . . _____

Fila ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12....

	Marca Token	Serial Token Log	Consecutivo Token grabacion Log	Tipo de Token	Fecha Expedición	Fecha Vencimiento	Fecha Cargue Sistema	Estado Token	Usuario Modifica	Fecha Modificación
953821	2	3560657608	1	1	20160805	20200805	20160812	N	MSL	20160812
953822	2	3560657608	2	1	20160805	20200805	20160812	X	BERUIMA1	20180213
953823	2	3560657608	3	1	20160805	20200805	20160812	E	MSL	20180213
953824	2	3560657608	4	1	20160805	20200805	20160812	L	BERUIMA1	20180215
953825	2	3560657608	5	1	20160805	20200805	20160812	A	BECRUDO1	20180215
953826	2	3560657615	1	1	20160805	20200805	20160812	N	MSL	20160812
953827	2	3560657615	2	1	20160805	20200805	20160812	X	BERUIMA1	20180214
953828	2	3560657615	3	1	20160805	20200805	20160812	E	MSL	20180214
953829	2	3560657615	4	1	20160805	20200805	20160812	L	BERUIMA1	20180216
953830	2	3560657615	5	1	20160805	20200805	20160812	A	BECRUDO1	20180216
953831	2	3560657615	6	1	20160805	20200805	20160812	A	79520307	20180222
953832	2	3560657622	1	1	20160805	20200805	20160812	N	MSL	20160812
953833	2	3560657622	2	1	20160805	20200805	20160812	X	BERUIMA1	20180214
953834	2	3560657622	3	1	20160805	20200805	20160812	E	MSL	20180214
953835	2	3560657622	4	1	20160805	20200805	20160812	L	BERUIMA1	20180226
953836	2	3560657622	5	1	20160805	20200805	20160812	A	BECRUDO1	20180226
953837	2	3560657639	1	1	20160805	20200805	20160812	N	MSL	20160812

Más...

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80

Figura 62. Log de Tokens Tabla: BDOD16

Salidas:

Aquí, el registro del Token queda listo a ser Autorizado por el área correspondiente (**BDOD14**) en estado '**X'**. y se muestra en una bandeja nueva que solo van a ver los autorizadores.

La otra salida es que el archivo de Log **BDOD16** quede adicionado un registro con el

cambio de estado de Token y quede con toda la historia del mismo.

Visualizar Informe

Ancho informe. . . . . : 603

Situar en línea . . . . . Desplaz. a columna . . . . .

Fila ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12....

	Marca Token	Serial Token	Tipo de Token	Fecha Expedición	Fecha Vencimiento	Fecha Cargue Sistema	Estado Token	Usuario Modifica	Fecha Modificación	Hora Modificación	Ident Usuar
000001	2	2820498470	1	20141009	20181009	20151110	X	GB1	20171031	15:33:00	8001

****** ******** Fin de informe ********

Figura 63. Registro con el cambio de estado de Token

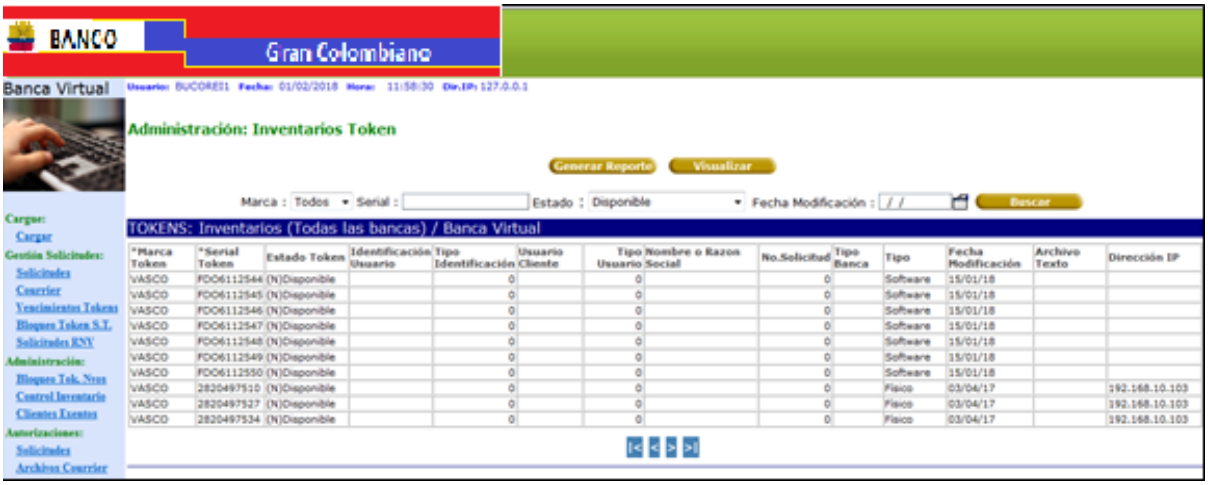
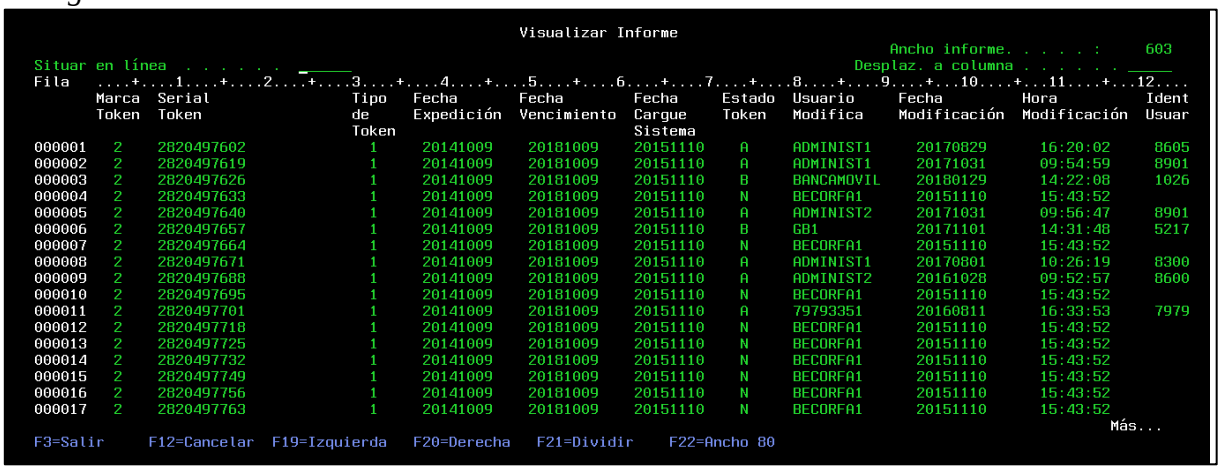


Figura 64. Consulta a la tabla de la base de datos DB2



Visualizar Informe

Ancho informe. . . . . : 603

Situar en línea . . . . . Desplaz. a columna . . . . .

Fila ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12....

	Marca Token	Serial Token	Tipo de Token	Fecha Expedición	Fecha Vencimiento	Fecha Cargue Sistema	Estado Token	Usuario Modifica	Fecha Modificación	Hora Modificación	Ident Usuar
000001	2	2820497602	1	20141009	20181009	20151110	A	ADMINIST1	20170829	16:20:02	8605
000002	2	2820497619	1	20141009	20181009	20151110	A	ADMINIST1	20171031	09:54:59	8901
000003	2	2820497626	1	20141009	20181009	20151110	B	BANCAMOVIL	20180129	14:22:08	1026
000004	2	2820497633	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000005	2	2820497640	1	20141009	20181009	20151110	A	ADMINIST2	20171031	09:56:47	8901
000006	2	2820497657	1	20141009	20181009	20151110	B	GB1	20171101	14:31:48	5217
000007	2	2820497664	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000008	2	2820497671	1	20141009	20181009	20151110	A	ADMINIST1	20170801	10:26:19	8300
000009	2	2820497688	1	20141009	20181009	20151110	A	ADMINIST2	20161028	09:52:57	8600
000010	2	2820497695	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000011	2	2820497701	1	20141009	20181009	20151110	A	79793351	20160811	16:33:53	7979
000012	2	2820497718	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000013	2	2820497725	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000014	2	2820497732	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000015	2	2820497749	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000016	2	2820497756	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000017	2	2820497763	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	

Más...

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80

4.7 Guía de auditoria Asignación de Token a la Solicitud.

AUDITORÍA SISTEMAS ADMINISTRACION DE TOKENS EN UN BANCO		
PROGRAMA DE AUDITORÍA		
DEPENDENCIA:	FECHA:	
PROCESO: Asignación de Token a la Solicitud	ELABORADO	
PROCEDIMIENTO DE AUDITORÍA	REF. P/T	POR
OBJETIVOS: Evaluación de todos los controles que se encuentran en las entradas, procesos y salidas del aplicativo para el proceso de Asignación de Token a la Solicitud.		
NORMATIVA APLICABLE: Norma aplicada, Un usuario de Personas en el Banco solo puede tener Activo un solo Token. El Token que se le asigne debe ser una semilla nueva.		
1. ENTRADA Y CAPTURA DE DATOS		
1.1 Verifíquese que el Cliente no tiene ningún Token asignado.		
1.2 Verificar que en el inventario de semillas o Tokens hay Tokens en estado N=Nuevo.		
1.3 El usuario que hace la asignación de la semilla a la Solicitud es un usuario de Gestión.		
1.4 Las Solicitudes se atienden una por una.		
1.5 Observe que el registro en la Solitud hará		

cambio en la asignación de la Solitud de la siguiente manera: Asigna cambio de Usuario, Fecha y hora de modificación de cada registro. Se cambia el estado de la Solicitud de Nuevo a X Por autorizar. El estado debe quedar para que los Autorizadores, usuarios Administradores aprueban la gestión para continuar con el proceso de envío al cliente a través del courrier.. Se prepara la bandeja para realizar la operación de asignación.		
2. PROCESAMIENTO		
2.1. El Usuario Gestor: Ingresa a la aplicación con usuario y contraseña del AS400. Si fue registrado en el aplicativo como gestor, el menú le enciende la opción de Solicitudes en el área de Gestión de Solicitudes.		
2.2. Si hay Solicitudes en estado P=Pendiente, salen en esta pantalla para ser gestionadas..		
2.3. Se usa la pantalla hTokensBV02 para hacer el cargue.		

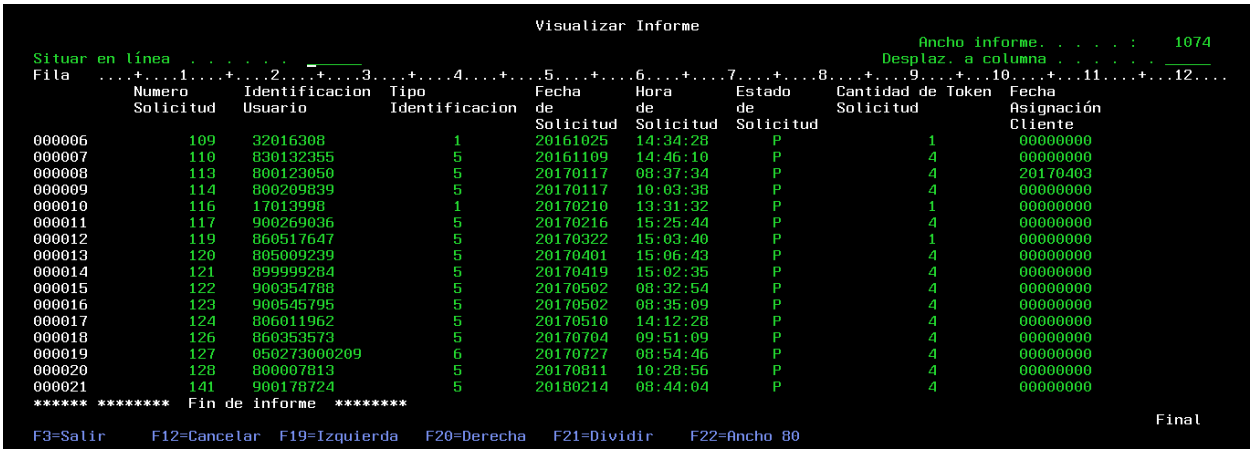
2.4. La pantalla muestra principalmente las columnas Nro de Solicitud, Id.Usuario, Tipo cliente, Fecha solicitud, Q Cantidad de tokens de la solicitud, Estado, Nombre cliente.		
2.5 Se presiona el botón de arriba que dice Asignar.		
2.6. Sale una nueva pantalla a través de la cual se puede asignar la solicitud ya sea manualmente o automáticamente. Si es manual, se puede asignar un número de Token especial, el que se quiera. Si es automático, el sistema ordena por números de Serial y asigna el que sigue.		
2.7. Hace las marcaciones respectivas tanto en la Solicitud como en el Inventario de Tokens.		
2.8. Hace el registro en el Log Tabla BDOD66, registrando el cambio que sufrió la solicitud.		
3. SALIDAS QUE GENERA LA APLICACIÓN		
3.1 Se verifica que el registro que estaba pendiente por asignar desaparece la pantalla de pendientes.		
3.2 Se verifica que le aparezca a los autorizadores para continuar el proceso.		

3.3. Se revisa con un Qry en el As400 que los cambios se hayan efectuados tanto en la BDOD14 como en la BDOD16.		
3.4. se verifica la contabilidad para ver el asiento de descargue del inventario.		
4. PISTAS DE AUDITORIA		
4.1. Grabación en las 2 tablas de Usuario, Fecha y hora de modificación.		
4.2 Graba Log de Auditoria en la tabla BDOD16. Deberían quedar 2 registros. El primero es cuando se cargaron las semillas en estado N=Nuevo y el segundo es el de esta asignación que es el registro de paso de Token a estado X=Asignado y Listo a ser aprobado.		
4.3. Se graba en el Token escogido la Fecha de asignación. El usuario que asignó, y la hora, etc.		
4.4. Se descarga del inventario el Token que se ha asignado haciendo los asientos de contabilidad respectivos.		

Diseño y Ejecución de Pruebas.

Prueba 1. Diseño. Asignación de Token a la solicitud

Se toma una Solicitud de Tokens que haya ingresado ya sea por la Banca Virtual o por la pantalla donde se recibe un Token que viene por Servicio Técnico. Hay varias:



Visualizar Informe

Ancho informe. . . . . : 1074
Situar en línea . . . . . _____ Desplaz. a columna . . . . . ____
Fila ...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12...

	Numero Solicitud	Identificacion Usuario	Tipo Identificacion	Fecha de Solicitud	Hora de Solicitud	Estado de Solicitud	Cantidad de Token Solicitud	Fecha Asignación Cliente
000006	109	32016308	1	20161025	14:34:28	P	1	00000000
000007	110	830132355	5	20161109	14:46:10	P	4	00000000
000008	113	800123050	5	20170117	08:37:34	P	4	20170403
000009	114	800209839	5	20170117	10:03:38	P	4	00000000
000010	116	17013998	1	20170210	13:31:32	P	1	00000000
000011	117	900269036	5	20170216	15:25:44	P	4	00000000
000012	119	860517647	5	20170322	15:03:40	P	1	00000000
000013	120	805009239	5	20170401	15:06:43	P	4	00000000
000014	121	899999284	5	20170419	15:02:35	P	4	00000000
000015	122	900354788	5	20170502	08:32:54	P	4	00000000
000016	123	900545795	5	20170502	08:35:09	P	4	00000000
000017	124	806011962	5	20170510	14:12:28	P	4	00000000
000018	126	860353573	5	20170704	09:51:09	P	4	00000000
000019	127	050273000209	6	20170727	08:54:46	P	4	00000000
000020	128	800007813	5	20170811	10:28:56	P	4	00000000
000021	141	900178724	5	20180214	08:44:04	P	4	00000000

****** ******** Fin de informe ********

Final

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80

Figura 65. Prueba 1 Diseño, Pantalla Solicitud de Token – Servicios Técnico

Figura 66. Pantalla Solicitud de Token – Banca virtual

Se hace la asignación del Token a la Solitud y se verifica que el proceso haya quedado muy bien. Se revisa posteriormente termine el proceso que las tablas y pantallas hayan registrado bien los cambios que se han comentado en el procesamiento, las salidas y las pistas

de auditoría.

Prueba 2. Diseño. Asignación de Token a la solicitud. Parte de Desasignación de Tokens.

La prueba número 2 puede ser hacer la desasignación del Token a la Solitud, descargar el Token es parte de la asignación. Seria desmarcarlo luego de ser asignado y volverlo al inventario. Y esto se puede hacer como un reverso del paso de asignación de Token.

Se hará por esta misma pantalla:

Figura 67. Prueba 2, Diseño Proceso de desasignación

Y se presiona botón Asignar:

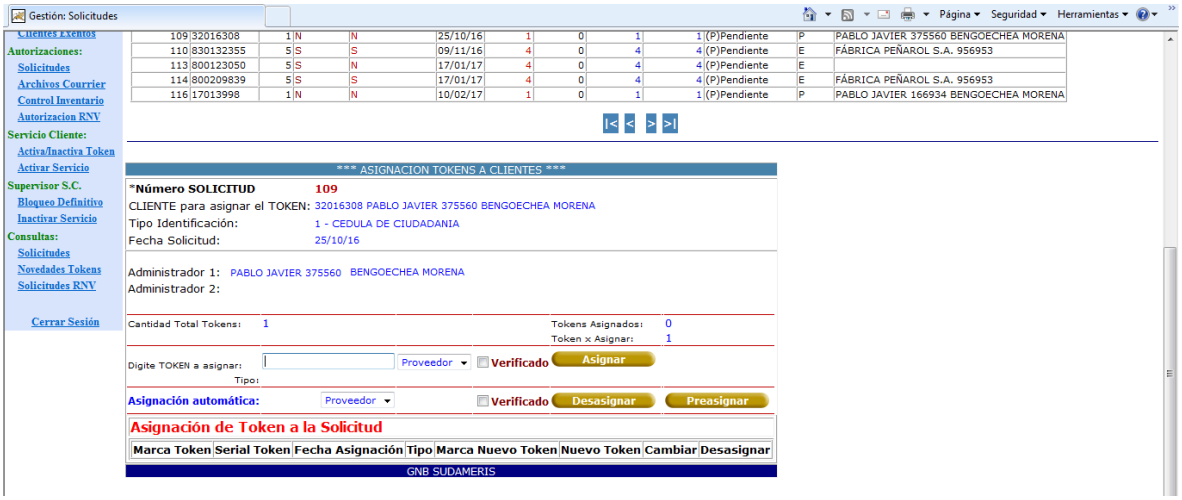


Figura 68. Proceso de desasignación 2

Y aquí luego de asignar se hace la devolución por el botón de Desasignar.

Prueba 3. Asignación manual de Token a la Solicitud. Esta Prueba consiste en asignar manualmente a la Solicitud el Serial que a gusto se quiera, o sea un Token es especial por alguna razón justificada.

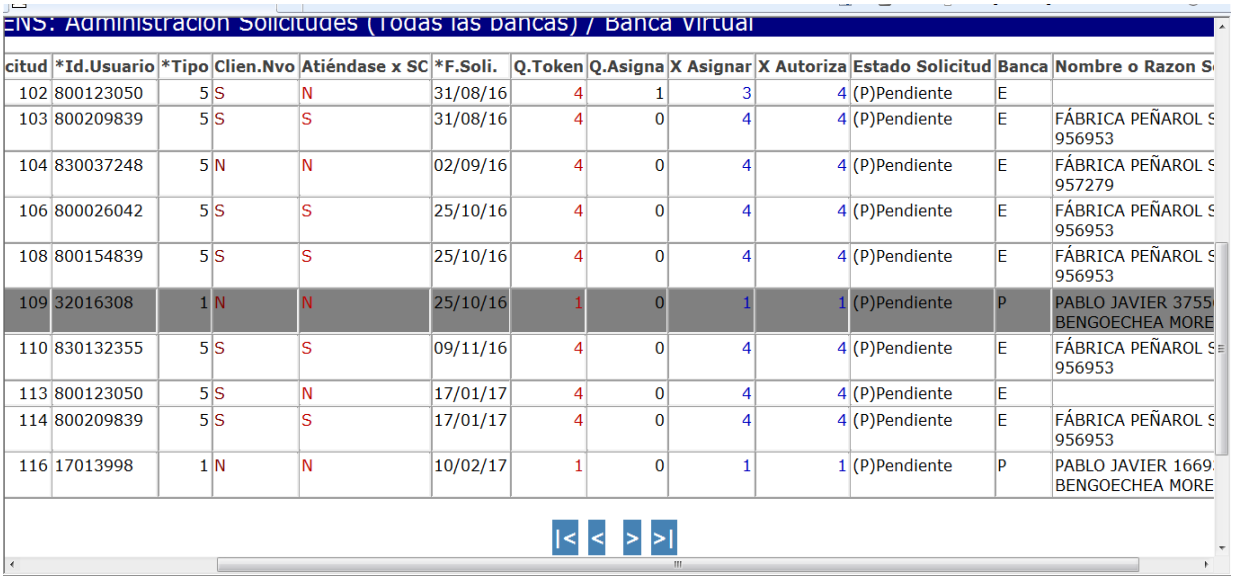
Se hace manualmente colocando el Nro. de Serial en la casilla a la izquierda del Botón **Asignar**, donde dice '**Digite TOKEN a asignar:**' se debe elegir el proveedor del Token **RSA** ó **Vasco**. Existe un control para todas las asignaciones que dice Cantidad Total de Tokens, Tokens asignados y Tokens x Asignar.

Ejecución de la Prueba 1. Asignación de Token a la Solicitud.

Se hace Logueo en el Sistema con Usuario: BUCOREI1. Se ubica la solicitud N- 109

Figura 69. Prueba 1, ejecución Asignación token a la solicitud

Figura 70. Módulo de administración de tokens – Gestión solicitudes



ENS: Administración Solicitudes (Todas las bancas) / Banca Virtual

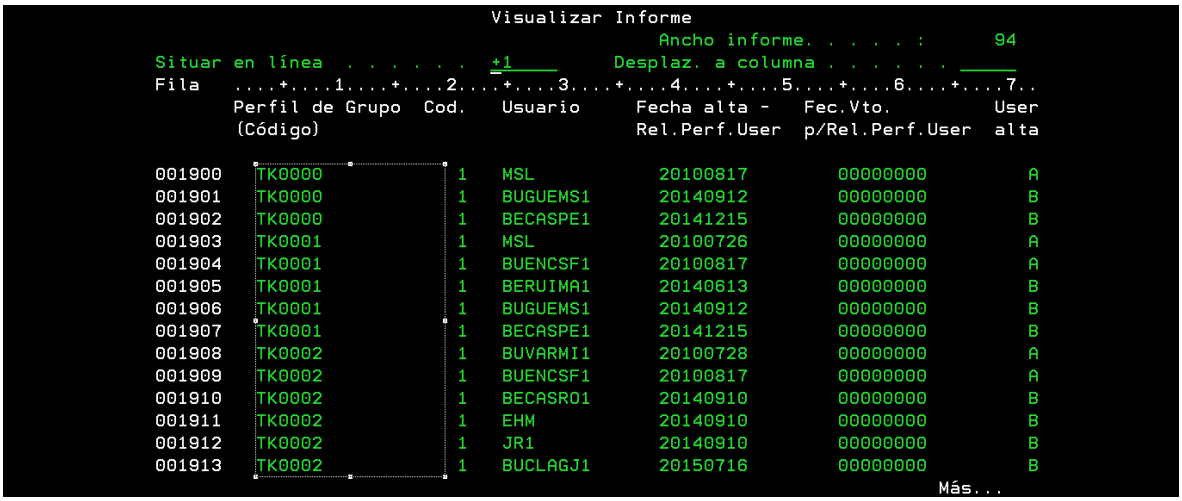
citud	*Id.Usuario	*Tipo	Clien.Nvo	Atiéndase x SC	*F.Soli.	Q.Token	Q.Asigna	X Asignar	X Autoriza	Estado Solicitud	Banca	Nombre o Razon S
102	800123050	5	S	N	31/08/16	4	1	3	4	(P)Pendiente	E	
103	800209839	5	S	S	31/08/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S 956953
104	830037248	5	N	N	02/09/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S 957279
106	800026042	5	S	S	25/10/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S 956953
108	800154839	5	S	S	25/10/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S 956953
109	32016308	1	N	N	25/10/16	1	0	1	1	(P)Pendiente	P	PABLO JAVIER 3755 BENGOECHEA MORE
110	830132355	5	S	S	09/11/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S 956953
113	800123050	5	S	N	17/01/17	4	0	4	4	(P)Pendiente	E	
114	800209839	5	S	S	17/01/17	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S 956953
116	17013998	1	N	N	10/02/17	1	0	1	1	(P)Pendiente	P	PABLO JAVIER 1669 BENGOECHEA MORE

Figura 71. Modulo de administración de tokens – Gestión solicitudes 2

Se hace marca presionando click encima de registro, esto marca la línea en gris, esto quiere decir que esa es la Solicitud, la 109 es la que se va a procesar.

Figura 72. Módulo de administración de tokens – Gestión solicitudes 3

Perfiles de la aplicación para el ingreso y gestión:



Visualizar Informe

Ancho informe. . . . . : 94

Situar en línea . . . . . +1 Desplaz. a columna . . . . . _____

Fila ....+....1....+....2....+....3....+....4....+....5....+....6....+....7..

	Perfil de Grupo (Código)	Cod.	Usuario	Fecha alta - Rel.Perf.User	Fec.Vto. p/Rel.Perf.User	User alta
001900	TK0000	1	MSL	20100817	00000000	A
001901	TK0000	1	BUGUEMS1	20140912	00000000	B
001902	TK0000	1	BECASPE1	20141215	00000000	B
001903	TK0001	1	MSL	20100726	00000000	A
001904	TK0001	1	BUENCSF1	20100817	00000000	A
001905	TK0001	1	BERUIMA1	20140613	00000000	B
001906	TK0001	1	BUGUEMS1	20140912	00000000	B
001907	TK0001	1	BECASPE1	20141215	00000000	B
001908	TK0002	1	BUVARMI1	20100728	00000000	A
001909	TK0002	1	BUENCSF1	20100817	00000000	A
001910	TK0002	1	BECASRO1	20140910	00000000	B
001911	TK0002	1	EHM	20140910	00000000	B
001912	TK0002	1	JR1	20140910	00000000	B
001913	TK0002	1	BUCLAGJ1	20150716	00000000	B

Más...

Figura 73. Perfiles de la aplicación para el ingreso y gestión

Se presiona el Botón Asignar en la aplicación: y se cae en la pantalla siguiente:

Figura 74. Vista de la solicitud 109

Se ve aquí la Información de la Solicitud Nro. **109**.

Se presiona el Botón de PreAsignar pero antes se marca la casilla de verificado para asegurar, el botón de Asignar es para colocar el nro. del Token a mano y asignar el serial

que el gestor quiera y no el que le proponga el orden del consecutivo por serial.

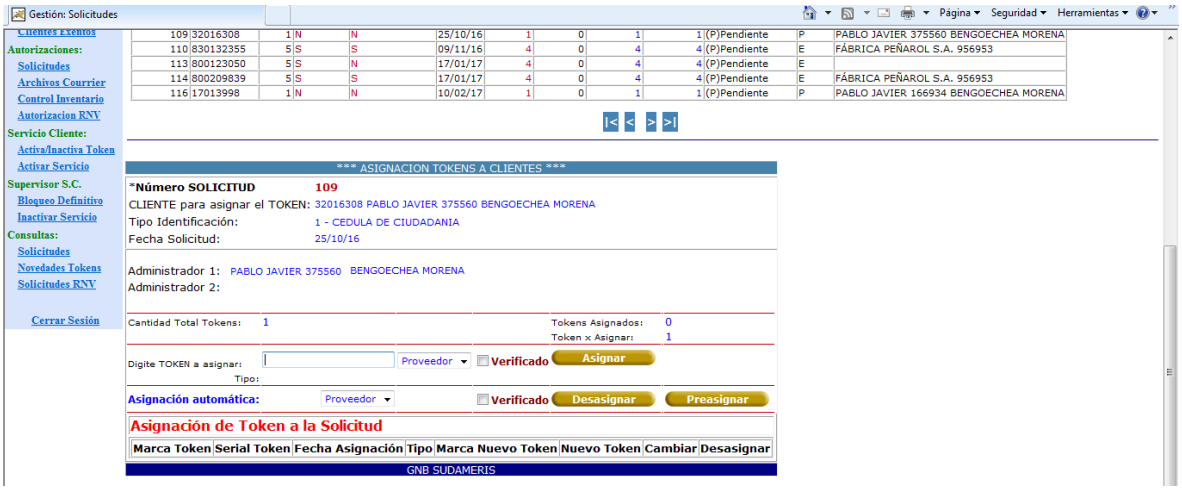


Figura 75. Numero de token y asignación de serial

Se elige el Proveedor Vasco y se marca la casilla de verificado presionando el Botón Preasignar:

Figura 76. Asignación de serial al Token - preasignar

Se acaba de asignar el Serial de Token Nro. **2820497510** a la Solicitud

Efectivamente se hacen las asignaciones de la cantidad de Tokens que necesita la

Solicitud, en este caso 1 solo Token quedó asignado.

Vamos a revisar el Token Nro. **2820497510** en el Inventario con un Qry:

Se asignaron aquí el Cliente que queda matriculado a ese Token y los logs de control:

Y la Solicitud paso a estado X también.

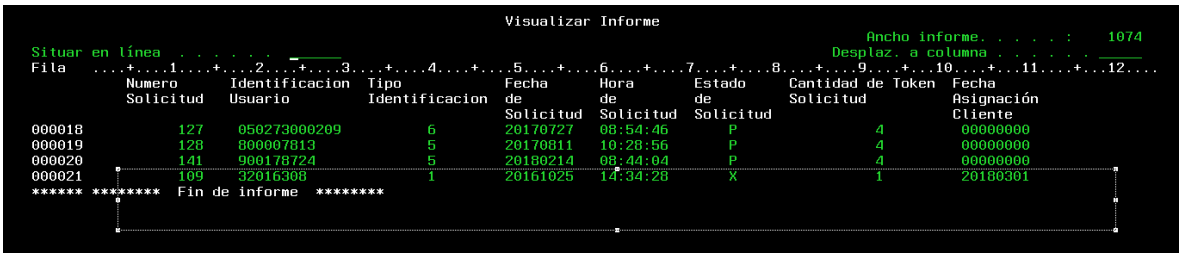


Figura 77. Proceso de revisión de token en el inventario.

La Solicitud Nro. 109 desapareció de las pendientes y paso a las Asignadas y listas a ser aprobadas en el área de Autorizaciones:

Figura 78. Pantalla área de autorizaciones

Verificamos el Log del Token también en la Tabla: BDOD16:

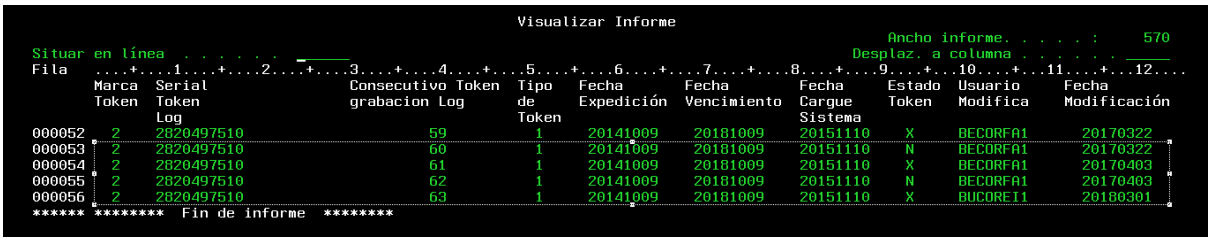


Figura 79. Log del Token también en la Tabla: BDOD16

Este Token ha tenido otras asignaciones en el transcurso de su vida en el inventario por eso se ven 63 asignaciones. Es porque es un Token de pruebas.

Revisamos ahora la contabilidad: La contabilidad se efectúa en el momento en que se aprueba esta asignación, por eso para este Modulo que es 26 y la transacción es 281, 281, 282. Se comentó en los apartes anteriores solo para verificar que la contabilidad solo se hace en el momento en que se hace la aprobación, esto porque es posible que se haga el reverso de la asignación, además se hace descargo del inventario cuando el inventario libera físicamente el Token.

Ejecución de la Prueba 2. DesAsignación de Token a la Solicitud.

Se parte de la pantalla de Solicitudes del Area de Autorizaciones:

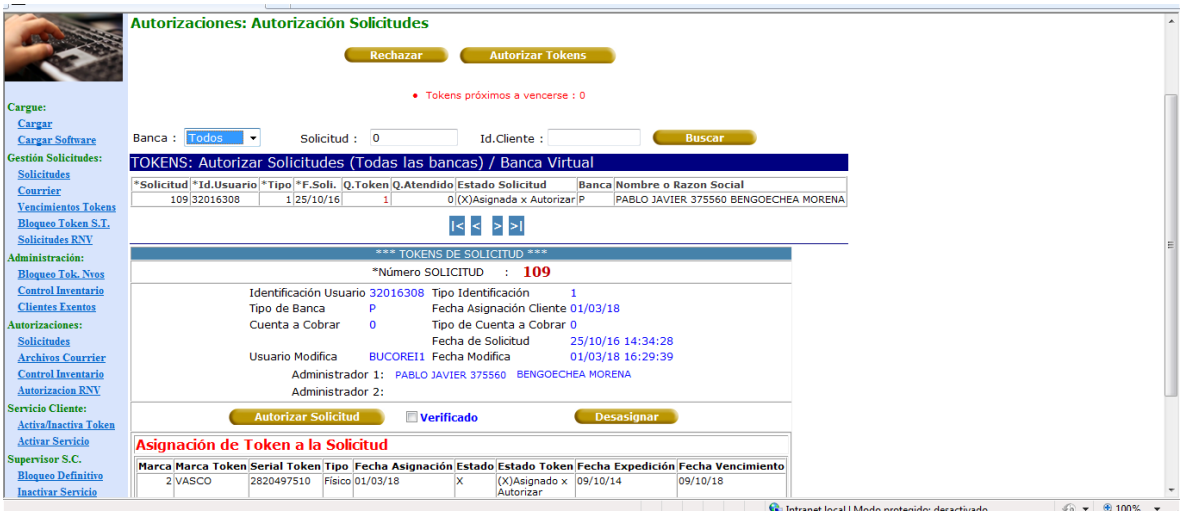


Figura 80. Ejecución prueba 2 Desasignación de Token a la Solicitud

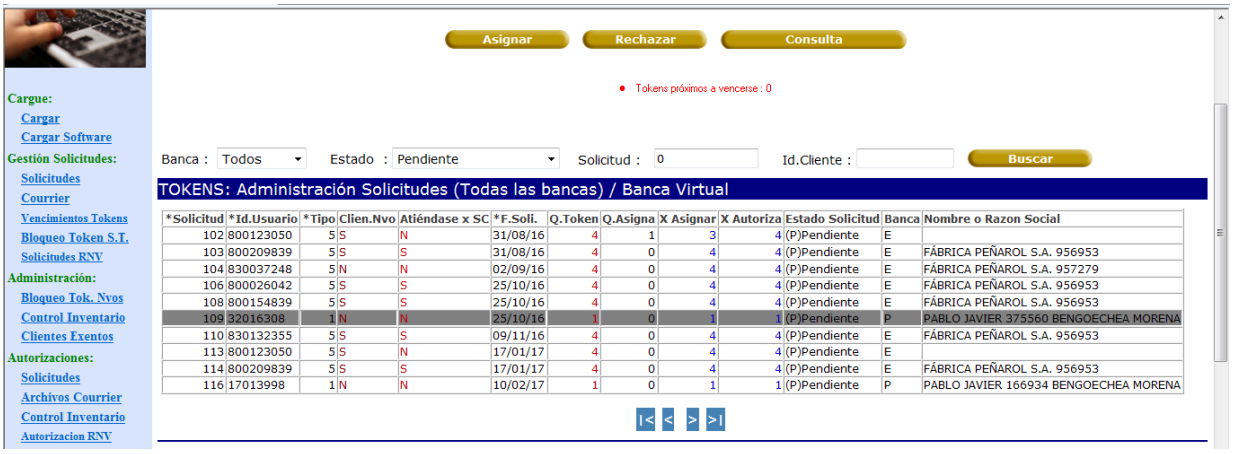
En donde se ubica la Solicitud Nro. 109. Se presiona el Botón Autorizar y abajo aparece el detalle de la Solicitud y su Token asignado. Para hacer la desasignación se presiona el Botón Desasignar se le marca el botón de verificado y también se da click a la línea del Token dejándolo en gris; y al realizar la operación se desasigan el Token:

Figura 81. Autorizar Solicitudes (Todas las bancas)

El mensaje que resulta es:

LISTO, TOKEN : 2820497510 - VASCO ha sido DesAsignado.....

Se produce lo siguiente en la tabla de Solicitudes, la solicitud 109 vuelve a su esta original:

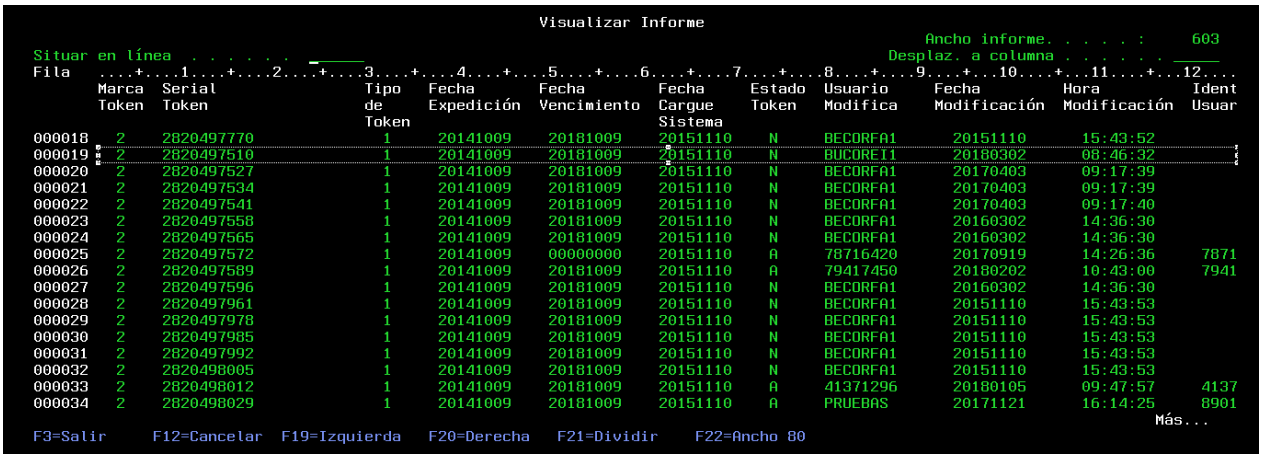


TOKENS: Administración Solicitudes (Todas las bancas) / Banca Virtual

*Solicitud	*Id.Usuario	*Tipo	Clien.Nvo	Atiéndase x SC	*F.Soli.	Q.Token	Q.Asigna	X Asignar	X Autoriza	Estado Solicitud	Banca	Nombre o Razon Social
102	800123050	5	S	N	31/08/16	4	1	3	4	(P)Pendiente	E	
103	800209839	5	S	S	31/08/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S.A. 956953
104	830037248	5	N	N	02/09/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S.A. 957279
106	800026042	5	S	S	25/10/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S.A. 956953
108	800154839	5	S	S	25/10/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S.A. 956953
109	32016308	1	N	N	25/10/16	1	0	1	1	(P)Pendiente	P	PABLO JAVIER 375560 BENGOECHEA MORENA
110	830132355	5	S	S	09/11/16	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S.A. 956953
113	800123050	5	S	N	17/01/17	4	0	4	4	(P)Pendiente	E	
114	800209839	5	S	S	17/01/17	4	0	4	4	(P)Pendiente	E	FÁBRICA PEÑAROL S.A. 956953
116	17013998	1	N	N	10/02/17	1	0	1	1	(P)Pendiente	P	PABLO JAVIER 166934 BENGOECHEA MORENA

Figura 82. Tabla de solicitud – verificación solicitud 109

Para ser procesada de nuevo. La tabla BDOD14 queda como inició:



Visualizar Informe

Ancho informe. . . . . : 603
Situar en línea . . . . . _____
Desplaz. a columna . . . . . ____

Fila ...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9...+...10...+...11...+...12...

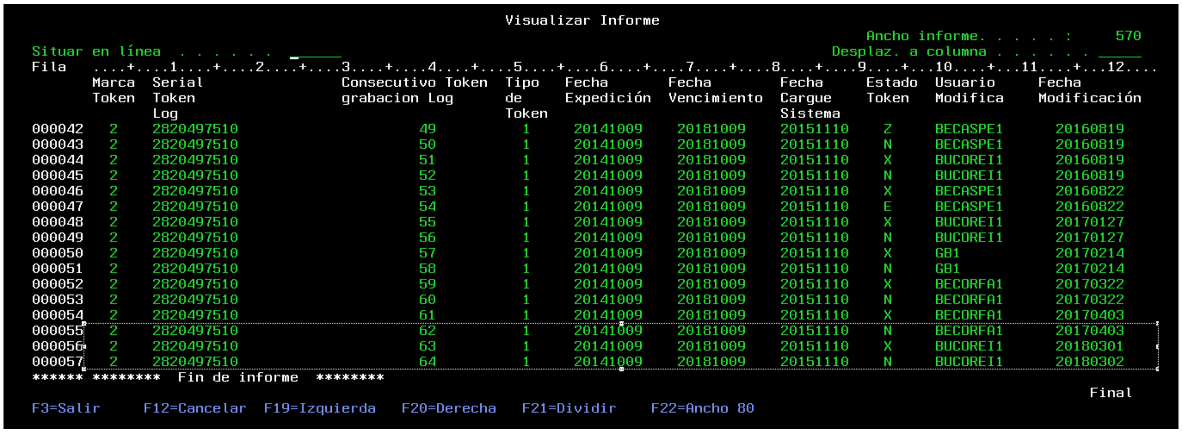
	Marca Token	Serial Token	Tipo de Token	Fecha Expedición	Fecha Vencimiento	Fecha Cargue Sistema	Estado Token	Usuario Modifica	Fecha Modificación	Hora Modificación	Ident Usuar
000018	2	2820497770	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:52	
000019	2	2820497510	1	20141009	20181009	20151110	N	BUCORE11	20180302	08:46:32	
000020	2	2820497527	1	20141009	20181009	20151110	N	BECORFA1	20170403	09:17:39	
000021	2	2820497534	1	20141009	20181009	20151110	N	BECORFA1	20170403	09:17:39	
000022	2	2820497541	1	20141009	20181009	20151110	N	BECORFA1	20170403	09:17:40	
000023	2	2820497558	1	20141009	20181009	20151110	N	BECORFA1	20160302	14:36:30	
000024	2	2820497565	1	20141009	20181009	20151110	N	BECORFA1	20160302	14:36:30	
000025	2	2820497572	1	20141009	00000000	20151110	A	78716420	20170919	14:26:36	7871
000026	2	2820497589	1	20141009	20181009	20151110	A	79417450	20180202	10:43:00	7941
000027	2	2820497596	1	20141009	20181009	20151110	N	BECORFA1	20160302	14:36:30	
000028	2	2820497961	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:53	
000029	2	2820497978	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:53	
000030	2	2820497985	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:53	
000031	2	2820497992	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:53	
000032	2	2820498005	1	20141009	20181009	20151110	N	BECORFA1	20151110	15:43:53	
000033	2	2820498012	1	20141009	20181009	20151110	A	41371296	20180105	09:47:57	4137
000034	2	2820498029	1	20141009	20181009	20151110	A	PRUEBAS	20171121	16:14:25	8901

Más...

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80

Figura 83. Tabla BDOD14 queda como inició

Y se registra el Token con una afectación más en su historial de Log:


Visualizar Informe

Ancho informe. . . . . : 570

Situar en línea . . . . . . Desplaz. a columna . . . . . .

Fila	Marca Token	Serial Token Log	Consecutivo Token grabacion Log	Tipo de Token	Fecha Expedición	Fecha Vencimiento	Fecha Cargue Sistema	Estado Token	Usuario Modifica	Fecha Modificación
000042	2	2820497510	49	1	20141009	20181009	20151110	Z	BECASPE1	20160819
000043	2	2820497510	50	1	20141009	20181009	20151110	N	BECASPE1	20160819
000044	2	2820497510	51	1	20141009	20181009	20151110	X	BUCOREI1	20160819
000045	2	2820497510	52	1	20141009	20181009	20151110	N	BUCOREI1	20160819
000046	2	2820497510	53	1	20141009	20181009	20151110	X	BECASPE1	20160822
000047	2	2820497510	54	1	20141009	20181009	20151110	E	BECASPE1	20160822
000048	2	2820497510	55	1	20141009	20181009	20151110	X	BUCOREI1	20170127
000049	2	2820497510	56	1	20141009	20181009	20151110	N	BUCOREI1	20170127
000050	2	2820497510	57	1	20141009	20181009	20151110	X	GB1	20170214
000051	2	2820497510	58	1	20141009	20181009	20151110	N	GB1	20170214
000052	2	2820497510	59	1	20141009	20181009	20151110	X	BECORFA1	20170322
000053	2	2820497510	60	1	20141009	20181009	20151110	N	BECORFA1	20170322
000054	2	2820497510	61	1	20141009	20181009	20151110	X	BECORFA1	20170403
000055	2	2820497510	62	1	20141009	20181009	20151110	N	BECORFA1	20170403
000056	2	2820497510	63	1	20141009	20181009	20151110	X	BUCOREI1	20180301
000057	2	2820497510	64	1	20141009	20181009	20151110	N	BUCOREI1	20180302

****** ******** Fin de informe ********

Final

F3=Salir F12=Cancelar F19=Izquierda F20=Derecha F21=Dividir F22=Ancho 80

Figura 84. Afectación más en su historial de Log

Informe Detallado: Cargue Token a la Solicitud de Token.

Se Observa que el Ingreso a la Aplicación es muy seguro, se hace a través del usuario que se creó en el AS400.

El Ingreso a la aplicación obliga a que al usuario de AS400 que se le tiene cargado unos perfiles, los ejecute y se le muestren las opciones en el la Aplicación. Los perfiles son:

Los perfiles son se han aplicado bien y se muestra en la pantalla que se opera solo las opciones para cada perfil.

Hay limitación de ejecución a solo la Solicitud 109. Lo cual es bueno para no confundirse con otra solicitud y hacer el trabajo de otra.

Hay control en lo asignado contra lo requerido.

Se ven buenos controles para asignación de Token porque hay que usar la casilla de Verificado, la cual permite afianzar la seguridad de que es eso lo que se quiere hacer.

Las marcas de Auditoria de Usuario, Fecha y Hora de modificación quedaron bien

asignadas.

La marca de fecha de asignación quedó también asignada.

La consignación en el Log del Token se está efectuando en forma correcta.

Se verifica que no se efectúa la contabilidad puesto que esta debe descargar el inventario cuando lo libere físicamente para enviárselo al courrier.

Si no hay actividad en 10 minutos en la aplicación, esta se sale sola para evitar intrusos porque el usuario que la está ejecutando posiblemente haya abandonado el puesto de trabajo dejando la pantalla libre para acceder.

5 EVALUACIÒN SIC – SISTEMA DE INFORMACIÒN COMPUTARIZADO.

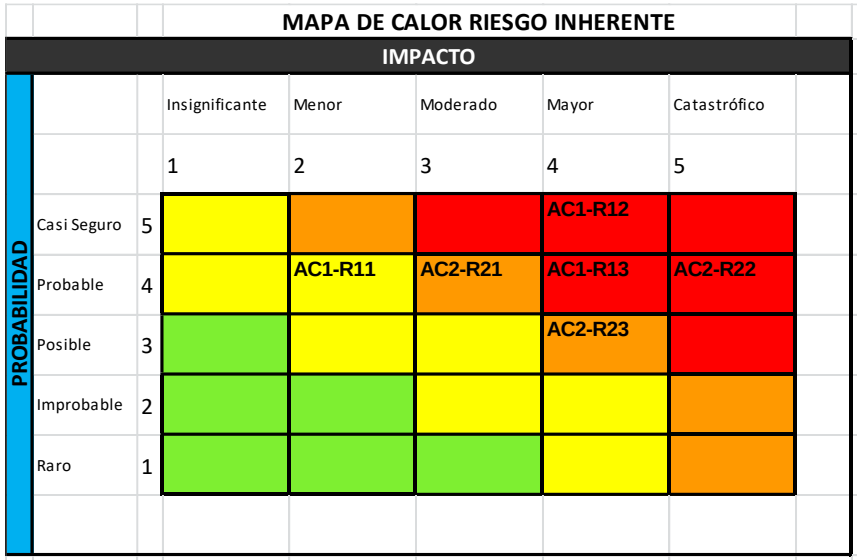
Convenciones: Utilizamos las siguientes convenciones que facilitan la clasificación de las probabilidades frente a los impactos.

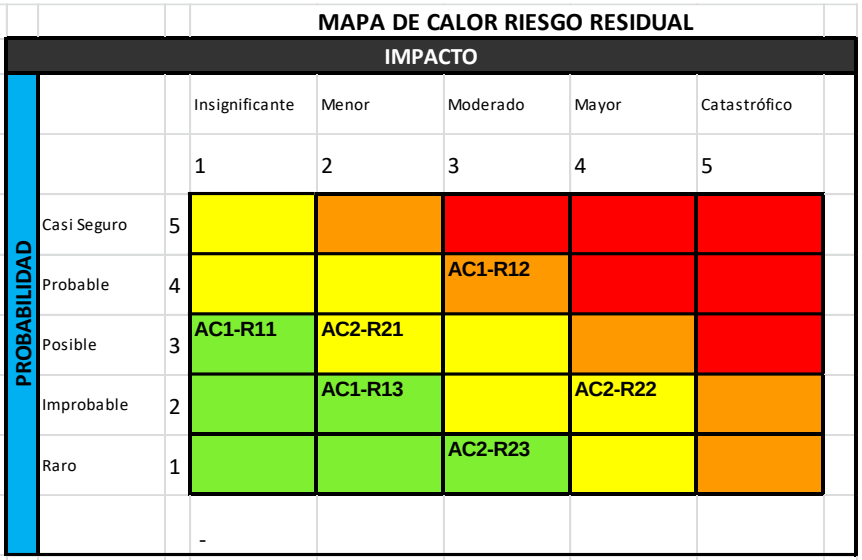
Probabilidad			Impacto	
Casi Seguro	5		Catastrófico	5
Probable	4		Mayor	4
Posible	3		Moderado	3
Improbable	2		Menor	2
Raro	1		Insignificante	1

5.1 Matriz riesgos y controles Seguridad Lógica y Pistas de Auditoría

SEGURIDAD LOGICA Y PISTAS DE AUDITORIA				
ACTIVIDADES	RIESGOS	CONTROLES	ESTADO CONTROL	RESPONSABLE
AC1. Gestión de Políticas de Creación y Uso de Usuarios para la Aplicación	R11. Pérdida de información originada por la mala creación de los Usuarios.	Ctrl-111: -Definición políticas claras que asignen nombres nemotécnicos a los usuarios. Ctrl-112: -Definir perfiles de responsabilidad dentro de la aplicación. Ctrl-113: -Registro de Usuario, Fecha y Hora de trabajo en las actividades de la Aplicación.	Implantado	DBA

	R12. Pérdida de Responsabilidades de manipulación de la Información.	Ctrl-121: -Realizar asignaciones de quienes manipulan la información. -Asegurar tareas para el manejo de información por Usuario en la Aplicación.	Implantado	DBA
	R13. Suplantación de responsables en el manejo de la Información de la Aplicación.	Ctrl-131: -Asignación de formatos con firma de responsables para la asignación de usuarios que gestionarán la Aplicación.	Implantado	DBA
AC2. Realización de Logs en Procesos críticos.	R21. Pérdida del seguimiento de casos especiales de consulta.	Ctrl-211: Consignar programas que disparen registros de seguimiento.	Implantado	DBA y Administrador de la Aplicación.
	R22. No poder establecer los responsables de operaciones fraudulentas.	Ctrl-221: Colocar programas disparadores para poder guardar los logs de transacción.	Implantado	DBA y Administrador de la Aplicación.
	R23. No poder justificar pérdidas de información por tanto pérdida de imagen ante algún evento a justificar.	Ctrl-231: Crear un acta de responsabilidad que debe ser firmada como responsabilidad	Implantado	DBA y Administrador de la Aplicación.





Estableciendo unas escalas de 1 a 5 tanto en la Probabilidad como en el impacto de los que pueda llegar a suceder, analizamos los riesgos del proyecto estableciendo unos controles aplicados que van a reducir el impacto en el caso de materializarse.

Al aplicar los controles Ctrl-111 al Ctrl-231 para la Seguridad lógica se logran bajar los riegos a un nivel entre probabilidad e impacto más tolerable.

5.2 Matriz riesgos y control Integridad

INTEGRIDAD				
ACTIVIDADES	RIESGOS	CONTROLES	ESTADO CONTROL	RESPONSABLE
AC3. Revisión de los diseños y arquitectura de la aplicación en la Base Datos	R31. Mala toma de decisiones debido al desconocimiento de la relación entre los componentes del sistema.	Ctrl-311: Definir el modelo entidad relación de la base de datos.	Implementado	DBA
	R32. Falla en los procesos que registran la información en tablas debido a la no correspondencia de la naturaleza y dominio de la información de los campos.	Ctrl-321: Construcción del diccionario de datos que muestren la naturaleza información de los objetos y las restricciones que debe cumplir la información contenida en los campos.	Implementado	DBA
	R33. Interrupción del servicio ocasionada por fallas internas durante el proceso.	Ctrl-331: Compilar los objetos de la base de datos para la disponibilidad en los diferentes procesos donde son utilizados.	Implementado	DBA
	R34. Repercusiones legales (sanciones) debido al no cumplimiento y/o implementación de las reglas del negocio.	Ctrl-341: Creación de restricciones y condiciones entre las tablas debido a las reglas del negocio.	Implementado	DBA
AC4.	R41.	Ctrl-411: Actualizar en tiempo real el estado de los Tokens	No implementado	DBA

Generación de Tokens disponibles para las transacciones	Daño y pérdida del Token, afectación del servicio ocasionado por la inconsistencia del sistema.			
	R42. Pérdida financiera y de competitividad debido a la afectación del servicio.	Ctrl-421: Sincronizar los servidores de la aplicación y Tokens de clientes	No implementado	DBA
	R43. Repercusiones legales debido a la no divulgación de las fechas de vencimiento del servicio del dispositivo.	Ctrl-431: Listar los usuarios cuyos Tokens tienen una fecha de vencimiento inferior o igual a 3 meses.	Implementado	DBA

MAPA DE CALOR RIESGO INHERENTE

PROBABILIDAD		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5
Casi Seguro	5		AC4-R41	AC3-R32	AC4-R42	
Probable	4			AC4-R43	AC3-R31	AC3-R33
Posible	3				AC3-R34	
Improbable	2					
Raro	1					

MAPA DE CALOR RIESGO RESIDUAL

PROBABILIDAD		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5
Casi Seguro	5					
Probable	4	AC3-R32				
Posible	3	AC4-R41				
Improbable	2	AC4-R42	AC3-R31	AC3-R34		
Raro	1		AC4-R43	AC3-R33		

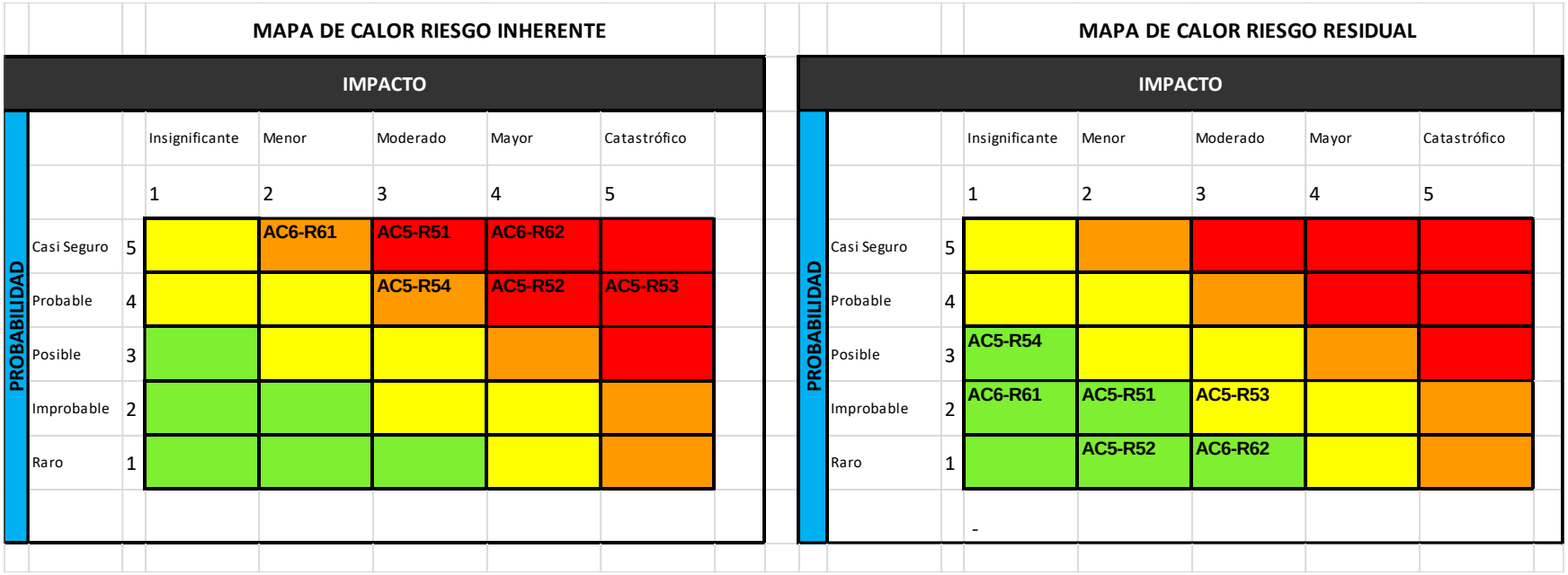
-

De la misma forma se baja la incertidumbre de riesgo en el Control de Integridad de datos al aplicar los controles.

5.3 Matriz riesgos y control Continuidad

MATRIZ DE CONTINUIDAD Y DISPONIBILIDAD DE LA INFORMACION				
ACTIVIDADES	RIESGOS	CONTROLES	ESTADO CONTROL	RESPONSABLE
AC5. Gestión de procesos de contingencia	R51. Perdida competitividad.	Ctrl-511: Políticas y documentación de los procesos de contingencia y recuperación en caso de desastre y o eventos desafortunados.	Implementado	DBA – director informática
		Ctrl-512: Árbol de llamadas para la activación de la contingencia.	No Implementado	DBA
	R52. Pérdida de clientes por mal servicio y o disponibilidad de la plataforma.	Ctrl-521: Capacitaciones cruzadas entre funcionarios, que permitan el conocimiento mutuo de sus procesos.	No Implementado	DBA - Analistas
	R53. Pérdida de credibilidad por no disponibilidad de los servicios.	Ctrl-531: Elaboración de pruebas de contingencia con periodicidad semestral.	Implementado	DBA
	R54. Repercusiones legales por no continuidad de la plataforma y manejo de su dinero.	Ctrl-541: Actualización de las contingencias y la recuperación según los cambios en procedimientos y mejoras tecnológicas.	Implementado	DBA
AC6.		Ctrl-611: Documentación y asignación de responsables sobre backups.	Implementado	DBA

Gestión de Backups	R61. Pérdida de clientes por mal servicio y o disponibilidad de la plataforma.	Realización de simulacros de contingencia y recuperación de backups.	Implementado	DBA
	R62. Pérdidas financieras	Ctrl-621: Realización de pruebas de los backups tomados.	Implementado	DBA

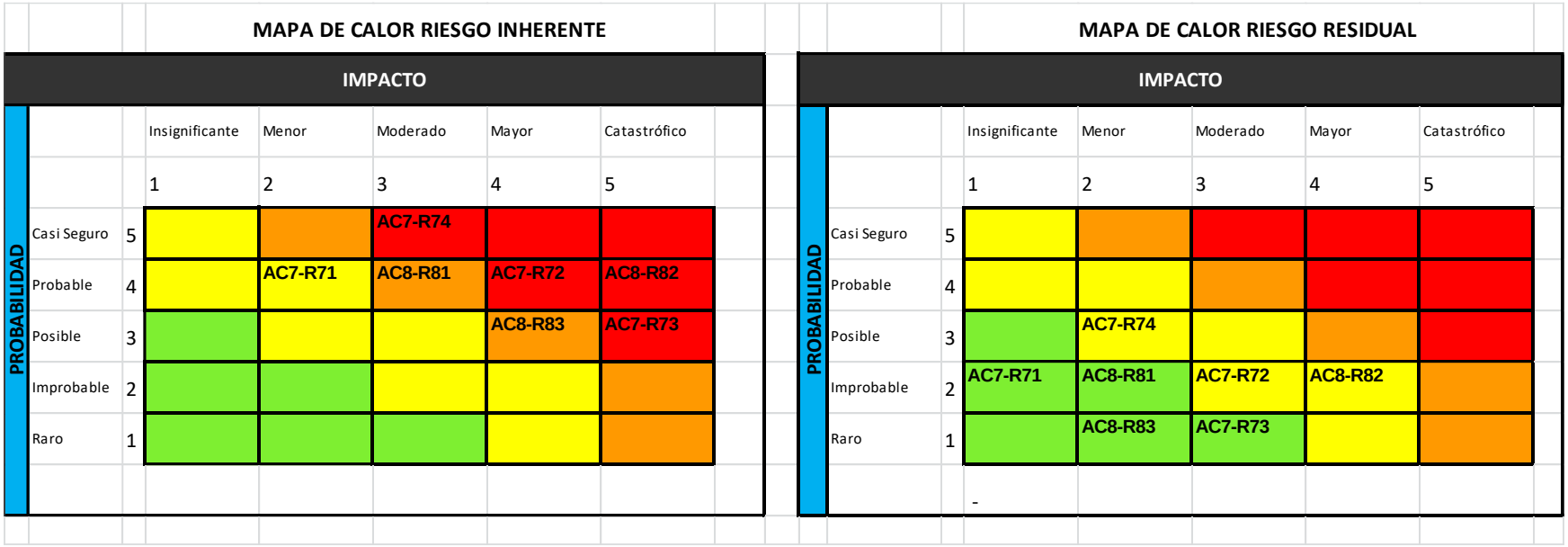


Para el Control de continuidad también los controles aplicados son efectivos porque bajan el riesgo en una forma especial pasando de una zona crítica a una zona de confort, aunque hay que tener cuidado y no estar tan tranquilos, estos riesgos son de mucho cuidado y cambiantes en cualquier momento.

5.4 Matriz riesgos y control Aseguramiento Ambiental

SEGURIDAD EN EL AMBIENTE				
ACTIVIDADES	RIESGOS	CONTROLES	ESTADO CONTROL	RESPONSABLE
AC7. Cumplimiento de políticas legales y operativas	R71. Mala toma de decisiones debido al desconocimiento de la topología de la red en la cual funciona la aplicación	Ctrl-711: Generar la topología en la cual opera la aplicación	Implementado	Administrador del centro de cómputo
	R72. Repercusiones y sanciones legales por el uso de software No licenciado	Ctrl-721: Licenciar la base de datos que contiene la semilla de los Tokens.	Implementado	DBA
	R73. Daño o pérdida de la información causada por ataques cibernéticos	Ctrl-731: Licenciar el software de antivirus el servidor que contiene la base de datos	Implementado	Administrador del servidor
	R74. Pérdida del soporte del sistema operativo por el uso de software No licenciado	Ctrl-741: Licenciar el sistema operativo del servidor	Implementado	Administrador del servidor
AC8. Aseguramiento de la información y equipo de cómputo	R81. Acceso a personal no autorizado debido suplantación de identidad	Ctrl-811: Instalar un lector biométrico para el ingreso al centro de cómputo	No implementado	Administrador del centro de cómputo
	R82. Pérdida o daño en equipos de cómputo ocasionado por incendio	Ctrl-821: Adquirir e instalar extintores para incendios en equipo de cómputo	Implementado	Administrador del centro de cómputo

	y uso de extintor no apto en conflagración en equipo de cómputo			
	R83. Interrupción del servicio y/o en los procesos de la aplicación, debido a la conexión equivocada de cables en el rack de comunicación	Ctrl-831: Identificar mediante etiquetas en origen y destino todos los cables de red del rack	Implementado	Administrador del centro de cómputo



El aseguramiento ambiental también tiene riesgos que hay que aplicarles controles reduciendo su impacto de la mejor y más aceptable forma.

6 METODOLOGIA DE APLICACIÒN

6.1 Conceptos generales:

Se entiende por Metodología, al proceso que se aplica paso a paso en forma cronológica y ordenada para la elaboración de una tarea o tareas aplicando normas exigentes e infranqueables que llevan a feliz término una aplicación o un fin.

La idea más concreta es seguir unas instrucciones que enmarcadas llevan a que los procesos sean controlados y no den la posibilidad de que se hagan desvíos que conlleven a huecos tanto de fondo como de forma. Esto es apuntándole a una buena seguridad y a una buena trazabilidad de los desarrollos de sistemas. A demás que se persigue aplicar los conceptos urgentes de disponibilidad, integridad, confidencialidad, etc., buscando autenticidad de las aplicaciones de sistemas.

Para el caso nuestro, se persigue que al adelantar desarrollos de sistemas para la administración de dispositivos de autenticación fuerte como son los Tokens, se siga paso a paso el modelo de desarrollo a la medida, pero adoptando las recomendaciones que se exponen y que buscan un afinamiento de desarrollo de un concepto que se ha puesto de moda, “Desarrollo Seguro”.

6.2 Aplicación:

Esta Metodología que se muestra, se puede aplicar a cualquier desarrollo de un proyecto de Administración de Tokens; el cual va desde el cargue de semillas de Tokens a una sistema de inventario para su control hasta el manejo de los diferentes escenarios que los Tokens atraviesan durante su ciclo de vida.

No es camisa de fuerza la adaptabilidad de lo expuesto y cada organización acomoda los desarrollos de acuerdo con su gestión, administración e importancia que le pueden dar a los

diferentes temas que se tocan. A demás que las organizaciones ya tienen estándares probados que pueden aplicar como variación a cada una de las partes del desarrollo de software.

Objetivos:

- Fijar las políticas a seguir dentro de los desarrollos de sistemas de información.
- Proponer pasos que deben adoptarse para avanzar en el desarrollo.
- Elaborar software seguro.
- Evitar posibles fallas y huecos de seguridad.
- Apoyar las consultas con trazabilidad elaborativa.
- Proporcionar a los clientes disponibilidad de sus canales virtuales al instante.
- Prestar apoyo al área de servicio al Cliente con los resultados de las consultar y agilizar las acciones que deben efectuarse para dar servicio al instante cuando se presenten problemas de autenticación.
- Disminuir los tiempos de desarrollo en los temas de Administración de Software.
- Escribir software con lineamientos y estándares ceñidos a las normas legales.

6.3 Metodología Tradicional:

Estos puntos no nos van a alejar de las metodologías tradicionales de desarrollo porque cada modelo de desarrollo propuesto a lo largo de todos los estudios tiene un enfoque bien marcado. Las metodologías en cascada enfocan a los desarrolladores a elabora planes, mapas conceptuales, requerimientos, seguimientos que siguen siendo de gran importancia para el logro de las mejores aplicaciones. Pero debemos enfocarnos en los desarrollos que se acomoden a los mejores y más seguros logros.

Aquí no nos vamos a olvidar de la generación y atención de requerimientos, del análisis de los mismos, de la aplicación de un buen diseño con fines exitosos; la elección de una buena

herramienta de desarrollo es muy importante, cada organización ya tiene las suyas y deben seguir con sus estándares, la codificación de programas y la nemotecnia es de gran importancia para que se hablen el mismo idioma dentro de las empresas o unidades de desarrollo en las organizaciones. Las pruebas de diferente índole, de unitarias de desarrollo, pruebas y análisis deben marchar de la misma forma dando cumplimiento a las necesidades de los requerimientos.

El mantenimiento de programas sigue de la misma manera aplicando las políticas propuestas. El modelado, la prototipación, la retroalimentación, y la puesta en marcha de los proyectos no varía, puede seguirse adoptando las que se llevan a cabo hasta el momento en las organizaciones, además que ya se sabe de algunas con excelentes resultados en cada empresa.

Las Metodología de desarrollo, Scrum, Kanban, XP, que son buenas prácticas de desarrollo de ingeniería no van a cambiar por las recomendaciones que se realizan para mejorar los desarrollos. Eso sí, y lo más importante, no olvidar la calidad de los trabajos que finalmente se obtengan porque ellos van a hablar bien de cuanto fue la importancia que fue aplicada a los trabajos encomendados para solucionar y gestionar el desarrollo del software y su uso.

6.4 Principios:

La Norma ISO 27002 en la cual se apoya la propuesta, proporciona lineamientos que se aplican y que se tienen en cuenta en las recomendaciones que se hacen en la aplicación metodológica. Cada uno de estos conceptos es claves para asegurar un Desarrollo Seguro de Software. Estos conceptos son la base que es utilizada en la propuesta metodológica.

Normas de Códigos de Buenas Prácticas.

Esta Norma publicada en el 2007. Ella detalla los objetivos de control recomendados en los aspectos de seguridad de la información. Es publicada en español por la empresa AENOR y en Colombia por: NTC-ISO 27002

ISO 27002 colabora con recomendaciones y medidas para adoptar en las empresas y asegurar los sistemas de información. Las secciones con las cuales proporciona ayuda son:

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de seguridad de la información.
- Gestión de continuidad del negocio.
- Conformidad.

6.5 Metodología final de resultado

METODOLOGIA PARA SEGURIDAD LOGICA				
ACTIVIDADES	**DEFICIENCIAS**	**METODOS DE APLICACIÓN**	**APOYO EN DOMINIO ISO27002**	
Gestión de Políticas de Creación y Uso de Usuarios para la Aplicación	Pérdida de información originada por la mala creación de los Usuarios.	**-Defininir políticas claras que asignen nombres nemotécnicos a los usuarios.**	5.1.1 Conjunto de políticas para la seguridad de la información.	12.1.1 Documentación de procedimientos de operación.
		-Definir perfiles de responsabilidad dentro de la aplicación.	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	6.1.1 Asignación de responsabilidades para la seguridad de la información.
		-Registrar Fecha y Hora y Usuario de trabajo en las actividades de la Aplicación y en las tablas de la misma.	5.1.1 Conjunto de políticas para la seguridad de la información.	
	Pérdida de Responsabilidades de manipulación de la Información.	**-Realizar asignaciones de quienes manipulan la información.**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	6.1.1 Asignación de responsabilidades para la seguridad de la información.
		-Asegurar tareas para el manejo de información por Usuario en la Aplicación.	5.1.1 Conjunto de políticas para la seguridad de la información.	6.1.1 Asignación de responsabilidades para la seguridad de la información.
	Suplantación de responsables en el manejo de la Información de la Aplicación.	**-Asignación de formatos con firma de responsables para la asignación de usuarios que gestionarán la Aplicación.**	5.1.1 Conjunto de políticas para la seguridad de la información.	6.1.2 Segregación de tareas
Realización de Logs en Procesos críticos.	Pérdida del seguimiento de casos especiales de consulta.	**Consignar programas que disparen registros de seguimiento.**	5.1.1 Conjunto de políticas para la seguridad de la información.	
	No poder establecer los responsables de operaciones fraudulentas.	**Colocar programas disparadores para poder guardar los logs de transacción.**	5.1.1 Conjunto de políticas para la seguridad de la información.	9.2.2 Gestión de los derechos de acceso asignados a usuarios.
	No poder justificar pérdidas de información por tanto pérdida de imagen ante algún evento a justificar.	**Crear un acta de registro que debe ser firmada por los responsables.**	5.1.1 Conjunto de políticas para la seguridad de la información.	

METODOLOGIA PARA INTEGRIDAD DE LA INFORMACION				
ACTIVIDADES	**DEFICIENCIAS**	**METODOS DE APLICACIÓN**	**APOYO EN DOMINIO ISO27002**	
Revisión de los diseños y arquitectura de la aplicación en la Base Datos	Mala toma de decisiones debido al desconocimiento de la relación entre los componentes del sistema.	**Definir el modelo entidad relación de la base de datos.**	12.1.1 Documentación de procedimientos de operación.	
	Falla en los procesos que registran la información en tablas debido a la no correspondencia de la naturaleza y dominio de la información de los campos.	**Construir el diccionario de datos que muestre la naturaleza de la información de los objetos y las restricciones que debe cumplir la información contenida en los campos.**	12.1.1 Documentación de procedimientos de operación.	
	Interrupción del servicio ocasionada por fallas internas durante el proceso.	**Compilar los objetos de la base de datos para la disponibilidad en los diferentes procesos donde son utilizados.**	12.1.1 Documentación de procedimientos de operación.	
	Repercusiones legales (sanciones) debido al no cumplimiento y/o implementación de las reglas del negocio.	**Crear restricciones y condiciones entre las entidades que cumnplan con las reglas del negocio.**	5.1.1 Conjunto de políticas para la seguridad de la información.	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
Generación de Tokens disponibles para las transacciones	Daño y pérdida del Token, afectación del servicio ocasionado por la inconsistencia del sistema.	**Actualizar en tiempo real el estado de los Tokens.**	10.1.1 Política de uso de los controles criptográficos.	
	Pérdida financiera y de competitividad debido a la afectación del servicio.	**Sincronizar los servidores de la aplicación y Tokens de clientes.**	10.1.1 Política de uso de los controles criptográficos.	
	Envio, recepción y compartir información.	**Asegurar que la información enviada y recibida venga encryptada de manera que no sea manipulable.**	10.1.1 Política de uso de los controles criptográficos.	
	Repercusiones legales debido a la no divulgación de las fechas de vencimiento del servicio del dispositivo.	**Listar los usuarios cuyos Tokens tienen una fecha de vencimiento inferior o igual a 3 meses.**	12.1.1 Documentación de procedimientos de operación.	

METODOLOGIA PARA CONTINUIDAD Y DISPONIBILIDAD DE LA INFORMACION				
ACTIVIDADES	**DEFICIENCIAS**	**METODOS DE APLICACIÓN**	**APOYO EN DOMINIO ISO27002**	
Gestión de procesos de contingencia	Perdida competitividad.	**Aplicar Políticas y documentación de los procesos de contingencia y recuperación en caso de desastre y o eventos desafortunados.**	5.1.1 Conjunto de políticas para la seguridad de la información.	
		Definir el árbol de llamadas para la activación de la contingencia.	5.1.1 Conjunto de políticas para la seguridad de la información.	
	Pérdida de clientes por mal servicio y o disponibilidad de la plataforma.	**Capacitar funcionarios, que permitan el conocimiento mutuo de los procesos.**	5.1.1 Conjunto de políticas para la seguridad de la información.	
	Pérdida de credibilidad por no disponibilidad de los servicios.	**Elaborar pruebas de contingencia con periodicidad semestral.**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Repercusiones legales por no continuidad de la plataforma y manejo de su dinero.	**Actualizar vitacora de contingencias y recuperación según los cambios en procedimientos y mejoras tecnológicas.**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
Gestión de Backups		**Documentar y asignar responsables sobre backups.**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Pérdida de clientes por mal servicio y o disponibilidad de la plataforma.	**Realizar simulacros de contingencia y recuperación con backups.**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Pérdidas financieras	**Realizar pruebas de los backups tomados.**	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	

Cada uno de los puntos que se vayan desarrollando en la aplicación que al acomodo de las organizaciones vayan realizando, deben apoyarse en las medidas metodológicas que se han definido en este modelo; de tal manera que al no descuidarse cada una de las recomendaciones, se vaya asegurando la credibilidad, la integridad, y la disponibilidad de la información para la empresa y en definitiva para los clientes, que son los principalmente afectados, y para los cuales es que se desarrollan la gran mayoría de los productos de apoyo

transaccional del Banco.

La dinámica consiste en establecer las actividades de acuerdo con la metodología, valorar y darle importancia a las deficiencias y aplicar las recomendaciones o métodos de aplicación que se derivan, para que los desarrollos tengan esa validez necesaria que aplica a los proyectos de esta envergadura y responsabilidad.

6.5.1 Pasó a Paso – Levantamiento y programación de los procesos:

- En cada uno de los procesos de trazabilidad de la información, deben levantarse los datos que conciernen tomar paso a paso todo el proceso aplicando cada uno de los ajustes propuestos en la metodología.
- Si la metodología dice que hay que aplicar nombres nemotécnicos a las tablas, los campos de las tablas, los procesos; estos en el momento del desarrollo debe tomarse como guía y cualquiera que sea la mecánica que se adopte, será bien tomada y debe respetarse durante todo el desarrollo.
- Todas las tablas deben guardar registro a registro los usuarios responsables de la información, y los momentos en los cuales se afectaron los registros, fecha y hora de aplicación, creación, modificado y borrado con un log de recuerdo en el caso que los registros se borren del todo de la tabla afectada.
- Deben asignarse responsables de los procesos con sus respectivos backups para que se encarguen de trabajar con la misma dinámica y conozcan sus roles por usuario y perfil dentro de la aplicación.
- La aplicación debe guardar uniformidad en pantallas y modos de trabajar que faciliten el entendimiento para cualquier

usuario que llega como nuevo a ejercer un papel importante dentro del manejo de la aplicación.

- No todos los usuarios deben poder ingresar y hacerlo en la aplicación puesto que hay restricciones de seguridad que solo permite que los usuarios autorizados lo hagan y se responsabilicen de las acciones realizadas dentro de la aplicación.
- Cada acción que se realice dentro de la aplicación, si requiere de apoyo contable debe hacerse en línea, y contabilizar directamente a los inventarios de los tokens, ya sea sumando o restando en el inventario. La idea es que todos los días estén cuadrados tanto el inventario físico como las cuentas que lo reflejan.
- Si se requiere transferencia de archivos entre los aplicativos, estos deben enviarse en forma encriptada y la aplicación receptora debe usar un algoritmo de desencripción provisto para tal fin.
- Si se va a usar un método de encripción y desencripción debe adquirirse uno externo que proporcione tranquilidad y del cual no se sepa internamente dentro de la empresa su algoritmo, esto para guardar independencia.
- Debe guardarse un log de las tablas que se decida hacerse y que requieran de trazabilidad para poder hacer seguimiento en caso de tener que justificar algunas inconsistencias que se puedan presentar. El log debe guardar todo el detalle del antes y el después de la operación realizada en el aplicativo.

6.6 Contrastación del proyecto:

La contrastación de los proyectos y su desarrollo lleva a verificar lo que inicialmente se bosquejó elaborar y lo que finalmente se obtuvo como producto final. Las utilidades que punto a punto se va a obtener en el desarrollo de los temas y todo el valor agregado que se deriva de tener una metodología de apoyo que asegure que los procesos no van a tener fugas de información, permitir abrir puertas de penetración a intrusos, facilitar los seguimientos de la trazabilidad de los procesos y mostrar de manera clara, espontanea, precisa y segura que la información de los clientes se administra con toda la responsabilidad y confiabilidad que ameritan estos casos.

Traemos a colación de nuevo los objetivos iniciales y los vamos a enumerarlos para facilitar la contrastación:

Objetivo General y Objetivos Específicos:

OBJETIVOS DEL PROYECTO	
OG = Objetivo General	• Desarrollar una Metodología para definir e inspeccionar la estructura de los puntos de control en las aplicaciones de Administración de Tokens Bancario
OE1 = Objetivo Específico 1	• Identificar los puntos de control auditables, contemplados en los módulos de cargue de semillas, creación de la Solicitud y asignación del Token para asegurar la confiabilidad de la aplicación y generar la matriz de riesgos.
OE2 = Objetivo Específico 2	• Realizar la auditoría a los módulos del sistema para verificar la metodología y asegurar que los procesos estén vigilados.
OE3 = Objetivo Específico 3	• Evaluar la metodología propuesta del sistema para mitigar las vulnerabilidades encontradas en el sistema de administración de Token.

A continuación, se muestra la correspondencia de la metodología propuesta y los objetivos que se plantearon para el desarrollo

del proyecto, cumpliendo con la destinación de cada punto metodológico y dando respuesta a los requerimientos y preocupaciones de cada actividad apropiando los riesgos de tal manera que la inherencia de los mismos alcance la residualidad esperada.

CONTRASTACION OBJETIVOS - METODOLOGIA				
ACTIVIDADES	DEFICIENCIAS	METODOS DE APLICACIÓN	OBJETIVOS INICIALES DEL PROYECTO	
Gestión de Políticas de Creación y Uso de Usuarios para la Aplicación	Pérdida de información originada por la mala creación de los Usuarios.	-Defininir políticas claras que asignen nombres nemotécnicos a los usuarios.	OG = Objetivo General	OE1 = Objetivo Específico 1
		-Definir perfiles de responsabilidad dentro de la aplicación.		OE1 = Objetivo Específico 1
		-Registrar Fecha y Hora y Usuario de trabajo en las actividades de la Aplicación y en las tablas de la misma.		OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2 OE3 = Objetivo Específico 3
	Pérdida de Responsabilidades de manipulación de la Información.	-Realizar asignaciones de quienes manipulan la información.		OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2 OE3 = Objetivo Específico 3
		-Asegurar tareas para el manejo de información por Usuario en la Aplicación.		OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2 OE3 = Objetivo Específico 3
	Suplantación de responsables en el manejo de la Información de la Aplicación.	-Asignación de formatos con firma de responsables para la asignación de usuarios que gestionarán la Aplicación.		OE1 = Objetivo Específico 1
Realización de Logs en Procesos críticos.	Pérdida del seguimiento de casos especiales de consulta.	Consignar programas que disparen registros de seguimiento.		OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2
	No poder establecer los responsables de operaciones fraudulentas.	Colocar programas disparadores para poder guardar los logs de transacción.		OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2
	No poder justificar pérdidas de información por tanto pérdida de imagen ante algún evento a justificar.	Crear un acta de registro que debe ser firmada por los responsables.		OE1 = Objetivo Específico 1 OE3 = Objetivo Específico 3

METODOLOGIA PARA INTEGRIDAD DE LA INFORMACION				
ACTIVIDADES	DEFICIENCIAS	METODOS DE APLICACIÓN	OBJETIVOS INICIALES DEL PROYECTO	
Revisión de los diseños y arquitectura de la aplicación en la Base Datos	Mala toma de decisiones debido al desconocimiento de la relación entre los componentes del sistema.	Definir el modelo entidad relación de la base de datos.	OG = Objetivo General	OE1 = Objetivo Específico 1
	Falla en los procesos que registran la información en tablas debido a la no correspondencia de la naturaleza y dominio de la información de los campos.	Construir el diccionario de datos que muestre la naturaleza de la información de los objetos y las restricciones que debe cumplir la información contenida en los campos.		OE1 = Objetivo Específico 1
	Interrupción del servicio ocasionada por fallas internas durante el proceso.	Compilar los objetos de la base de datos para la disponibilidad en los diferentes procesos donde son utilizados.		OE1 = Objetivo Específico 1
	Repercusiones legales (sanciones) debido al no cumplimiento y/o implementación de las reglas del negocio.	Crear restricciones y condiciones entre las entidades que cumnplan con las reglas del negocio.		OE1 = Objetivo Específico 1 OE3 = Objetivo Específico 3
Generación de Tokens disponibles para las transacciones	Daño y pérdida del Token, afectación del servicio ocasionado por la inconsistencia del sistema.	Actualizar en tiempo real el estado de los Tokens.		OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2 OE3 = Objetivo Específico 3
	Pérdida financiera y de competitividad debido a la afectación del servicio.	Sincronizar los servidores de la aplicación y Tokens de clientes.		OE1 = Objetivo Específico 1 OE3 = Objetivo Específico 3
	Envio, recepción y compartir información.	Asegurar que la información enviada y recibida venga encryptada de manera que no sea manipulable.		OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2 OE3 = Objetivo Específico 3
	Repercusiones legales debido a la no divulgación de las fechas de vencimiento del servicio del dispositivo.	Listar los usuarios cuyos Tokens tienen una fecha de vencimiento inferior o igual a 3 meses.		OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2 OE3 = Objetivo Específico 3

METODOLOGIA PARA CONTINUIDAD Y DISPONIBILIDAD DE LA INFORMACION				
ACTIVIDADES	DEFICIENCIAS	METODOS DE APLICACIÓN	OBJETIVOS INICIALES DEL PROYECTO	
Gestión de procesos de contingencia	Perdida competitividad.	Aplicar Políticas y documentación de los procesos de contingencia y recuperación en caso de desastre y o eventos desafortunados.	OG = Objetivo General	OE1 = Objetivo Específico 1 OE2 = Objetivo Específico 2 OE3 = Objetivo Específico 3
		Definir el árbol de llamadas para la activación de la contingencia.		OE1 = Objetivo Específico 1 OE3 = Objetivo Específico 3
	Pérdida de clientes por mal servicio y o disponibilidad de la plataforma.	Capacitar funcionarios, que permitan el conocimiento mutuo de los procesos.		OE1 = Objetivo Específico 1 OE3 = Objetivo Específico 3
	Pérdida de credibilidad por no disponibilidad de los servicios.	Elaborar pruebas de contingencia con periodicidad semestral.		OE1 = Objetivo Específico 1
	Repercusiones legales por no continuidad de la plataforma y manejo de su dinero.	Actualizar vitacora de contingencias y recuperación según los cambios en procedimientos y mejoras tecnológicas.		OE1 = Objetivo Específico 1
Gestión de Backups		Documentar y asignar responsables sobre backups.		OE1 = Objetivo Específico 1
	Pérdida de clientes por mal servicio y o disponibilidad de la plataforma.	Realizar simulacros de contingencia y recuperación con backups.		OE1 = Objetivo Específico 1
	Pérdidas financieras	Realizar pruebas de los backups tomados.		OE1 = Objetivo Específico 1

Los Objetivos propuestos desde el comienzo del tema investigativo se han cumplido. Se ha creado una metodología para tener en cuenta y aplicar en el momento de realizar los desarrollos de cada uno de los módulos de la aplicación que administre los Tokens que usarán los clientes para garantizar que estos son bien custodiados de principio a fin. Definir una metodología no es nada fácil, porque ella debe contemplar muchos temas que aseguren que todos los ítems sean bien contemplados, dominados y responsablemente tratados. La trazabilidad es muy importante, porque debe usarse posteriormente para justificar y explicar los temas solicitados.

Los objetivos específicos están a la vista, la extracción y definición de los tres procesos importantes de la aplicación se logra

definir con mucho detalle; el cargue de semillas de Tokens apunta a ser la cabeza o insumo sobre el cual se centra la aplicación, y su administración es el embalaje evolutivo que hace de la aplicación un sistema ordenado y confiable. Los procesos de auditoría aplicada al desarrollar la metodología se elaboran en paralelo para evidenciar que cada proceso tiene un comportamiento especial y que debe controlarse de diferentes maneras.

6.7 Informe de Auditoría - Evaluación de procesos auditados.

Antes, después, aprovechamiento y ganancia con la aplicación de la metodología.

En evaluación de los procesos de Cargue de Semillas de Tokens, Creación de las solicitudes de Tokens y Cargue de los Tokens a las Solicitudes; y la respectiva atención y revisión realizada para el segundo semestre del año en curso detectan varios temas de NO conformidad frente a los procesos, y recomienda realizar los cambios pertinentes para cumplir con los lineamientos de los Dominios de la Norma de Procesos y Seguridad ISO27002. La aplicación de Administración de Tokens cumple con varios de los temas que promueve y ordena la Norma de referencia; y en varios puntos se destaca, que hay que realizar ajustes para llegar a cumplir con los estándares que se promueven. El informe en forma de cuadro que se presenta a continuación pretende resumir al detalle y facilitar la evacuación de los puntos y la posterior revisión y adopción, para finalmente realizar los ajustes que se programe efectuar. El informe esta por procesos revisados y compara lo que se encontró con lo que debería adoptarse como recomendación del proceso bien realizado. Y resalta los aprovechamientos que se alcanzarán al adoptarlos. Favoreciendo los procesos que desea proteger, adopte estas recomendaciones y verá con más seguridad la confiabilidad, integridad y disponibilidad que la aplicación de Tokens merece exponer tanto al interior de la empresa como a sus clientes en potencia.

INFORME - PRIMER PROCESO DE EVALUACION - FAVORABLES OBTENIDOS			
PUNTOS DE CONTROL	**ANTES**	**DESPUES-RECOMENDACIÓN**	**APROVECHAMIENTOS-GANACIAS**
Cargue de Semillas para Tokens	Se usa perfilamiento simple de acuerdo a los cargos dentro de la aplicación.	Se recomienda perfilar los usuarios paralelos de acuerdo a los lineamientos de Servicios de TI. Usuario red-Perfil aplicación.	Perfilar usuarios en la aplicación hace que cada usuario tenga sus tareas marcadas y bien definidas para asumir responsabilidades y roles.
	Nombres de objetos, tablas y campos de forma arbitraría.	Uso de una nemotecnia de acuerdo con la destinación de los objetos. Adopte una estrategia probada.	Adoptar una política de nemotecnia que permite mejorar, e identificar con claridad tanto a objetos, como a tabla y campos.
	Mucho colorido en la aplicación e imágenes disparejas.	Definición de colores institucionales del Banco. Logos e imágenes parejas que se unifican por todas las pantallas. Si es posible elabore plantillas con temas para facilitar los desarrollos o contrate diseños gráficos.	Se gana en imagen corporativa pareja y diciente de las aplicaciones estandar del Banco.
	Las semillas se instalan en el servidor de Tokens y se extrae un archivo tipo csv legible que se envía por correo a la Gerente de Tarjetas para hacer el cargue en el inventario de Administración de Tokens.	Los archivos generados como semillas tipo csv deben ser encriptados para ser enviados al dueño del proceso. Debe usarse un algoritmo de encripción y desencripción.	El compartir información de tipo confidencial debe cifrarse para proteger la confidencialidad en los procesos y asegurar fugas de información o fraudes con ella.
	El cargue de semillas tiene 2 componentes importantes, enriquece legalizando el inventario físico y alimenta las cuentas contables de inventarios porque son un activo más del Banco.	Asegure que los procesos se lleven acabo y genere planillas de arqueo diario entre lo físico y lo contable.	El ingreso al inventario es de vez en cuando, pero las salidas por asignaciones son a diario; es por eso que se gana en el control entre lo físico y lo contable haciendo un arqueo diario de este rubro.
	El ejercicio de cargue se hace desde cualquier equipo de cómputo dentro del Banco.	Se aconseja realizarlo desde equipos propietarios de los dueños del proceso. Para asegurar que quien ejecuta el proceso lo haga desde sus terminales asignadas.	Operaciones delicadas como este cargue debe hacerse desde equipos propietarios; porque la auditoría debe verificar que las direcciones IP sean las permitidas legalmente; sin embargo no pueden bloquearse otras direcciones porque es posible que por algún motivo de fuerza mayor tenga que hacerse desde otro equipo.
	Muestra al final del proceso: Cantidad de Tokens subidos y cantidad de Tokens que contenía el archivo.	Muestra al final de subidas las semillas, el número de las que fueron cargadas correctamente y el número de las que no fueron cargadas.	Se está haciendo bien en la aplicación actual.
	En la tabla del inventario se guardan datos del Log Usuario, Fecha y Hora cuando se subieron las semillas.	Guardar como log de auditoría Fecha, hora y Usuario que realizó el proceso.	Se está haciendo bien en la aplicación actual.
	En la tabla de inventario se guarda la dirección IP de la máquina desde donde se subió el archivo de semillas.	Grabar en la tabla de semillas la dirección IP desde donde se hizo el proceso de cargue.	Se está haciendo bien en la aplicación actual.
	Se están llenando las fechas de cargue, actualización, vencimiento, etc.	Guardar fechas, hora, usuario de los diferentes momentos que viene siendo creados, modificados los datos del inventario de semillas.	Se guarda historia de compromiso de los datos en la tabla de inventarios para responsabilizar las acciones sobre la administración de esta información.
	Los Tokens Semillas vienen consecutivos por lotes. Se cuida de que un lote venga completo.	Revisar que al subir el lote de semillas, estas vengan completas en número consecutivo.	Asegurar que las semillas estén consecutivas en su Número de Token y no vengan salteados dentro de cada lote.
	Existe una tabla BDOD16 paralela para guardar la trazabilidad de los Tokens y se llena cada vez que se ejecutan cambios en los Tokens. En algunos casos particulares no se esta guardando esta información según se revisa en una muestra.	Rigurosamente guardar en la tabla Log BDOD16 cada una de las acciones que se ejecutan sobre la tabla BDOD14 para justificar cualquier cambio hecho al tokens y poderlo explicar.	Asegurar que se esta guardando en un archivo log cada uno de los movimientos de la tabla BDOD14, esto para explicar detalles de cualquier movimiento que haya que explicar, o si se quiere saber los pasos que ha recibido un Token.
	Luego de que se carguen las semillas no se pueden borrar.	Al cargar las semillas al inventario estas no se pueden borrar en ningún momento, si fuese necesario debe hacerse un control de cambios autorizado por SQL	Se asegura que las semillas no se pueden borrar, porque siendo un inventario, ellas se manejan con un estado y cuando se entregan a los clientes se descargan del inventario y cambian su estado N= Nuevas a cualquier otro estado que se considera están fuera del inventario.

INFORME - SEGUNDO PROCESO DE EVALUACION - FAVORABLES OBTENIDOS			
PUNTOS DE CONTROL	**ANTES**	**DESPUES-RECOMENDACIÓN**	**APROVECHAMIENTOS-GANACIAS**
Creación de las Solicitudes de Tokens	Las solicitudes se crean desde 2 lados. Por la Banca Virtual en el momento del registro o cuando un Token sale dañado y se devuelve por servicio técnico.	Crear las Solicitudes de Tokens en forma obligatoria para forzar a que los clientes tengan que tener Token para el uso de la Banca Virtual	Se gana obligatoriedad en el uso de los Tokens para asegurar que la autenticación fuerte sea utilizada.
	Cuando el Tokens se reporta como perdido, debe usarse la opción: Olvidó usuario y solicitarlo como reposición de perdido.	Cobrar el Token perdido, para penalizar al cliente por su descuido. Y se hace por las opción del Olvido su clave.	Aseguramos el cuidado del Token por parte del cliente castigando su pérdida con cargo a una de las cuentas del cliente.
	Las nuevas solicitudes se crean en la tabla: BBVD87 donde se hace su manejo.	Manejar una trazabilidad con una numeración consecutiva al crear la solicitud. y unos estados que permita conocer donde va su atención.	Se gana en control de numeración consecutiva de solicitudes y por estados de la solicitud saber cual es su trazabilidad.
	Las solicitudes de Tokens no manejan mucha historia porque ellas tienen estados fijos y son muy pocos y rigidos.	Manejar los estados siguientes en la Solicitudes ('P'=Pendiente, 'X' = Asignados y x Autorizar, 'E' = En Tránsito (Courrier),'D' = Devuelta Courrier,'A' = Atendida o Autorizada,'C' = Cancelado,'R' = Rechazado) y conocer así su trazabilidad.	Los estados definen muy bien el momento de atención del proceso de Solicitudes de Tokens. Hay que ganar en consultas para Servicio al Cliente, esto permite entregar una ayuda que facilite las consultas.
	Al crear la Solicitud de Tokens se trae la información del cliente para poder enviarle el token por correo certificado a su lugar de residencia.	Permitir modificar la información al cliente con el objeto de que cuando genere la Solicitud de Tokens la información quede actualizada.	De esta manera se responsabiliza al cliente para que sus datos personales queden listos y actualizados para poder enviarle el Token a su lugar de recepción y luego poder activárselo.
	Se guarda dirección IP desde donde se crea la Solicitudes de Tokens, guardar fecha. Hora y usuario de creacón, modificación, etc.	Guardar dirección IP desde donde se crea la Solicitudes de Tokens, guardar fecha. Hora y usuario de creación, modificación, etc.	Se viene haciendo en forma correcta.

INFORME - TERCER PROCESO DE EVALUACION - FAVORABLES OBTENIDOS			
PUNTOS DE CONTROL	**ANTES**	**DESPUES-RECOMENDACIÓN**	**APROVECHAMIENTOS-GANACIAS**
Asignación de los Tokens a las Solicitudes	Usuarios perfilados para hacer la asignación de Tokens según el número de Tokens por Solicitud.	Debe matricularse usuarios que hayan sido autorizados para desarrollar la tarea de gestionadores de las solicitudes.	Se gana en segregación de funciones y validación de autorizaciones para realizar el proceso.
	En esta etapa hay supervisión por parte de un usuario autorizador que garantiza el proceso de asignación.	Debe hacerse que haya un usuario aprobador del trabajo de asignación de Tokens a la solicitud para garantizar y cubrir el proceso de asignación.	Se gana en asegurar que los procesos los mira más de una persona y son aprobados por un supervisor.
	El cliente de Personas solo puede tener un Token activo en su poder, se evalúa en la tabla de Tokens y en la de Solicitudes esta condición.	Validar que el cliente de personas solo puede tener un Token activo y nada más	Por uniformidad e integridad un cliente de personas solo puede tener un Token activo que es con el que se valida en la Banca Virtual para su ingreso y transacciones dentro de la misma.
	Para empresas se asignan los Tokens a los 2 administradores de la Banca de Empresas. Y ellos los asignan a los transaccionales de cada empresa.	Para empresas se asignan los Tokens a los 2 administrador de la Banca de Empresas. Y ellos los asignan a los transaccionales de cada empresa.	Se hace en forma correcta.
	La asignación de Tokens a las solicitudes consiste en nombrar en cada Token o semilla su propietario y cambiar el estado de N=Nuevo a X=Por autorizar.	La asignación de Tokens a las solicitudes consiste en nombrar en cada Token o semilla su propietario y cambiar el estado de N=Nuevo a X=Por autorizar.	Se hace en forma correcta. Se asignan hora, fecha y usuario desde donde se hizo las asignaciones y se graba el rastro de ausitoría.
	Se consignan marcas de auditoría donde se registra quien hace o gestiona el registro y como lo deja	Consignar marcas de auditoría donde se registra quien hace o gestiona el registro y como lo deja	Se hace en forma correcta.

7 CONCLUSIONES, RECOMENDACIONES, APORTES, Y APORTES FUTUROS

7.1 Conclusiones

- La matriz de riesgos generada permitió identificar que controles de la ISO 27002 son los más adecuado para asignarlos o asociarlos al riesgo detectado. Con esto se pudo enfatizar en los riesgos de mayor impacto buscando controles más efectivos que disminuyan su probabilidad de ocurrencia. Identificando así dentro de la aplicación cuales son los puntos de control auditables dentro de los módulos de cargue de semillas, creación de la Solicitud y asignación del Token para asegurar la confiabilidad, integridad y disponibilidad de la información y generar la matriz de riesgos.
- La elaboración del plan y el tratamiento del riesgo ayudo a implementar e identificar los controles recomendados de la ISO 27002, que redujeron el impacto y la probabilidad del riesgo. Todo esto soportado y graficado en las matrices de riesgo generadas para cada área del proceso.
- El token es un método que busca brindar seguridad a los usuarios de transacciones electrónicas, pero es contradictorio que, en su proceso interno de cargue de semillas no cuente con la confiabilidad esperada, puesto que los archivos de cargue de semillas son legibles y no vienen encriptados cuando se trasladan entre aplicativos o correos electrónicos.
- El levantamiento de información y la auditoría realizada permitió conocer cuáles eran las falencias de la organización en relación con los tres procesos que se manejan en cuanto al token bancario, requiriendo que se implementen recomendaciones de la ISO 27002, buscando así la mejoría de los procesos que impactan directamente al CORE del negocio, y la mejoría en el control de las funciones en cada cargo que interviene en el proceso.

- Dentro de la auditoria se reconocieron también procesos, que fueron impactados de forma más directa por la metodología;
    - Nos permitió identificar que de las diferentes tablas creadas en los procesos de cargue de semillas, creación de la solicitud y asignación del token a la solicitud, en algunas no se guarda un registro de los que las crean o las modificaciones posteriores que se realizan, volviendo vulnerable la información y comprometiendo su integridad. Todas las tablas que se crean o que son utilizadas como consulta deben asegurar y guardar el registro a registro de los usuarios responsables de la información, y los momentos en los cuales se afectaron los registros, fecha y hora de aplicación, creación, modificado y borrado con un log de recuerdo en el caso que los registros se borren del todo de la tabla afectada, y por medio de la recomendación de la ISO 27002 por la aplicación de la metodología propuesta esta vulnerabilidad se ve reducida.
    - Al ser una aplicación creada por la entidad se puede vislumbrar que no hay un marco de visualización establecido para las diferentes pantallas de la aplicación, logrando por medio de la metodología que esto sea uniforme recomendando la elaboración de plantillas con temas para facilitar los desarrollos y teniendo de presente la imagen institucional de la entidad.
    - Los usuarios cuentan con perfiles simples, pero se identifica que se deben perfilar ajustando las necesidades y/o responsabilidades que se les atañen, siguiendo la metodología de usuario red, perfil, aplicación.
    - Se pudo constatar que en el proceso de solicitud de token, no se puede establecer el estado en el que se encuentran las solicitudes y durante su vida dentro de la

aplicación es difícil establecer su presente. (Si existen estados, pero son pocos y rígidos), situación que según las recomendaciones de la metodología tomadas de la ISO27002 se alivia dada la necesidad de ser claros con la información que se cuenta.

  - Al crear la Solicitud de Tokens se trae la información del cliente para poder enviarle el token por correo certificado a su lugar de residencia, con la metodología se debe permitir modificar la información al cliente con el objeto de que cuando genere la Solicitud de Tokens la información quede actualizada.
  - Luego de que se carguen las semillas no se pueden borrar, si fuera necesario por algún motivo los cambios deben ser autorizados por un superior que cuente con las atribuciones necesarias, generando así un mayor control sobre la información de la aplicación.
  - En las entrevistas para el levantamiento de la información se nota cierto desconocimiento de procesos y documentación existente por parte de los colaboradores, haciéndose necesario buscar herramientas que permitan que la información sea de conocimiento general para las personas que intervienes en los procesos.

- La metodología crea recomendaciones basadas en un estándar, al ser una herramienta que busca disminuir el impacto y la probabilidad de los riesgos que existen dentro de la aplicación, es de gran asimilación en otras entidades dado el parecido del proceso que conlleva tener una semilla y que esta deba ser asimilada aun aparato físico.

Todo proyecto tiene un grado de incertidumbre muy alto, el cual a medida que se va ahondando en él, va viéndose un horizonte más despejado que va asomando resultados que con toda seguridad

tendrán un beneficio especial para quienes los adopten y los lleven a la práctica, es el caso de este proyecto que ha significado un esfuerzo de muchos, aplicando conocimientos aprendidos en todas las dimensiones y llegando a obtener un producto que enorgullece a sus autores.

Hay grandes esfuerzos de dirección del proyecto, a quien damos un parte de agradecimiento por su esfuerzo, dedicación, y sabiduría en los temas versados. La Dra. Alexandra María López Sevillano miembro de la facultad de ingeniería de la universidad, ha sido de gran apoyo que rigurosamente fue llevando el proyecto a feliz término.

Se ha creído que la Auditoría es un régimen policivo que pareciera obstaculizar los procesos administrativos, pero nos hemos dado cuenta, de que de ella se extrae gran apoyo que coadministra las acciones de las compañías y asegura que se siga el camino correcto en los procesos de exposición de imagen ante terceros.

Finalmente, un hilo más en la cadena de conocimientos asegura la alta credibilidad de los procesos y enriquece al hombre poniéndolo en un pedestal que visiona mejores cosas para el futuro propio, de las empresas y de todos en general.

7.2 Recomendaciones

- Se recomienda que, al momento de utilizar la metodología creada, en la institución que la implemente se adquiera el paquete de documentación de la ISO/IEC 27002, en donde podrán encontrar más información, y recomendaciones, esto con el fin de poder ampliar y reforzar sus conocimientos en los temas referentes a la seguridad de la información tanto a un nivel físico como lógico de los procesos aplicados para el uso del Token.
- Se recomienda revisar frecuentemente el cumplimiento de las políticas establecidas dentro de la organización, y el cumplimiento del apetito del riesgo, esto con el fin de buscar un eficiente aseguramiento de la información y un eficaz control en la información.

- Es importante que la entidad brinde capacitaciones constantes y charlas referidas a la encriptación de la información sensible manejada por el área de TI, puesto que se establece en el levantamiento y posteriores controles de información existente, que no hay una concientización sobre la seguridad de los activos de información y existe información importante que no se está asegurando apropiadamente.
- Deben guardarse log´s de auditoria para las tablas que se decidan hacer, y que requieran de trazabilidad para evidenciar seguimiento en caso de tener que justificar algunas inconsistencias que se puedan presentar. El log debe guardar todo el detalle del antes y el después de la operación realizada en el aplicativo.
- Los procesos deben tener responsables directos, y deben contar con el backup correspondiente en caso de falta de personal, para que se encarguen de trabajar con la misma dinámica y conozcan sus roles por usuario y perfil dentro de la aplicación.
- Se recomienda que la aplicación guarde uniformidad en las pantallas y los modos de trabajar, buscando el fácil entendimiento para cualquier usuario que llegue como nuevo, a intervenir de manera importante dentro de la aplicación, y el manejo de los tokens´s.
- Se recomienda que todo el movimiento que se realice con afectación contable debe realizarse en línea, contabilizando directamente a los inventarios de los tokens, ya sea sumando o restando en el inventario físico.
- Todos los días debe estar cuadrado el inventario físico de token´s vs el inventario de las cuentas contables.
- La transferencia de archivos entre aplicativos, y/o envíos en correo electrónico debe adoptar las recomendaciones de la ISO 27002 en su dominio 10 de cifrado de información.
- Crear políticas para la encriptación, que tengan en cuenta la posibilidad de proveedores

externos y los condicionamientos que estos deben tener.

- Si bien existen políticas y documentación sobre la continuidad de la operación en caso de imprevistos o siniestros, se hace necesario elevar ese conocimiento, pruebas y resultados a todos los que intervienen en los procesos, ya que no se tiene el conocimiento necesario por parte de todos los interesados y en caso de no disponibilidad del aplicativo se demoran mucho más los tiempos de recuperación y normalización de la operación.
- Se hace necesario establecer un medio claro de comunicación inicial hacia los colaboradores, cuando se presenta un evento que afecte la disponibilidad lógica o física de las instalaciones.

7.3 Aportes

- La Metodología, se puede aplicar a cualquier desarrollo de un proyecto de Administración de Tokens, que va desde el cargue de semillas de Tokens, a un sistema de inventario para su control, hasta el manejo de los diferentes escenarios que los Tokens atraviesan durante su ciclo de vida.
- La normatividad colombiana para el establecimiento de herramientas de seguridad a sus usuarios no es rígida y permite a las entidades financieras brindar a sus usuarios la mejor alternativa que ellos consideren lo suficientemente apta. El token al ser una herramienta común y eficaz suele ser el medio utilizado por estas entidades para blindar a sus clientes, y como no hay un marco establecido para la creación de estos procesos dentro de una entidad, suele existir vacíos en la seguridad de estos procesos. Por lo que esta metodología basada en recomendaciones de la ISO 27002 es una alternativa confiable para la implantación del sistema de seguridad dentro de una entidad financiera.
- Si bien dentro de las compañías existen controles hacia los riesgos de TI, esta metodología

brinda un marco de referencia directamente a la creación y establecimiento de los puntos de control de las aplicaciones para token´s.

- Siendo la información bancaria sensible y confidencial, pudimos establecer que el manejo en los procesos de tokens en la entidad financiera es similar, debido al tránsito que conlleva tener una semilla y asignarla a un elemento físico, por lo que el proceso interno es parecido y con la metodología propuesta se hace ajustable a los diferentes procesos que se manejan en otras entidades.

7.4 Aportes futuros

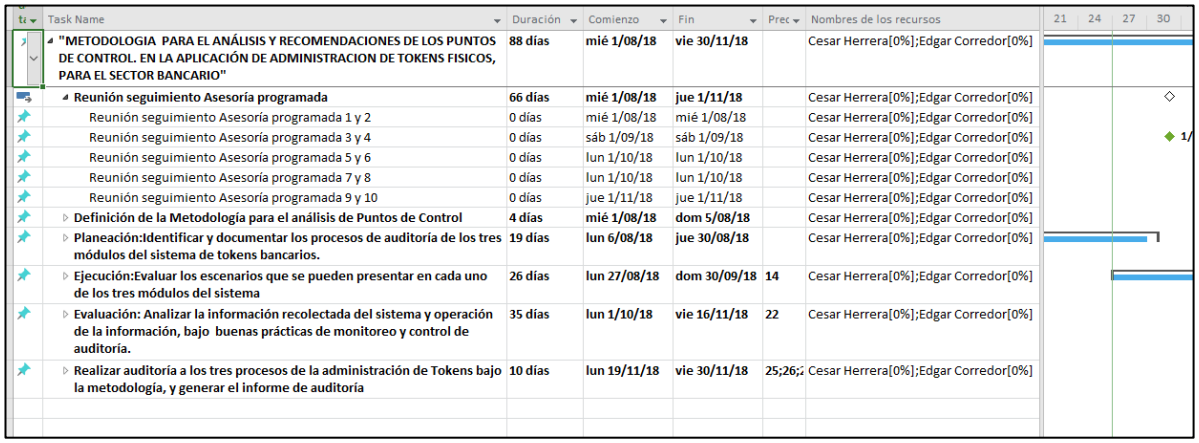
- Adaptación de la metodología propuesta para los tokens de software, que son token que se cargan virtualmente dentro de los dispositivos móviles o computadores personales.
- Adaptar e incluir dentro de la metodología presentada las norma establecidas en la ISO 27001 debido a que esta norma define el sistema de gestión de seguridad de la información, Este sistema de gestión significa que la seguridad de la información debe ser planificada, implementada, supervisada, revisada y mejorada.
- Buscar la asimilación de la metodología hacia otros procesos de TI y aplicativos del Banco, buscando así la ejecución en línea.
- Facilitar que la metodología pueda manejar varios proveedores de estos dispositivos al mismo tiempo, e integrarlos a un mismo proceso de administración token´s.

8 ANEXOS

Los siguientes son los documentos complementarios a la planeación, desarrollo y ejecución del proyecto, válidos para sustentar los resultados obtenidos.

Cronograma de anteproyecto y planeación inicial.

Las actividades se realizan en general de la siguiente manera para plasmar un trabajo significativo que presenta una Metodología de confianza que adopta mecanismos que aseguran el desarrollo de los proyectos de Administración de Tokens:



Task Name	Duración	Comienzo	Fin	Prec	Nombres de los recursos
"METODOLOGIA PARA EL ANÁLISIS Y RECOMENDACIONES DE LOS PUNTOS DE CONTROL. EN LA APLICACIÓN DE ADMINISTRACION DE TOKENS FISICOS, PARA EL SECTOR BANCARIO"	88 días	mié 1/08/18	vie 30/11/18		Cesar Herrera[0%];Edgar Corredor[0%]
Reunión seguimiento Asesoría programada	66 días	mié 1/08/18	jue 1/11/18		Cesar Herrera[0%];Edgar Corredor[0%]
Reunión seguimiento Asesoría programada 1 y 2	0 días	mié 1/08/18	mié 1/08/18		Cesar Herrera[0%];Edgar Corredor[0%]
Reunión seguimiento Asesoría programada 3 y 4	0 días	sáb 1/09/18	sáb 1/09/18		Cesar Herrera[0%];Edgar Corredor[0%]
Reunión seguimiento Asesoría programada 5 y 6	0 días	lun 1/10/18	lun 1/10/18		Cesar Herrera[0%];Edgar Corredor[0%]
Reunión seguimiento Asesoría programada 7 y 8	0 días	lun 1/10/18	lun 1/10/18		Cesar Herrera[0%];Edgar Corredor[0%]
Reunión seguimiento Asesoría programada 9 y 10	0 días	jue 1/11/18	jue 1/11/18		Cesar Herrera[0%];Edgar Corredor[0%]
Definición de la Metodología para el análisis de Puntos de Control	4 días	mié 1/08/18	dom 5/08/18		Cesar Herrera[0%];Edgar Corredor[0%]
Planeación:Identificar y documentar los procesos de auditoría de los tres módulos del sistema de tokens bancarios.	19 días	lun 6/08/18	jue 30/08/18		Cesar Herrera[0%];Edgar Corredor[0%]
Ejecución:Evaluar los escenarios que se pueden presentar en cada uno de los tres módulos del sistema	26 días	lun 27/08/18	dom 30/09/18	14	Cesar Herrera[0%];Edgar Corredor[0%]
Evaluación: Analizar la información recolectada del sistema y operación de la información, bajo buenas prácticas de monitoreo y control de auditoría.	35 días	lun 1/10/18	vie 16/11/18	22	Cesar Herrera[0%];Edgar Corredor[0%]
Realizar auditoría a los tres procesos de la administración de Tokens bajo la metodología, y generar el informe de auditoría	10 días	lun 19/11/18	vie 30/11/18	25;26;2	Cesar Herrera[0%];Edgar Corredor[0%]

Figura. 9

8.1 Presupuesto

Para la preparación y presentación del presupuesto se deben tener en cuenta las siguientes indicaciones:

Equipos: La financiación para compra de equipos nuevos deberá estar sustentada en la estricta necesidad de los mismos para el desarrollo de la investigación. Es importante que los investigadores verifiquen si el equipo que necesitan ya existe en otra dependencia de su universidad, de la cual pudiese solicitarse en préstamo, arrendamiento o la prestación de

servicios técnicos. Este último se refiere al que ya existe en la institución y que por utilizarse en la investigación se acepta también como contrapartida institucional por un valor máximo del 10% de su precio comercial al estar nuevo. Las cotizaciones de los equipos deberán estar disponibles para consulta en el caso en que esta entidad considere necesario verificar los costos de los equipos solicitados.

Salidas de campo: Se aplica a gastos de medios de transporte para el traslado a zonas de muestreo y ejecución de las labores de campo propias de la investigación. Se refiere principalmente a costos de combustible, aceite o alquiler de medios de transporte cuando se requiere. Deberán desglosarse y justificarse en la Figura 5.7

Desarrollo de la investigación o de la tecnología y deben presentarse a manera de listado detallado agrupado por categorías sobre las cuales se debe hacer una justificación de su necesidad y uso dentro del proyecto. El tipo de servicios técnicos (exámenes, pruebas, análisis o servicios especializados).

Material Bibliográfico: Se podrá financiar bibliografía debidamente justificada y directamente relacionada con la temática del proyecto en la forma de libros y/o suscripciones a revistas científicas del tema.

Tabla 2.

Presupuesto global de la propuesta por fuentes de financiación.

Rubro	Cantidad	Valor unitario	Valor total
Personal (Contador, Ingeniero)	2	$4.000.000	$8.000.000
Equipos – Pc (Portatil)	2	$2.250.000	$4.500.000
Software	1	$4.500.000	$4.500.000
Salidas al campo	10	$1.000.000	$1.000.000
Material Bibliográfico	1	$140.000	$140.000
Servicios Técnicos	1	$200.000	$200.000
Viajes	1	$200.000	$200.000
Administración	1	$500.000	$500.000
Materiales	1	$100.000	$100.000
		Total	**$19.140.000**

Tabla 3.

Descripción de los Gastos de personal.

Funcionario	Formación académica	Función en proyecto	Valor total
Contador	Contador Público	• Gobernanza legal y financiera. • Aplicación de temas contables. • Elaboración de encuestas. • Seguimiento de reuniones del proyecto. • Aseguramiento de sitio para pruebas.	4.000.000
Ingeniero	Ingeniero de Sistemas	○ Manejo del Proyecto en aplicación de Normas ISO. ○ Elaboración de encuestas y aplicación de las mismas. ○ Manejo del tiempo para pruebas. ○ Recorrido de la aplicación. ○ Seguimiento de reuniones. ○ Manejo de los tiempos de afinación de los desarrollos.	4.000.000
		Total……	8.000.000

Tabla 4

Descripción de los equipos que se planea adquirir.

Rubros	Cantidad	Valor unitario	Valor tyotal
Portátil 1 Lenovo	1	2.000.000	2.000.000
Portátil 2 Lenovo	1	2.000.000	2.000.000
Impresora HP	1	500.000	500.000
		Total	4.500.000

Tabla 5.

Descripción del software que se planea adquirir

Rubros	Cantidad	Valor unitario	Valor total
Licencia MSOffice 2016 (5 usuarios)	1	1.500.000	2.000.000
Licencia MSOffice Visión 2016 (5 usuarios)	1	1.500.000	2.000.000
Licencia MS Project (5 usuarios)	1	2.000.000	500.000
		Total	4.500.000

Tabla 6

Descripción y Justificación de los viajes. Salidas de Campo.

Rubros	Cantidad	Valor unitario	Valor total
Desplazamiento de las oficinas de TI del Banco Para reuniones de trabajo en las cuales se levanta información y se plantea los desarrollos y ajustes a que haya lugar	30	20.000	600.000
Transporte a las oficinas de usuario. Se efectúan viajes que deben hacerse para elaboración de pruebas que apropian información de ajustes a la norma ISO 27002	10	20.000	200.000
Transporte a las oficinas del COC Para las pruebas de contingencia se hacen viajes a las oficinas del centro de operaciones alterno para verificar que allí todo funcione bien.	10	20.000	200.000
		Total	1.000.000

Tabla 7.

Material Bibliográfico.

Rubros	Cantidad	Valor unitario	Valor total
Compra suscripción de la norma ISO 27002 DE International Electrotechnical Commission	2	50.000	100.000
Suscripción para el inicio de la certificación ISO 27002	2	20.000	40.000
		Total	140.000

Tabla 8.

Servicios Técnicos.

Rubros	Cantidad	Valor unitario	Valor total
Mantenimiento equipos de cómputo portátiles	2	45.000	90.000
Mantenimiento impresora	2	20.000	40.000
Mantenimiento redes de conexión	2	35.000	70.000
		Total	200.000

Tabla 9.

Viajes, Administración y Materiales.

Rubros	Cantidad	Valor unitario	Valor total
Viajes: se separa rubro para este Item para viajes fortuitos hacia alguna de las sedes	1	200.000	200.000
Administración: Apropiamos presupuesto para el mantenimiento de oficinas y equipos.	1	500.000	500.000
Materiales y papelería general	1	100.000	100.000
		Total	800.000

8.1.1 Análisis del presupuesto a octubre

Presupuesto hasta la conclusión (BAC) y Valor planificado por mes (PV)								
Presupuesto total	BAC	PV1 - Julio	PV2 - Agosto	PV3 - Septiembre	PV4 - Octubre	PV5 - Noviembre	PV6 - Diciembre	TOTAL presupuestado
Personal	$ 8.000.000	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 8.000.000
Equipos - PCS	$ 4.500.000	$ 4.500.000						$ 4.500.000
Software	$ 4.500.000	$ 4.500.000						$ 4.500.000
Salidas de campo	$ 1.000.000		$ 200.000	$ 500.000	$ 100.000	$ 100.000	$ 100.000	$ 1.000.000
Material Bibliografico	$ 140.000			$ 140.000				$ 140.000
Servicios tecnicos	$ 200.000	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 200.000
Viajes	$ 200.000	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 200.000
Adimistración	$ 500.000	$ 83.333	$ 83.333	$ 83.333	$ 83.333	$ 83.333	$ 83.333	$ 500.000
Materiales	$ 100.000	$ 16.667	$ 16.667	$ 16.667	$ 16.667	$ 16.667	$ 16.667	$ 100.000
	$ 19.140.000			**PV Octubre**	**$ 15.940.000**			**$ 19.140.000**

Costo real (AC)							
Presupuesto total	BAC	PV1 - Julio	PV2 - Agosto	PV3 - Septiembre	PV4 - Octubre	**AC** Costo real a 31 de Octubre	Valor por ejecutar
Personal	$ 8.000.000	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 5.333.333	$ 2.666.667
Equipos - PCS	$ 4.500.000	$ 4.500.000				$ 4.500.000	$ -
Software	$ 4.500.000	$ 4.500.000				$ 4.500.000	$ -
Salidas de campo	$ 1.000.000		$ 300.000	$ 500.000	$ -	$ 800.000	$ 200.000
Material Bibliografico	$ 140.000			$ 140.000		$ 140.000	$ -
Servicios tecnicos	$ 200.000					$ -	$ 200.000
Viajes	$ 200.000				$ 45.000	$ 45.000	$ 155.000
Adimistración	$ 500.000	$ 50.000	$ 40.000	$ 35.000	$ 55.000	$ 180.000	$ 320.000
Materiales	$ 100.000			$ 10.000	$ 20.000	$ 30.000	$ 70.000
	$ 19.140.000					**$ 15.528.333**	**$ 3.611.667**

Estimado hasta la conclusión (ETC)				
Presupuesto total	BAC	PV5 - Noviembre	PV6 - Diciembre	Estimado hasta la conclusión **(ETC)**
Personal	$ 8.000.000	$ 1.333.333	$ 1.333.333	$ 2.666.667
Equipos - PCS	$ 4.500.000			$ -
Software	$ 4.500.000			$ -
Salidas de campo	$ 1.000.000	$ 100.000	$ 100.000	$ 200.000
Material Bibliografico	$ 140.000			$ -
Servicios tecnicos	$ 200.000	$ 33.333	$ 33.333	$ 66.667
Viajes	$ 200.000	$ 33.333	$ 33.333	$ 66.667
Adimistración	$ 500.000	$ 83.333	$ 83.333	$ 166.667
Materiales	$ 100.000	$ 16.667	$ 16.667	$ 33.333
	$ 19.140.000			**$ 3.200.000**

Estimado a la conclusión EAC						(Estimación)		
Presupuesto total	BAC	PV1 - Julio	PV2 - Agosto	PV3 - Septiembre	PV4 - Octubre	PV5 - Noviembre	PV6 - Diciembre	Estimado a la conclusión EAC
Personal	$ 8.000.000	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	**$ 1.333.333**	**$ 1.333.333**	$ 8.000.000
Equipos - PCS	$ 4.500.000	$ 4.500.000						$ 4.500.000
Software	$ 4.500.000	$ 4.500.000						$ 4.500.000
Salidas de campo	$ 1.000.000		$ 300.000	$ 500.000	$ -	**$ 100.000**	**$ 100.000**	$ 1.000.000
Material Bibliografico	$ 140.000			$ 140.000				$ 140.000
Servicios tecnicos	$ 200.000					**$ 33.333**	**$ 33.333**	$ 66.667
Viajes	$ 200.000				$ 45.000	**$ 33.333**	**$ 33.333**	$ 111.667
Adimistración	$ 500.000	$ 50.000	$ 40.000	$ 35.000	$ 55.000	**$ 83.333**	**$ 83.333**	$ 346.667
Materiales	$ 100.000			$ 10.000	$ 20.000	**$ 16.667**	**$ 16.667**	$ 63.333
	$ 19.140.000							**$ 18.728.333**

VARIACIÓN A LA CONCLUSIÓN (VAC) = Presupuesto hasta la conclusión (BAC) - Estimado a la conclusión (EAC)

Presupuesto hasta la conclusión (BAC)	$ 19.140.000	(+)
Estimado a la conclusión (EAC)	$ 18.728.333	(-)
VARIACIÓN A LA CONCLUSIÓN (VAC)	$ 411.667	(=)

CALCULO DEL VALOR GANADO

Ejecución del proyecto	80%	(+)
Presupuesto Inicial	$ 19.140.000	(*)
(VE) =	**$ 15.312.000**	(=)

Variaciones

Valor ganado (EV)	$ 15.312.000	(+)
Costo real (AC)	$ 15.528.333	(-)
Variación del costo (C	$ (216.333)	(=)

Valor ganado (EV)	$ 15.312.000	(+)
Valor planificado (PV)	$ 15.940.000	(-)
Variación del Cronogr	$ (628.000)	(=)

Indices

Valor ganado (EV)	$ 15.312.000	(+)
Costo real (AC)	$ 15.528.333	(/)
Indice del desempeño del	0,99	(=)

Valor ganado (EV)	$ 15.940.000	(+)
Valor planificado (PV)	$ 15.940.000	(/)
Indice del desempeño del	1,00	(=)

8.1.2 Análisis del presupuesto a diciembre, entrega del proyecto.

Presupuesto hasta la conclusión (BAC) y Valor planificado por mes (PV)								
Presupuesto total	BAC	PV1 - Julio	PV2 - Agosto	PV3 - Septiembre	PV4 - Octubre	PV5 - Noviembre	PV6 - Diciembre	TOTAL presupuestado
Personal	$ 8.000.000	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 8.000.000
Equipos - PCS	$ 4.500.000	$ 4.500.000						$ 4.500.000
Software	$ 4.500.000	$ 4.500.000						$ 4.500.000
Salidas de campo	$ 1.000.000		$ 200.000	$ 500.000	$ 100.000	$ 100.000	$ 100.000	$ 1.000.000
Material Bibliografico	$ 140.000			$ 140.000				$ 140.000
Servicios tecnicos	$ 200.000	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 200.000
Viajes	$ 200.000	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 33.333	$ 200.000
Adimistración	$ 500.000	$ 83.333	$ 83.333	$ 83.333	$ 83.333	$ 83.333	$ 83.333	$ 500.000
Materiales	$ 100.000	$ 16.667	$ 16.667	$ 16.667	$ 16.667	$ 16.667	$ 16.667	$ 100.000
	$ 19.140.000					**PV Diciembre**	**$ 19.140.000**	**$ 19.140.000**

Costo real (AC)									
Presupuesto total	BAC	PV1 - Julio	PV2 - Agosto	PV3 - Septiembre	PV4 - Octubre	PV5 - Noviembre	PV6 - Diciembre	**AC** Costo real a 02 de Diciembre	Valor sin ejecutar
Personal	$ 8.000.000	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 1.333.333	$ 88.888	$ 6.755.555	$ 1.244.445
Equipos - PCS	$ 4.500.000	$ 4.500.000						$ 4.500.000	$ -
Software	$ 4.500.000	$ 4.500.000						$ 4.500.000	$ -
Salidas de campo	$ 1.000.000		$ 300.000	$ 500.000	$ -			$ 800.000	$ 200.000
Material Bibliografico	$ 140.000			$ 140.000				$ 140.000	$ -
Servicios tecnicos	$ 200.000							$ -	$ 200.000
Viajes	$ 200.000				$ 45.000			$ 45.000	$ 155.000
Adimistración	$ 500.000	$ 50.000	$ 40.000	$ 35.000	$ 55.000	$ 10.000	$ 10.000	$ 200.000	$ 300.000
Materiales	$ 100.000			$ 10.000	$ 20.000			$ 30.000	$ 70.000
	$ 19.140.000							**$ 16.970.555**	**$ 2.169.445**

VARIACIÓN A LA CONCLUSIÓN (VAC) = Presupuesto hasta la conclusión (BAC) - Estimado a la conclusión (EAC)

Presupuesto hasta la conclusión (BAC)	$ 19.140.000	(+)
Estimado a la conclusión (EAC)	$ 16.970.555	(-)
VARIACIÓN A LA CONCLUSIÓN (VAC)	$ 2.169.445	(=)

CALCULO DEL VALOR GANADO

Ejecución del proyecto		100%	(+)
Presupuesto Inicial	$	19.140.000	(*)
(VE) =	**$**	**19.140.000**	(=)

Variaciones

Valor ganado (EV)	$	19.140.000	(+)
Costo real (AC)	$	16.970.555	(-)
Variación del costo (CV)	$	2.169.445	(=)

Valor ganado (EV)	$	19.140.000	(+)
Valor planificado (PV)	$	19.140.000	(-)
Variación del Cronogran	$	-	(=)

Indices

Valor ganado (EV)	$	19.140.000	(+)
Costo real (AC)	$	16.970.555	(/)
Indice del desempeño del costo (CPI)		1,13	(=)

Valor ganado (EV)	$	19.140.000	(+)
Valor planificado (PV)	$	19.140.000	(/)
Indice del desempeño del Cronograma (SPI)		1,00	(=)

8.1.3 Cronograma final

Nombre de la tarea	Duraciòn dias	Comienzo	Fin	Nombre del recurso	Julio			Agosto			Septiembre			Octubre			Noviembre			Diciembre		
Justificaciòn	30	12/06/2018	12/07/2018	Edgar Isauro																		
Polanteamiento, antecedentes, y variables, del problema				Cesar Augusto																		
Plantemaiento de Objetivos	20	12/07/2018	01/08/2018	Cesar Augusto																		
				Edgar Isauro																		
Elaboracion de Marcos de referencia		02/08/2018	02/09/2018																			
Marco Conceptual	30	02/08/2018	12/08/2018	Cesar Augusto																		
Marco Juridico		13/08/2018	23/08/2018	Cesar Augusto																		
Marco teorico		24/08/2018	30/08/2018	Cesar Augusto																		
Marco geografico		31/08/2018	02/09/2018	Cesar Augusto																		
Elaboraciòn metodologia	30	02/08/2018	02/09/2018	Edgar Isauro																		
DESARROLLO DE LA PROPUESTA																						
Levantamiento de informaciòn	30	02/09/2018	02/10/2018	Edgar Isauro																		
Elaboraciòn guias de auditoria	30	02/09/2018	02/10/2018	Cesar Augusto																		
EVALUACION SIC																						
Elaboraciòn matrices de riesgo	15	02/10/2018	17/10/2018	Edgar Isauro																		
Elaboraciòn mapas de calor	15	02/10/2018	17/10/2018	Cesar Augusto																		
Elaboraciòn de la metodologia	20	17/10/2018	02/11/2018	Edgar Isauro																		
		17/10/2018	02/11/2018	Cesar Augusto																		
Evaluaciòn de la metodologia propuesta	18	02/11/2018	20/11/2018	Edgar Isauro																		
		02/11/2018	20/11/2018	Cesar Augusto																		
PRESENTACIÒN PROYECTO	1	19/12/2018	19/12/2018	Edgar Isauro																		
		19/12/2018	19/12/2018	Cesar Augusto																		

8.2 Cuestionarios para las entrevistas y tabulaciones.

Instrumentos o Herramientas utilizadas:

Los cuestionarios para aplicar a la población son:

Cuestionario 1:

CUESTIONARIO GENERAL

Objetivo: Detectar, analizar e identificar pasó a paso las operaciones que se realizan en la administración de Tokens en el Banco.

Fecha _____ Hora _____ Ciudad _____

Datos generales de la Empresa_____

Datos generales del encuestado_____

Área de aplicación de la encuesta_____

No.	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1	¿Cada cuánto se negocia los lotes de Tokens? a). Mensual: ( ) b). Semestral: ( ) c). Anual: ( ) d). No Hay Periodicidad (X)				
2	¿Cuál es la cantidad de Tokens que se compran por lote?: a). 10.000: (X) b). 20.000: ( ) c). 30.000: ( ) d). 40.000 y más: ( )				
3	¿Cuantos Tokens están Activos hoy día?: a). Menos de 5.000: ( ) b). 10.000: ( ) c). 30.000: (X) d). Más de 50.000 ( ).				

4	¿Cuál es el número de clientes del Banco aproximadamente?: a). Menos de 50.000: ( ) b). 100.000: (X) c). 300.000: ( ) d). Más de 500.000 ( ).				
5	¿Hay más número de clientes de empresas, que de personas?				
6	¿Cada cuánto tiempo se cambia un Token por deterioro o vencimiento?: a). Bimestral: ( ) b). Semestral: ( ) c). Anual: ( ) d). No Hay Periodicidad (X)				
7	¿Se siente seguridad en la manipulación de los Tokens dentro del Banco ?:				
8	¿Se siente seguridad en la manipulación de los Tokens fuera del Banco?				
9	¿Se percibe seguridad en los Clientes con los manejos de productos de los Clientes que usan Tokens ?:				
10	¿Bajo cuantas personas está el manejo de los Tokens en el Banco ?: a). Menos de 5 ( ) b). Entre 5 y 10 (X) c). Entre 11 y 15 ( ) d). Más de 16 ( ).				
11	¿Hay demoras y Bloqueos en la manipulación de los Tokens en los diferentes canales BV, Banca Móvil, etc				
12	¿Está dividido el trabajo y las responsabilidades en el manejo de la Administración de los Tokens ?:				
13	¿Hay personal Backups que suplan las				

	ausencias de los titulares en caso de ausencias?				
14	¿Se presentan muchas ausencias en los puestos claves de administración de Tokens?				
15	¿Hay sección de autorizaciones en los módulos de administración de Tokens?:				
16	¿Hay segmentación en los módulos de administración de Tokens ?:				
17	¿Los datos se pasan encriptados entre máquinas al necesitar cargar información externa a los módulos?				
18	¿La Aplicación es Modular?:				
19	¿Hay segmentación especial por área en los módulos de administración de Tokens?:				
20	¿La numeración de Tokens es consecutiva?:				
21	¿Hay informes diarios, mensuales o de oportunidad al requerir alguna información del sistema de Tokens?:				
22	¿Hay perfiles que manejan la trazabilidad de la aplicación de Tokens, ejemplo: Administrador, Operador?:				
23	¿En los informes solicitados se puede colocar datos de quien realiza las operaciones y en qué fecha y hora?:				
24	¿Se presentan muchas fallas de tipo procedimental en el manejo del sistema? Ejemplo: No se pudo activar un Token ?				
25	¿Se presentan muchas llamadas por Servicio				

	al Cliente de fallas producidas por los Tokens ?:				
26	¿Los Tokens dañados son reemplazados con facilidad ?:				
27	¿Cuánto tarda en promedio un Token en llegar a su destino y ser activado?: a). Menos de 3 días b). Entre 4 y 6 (X) c). Entre 7 y 10 ( ) d). Más de 11 ( ).				
28	¿Se le da importancia a la efectividad de las consultas y transacciones de los clientes por los canales virtuales ?:				
29	¿El Token es esencialmente obligatorio en el Banco para todos los clientes? Empresas y Personas?				

Cuestionario 2

CUESTIONARIO SEGURIDAD LOGICA

Objetivo: Seguridad Lógica: Identificación, autenticación, autorización, trazabilidad y recuperación.

Fecha_____ Hora, _____Ciudad___ _____

Datos generales de la Empresa _____

Datos generales del encuestado _____

Área de aplicación de la encuesta_____

	PREGUNTAS	SI	NO	N/A	OBSERVACIONES

1	¿Tiene políticas definidas para la creación de usuarios que interactúan con la aplicación?				
2	¿Tiene políticas definidas para la creación de usuarios que interactúan con la Base de Datos?				
3	¿Existen formatos de solicitud de creación de usuarios de la aplicación?				
4	¿Existen formatos de solicitud de creación de usuarios de la Base de Datos?				
5	¿Los formatos de solicitud de creación de usuarios para la aplicación tienen niveles de autorización?				
6	¿Los formatos de solicitud de creación de usuarios para la base de datos tienen niveles de autorización?				
7	¿Si una solicitud de creación de usuario no tiene las autorizaciones correspondientes, se realiza el proceso de creación del usuario?				
8	¿Cuenta con un listado actualizado de los usuarios que ingresan a la base de datos?				
9	¿Cuenta con un listado actualizado de los usuarios que existen en la base de datos?				
10	¿El Usuario de la aplicación es el mismo de la Base de Datos?				
11	¿Existen procedimientos definidos para crear, gestionar y eliminar usuarios (creación, actualización y eliminación) de la base de datos y la aplicación?				
12	¿Los procedimientos de gestión de los usuarios				

	de la base de datos se encuentran documentados?				
13	¿Los procedimientos de gestión de los usuarios de la aplicación se encuentran documentados?				
14	¿Existen controles inmediatos de acceso a los usuarios de la aplicación cuando este termina su contrato con la empresa?				
15	¿Existen controles inmediatos de acceso a los usuarios de la Base de Datos cuando este termina su contrato con la empresa?				
16	¿Cada usuario de la base de datos es único y pertenece a una única persona?				
17	¿La Base de datos es consistente, de tal manera que si los usuarios en su operación sobre la aplicación se desconectan abruptamente no se pierdan los datos?				
18	¿Si los usuarios en sus terminales tienen tiempos de inactividad, estas se bloquean automáticamente?				
19	¿Ocurre lo mismo en la aplicación? ¿Si el usuario no está realizando ninguna tarea, su aplicación se bloquea?				
20	¿Los usuarios dentro de la aplicación son independientes para realizar diferentes temas?				
21	¿Existen perfiles dentro de la aplicación?				
22	¿Cada perfil tiene sus tareas asignadas?				
23	¿Cada perfil de la aplicación tiene correspondiente en usuario de logueo al				

	sistema? Es decir uno a uno.?				
24	¿Utilizan los mismos usuarios del sistema para trabajar dentro de la aplicación?				
25	¿El administrador puede poner o quitar privilegios dentro de la aplicación?				
26	¿La base de datos es consistente? ¿Si se va la energía, al recuperarse el servicio no parece haber pasado nada?				
27	¿Existen perfiles dentro de la aplicación?				
28	Si hay perfiles. ¿Cada perfil tiene su tarea bien definida?				
29	Cada perfil tiene derechos de crear, modificar, ¿eliminar registros?				
30	¿En la creación de registros existen logs de seguimiento?				
31	¿Si hay logs de seguimiento? ¿Estos pueden obtener la trazabilidad de un tema a resolver?				
32	¿Los Log de seguimiento tienen vigencia? ¿Es decir, se guardan solo por un tiempo?				
33	Las políticas de Backup cubren a la configuración de sistema, servidores, ¿etc? ¿Cada cuánto se hace?				
34	¿Las políticas de backup de datos dicen hacerlo a diario?				
35	¿Se hace Backus de la aplicación? ¿Cada cuánto?				Diario
36	¿Se manejan planes de contingencia locales?				
37	¿Tienen control de contingencia externo?				

38	¿Dónde hacen las pruebas de contingencia?				IBM y Data Center
39	¿Es allí donde se ejecutaría la contingencia en caso de tal evento?				
40	¿Los contratos con el proveedor de contingencia están al día?				
41	¿Los contratos con los proveedores de mantenimiento de equipos están al día?				
42	¿Los contratos con el proveedor de la aplicación están al día?				
43	¿Existen logs de las operaciones más críticas o de todo?				
44	¿Cada tabla en cada registro guarda usuario que creó, modificó y eliminó?				Algunas tablas
45	¿El servicio de Autenticación de dispositivos es estable?				
46	¿La identificación en los dispositivos es única?				
47	¿Para cada dispositivo de autenticación (Token) solo existe una sola identificación?				
48	¿Los dispositivos de autenticación son desechables?				
49	¿Si se daña un dispositivo de identificación es fácil cambiarlo?				
50	¿Los dispositivos son sellados?				
52	¿Si se mojan los dispositivos se dañan?				
53	¿Los dispositivos son identificados por algún serial?				
54	¿A los dispositivos se les hace mantenimiento en				

	caso de presentar daños?				
55	¿La consola de autenticación está en Colombia?				
56	¿Es fácil saber cuál es el algoritmo que se usa cada vez que se cambia el número en la pantalla del dispositivo?				
57	¿La aplicación posee informes?				
58	¿Los informes son fácilmente obtenibles?				
59	¿Son informes en Excel?				
60	¿Hay información estadística?				
61	¿Se producen archivos planos en la aplicación?				
62	¿Los archivos planos Sirven para hacer envíos de otro tipo de información?				
63	¿Para la entrega de los dispositivos hay algún procedimiento de seguridad establecido?				
64	¿El envío se hace a través de alguna empresa especializada?				
65	¿Hacen todos los días envío de estos dispositivos?				
66	Las solicitudes se cierran con frecuencia en feliz término. ¿O muchas de ellas se cancelan?				
67	¿Para la trazabilidad hay estados en las solicitudes?				
68	¿Para la trazabilidad hay estados en los dispositivos?				
69	¿Es necesario tener permisos de administrador para usar la aplicación?				
70	¿La aplicación tiene diferentes ambientes?				
71	¿La aplicación es web?				

72	¿La aplicación es Interna o externa?				Interna.
73	¿Externa, la usan los clientes al exterior de la empresa?				
74	¿Si la aplicación es web, corre en cualquier navegador?				
75	¿Es posible que la aplicación no corra en Windows XP o inferior?				
76	¿Puede haber sospechas que alguien esté haciendo algo que no corresponda a la dirección normal de la aplicación?				
77	¿Se hace monitoreo de transacciones en la aplicación?				
78	¿Si un usuario está haciendo muchas aprobaciones puede ser inusual?				
79	¿Da permisos a los usuarios el administrador de la red o de la aplicación?				
80	¿Esta adjudicación de permisos la hace seguridad informática?				

Cuestionario 3

CUESTIONARIO DE LA INTEGRIDAD

Objetivo: Revisar el estado de la Integridad de la Información:

Fecha_____ Hora,_____ Ciudad _____

Datos generales de la Empresa _____

Datos generales del encuestado_____

Área de aplicación de la encuesta_____

No.	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1	¿Existe un modelo entidad relación de la base de datos del proceso?				
2	¿Existe un Diccionario de Datos de los objetos de la base de datos?				
3	El Diccionario de Datos contiene la información descriptiva mínima requerida tal como (nombre campo, ¿tipo de campo, dominio y descripción)?				
4	¿El Diccionario de Datos es actualizado constantemente?				
5	¿Se realiza revisión periódica de la coherencia entre modelo relacional de la BD y el diseño actual de la BD?				
6	¿Las BD de los distintos ambientes (DEV, QA y PROD) se encuentran alojadas en diferentes servidores?				
7	¿La base datos se encuentra licenciada?				
8	¿En el caso de la aplicación, la consola de autenticación se encuentra licenciada?				
9	¿Cada ambiente (DEV, QA y PROD) tienen configuraciones de acceso diferentes?				
10	¿Existen los mismos roles en los distintos ambientes?				
11	¿Los roles cuentan con restricciones de acceso objetos core de la BD?				

12	¿Los roles cuentan con restricciones de acceso a información confidencial de objetos de la BD?				
13	¿El DBA puede realizar modificación de la información contenida en los objetos de la BD de la aplicación?				
14	Existe un proceso de cambios definido?				
15	¿Se realizan solicitudes autorizadas de los cambios a realizar en los objetos de la BD?				
16	¿Los cambios que se efectúan en la base de datos se documentan?				
17	¿Se valida el estado de compilación de los objetos desplegados en el ambiente?				
18	¿Se comunica el estado final de los cambios realizados en la Base de datos?				
19	Se comunica con anticipación los cambios y/o mantenimientos a realizar en el Servidor y Base de datos? (actualizaciones, parcheos, no disponibilidad)?				
20	¿Al realizar un backup de la BD se verifica la sincronización en los archivos de configuración de la BD?				
21	¿Se valida el funcionamiento de la BD posterior a una restauración de un Backup?				
22	¿El canal de comunicación se encuentra	X			

	protegido mediante el uso de VPN por usuario?				
23	¿Existen procesos definidos para la recuperación del sistema después de una caida?				
24	¿El inventario de Tokens nuevos está bajo custodia?				
25	¿Existe contrato de mantenimiento para el servicio de Tokens?				
26	¿La aplicación contiene cifrado de datos?				

Cuestionario 4

CUESTIONARIO DE LA CONTINUIDAD

Objetivo: Revisar el estado de la Continuidad de la Información:

Fecha_____ Hora,_____ Ciudad _____

Datos generales de la Empresa: _____

Datos generales del encuestado _____

Área de aplicación de la encuesta _____

	Preguntas	Si	No	N/A	OBSERVACIONES
1	¿Existe un mapa de riegos establecidos?				
2	¿Se tiene políticas de Backus para la base datos?				
3	¿Qué clase de base de datos maneja?				AS400

4	¿El proceso de backups se encuentra documentado?				
5	¿Qué tipos de backups se realizan sobre la base de datos?				INCREMENTAL
6	¿Se realizan backups en diferentes tipos de medios?				
7	¿Con que herramienta se hacen esos backups?				Software establecido
8	¿Con que periodicidad se realizan los backups?				DIARIOS
9	¿Se realiza comprobación de los backups obtenidos?				
10	¿Se encuentra definida la persona que realiza la actividad de Backup?				
11	¿Los procesos y estrategias backups se encuentran documentados?				
12	¿Se cuentan con manuales de funciones para las personas que intervienen en el proceso de backups?				
13	¿Se cuentan con manuales de funciones para las personas que intervienen en el proceso de recuperación de información y establecimiento de los backups?				
14	¿Se cuenta con planillas (minutas) para evidenciar los procesos y estados de los backups?				
15	¿Quién custodia estos backups?				IBM
16	¿Una copia del backup lo custodia fuera de la entidad?				
17	¿Qué métodos emplea para realizar los backups?				Incremental.
18	¿Cada vez que se realiza alguna actualización o cambio en la producción se genera un backup?				
19	¿Los usuarios cuentan con la capacitación para				

	realizar los procesos según las políticas de contingencia?				
20	¿Se cuentan con manuales de funciones para las personas que intervienen en el proceso de contingencia?				
21	¿En caso de desastre existe otra ubicación física para la continuidad de la operación?				
22	¿En caso de tener ubicación física quienes tienen acceso a ella?				DBA, director tecnología y funcionaros encargados de la contingencia.
23	¿A estos sistemas físicos independientes se les da mantenimiento?				
24	¿Con que periodicidad se les da mantenimiento?				Anual
25	¿Se encuentra documentado el proceso de contingencia?				
26	¿En caso de no tener otra ubicación física para la contingencia, se cuenta con una UPS de respaldo?				
27	¿Se realizan simulacros para determinar la confianza en las medidas de continuidad?				
28	¿Con que periodicidad se realizan estos simulacros?				Anual
29	¿Las actividades a realizar en caso de contingencia están documentadas?				
30	¿Los resultados de los simulacros o pruebas se informan?				
31	¿Cómo se informan los resultados de los simulacros				Informe

	o pruebas?				gerencial.
32	¿Se realizan actualizaciones sobre los planes de contingencia?				
33	¿Qué alternativa para la continuidad del negocio existe en caso de presentación de un siniestro?				Core de negocio y Equipos en IBM.
34	¿Se realizan pruebas para las herramientas de continuidad del aplicativo?				
35	¿El plan de recuperación de negocio está documentado?				
36	¿Existe un árbol de llamadas al momento de presentarse un desastre?				
37	¿Quién activa ese árbol de llamadas?				
38	¿Qué medidas tienen con los proveedores en caso de presentarse un desastre?				Según contratos de mantenimiento.

Cuestionario 5

CUESTIONARIO DE LA SEGURIDAD DEL AMBIENTE

Objetivo: Revisar el estado de la Seguridad del Ambiente de la Información:

Fecha_____ Hora, _____Ciudad_____

Datos generales de la Empresa _____

Datos generales del encuestado _____

Área de aplicación de la encuesta_____

	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1	¿Existe un diagrama de la Topología de red de la aplicación y Bases de datos involucradas?				
2	¿Cuál es el tipo de Topología utilizada para el servicio de Tokens?				ESTRELLA
3	¿Cuántos servidores soportan la aplicación?				2
4	¿Qué sistema operativo tienen los servidores donde se encuentran las Bases de Datos?				LINUX
5	¿El sistema operativo se encuentra licenciado?				
6	¿El sistema contiene "parches" de actualizaciones?				
7	¿El aplicativo cuenta con la última versión de la base de datos?				
8	¿La Base de datos tiene "parches" de actualizaciones?				
9	¿El servidor tiene un antivirus?				
10	¿El antivirus del servidor se encuentra activo?				
11	¿El servidor tiene un proxy definido?				
12	¿Es una aplicación Cliente servidor?				
13	¿Es una aplicación WEB?				
14	¿Los usuarios acceden a la información de bases de datos mediante la aplicación o una herramienta administrativa de Base de Datos?				
15	¿Los usuarios pueden acceder a la Base de Datos únicamente mediante un canal seguro como VPN?				

16	Existen políticas documentadas para accesos y control de usuarios en el sistema operativos				
17	¿La aplicación y Base de Datos cuentan con protección de firewall?				
18	¿El Firewall se encuentra actualizado y activo?				
19	¿Existe un protocolo de seguridad para el manejo de usuarios y contraseñas de acceso a servidores, aplicaciones y Bases de Datos?				
20	Se almacena en una caja se seguridad la información de usuarios administradores, ¿contraseñas de acceso a servidores, aplicaciones y Bases de Datos?				
21	¿El centro de cómputo cuenta con un segundo canal de red de internet?				
22	¿El centro de cómputo cuenta con una UPS?				
23	¿La UPS se encuentra en funcionamiento?				
24	¿Los equipos (servidores) se encuentran conectados a la UPS?				
25	¿Se realiza regularmente mantenimiento preventivo a la UPS?				
26	¿El centro de cómputo cuenta una línea eléctrica alterna?				
27	¿La red eléctrica alterna se encuentra en funcionamiento?				
28	¿Tanto la red principal como la alterna son reguladas?				
29	¿Se realizan revisiones regulares a la red eléctrica principal y alterna?				

30	¿El centro de cómputo aplica las buenas prácticas para el cableado en los servidores?				
31	¿Todos los cables en el centro de cómputo se encuentran identificados en origen y destino?				
32	¿Se realizan revisiones y mantenimiento preventivo regular los dispositivos del centro de cómputo?				
33	¿El centro de cómputo tiene sistema de ventilación y enfriamiento temperatura?				
34	¿Se realiza regularmente mantenimiento preventivo al sistema regulatorio de temperatura del centro de cómputo?				
35	¿Existen políticas sobre el no consumo de alimentos dentro del centro de cómputo?				
36	¿Se cumplen las políticas de consumo de alimentos dentro del centro de cómputo?				
37	¿El centro de cómputo tiene alarmas detectoras de incendios?				
38	¿El centro de cómputo cuenta con un sistema de riego contra incendios?				
39	¿Existe al menos un extintor en el centro de cómputo?				
40	¿La fecha de vencimiento de(l) (los) (extintor(es) se encuentra vigente?				
41	¿El centro de cómputo se encuentra en una edificación sismorresistente?				
42	¿El centro de cómputo cuenta con un sistema de desagüe en caso de inundación?				

43	¿El centro de cómputo cuenta con restricción para el ingreso del personal (solo personal autorizado e identificado)?				
44	¿El centro de cómputo tiene seguridad lectora de carnet para el ingreso del personal autorizado?				
45	¿El centro de cómputo tiene seguridad lectora de huella dactilar para el ingreso del personal autorizado?				
46	¿El centro de cómputo tiene seguridad biométrica para el ingreso del personal autorizado?				
47	¿Existe un protocolo de evacuación de las instalaciones en el caso de alguna emergencia? (actividades en equipos antes de abandonar el lugar)				
48	¿Existe una ruta de salida de emergencia del centro de cómputo?				
49	¿Se cuenta con un segundo centro de cómputo físico en el caso de una contingencia para la operación?				
50	¿El segundo centro de cómputo cumple la norma de la distancia mínima entre centros de cómputo?				
51	¿Existe un protocolo para activar el segundo centro de cómputo físico en la contingencia?				
52	¿El segundo centro de cómputo cumple las anteriores preguntas?				

8.2.1 Tabulaciones

Cuestionario general

AREA	Encargado	¿Bajo cuantas personas está el manejo de los Tokens en el Banco ?:	¿Cada cuánto se negocian los lotes de Tokens?	¿Cada cuánto tiempo se cambia un Token por deterioro o vencimiento?:	¿Cuál es el número de clientes del Banco aproximadamente?:	¿Cuál es la cantidad de Tokens que se compran por lote?:	¿Cuánto tarda en promedio un Token en llegar a su destino y ser activado?:	¿Cuantos Tokens están Activos hoy día?:	¿El Token es esencialmente obligatorio en el Banco para todos los clientes? Empresas y Personas ?	¿En los informes solicitados se puede colocar datos de quien realiza las operaciones y en qué fecha y hora ?:	¿Está dividido el trabajo y las responsabilidades en el manejo de la Administración de los Tokens ?:
Area de tarjeta de credito	Laura Florez	4	No tiene periocidad	No tiene periocidad	100000	10000	Menos de 5 dias	Mas de 10000	NO	SI	SI
Area de tarjeta de credito	Angelica Sarmiento	5	No tiene periocidad	No tiene periocidad	50000	80000	menos de 4 dias	Mas de 20000	NO	SI	SI
Area de tarjeta de credito	Edison Briceño	4	No tiene periocidad	No tiene periocidad	500000	40000	menos de 4 dias	Mas de 30000	NO	SI	SI
Area de tarjeta de credito	Diego Espitia	3	No tiene periocidad	No tiene periocidad	10000	500	menos de 4 dias	Mas de 10000	NO	SI	SI
Area de tarjeta de credito	Nubia Gomez	4	No tiene periocidad	No tiene periocidad	500000	100000	menos de 4 dias	Mas de 10000	NO	SI	SI
Area de tecnologia	Ricardo Espitia	4	No tiene periocidad	cada año	40000	20000	menos de 4 dias	Mas de 10000	NO	SI	SI
Area de tecnologia	Jorge Samuel A	4	No tiene periocidad	No tiene periocidad	600000	60000	menos de 4 dias	Mas de 30000	NO	SI	SI
Area de tecnologia	Cesar Huerfano	4	Cada semana	cada año	20000	10000	menos de 3 dias	Mas de 30000	NO	SI	SI
Area de tecnologia	Claudia buendia	4	Cada semana	cada año	10000	10000	menos de 3 dias	Mas de 20000	NO	SI	SI
Area de tecnologia	Gina Jimenez	5	No tiene periocidad	No tiene periocidad	150000	10000	Menos de 5 dias	Mas de 20000	NO	SI	SI
Area de custodia	Paola Huertas	5	No tiene periocidad	cada año	120000	10000	Menos de 5 dias	Mas de 20000	NO	NO	SI
Area de custodia	Santiago Robles	4	No tiene periocidad	cada año	240000	10000	Menos de 5 dias	Mas de 30000	NO	NO	SI
Area de custodia	Jairo Parrado	4	No tiene periocidad	cada año	500000	10000	Menos de 5 dias	Mas de 20000	NO	NO	SI
Area de custodia	Santiago Hernandez	4	No tiene periocidad	No tiene periocidad	300000	10000	Menos de 5 dias	Mas de 20000	NO	NO	SI
Area de custodia	Brayan Hernandez	4	No tiene periocidad	No tiene periocidad	100000	10000	Menos de 5 dias	Mas de 40000	NO	NO	SI

¿Hay demoras y Bloqueos en la manipulación de los Tokens en los diferentes canales BV, Banca Móvil, etc ?	¿Hay informes diarios, mensuales o de oportunidad al requerir alguna información del sistema de Tokens ?:	¿Hay más número de clientes de empresas, que de personas?	¿Hay perfiles que manejan la trazabilidad de la aplicación de Tokens, ejemplo: Administrador, Operador?:	¿Hay personal Backups que suplan las ausencias de los titulares en caso de ausencias?	¿Hay sección de autorizaciones en los módulos de administración de Tokens ?:	¿Hay segmentación en los módulos de administración de Tokens ?:	¿Hay segmentación especial por área en los módulos de administración de Tokens ?:	¿La Aplicación es Modular ?:	¿La numeración de Tokens es consecutiva ?:	¿Los datos se pasan encriptados entre máquinas al necesitar cargar información externa a los módulos?	¿Los Tokens dañados son reemplazados con facilidad ?:	¿Se le da importancia a la efectividad de las consultas y transacciones de los clientes por los canales virtuales ?:	¿Se percibe seguridad en los Clientes con los manejos de productos de los Clientes que usan Tokens ?:	¿Se presentan muchas ausencias en los puestos claves de administración de Tokens?	¿Se presentan muchas fallas de tipo procedimental en el manejo del sistema? Ejemplo: No se pudo activar un Token ?
SI	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO	SI	NO	NO	SI	SI
SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	NO	SI	NO	NO	SI	SI
SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	NO	SI	NO	NO	SI	SI
SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	NO	SI	NO	NO	NO	SI
SI	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO	SI	SI	NO	NO	SI
SI	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO	SI	NO	SI	NO	SI
SI	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI
SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	NO	NO	NO	SI	SI	SI
SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	NO	SI	NO	SI	SI	SI
SI	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO	SI	SI	SI	NO	SI
SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	NO	NO	NO	SI	NO	NO
SI	SI	NO	SI	NO	SI	SI	SI	SI	SI	NO	NO	NO	SI	NO	NO
SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	NO	NO	NO	SI	NO	NO
SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	NO	NO	NO	SI	NO	NO
SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	NO	NO	NO	SI	NO	NO

¿Se presentan muchas llamadas por Servicio al Cliente de fallas producidas por los Tokens ?:	¿Se siente seguridad en la manipulación de los Tokens dentro del Banco ?:	¿Se siente seguridad en la manipulación de los Tokens fuera del Banco?
NO	SI	SI
NO	SI	SI
NO	SI	SI
NO	SI	SI
NO	SI	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI
NO	NO	SI

El primer cuestionario se hace para dar un vistazo general a la aplicación de administración de token´s, buscando obtener el conocimiento esencial del manejo del aplicativo, de los dispositivos físicos, los usuarios que manejan la aplicación, los tiempos del proceso, el tipo de clientes que se impactan más por este activo de información, y la estructura general del proceso.

Como análisis del presente cuestionario se puede evidenciar lo siguiente:

- Existe un desconocimiento de algunos procesos dentro del aplicativo, como lo es la cantidad de personas que tienen a cargo la administración del token y a periocidad con la que se negocian los token´s.
- El promedio de entrega de un token una vez solicitado por la página de internet o por medio de la oficina es de 5 días.
- El token no es obligatorio para los clientes.
- Según el área de impacto el cambio de un dispositivo varía su percepción de dificultad en el reemplazo.

- El 83.3% de los encuestados piensan que no se le da la importancia necesaria a la efectividad de las consultas y transacciones por la banca virtual.
- Dado el nicho de los clientes que atiende esta institución financiera (Personas de la tercera edad y pensionados), el 66.6% de los encuestados percibe que el cliente no sienten seguridad al momento de realizar las transacciones y consultas por la banca virtual.

Cuestionario seguridad Lógica

AREA	Encargado	¿La Base de datos es consistente, de tal manera que si los usuarios en su operación sobre la aplicación se desconectan abruptamente no se pierdan los	¿A los dispositivos se les hace mantenimiento en caso de presentar daños?	¿Cada perfil de la aplicación tiene correspondiente en usuario de logueo al sistema? Es decir uno a uno.?	¿Cada perfil tiene sus tareas asignadas?	¿Cada tabla en cada registro guarda usuario que creó, modificó y eliminó?	¿Cada usuario de la base de datos es único y pertenece a una única persona?	¿Cuenta con un listado actualizado de los usuarios que existen en la base de datos?	¿Cuenta con un listado actualizado de los usuarios que ingresan a la base de datos?	¿Da permisos a los usuarios el administrador de la red o de la aplicación?	¿Dónde hacen las pruebas de contingencia?	¿El administrador puede poner o quitar privilegios dentro de la aplicación?	¿El envío se hace a través de alguna empresa especializada?
Area de tecnologia	Ricardo Espitia	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Jorge Samuel A	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Cesar Huerfano	SI	SI	SI	Se cumplen tareas mixtas	NO	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Claudia buendia	SI	SI	SI	Se cumplen tareas mixtas	NO	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Gina Jimenez	SI	SI	SI	Se cumplen tareas mixtas	NO	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Paola Huertas	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Santiago Robles	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Jairo Parrado	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI

¿El servicio de Autenticación de dispositivos es estable?	¿El Usuario de la aplicación es el mismo de la Base de Datos?	¿En la creación de registros existen logs de seguimiento?	¿Es allí donde se ejecutaría la contingencia en caso de tal evento?	¿Es fácil saber cuál es el algoritmo que se usa cada vez que se cambia el número en la pantalla del dispositivo?	¿Es necesario tener permisos de administrador para usar la aplicación?	¿Es posible que la aplicación no corra en Windows XP o inferior?	¿Esta adjudicación de permisos la hace seguridad informática?	¿Existen controles inmediatos de acceso a los usuarios de la aplicación cuando este termina su contrato con la empresa?	¿Existen controles inmediatos de acceso a los usuarios de la Base de Datos cuando este termina su contrato con la empresa?	¿Existen formatos de solicitud de creación de usuarios de la aplicación?	¿Existen formatos de solicitud de creación de usuarios de la Base de Datos?	¿Existen logs de las operaciones más críticas o de todo?	¿Existen perfiles dentro de la aplicación?	¿Existen procedimientos definidos para crear, gestionar y eliminar usuarios (creación, actualización y eliminación) de la base de datos y la aplicación?	¿Externa, la usan los clientes al exterior de la empresa?
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI

En las preguntas relacionadas anteriormente podemos identificar que los registros que se modifican cambian o eliminan en las tablas en las diferentes tablas utilizadas en el aplicativo no guardan ni evidencian el usuario que realiza dicho cambio. Adicional a esto también que existen perfiles el 33% de los encuestados dentro de la aplicación con más de una tarea asignada, y que pueden hacer consultas, modificaciones, y revisión de información. Se identifica también que el aplicativo no funciona en aquellos equipos que tiene instalado el Windows XP o inferiores modelos. Y que algunos trabajadores presentan inconsistencias en su conocimiento, respondiendo que no existen LOGS en las operaciones más críticas.

¿Hacen todos los días envío de estos dispositivos?	¿Hay información estadística?	¿La aplicación es Interna o externa?	¿La aplicación es web?	¿La aplicación posee informes?	¿La aplicación tiene diferentes ambientes?	¿La base de datos es consistente? ¿Si se va la energía, al recuperarse el servicio no parece haber pasado nada?	¿La consola de autenticación está en Colombia?	¿La identificación en los dispositivos es única?	¿Las políticas de backup de datos dicen hacerlo a diario?	¿Los archivos planos Sirven para hacer envíos de otro tipo de información?	¿Los contratos con el proveedor de contingencia están al día?	¿Los contratos con el proveedor de la aplicación están al día?	¿Los contratos con los proveedores de mantenimiento de equipos están al día?	¿Los dispositivos de autenticación son desechables?	¿Los dispositivos son identificados por algún serial?
SI	SI	Interna	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	Interna	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	Interna	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	Interna	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	Interna	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	Interna	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	Interna	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	Interna	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

¿Los dispositivos son sellados?	¿Los formatos de solicitud de creación de usuarios para la aplicación tienen niveles de autorización?	¿Los formatos de solicitud de creación de usuarios para la base de datos tienen niveles de autorización?	¿Los informes son fácilmente obtenibles?	¿Los Log de seguimiento tienen vigencia? ¿Es decir, se guardan solo por un tiempo?	¿Los procedimientos de gestión de los usuarios de la aplicación se encuentran documentados?	¿Los procedimientos de gestión de los usuarios de la base de datos se encuentran documentados?	¿Los usuarios dentro de la aplicación son independientes para realizar diferentes temas?	¿Ocurre lo mismo en la aplicación? ¿Si el usuario no está realizando ninguna tarea, su aplicación se bloquea?	¿Para cada dispositivo de autenticación (Token) solo existe una sola identificación?	¿Para la entrega de los dispositivos hay algún procedimiento de seguridad establecido?	¿Para la trazabilidad hay estados en las solicitudes?	¿Para la trazabilidad hay estados en los dispositivos?	¿Puede haber sospechas que alguien esté haciendo algo que no corresponda a la dirección normal de la aplicación?	¿Se hace Backus de la aplicación? ¿Cada cuánto?	¿Se hace monitoreo de transacciones en la aplicación?
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Puntos relevantes;

- Con el cuestionario se puede identificar que la aplicación tiene la posibilidad de generar informes según el usuario lo requiera y con el condicionamiento que se solicite y que el 100% de los encuestados está satisfecho con los comandos existentes para generar dichos informes.
- Existe una política de creación de Backups diarios.
- Los dispositivos físicos cuentan con serial para su identificación y están sellados y que su presentan un estado en el sistema según su actualidad
- Existe niveles de autorización para creación de usuarios y el 70% d ellos encuestados conoce d es estas atribuciones.

¿Se manejan planes de contingencia locales?	¿Se producen archivos planos en la aplicación?	¿Si hay logs de seguimiento? ¿Estos pueden obtener la trazabilidad de un tema a resolver?	¿Si la aplicación es web, corre en cualquier navegador?	¿Si los usuarios en sus terminales tienen tiempos de inactividad, estas se bloquean automáticamente?	¿Si se daña un dispositivo de identificación es fácil cambiarlo?	¿Si se mojan los dispositivos se dañan?	¿Si un usuario está haciendo muchas aprobaciones puede ser inusual?	solicitud de creación de usuario no tiene las autorizaciones correspondientes, se realiza el proceso de creación del usuario?	¿Son informes en Excel?	¿Tiene políticas definidas para la creación de usuarios que interactúan con la aplicación?	¿Tiene políticas definidas para la creación de usuarios que interactúan con la Base de Datos?	¿Tienen control de contingencia externo?	¿Utilizan los mismos usuarios del sistema para trabajar dentro de la aplicación?	Cada perfil tiene derechos de crear, modificar, ¿eliminar registros?	Las políticas de Backup cubren a la configuración de sistema, servidores, ¿etc? ¿Cada cuánto se hace?
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI

Las solicitudes se cierran con frecuencia en feliz término. ¿O muchas de ellas se cancelan?	Si hay perfiles. ¿Cada perfil tiene su tarea bien definida?
SI	SI
SI	SI
SI	SI
SI	SI
SI	SI
SI	SI
SI	SI
SI	SI

- Dispositivos de identificación son difíciles de cambiar y esto es reconocido por el 100% de los encuestados., debido a que están sujetos a una semilla, y para poder cambiarlo hay que asignarle una nueva semilla y el proceso que conlleva entregar un nuevo token.
- Se debe revisar cómo se identifica que un usuario está haciendo varias aprobaciones, y si es inusual como generar el reporte y el tratamiento.
- Existen políticas definidas para la creación de los usuarios, se debe verificar contra política documentada ya que el personal el 100% encuestado conoce de estas políticas.
- Verificar las atribuciones de los perfiles de usuario, y quienes están autorizados para eliminar y modificar registros.
- Las solicitudes se cierran con frecuencia a feliz término según el 100% de los encuestados, hay que identificar los porcentajes de cuantas no se cierran o se cancelan.

Cuestionario Integridad

AREA	Encargado	¿Al realizar un backup de la BD se verifica la sincronización en los archivos de configuración de la BD?	¿Cada ambiente (DEV, QA y PROD) tienen configuraciones de acceso diferentes?	¿El canal de comunicación se encuentra protegido mediante el uso de VPN por usuario?	¿El DBA puede realizar modificación de la información contenida en los objetos de la BD de la aplicación?	¿El Diccionario de Datos es actualizado constantemente?	¿El inventario de Tokens nuevos está bajo custodia?	¿En el caso de la aplicación, la consola de autenticación se encuentra licenciada?	¿Existe contrato de mantenimiento para el servicio de Tokens?	¿Existe un Diccionario de Datos de los objetos de la base de datos?	¿Existe un modelo entidad relación de la base de datos del proceso?	¿Existen los mismos roles en los distintos ambientes?	¿Existen procesos definidos para la recuperación del sistema después de una caida?
Area de tecnologia	Ricardo Espitia	SI	NO	NO	NO	NO	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Jorge Samuel A	SI	NO	NO	NO	NO	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Cesar Huerfano	SI	NO	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Claudia buendia	SI	NO	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Gina Jimenez	SI	NO	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Paola Huertas	SI	NO	NO	NO	NO	SI	NO	SI	SI	SI	SI	SI
Area de custodia	Santiago Robles	SI	NO	NO	NO	NO	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Jairo Parrado	SI	NO	NO	NO	NO	SI	SI	SI	SI	SI	SI	SI

¿La aplicación contiene cifrado de datos?	¿La base datos se encuentra licenciada?	¿Las BD de los distintos ambientes (DEV, QA y PROD) se encuentran alojadas en diferentes servidores?	¿Los cambios que se efectúan en la base de datos se documentan?	¿Los roles cuentan con restricciones de acceso a información confidencial de objetos de la BD?	¿Los roles cuentan con restricciones de acceso objetos core de la BD?	¿Se comunica el estado final de los cambios realizados en la Base de datos?	¿Se realiza revisión periódica de la coherencia entre modelo relacional de la BD y el diseño actual de la BD?	¿Se realizan solicitudes autorizadas de los cambios a realizar en los objetos de la BD?	¿Se valida el estado de compilación de los objetos desplegados en el ambiente?	¿Se valida el funcionamiento de la BD posterior a una restauración de un Backup?	El Diccionario de Datos contiene la información descriptiva mínima requerida tal como (nombre campo, ¿tipo de campo, dominio y descripción)?	Existe un proceso de cambios definido?	Se comunica con anticipación los cambios y/o mantenimientos a realizar en el Servidor y Base de datos? (actualizaciones, parcheos, no disponibilidad)?
SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI	SI	SI

El cuestionario anterior se pregunta a 7 personas de la organización que tienen que ver directamente en el proceso tecnológico de la aplicación, y se logra identificar lo siguiente;

- No existe protección de VPN por usuario.
- La información obtenida para el diccionario de datos no es similar, se debe verificar si se le realiza las actualizaciones constantes. Del personal encuestado el 62.5% informa que no se actualiza el diccionario de datos.
- Un funcionario el 12.5% de los encuestados informo que la consola de autenticación no se encuentra licenciada. Se debe revisar esta información y/o hacer la retroalimentación.
- No existe una revisión periódica sobre los cambios en la BD actual y el modelo relacional de la BD.
- La aplicación está en distintos servidores, hay que revisar quienes tienen acceso y los perfiles que tienen, así como los backup que se generan.

Cuestionario disponibilidad

AREA	Encargado	¿A estos sistemas físicos independientes se les da mantenimiento?	¿Cada vez que se realiza alguna actualización o cambio en la producción se genera un backup?	¿Como se informan los resultados de los simulacros o pruebas?	¿Con que herramienta se hacen esos backups?	¿Con que periodicidad se les da mantenimiento?	¿Con que periodicidad se realizan estos simulacros?	¿Con que periodicidad se realizan los backups?	¿El plan de recuperación de negocio está documentado?	¿El proceso de backups se encuentra documentado?	¿En caso de desastre existe otra ubicación física para la continuidad de la operación?	¿En caso de no tener otra ubicación física para la contingencia, se cuenta con una UPS de respaldo?
Area de tarjeta de cre	Laura Florez	SI	SI	NO SABE	NO SABE	NO SABE	NO SABE	DIARIOS	NO	SI	SI	SI
Area de tarjeta de cre	Angelica Sarmiento	SI	NO	NO SABE	NO SABE	Anual	anual	DIARIOS	NO	SI	SI	SI
Area de tarjeta de cre	Edison Briceño	SI	NO	NO SABE	NO SABE	NO SABE	anual	DIARIOS	NO	SI	SI	SI
Area de tarjeta de cre	Diego Espitia	SI	NO	NO SABE	NO SABE	NO SABE	Semestral	DIARIOS	NO	SI	SI	SI
Area de tarjeta de cre	Nubia Gomez	SI	NO	NO SABE	NO SABE	NO SABE	anual	DIARIOS	NO	SI	SI	SI
Area de tecnologia	Ricardo Espitia	SI	SI	INFORME GERENCI	Software establecido	Anual	anual	DIARIOS	NO	SI	SI	SI
Area de tecnologia	Jorge Samuel A	SI	SI	INFORME GERENCI	Software establecido	Anual	anual	DIARIOS	NO	SI	SI	SI
Area de tecnologia	Cesar Huerfano	SI	SI	INFORME GERENCI	Software establecido	Anual	anual	DIARIOS	NO	SI	SI	SI
Area de tecnologia	Claudia buendia	SI	SI	INFORME GERENCI	Software establecido	Anual	anual	DIARIOS	NO	SI	SI	SI
Area de tecnologia	Gina Jimenez	SI	SI	INFORME GERENCI	Software establecido	Anual	anual	DIARIOS	NO	SI	SI	SI
Area de custodia	Paola Huertas	SI	SI	NO SABE	NO SABE	NO SABE	anual	DIARIOS	NO	SI	SI	SI
Area de custodia	Santiago Robles	SI	SI	NO SABE	NO SABE	NO SABE	anual	DIARIOS	NO	SI	SI	SI
Area de custodia	Jairo Parrado	SI	SI	NO SABE	NO SABE	NO SABE	anual	DIARIOS	NO	SI	SI	SI
Area de custodia	Santiago Hernandez	SI	SI	NO SABE	NO SABE	Anual	anual	DIARIOS	NO	SI	SI	SI
Area de custodia	Brayan Hernandez	SI	SI	NO SABE	NO SABE	Anual	anual	DIARIOS	NO	SI	SI	SI

¿En caso de tener ubicación física quienes tienen acceso a ella?	¿Existe un árbol de llamadas al momento de presentarse un desastre?	¿Existe un mapa de riegos establecidos?	¿Las actividades a realizar en caso de contingencia están documentadas ?	¿Los procesos y estrategias backups se encuentran documentados ?	¿Los resultados de los simulacros o pruebas se informan?	¿Los usuarios cuentan con la capacitación para realizar los procesos según las políticas de contingencia?	¿Qué alternativa para la continuidad del negocio existe en caso de presentación de un siniestro?	¿Qué clase de base de datos maneja?	¿Qué medidas tienen con los proveedores en caso de presentarse un desastre?	¿Qué métodos emplea para realizar los backups?
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	NO	NO	NO	SI	NO	Core de negocio y Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	NO	NO	NO	SI	NO	Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	NO	NO	NO	SI	NO	Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	NO	NO	NO	SI	NO	Core de negocio y Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	NO	NO	NO	SI	SI	Core de negocio y Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	NO	NO	NO	SI	SI	Equipos en IBM.	AS400	Las establecidas en los ctos de	Incremental
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	SI	Equipos en IBM.	AS400	Las establecidas en los ctos de	Incremental
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	SI	Equipos en IBM.	AS400	Las establecidas en los ctos de	Incremental
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	NO	Equipos en IBM.	AS400	Las establecidas en los ctos de	Incremental
DBA, director tecnología y funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	NO	Equipos en IBM.	AS400	Las establecidas en los ctos de	Incremental
Funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	NO	Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
Funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	NO	Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
Funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	SI	Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
Funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	SI	Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo
Funcionaros encargados de la contingencia.	NO	SI	NO	NO	SI	NO	Core de negocio y Equipos en IBM.	AS400	Las establecidas en los ctos de	No lo realiza mi cargo

Se decide realizar el cuestionario de disponibilidad, dado que un siniestro puede tener afectación en toda la población escogida;

- Se evidencia que el 65% de los encuestados tiene desconocimiento en cuanto a las medidas de continuidad de la operación, y los procesos que conlleva elaborar un escenario de contingencia.
- Algunos usuarios el 66.6% de los encuestados no hacen parte del personal que se encarga de las contingencias, por lo que sus respuestas nos son correctas o no tienen el conocimiento.
- No hay una formalidad en las comunicaciones en caso de presentarse siniestro.
- De los encuestados solo el 44% tienen la capacitación en caso de presentarse un escenario de contingencia.
- Falta formalidad y documentación en los procesos de contingencia

¿Quién activa ese árbol de llamadas?	¿Quién custodia estos backups?	¿Se cuenta con planillas (minutas) para evidenciar los procesos y estados de los backups?	¿Se cuentan con manuales de funciones para las personas que intervienen en el proceso de backups?	¿Se cuentan con manuales de funciones para las personas que intervienen en el proceso de contingencia?	¿Se cuentan con manuales de funciones para las personas que intervienen en el proceso de recuperación de información y establecimiento de los backups?	¿Se encuentra definida la persona que realiza la actividad de Backup?	¿Se encuentra documentado el proceso de contingencia?	¿Se realiza comprobación de los backups obtenidos?	¿Se realizan actualizaciones sobre los planes de contingencia?	¿Se realizan backups en diferentes tipos de medios?	¿Se realizan pruebas para las herramientas de continuidad del aplicativo?	¿Se realizan simulacros para determinar la confianza en las medidas de continuidad?	¿Se tiene políticas de Backus para la base datos?	¿Una copia del backup lo custodian fuera de la entidad?
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	SI	SI	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	NO	NO SABE	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	NO	NO SABE	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	NO	NO SABE	SI	SI	SI	SI
No hay arbol	IBM	SI	SI	NO	NO	SI	SI	SI	NO	NO SABE	SI	SI	SI	SI

Cuestionario de la seguridad del ambiente

AREA	Encargado	¿Cuál es el tipo de Topología utilizada para el servicio de Tokens?	¿Cuántos servidores soportan la aplicación?	¿El antivirus del servidor se encuentra activo?	¿El aplicativo cuenta con la última versión de la base de datos?	¿El centro de cómputo aplica las buenas prácticas para el cableado en los servidores?	cómputo cuenta con restricción para el ingreso del personal (solo personal autorizado e identificado)?	¿El centro de cómputo cuenta con un segundo canal de red de internet?	¿El centro de cómputo cuenta con un sistema de desagüe en caso de inundación?	¿El centro de cómputo cuenta con un sistema de riego contra incendios?	¿El centro de cómputo cuenta con una UPS?	¿El centro de cómputo cuenta una línea eléctrica alterna?	¿El centro de cómputo se encuentra en una edificación sismorresisten te?
Area de tarjeta de credito	Laura Florez	NO SABE	NO SABE	SI	NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	NO SABE	NO SABE
Area de tarjeta de credito	Angelica Sarmiento	NO SABE	NO SABE	SI	NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	NO SABE	NO SABE
Area de tarjeta de credito	Edison Briceño	NO SABE	NO SABE	SI	NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	NO SABE	NO SABE
Area de tarjeta de credito	Diego Espitia	NO SABE	NO SABE	SI	NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	NO SABE	NO SABE
Area de tarjeta de credito	Nubia Gomez	NO SABE	NO SABE	SI	NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	NO SABE	NO SABE
Area de tecnologia	Ricardo Espitia	ESTRELLA	2	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Jorge Samuel A	ESTRELLA	2	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Cesar Huerfano	ESTRELLA	2	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Claudia buendia	ESTRELLA	2	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Area de tecnologia	Gina Jimenez	ESTRELLA	2	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Paola Huertas	ESTRELLA	2	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Santiago Robles	ESTRELLA	2	SI	SI	NO	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Jairo Parrado	ESTRELLA	2	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Area de custodia	Santiago Hernandez	NO SABE	NO SABE	SI	NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	NO SABE	NO SABE
Area de custodia	Brayan Hernandez	NO SABE	NO SABE	SI	NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	NO SABE	NO SABE

¿El centro de cómputo tiene alarmas detectoras de incendios?	¿El centro de cómputo tiene seguridad biométrica para el ingreso del personal autorizado?	¿El centro de cómputo tiene seguridad lectora de carnet para el ingreso del personal autorizado?	¿El centro de cómputo tiene seguridad lectora de huella dactilar para el ingreso del personal autorizado?	¿El centro de cómputo tiene sistema de ventilación y enfriamiento temperatura?	¿El Firewall se encuentra actualizado y activo?	¿El segundo centro de cómputo cumple la norma de la distancia mínima entre centros de cómputo?	¿El servidor tiene un antivirus?	¿El servidor tiene un proxy definido?	¿El sistema contiene "parches" de actualizaciones ?	¿El sistema operativo se encuentra licenciado?	¿Es una aplicación Cliente servidor?	¿Es una aplicación WEB?	¿Existe al menos un extintor en el centro de cómputo?	¿Existe un protocolo de evacuación de las instalaciones en el caso de alguna emergencia? (actividades en equipos antes de abandonar el lugar)	¿Existe un protocolo de seguridad para el manejo de usuarios y contraseñas de acceso a servidores, aplicaciones y Bases de Datos?
NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	SI	SI	SI	SI	NO	SI	SI	SI	SI
NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	SI	SI	SI	SI	NO	SI	SI	SI	SI
NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	SI	SI	SI	SI	NO	SI	SI	SI	SI
NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	SI	SI	SI	SI	NO	SI	SI	SI	SI
NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	SI	SI	SI	SI	NO	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI	SI	SI	SI
NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	SI	SI	SI	SI	NO	SI	SI	SI	SI
NO SABE	NO SABE	SI	SI	NO SABE	NO SABE	NO SABE	SI	SI	SI	SI	NO	SI	SI	SI	SI

¿Existe un protocolo para activar el segundo centro de cómputo físico en la contingencia?	¿Existe una ruta de salida de emergencia del centro de cómputo?	¿Existen políticas sobre el no consumo de alimentos dentro del centro de cómputo?	¿La aplicación y Base de Datos cuentan con protección de firewall?	¿La Base de datos tiene "parches" de actualizaciones?	¿La fecha de vencimiento de(l) (los) (extintor(es) se encuentra vigente?	¿La red eléctrica alterna se encuentra en funcionamiento?	¿La UPS se encuentra en funcionamiento?	¿Los equipos (servidores) se encuentran conectados a la UPS?	¿Los usuarios acceden a la información de bases de datos mediante la aplicación o una herramienta administrativa de Base de Datos?	¿Los usuarios pueden acceder a la Base de Datos únicamente mediante un canal seguro como VPN?	¿Qué sistema operativo tienen los servidores donde se encuentran las Bases de Datos?	¿Se cuenta con un segundo centro de cómputo físico en el caso de una contingencia para la operación?	¿Se cumplen las políticas de consumo de alimentos dentro del centro de cómputo?	¿Se realiza regularmente mantenimiento preventivo a la UPS?	¿Se realiza regularmente mantenimiento preventivo al sistema regulatorio de temperatura del centro de cómputo?
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	NO SABE	SI	NO SABE	NO SABE	NO SABE
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	NO SABE	SI	NO SABE	NO SABE	NO SABE
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	NO SABE	SI	NO SABE	NO SABE	NO SABE
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	NO SABE	SI	NO SABE	NO SABE	NO SABE
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	NO SABE	SI	NO SABE	NO SABE	NO SABE
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	LINUX	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	LINUX	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	LINUX	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	LINUX	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	LINUX	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	LINUX	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	LINUX	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	LINUX	SI	SI	SI	SI
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	NO SABE	SI	NO SABE	NO SABE	NO SABE
SI	SI	SI	SI	SI	NO SABE	SI	SI	SI	SI	SI	NO SABE	SI	NO SABE	NO SABE	NO SABE

¿Se realizan revisiones regulares a la red eléctrica principal y alterna?	¿Se realizan revisiones y mantenimiento preventivo regular los dispositivos del centro de cómputo?	¿Tanto la red principal como la alterna son reguladas?	¿Todos los cables en el centro de cómputo se encuentran identificados en origen y destino?	Existen políticas documentadas para accesos y control de usuarios en el sistema operativos	Se almacena en una caja se seguridad la información de usuarios administradores, ¿contraseñas de acceso a servidores, aplicaciones y Bases de Datos?
NO SABE	NO SABE	NO SABE	NO SABE	SI	SI
NO SABE	NO SABE	NO SABE	NO SABE	SI	SI
NO SABE	NO SABE	NO SABE	NO SABE	SI	SI
NO SABE	NO SABE	NO SABE	NO SABE	SI	SI
NO SABE	NO SABE	NO SABE	NO SABE	SI	SI
SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI
SI	SI	SI	SI	SI	SI
NO SABE	NO SABE	NO SABE	NO SABE	SI	SI
NO SABE	NO SABE	NO SABE	NO SABE	SI	SI

Con el cuestionario realizado se denota que la área de tarjeta de crédito y unos funcionario de custodia el 46.6% del total de los encuestados no tienen conocimiento de algunos procesos tecnológicos de la administración de token´s, también que entre los encuestados el 20% manifiesta que el banco no cumple con las buenas prácticas respecto al cableado de los servidores, el 46.6% no saben si se cumple con esto y solo el 33.3% afirma que en la institución se cumplen con estas buenas prácticas.

- La topología usada para el servidor de token es tipo estrella, pero esto solo lo conocen el 53.3% del total de los encuestados.
- El centro de cómputo cuenta con UPS de respaldo, pero esto solo lo conocen el 53.3% del total de los encuestados.

- El 100% del total de los encuestados saben de la existencia de medidas contra incendio (extintores, pero ninguno conoce o esta al tanto de sus fechas de vencimiento).
- El 100% del total de los encuestados saben de la existencia del centro de respaldo para contingencia.
- El 100% del total de los encuestados saben que los softwares utilizados están licenciados y cuentan con las actualizaciones debido a los mensajes del sistema que les indican de este proceso.
- El 100% del total de los encuestados saben de la existencia de protocolos para activación de contingencia, y medidas para retiro de equipo en caso de emergencia.

9 BIBLIOGRAFIA

27005, N. -I. (19 de 08 de 2009). *Nomra Tecnica Colombiana NTC-ISO 27005.* Recuperado el 21 de 09 de 2018, de Nomra Tecnica Colombiana NTC-ISO 27005: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf

31000, N. (16 de 02 de 2011). *Norma Tecnica Colombiana NTC-ISO 31000.* Recuperado el 21 de 09 de 2018, de Norma Tecnica Colombiana NTC-ISO 31000: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

Aranda Software. (09 de 05 de 2012). *ITIL Y COBIT; ALGUNAS DIFERENCIAS*. Recuperado el 26 de 08 de 2018, de Aranda Software: https://arandasoft.com/itil-y-cobit-algunas-diferencias/

ASOBANCARIA. (29 de 09 de 2016). *¿Que es Leasing?* Recuperado el 02 de 08 de 2018, de ASOBANCARIA: http://www.asobancaria.com/sabermassermas/que-es-leasing/

ASOBANCARIA. (04 de 08 de 2016). *¿Que son las CFC?* Recuperado el 07 de 09 de 2018, de ASOBANCARIA: http://www.asobancaria.com/sabermassermas/que-es-CFC/

ASOBANCARIA. (02 de 08 de 2018). *Canales y seguridad*. Recuperado el 02 de 08 de 2018, de ASOBANCARIA: http://www.asobancaria.com/sabermassermas/home/consumidor-informado/mas-acerca-de-los-bancos/canales-y-seguridad/

Avila Forero, R. (13 de 08 de 2018). *Revista Dinero*. Recuperado el 21 de 09 de 2018, de ¿Bancarizar o no bancarizar?: https://www.dinero.com/Item/ArticleAsync/260869

Ayala , V. (04 de 06 de 2010). Tradición y modernidad en la era de internet. *El Nuevo Diario* .

Benavides, C., & Arias, A. (2011). Aplicación de la norma COBIT en el monitoreo de transferencias electrónicas de datos contable-financieros. *5*(1).

Bocanegra Requena, J. M., & Bocanegra Gil, B. (2011). *ADMINISTRACION ELECTRONICA EN ESPAÑA, LA. Implantación y régimen jurídico.* Barcelona: Atelier Libros Juridicos.

Bonilla, C. (15 de 01 de 2013). *Estándar iso iec 27002 2005*. Recuperado el 02 de 10 de 2018, de Slideshare.net: https://es.slideshare.net/cirobonilla/estndar-iso-iec-27002-2005

BOON, S., & HOLMES, J. (1991). *The dynamics of interpersonal trust: Resolving uncertainty in the face of risk.* Cambridge : Cambridge University Press, UK.

CITIBANK. (07 de 09 de 2018). *Sistema Financiero / ¿Que son las entidades Fiduciarias?* Obtenido de CITIBANK: https://www.citibank.com.co/educacionfinanciera/sistfinan/quesonsociefiducia.htm

COBIT NORMAS AUDITORIA. (s.f.).

Dacchan T., J. C. (21 de 09 de 2018). *Ley de Delitos Informáticos en Colombia*. Recuperado el 21 de 09 de 2018, de DELTA Asesores: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Economia Simple.Net. (02 de 08 de 2018). *Definición de Banca electrónica*. Recuperado el 02 de 08 de 2018, de Economia Simple.Net: https://www.economiasimple.net/glosario/banca-electronica

Economia Simple.Net. (16 de 09 de 2018). *Definición de Transacción*. Recuperado el 16 de 09 de 2018, de Economia Simple.Net: https://www.economiasimple.net/glosario/transaccion

El Tiempo. (08 de 01 de 2002). *BANCA VIRTUAL, OPORTUNIDADES Y RIESGOS*. Recuperado el 02 de 08 de 2018, de El Tiempo: https://www.eltiempo.com/archivo/documento/MAM-1377742

FONCEP Fondo de prestaciones economicas, cesantias y pensiones. (03 de 05 de 2016). *Glosario*. Recuperado el 07 de 09 de 2018, de FONCEP Fondo de prestaciones economicas, cesantias y pensiones.: http://www.foncep.gov.co/index.php/glosario

GRUPO SANTANDER S.A. (2018). *¿Qué es el Token de Seguridad?* Recuperado el 07 de 09 de 2018, de GRUPO SANTANDER S.A.: https://www.santanderrio.com.ar/banco/online/personas/pagar-y-transferir/token-de-seguridad/faq

Mercado, I. (23 de 04 de 2018). *Internet Society - Capitulo Republica Dominicana*. Recuperado el 21 de 09 de 2018, de SEGURIDAD DE LAS TRANSACCIONES ELECTRÓNICAS: https://isoc-rd.org.do/publicaciones/recursos/seguridad-de-las-transacciones-electronicas/

MyTripleA. (02 de 07 de 2018). *Diccionario Financiero*. Recuperado el 02 de 07 de 2018, de MyTripleA: https://www.mytriplea.com/diccionario-financiero/banco-comercial/

Navarro, H. (21 de 11 de 2010). *Muestreo Aleatorio SImple*. Recuperado el 02 de 10 de 2018, de Slideshare.net: https://es.slideshare.net/milit/muestreo-aleatorio-simple

Pabón Cadavid, J. A. (02 de 08 de 2018). La criptografía y la protección a la información digital. *Revista U Externado*,

https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636. Obtenido de La criptografía y la protección a la información digital: https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

Pavlou, P. (03 de 2003). *ResearchGate*. Recuperado el 21 de 09 de 2018, de Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model: https://www.researchgate.net/publication/234775493_Consumer_Acceptance_of_Electronic_Commerce_Integrating_Trust_and_Risk_with_the_Technology_Acceptance_Model

Periodico el Colombiano. (12 de 04 de 2018). *Colombia, el sexto país con más ciberataques en 2017*. Recuperado el 02 de 06 de 2018, de El Colombiano: http://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174

Portafolio. (07 de 05 de 2015). *Así están distribuidos los colombianos por estratos sociales*. Recuperado el 10 de 09 de 2018, de Portafolio: https://www.portafolio.co/tendencias/distribuidos-colombianos-estratos-sociales-57300

RAE (Real Academia Española). (21 de 09 de 2018). *Diccionario*. Recuperado el 21 de 09 de 2018, de RAE (Real Academia Española): http://www.rae.es/

Ramirez, M. C. (13 de 03 de 2015). *La Republica*. Recuperado el 16 de 09 de 2018, de https://www.larepublica.co/consumo/pereira-y-manizales-las-ciudades-que-mas-compran-online-2231601: https://www.larepublica.co/consumo/pereira-y-manizales-las-ciudades-que-mas-compran-online-2231601

Ratnasingam, P. (03 de 05 de 2005). *ScienceDirfect.* Obtenido de rust in inter-organizational

exchanges: a case study in business to business electronic commerce: https://www.sciencedirect.com/science/article/pii/S0167923604000314?via%3Dihub

Revista Dinero. (07 de 07 de 2016). *Bancos se preparan para la nueva era de transacciones móviles*. Recuperado el 21 de 09 de 2018, de Revista Dinero: https://www.dinero.com/edicion-impresa/tecnologia/articulo/bancos-se-preparan-para-la-nueva-era-de-transacciones-moviles/225415

Revista Dinero. (02 de 02 de 2017). *El apetitoso negocio del cibercrimen*. Recuperado el 02 de 07 de 2018, de Revista Dinero: https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593

Revista Dinero. (02 de 02 de 2017). *www.dinero.com*. Recuperado el 20 de 08 de 2018, de www.dinero.com: https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593

Revista Dinero. (13 de 03 de 2018). *Internet le roba terreno a las oficinas a la hora de hacer trámites financieros*. Recuperado el 15 de 08 de 2018, de Revista Dinero: https://www.dinero.com/economia/articulo/operaciones-financieras-en-colombia-en-2017/256283

seguridadensistemascomputacionales.zonalibre.org. (04 de 02 de 2011). *Encriptación.* Recuperado el 07 de 09 de 2018, de seguridadensistemascomputacionales.zonalibre.org: http://seguridadensistemascomputacionales.zonalibre.org/

Superintendencia Financiera de Colombia. (s.f.). Obtenido de https://www.superfinanciera.gov.co/publicacion/20148

SUPERINTENDENCIA FINANCIERA DE COLOMBIA . (2009). *Ley 1328 de 2009 Protección al Consumidor Financiero*. Recuperado el 21 de 09 de 2018, de SUPERINTENDENCIA FINANCIERA DE COLOMBIA: https://www.superfinanciera.gov.co/SFCant/ConsumidorFinanciero/reformafinanciera.html

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. (11 de 08 de 2016). *Banca movil, banca por internet, normatividad*. Recuperado el 30 de 09 de 2018, de SUPERINTENDENCIA FINANCIERA DE COLOMBIA: https://www.superfinanciera.gov.co/publicacion/10087124

Superintendencia Financiera de Colombia. (05 de 09 de 2017). *Informe de Operaciones segundo semestre 2016*. Recuperado el 04 de 10 de 2018, de Superintendencia Financiera de Colombia: https://www.superfinanciera.gov.co/jsp/10082624

Superintendencia Financiera de Colombia. (01 de 12 de 2017). *Reporte de inclusión Financiera*. Recuperado el 20 de 08 de 2018, de Superintendencia Financiera de Colombia: https://www.superfinanciera.gov.co/inicio/informes-y-cifras/informes/10085394

Superintendencia Financiera de Colombia. (04 de 02 de 2017). *Reporte Inclusión Finaniera 2016*. Recuperado el 04 de 10 de 2018, de Superintendencia Financiera de Colombia: http://bancadelasoportunidades.gov.co/sites/default/files/2017-07/RIF%202016-%20final.pdf

Superintendencia Financiera de Colombia. (02 de 07 de 2018). *Glosario*. Recuperado el 02 de 07 de 2018, de Superintendencia Financiera de Colombia: https://www.superfinanciera.gov.co/jsp/Glosario/user/main/letra/B/f/0/c/00

Superintendencia Financiera de Colombia. (07 de 09 de 2018). *www.superfinanciera.gov.co*. Obtenido de https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=11268&dPrint=1

Textos Cientificos. (09 de 11 de 2006). *Encriptación*. Recuperado el 21 de 09 de 2018, de Textos Cientificos: https://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptacion

TIMMERS, P., & VEER, J. (23 de 06 de 1999). *The European Electronic*. Recuperado el 07 de 09 de 2018, de «Electronic Commerce: A Challenge for Europe»: http://www.ispo.cec.be/ecommerce/what/challenge.htm

webscolar. (2018). *Método de Muestreo*. Recuperado el 21 de 09 de 2019, de webscolar: http://www.webscolar.com/metodo-de-muestreo

Webscolar. (30 de 08 de 2018). *Método de Muestreo*. Recuperado el 14 de 09 de 2018, de http://www.webscolar.com/metodo-de-muestreo: http://www.webscolar.com/metodo-de-muestreo

Welive Security. (20 de 05 de 2017). *Cambios en la norma para gestionar la seguridad de la información*. Recuperado el 02 de 09 de 2018, de Welive Security: https://www.welivesecurity.com/

XARXA AFIC El portal del Comerciante. (07 de 09 de 2018). *LA SEGURIDAD EN LAS TRANSACCIONES*. Recuperado el 07 de 09 de 2018, de XARXA AFIC El portal del Comerciante: https://www.portaldelcomerciante.com/es/articulo/la-seguridad-transacciones#arriba

Yañez, C. (08 de 11 de 2017). *CEAC Planeta Formación y Universidades*. Recuperado el 21 de 09 de 2018, de TIPOS DE SEGURIDAD INFORMÁTICA: https://www.ceac.es/blog/tipos-de-seguridad-informatica