UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERÍA
POSTGRADO EN SISTEMAS DE INFORMACIÓN

Trabajo de Grado de Maestría

PROPUESTA DE UN MODELO PARA LA DETECCIÓN DE VULNERABILIDADES EN LOS CANALES ELECTRÓNICOS DE LAS INSTITUCIONES BANCARIAS DEL SECTOR PRIVADO EN VENEZUELA.

Presentado por
Morín Canino, Nelson Eduardo

Para optar al título de
Magister en Sistemas de información

Tutor
MSc. José Antonio Gil

Caracas, Junio de 2015

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

VICERRECTORADO ACADÉMICO

ESTUDIOS DE POSTGRADO

ÁREA DE INGENIERÍA

POSTGRADO EN SISTEMAS DE INFORMACIÓN

ACEPTACIÓN DEL TUTOR

Por la presente hago constar que he leído el Trabajo de Grado de Maestría, presentado por el **ciudadano Nelson Eduardo Morín Canino**, titular de la Cédula de Identidad N° V.- 17.978.019 para optar al Título de Magíster en Sistemas de Información, cuyo título tentativo es: **Propuesta de un modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela**; y que acepto asesorar a la estudiante, durante la etapa de desarrollo del Trabajo hasta su presentación y evaluación.

En la ciudad de Caracas, a los 20 días del mes de junio de 2015.

_____

MSc. José Antonio Gil

CI. V- 10.627.442

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

VICERRECTORADO ACADÉMICO

ESTUDIOS DE POSTGRADO

ÁREA DE INGENIERÍA

POSTGRADO EN SISTEMAS DE INFORMACIÓN

PROPUESTA DE UN MODELO PARA LA DETECCIÓN DE VULNERABILIDADES EN LOS CANALES ELECTRÓNICOS DE LAS INSTITUCIONES BANCARIAS DEL SECTOR PRIVADO EN VENEZUELA.

Autor: Morín, C. Nelson E.
Asesor: MSc. José Antonio Gil
Fecha: Junio 2015

RESUMEN

El objetivo de esta investigación fue el de diseñar una propuesta de un Modelo para la Detección de Vulnerabilidades en los canales Electrónicos de las Instituciones Bancarias del sector privado en Venezuela. La metodología aplicada para el logro de este objetivo se fundamentó en la modalidad de proyecto factible de nivel descriptivo apoyado en un diseño de investigación mixto. Se diseñaron como instrumentos de medición dos (2) listas de chequeo (Check list) y un cuestionario tipo Likert, las cuales se aplicaron a una muestra de diez (10) Instituciones Bancarias del sector privado en Venezuela, con la finalidad de determinar las condiciones actuales del proceso de detección de vulnerabilidades en los canales electrónicos de dichas Instituciones; así como, los requerimientos mínimos que a juicio del personal de seguridad de la información de los Bancos que conformaron la muestra deberían estar presentes en un modelo de análisis de vulnerabilidades. El modelo propuesto quedó estructurado en cinco (5) fases: Reconocimiento, Escaneo de Puertos y enumeración de servicios, Escaneo de vulnerabilidades, Análisis y presentación de los resultados. El mismo fue validado por el juicio de expertos en Riesgo Tecnológico y Seguridad de la Información de la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN) a través de los métodos de focus group y Delphi. Esta propuesta permite establecer un modelo conceptual para la detección oportuna de vulnerabilidades que ayudará a prevenir y a solventar el problema de seguridad en los canales electrónicos de dichas Instituciones, bajo una perspectiva de riesgo tecnológico y de cumplimiento.

Palabra clave: *Propuesta de Modelo, Detección de Vulnerabilidades.*
Línea de Investigación: Ingeniería del software

DEDICATORIA

Es el final de una etapa e inicio de otra, es el aprendizaje que dejan estos dos (2) años de postgrado, es por ello, que es digna de dedicar a personas tan importantes en mi vida que confiaron en mí y me hicieron sentir orgulloso de ser parte de sus vidas. A ti mi Dios por darme la oportunidad de vivir y brindarme tu mano para seguir adelante en los momentos más difíciles, en especial a mi madre Tibisay Canino por estar ahí cuando la necesito y darme aliento por seguir luchando por la vida y la búsqueda de mis objetivos. A mi padre Nelson Morin por ser tan ejemplar.

Nelson Morin

AGRADECIMIENTO

A Dios Todopoderoso por darnos la vida, la inteligencia, las fuerzas y las fortalezas necesarias y no dejarme flaquear en los momentos más difíciles, para llevar a cabo esta meta.

A mis padres Tibisay Canino y Nelson Horacio Morín, por haberme brindado todo su apoyo y colaboración tanto moral como espiritualmente en la elaboración de éste trabajo especial de grado.

A la Superintendencia de Bancos y otras Instituciones Financiera (SUDEBAN) por haberme abierto sus puertas, brindado todo su apoyo y confianza para la elaboración de éste trabajo especial de grado.

A la Universidad Católica Andrés Bello por darme la oportunidad de formarme profesional, moral y éticamente.

A mi tutor José Antonio Gil por haberme brindado todo su apoyo y colaboración tanto moral como profesionalmente en la elaboración de éste trabajo especial de grado.

A todo el personal docente de la Universidad Católica Andrés Bello, por compartir conmigo todos sus conocimientos tanto académicos como profesionales, gracias por el apoyo brindado durante el desarrollo de la maestría.

Nelson Morin

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad, se reconoce a la Seguridad como un proceso continuo que debe estar presente en todas las dimensiones de la sociedad y particularmente en el funcionamiento de las empresas y en todos sus procesos, independientemente del sector donde se ubique. Condición que debe estar presente, en virtud de evitar vulnerabilidades específicamente en el activo más preciado para las mismas: la información.

Importante es señalar, que hoy en día las organizaciones y sus Sistemas de Información a nivel mundial, se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones; también ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados; por lo cual, deberían estar sometidos al control correspondiente.

Por tal motivo, el tema de la Seguridad en los Sistemas de Información, es abordado desde un enfoque estratégico y en ese marco, se tienden a proponer mecanismos, sistemas y modelos que permitan detectar posibles vulnerabilidades y a su vez, gestionar de manera efectiva, la seguridad de la información, respondiendo a las necesidades particulares de una organización determinada, cumpliendo con los requisitos establecidos por la legislación vigente y con algunas normas referentes a este tema aceptadas internacionalmente.

Sin embargo, en la última década, las instituciones bancarias del sector privado en Venezuela, han experimentado una serie de debilidades en relación a la detección de vulnerabilidades en sus canales electrónicos, lo

cual pone en riesgo, la información que se maneja de manera cotidiana en las mencionadas instituciones; razón por la cual, surge el interés por parte del autor, de emprender una investigación que permita formular una propuesta de un modelo basado en software libre para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

Al respecto, el proyecto de investigación, queda estructurado de acuerdo al siguiente orden:

Capítulo I. **El Problema**. Describe el planteamiento de la problemática que se pretende solucionar, las razones por las cuales se selecciona el tema de estudio, la descripción del contexto donde se va a realizar la investigación, así como también, se formulan las interrogantes de la misma. De igual forma, se indica el objetivo general de la investigación y los objetivos específicos que van a permitir su consecución, su justificación e importancia, cerrando este capítulo, con el alcance y las posibles limitaciones de la misma.

Capítulo II. **Marco Teórico.** Es uno de los más extensos, pues se describen los fundamentos que sustentarán el presente estudio. Inicia con la revisión de antecedentes, los cuales se seleccionan luego de una respectiva revisión bibliográfica a trabajos de grado de maestría, ascenso y artículos científicos.

Capítulo III. **Marco Metodológico**. En el que se detalla la estructura que tendrá la investigación y los procedimientos pautados para alcanzar efectivamente los objetivos. Se describen el tipo y nivel de la investigación, sustentando las razones por las que se eligen, las variables que determinan los objetivos específicos y su respectiva Operacionalización.

Igualmente, como parte de este capítulo, se describen las técnicas e instrumentos para la recolección de datos, se especifica la población y muestra, el cómo se va a realizar el análisis e interpretación de los datos, los procedimientos para determinar la confiabilidad y validez de los instrumentos, y por último las consideraciones éticas y legales que regirán la investigación.

Capítulo IV. **Resultados**. En el que se presentan la totalidad de los resultados arrojados como producto de la aplicación de los instrumentos de recolección de datos.

Capítulo V. **La Propuesta.** Capítulo donde se materializa la propuesta del modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

Capítulo VI. **Conclusiones y Recomendaciones.** En el cual se presentan las conclusiones y recomendaciones a las cuales se llegaron una vez finalizado el proceso de investigación.

Finalmente se presentan las referencias bibliográficas consultadas para el desarrollo de la investigación y los anexos respectivos.

CAPÍTULO I: EL PROBLEMA

Ante la presencia del mundo globalizado que actualmente se percibe, las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones; también ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados.

Es por ello que la presente investigación, se encuentra enfocada hacia la generación de un modelo que brinde la oportunidad de detectar las vulnerabilidades en los Canales Electrónicos, específicamente en las Instituciones bancarias del sector privado en Venezuela.

Para su desarrollo, se tomaron en consideración la totalidad de los aspectos que forman parte de este capítulo, entre los cuales se señalan; el planteamiento del problema, la formulación de las interrogantes, el enunciado del objetivo general de la investigación y de los objetivos específicos que van a permitir su consecución, la justificación e importancia, cerrando este capítulo, con el alcance y las posibles limitaciones de la misma.

1.1 Planteamiento del Problema

Al vislumbrar el inicio del siglo XXI, los Sistemas Informáticos se han constituido, en poderosos recursos que permiten materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los Sistemas de Información. Ante este panorama, Osorio (2010) explica: “la Informática hoy en día, suele ser la base en la gestión integral de la empresa, razón por la que las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a controles” (p. 33).

Menester es acotar, que la Informática no gestiona propiamente a la empresa, por el contrario, apoya la toma de decisiones, pero no decide por sí misma. Por ende y debido a su importancia en el funcionamiento de una empresa, se hace uso de la gestión de seguridad para la información de la empresa.

Ante esta afirmación, la información de una empresa u organización, es considerada como uno de los más importantes activos que esta posee; hallazgo que invita, a desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información, esta última, sujeta a muchas vulnerabilidades y amenazas tanto de índole interna como externa.

En la actualidad, las organizaciones a escala mundial y sus respectivos sistemas de información, se enfrentan, cada vez con mayor frecuencia, a un conjunto de riesgos, vulnerabilidades o amenazas que deberían estar sometidas al control correspondiente, con el propósito de evitar perturbaciones que pudiesen alterar el curso normal de las actividades cotidianas de la organización, independientemente del ramo al cual se dedique.

Muestra de ello, se puede evidenciar en la “Encuesta sobre Seguridad y Crimen de Computación 2009” llevada a cabo por el Instituto de Computación (*CSI, por sus siglas en Inglés*) donde, sobre la base de cuatrocientos treinta y tres (433) respuestas suministradas por diferentes entidades privadas y estatales de los Estados Unidos, se detectaron algunas de las amenazas más preocupantes, tal y como se refleja en el Gráfico N° 1.

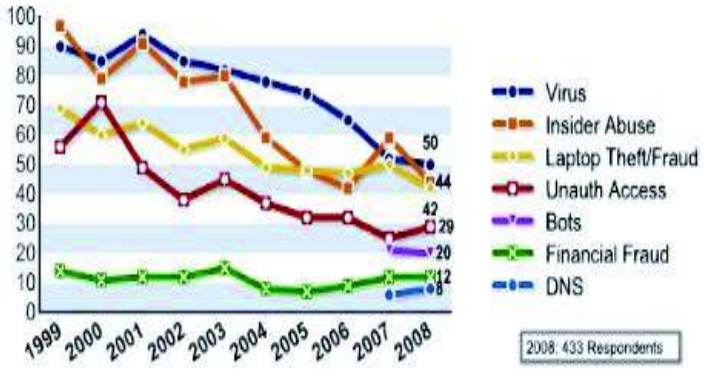


Gráfico N° 1. Amenazas a los Sistemas de Información.
Fuente: Instituto de Computación (CSI), 2008.

Al respecto, en el gráfico anterior, se observa que la mayor amenaza a los sistemas de información, la representan los virus con un 50%, mientras que el porcentaje más bajo lo presenta el DNS. Ahora bien, para el año 2012, la misma organización, realizó una encuesta a treinta y cuatro (34) organizaciones sociales a nivel centroamericano, la cual estuvo orientada hacia la medición del tipo de impacto de las distintas amenazas a los sistemas de información, lo que se demuestra en el Gráfico N° 2.

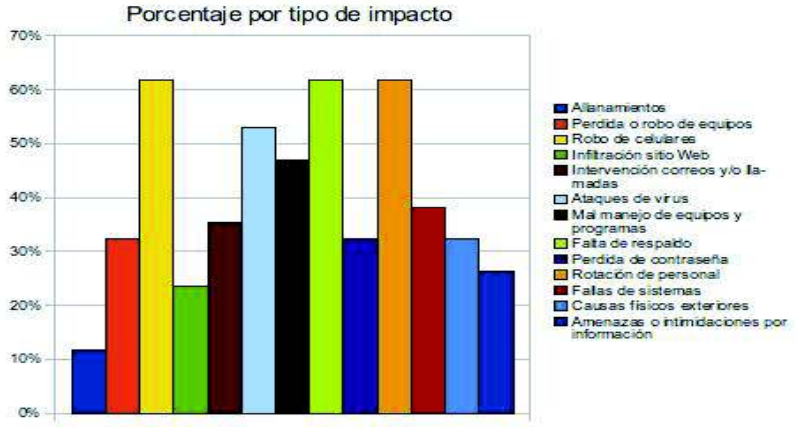


Gráfico N° 2. Porcentaje por tipo de impacto de las amenazas a los Sistemas de Información. Fuente: Instituto de Computación (CSI), 2012.

De los resultados presentados en el Gráfico N° 2, se concluye que la pérdida o robo de equipos, la falta de respaldo y la rotación de personal,

constituyen en un 60 %, las amenazas de mayor preocupación que tienden a vulnerar la información en las organizaciones sociales encuestadas. Además, al comparar los resultados de ambos gráficos, se puede inferir que existen ciertas similitudes con relación a las amenazas consideradas como de mayor preocupación, las cuales responden a:

- Ataques de virus (>50%)
- Robo de celulares, portátiles y otros equipos (>40%).

En este orden de ideas, para el año 2013, la Red de la Universidad Nacional Autónoma de México (UNAM) presentó los resultados de un estudio donde se detectaron los distintos tipos de incidentes ocurridos durante ese año, a propósito de la vulnerabilidad de los sistemas de información, hallazgos que se reflejan en el Gráfico N° 3.

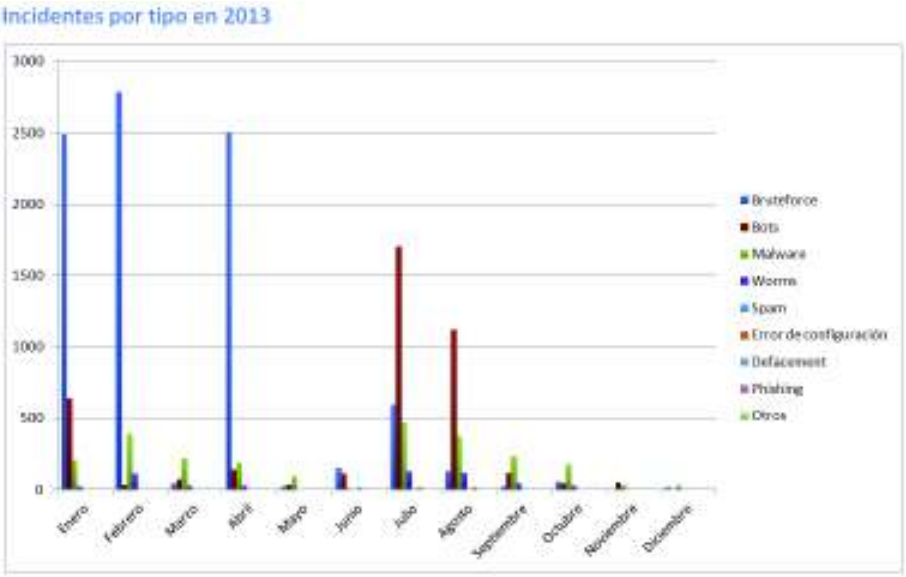


Gráfico N° 3. Incidentes ocurridos por tipo.

Fuente: Universidad Nacional Autónoma de México (UNAM), 2013.

Como se puede observar, el incidente que ocurrió con mayor frecuencia durante los meses de Enero, Febrero y Marzo, respondió al Bruteforce, mientras que durante Julio y Agosto los Bots ocuparon el mayor nivel de ocurrencia. Por otro lado, entre los de menor ocurrencia, destacan los Spam, Malware y los Worms entre otros.

Considerando los hallazgos presentados anteriormente, implementar la seguridad de la información dentro de una organización, suele ser un proceso sumamente complejo, que requiere además de la cooperación, el trabajo en equipo de las diferentes áreas organizacionales que componen una empresa o institución, ya que cada área, cuenta con un conjunto de saldos de información valiosos y orientados a mantener su gestión empresarial. Por ello, las instituciones bancarias no son ajenas a esta realidad y ante esta situación, hoy en día, se ven obligadas a hacer uso de la tecnología para poder satisfacer las necesidades de seguridad generando adicionalmente, sus propias políticas para garantizar el resguardo y la protección de uno de sus activos más preciados: la información.

Específicamente en la República Bolivariana de Venezuela, las instituciones bancarias del sector privado, de acuerdo a un estudio de doctorado realizado por Ruíz (2013) se señala que:

> En la actualidad, múltiples vulnerabilidades y amenazas asociadas a los activos de información que conforman la plataforma tecnológica de los canales de servicios bancarios, ha cobrado fuerzas en las dos últimas décadas, razón por la cual, las instituciones bancarias venezolanas, se han visto en la necesidad de acudir al desarrollo y activación de mecanismos orientados hacia el resguardo de la información, con el propósito de evitar posibles interrupciones de los servicios que prestan, así como también el temido fraude (p. 179).

Afirmación que permite inferir, que aún sigue latente la probabilidad de ocurrencia de eventos que alteren la seguridad de la información de las instituciones bancarias venezolanas, situación que de seguir repitiéndose, pudiera generar un clima de desconfianza por parte de los clientes de las señaladas organizaciones, ante posibles interrupciones de los servicios que prestan y posibles fraudes electrónicos, incrementando además, de forma progresiva los costos asociados a las pérdidas generadas por la ocurrencia de los mencionados hallazgos.

Con relación a los fraudes electrónicos, la Gerencia de Investigación y y Desarrollo Estadístico de la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN), realizó un estudio de su evolución trimestral, aunado a la situación de los distintos reclamos como producto de los fraudes en los distintos canales e instrumentos financieros durante el período 2013-2014, obteniendo como resultados relevantes, los presentados en el Gráfico N° 4.

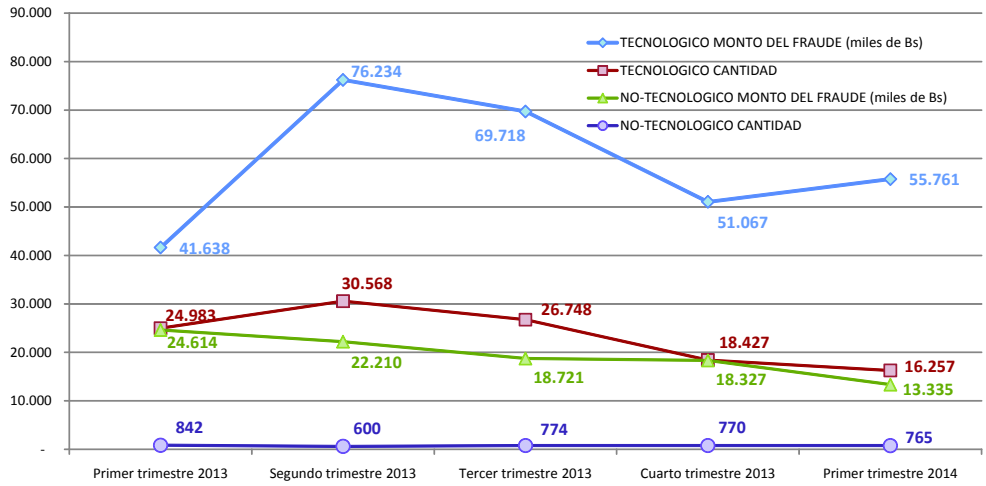


Gráfico N° 4. Evolución de los fraudes según sean tecnológicos o no tecnológicos por monto y cantidad.

Fuente: Gerencia de Investigación y Desarrollo Estadístico de la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN), 2014.

Al evidenciar el gráfico anterior, se puede observar que los montos de los fraudes tecnológicos superan en gran escala a los no tecnológicos, razón por la cual se requiere implementar medidas de seguridad que mitiguen la ocurrencia de los mismos. Ahora bien, la siguiente Tabla, refleja la Cantidad y monto de la pérdida por fraude en cada canal, según el instrumento financiero, al último trimestre del estudio realizado por la misma dependencia.

Tabla N° 1. Cantidad y monto de la pérdida por fraude en cada canal, según el instrumento financiero.

INSTRUMENTO	POS		ATM		INTERNET BANKING		OFICINA Y/O AGENCIA		AUTOBANCO		IVR		NO APLICA		TAQUILLA EXTERNA		TOTAL MONTO	TOTAL CANTIDAD
	CANTIDAD	MONTO DEL FRAUDE	CANTIDAD	MONTO DEL FRAUDE	CANTIDAD	MONTO DEL FRAUDE	CANTIDAD	MONTO DEL FRAUDE	CANTIDAD	MONTO DEL FRAUDE	CANTIDAD	MONTO DEL FRAUDE	CANTIDAD	MONTO DEL	CANTIDAD	MONTO DEL FRAUDE		
TARJETA CRÉDITO	2.829	6.848	11	3	2	1	2	1		-	9	331		-	13	6	7.189	2.866
TARJETA DÉBITO	777	2.638	880	1.049	264	716	105	995		-		-		-		-	5.397	2.026
CUENTA CORRIENTE		-		-	87	4.934	71	445		-		-		-		-	5.379	158
CHEQUES		-		-		-	27	904	14	464		-		-		-	1.368	41
NO APLICA	3	78	18	6		-	3	10		-		-		-		-	94	24
CUENTA DE AHORROS		-		-		-	7	38		-		-	3	9		-	47	10
LIBRETA DE AHORRO		-		-		-	9	33		-		-		-		-	33	9
Total	3.609	9.564	909	1.058	353	5.651	224	2.426	14	464	9	331	3	9	13	6	19.507.645	5.134

Fuente: Gerencia de Investigación y Desarrollo Estadístico de la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN), 2014.

Al respecto, se observa que los montos y las cantidades que impactan mayormente sobre las pérdidas por fraude en el sector bancario se realizan a través de los canales "*POS*", "*ATM*" e "*Internet Banking*" por medio de los instrumentos: "*Tarjeta de crédito*" y "*Tarjeta de débito*". Además cabe acotar

que para los meses de marzo y junio la cantidad de bancos que reportaron fraudes es: veintidós (22), para septiembre: dieciocho (18) y para diciembre: diecisiete (17). Importante es señalar, que estos hallazgos, reflejan solo una muestra de las distintas vulnerabilidades a las cuales están expuestos los canales electrónicos de las instituciones bancarias del país, lo cual permite inferir la necesidad de implementar mecanismos que permitan mitigar progresivamente la ocurrencia de estos eventos, garantizando a su vez, la seguridad de la información que se maneja en las mismas.

En este orden de ideas, son variados los mecanismos, herramientas, software u otras aplicaciones, que se emplean en virtud de garantizar la seguridad de los activos de información. Tal es el caso de Kali Linux, software que entre sus atributos más relevantes, permite la adhesión a una red determinada con el propósito fundamental, de ejecutar el análisis de los equipos que estén conectados, a fin de detectar vulnerabilidades tales como, puertos abiertos, configuraciones inseguras, antivirus vencidos y cualquier otra, que pudiese ser aprovechada para penetrar de forma inescrupulosa a la red.

Igualmente, Kali Linux, brinda la oportunidad de colocar las vulnerabilidades señaladas, en un archivo de texto plano, sin ningún orden en específico, para luego, construir un modelo de datos donde se pueda clasificar y categorizar las posibles debilidades y riesgos que pudiese afrontar la información, en este caso en particular, de los Canales electrónicos de las Instituciones bancarias venezolanas del sector privado.

Por tal motivo, surgió el interés por parte del investigador de emprender una investigación que permita proponer un modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela; planteamiento que promueve la formulación

de una serie de interrogantes que darán paso al cumplimiento efectivo de un proceso de investigación que otorgará respuesta efectiva a cada una de las mismas.

1.1.1 Formulación del Problema

¿De qué manera debe formularse una propuesta de modelo que permita facilitar la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela?

1.1.2 Sistematización del Problema

¿En qué condiciones se encuentra actualmente el proceso de detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela?

¿Qué requerimientos se deben considerar para la formulación de una propuesta de modelo que permita la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela?

¿Cuáles son las fases que se deben cumplir para formular una propuesta de modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela?

1.2 Objetivos de la Investigación

1.2.1 Objetivo General

Proponer un modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

1.2.2 Objetivos Específicos

La investigación plantea los siguientes objetivos específicos:

1. Diagnosticar las condiciones actuales del proceso de detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

2. Determinar los requerimientos a considerar para la formulación de una propuesta de modelo que permita la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

3. Realizar un modelo de datos que permita relacionar las vulnerabilidades detectadas con los controles descritos en los artículos de las Normativas relacionadas con la tecnología de la información.

4. Formular una propuesta de modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

5. Validar el Modelo a través del juicio experto de personal calificado en la Superintendencia de las Instituciones del sector Bancario en Venezuela.

1.3 Justificación de la Investigación

Tomando en consideración, el panorama globalizado que se vive a nivel mundial y latinoamericano con incidencia nacional, lo cual ha generado profundas transformaciones en áreas clave de la sociedad, incluyendo la que atañe a la tecnología, la propuesta de un modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela, constituye una posible alternativa solución ante los hallazgos evidenciados que denotan la presencia de una situación

problemática que afecta específicamente a la seguridad de la información de las mencionadas instituciones.

De allí, que esta investigación posea una relevancia desde el punto de vista referencial, ya que recopila y organiza un conjunto de teorías, principios, leyes y demás información, relacionada con la propuesta de modelos automatizados que brindan la oportunidad de detectar efectivamente, las vulnerabilidades de los sistemas automatizados que soportan los canales electrónicos en la Banca Venezolana. Lo que coadyuvaría en la determinación de los posibles riesgos que se deriven de estos y de las amenazas que pudieran explotarlos. Así mismo, se generaría información que podrá ser objeto de consulta para investigadores que muestren interés por el área de desarrollos de modelos y sistemas automatizados.

Igualmente, es importante destacar, la relevancia que desde el enfoque metodológico, deja plasmada esta investigación, ya que de una manera previamente estructurada, remite al lector a la consulta de diferentes autores que definen su postura en relación al tipo y diseño de investigación desarrollado, así como también, el conjunto de técnicas e instrumentos diseñados para la recopilación de la información, las cuales pueden ser consideradas para la formulación de otras propuestas afines al tema que se desarrolla.

En relación con los beneficios y aportes que brindó el desarrollo de esta investigación, los mismos estuvieron orientados hacia la generación de una alternativa viable de solución que de ser acogida, permitirá una adecuada determinación de vulnerabilidades como parte del proceso de gestión de riesgos de TI en las instituciones bancarias del sector privado en Venezuela, quienes se constituirán en los beneficiarios directos de la misma.

De igual manera, con la ejecución de este proceso de investigación, se puso de manifiesto el conjunto de conocimientos, habilidades y destrezas adquiridas por el autor, durante su proceso de formación académica en el programa de postgrado, Maestría en Sistemas de Información de la Universidad Católica “Andrés Bello”. Además, el colectivo de estudiantes y los docentes de la UCAB, contarán con un referente teórico y metodológico inherente a la propuesta de un modelo para la determinación de vulnerabilidades en sistemas computacionales.

1.4 Alcance y Limitaciones de la Investigación

En la presente investigación, la detección de vulnerabilidades se limita a los sistemas de información y al hardware que soportan los procesos operativos y de negocio presentes en las soluciones que ofrece la Banca Venezolana a través de los canales electrónicos, específicamente, mediante la banca por internet. De esta manera, la detección de vulnerabilidades a proponer incluye: las vulnerabilidades de red, aplicaciones inseguras, servicios orientados a web diseñados o implementados de forma deficiente y los equipos obsoletos o con mantenimientos deficiente.

Así mismo, el modelo resultante de la presente investigación, estará orientado a la evaluación de vulnerabilidades de forma automatizada, dada la capacidad de filtrar grandes volúmenes de datos: Se excluye, por tanto, la evaluación manual.

En función de cumplir con los objetivos planteados en la presente investigación, de un universo de diecinueve (19) instituciones bancarias del sector privado de Venezuela, solo se obtuvo acceso a diez (10), lo cual constituyó una limitante para el desarrollo del mismo.

CAPÍTULO II: MARCO TEÓRICO

El Marco teórico o referencial del presente Trabajo de Investigación estuvo estructurado tomando en consideración en primer lugar los antecedentes relacionados con el tema de estudio, y en segundo lugar, el conjunto de basamentos teóricos sobre los cuales se sustentó el mismo. En cuanto a este aspecto, Padrón (2000) señala que,

> En esta fase de proyecto, es importante que para cada una de las teorías seleccionadas se indique, por lo menos, lo siguiente: nombre de la teoría; nombres y referencias de sus creadores y propulsores originales; abarque empírico (sistema de hechos que pretende explicar); conceptos teóricos fundamentales; función que cumple la teoría en la ejecución de la investigación (p. 1).

2.1 Antecedentes de la investigación

Los antecedentes se refieren a los estudios anteriores o previos que se identifican con la investigación en curso y constituyen la base o apoyo dentro del tema objeto de estudio. Al respecto, Arias (2006) señala: "se refieren a los estudios previos y tesis de grado que están relacionados con el problema investigado" (p.38). Seguidamente, se presentan un conjunto de investigaciones realizadas que guardan estrecha vinculación con el tema desarrollado en este Trabajo de Grado.

Villamizar (2013), desarrolló un Trabajo de Maestría titulado **"Desarrollo de un Sistema Integrado de Gestión de la Seguridad de la Información del área de Control de operaciones de la empresa Plumrose Latinoamericana C.A."**, ante la Universidad Nacional Yacambú (UNY) para optar al grado académico de Magister Scientiarum en Gerencia, Mención: Sistemas de Información, teniendo como objetivo general, desarrollar un

Sistema Integrado de Gestión de la Seguridad de la Información del área de Control de operaciones de la empresa Plumrose Latinoamericana C.A.

Desde el punto de vista metodológico, este trabajo se fundamentó en un tipo de investigación de campo de nivel descriptivo; mediante el cual se recabaron una serie de datos relacionados con el manejo de la información en el área de Control de operaciones de la referida empresa. Para tal fin, se aplicó la observación estructurada mediante una Lista de Chequeo, con la que se pudo realizar un diagnóstico del manejo de la información en el área de Control de operaciones. Además, se apoyó en la metodología de desarrollo de software basada Ebios

Posteriormente, se obtuvieron una serie de resultados que permitieron redactar las conclusiones de la investigación, entre las cuales destacó que: El área de Control de operaciones de la empresa Plumrose Latinoamericana C.A. presenta una serie de debilidades reflejadas en el diagnóstico realizado, entre las cuales se percibe, los altos niveles de vulnerabilidad en la información almacenada relativa a esta área tan importante de la empresa.

Además, se recomendó a la empresa, la implementación del SGSI, el cual empleó la metodología Ebios para el desarrollo de software y aplicar el plan de pruebas correspondientes, a propósito de garantizar el buen funcionamiento del sistema.

Ahora bien, al vincular este antecedente con la presente investigación, se obtuvo que el mismo, facilitó una serie de referentes teóricos relacionados con Seguridad de la Información, amenazas y vulnerabilidades en la información, los cuales fueron consultados para ser incluidos en el marco teórico. Así mismo, la metodología empleada para el cumplimiento de los

objetivos planteados en el trabajo, brindó orientaciones para fortalecer desde el punto de vista teórico, su marco metodológico.

En este orden de ideas, Zúñiga (2012), presentó como Trabajo de Grado una **"Propuesta de un Modelo para la detección de Vulnerabilidades en los Sistemas de Información de las pequeñas y medianas empresas del Estado Aragua",** ante la Universidad Bicentenaria de Aragua (UBA) para optar al grado académico de Magister Scientiarum en Gerencia, mención: Sistemas de Información, planteando como objetivo general, proponer un Modelo para la detección de Vulnerabilidades en los Sistemas de Información de las pequeñas y medianas empresas del Estado Aragua.

En relación a la metodología desarrollada, esta se basó en un tipo de investigación de campo no experimental con un diseño de investigación descriptivo, sin obviar la revisión de literatura especializada tanto física como digitalizada. Como técnica e instrumento de recolección de datos, se emplearon la observación apoyada en una Check List basada en estándares ISO y un cuestionario tipo Likert, con la finalidad de recolectar información de las empresas seleccionadas, cuyos resultados permitieron formular un modelo que permitiese detectar vulnerabilidades en los Sistemas de Información de las pequeñas y medianas empresas ubicadas en el Estado Aragua, en virtud de garantizar la Seguridad de la Información en las mencionadas organizaciones.

Entre sus conclusiones, la autora de la investigación señala que se detectó la presencia de un conjunto de vulnerabilidades en los Sistemas de información de las empresas, lo cual pone en riesgo el activo de la información que se maneja de manera cotidiana en las mismas, situación que permite afirmar la necesidad de formular y proponer un modelo para

detectar las señaladas vulnerabilidades y poder aplicar las medidas y correctivos que sean requeridos de forma precisa y oportuna.

Este antecedente, aportó a la presente investigación, una serie de referentes de consulta relacionados con la detección de vulnerabilidades en la información y la seguridad de la información, así como aspectos relacionados con el marco metodológico, lo cual sirvió de guía orientadora para reforzar la teoría y la metodología a desarrollar en la investigación.

Otro hallazgo vinculado a esta investigación, fue el Trabajo de Grado presentado por Jiménez, (2012), titulado **"Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), para el resguardo y protección de los activos informáticos de la Universidad Bicentenaria de Aragua (UBA)"***,* ante la Universidad Bicentenaria de Aragua (UBA) para optar al grado académico de Magister Scientiarum en Gerencia, mención: Sistemas de Información. En relación al objetivo general, este giró en torno a diseñar un Sistema de Gestión de Seguridad de la Información, para el resguardo y protección de los activos informáticos de la Universidad Bicentenaria de Aragua (UBA).

Su metodología se basó en un tipo de investigación descriptiva, apoyada en un diseño de investigación de campo, lo que permitió recopilar información relacionada al tema de estudio, procesarla y analizarla para posteriormente obtener los resultados que generaron la base para el diseño del sistema de gestión de seguridad de la información.

Ahora bien, una de las conclusiones determinó que la Universidad Bicentenaria de Aragua (UBA) debe establecer un conjunto de políticas de seguridad para la información, así como también, resguardar sus activos tecnológicos y mantener documentados los procesos de seguridad en

función de proteger igualmente, la infraestructura tecnológica de posibles amenazas y ataques. Además, se recomendó a toda organización de carácter público o privado, implementar medidas de protección que permitan resguardar sus plataformas tecnológicas, aplicando auditorías permanentes de forma integral, a fin de reducir las vulnerabilidades y posibles riesgos que atenten contra sus sistemas de información.

Este antecedente, aportó una serie fuentes bibliográficas de interés para el autor de este trabajo, relacionadas con la seguridad de la información, así como también, con el proceso de detección de vulnerabilidades, las cuales fueron consultadas para reforzar el marco teórico de la investigación en desarrollo.

Igualmente, De León (2012), presentó un "**Modelo de Automatización basado en estándares de Software Libre para proteger la información. Caso: Gerencia Administrativa de la empresa TECNOLOGY 395 C.A."** para optar al grado académico de Magister Scientiarum en Gerencia de Sistemas ante la Universidad Metropolitana, planteando como objetivo general, desarrollar un Modelo de automatización basado en estándares de Software Libre para proteger la información de la Gerencia Administrativa de la empresa TECNOLOGY 395 C.A.

Su metodología estuvo apoyada en la modalidad de Proyecto factible, bajo un tipo de investigación mixto con nivel descriptivo, pudiendo recabar información de interés con la temática desarrollada, tanto de fuentes bibliográficas físicas y digitales, como directamente de la realidad objeto de estudio, en este caso en particular, de la Gerencia Administrativa de la empresa TECNOLOGY 395 C.A.

Una vez arrojados los hallazgos producto del análisis e interpretación de datos, se pudo concluir que la Gerencia Administrativa de la empresa TECNOLOGY 395 C.A. presenta un conjunto de vulnerabilidades y amenazas que afectarían considerablemente el tratamiento de la información que allí se maneja, razón por la cual, se propone automatizar los procesos, considerando los estándares de Software Libre, a fin de proteger los activos de información de la empresa en general.

Con respecto al aporte brindado por parte de este estudio, destaca el conjunto de elementos inherentes a la teoría que sustenta el software libre y a la validación de modelos de automatización, entre los cuales, cabe señalar, la recopilación de la información. El análisis de datos y de la fiabilidad del modelo, así como también, las fases del proceso de validación predictiva y confirmativa, aspectos que fueron considerados como orientaciones para ser recomendadas ante la futura aplicación del proceso de validación de modelo planteado en esta propuesta.

También, Quintero (2010), presentó una investigación titulada **"Gestión de Seguridad de la Información para instituciones bancarias del Estado Táchira"** ante la Universidad Nacional Experimental del Táchira (UNET) para optar al grado académico de Magister Scientiarum en Informática. Su objetivo general fue, desarrollar un modelo de gestión de seguridad de la información para instituciones bancarias del Estado Táchira.

Metodológicamente se fundamentó, en un tipo de investigación de campo de nivel descriptivo, permitiendo recabar información relacionada con la gestión de seguridad llevada a cabo en las instituciones bancarias, hallazgos que permitieron orientar la propuesta de gestión de seguridad generada. la población de estudio, estuvo conformada por el total de instituciones bancarias que se encuentran en el Estado Táchira, siendo

seleccionada como muestra intencional, un total de seis (6) instituciones bancarias.

En relación a los resultados obtenidos, se llegó a la conclusión, entre otras, que la actual gestión de seguridad de la información en las instituciones bancarias del Estado Táchira, presenta un conjunto de debilidades, entre las cuales destacan, una serie de vulnerabilidades y amenazas que ponen en riesgo los activos informáticos de las instituciones señaladas. Se recomendó a las instituciones bancarias del Estado Táchira, implementar procesos de control y seguimiento permanente mediante la aplicabilidad de auditorías al área de seguridad de la información para garantizar el resguardo y la protección de los activos de las mencionadas instituciones.

El aporte brindado a esta investigación, se fundamentó en la teoría relacionada con las generalidades de las instituciones bancarias, así como también, lo concerniente a la seguridad de la información y la detección de vulnerabilidades, lo cual permitió realizar las consultas de las fuentes seleccionadas y por consiguiente, ampliar el marco teórico de la misma.

2.2 Fundamentos teóricos

Según Bavaresco (2006), las bases teóricas tiene que ver con las teorías que brindan al investigador el apoyo inicial dentro del conocimiento del objeto de estudio (p.18). Es decir, cada problema posee algún referente teórico, lo que indica, que el investigador no puede hacer abstracción por el desconocimiento, salvo que sus estudios se soporten en investigaciones puras o bien exploratorias. Las bases o fundamentos teóricos de esta investigación, se presentarán de acuerdo al siguiente orden.

2.2.1. Proceso de detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela

2.2.1.1. Definición de Vulnerabilidad

De acuerdo a la perspectiva de la seguridad de la información, para León (2009), "una vulnerabilidad, constituye una debilidad que se detecta en un activo o en un control determinado y que se caracteriza porque ser explotada por una o más amenazas, lo que se trasforma, en un riesgo de seguridad" (p. 29). Al respecto, una vulnerabilidad informática, se entiende como elemento de un sistema informático, que suele ser considerado, por un atacante para lograr irrumpir la seguridad, causando igualmente, un conjunto de daños por sí mismos, sin tratarse de un ataque premeditado.

2.2.1.2. Tipos de Vulnerabilidades

Para describir los tipos de vulnerabilidades, se ha considerado el conjunto de postulados y señalamientos planteados por León (2009). Seguidamente, se sintetizan los tipos de vulnerabilidades existentes, considerando al mencionado autor:

Física. Vinculada con el acceso físico al sistema. Hace referencia al acceso y a las instalaciones donde se encuentran los equipos de cómputo que poseen la información o forman parte esencial de los procesos inherentes al sistema. Menester es señalar, que esta modalidad de vulnerabilidades, generalmente, se presentan materializadas en malas prácticas de las políticas de acceso de personal a los sistemas y en el uso poco asertivo, de medios físicos de almacenamiento de información que extraen los datos del sistema de manera no autorizada.

Natural. Todas las amenazas naturales están relacionadas directamente con desastres originados por fuerzas naturales que dañan un

sistema. Por ello, este tipo de amenazas, hacen referencia al grado en que un sistema, puede verse afectado por este tipo de eventos. Además, las vulnerabilidades naturales, se presentan primordialmente en aquellas deficiencias relacionadas con las medidas consideradas para hacerle frente a los desastres, por ejemplo no disponer de reguladores, no-breaks, carencias en el sistema de ventilación o calefacción, entre otros.

Hardware. Esta modalidad de vulnerabilidades de hardware, constituyen la probabilidad de que las piezas físicas del sistema fallen; bien sea por uso poco asertivo o por descuido e inclusive por fallas en el diseño, dejando al sistema, totalmente desprotegido o inoperativo. Igualmente, se relaciona con las formas en que el hardware, es empleado por personas inescrupulosas, para atacar la seguridad del sistema.

Software. Cada programa, independientemente si es de paquete o de sistema operativo, puede ser empleado, como un recurso para atacar a un sistema más grande. Tal situación, tiene su origen en errores de programación, o en virtud de que en el diseño, no fueron considerados, controles de acceso; seguridad; implantación, entre otros; lo que lo hace susceptible a las amenazas de software.

Redes. Las redes suelen llegar a constituirse en sistemas altamente vulnerables, ya que estas representan, una serie de equipos que se encuentran conectados entre sí y que comparten recursos. Por tal razón, existe la latente posibilidad, de atacar la totalidad de la red penetrando en primer lugar, en uno de los equipos y posteriormente expandirse al resto.

Cabe acotar, que en toda red, lo prioritario es la transmisión de la información, por consiguiente, la totalidad vulnerabilidades están interrelacionadas con la posibilidad de que la información, sean irrumpida por

personas no autorizadas y con fallas en relación a la disponibilidad del servicio. Tales situaciones, ocasionan que las vulnerabilidades de las redes lleguen a constituirse en una combinación de vulnerabilidades de hardware, software, físicas e incluso naturales.

Factor humano. En cuanto a este aspecto, cabe señalar que en un sistema, el factor humano, es el más complicado de controlar, constituyéndose en constantes amenazas y siendo uno de los elementos, que ocasiona mayor vulnerabilidad en todo sistema. Tal afirmación, responde que este tipo de vulnerabilidad, atiende generalmente a la falta de capacitación y conciencia, lo que genera situaciones donde se percibe, negligencia en el seguimiento de las políticas de seguridad, y mal uso del equipo.

Ejemplo de ello, es el robo de información o la destrucción de sistemas, los cuales, pueden ser producto, de una vulnerabilidad humana, ya sea porque un usuario de manera accidental, reveló las contraseñas de acceso o no revisó de forma periódica los registros de las actividades ejecutadas por el equipo. Finalmente, es de suma relevancia, reflexionar en relación a que toda vulnerabilidad, se pueden mitigar, eliminar o controlar lo que contribuye a contrarrestar la posibilidad de que una amenaza se llegue a materializar, llegando a convertirse en un ataque.

2.2.1.3. Detección de Vulnerabilidades

El proceso para la detección de vulnerabilidades en redes de datos que se propone en esta investigación, está sustentado en la metodología de Franco, David A, Perea, Jorge L, & Puello, Plinio. (2012). El mismo, consta de tres (3) fases que se encuentran soportadas por herramientas de software, a través de las cuales, se pretende obtener las vulnerabilidades en

los equipos de red y servidores en los canales electrónicos de las Instituciones bancarias venezolanas del sector privado.

Al respecto, este proceso se diferencia de otros en la medida en que se soporta cada etapa en herramientas software. Por tal razón, en cada fase se puntualizan las acciones que se deben realizar y cómo se deben llevar a cabo a través de las herramientas apropiadas. El esquema del proceso para detección de vulnerabilidades en redes de datos, se presenta en la siguiente figura.

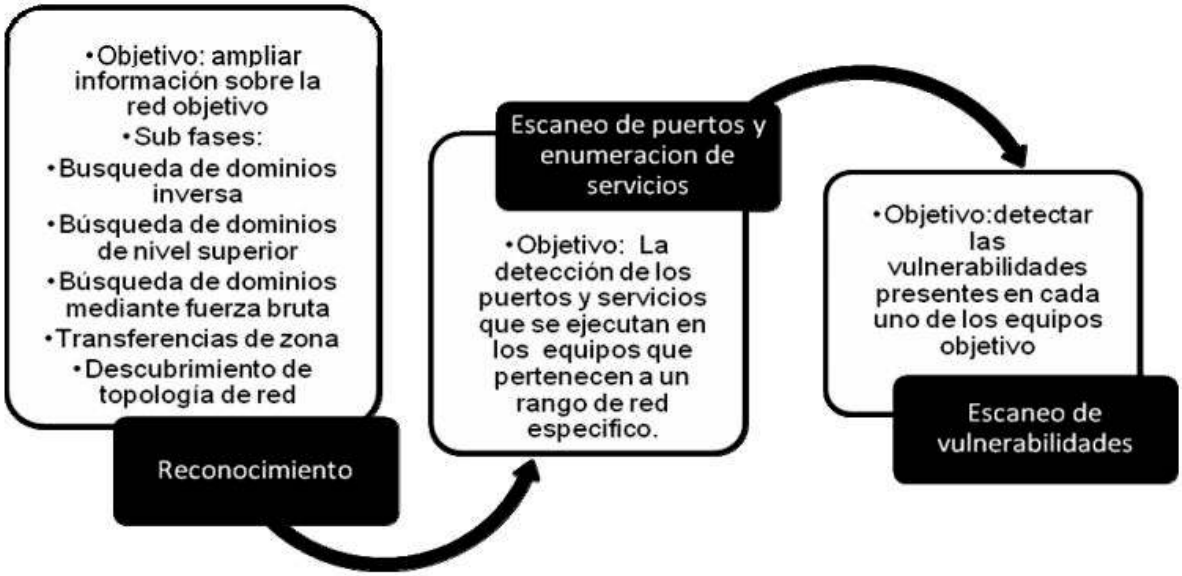


Figura 1. Esquema de la metodología para la detección de vulnerabilidades en redes de datos. Fuente: Franco, David A, Perea, Jorge L, & Puello, Plinio. (2012)

La figura anterior, permite evidenciar cada una de las fases que deben llevarse a cabo. Con relación a la primera fase, esta consiste en obtener tanta información como sea posible de la red o canal objetivo, para esto, se implementan técnicas basadas en diferentes tipos de consultas a servidores

DNS y otras que se fundamentan en el análisis de los mensajes de enrutamiento.

Cabe acotar, que esta fase no busca obtener vulnerabilidad alguna, lo que se pretende con ella, es obtener una lista lo más amplia posible sobre los equipos con presencia en internet de la red objetivo. Dicha lista de equipos de red, es empleada en la segunda fase, denominada escaneo de puertos y enumeración de servicios, en esta fase se evalúan los equipos obtenidos para determinar los puertos y servicios que están activos en cada uno de ellos.

Ahora bien, dependiendo del tipo de puerto y servicio que este activo en cada equipo se puede inferir, el rol que este juega dentro de la organización. Nuevamente, se anota que en esta fase no se pretende encontrar vulnerabilidad alguna, sino determinar los equipos críticos de la red objetivo a los cuales se les aplicará el escaneo de vulnerabilidades, que constituye la fase final de esta metodología.

Una vez obtenida la lista de los equipos de la red objetivo con presencia en internet y habiendo determinado cuáles de ellos juegan un rol crítico para la red, se procede con la fase final de la metodología propuesta. La cual evaluará a los equipos críticos en busca de vulnerabilidades. Es en esta última fase en la que se realiza la evaluación de todos los servicios y puertos activos de cada uno de los equipos encontrados como críticos para la red objetivo.

2.2.2. Requerimientos a considerar para el desarrollo de una propuesta de modelo para la detección de vulnerabilidades en los canales electrónicos de las Instituciones bancarias

2.2.2.1. Automatización

2.2.2.1.1. Concepto de Automatización

Para Cánchica (2012), la automatización “es un sistema mediante el cual, se trasfieren tareas de producción, realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos” (p. 33). Lo que permite afirmar, que la automatización está constituida por la tecnología que trata de la aplicación de sistemas mecánicos, electrónicos y de bases computacionales para operar y controlar tareas y/o actividades, que inicialmente se llevaban a cabo manualmente. Esta tecnología suele incluir algunos aspectos tales como:

a) Herramientas automáticas para procesar partes.
b) Máquinas de montaje automática.
c) Manejo automático de material y sistemas de almacenamiento.
d) Sistemas de inspección automática para control de calidad.
e) Control de reaprovechamiento y control de proceso de computadora.
f) Sistemas computarizados para la planeación de recolección de datos y toma de decisiones para apoyar las actividades manufactureras.

Menester es señalar, que un sistema automatizado consta de dos partes principales:

La parte de mando, la cual suele ser una tecnología programada, aunque hasta no hace mucho tiempo, se utilizaban relés electromagnéticos, tarjetas electrónicas o módulos lógicos neumáticos; los cuales atienden a la tecnología cableada. Importante es acotar, que en un sistema automatizado, el autómata programable está en el centro del sistema, siendo capaz de comunicarse con todos los constituyentes del sistema.

Por otro lado, se encuentra la *parte operativa* la que actúa directamente sobre la máquina. Son los elementos que hacen que la máquina se mueva y realice la operación deseada, los que forman la parte operativa son los accionadores de las máquinas como motores, cilindros, compresores y los captadores como fotodiodos, finales de carrera. En este orden de ideas, la automatización tiene los siguientes propósitos:

- Mejorar la operatividad de la empresa u organización, reduciendo los costos y mejorando su productividad.
- Mejorar las condiciones de trabajo del personal, suprimiendo los trabajos engorrosos e incrementando los niveles de seguridad.

- Realizar operaciones cuyo control intelectual o manual se dificulta.

- Simplificar las actividades de mantenimiento del proceso operativo y de control y seguimiento.

2.2.2.1.2. Tipos de Automatización

Ahora bien, se encuentran varios tipos de automatización, entre los cuales se señalan:

1. *Automatización fija:* La cual se caracteriza por contar con una fuerte inversión inicial, generar altos índices de operatividad y ser relativamente flexible en virtud de adaptarse a los cambios.

2. *Automatización programable:* En la cual se debe contar con una fuerte inversión financiera específicamente en cuanto a la adquisición de equipos, siendo flexible de igual forma, para lidiar con cambios de configuración.

3. *Automatización flexible:* Caracterizada por generar una fuerte inversión monetaria, generar índices de operatividad media y ser flexible, igual que las modalidades anteriores.

Importante es acotar, que entre algunas de las ventajas o beneficios que implica el automatizar procesos, se pueden citar: Incremento de la operatividad, disminución del alto costo de mano de obra, seguridad, mejoras en la calidad de servicio y la reducción de tiempo y espacio.

2.2.2.2. Requerimientos para un modelo para la detección de vulnerabilidades en los canales electrónicos de las Instituciones bancarias

2.2.2.2.1. Software Libre

El Software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere parafraseando a lo señalado por Arriola (2008) a cuatro libertades de los usuarios del software:

- La libertad de usar el programa, con cualquier propósito (libertad 0).

- La libertad de estudiar cómo funciona el programa y adaptarlo a sus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.

- La libertad de distribuir copias, con lo que se puede ayudar a otros colegas (libertad 2).

- La libertad de mejorar el programa y publicar las mejoras de modo que toda la comunidad se beneficie. (libertad 3). El acceso al código fuente es un requisito previo para esto.

Por su parte, Rodríguez (2010), también hace referencia que cuando se habla de Software Libre, se refiere a libertad, no al precio. Las licencias "General Public Licenses" están diseñadas para asegurar:

1. La libertad de distribuir copias del software libre (y cobrar por ese sencillo servicio si así lo desea).
2. Recibir el código fuente (o tener la posibilidad de obtenerlo si así lo desea).
3. La libertad de modificar el software o utilizar partes de el en nuevos programas de software libre.
4. La libertad de ejecutar el programa con cualquier propósito.
5. La libertad de estudiar cómo funciona el programa y adaptarlo a las necesidades propias.
6. La libertad de mejorar el programa y liberar esas mejoras al público y de ese modo beneficiar a toda la comunidad.
7. La Libertad de que el usuario este informado, de que tiene la posibilidad de hacer todas estas cosas.

Cabe acotar, que para que estas libertades sean reales, deben ser irrevocables mientras no se haga nada incorrecto. Por consiguiente, si el desarrollador del software tiene el poder de revocar la licencia aunque no se le haya dado motivos, el software no es libre.

Con relación a la ubicación del software libre en distintas clasificaciones, se consideran las siguientes:

a) De acuerdo al costo de adquisición: el Software Libre puede ser de las dos clases, es decir, de costo cero o de costo mayor que cero. Lo que lo diferencia del Software Propietario es que su costo es independiente del número de computadoras que se poseen. Por ejemplo, en el caso del Sistema Operativo Microsoft Windows 3.1/95/98/Me/NT/2000/XP por cada computadora en que lo instale debo pagar una licencia. En cambio, si utilizo en Sistema Operativo GNU/Linux (en cualquiera de sus distribuciones, como Red Hat, Mandrake, Debian, Ututo) debo pagar una sola licencia (no obstante, algunas licencias no tienes costo).

b) De acuerdo a la apertura del código fuente: el Software Libre siempre es “open source”, es decir, de código fuente abierto, ya que dijimos que el acceso al código fuente es necesario para el ejercicio de las libertades 1 y 3 arriba descriptas. El ser “open source” implica una serie de ventajas que serán descriptas en la sección “Ventajas del Software Libre”.

c) De acuerdo a su protección: el Software Libre siempre está protegido con licencias, y más específicamente, con licencias de copyleft. ¿Por qué no de dominio público? Porque de ese modo cualquiera puede adueñarse de el, por ejemplo, adquiere un Software Libre, lo modifica, lo compila y lo distribuye con código cerrado. ¿Por qué no con Copyright? Porque de esa manera alguien le puede agregar alguna restricción, por lo tanto no va a seguir siendo Software Libre.

d) De acuerdo a su legalidad: el Software Libre siempre es legal, porque al usarlo, estudiarlo, modificarlo, adaptarlo y/o mejorarlo no estoy violando ninguna norma, ya que de por si este tipo de software

me permite hacerlo, con la única salvedad de no poder agregarle ninguna restricción adicional cuando lo transfiera a otra persona.

A manera de síntesis, el Software Libre tiende a ofrecer una serie de "libertades" a los usuarios, tales como: el uso del programa para los fines que fue creado o con el propósito que desee el usuario; permite el estudio completo del programa (incluido el código fuente) para su adecuación a las necesidades individuales; la distribución de copias del software con el propósito de darlo a conocer y de alcanzar una mayor cobertura; asimismo, persigue, que este se enriquezca con las experiencias de uso y mejoras que propongan los beneficiarios.

También, se pretende la difusión de las mejoras y modificaciones que se hayan realizado progresivamente al sistema, y con esto, su constante adaptación a las necesidades que surgen con el paso del tiempo. Importante es resaltar, que los conceptos señalados requieren de reflexiones cuidadosas para su correcta interpretación y aplicación. Para decidir si una licencia de software concreta es una licencia de software libre, deberá juzgarse sobre estas bases.

2.2.2.2.4. Base de datos de vulnerabilidades

También llamadas Listas de Vulnerabilidades, son recopilaciones de vulnerabilidades o condiciones predisponentes que existen en los sistemas y que deben ser identificadas y resueltas antes que una amenaza pueda materializarse a través de estas. En este sentido, la publicación *NIST Special Publication 800-30 Revision I: Guide to Conducting Risk Assesment*, proporciona una lista de vulnerabilidades a considerar. Otras fuentes con listas de vulnerabilidades a consultar incluyen: El National Vulnerabilit Database (NVD), es el repositorio oficial del Gobierno de Estados Unidos, en el que se encuentran, los datos de gestión de vulnerabilidades basadas en

estándares, representado mediante el Protocolo de Seguridad de Contenido Automatización (SCAP); Common Weakness Enumeration; Open Web Application Security Project – OWASP; entre otros.

Estos datos, permiten la automatización de la gestión de la vulnerabilidad, la medición de la seguridad y el cumplimiento. Al respecto, NVD incluye bases de datos de listas de control de seguridad, fallas de software relacionados con la seguridad, errores de configuración, nombres de productos y métricas de impacto.

2.2.2.2.5. Normativas de Tecnología de la Información

Son las Normativas regulatorias vigentes emitidas por la Superintendencia de las Instituciones del Sector Bancario en Venezuela (SUDEBAN), las cuales tienen como objetivo establecer los lineamientos básicos que deberán cumplir los sujetos sometidos a la supervisión de ese Organismo, en la implantación y uso de Tecnología de la Información, así como, en la prestación de servicios financieros desmaterializados, banca en línea, electrónica y virtual. Entre las normas más destacadas, se encuentran la "*Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones bancarias* y las *"Normas que Regulan el uso de los Servicios de la Banca Electrónica",* mejor conocida como la Resolución 641.10.

2.2.3.1. Seguridad de la Información

Para el Instituto Colombiano de Normas Técnicas y Certificación (INCOTEC) (2004) "La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en

películas o hablada en una conversación (p. 67). Lo que significa que, cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debería estar apropiadamente protegida.

Al respecto, Espiñeira, Sheldon y Asociados (2005) brindan una definición de Seguridad de la información, también conocida como Seguridad informática refiriéndose a ella como "la encargada de proteger los activos de información de una organización contra pérdidas o el uso indebido de la misma, además de permitir el acceso a los activos de la información, dando apoyo a los objetivos de la organización" (p. 32).

En función de la definición anterior, la misma desempeña un rol estratégico fundamental en todos los procesos de negocios, ya que identifica los recursos que deben resguardarse o restringirse dentro de una empresa, lo cual promueve la mejora de las operaciones con clientes, socios, proveedores y trabajadores de la misma. Complementando esta afirmación, la figura 2, muestra la relación que existe entre la Seguridad de la información con los recursos de la organización.

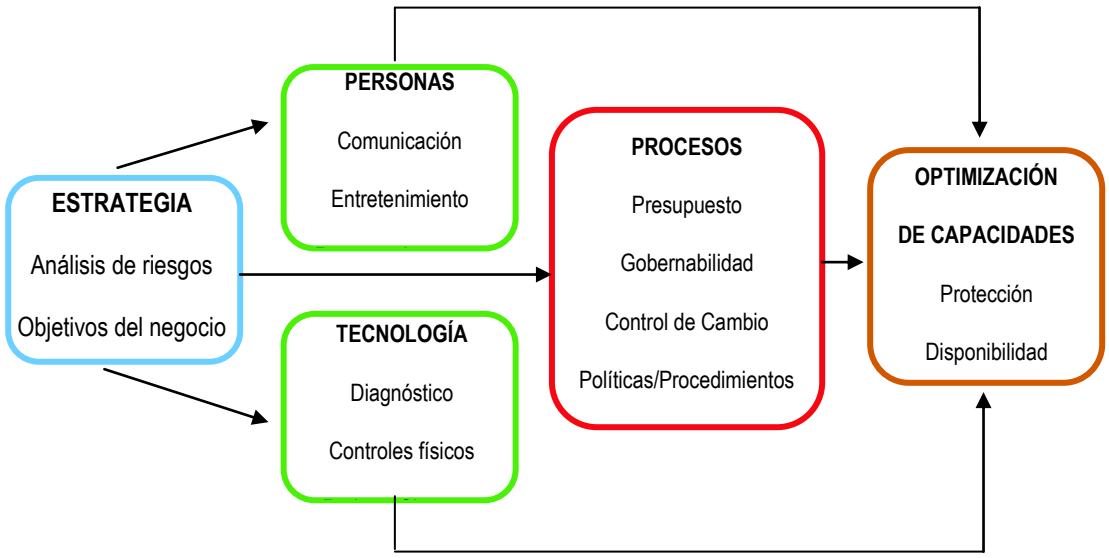


Figura 2. Seguridad de la Información: Componente organizacional, Recursos, Procesos y Tecnología Fuente: Adaptado de Espiñeira, Sheldon y Asociados (2005).

De esta figura se desprende, que el término de seguridad de la información, no constituye exclusivamente un aspecto tecnológico, sino que también, representa una solución integrada de negocio que suele fusionar recursos organizacionales, procesos y tecnología. Por tal razón, el investigador considera, que debe contarse con un conjunto de normas, lineamientos, asignación de funciones, además de considerar los procedimientos previamente establecidos y el talento humano capacitado para la gestión del proceso.

Por su parte, Bossio y Gros (2003), afirman que “el término Seguridad informática para referirse a Sistemas de información, existe desde hace tiempo y se encuentra en fase de evolución en virtud de las constantes transformaciones en el área de Informática” (p. 36).

Por ello, el autor de esta investigación afirma que, los cambios contemporáneo, aunado a la globalización y el crecimiento desmesurado de las telecomunicaciones, aumentan considerablemente las vulnerabilidades y las amenazas. Ahora bien, la seguridad de la información se sustenta en tres elementos claves, los cuales se resumen en el Cuadro 1:

Cuadro 1

Elementos claves de la Seguridad de la Información

Criterios	Descripción
Integridad	Garantía de que la información, es creada modificada o intervenida sólo
Disponibilidad	Garantía de que la información estará en el momento y la manera justa en la que es requerida por el personal autorizado.
Confidencialidad	Certeza de que la información, no es intervenida por personas o entidades no autorizadas.

Fuente: Elaboración propia.

Adicionalmente, a los elementos claves de la seguridad de la información, se tiene que su propósito fundamental, es preservar y distribuir de manera adecuada la información, y para ello, a juicio de Oz (2005), la seguridad de la información:

- Tiende a reducir considerablemente el riesgo de que los Sistemas de información cese sus operaciones.
- Contribuye al mantenimiento de la confidencialidad de la información que maneja la organización.
- Promueve la formulación y diseño de estrategias orientadas a garantizar la integridad y confiabilidad de los datos.
- Permite que la información sea mantenga disponible.
- Garantiza el cumplimiento de las disposiciones legales en la materia, así como también las políticas y procedimientos de la empresa en materia de resguardo de la información.

Por ello, a juicio de Bossio y Gros (2003), la seguridad de la información, es considerada

> Como un conjunto sistémico de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos administrativos y humanos, integrados en función de proveer toda la protección debida, requerida y oportuna, a la información y a los recursos informáticos de una empresa, institución u organización (p. 42).

Ahora bien, existen algunos tipos de seguridad de la información, vinculados con las diversas dimensiones que posee la información. tal tipología, responde a los aspectos físicos; es decir, a los soportes físicos, los lógicos; necesarios para emplear la información y el software, los administrativos; los cuales, generan planes para contingencias y los legales; relacionados con la normativa legal que rige todo lo inherente a la seguridad de la información. Seguidamente, esta tipología, se detalla en el Cuadro 2, basándose en los señalamientos realizados por Ramió (2006), y Donado y otros (2002):

Cuadro 2

Tipos de Seguridad de la Información

Tipos de Seguridad	Descripción
Física	Relacionada con la totalidad de los soportes físicos que emplean los sistemas de informática para el manejo de la información; pretende asegurar la plataforma básica donde circula la información
Lógica	Vinculada con los elementos necesarios para emplear la información y el software; garantiza la confidencialidad y disponibilidad de la información, consistencia en el sistema de información y un efectivo control de acceso al mismo.
Administrativa	Es complementaria y atiende a la protección de las políticas de seguridad, personal y gestión de riesgos, generando además, planes de contingencia ante posibles hechos fortuitos.
Legal	Pretende la aprobación de la normativa legal vigente en la materia, a fin de resguardar de manera efectiva la información.

Fuente: Elaboración propia.

2.3 Bases Legales

Esta sección de la presente investigación, señala las disposiciones que sustentan legalmente la realidad objeto de estudio. Para el Manual, Normas y Orientaciones para la Elaboración del Trabajo de Grado de la Universidad Alejandro Humboldt (UAH) (2011), las bases legales, "Se refieren a lo señalado en la Constitución de la República Bolivariana de Venezuela, las Leyes Orgánicas, los Reglamentos y Normas que le dan un basamento jurídico que puede condicionar el desarrollo del trabajo de investigación, cuando este así lo amerite (p. 18). A continuación se presenta el fundamento legal que sustenta la investigación.

La Constitución de la República Bolivariana de Venezuela, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela, Número: 36.860, de fecha 30 de Diciembre de 1999, establece en el Título III, De los Derechos Humanos y Garantías, y de los Deberes, específicamente en el Artículo 110, donde se reconoce, el interés público por la ciencia, la tecnología, el conocimiento, la innovación y sus respectivas aplicaciones, señalando en el Capítulo VI, De los Derechos Culturales y Educativos, que:

> ***Artículo 110.*** El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía (p. 16).

Como se puede observar, en este artículo se plasma el interés del Estado en impulsar la ciencia y la tecnología, así como también, todas aquellas actividades orientadas hacia la innovación y en beneficio del desarrollo del país, esto incluye los Servicios de información, los cuales deben regirse de acuerdo a las disposiciones legales vigentes, lo cual se vincula directamente con el propósito fundamental de esta investigación, el cual está orientado hacia la propuesta de un modelo basado en software libre para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

Por su parte, la Ley Especial contra Delitos Informáticos es publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.313 del 30 de Octubre de 2001, con el propósito fundamental, brindar protección integral de todos los sistemas que empleen tecnologías de información, sean de carácter público o privado. Es por ello, que en el Título I, Capítulo I, Disposiciones Generales, establece:

> ***Artículo 1.*** Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley (p. 1).

Al respecto, este instrumento legal fortalece el auge de las comunicaciones y el desarrollo de las tecnologías en el país. En su contenido, se refleja de igual forma todo lo referente a los sistemas informáticos y a los posibles delitos que se cometan haciendo uso de los mismos, lo cual incluye los modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

De igual forma, en este mismo Capítulo, presentan un conjunto de definiciones que guardan estrecha vinculación con la investigación en curso, y las cuales se presentan a continuación:

> ***Artículo 2.*** Definiciones. A los efectos de la presente ley y cumpliendo con lo previsto en el art. 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por: a. **Tecnología de Información:** rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data. b. **Sistema**: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas. c. **Data (datos)**: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado. d. **Información**: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas. e. **Documento**: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos. f. **Computador**: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas. g. ***Hardware***: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes. h. ***Firmware***: programa o segmento de programa incorporado de manera permanente en algún componente de hardware. i. ***Software***:

información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas. j. **Programa**: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador. k. **Procesamiento de data o de información:** realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo. l. **Seguridad**: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación. m. **Virus**: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema. n. **Tarjeta inteligente:** rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla. o. **Contraseña (*password*):** secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema. p. **Mensaje de datos:** cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones (p. 3).

Ahora bien, en el Capítulo I: De los Delitos contra los Sistemas que utilizan Tecnologías de Información, se describen en el Título II, desde el Artículo 6 hasta el Artículo 12, una serie de Delitos, con sus respectivas penas; entre los cuales cabe señalar: el acceso indebido a un sistema, el sabotaje, el espionaje y la falsificación.

> ***Artículo 6.*** Acceso indebido. El que sin la debida autorización o excediendo la que hubiera obtenido, acceda, intercepte, interfiera

o use un sistema que utilice tecnología de la información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Artículo 7. Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de la información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de la información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y la multa será de quinientos y mil unidades tributarias, si los efectos indicados en el presente artículo se realizaran mediante la creación, introducción, o transmisión, por cualquier medio, de un virus o programas análogos.

Artículo 9. Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de la información protegido por medios de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Artículo 11. Espionaje Informático. El que indebidamente obtenga, revele o difunda la data o información contenida en un sistema que utilice tecnología de la información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multado con cuatrocientos a ochocientas unidades tributarias. La pena será de un tercio a la mitad, si el delito previsto en el presente artículo se cometiera con el fin de obtener algún tipo de beneficio para si o para otros. El aumento será de la mitad a dos tercios, si se pusiera en peligro la seguridad del estado. La confiabilidad del estado de la operación de las instituciones afectadas o resultara algún daño para las personas naturales o jurídicas como consecuencia de la relación de las informaciones de carácter reservado.

Artículo 12. Falsificación de documentos. El que, a través de cualquier medio, cree, modifique, o elimine un documento que se encuentre incorporado a dicho sistema, un documento

> inexistente, será penado con prisión de tres a seis años y multa de trescientos y seiscientas unidades tributarias. Cuando el agente hubiera actuado con el fin de procurar para si o para otro algún tipo de beneficio, la pena se aumentara en precio un tercio y la mitad.

Al respecto, el articulado anteriormente señalado guarda estrecha vinculación con el objetivo general de esta investigación, en virtud de que se pretende generar una propuesta de un modelo basado en software libre para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela y por lo tanto, se deben considerar los diferentes delitos informáticos planteados anteriormente, a fin de aplicar los mecanismos necesarios que permitan resguardar la mencionada información, librándola de posibles riesgos que pudieran vulnerarla.

2.4 Definición de Términos

Administración Integral de Riesgo: Conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y revelar los distintos tipos de riesgos a que se encuentran expuestas las Instituciones bancarias. (León, 2009).

Amenaza: Posibles eventos que pueden desencadenar un incidente en la Institución Financiera, produciendo daños materiales o pérdidas inmateriales en sus activos y en las operaciones normales del negocio, interrumpiendo en algunos casos los servicios que prestan (Harris, 2009).

Autenticación: Proceso de comprobación de la identidad de una persona, de un usuario emisor o receptor de información (León, 2009).

.

Banca Electrónica: Comprende a todo servicio bancario y/o financiero, ofrecido por una entidad y basado en el uso de tecnología para la ejecución de operaciones y transacciones por parte de un usuario de servicios financieros, con mínima o ninguna asistencia o participación de un operador humano (Ruiz, 2008).

Banca en Línea: Incluye todos los sistemas, equipos, servicios y productos que son ofrecidos a los usuarios de las Instituciones bancarias a nivel de sus agencias, oficinas y sucursales (Ruiz, 2008).

Base de Datos: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior empleo (Oz, 2005).

Canal Electrónico: Comprende a los medios, dispositivos, redes y servicios informáticos dispuestos por las entidades financieras, por sí o por intermedio de terceros en calidad de prestadores asociados, para la instrucción de operaciones bancarias, con efecto sobre las cuentas de uno o más usuarios de servicios financieros y/o clientes de esas entidades (Ruiz, 2008).

Control de Acceso: Proceso relacionado con la evaluación, desarrollo e implementación de medidas de seguridad para la protección de la identidad, mecanismos de autenticación, segregación de roles y funciones y demás características del acceso a los Canales Electrónicos (Harris, 2009).

Dispositivos: Comprende a los elementos físicos específicamente diseñados y dispuestos para la interacción directa entre los clientes y el Canal Electrónico, así como otros usuarios calificados para el mantenimiento y control en sitio. Incluye los elementos lógicos y/o aplicaciones necesarios para brindar funcionalidad y operación a los elementos físicos (Oz, 2005).

Incidente de seguridad en Canales Electrónicos: Se conforma por el evento o serie de eventos de seguridad, operativos y tecnológicos interrelacionados que generen una exposición no deseada o esperada de las credenciales, transacciones, datos de los clientes y el servicio bancario asociado y que posean una probabilidad significativa de comprometer las operaciones y amenazar la seguridad informática (Oz, 2005).

Institución Financiera: Ente que facilita servicios financieros a sus clientes o miembros permanentes (Ruiz, 2008).

Plataforma Tecnológica: Agrupación de equipos, aplicaciones y sistemas destinados a ofrecer productos y servicios a través del uso de los recursos tecnológicos disponibles, a una comunidad de usuarios, públicos y privados, tanto a nivel local, regional como nacional (León, 2009).

Riesgo: Posibilidad de que se produzca un acontecimiento que conlleve a pérdidas materiales en el resultado de las operaciones y actividades que desarrollen las Instituciones bancarias (León, 2009).

Riesgo Tecnológico: Se define como la posible pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en los equipos, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios bancarios o financieros con los clientes (León, 2009).

Seguridad de la información: Es la encargada de proteger los activos de información de una organización contra pérdidas o el uso indebido de la misma, además de permitir el acceso a los activos de la información, dando apoyo a los objetivos de la institución u organización (Osorio, 2010).

Servicios Financiero: Incluye la prestación de operaciones bancarias, cambiarias y/o financieras, de instrucción legal por medio bancario o pago de bienes y servicios (Ruiz, 2008).

Sistema de Información: Mecanismo que involucra la dualidad hombre /máquina integrada en una sola unidad, que provee información para el apoyo de las funciones de operaciones, gerencia y toma de decisiones en una organización determinada (Osorio, 2010).

Software: Es un conjunto de programas, documentos, procedimientos y rutinas asociados con la operación de un sistema de cómputo (Arriola, 2008).

Vulnerabilidades: Disposición interna a ser afectado por una amenaza, diferentes aspectos de la realidad. Desde el punto de vista informático, se define como una debilidad de cualquier tipo que compromete la seguridad del sistema informático (Harris, 2009).

CAPÍTULO III: MARCO METODOLÓGICO

El marco metodológico de la investigación, se refiere a las vías a seguir desde que se inicia la investigación hasta la finalización de la misma. Al respecto, Balestrini (2006), define el marco metodológico como

> La instancia referida a los métodos, las diversas reglas, registros, técnicas y protocolos con los cuales una teoría y su método calculan las magnitudes de lo real. De allí que se deberán plantear el conjunto de operaciones técnicas que se incorporan en el despliegue de la investigación en el proceso de obtención de los datos. El fin esencial del marco metodológico es el de situar en el lenguaje de investigación los métodos e instrumentos que se emplearán en el trabajo planteado, desde la ubicación acerca del tipo de estudio y el diseño de investigación, su universo o población, su muestra, los instrumentos y técnicas de recolección de datos, la medición, hasta la codificación, análisis y presentación de los datos. De esta manera se proporcionará al lector una información detallada sobre cómo se realizará la investigación (p. 114).

3.1 Tipo y Nivel de Investigación

La propuesta de un modelo para la detección de vulnerabilidades, constituye una solución viable a la problemática o necesidades de seguridad de información, detectadas en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela, las cuales representan la realidad objeto de estudio de esta investigación, por lo tanto, el tipo de investigación quedó enmarcado en la modalidad de proyecto factible.

En relación a su definición, el Manual de normas para la elaboración, presentación y evaluación de los trabajos especiales de grado de la Universidad Santa María (USM) (2010), establece que “el proyecto factible consiste en elaborar una propuesta viable que atiende a necesidades de una institución, organización o grupo social, que se han evidenciado a través de

una investigación documental o de una investigación de campo" (p.44). Por otro lado, el nivel de la investigación, atendió al descriptivo; el cual es definido por Tamayo y Tamayo (2007), como aquel que:

> Comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o proceso de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre grupo de personas, grupo o cosas, se conduce o funciona en presente" La investigación de tipo descriptiva trabaja sobre realidades de hechos, y su característica fundamental es la de presentar una interpretación correcta (p. 35).

Al respecto, la investigación partirá de la realización de un diagnóstico que permitirá describir las condiciones actuales del proceso de detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela, para posteriormente, determinar los requerimientos a considerar para la formulación de la propuesta de un modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

3.2 Diseño de la Investigación

El diseño de investigación, constituye el plan, organización, coordinación, control y seguimiento de toda la estructura de la investigación, con el fin de dar respuestas coherentes, significativas y relevantes a las preguntas de investigación formuladas en el planteamiento del problema presentado. A juicio de Fernández (2008), "el diseño señala al investigador, lo que debe hacer para alcanzar sus objetivos de estudios, contestar las interrogantes que se han planteado y analizar la certeza de las hipótesis formuladas en un contexto en particular" (p. 106).

Ahora bien, en cuanto al diseño de investigación, se enmarcó dentro de un diseño de investigación mixto, el que según Zorrilla (1993) "es aquel que

participa de la naturaleza de la investigación documental y de la investigación de campo (p. 43). Por ello, el presente trabajo se desprendió en primera instancia, directamente de la realidad objeto de estudio, en este caso, de las instituciones bancarias venezolanas del sector privado, situación que permitió reafirmar el apoyo de un diseño de campo, definido por Arias (2006), como aquella que "consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna" (p.31).

En segunda instancia, se apoyó en la consulta de fuentes para sustentar teóricamente la investigación, característica fundamental del diseño bibliográfico, el cual es definido por la Universidad Santa María (2009) como "el diseño básico de las investigaciones documentales, ya que a través de la revisión del material documental de manera sistémica, rigurosa y profunda se llega al análisis de diferentes fenómenos a la determinación de la relación entre las variables" (p. 44).

3.3 Población y Muestra

Para Palella y Martins (2006), la población es un:

> "conjunto de unidades de las que se desea obtener información y sobre las que se van a generar conclusiones. La población puede ser definida como el conjunto finito o infinito de elementos, personas o cosas pertinentes a una investigación y que generalmente suele ser inaccesible" (p. 115).

En tal sentido, la población objeto de estudio, estará constituida por la totalidad de diecinueve (19) instituciones Bancarias pertenecientes al sector privado en Venezuela. Para la selección de la muestra y en virtud de que la población es finita; se tomará en consideración el muestreo intencional, el cual se basa según Linares (2010), "en la escogencia de los elementos muestrales de acuerdo a criterios o juicios preestablecidos por el investigador" (p.32). En este caso, la muestra se encuentra compuesta por

diez (10) instituciones bancarias del sector privado en Venezuela a las cuales el investigador tuvo acceso sin ningún inconveniente (criterio de accesibilidad).

3.4 Técnicas e Instrumentos de Recolección de Datos

La técnica, es la forma como será recabada la información en la realidad objeto de estudio. Entre estas técnicas, se pueden mencionar, la observación. En esta investigación, se considerará en primer lugar, la observación, que de acuerdo a Sánchez (2009), "es una técnica de investigación que consiste en observar personas, fenómenos, hechos, acontecimientos, casos, objetos, acciones, situaciones, entre otros, con el fin de obtener y determinar información de interés para una investigación" (p. 23).

Específicamente, se utilizará la observación estructurada, materializada en una Lista de Chequeo (*Checklist*), con la cual, se podrá recabar un conjunto de datos relacionados con las condiciones actuales del proceso de detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela (ver Check List N° 1 en el Anexo A). Adicionalmente, se aplicará otra *Checklist*, para recoger información sobre las posibles pruebas de validación fundamentadas en las Normativas de TI (ver Check List N° 2 en el Anexo B).

En segundo lugar, se aplicará la técnica de la encuesta, definida por Méndez (2004), como "la recolección de información que se realiza a través de formularios, los cuales tienen aplicación a aquellos problemas que se pueden investigar por métodos de observación, análisis de fuentes documentales y opiniones de los individuos con relación a su objeto de investigación" (p.37).

Cabe señalar, que esta técnica, facilita el proceso de consulta tipificada a personas elegidas de forma estática. Cabe destacar, que el cuestionario, de acuerdo a la postura de Linares (2010) constituye:

> Un medio de comunicación escrito y básico, entre el encuestador y el cuestionado, que facilita traducir los objetivos y las variables de la investigación a través de una serie de preguntas muy particulares, preparadas previamente de forma cuidadosa, susceptibles de analizarse con relación al problema estudiado (p. 26).

3.5 Fases de la Investigación

La elaboración del presente trabajo de investigación se basó en las siguientes fases o etapas:

3.6 Procedimientos por Objetivos

1. **Diagnosticar las condiciones actuales del proceso de detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela**. Se elaborará un cuestionario (ver Check List N° 1 en el Anexo A) y se aplicarán las preguntas del mismo, a fin de determinar la realización de análisis de vulnerabilidades e identificación de las mismas, por parte de la Banca venezolana; así como, políticas de seguridad, inventarios de activos y herramientas propias para el escaneo de vulnerabilidades.

   Seguidamente, se tabularán los resultados obtenidos y finalmente se analizarán los resultados, considerando lo siguiente:

Cuadro 3

Escalas de Resultados

Porcentaje de respuestas positivas	Calificación
De 0% a 40%	Deficiente
De 41% a 60%	Malo
De 61% a 80%	Aceptable
De 81 a 100%	Excelente

Fuente: Elaboración Propia

2. **Determinar los requerimientos a considerar para la formulación de una propuesta de modelo**. Se aplicará un cuestionario con treinta (30) requerimientos (ver Cuestionario tipo Likert en Anexo C) a fin de determinar cuáles son los más importantes para la Banca los cuales incluyen requerimientos de uso y de implementación. Se consideró una escala tipo Likert con opciones de respuesta Siempre (S), Casi Siempre (CS), Algunas Veces (AV), Nunca (N).

   En segundo término, se determinará cuales requerimientos son considerados como que deben estar presentes siempre o casi siempre en el cien por ciento (100%) de las respuestas.

   Del listado resultante, se seleccionarán aquellos requerimientos que los entrevistados hayan considerado que deben estar presentes en el ochenta por ciento o más (mayor a 80%), en un modelo de análisis de vulnerabilidades.

3. **Realizar un modelo de datos**. Inicialmente se esquematizará el proceso de detección de vulnerabilidades, a fin de determinar los elementos que deben estar presentes; así como sus relaciones.

Como siguiente paso, se ubicarán bases de datos de vulnerabilidades en las páginas web de los organismos internacionales de mayor relevancia en la materia.

Se seleccionarán los artículos de las normativas de TI, asociados con la banca por internet. Asimismo, se escogerán estándares o mejores prácticas internacionales que contengan controles u objetivos de control, a fin de relacionar los hallazgos del escáner con estas y determinar el estado actual de la plataforma a escanear con respecto a las mismas.

Finalmente, se realizará un diagrama de entidad relación donde se identifiquen las tablas que se utilizarán con sus atributos y claves.

4. **Formular una propuesta de modelo**. Inicialmente se ubicarán los requerimientos mínimos necesarios que debe contener el modelo, determinados en la fase 2.

   Se construirá un modelo que compare el resultado del scanner con vulnerabilidades conocidas a fin de determinar la existencia de hallazgos o debilidades de control, y a su vez, estos hallazgos deberán relacionarse con los artículos de las Normativas asociadas a la TI, con el propósito de determinar el riesgo de incumplimiento (Riesgo Legal) y el tecnológico derivado de este.

   Finalmente, se realizará un diagrama del modelo conceptual donde se identifiquen las fases que componen el modelo propuesto con sus respectivos requerimientos, conjuntamente con las herramientas tecnológicas que las soportan.

5. **Validar el Modelo a través del juicio experto**. Primeramente se seleccionará una muestra de personal con experiencia en seguridad de la información de las Gerencias de Riesgo Tecnológico, Tecnología de la Información y Seguridad de la Información de la Superintendencia de las Instituciones del sector Bancario de Venezuela. Para ello se tomarán los siguientes principios: Cargos superiores al Nivel III, Experiencia en seguridad de la información y riesgo de TI, experiencia mayor a ocho (8) años en el área. El número de los integrantes deberá ser impar y en ningún caso superará los siete (7) integrantes.

   Una vez seleccionados los integrantes, se les mostrará el resultado de la investigación en reuniones tipo "focus group" a fin de generar un debate sobre el modelo propuesto. Finalmente, se buscará que el grupo de experto realice sus comentarios u observaciones; así como, la validación del modelo propuesto, utilizando el método Delphi,

3.7 Variables, Definición Conceptual y Operacional e Indicadores

La variable es definida por Hernández, Fernández y Baptista (2010), como "una propiedad que puede variar y cuya variación es susceptible de medirse u observarse" (p. 143). Esta, desempeña un papel importante por cuanto permiten representar la dimensión del trabajo de investigación y pueden ser definidas de manera conceptual, nominal y operacionalmente.

Por su parte, Arias (2006), señala que una variable "es una cualidad susceptible de sufrir cambios; por lo que un sistema de variable está conformado por un conjunto de características operacionalizadas" (p. 57). De acuerdo a esa definición, el autor de esta investigación asume una postura que le permite señalar que una variable es una característica que puede ser

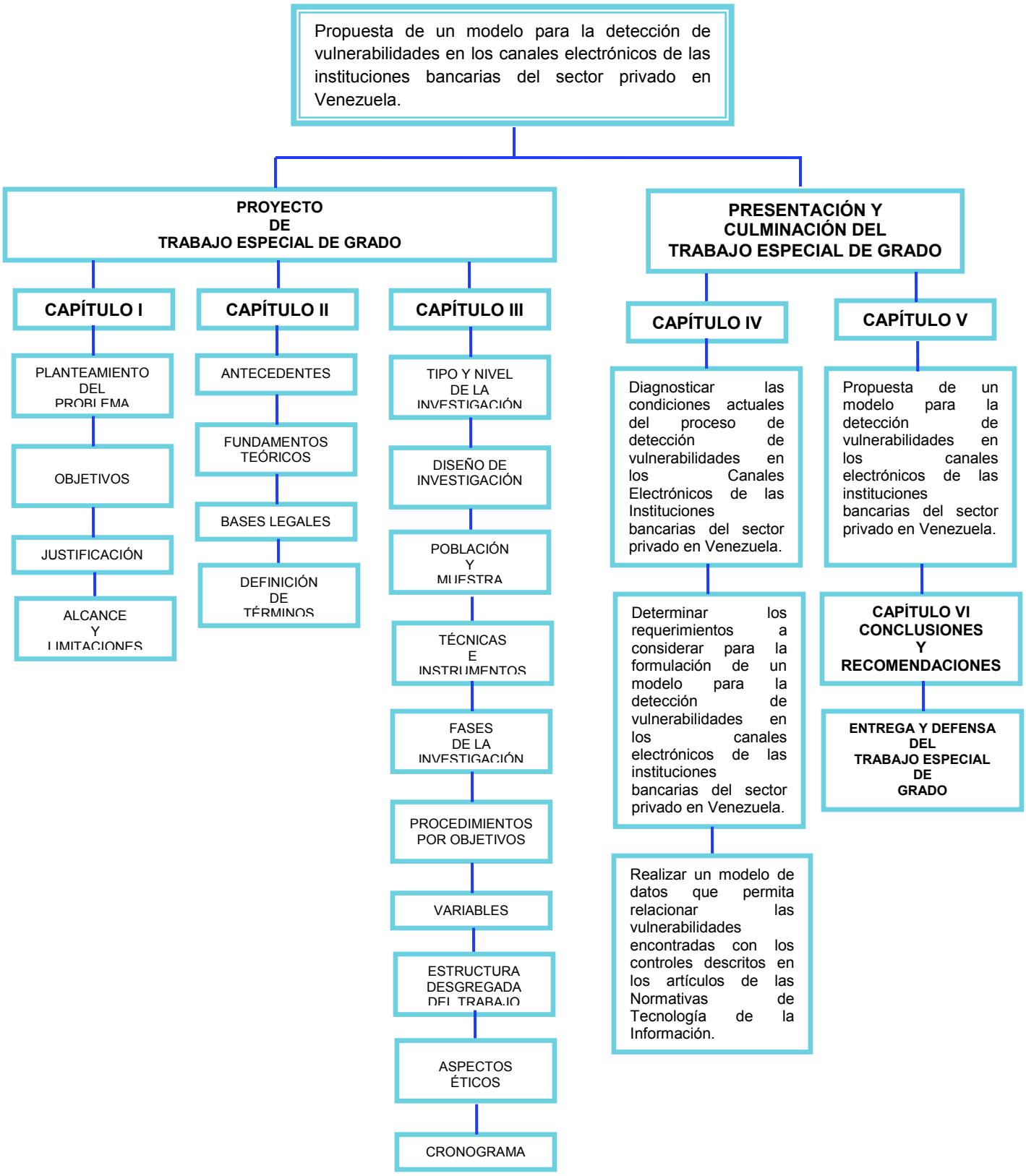
observable y medible, que consta de dos dimensiones; conceptual y nominal, y es susceptible a sufrir cambios al ser intervenida.

Cuadro 4
Cuadro de Operacionalización de las Variables

Objetivos Específicos	Variable	Dimensión	Indicadores	Técnica e Instrumento	Ítems
Diagnosticar las condiciones actuales del proceso de detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.	**(VI)** Condiciones actuales del proceso de detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.	Diagnóstico	Inventario de activos de información hardware y software. Identificación de vulnerabilidades y amenazas de los activos de información. Aplicación del escáner para determinar vulnerabilidades. Priorización de vulnerabilidades. Análisis de riesgo de las vulnerabilidades. Presentación del informe de análisis de riesgo con las recomendaciones.	Técnica: Observación estructurada Instrumento: Listas de Chequeo (CHECK LIST)	1 2 3 4 5 6
Determinar los requerimientos a considerar para la formulación de un modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.		Requerimientos	Pendrive con el software de escaneo que se conecte a la Red. Base de datos de vulnerabilidades. Normativa de tecnología de la información. Normativa 641.10 de Banca Electrónica.	Técnica: Encuesta Instrumento: Cuestionario tipo Likert	1 2 3 4 5 6 7 8 9
Realizar un modelo de datos que permita relacionar las vulnerabilidades encontradas con los controles descritos en los artículos de la Normativa de TI.		Controles de la Normativa de TI	Identificación de las Vulnerabilidades Características de las vulnerabilidades Características de los Controles Relación Controles-Vulnerabilidad Modelo de relación resultante del análisis de la relación entre las vulnerabilidades y los controles.		10 11 12 13 14 15 16
Formular un modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.	**(VD)** Modelo para la detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.	Formulación de la propuesta de Modelo	Identificación de requerimientos Definición del alcance del Modelo Establecimiento de Políticas de seguridad Definición de la metodología para clasificación y priorización de los riesgos y vulnerabilidades Gestión de activos Seguridad del Recurso humano Seguridad física y ambiental Controles de acceso Gestión de incidentes Validación		17 18 19 20 21 22 23 24 25 26 27 28 29 30
Validar el Modelo a través del juicio experto de personal calificado en la Superintendencia de las Instituciones del sector Bancario en Venezuela.		Validación de la propuesta de Modelo		Técnica: Focus Group Método Delphi Minuta	

Fuente: Elaboración propia.

3.8 Estructura Desagregada de Trabajo



3.9 Aspectos Éticos

El desarrollo de esta investigación se realizará respetando las consideraciones éticas establecidas por la Universidad Católica “Andrés Bello” (UCAB). Por ello, se asegura el respeto de las normas relacionadas con el manejo y uso de la información, evitando en todo momento el plagio. Adicionalmente, se garantiza la absoluta confidencialidad en la información suministrada por parte de las instituciones bancarias del sector privado en Venezuela, involucradas en la investigación; teniendo presente que la misma exclusivamente, persigue fines académicos.

CAPÍTULO IV: RESULTADOS

A continuación se presentan los resultados obtenidos en la presente investigación, así como, los análisis correspondientes. Tal y como se establece en el objetivo del presente Trabajo de Grado, el resultado es la propuesta de un modelo para la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.

4.1 Diagnostico de las condiciones actuales del proceso de detección de vulnerabilidades.

4.1.1 Políticas de Seguridad de la Información.

En lo que respecta a las políticas de seguridad de la información, se pudo determinar, con base en los resultados obtenidos producto de la aplicación del Check List N° 1 (ver Anexo A) que existe una gestión deficiente de las Políticas de Seguridad de la Información. Afirmación que se sustenta en que lo siguiente:

- Los objetivos de las Políticas de Seguridad de la Información no están identificados ni cumplen con los requerimientos organizacionales en un setenta por ciento (70%) de las Instituciones evaluadas (ver anexo E, tabla 2);
- Las políticas no son revisadas a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad y actualización, en un ochenta por ciento (80%) de la Instituciones objeto de estudio:
- Sólo en el cuarenta por ciento (40%) de las Instituciones Bancarias objeto de estudio, las Políticas de Seguridad de la Información se encuentran documentadas;

- No existen directrices claras para el uso y manejo de los activos de información en el sesenta por ciento (60%) de las Instituciones objeto de estudio.

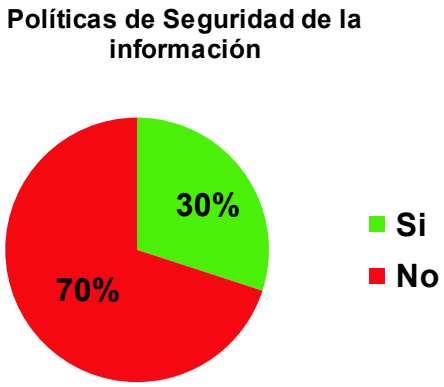


Gráfico N° 5. Resultado Check List N° 1.

Fuente: Elaboración Propia.

4.1.2 Inventario de Activos de Información (Hardware y Software)

En lo que respecta al inventario de activos de información, (ver Anexo E, tabla 2), se pudo determinar que no existe un listado de todos los activos de información indicando: marca, modelo, sistema operativo, tipo de teclado y su versión, ubicación física, cifrado, tipo de conexión y proveedor del equipo en el setenta por ciento (60%) de las Instituciones Bancarias objeto de estudio.

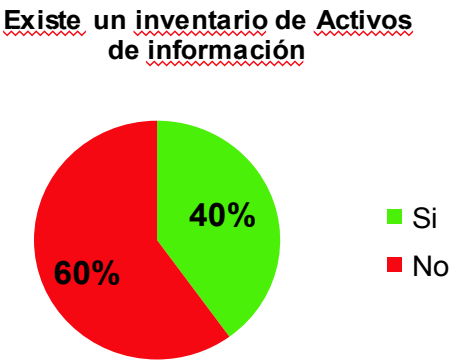


Gráfico N° 6. Resultado Check List N° 1.

Fuente: Elaboración Propia.

De igual forma, solo el cincuenta por ciento (50%) de las Instituciones Bancarias visitadas, cuenta con un inventario de equipos críticos de la red objetivo a los cuales se les aplicará el escaneo de vulnerabilidades.

Por otro lado, solo el cuarenta por ciento (40%) de las Instituciones Bancarias, cumple con el hecho de que dentro de su inventario, evalúan todos los servicios y puertos activos de cada uno de los equipos encontrados como críticos para la red objetivo, adicionalmente, el setenta por ciento (70%) no tiene un listado ordenado de equipos críticos de acuerdo a su nivel riesgo en alto, (ver Anexo E, tabla 8).

Resultados que denotan debilidades en cuanto al deber ser, ya que Espiñeira, Sheldon y Asociados (2005), señalan que la Seguridad de la información, es “la encargada de proteger los activos de información de una organización contra pérdidas o el uso indebido de la misma, además de permitir el acceso a los activos de la información, dando apoyo a los objetivos de la organización” (p. 32). Por consiguiente, complementa el investigador, que la misma desempeña un rol estratégico fundamental en

todos los procesos inherentes a las Instituciones Bancarias, ya que identifica los recursos que deben resguardarse o restringirse dentro de una empresa, lo cual promueve la mejora de las operaciones con clientes, socios, proveedores y trabajadores de la misma.

4.1.3 Identificación de vulnerabilidades y amenazas en los canales electrónicos.

En cuanto a la identificación de vulnerabilidades y amenazas en los canales electrónicos, los resultados reflejados en el instrumento, (Ver anexo E, tablas 3, 4, 5 y 6), se pudo determinar que en el sesenta por ciento (60%) de las instituciones objeto de estudio, no se establecen mecanismos continuos que permitan analizar los sitios web de la Banca por Internet, a fin de detectar en línea vulnerabilidades y otros tipos de amenazas.

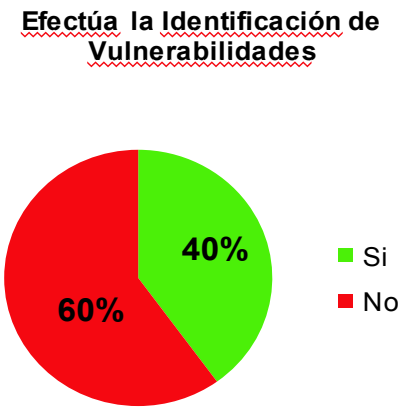


Gráfico N° 7. Resultado Check List N° 1.

Fuente: Elaboración Propia.

Otra debilidad evidenciada, es que solo un veinte por ciento (20%) de las Instituciones Bancarias objeto de estudio, cuenta con un cronograma de

actividades para la revisión, detección y análisis de vulnerabilidades en los canales electrónicos de la institución (ver anexo E, tabla 8).

En relación a la clasificación de riesgo de los activos de información, sólo el treinta por ciento (30%) de las instituciones tiene un listado ordenado de equipos críticos de acuerdo a su nivel riesgo (alto, medio o bajo), (ver anexo E tabla 8), llegando a la conclusión que es necesario establecer las acciones correctivas para regularizar esta situación, a fin de prevenir futuros riesgos asociados al aprovechamiento de vulnerabilidades no identificadas en algunos de los equipos críticos de forma oportuna.

De igual manera, se pudo determinar que en lo concerniente a las políticas, normas y procedimientos asociadas al uso de los factores de autenticación (persona natural y jurídica), un ochenta por ciento (80%) no otorga relevancia a las campañas educacionales para resguardar la seguridad de la información relacionada con la Banca por Internet.

4.1.4 Aplicación del escáner para determinar vulnerabilidades

En cuanto a la aplicación del escáner para determinar vulnerabilidades, los resultados reflejados en el instrumento, (ver Anexo E, tabla 7), se pudo determinar que el setenta por ciento (70%) de las Instituciones Bancarias, no cuenta actualmente con herramientas tecnológicas para la detección de vulnerabilidades en los canales electrónicos de la Institución, tampoco realizan un plan o ejecución con las actividades a realizar para mitigar el riesgo asociado a las vulnerabilidades detectadas en los canales electrónicos de la Institución y no poseen un instrumento que permite medir la eficiencia y eficacia con la que se realiza el proceso de detección de vulnerabilidades (Revisión, detección, análisis, control y seguimiento).

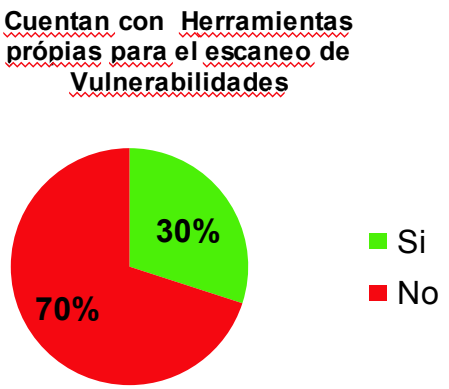


Gráfico N° 8. Resultado Check List N° 1.

Fuente: Elaboración Propia.

4.1.5 Análisis de riesgo de las vulnerabilidades.

En cuanto al análisis de riesgo de las vulnerabilidades (ver Anexo E, tabla 8), es relevante evidenciar que en sólo en un veinte por ciento (20%) de las Instituciones Bancarias se lleva a cabo un proceso de control y seguimiento a los casos de vulnerabilidades atendidas y existe un área encargada de centralizar y evaluar todos los informes generados lo cual implica que en el ochenta por ciento (80%) de las Instituciones objeto de estudio no se efectúa un análisis de riesgo de vulnerabilidades, adicionalmente se pudo observar que el setenta por ciento (70%) de las Instituciones Bancarias consultadas, no cuenta con una gestión de seguridad de la información basada en una metodología de análisis de riesgo de la organización que produzca resultados comparables y reproducibles y mantiene un histórico de las vulnerabilidades detectadas en el tiempo.

Gráfico N° 9. Resultado Check List N° 1.

Fuente: Elaboración Propia.

Esta situación empeora cuando solo un veinte por ciento (20%) de dichas Instituciones realiza control y seguimiento a los casos de vulnerabilidades resueltos y el cuarenta por ciento (40%) de las mismas no cuenta con una base de datos de vulnerabilidades detectadas que sirva como apoyo para la debida gestión de las incidencias asociadas a la seguridad lógica.

En lo que respecta a la priorización de vulnerabilidades, la tabla 8 (ver Anexo E, tabla 8) refleja que en un sesenta por ciento (60%) de las Instituciones objeto de estudio no se atienden los casos de vulnerabilidades de acuerdo al nivel de riesgo que estos representen, además que no se prioriza en base a la criticidad asociada a cada vulnerabilidad identificada ni del activo que se ve afectado.

Ocasionando dificultades al momento de implementar los planes de remediación, situación que dificulta el establecimiento de las medidas correctivas y el tratamiento de las vulnerabilidades sobre los activos de

acuerdo al riesgo que estas representan en cuanto al impacto que pudieran ocasionar si se llegase a materializar una amenaza.

Con base a lo antes expuesto, se puede concluir que el proceso de análisis de riesgo de vulnerabilidades carece de mecanismos eficientes que permitan una adecuada gestión del riesgo.

4.1.6 Presentación del informe de análisis de riesgo con las recomendaciones.

Finalmente en relación con la presentación del informe de análisis de riesgo con las recomendaciones respectivas, se pudo evidenciar de acuerdo a los resultados arrojados por la tabla 9 del anexo E, que solo en el cuarenta por ciento (40%) de las Instituciones Bancarias consultadas, existen roles y responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información y el informe presentado se encuentra formalizado por la máxima autoridad de TI y el área de seguridad de la información, lo que no es cumplido por el 60% de las mismas.

Por otra parte, el treinta por ciento (30%) cumple con la realización periódica de un informe de análisis de riesgo, mientras que el setenta por ciento (70%) no lo cumple, este escenario origina que se obstaculice el proceso de revisión del informe. Aunado a eso, se determinó que solo un sesenta por ciento (60%) de dichas Instituciones, realiza recomendaciones para mitigar los riesgos detectados y solo dos (2) de las diez (10) Instituciones, cuentan con un área encargada de centralizar y evaluar todos los informes generados, trayendo como consecuencia una mala praxis en la gestión documental.

Todo lo anterior, evidencia que las condiciones actuales de la detección de vulnerabilidades en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela son deficientes.

4.2 Determinación de los requerimientos a considerar en la propuesta del modelo.

Para establecer los requerimientos mínimos necesarios que debe contemplar la propuesta de modelo objeto del presente trabajo de investigación, se aplicó a las diez (10) instituciones bancarias del sector privado que componen la muestra, el cuestionario tipo Likert (ver Anexo C), obteniendo el siguiente resultado.

Cuadro 5

Resultados cuestionario tipo Likert

Nº	ÍTEM	(S)	(CS)	(AV)	(N)
Requerimientos a considerar para la propuesta de un Modelo para la detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					
1	**¿Considera Ud. que es necesario contar regularmente con un software de escaneo que se conecte a la Red?**	**88%**	**12%**	**0**	**0**
2	¿Para formular una propuesta de un modelo para la detección de vulnerabilidades en los canales electrónicos de las Instituciones bancarias, se requiere acceder a la base de datos de vulnerabilidades?	88%	12%	0	0
3	¿La formulación de una propuesta de un Modelo para la detección de vulnerabilidades en los Canales Electrónicos debe estar fundamentada en lo establecido en la Normativa 641.10 de Banca Electrónica?	100%	0	0	0
I. Controles de Seguridad de Información que se ajusten a los requerimientos de los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					
II.1. Control de acceso a Redes:					
4	¿Se debe evaluar el acceso de los usuarios para	88%	12	0	0

	constatar que se permita sólo a los servicios para los cuales hayan sido específicamente autorizados?				
5	¿Se deben considerar las redes y servicios de la red a los cuales se tienen acceso?	100%	0	0	0
6	¿Se requieren establecer lineamientos para los procedimientos de autorización para determinar quién está autorizado a tener acceso a cuáles redes y servicios de redes?	0	88	12	0
7	¿Es necesario establecer controles y procedimientos gerenciales para proteger el acceso a las conexiones de red y los servicios de red?	0	75%	25%	0
8	¿Se deben establecer condiciones para permitir el acceso a un proveedor del servicio de Internet o sistema remoto?	88%	12%	0	0
9	¿Se requiere de métodos de autenticación apropiados para controlar el acceso de usuarios remotos?	100%	0	0	0
II.2. Controles Criptográficos:					
10	¿Se deben especificar mecanismos de conexión basados en la encriptación para los usuarios Remotos Vg.. VPN?	88%	12%	0	0
11	¿Es necesario el uso de mecanismos de encriptación para Conexiones Inalámbricas, preferiblemente a través del uso de PKI?	88%	0	12%	0
II.3. Control de acceso a los Sistemas Operativos:					
12	¿El acceso a los sistemas operativos debería ser controlado mediante u procedimiento de registro seguro?	75%	25%	0	0
13	¿Se deben revisar los perfiles de usuarios con la finalidad de constatar que los usuarios tienen un identificador único (ID de usuario) para su uso personal?	88%	12%	0	0
14	¿Es necesario definir una técnica de autenticación adecuada para sustanciar la identidad del usuario?	63%	12%	25%	0
15	¿Los mecanismos para el manejo de claves secretas deben ser seguros?	88%	12%	0	0
16	¿Deben seleccionarse mecanismos adecuados para la restricción y control del uso de programas de utilidad que puedan ser capaces de superar los controles del sistema?	75%	25%	0	0
II.4. Control de acceso a la Aplicación de la Información:					

17	¿El acceso de los usuarios y del personal de soporte a la información y las funciones del sistema de la aplicación debe limitarse en concordancia con la política de control de acceso definida?	63%	37%	0	0
18	¿Se debe verificar la existencia y aprobación de una Documentación de Perfiles, Grupos y Opciones de las distintas aplicaciones críticas?	63%	37%	0	0
19	¿Se requieren proporcionar menús para controlar el acceso a las funciones del sistema de aplicación?	75%	25%	0	0
20	¿Es necesario realizar una revisión de los módulos para reportes con la finalidad de evaluar que no se muestre información sensible en los casos que no se amerite?	63%	37%	0	0
21	¿Los sistemas confidenciales deberían contar con un ambiente de cómputo dedicado (aislado)?	75%	25%	0	0

Fuente: Elaboración propia.

Se realizó la evaluación de los porcentajes de aceptación de cada uno de los Ítems del cuestionario y se aplicó un primer filtro donde se seleccionaron los requerimientos de mayor relevancia que, de acuerdo a las respuestas obtenidas, siempre deberían estar presentes en una propuesta de modelo de detección de vulnerabilidades. Este filtro consistió en seleccionar los requerimientos que de acuerdo al criterio experto de los entrevistados, deberían estar presentes siempre o casi siempre en el cien por ciento (100%) de las veces.

La opción de respuesta "Siempre" sumada con la opción "Casi Siempre" fuera igual al cien por ciento (S + CS = 100%)

Con este primer filtro, se obtuvieron diez y siete (17) requerimientos

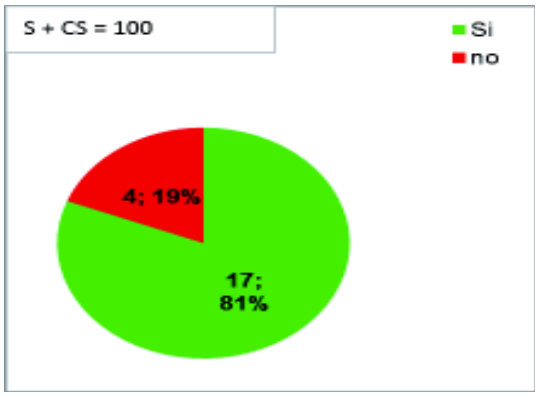


Gráfico N° 10. Resultado del Primer Filtro.

Fuente: Elaboración Propia.

Cuadro 6
Resultados de la aplicación del primer filtro.

Nº	ÍTEM	(S)	(CS)	(AV)	(N)
II. Requerimientos a considerar para la propuesta de un Modelo para la detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					
1	¿Considera Ud. que es necesario contar regularmente con un software de escaneo que se conecte a la Red?	88%	12%	0	0
2	¿Para formular una propuesta de un modelo para la detección de vulnerabilidades en los canales electrónicos de las Instituciones bancarias, se requiere acceder a la base de datos de vulnerabilidades?	88%	12%	0	0
3	¿La formulación de una propuesta de un Modelo para la detección de vulnerabilidades en los Canales Electrónicos debe estar fundamentada en lo establecido en la Normativa 641.10 de Banca Electrónica?	100%	0	0	0
III. Controles de Seguridad de Información que se ajusten a los requerimientos de los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					
II.1. Control de acceso a Redes:					
4	¿Se debe evaluar el acceso de los usuarios para constatar que se permita sólo a los servicios para los cuales hayan sido específicamente autorizados?	88%	12%	0	0
5	¿Se deben considerar las redes y servicios de la red a los cuales se tienen acceso?	100%	0	0	0

8	¿Se deben establecer condiciones para permitir el acceso a un proveedor del servicio de Internet o sistema remoto?	88%	12%	0	0
9	¿Se requiere de métodos de autenticación apropiados para controlar el acceso de usuarios remotos?	100%	0	0	0
II.2. Controles Criptográficos:					
10	¿Se deben especificar mecanismos de conexión basados en la encriptación para los usuarios Remotos Vg.. VPN?	88%	12%	0	0
II.3. Control de acceso a los Sistemas Operativos:					
12	¿El acceso a los sistemas operativos debería ser controlado mediante u procedimiento de registro seguro?	75%	25%	0	0
13	¿Se deben revisar los perfiles de usuarios con la finalidad de constatar que los usuarios tienen un identificador único (ID de usuario) para su uso personal?	88%	12%	0	0
15	¿Los mecanismos para el manejo de claves secretas deben ser seguros?	88%	12 %	0	0
16	¿Deben seleccionarse mecanismos adecuados para la restricción y control del uso de programas de utilidad que puedan ser capaces de superar los controles del sistema?	75%	25%	0	0
II.4. Control de acceso a la Aplicación de la Información:					
17	¿El acceso de los usuarios y del personal de soporte a la información y las funciones del sistema de la aplicación debe limitarse en concordancia con la política de control de acceso definida?	63%	37%	0	0
18	¿Se debe verificar la existencia y aprobación de una Documentación de Perfiles, Grupos y Opciones de las distintas aplicaciones críticas?	63%	37%	0	0
19	¿Se requieren proporcionar menús para controlar el acceso a las funciones del sistema de aplicación?	75%	25%	0	0
20	¿Es necesario realizar una revisión de los módulos para reportes con la finalidad de evaluar que no se muestre información sensible en los casos que no se amerite?	63%	37%	0	0
21	¿Los sistemas confidenciales deberían contar con un ambiente de cómputo dedicado (aislado)?	75%	25%	0	0

Fuente: Elaboración propia.

Seguidamente, se aplicó un segundo filtro, con el propósito de obtener un listado de requerimientos mínimos, necesarios y de verdadera relevancia para un modelo de análisis de vulnerabilidades. Con este segundo filtro, se seleccionaron del listado resultante (del primer filtro), aquellos requerimientos que los entrevistados consideraron que deben estar presentes “Siempre” en el ochenta por ciento o más (mayor a 80%), en un modelo de análisis de vulnerabilidades. Como resultado se obtuvo diez (10) requerimientos, que fueron tomados como los requerimientos mínimos necesarios a considerar en la propuesta del modelo, tal como se puede observar en los siguientes gráficos.

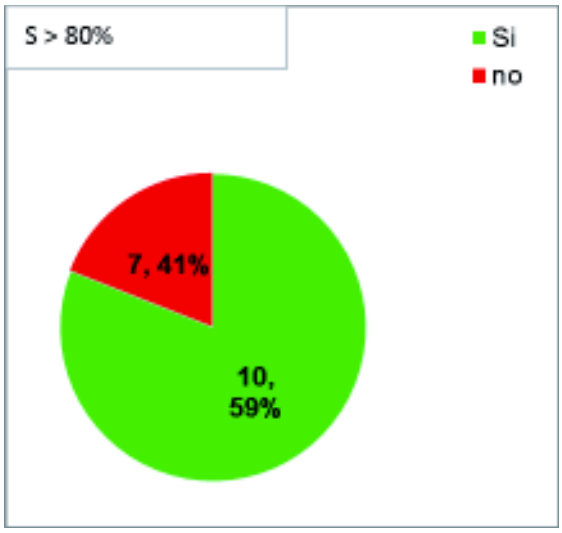


Gráfico N° 11. Resultado del segundo Filtro.

Fuente: Elaboración Propia.

Cuadro 7
Resultados de la aplicación del segundo filtro.

Nº	ÍTEM	(S)	(CS)	(AV)	(N)
IV. Requerimientos a considerar para la propuesta de un Modelo para la detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					

1	¿Considera Ud. que es necesario contar regularmente con un software de escaneo que se conecte a la Red?	88%	12%	0	0
2	¿Para formular una propuesta de un modelo para la detección de vulnerabilidades en los canales electrónicos de las Instituciones bancarias, se requiere acceder a la base de datos de vulnerabilidades?	88%	12%	0	0
3	¿La formulación de una propuesta de un Modelo para la detección de vulnerabilidades en los Canales Electrónicos debe estar fundamentada en lo establecido en la Normativa 641.10 de Banca Electrónica?	100%	0	0	0
V. Controles de Seguridad de Información que se ajusten a los requerimientos de los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					
II.1. Control de acceso a Redes:					
4	¿Se debe evaluar el acceso de los usuarios para constatar que se permita sólo a los servicios para los cuales hayan sido específicamente autorizados?	88%	12%	0	0
5	¿Se deben considerar las redes y servicios de la red a los cuales se tienen acceso?	100%	0	0	0
8	¿Se deben establecer condiciones para permitir el acceso a un proveedor del servicio de Internet o sistema remoto?	88%	12%	0	0
9	¿Se requiere de métodos de autenticación apropiados para controlar el acceso de usuarios remotos?	100%	0	0	0
II.2. Controles Criptográficos:					
10	¿Se deben especificar mecanismos de conexión basados en la encriptación para los usuarios Remotos Vg.. VPN?	88%	12%	0	0
II.3. Control de acceso a los Sistemas Operativos:					
13	¿Se deben revisar los perfiles de usuarios con la finalidad de constatar que los usuarios tienen un identificador único (ID de usuario) para su uso personal?	88%	12%	0	0
15	¿Los mecanismos para el manejo de claves secretas deben ser seguros?	88%	12 %	0	0

Fuente: Elaboración propia.

Finalmente, los diez (10) requerimientos obtenidos, se clasificaron en “requerimientos de uso” (aquellos que están relacionados con la parte conceptual del modelo y que sin ellos no se puede implementar el modelo) y

“requerimientos de implementación” (aquellos que están relacionados con la implementación del modelo), tal como se puede observar en la siguiente tabla.

Cuadro 8
Requerimientos mínimos necesarios.

Requerimientos de uso	
1	Pendrive que contenga el software de escaneo que se conecte a la red.
2	Se requiere acceder a la base de datos de vulnerabilidades.
3	Debe estar fundamentado en la Normativa de tecnología de la información vigente.
4	Evaluar el acceso de los usuarios para constatar que se permita sólo a los servicios para los cuales hayan sido específicamente autorizados.
5	Considerar las redes y servicios de la red a las cuales se tienen acceso.
Requerimientos de implementación	
6	Establecer condiciones para permitir el acceso a un proveedor del servicio.
7	Contar con métodos de autenticación apropiados para controlar el acceso de usuarios remotos.
8	Especificar mecanismos de conexión basados en la encriptación para los usuarios Remotos.
9	Revisar los perfiles de usuarios con la finalidad de constatar que los usuarios tienen un identificador único (ID de usuario) para su uso personal.
10	Contar con mecanismos seguros para el manejo de claves secretas.

Fuente: Elaboración propia.

4.3 El modelo de Datos.

4.3.1 Determinación de los elementos que componen el modelo y sus relaciones.

Se realizó análisis de los resultados arrojados por los Checklist 1 y Checklist 2, observándose las Instituciones Bancarias no relacionan las vulnerabilidades detectadas con el marco legal vigente, específicamente con

los artículos que establecen controles obligatorios, contenidos en ellos, ni cuentan con un modelo para materializar relación alguna; tal como puede evidenciarse en los cuadros 9 y 10.

Cuadro 9
Resultados CheckList 2

Alternativas	Se cumple	FR	No se cumple	FR
5.1 Existe un modelo de relación resultante del análisis de la relación entre las vulnerabilidades y los controles que abarque todos los artículos de la Normativa de Banca Electrónica y Normativa de TI y Servicios Financieros.	2	20%	8	80%

Fuente: Elaboración Propia

Cuadro 10
Extracto de Resultados CheckList 2

Alternativas	Se cumple	FR	No se cumple	FR
1.3 La información producto del escaneo puede ser usada para identificar algún incumplimiento de los artículos estipulados en la Resolución de Banca Electrónica y Normativa de TI y Servicios Financieros.	3	30%	7	70%
2.1 Las características de las vulnerabilidades a ser evaluadas se corresponden con las estipuladas en los artículos de la Normativa de Banca Electrónica y Normativa de TI y Servicios Financieros.	4	40%	6	60%

Fuente: Elaboración propia

Continuando con el análisis de la información recabada a través de los Checklist 1 y 2, se pudo observar que solo un veinte por ciento (20%) de dichas instituciones cuenta con una base de datos actualizada de vulnerabilidades conocidas donde se especifiquen las características de las mismas y la manera de solucionarlas, mientras que el ochenta por ciento

(80%) no cumple con este planteamiento, como se puede observar en el Cuadro 11.

Cuadro 11
Extracto de Resultado CheckList 1 y CheckList 2

Alternativas	Se cumple	FR	No se cumple	FR
2.3 Se cuenta con una base de datos actualizada de vulnerabilidades conocidas donde se especifiquen las características de las mismas y la manera de solucionarlas.	2	20%	8	80%
4.4. Se cuenta con una base de datos de vulnerabilidades detectadas que sirva como apoyo para la debida gestión de las incidencias asociadas a la seguridad lógica.	4	40%	6	60%

Fuente: Elaboración Propia

Igualmente se pudo determinar con base a los resultados obtenidos producto de la aplicación del Checklist 1 (ver anexo A) que actualmente en un sesenta por ciento (60%) de la Instituciones objeto de estudio, no cuentan con una base de datos de vulnerabilidades detectadas que sirva como apoyo para la debida gestión de las incidencias asociadas a la seguridad lógica, razón que justifica la implementación de una base de datos que contenga los hallazgos encontrados durante las revisiones.

Con las carencias antes señaladas y en el entendido que un modelo de análisis de vulnerabilidades debe contener al menos un (1) elemento de lectura y captación de datos se realizó un bosquejo del modelo considerando el siguiente flujo de información:

1) Escaneo de la plataforma tecnológica.

2) Comparación de los hallazgos detectados producto del escaneo con la base de datos de vulnerabilidades.

3) Comparación de los hallazgos con las Tablas normativas a fin de determinar el riesgo de incumplimiento o riesgo legal; así como, el riesgo tecnológico que pudiese derivarse de este.

4) Comparación de los artículos incumplidos con las mejores prácticas seleccionadas a fin de determinar las brechas existentes.

El bosquejo puede visualizarse en la Figura 3, que se muestra a continuación:

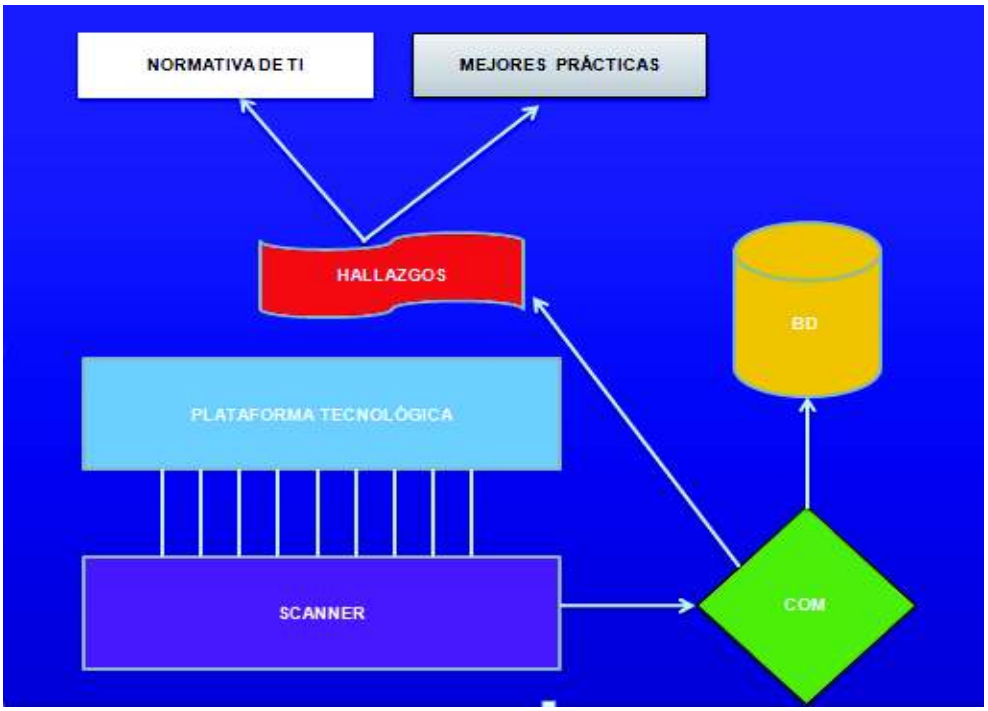


Figura 3. Proceso de Detección de Vulnerabilidades Fuente: Elaboración Propia.

4.3.2 Bases de Datos de Vulnerabilidades

Como se observa en la Figura 3, el modelo requiere de una base de datos de vulnerabilidades contra quien realizar las comparaciones de las lecturas tomadas por el scanner, a fin de determinar si la situación detectada puede ser considerada un hallazgo; es decir, si representa una vulnerabilidad para la plataforma tecnológica en análisis.

Para solventar esta situación se ubicaron diferentes bases de datos de vulnerabilidades en las páginas web de los organismos internacionales de mayor relevancia en la materia, las cuales se pueden observar en el siguiente cuadro.

Cuadro 12
Bases de datos de Vulnerabilidades

Base de Datos	Enlace de obtención
National Vulnerability Database	https://nvd.nist.gov/
CVE List	http://cve.mitre.org/
SecurityFocus	http://www.securityfocus.com/bid
Open Source Vulnerability Database	http://osvdb.org/
Secunia	http://secunia.com/community/
VUPEN Security	http://www.vupen.com/english/
Computer Security Vulnerabilities	http://securityvulns.com/

Fuente: Elaboración Propia

4.3.3 Normativas de TI y mejores prácticas.

Se seleccionaron las Normativas de TI y la Resolución 641.10 de Banca Electrónica, dado que son las principales normas que en materia tecnológica y específicamente en materia de banca por internet rige a la Banca venezolana.

De esas normativas, se seleccionaron los artículos que tuvieran relación con la operatividad de la banca por internet, consolidándose en una sola tabla de controles normativos (ver tabla de Normativa de TI en el anexo G), la

cual contiene todos los artículos asociados a la seguridad de los activos informáticos, seguridad del servicio de banca virtual y las Normas que regulan el uso de los Servicios de la Banca Electrónica.

Seguidamente, se escogieron los estándares o mejores prácticas internacionales que contienen controles u objetivos de control, a fin de relacionar los hallazgos del escáner con estas y determinar el estado actual de la plataforma a escanear con respecto a las mismas.

Dado que los controles del marco legal, pueden corresponderse con las mejores prácticas comúnmente aceptadas, se elaboró una tabla que contiene la consolidación de las mejores prácticas (ver Anexo F), usando como fuente de información el Mapeo de La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library (ITIL v3), ISO/IEC 27002 (anteriormente denominada ISO 17799) el cual es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional; y los Objetivos de Control para Información y Tecnologías Relacionadas (COBIT 4.1, en inglés: Control Objectives for Information and related Technology).

Cabe destacar, que la selección de los estándares COBIT 4.1, ITIL v3 e ISO 27002, dado que el primero de ellos se relaciona con el gobierno de TI y su alineación con las estrategias del negocio, amén de considerar un conjunto de dominios que contienen objetivos de control que sirven de guía para una correcta implementación de la plataforma tecnológica. La segunda, debido a que ve a la TI como un servicio que soporta las distintas actividades del negocio y que ordena los servicios tecnológicos en torno a unas prácticas tendientes a preservar el valor de la TI y por ende, del negocio. Finalmente, la tercera se seleccionó porque es el estándar de mayor reconocimiento en

materia de seguridad de la información y contiene una serie de objetivos de control y controles tendientes a coadyuvar en el establecimiento y mantenimiento de plataformas tecnológicas seguras.

4.3.4 Diagrama de entidad relación (DER).

Finalmente, se realizo un diagrama de entidad relación donde se identificaron las tablas que se utilizaron con sus atributos y claves, cabe destacar que el diagrama de entidad relación es una herramienta para el modelado de datos que permite representar las entidades relevantes de un sistema de información así como sus interrelaciones y propiedades.

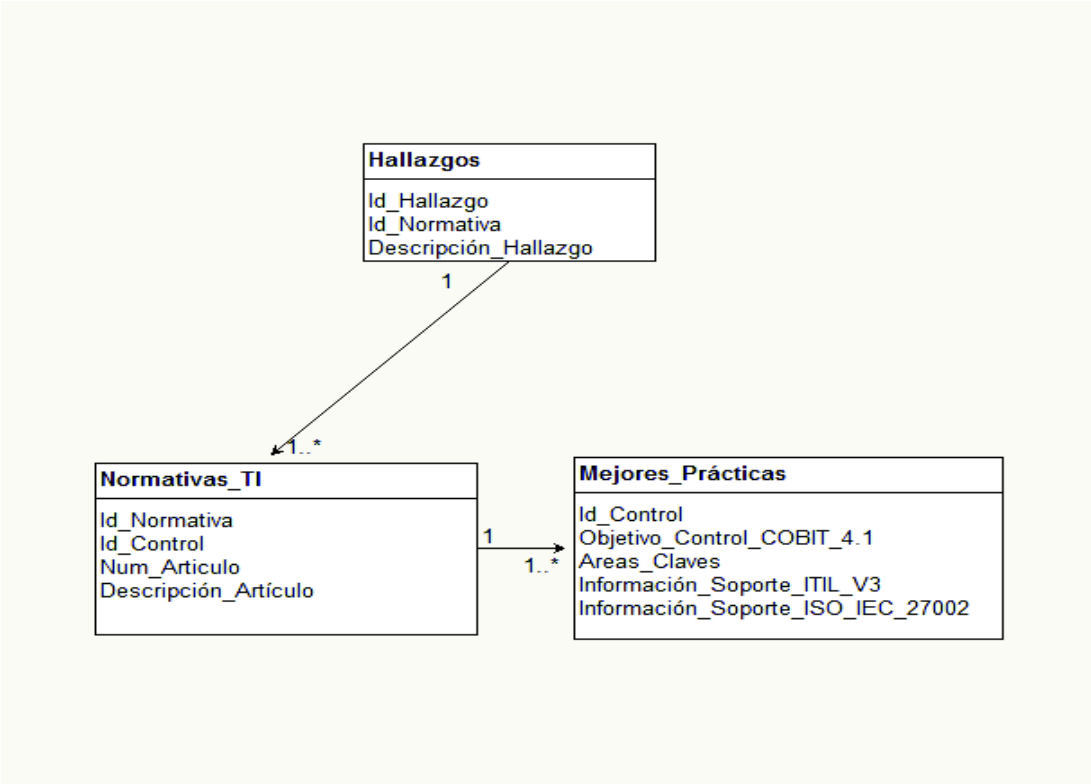


Figura 4. Modelo de Entidad Relación (DER) Fuente: Elaboración Propia.

Para complementar el diagrama de entidad relación , se realizo un diagrama de clases, el cual en ingeniería de software es un tipo de diagrama de estructura estática que describe la estructura de un sistema mostrando las clases del sistema, sus atributos, operaciones (o métodos), y las relaciones entre los objetos.

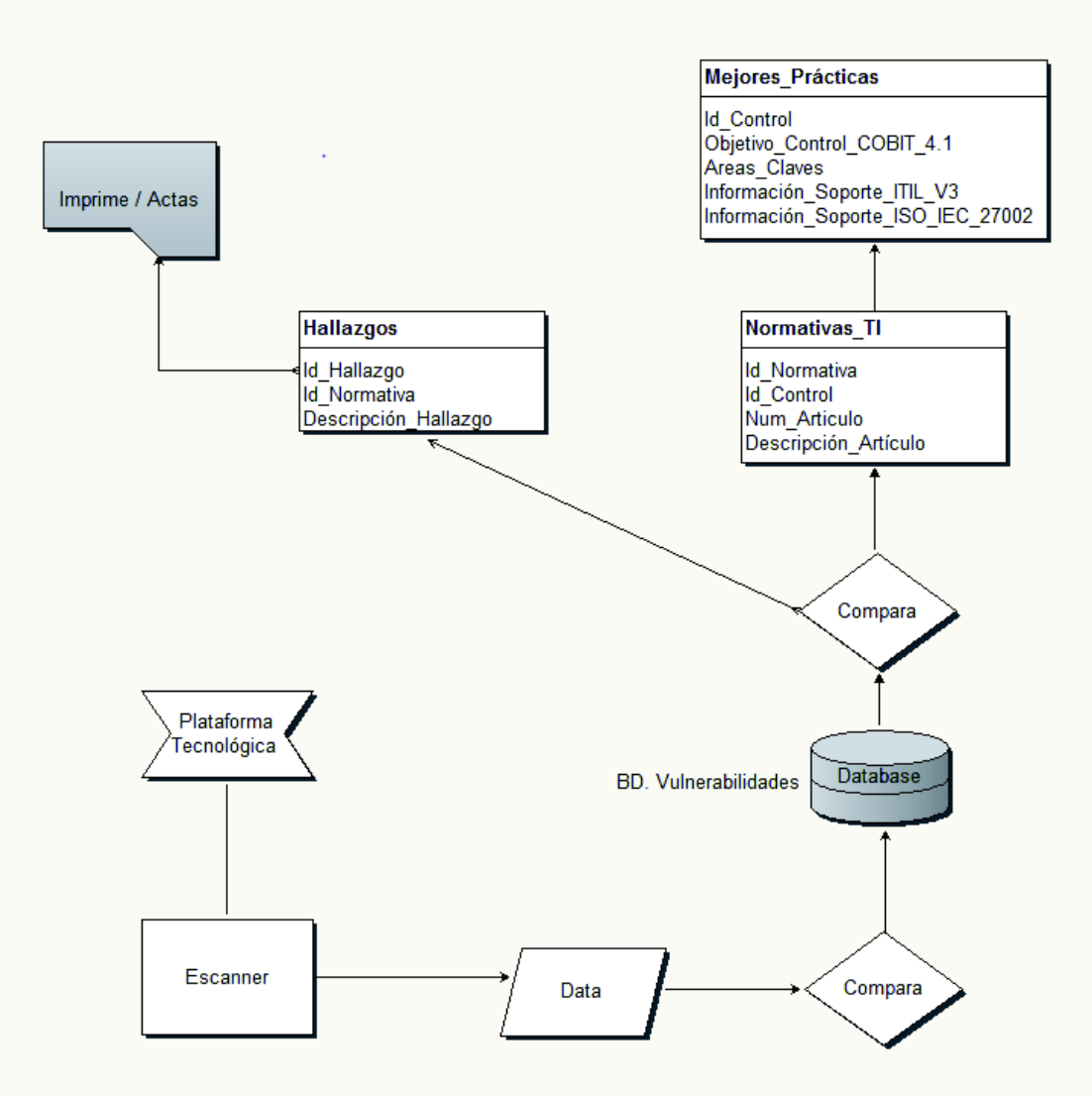


Figura 5. Diagrama de Clases Fuente: Elaboración Propia.

En la figura anterior, se muestra la interrelación existente entre cada una de las tablas que se tomaron en cuenta en la realización de la base de datos para el desarrollo del modelo propuesto. Según Herrarte, (2005), la información de una base de datos se guarda en tablas. Una tabla es una especie de archivo en el cuál definimos una estructura de filas y columnas con la información que deseamos almacenar. Adicionalmente, se presenta un total de tres (3) tablas las cuales están estrechamente vinculadas con el Diccionario de Datos requerido para identificar las vulnerabilidades y hallazgos en función de las Normativas de TI, las cuales se describen a continuación.

Tabla 12. Mejores Prácticas

Campo	Tipo	Long.	PK	FK	Observaciones
Id_Control	Varchar	10	SI	SI	Código que identifica el estándar o mejor práctica
Objetivo_Control_COBIT_4.1	Varchar	1000	----	----	Titulo del Objetivo de Control
Areas_Clave	Varchar	1000	----	----	Listado de áreas claves de acuerdo al objetivo de control
Información_Soporte_ITIL_V3	Varchar	2000	----	-----	Listado de los procesos soportados por ITIL V3
Información_Soporte_ISO_IEC_27002	Varchar	2000	----	----	Listado de los procesos soportados por ISO IEC 27002

Fuente: Elaboración propia.

Tabla 13. Normativas TI (Articulos_Normativa_TI).

Campo	Tipo	Long.	PK	FK	Observaciones
Id_Normativa	Varchar	10	SI	SI	Código que identifica el artículo de la normativa
Id_Control	Varchar	1000	----	SI	Código que identifica el estándar o mejor práctica asociado al artículo
Num_Artículo	Varchar	10	----	----	Número que identifica al artículo de la Normativas
Descripción_Artículo	Varchar	5000	----	----	Redacción del artículo

Fuente: Elaboración propia.

Tabla 14. Hallazgos.

Campo	Tipo	Long.	PK	FK	Observaciones
Id_Hallazgo	Varchar	10	SI	SI	Identificador del hallazgo
Id_Normativa	Varchar	10	----	----	Identificador de la normativa
Descripción_Hallazgo	Varchar	1000	----	----	Redacción del hallazgo

Fuente: Elaboración propia.

Como se puede evidenciar la tabla número 12, relacionada con los estándares y mejores prácticas, contiene la descripción de los estándares, el identificador del control y las áreas claves.

Por su parte, la tabla 13, inherente a los artículos de las Normativas de TI, presenta la descripción de artículo, el identificador de la Normativa, el identificador del control y el número de los artículos estipulados en los marcos legales emitidos por la SUDEBAN.

Por último, la tabla 14, relacionada con los hallazgos, contiene identificador del hallazgo, identificador de la normativa y la redacción de los hallazgos producto del incumplimiento de los artículos de la normativa.

4.4 La propuesta del Modelo.

4.4.1 Ubicación de los requerimientos.

Se estableció la ubicación que tienen los requerimientos de uso y de implementación obtenidos en la fase 2 dentro de cada una de las etapas que componen el modelo, determinando la relación que existe entre dichos requerimientos con los objetivos establecidos en cada etapa, de acuerdo a la funcionalidad que ofrece cada una de estas en el mismo.

4.4.2. Construcción del Modelo

Se construyo un modelo que compara el resultado del scanner con vulnerabilidades conocidas a fin de determinar la existencia de hallazgos o debilidades de control, y a su vez, estos hallazgos se relacionaron con los artículos de las Normativas asociadas a la TI, con el propósito de determinar el riesgo de incumplimiento (Riesgo Legal) y el tecnológico derivado de este el cual se explica en cada una de las siguientes fases:

4.4.3. Fase I: Reconocimiento (recolección de información)

Esta fase tuvo como objetivo obtener y ampliar información sobre la red objetivo a partir de su nombre de dominio. Principalmente se pretendió ampliar el número de equipos de cómputo (en adelante: equipos) que se evaluaron posteriormente. Para ello se realizo lo siguiente: búsqueda de nombres de dominio a partir de direcciones IP, búsqueda de dominios de nivel superior, búsqueda de dominios mediante fuerza bruta, transferencias de zona, descubrimiento de topología de red.

Cabe resaltar, que en esta fase no se busco la detección de ninguna vulnerabilidad, pues, se pretendió fue obtener la mayor cantidad posible de equipos que la red objetivo tuvo con presencia en internet. De igual forma, se presentaron varias sub fases, las cuales se describen seguidamente

Búsqueda de dominios inversa: El objetivo de esta sub fase fue encontrar nombres de dominios relacionados con el dominio objetivo y que se encontraban en el mismo segmento de red, es decir, una vez determinada la dirección IP del dominio objetivo (esta dirección pudo obtenerse mediante el comando ping), se busco en el segmento IP/24 aquellos nombres de dominio que tenian relación con el dominio principal.

Esta búsqueda, fue soportada por la herramienta dnsrecon (ubicado en BT 4-R2 bajo la ruta /pentest/enumeration/dnsrecon). Con lo anterior se sumaron equipos potenciales para posterior evaluación. La ejecución de esta herramienta suministro todos los dominios registrados a las direcciones IP en el rango del dominio objetivo, con lo que se pudo detectar cuáles de ellos pertenecían o tenían relación con este, lo cual amplio la lista de equipos que se evaluaron posteriormente.

Búsqueda de dominios de nivel superior: Esta búsqueda, permitió detectar dominios de nivel superior (ejemplo de tales dominios: .com, .net, .org) asociados al nombre de dominio objetivo. En los casos donde se encontraron un dominio de nivel superior asociado al dominio objetivo, este se incluyo a la lista de equipos que se evaluaron en la fase siguiente. La búsqueda descrita anteriormente fue soportada por la herramienta dnsrecon.

Búsqueda de dominios mediante fuerza bruta: Esta búsqueda, permitió hallar subdominios del dominio principal objetivo, mediante fuerza bruta. Subdominios como ftp.dominio, smtp.dominio, entre otros, fueron el objetivo de esta etapa. Una vez más, si se detectaba un subdominio relacionado con la red objetivo se sometían a evaluación en la fase siguiente. Por otro lado se anoto que la herramienta dnsrecon también soporto esta etapa.

Transferencias de zona: Consistió en realizar consultas a los servidores de nombres de dominios encargados del dominio objetivo. Esto permitió conocer subdominios o dominios relacionados con este último. Cabe señalar, que esta técnica se aprovecha de la mala gestión de servidores DNS, que no se configuran para impedir que compartan base de datos de dominios con equipos diferentes de otros servidores DNS. El soporte de esta etapa fue la herramienta dnsenum.

Descubrimiento de topología de red: En este caso, la evaluación de seguridad se realizo desde el interior de la red objetivo, en dicha situación fue posible determinar la topología completa de la red mediante la escucha pasiva realizada con un sniffer. Esto capturo la información del protocolo de enrutamiento concerniente a las subredes que conformaban la topología.

Es importante mencionar que para esta fase fueron necesarios los siguientes requerimientos:

Requerimiento de Uso:

- Pendrive que contenga el software de escaneo que se conecte a la red.
- Se requiere acceder a la base de datos de vulnerabilidades.
- Debe estar fundamentado en la Normativa de tecnología de la información vigente.
- Evaluar el acceso de los usuarios para constatar que se permita sólo a los servicios para los cuales hayan sido específicamente autorizados.
- Considerar las redes y servicios de la red a las cuales se tienen acceso.

Requerimiento de Implementación:

- Establecer condiciones para permitir el acceso a un proveedor del servicio.

4.4.4. Fase II: Escaneo de puertos y enumeración de servicios

Producto de la ejecución de la fase anterior, se obtuvo una lista de todos los equipos de la red objetivo con presencia en internet. En la fase actual se examinaron los puertos y servicios de cada uno de estos equipos y con base en el tipo de servicios que ofrecían, se realizo inferencia sobre el papel que cada uno juega dentro de la red objetivo, así como también la naturaleza de los mismos (servidores, enrutadores, equipos inalámbricos o nodos terminales).

Adicionalmente, la información obtenida de la fase anterior, también fue de suma utilidad, para realizar una evaluación indiscriminada de todos los segmentos de red de la organización objeto de análisis. Es importante indicar, que en esta fase no se pretendió encontrar vulnerabilidad alguna, sino determinar los equipos críticos de la red objetivo a los cuales se les aplico el procedimiento que se describe en la fase de la siguiente sección.

Es importante mencionar que para esta fase fueron necesarios los siguientes requerimientos:

Requerimiento de Uso:

- Evaluar el acceso de los usuarios para constatar que se permita sólo a los servicios para los cuales hayan sido específicamente autorizados.
- Considerar las redes y servicios de la red a las cuales se tienen acceso.

4.4.5. Fase III: Escaneo de vulnerabilidades

En virtud de que la fase anterior proporciono una lista de equipos que se consideraron críticos o sensibles para la red objetivo, este subconjunto de equipos fue obtenido de un conjunto más grande (el conjunto de todos los equipos que la red objetivo tenia con presencia en internet) mediante la ejecución de la primera fase del modelo. Los equipos que se encontraron

como críticos, fueron los que finalmente se sometieron a evaluación en esta fase, en la que se procedió a la utilización de un escáner de vulnerabilidades.

Este tuvo como objetivo detectar los potenciales riesgos al que estuvieron expuestos los equipos seleccionados, debido a que estos juegan el rol más crítico para la red objetivo, una vez descargado e instalado el escáner, se ingreso el conjunto de equipos y/o segmento de red a escanear (estos equipos se seleccionaron a partir de la fase anterior), posteriormente este presento la opción de generar reportes en los que se indico con amplia descripción cada una de las vulnerabilidades encontradas con sus respectivas sugerencias de solución.

Igualmente, se sugirió seguir el manual de usuario de las herramientas de Kali Linux para llevar a cabo el escaneo de vulnerabilidades. Finalmente se recomendó que el escáner utilice el repositorio de vulnerabilidades del gobierno de los Estados Unidos, con lo que se garantizo que en todo momento las vulnerabilidades analizadas, fueron todas las que han sido reportadas hasta la actualidad.

Es importante mencionar que para esta fase fueron necesarios los siguientes requerimientos:

Requerimiento de Implementación:

- Contar con métodos de autenticación apropiados para controlar el acceso de usuarios remotos.
- Especificar mecanismos de conexión basados en la encriptación para los usuarios Remotos.
- Revisar los perfiles de usuarios con la finalidad de constatar que los usuarios tienen un identificador único (ID de usuario) para su uso personal.

- Contar con mecanismos seguros para el manejo de claves secretas.

4.4.6. Fase IV: Análisis de los resultados

Una vez obtenida la lista de los equipos de la red objetivo con presencia en internet y habiendo determinado cuáles de ellos juegan un rol crítico para la red, se procedió a desarrollar la tercera fase del modelo propuesto, desde la cual, se evaluaron los equipos críticos en busca de vulnerabilidades. Es en esta fase, donde se realizo la evaluación de todos los servicios y puertos activos de cada uno de los equipos encontrados como críticos para la red objetivo.

Cabe destacar, que el número total de vulnerabilidades evaluadas pudo haber ascendido hasta el total registrado según el Repositorio de vulnerabilidades de los Estados Unidos (base de datos nacional de vulnerabilidades, NVD por sus siglas en inglés), la cual desde el año 2002, reúne la información de todas las vulnerabilidades reportadas y se mantiene en actualización diaria con una tasa media de diez (10) vulnerabilidades nuevas diariamente (NIST, 2011),

Asimismo, se tomaron en cuenta los controles de las Normativas de TI emitidas por la SUDEBAN, estándares y mejores prácticas (COBIT 4.1, ITIL v3 e ISO 27002). Ahora bien, el hecho de que se pudieran evaluar la totalidad de las vulnerabilidades reportadas en todas las librerías señaladas, fue posible debido a que la herramienta sugerida para llevar a cabo esta fase de la propuesta del modelo, utilizo dicha base de datos para realizar la búsqueda de vulnerabilidades, esto además permitió que se pudieran evaluar la mayoría de los servicios ejecutados en un equipo de cómputo.

Es importante mencionar que para esta fase fueron necesarios los siguientes requerimientos:

Requerimiento de Uso:

- Se requiere acceder a la base de datos de vulnerabilidades.
- Debe estar fundamentado en la Normativa de tecnología de la información vigente.

4.4.7. Fase V: Presentación de los resultados

En relación al escaneo de vulnerabilidades, fue necesario considerar los siguientes pasos:

a. Presentación de hallazgos detectados producto del cruce entre las vulnerabilidades encontradas y los controles establecidos en las Normativas de TI emitidas por la SUDEBAN, estándares y mejores prácticas (ITIL, ISO 27001, ISO 27002, COBIT ,NVD).

b. Generación de un informe detallado con los resultados obtenidos durante todo el proceso de ejecución de las pruebas, con el correspondiente análisis de dicha información para poder ser interpretada de manera correcta y entender las implicaciones a nivel de seguridad sobre la infraestructura informática analizada

4.4.8. Diagrama del Modelo Conceptual

Para finalizar en la siguiente figura se muestra cada una de las fases propuestas en el modelo para la detección de vulnerabilidades en los canales electrónicos de las Instituciones Bancarias del sector privado en Venezuela; es importante destacar, que en el mismo se pueden apreciar los requerimientos mínimos necesarios en cada una de las fases, conjuntamente con las herramientas tecnológicas que las soportan.

. .

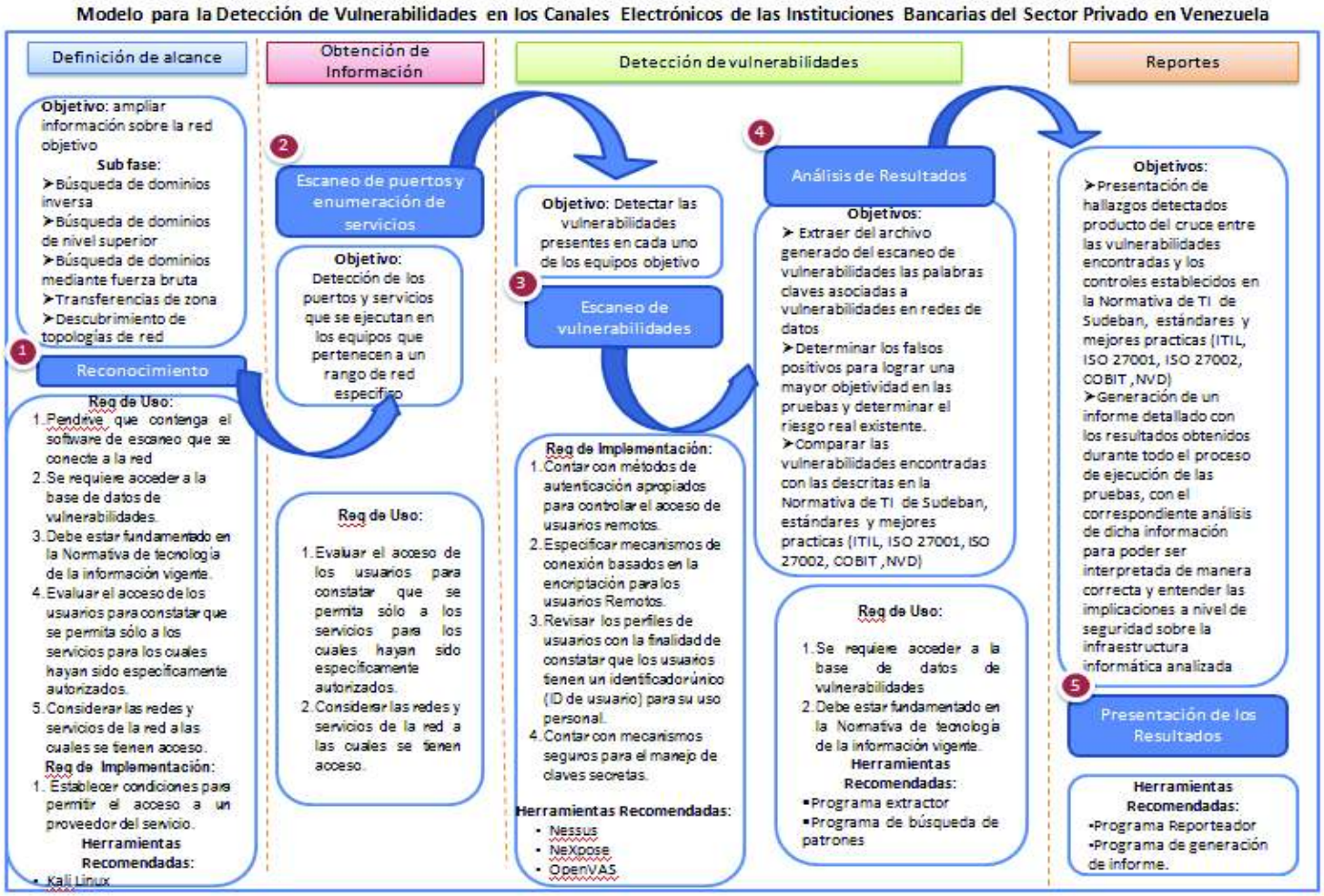


Figura 6. Propuesta del modelo. Elaborado por el autor (2015).

4.5 Validación del modelo.

El criterio para la selección de las personas a las cuales se les iba a mostrar el modelo resultante para su validación fue el siguiente:

a) Poseer cargos superiores al Nivel III. En este rango, entran los Examinador de Riesgo Tecnológico III y IV, Consultor Especialista de Riesgo tecnológico, Analista de Seguridad de la Información III, Coordinador de Seguridad de la Información, Analistas de Tecnología III y Coordinador de Tecnología. Asimismo, se incluyen en este grupo, los respectivos Gerentes de Área, como el Gerente de Riesgo Tecnológico, el Gerente de Seguridad de la Información y el Gerente de Tecnología. Este primer grupo estuvo compuesto por veintiún (21) personas en total.
b) Conocer el Sector Bancario. Al respecto, se determinó que del total de veintiún (21) personas, catorce (14) tenían experiencia en el sector bancario venezolano; es decir, habían laborado o tuvieron relación directa con este sector.
c) Tener experiencia mayor a ocho (8) años en el área de seguridad de la Información. Se determinó que de los catorce (14) personas resultantes del filtro anterior, doce (12) reunían el requisito de tener experiencia mayor a ocho (8) años en seguridad de la información.
d) Tener experticia en el área de Riesgo Tecnológico. Con este último filtro, el grupo se redujo a diez (10) personas. Nueve (9) de ellas pertenecientes a la Gerencia de Riesgo Tecnológico y una (1) a la Gerencia de Seguridad de la Información.
e) Finalmente, del grupo resultante, se retiraron a las personas que tienen cargos gerenciales, dado la poca disponibilidad de tiempo, quedando el grupo compuesto por siete (7) personas.

La validación del modelo para la detección de vulnerabilidades en las Instituciones Bancarias del Sector Privado en Venezuela consistió en aplicar el método de Delphi y se fundamento en la consulta a los siete (7) expertos antes mencionados. La aplicación de este método debió reunir, consolidar y distribuir respuestas a los miembros del grupo de expertos en cada una de las tres iteraciones, el proceso concluye cuando todos los expertos están de acuerdo con las recomendaciones o cambios realizados y no tienen más al respecto. Las consideraciones más notables que se obtuvieron de la aplicación del método Delphi fueron:

Fase de Reconocimiento:

Es importante mencionar que en esta fase se busca, identificar cada uno de los dispositivos de hardware o software residentes en la infraestructura que soportan los procesos del negocio. En la cual los especialistas opinaron que esta selección debe iniciarse con los servicios prestados, continuar luego con los procesos asociados a estos servicios y de allí, determinar los activos o dispositivos que soportan estos procesos.

Dentro de los posibles elementos de la infraestructura, que en un momento dado pudieran llegar a albergar vulnerabilidades a nivel de software se mencionaron los siguientes:

1. Servidores
2. Aplicaciones
3. Estaciones de trabajo
4. Bases de datos
5. Firewalls
6. Enrutadores

Continuando con la evaluación de esta fase el personal especialista debatió diversas opiniones y puntos de vista partiendo de que una vez determinada la dirección IP del dominio objetivo mediante el comando ping, se buscará en el segmento IP/24 aquellos nombres de dominio que tengan relación con el dominio principal. Al respecto, algunos recomendaron que esta búsqueda se hiciera con la herramienta dnsrecon dado que esta herramienta permite la búsqueda de dominios de nivel superior. También sugirieron la búsqueda mediante fuerza bruta y la transferencia de zona con la herramienta dnsenum. Otros consideraron importante realizar dentro de esta fase el descubrimiento de la Topología de Red para lo cual algunos recomendaron la herramienta wireshark porque sirve para escuchar pasivamente a través de una interfaz de red específica y otros recomendaron el uso del protocolo CDP para la evaluación de los equipos CISCO conectados en la red objetivo, dado que en la mayorías de los Bancos se utilizan equipos de esta marca. En cuanto a las herramientas de seguridad recomendadas, se hizo énfasis en usar Kali Linux ya que esta distribución posee un compendio de todas las herramientas sugeridas anteriormente.

El personal que estuvo presente en esta reunión opino de forma conjunta que el objetivo principal de esta fase debe ser el de suministrar todos los dominios registrados a las direcciones IP en el rango del dominio objetivo, para poder detectar cuáles de ellos pertenecen o tienen relación con este, y así poder ampliar la lista de equipos que se evaluarán posteriormente.

Fase de Escaneo Puertos.

El personal experto considero que esta fase es de gran importancia ya que permite el filtrado de los equipos que se consideran como críticos o sensibles para la red objetivo, por lo cual recomendó que se examinarán los puertos y servicios de cada uno de los equipos identificados en la fase anterior con base en el tipo de servicios que ofrecen. A su vez indicaron, que

se debe deducir el papel que cada uno de los equipos identificados juega dentro de la red que va a ser escaneada; así como la naturaleza de los mismos (servidores, enrutadores, equipos inalámbricos o nodos terminales). Adicionalmente. el grupo en consenso sugirió, que para la detección de puertos y servicios se debe bajar el RFC de los protocolos interesados como el ftp y el http con el objetivo de documentase bien acerca de su funcionamiento, dado que los mismos son muy utilizados para el desarrollo de esta fase.

En cuanto a la herramienta sugerida por el grupo, estuvo de primer lugar NMAP dado que en consenso se determinó que dicha herramienta es capaz de realizar escaneos de forma oculta (indetectable para firewalls) lo cual facilita las labores de escaneos sobre ciertos puertos, entre rangos de IP.

Fase de Escaneo Vulnerabilidades.

En esta fase los expertos recomendaron someter al escáner de vulnerabilidades solo al grupo de equipos que se consideren como críticos. Esto con el objetivo de detectar los potenciales riesgos al que están expuestos los mismos. Con respecto a las herramientas, se creó una polémica en cuanto a las ventajas y desventajas de cada una, llegando a estar de acuerdo en consenso por dos (2) de ellas, las cuales son, NeXpose y Nessus. Para la generación de reportes la mayor cantidad de votos fue para el escáner NeXpose debido a que este presenta la opción de generar reportes en los que se indican con amplia descripción cada una de las vulnerabilidades encontradas y de una vez se presentan sugerencias de solución. Además se tomó en consideración que el escáner NeXpose utiliza el repositorio de vulnerabilidades del gobierno de los Estados Unidos, con lo que se garantiza que en todo momento las vulnerabilidades analizadas, son todas las que han sido reportadas hasta la actualidad. Finalmente, los

especialistas discutieron las medidas preventivas adecuadas para la ejecución de escáner, esto con el fin de prevenir efectos adversos sobre la prestación de los servicios; quedando en definitiva las siguientes:

1. Definir hora adecuada de pruebas
    a. Horas de bajo tráfico
    b. Horarios de no prestación de servicios, si esto fuera posible

2. Realizar un análisis de riesgo cualitativo sobre la prueba
    a. Análisis sobre la no disponibilidad de activos críticos de la prueba
        I. Estimar una probabilidad
        II. Estimar un impacto

3. Tomar algunas medidas de contingencia
    a. Definir estrategias de contingencia para activos críticos
    b. Involucrar al oficial de seguridad y coordinador BCP, DRP
    c. Realizar respaldos de la información de los activos involucrados
    d. Guardar en formato electrónico y físico configuraciones de equipos involucrados

4. Realizar monitoreo de los servicios durante las pruebas
        I. Tiempos de respuesta excesivos
        II. Eventos o incidentes de seguridad

5. Se debe informar a operaciones de la realización de las pruebas

6. Se debe monitorear el tráfico de la red
        I. Utilización de los segmentos críticos
        II. Condiciones de error (CRC, Bad checksum)
        III. Utilización de CPU en servidores críticos

7. Informar a los dueños de los activos

Fase de Análisis de Resultados

Para esta fase, el grupo de especialistas recomendó que durante el proceso de extracción de datos se filtren los falsos positivos con objetivo de ofrecer un informe con el mínimo número de falsos positivos posibles. Como segunda recomendación dijeron, que se debe afinar los controles de las Normativas asociadas a la TI para que la comparación de las vulnerabilidades con la misma sea más eficaz. También se sugirió verificar que la base de datos de vulnerabilidades se encuentre actualizada y completa de vulnerabilidades aceptadas por la industria (CERT, SANS) y con un criterio común de clasificación como el CVE1 (common vulnerabilities and exposure).

Finalmente una vez realizadas las pruebas y contando con las anteriores recomendaciones, se apuntó en aprobación de los presentes realizar una reunión técnica para informar de estos resultados y realizar una revisión general de las vulnerabilidades encontradas y la clasificación realizada por la herramienta.

Se acordó que en esta reunión deben participar:

1. Oficial de seguridad
2. Dueños de procesos
3. Gerente de área
4. Comité de seguridad
5. Dueños de activos
6. Coordinador del plan de contingencias.

Fase de Presentación de Resultados

Para esta última fase, se recomendó desarrollar un estándar para la presentación de los hallazgos y la generación del Informe con el objetivo de que se mantenga la estructura homologada y los resultados puedan ser comparados en el tiempo durante futuras revisiones.

Para finalizar, se recomendó proponer un plan de remediación específico para las vulnerabilidades, el cual podría ser parte del plan de tratamiento general de riesgos, una vez se haya hecho un análisis formal y detallado de los resultados obtenidos tanto de la prueba de vulnerabilidades como de las de explotación. En este plan de remediación se deben clasificar con ayuda de la herramienta de vulnerabilidades y de explotación, la criticidad de cada una de las vulnerabilidades encontradas y sugerir cuales deben ser solucionadas en corto, mediano o largo plazo. Esta decisión sobre el tiempo a implantar el control respectivo a la vulnerabilidad, también debe contemplar costo del control, capacidad, administración y facilidad de implementación.

Cabe destacar que estas recomendaciones se realizaron basadas en la verdad consensual.

En definitiva las recomendaciones al modelo lo flexibilizan y ajustan a la realidad que existe en la Banca Venezolana, el modelo propuesto quedó constituido por cinco (5) fases: Reconocimiento, Escaneo de Puertos y enumeración de servicios, Escaneo de vulnerabilidades, Análisis y presentación de los resultados y cada una de ellas tiene a su vez los requerimientos mínimos necesarios que deben estar presentes para su implementación.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Del análisis y resultados obtenidos en el presente Trabajo de Grado el autor puede concluir:

- La situación actual del proceso de detección de vulnerabilidades en la Banca Venezolana; así como, los resultados obtenidos en la determinación de los requerimientos, el modelo relacional y la validación de los expertos, indican que el modelo propuesto es viable operativamente.
- La situación actual del proceso de detección de vulnerabilidades en los canales electrónicos de las instituciones Bancarias en Venezuela es deficiente.
- Los requerimientos mínimos necesarios para la formulación de la propuesta del modelo, se clasifican en requerimientos de uso y de implementación.
- El modelo debe relacionar las vulnerabilidades detectadas con los controles descritos en el marco legal, y a su vez, estos controles deben relacionarse con los artículos de las Normativas asociadas a la TI. De esta manera, se determina el riesgo tecnológico y de incumplimiento.
- Las fases a considerar para la implementación del modelo son: Reconocimiento, Escaneo de puertos y enumeración de servicios, Escaneo de vulnerabilidades, Análisis de resultados y Presentación de resultados.

5.2. Recomendaciones

El autor del presente Trabajo de Grado, basado en el análisis y los resultados obtenidos en la presente investigación recomienda:

- Implementar el modelo propuesto, tomando en consideración, que el mismo, representa una innegable oportunidad para el establecimiento de estrategias que permitirán gestionar las vulnerabilidades y el riesgo asociado de manera eficaz.

- El proceso de detección de vulnerabilidades se debe realizar bajo una gestión de accesos controlada y en días y horas de bajo impacto operacional.

- Efectuar periódicamente y con el apoyo de la Alta Gerencia, un análisis de vulnerabilidades a la plataforma tecnológica.

- Definir un proceso interno para la debida gestión de las vulnerabilidades detectadas y los riesgos asociados.

- Llevar un registro de los controles establecidos en las normativas vigentes asociadas a la TI, con el objeto de reducir el riesgo de incumplimiento derivado de las vulnerabilidades detectadas.

- Al aplicar los instrumentos de medición en otras instituciones Bancarias del país permitirá obtener una visión más amplia, en cuanto a la situación de la Seguridad de la Información en los Bancos nacionales.

- Se recomienda analizar la pertinencia de incorporar nuevas variables que ayuden ampliar los instrumentos, para así obtener una mayor profundidad en la evaluación del modelo.

REFERENCIAS BIBLIOGRÁFICAS

Arias, F. (2006). *El proyecto de investigación, Introducción a la metodología científica.* (5ta. Ed.). Caracas: Episteme.

Arriola, O. (2008). *"El Software Libre y la Enseñanza de la Catalogación: una relación amistosa".* En: Revista CODICE. Vol. 4, No. 2 (Julio-Diciembre 2008)

Balestrini, M. (2006). *Cómo se elabora el Proyecto de investigación***.** (7ma. Edición). Caracas: Consultores Asociados OBL.

Bavaresco, (2006). *Procesos metodológicos de la investigación.* Venezuela: Academia Nacional de Ciencias Económicas.

Bossio, H. y Gros, C. (2003). *Seguridad Informática parte de la Cultura de Control.* Argentina: Consejo Profesional en Ciencias Informáticas.

Cánchica, M. (2012). *El Proceso de Automatización.* (1ª Ed.). España: Académica Española.

Constitución de la República Bolivariana de Venezuela (1999). *Gaceta Oficial de la República Bolivariana de Venezuela, Número: 36.860*, Diciembre 30, 1999.

De León, Y. (2012). *"Modelo de Automatización basado en estándares de Software Libre para proteger la información. Caso: Gerencia Administrativa de la empresa TECNOLOGY 395 C.A.".* Trabajo Especial de Maestría no publicado. Universidad Metropolitana. Caracas.

Donado, S. Agredo, G. y Carrascal, C. (2002). *Políticas de Seguridad Computacional. Facultad de Ingeniería Electrónica y Telecomunicaciones.* Universidad del Cauca- Colombia. Documento en línea. Disponible desde: http:/www.criptored.upm.es/quiateoria/gt_m124c.htm. [Fecha de la consulta: Enero, 10, 2015]

Espiñeira, Sheldon y Asociados (2005). Seguridad de la Información: Un nuevo enfoque para el control de riesgos de negocio. Artículo en línea, Recuperado desde: www.pc-news.com/detalle.asp?&if=11&Ida=1926 [Fecha de la consulta: Enero, 12, 2015]

Fernández (2008). Investigación Aplicada. (2ª Ed.) Bogotá: Plaza & Janes.

Harris, L. (2009). Detección de Vulnerabilidades. (1ª Ed.). España: Gedisa.

Hernández, R. Fernández, C. y Baptista, P. (2010). *Metodología de la Investigación.* (5ª Ed.). México: McGraw-Hill Interamericana.

Instituto Colombiano de Normas Técnicas y Certificación. (INCOTEC) (2004). *Sistemas de Gestión de la Seguridad de la Información* (SGSI). Bogotá: ICONTEC.

Jiménez, F. (2012). **"***Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), para el resguardo y protección de los activos informáticos de la Universidad Bicentenaria de Aragua (UBA)"*. Trabajo de Maestría no publicado. Universidad Bicentenaria de Aragua (UBA), Aragua.

León, W. (2009). Vulnerabilidades y Amenazas Informáticas. (2ª Ed.). Chile: Tecnolibros.

Ley Especial Contra Delitos Informáticos (2001). *Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.313*, Octubre, 30, 2001.

Linares, D. (2010). *Elaboración de Proyectos de investigación, Tesinas y Tesis.* Carabobo: Educatec.

Méndez, C. (2004). *Metodología, diseño y desarrollo del proceso de investigación.* (3era. Ed). México: Mcgraw-Hill.

Osorio, R. (2010). *Sistemas de Información.* Chile: Tecnolibros.

Oz, E. (2005). *Administración de Sistemas de Información.* (4ª Ed.). México: Thomson Learning.

Padrón, J. (2000). *La forma del Proyecto de Tesis. Fragmento de "Recomendaciones para Seminario de Tesis".* Doctorado de UNEG. Puerto Ordaz. Recuperado desde: http://padron.entretemas.com/LaFormaDelProyectoDeTesis.htm [Fecha de la consulta: Enero, 30, 2015]

Palella, S. y Martins, F. (2006). *Metodología de la investigación Cuantitativa.* (2ª Ed.). Caracas: FEDEUPEL.

Quintero, W. (2010). *"Gestión de Seguridad de la Información para instituciones bancarias del Estado Táchira"*. Trabajo de Maestría no publicado. Universidad Nacional Experimental del Táchira (UNET). Táchira.

Ramió, J. (2006). Libro Electrónico de Seguridad Informática. Versión 41. Universidad Politécnica de Madrid. Documento en línea. Recuperado desde: http://www.criptored.upm.es/quiateoria/gt_m001a.htm (Fecha de la consulta: Enero, 23, 2015)

Rodríguez, D. (2010). *Ventajas y Desventajas del Software Libre.* Chile: Alianza Universidad Texto.

Ruiz, A. (2008). *Terminología empleada en el área: Instituciones bancarias.* Bogotá: Plaza & Janes.

Ruíz, I. (2013). *"Estudio de las Vulnerabilidades y Seguridad de la Información en las Instituciones bancarias de Venezuela, período 2000-2010".* Trabajo de Doctorado no publicado. Universidad Central de Venezuela. Caracas.

Sánchez, D. (2009). *Técnicas de investigación.* (1ª Ed.). Bogotá: Grupo Norma.

Tamayo y Tamayo, M. (2007). *El Proceso de Investigación Científica.* México: Limusa.

Universidad Pedagógica Experimental Libertador (2010). Vicerrectorado de Investigación Educativa. *Manual de Trabajos de Grado de Maestría y Tesis Doctórales.* Caracas: Autor.

Villamizar, J. (2013). *"Diseño de un Sistema Integrado de Gestión de la Seguridad de la Información del área de Control de operaciones de la empresa Plumrose Latinoamericana C.A."*. Trabajo de Maestría no publicado. Universidad Nacional Yacambú (UNY). Caracas.

Zúñiga, M. (2012). **"***Propuesta de un Modelo para la detección de Vulnerabilidades en los Sistemas de Información de las pequeñas y medianas empresas del Estado Aragua"*. Trabajo de Maestría no publicado. Universidad Bicentenaria de Aragua (UBA). Aragua.

Franco, David A, Perea, Jorge L, & Puello, Plinio. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. Información tecnológica, 23(3), 113-120. Recuperado en 11 de diciembre de 2015, de

http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S07180764201200 0300014&lng=es&tlng=es.. 10.4067/S0718-07642012000300014.

ANEXOS

Anexo A
[Check List N° 1]

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

VICERRECTORADO ACADÉMICO

ESTUDIOS DE POSTGRADO

ÁREA DE INGENIERÍA

Postgrado en Sistemas de Información

CHEKLIST Nº 1

OBJETIVO: Recabar información relacionada con las condiciones actuales del proceso de detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.			
ALCANCE Nº 1			
INVENTARIO DE ACTIVOS DE INFORMACIÓN (HARDWARE Y SOFTWARE)			
Aspectos	**Se cumple**	**No se cumple**	**Observaciones**
1.1. Políticas de Seguridad de la Información:			
1.1.1. Las Políticas de Seguridad de la Información están documentadas.			
1.1.2. Las Políticas de Seguridad de la Información están redactadas en conformidad con los requerimientos legislativos, reguladores y restrictivos.			
1.1.3. Las Políticas de Seguridad de la Información se encuentran aprobadas por la Junta Directiva.			
1.1.4. Los objetivos de las Políticas de Seguridad de la Información están identificados y cumplen con los requerimientos organizacionales.			
1.1.5. Existe un enunciado que especifique la Intención y participación de la Alta Gerencia fundamentando sus objetivos y principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales de la			

organización.			
1.1.6. Las Políticas de Seguridad de la Información son revisadas a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad y actualización.			
1.1.7. Existe un listado de todos los activos de información indicando: marca, modelo, sistema operativo, tipo de teclado y su versión, ubicación física, cifrado, tipo de conexión y proveedor del equipo			
ALCANCE Nº 2			
IDENTIFICACIÓN DE VULNERABILIDADES Y AMENAZAS EN LOS CANALES ELECTRÓNICOS			
2.1. Cajeros Automáticos y Puntos de Venta:			
2.1.1. Se cuenta con el Esquema transaccional de las operaciones entre el Core Bancario y los ATM y POS y el TANDEM.			
2.1.2. Existe el diagrama físico y lógico de la red de telecomunicaciones, en el cual se identifiquen los computadores, servidores, conexiones a proveedores, entes externos, empresas; así como, todos los dispositivos conectados			
2.1.3. Se describe el funcionamiento de la infraestructura tecnológica incluyendo (enlaces de comunicación, redes y servidores asociados a los servicios de ATM y POS.			
2.1.4. Se cuenta con un registro de la cantidad de transacciones mensuales procesadas a través de Cajeros Automáticos y Puntos de Venta.			
2.1.5. Se cuentan con registros de Indicadores manejados y estadísticas de disponibilidad de Cajeros Automáticos y POS.			
2.1.6. Se cuentan con servicios monitoreados y herramienta utilizada por cada tipo de monitoreo.			
2.2. Banca por Internet:			
Las políticas, normas y procedimientos asociadas al uso de los factores de autenticación (persona natural y jurídica) contienen lo siguiente:			
2.2.1. Generación, custodia, distribución, asignación y reposición de dichos factores.			
2.2.2. Gestión de accesos.			
2.2.3. Que se prohíba divulgar la información protegida por los factores de autenticación.			
2.2.4. Que se prohíba solicitar a sus Clientes, a			

través de sus funcionarios, empleados, representantes o terceros, la información parcial o completa, establecida en los factores de autenticación de las categorías 2 ó 3.			
2.2.5. Campañas educacionales.			
2.3. Autenticación del Sitio Web:			
Antes de que el Cliente se autentique en Banca por Internet, se considera como mínimo lo siguiente:			
2.3.1. Certificados electrónicos (SSL) u otros mecanismos que permitan autenticar el sitio transaccional. (Verificar que el certificado ofrecido está vigente).			
2.3.2. Una vez que el Cliente verifica que se trata de la Institución e inicia una sesión segura, se muestra en forma notoria y visible, al menos la siguiente información: Fecha y hora del ingreso a su última sesión y el Nombre y apellido del Cliente.			
2.3.3. Se establecen mecanismos continuos que permiten analizar los sitios web de la Banca por Internet, a fin de detectar en línea vulnerabilidades y otros tipos de amenazas.			
2.4. Identificación y Autenticación del Cliente:			
2.4.1. Existe un esquema de autenticación utilizado para internet Banking (persona natural y persona jurídica).			
2.4.2. Se valida el identificador del cliente.			
2.4.3. Existen Mecanismos de protección utilizados para la transmisión, validación y almacenamiento del identificador, preguntas de seguridad, contraseña, (si fuera el caso). Esta información, donde se almacena personas y privilegios para acceder a la tabla, base datos u otros.			
2.4.4. Se chequean las pistas de auditorías activas.			
2.4.5. En el caso de las contraseñas asignadas por las Instituciones Bancarias, para el acceso a la Banca por Internet, se requiere en forma automática que el Cliente la modifique inmediatamente después de iniciar la primera sesión.			
2.4.6. Se revisa el mecanismo de generación y entrega de las claves dinámicas (OTP, Coordenadas, Token, Storage).			
2.4.7. Se evalúan los parámetros de inicio de sesión del cliente, con la finalidad de determinar			

que cumplan con los mismos.			
2.4.8. Se evalúan los mecanismos establecidos para notificar a través de campañas el funcionamiento de los canales electrónicos y de prevención del fraude que permitan educar y generar una cultura que proteja a los usuarios y usuarias de los servicios bancarios, de operaciones fraudulentas por parte de terceros.			
2.4.9. Se solicitan los procedimientos relacionados con las alerta tempranas y se comprueban que se encuentren documentados y formalizados.			
2.4.10. Se realizan las pruebas de control respectivas.			
2.4.11. Se solicita el árbol de opciones del IVR y se comprueba que cuentan con aquellas opciones que habilitan al cliente la posibilidad de reportar presuntos fraudes y obtener asistencia al reclamo.			
2.4.12. Se cuentan con procesos, mecanismos y sistemas asociados al bloqueo preventivo de acceso a la banca por Internet, ATM y POS.			
2.4.13. Existen mecanismos y sistemas utilizados para la detección de fallas de dispensación de efectivo en ATMs. y comprobación del reintegro del monto comprometido se hace de manera inmediata, incluyendo, la revisión de las tablas de error.			
2.4.14. Existen reportes y estadísticas asociados a los eventos por fallas de dispensación de efectivo en ATMs.			
2.4.15. Se cuenta con sistema de monitoreo de Seguridad y Antifraude.			
2.4.16. Se realiza un estudio establecido por la UAIR en el cual se reflejan los montos máximos diarios para retiro por cada canal, y se evalúan los parámetros establecidos en los sistemas de banca electrónica, a fin de determinar la homogeneidad en los montos.			
ALCANCE Nº 3			
APLICACIÓN DEL ESCÁNER PARA DETERMINAR VULNERABILIDADES			
3.1. Se cuenta actualmente con herramientas tecnológicas para la detección de vulnerabilidades en los canales electrónicos de la Institución.			
3.2. Cuenta con un cronograma de actividades para la revisión, detección y análisis de vulnerabilidades en los canales electrónicos de			

la institución.			
3.3. Se realizan plan o ejecución con las actividades a realizar para mitigar el riesgo asociado a las vulnerabilidades detectadas en los canales electrónicos de la Institución.			
3.4. Se realiza control y seguimiento a los casos de vulnerabilidades identificadas.			
3.5. Cuenta con algún instrumento que permita medir la eficiencia y eficacia con la que se realiza el proceso de detección de vulnerabilidades. (Revisión, detección, análisis, control y seguimiento)			
ALCANCE N° 4			
ANÁLISIS DE RIESGO DE LAS VULNERABILIDADES			
4.1. Se cuenta con una gestión de Seguridad de la Información basada en una metodología de Análisis de Riesgo de la organización que produzca resultados comparables y reproducibles.			
4.2. Se mantiene un histórico de las vulnerabilidades detectadas en el tiempo.			
4.3. Se realiza un control y seguimiento a los casos de vulnerabilidades resueltos.			
4.4. Se cuenta con una base de datos de vulnerabilidades detectadas que sirva como apoyo para la debida gestión de las incidencias asociadas a la seguridad lógica.			
4.5. Se cuenta con un inventario de equipos críticos de la red objetivo a los cuales se les aplicará el escaneo de vulnerabilidades.			
4.6. Dentro del inventario se evalúan todos los servicios y puertos activos de cada uno de los equipos encontrados como críticos para la red objetivo.			
4.7. Se tiene un listado ordenado de equipos críticos de acuerdo a su nivel riesgo en alto, medio o bajo.			
4.8. Se atienden los casos de vulnerabilidades de acuerdo al nivel de riesgo que estos representen.			
ALCANCE N° 5			
PRESENTACIÓN DEL INFORME DE ANÁLISIS DE RIESGO CON LAS RECOMENDACIONES			
5.1. Existen Roles y Responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información.			
5.2. Se realiza un informe del análisis de riesgo			

periódicamente.			
5.3. Se realizan recomendaciones para mitigar los riesgos detectados.			
5.4. El informe presentado se encuentra formalizado por la máxima autoridad de TI y el área de seguridad de la Información.			
5.5. Existe un área encargada de centralizar y evaluar todos los informes generados.			

Anexo B
[Check List N° 2]

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

VICERRECTORADO ACADÉMICO

ESTUDIOS DE POSTGRADO

ÁREA DE INGENIERÍA

Postgrado en Sistemas de Información

CHEKLIST Nº 2

OBJETIVO: Recabar información relacionada con el proceso de realización de las pruebas de validación al Modelo planteado, fundamentadas en la Normativa de Banca Electrónica y Normativa de TI y Servicios Financieros.			
ALCANCE Nº 1			
IDENTIFICACIÓN DE LAS VULNERABILIDADES			
Aspectos	**Se cumple**	**No se cumple**	**Observaciones**
1.1 Se realiza actualmente un proceso de reconocimiento o identificación de vulnerabilidades en las redes de la institución en la cual se contempla el escaneo de puertos y la numeración de servicios.			
1.2 Se realiza un escaneo de vulnerabilidades presentes en cada uno de los equipos objetivo.			
1.3 La información producto del escaneo puede ser usada para identificar algún incumplimiento de los artículos estipulados en la Normativa de Banca Electrónica y Normativa de TI y Servicios Financieros.			
ALCANCE Nº 2			
CARACTERÍSTICAS DE LAS VULNERABILIDADES			
2.1 Las características de las vulnerabilidades a ser evaluadas se corresponden con las estipuladas en los artículos de la Normativa de Banca Electrónica y Normativa de TI y			

Servicios Financieros.			
2.2 Se cuenta con la identificación de las vulnerabilidades y sus características.			
2.3 Se cuenta con una base de datos actualizada de vulnerabilidades conocidas donde se especifiquen las características de las mismas y la manera de solucionarlas.			
ALCANCE N° 3			
CARACTERÍSTICAS DE LOS CONTROLES			
3.1 Las características de los controles de seguridad usados actualmente para la prevención de ataques a los canales electrónicos contemplan todos los descritos en los artículos de la Normativa de Banca Electrónica y Normativa de TI y Servicios Financieros.			
3.2 Los controles de seguridad usados por el banco actualmente cuentan con características que se ajustan a las modalidades de fraudes más recientes.			
3.3 Los controles de seguridad usados tienen características particulares para el medio en el cual son empleados.			
ALCANCE N° 4			
RELACIÓN CONTROLES-VULNERABILIDAD			
4.1 Los objetivos de control de la Normativa de Banca Electrónica y Normativa de TI y Servicios Financieros permiten mitigar los riesgos asociados a las vulnerabilidades presentes en los canales electrónicos de las instituciones bancarias del sector privado en Venezuela.			
4.2 Se lleva un registro de los controles establecidos con el objetivo de eliminar las vulnerabilidades presentes en los canales electrónicos.			
4.3 El banco cuenta con algún servicio adicional que permita establecer una relación entre un control y alguna vulnerabilidad detectada que no esté registrada en la base de datos de la institución.			
4.4 De no contar con un servicio externo se tiene definido algún proceso interno para la debida gestión de las vulnerabilidades detectadas bajo esta condición.			
ALCANCE N° 5			
MODELO DE RELACIÓN RESULTANTE DEL ANÁLISIS DE LA RELACIÓN ENTRE LAS VULNERABILIDADES Y LOS CONTROLES.			

5.1 Existe un modelo de relación resultante del análisis de la relación entre las vulnerabilidades y los controles abarca todos los artículos de la Normativa de Banca Electrónica y Normativa de TI y Servicios Financieros.			
5.2 Existe algún otro modelo o metodología que siga la institución con la finalidad de establecer las contra medidas necesarias en caso de que se detecten ciertos tipos de vulnerabilidades no identificadas.			

Anexo C
[Cuestionario tipo Likert]

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

VICERRECTORADO ACADÉMICO

ESTUDIOS DE POSTGRADO

ÁREA DE INGENIERÍA

Postgrado en Sistemas de Información

CUESTIONARIO

Estimado Gerente:

El siguiente cuestionario forma parte de un estudio para generar una **Propuesta de un Modelo basado en Software Libre para la detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela**, con el que se realiza un Trabajo Especial de Grado para optar al título de Magister en Sistemas de información del postgrado en Sistemas de Información de la Universidad Católica "Andrés Bello". Para lo cual agradecería su valiosa colaboración, tomando en cuenta que, la información que UD. suministre, será manipulada y procesada con total y absoluta privacidad.

Instrucciones:

1. Seguidamente se presentan una serie de interrogantes relacionadas con la temática de estudio de la investigación, las cuales deben ser respondidas en su totalidad.
2. Se presentan cuatro (4) alternativas de respuesta:
   - **Siempre (S)**
   - **Casi Siempre (CS)**
   - **Algunas Veces (AV)**
   - **Nunca (N)**
3. Marque con una equis (X) la opción que usted considere y exprese de manera favorable su criterio personal al respecto.

Muchas gracias por su contribución.

Nº	ÍTEM	(S)	(CS)	(AV)	(N)
VI. Requerimientos a considerar para la propuesta de un Modelo para la detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					
1	¿Considera Ud. que es necesario contar regularmente con un software de escaneo que se conecte a la Red?				
2	¿Para formular una propuesta de un modelo para la detección de vulnerabilidades en los canales electrónicos de las Instituciones bancarias, se requiere acceder a la base de datos de vulnerabilidades?				
3	¿La formulación de una propuesta de un Modelo para la detección de vulnerabilidades en los Canales Electrónicos debe estar fundamentada en lo establecido en la Normativa 641.10 de Banca Electrónica?				
VII. Controles de Seguridad de Información que se ajusten a los requerimientos de los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					
II.1. Control de acceso a Redes:					
4	¿Se debe evaluar el acceso de los usuarios para constatar que se permita sólo a los servicios para los cuales hayan sido específicamente autorizados?				
5	¿Se deben considerar las redes y servicios de la red a los cuales se tienen acceso?				
6	¿Se requieren establecer lineamientos para los procedimientos de autorización para determinar quién está autorizado a tener acceso a cuáles redes y servicios de redes?				
7	¿Es necesario establecer controles y procedimientos gerenciales para proteger el acceso a las conexiones de red y los servicios de red?				
8	¿Se deben establecer condiciones para permitir el acceso a un proveedor del servicio de Internet o sistema remoto?				
9	¿Se requiere de métodos de autenticación apropiados para controlar el acceso de usuarios remotos?				
II.2. Controles Criptográficos:					
10	¿Se deben especificar mecanismos de conexión basados en la encriptación para los usuarios Remotos Vg.. VPN?				
11	¿Es necesario el uso de mecanismos de encriptación para Conexiones Inalámbricas, preferiblemente a través del uso de PKI?				

II.3. Control de acceso a los Sistemas Operativos:					
12	¿El acceso a los sistemas operativos debería ser controlado mediante u procedimiento de registro seguro?				
13	¿Se deben revisar los perfiles de usuarios con la finalidad de constatar que los usuarios tienen un identificador único (ID de usuario) para su uso personal?				
14	¿Es necesario definir una técnica de autenticación adecuada para sustanciar la identidad del usuario?				
15	¿Los mecanismos para el manejo de claves secretas deben ser seguros?				
16	¿Deben seleccionarse mecanismos adecuados para la restricción y control del uso de programas de utilidad que puedan ser capaces de superar los controles del sistema?				
II.4. Control de acceso a la Aplicación de la Información:					
17	¿El acceso de los usuarios y del personal de soporte a la información y las funciones del sistema de la aplicación debe limitarse en concordancia con la política de control de acceso definida?				
18	¿Se debe verificar la existencia y aprobación de una Documentación de Perfiles, Grupos y Opciones de las distintas aplicaciones críticas?				
19	¿Se requieren proporcionar menús para controlar el acceso a las funciones del sistema de aplicación?				
20	¿Es necesario realizar una revisión de los módulos para reportes con la finalidad de evaluar que no se muestre información sensible en los casos que no se amerite?				
21	¿Los sistemas confidenciales deberían contar con un ambiente de cómputo dedicado (aislado)?				
VIII. Formulación del Modelo para la detección de vulnerabilidades en los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela.					
22	¿Se deben identificar la totalidad de las vulnerabilidades de los Canales Electrónicos de las Instituciones bancarias del sector privado en Venezuela?				
23	¿La definición del alcance del Modelo debe atender a los objetivos y estrategias comerciales establecidas en las Instituciones bancarias del sector privado?				
24	¿Se requiere el establecimiento de Políticas de seguridad qua atiendan a lo dispuesto en las				

	Normativa de tecnología de la información y la Normativa 641.10 de Banca Electrónica?				
25	¿Se debe definir claramente una metodología para clasificación y priorización de los riesgos y vulnerabilidades?				
26	¿Se requieren establecer responsabilidades y procedimientos para gestionar efectivamente los activos?				
27	¿La Gerencia debe comprometerse a garantizar el cumplimiento de los mecanismos y procedimientos para resguardar la seguridad del Recurso humano?				
28	¿Se requiere el establecimiento de controles que garanticen la seguridad física y ambiental de los activos de Información?				
29	¿Se deben establecer, documentar y revisar periódicamente las políticas de controles de acceso en base a los requerimientos comerciales y de seguridad de acceso?				
30	¿Es necesario determinar responsabilidades y establecer los procedimientos de Gestión de incidentes de Seguridad de Información para asegurar una respuesta rápida, efectiva y metódica ante los eventos ocurridos?				

Anexo D
[Minuta de validación del Modelo]

MINUTA

Fecha:	13 de mayo de 2015
Unidad:	Gerencia de Riesgo Tecnológico

Invitados	Cargo	Asistencia	Observaciones
Mario Duran	Examinador de Riesgo Tecnológico III	X	
Julio García	Examinador de Riesgo Tecnológico III	X	
Juan Echeverría	Examinador de Riesgo Tecnológico III	X	
Carlos Mora	Examinador de Riesgo Tecnológico III	X	
Franklin Santander	Examinador de Riesgo Tecnológico IV	X	
David Prada	Consultor Especialista	X	
Nelly Lugo	Consultor Especialista	X	

Asunto:	**Validación de la Propuesta de un Modelo para la Detección de Vulnerabilidades en los Canales Electrónicos de las Instituciones Bancarias del Sector Privado en Venezuela.**

Motivo de la Reunión:

1. Presentación de la definición de las fases del modelo.
2. Determinar la viabilidad operativa y técnica del modelo.

3. Presentar las recomendaciones y comentarios acerca del modelo.

Puntos Tratados y acuerdos:

- Se hizo una exposición en la que presentó la definición de cada una de las fases del modelo.
- Se mencionó el punto referido a la disponibilidad de los recursos necesarios para llevar a cabo el análisis de vulnerabilidades propuesto en el modelo.
- Se determinó la probabilidad de que el modelo se use como se supone y sea de utilidad para la detección de vulnerabilidades de forma oportuna.
- Por último los invitados dieron sus recomendaciones e hicieron comentarios de cada una de las fases del modelo, finalizando con una conclusión general del modelo evaluado.

Fase de Reconocimiento:

- La selección debe iniciarse con los servicios prestados, continuar luego con los procesos asociados a estos servicios y de allí, determinar los activos o dispositivos que soportan estos procesos.
- El personal que estuvo presente en esta reunión opino de forma conjunta que el objetivo principal de esta fase debe ser el de suministrar todos los dominios registrados a las direcciones IP en el rango del dominio objetivo, para poder detectar cuáles de ellos pertenecen o tienen relación con este, y así poder ampliar la lista de equipos que se evaluarán posteriormente.

Fase de Escaneo Puertos.

- Examinar los puertos y servicios de cada uno de los equipos identificados en la fase anterior con base en el tipo de servicios que ofrecen.
- Deducir el papel que cada uno de los equipos identificados juega dentro de la red que va a ser escaneada; así como la naturaleza de los mismos (servidores, enrutadores, equipos inalámbricos o nodos terminales).
- Bajar el RFC de los protocolos interesados como el ftp y el http con el objetivo de documentase bien acerca de su funcionamiento, dado que los mismos son muy utilizados para el desarrollo de esta fase.

- Usar NMAP dado que en consenso se determinó que dicha herramienta es capaz de realizar escaneos de forma oculta (indetectable para firewalls) lo cual facilita las labores de escaneos sobre ciertos puertos, entre rangos de IP.

Fase de Escaneo Vulnerabilidades.

- Someter al escáner de vulnerabilidades solo al grupo de equipos que se consideren como críticos.
- Usar las herramientas, NeXpose y Nessus.
- Tomar las medidas preventivas adecuadas para la ejecución de escáner, esto con el fin de prevenir efectos adversos sobre la prestación de los servicios

Fase de Análisis de Resultados

- Filtrar los falsos positivos con objetivo de ofrecer un informe mas preciso y confiable.
- Afinar los controles de las Normativas asociadas a la TI para que la comparación de las vulnerabilidades con la misma sea más eficaz.
- Verificar que la base de datos de vulnerabilidades se encuentre actualizada y completa de vulnerabilidades aceptadas por la industria (CERT, SANS) y con un criterio común de clasificación como el CVE1 (common vulnerabilities and exposure).

Fase de Presentación de Resultados

- Desarrollar un estándar para la presentación de los hallazgos y la generación del Informe con el objetivo de que se mantenga la estructura homologada y los resultados puedan ser comparados en el tiempo durante futuras revisiones.
- Proponer un plan de remediación específico para las vulnerabilidades, el cual podría ser parte del plan de tratamiento general de riesgos, una vez se haya hecho un análisis formal y detallado de los resultados obtenidos tanto de la prueba de vulnerabilidades como de las de explotación.

- Clasificar con ayuda de la herramienta de vulnerabilidades y de explotación, la criticidad de cada una de las vulnerabilidades encontradas y sugerir cuales deben ser solucionadas en corto, mediano o largo plazo.

Conclusiones Generales.

Se recomendó utilizar herramientas de análisis de vulnerabilidades que cuenten con una base de datos completa y actualizada de vulnerabilidades, adicionándole que en lo posible sea una herramienta automatizada para mejorar la efectividad de este proceso. A su vez es importante considerar la efectividad del plan de remediación, que como tal es la salida principal de todo este proceso de análisis de vulnerabilidad, y en últimas lo que garantizará la confiabilidad de los resultados producto de la aplicación del modelo propuesto.

Anexo E
[Tablas de Resultados CheckList N°1]

Alcance Nº 1.

Inventario de Activos de Información (Hardware y Software)

Tabla 2. Políticas de Seguridad de la Información.

Alternativas	Se cumple	FR	No se cumple	FR
1.1.1. Las Políticas de Seguridad de la Información están documentadas.	4	40%	6	60%
1.1.2. Las Políticas de Seguridad de la Información están redactadas en conformidad con los requerimientos legislativos, reguladores y restrictivos.	4	40%	6	60%
1.1.3. Las Políticas de Seguridad de la Información se encuentran aprobadas por la Junta Directiva.	3	30%	7	70%
1.1.4. Los objetivos de las Políticas de Seguridad de la Información están identificados y cumplen con los requerimientos organizacionales.	3	30%	7	70%
1.1.5. Existe un enunciado que especifique la Intención y participación de la Alta Gerencia fundamentando sus objetivos y principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales de la organización.	2	20%	8	80%
1.1.6. Las Políticas de Seguridad de la Información son revisadas a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad y actualización.	2	20%	8	80%
1.1.7. Existe un listado de todos los activos de información indicando: marca, modelo, sistema operativo, tipo de teclado y su versión, ubicación física, cifrado, tipo de conexión y proveedor del equipo	3	30%	7	70%

Alcance Nº 2.

Identificación de vulnerabilidades y amenazas en los canales electrónicos.

Tabla 3. 2.1. Cajeros Automáticos y Puntos de Venta.

Alternativas	Se cumple	FR	No se cumple	FR
2.1.1. Se cuenta con el Esquema transaccional de las operaciones entre el Core Bancario los ATM y POS.	3	30%	7	70%
2.1.2. Existe el diagrama físico y lógico de la red de telecomunicaciones, en el cual se identifiquen los computadores, servidores, conexiones a proveedores, entes externos, empresas; así como, todos los dispositivos conectados.	2	20%	8	80%
2.1.3. Se describe el funcionamiento de la infraestructura tecnológica incluyendo (enlaces de comunicación, redes y servidores asociados a los servicios de ATM y POS.	4	40%	6	60%
2.1.4. Se cuenta con un registro de la cantidad de transacciones mensuales procesadas a través de Cajeros Automáticos y Puntos de Venta.	4	40%	6	60%
2.1.5. Se cuentan con registros de Indicadores manejados y estadísticas de disponibilidad de Cajeros Automáticos y POS.	3	30%	7	70%
2.1.6. Se cuentan con servicios monitoreados y herramienta utilizada por cada tipo de monitoreo.	2	20%	8	80%

Fuente: Elaboración propia.

Tabla 4. 2.2. Banca por Internet. Las políticas, normas y procedimientos asociadas al uso de los factores de autenticación (persona natural y jurídica) contienen lo siguiente:

Alternativas	Se cumple	FR	No se cumple	FR
2.2.1. Generación, custodia, distribución, asignación y reposición de dichos factores.	6	60%	4	40%
2.2.2. Gestión de accesos.	4	40%	6	60%
2.2.3. Que se prohíba divulgar la información protegida por los factores de autenticación.	6	60%	4	40%
2.2.4. Que se prohíba solicitar a sus Clientes, a través de sus funcionarios, empleados, representantes o terceros, la información parcial o completa, establecida en los factores de autenticación de las categorías 2 ó 3.	8	80%	2	20%
2.2.5. Campañas educacionales.	3	30%	7	70%

Fuente: Elaboración propia.

Tabla 5. 2.3. Autenticación del Sitio Web. Antes de que el Cliente se autentique en Banca por Internet, se considera como mínimo lo siguiente:

Alternativas	Se cumple	FR	No se cumple	FR
2.3.1. Certificados electrónicos (SSL) u otros mecanismos que permitan autenticar el sitio transaccional. (Verificar que el certificado ofrecido está vigente).	8	80%	2	20%
2.3.2. Una vez que el Cliente verifica que se trata de la Institución e inicia una sesión segura, se muestra en forma notoria y visible, al menos la siguiente información: Fecha y hora del ingreso a su última sesión y el Nombre y apellido del Cliente.	8	80%	2	20%
2.3.3. Se establecen mecanismos continuos que permiten analizar los sitios web de la Banca por Internet, a fin de detectar en línea vulnerabilidades y otros tipos de amenazas.	4	40%	6	60%

Fuente: Elaboración propia.

Tabla 6. 2.4. Identificación y Autenticación del Cliente.

Alternativas	Se cumple	FR	No se cumple	FR
2.4.1. Existe un esquema de autenticación utilizado para internet Banking (persona natural y persona jurídica).	7	70%	3	30%
2.4.2. Se valida el identificador del cliente.	8	80%	2	20%
2.4.3. Existen Mecanismos de protección utilizados para la transmisión, validación y almacenamiento del identificador, preguntas de seguridad, contraseña, (si fuera el caso). Esta información, donde se almacena personas y privilegios para acceder a la tabla, base datos u otros.	6	60%	4	40%
2.4.4. Se chequean las pistas de auditorías activas.	7	70%	3	30%
2.4.5. En el caso de las contraseñas asignadas por las Instituciones Bancarias, para el acceso a la Banca por Internet, se requiere en forma automática que el Cliente la modifique inmediatamente después de iniciar la primera sesión.	5	50%	5	50%
2.4.6. Se revisa el mecanismo de generación y entrega de las claves dinámicas (OTP, Coordenadas, Token, Storage).	6	60%	4	40%
2.4.7. Se evalúan los parámetros de inicio de sesión del cliente, con la finalidad de determinar que cumplan con los mismos.	7	70%	3	30%
2.4.8. Se evalúan los mecanismos establecidos para notificar a través de campañas el funcionamiento de los canales electrónicos y de prevención del fraude que permitan educar y generar una cultura que proteja a los usuarios y usuarias de los servicios bancarios, de operaciones fraudulentas por parte de terceros.	8	80%	2	20%
2.4.9. Se solicitan los procedimientos relacionados con las alerta tempranas y se comprueban que se encuentren documentados y formalizados.	5	50%	5	50%
2.4.10. Se realizan las pruebas de control respectivas.	8	80%	2	20%
2.4.11. Se solicita el árbol de opciones del IVR y se comprueba que cuentan con	7	70%	3	30%

aquellas opciones que habilitan al cliente la posibilidad de reportar presuntos fraudes y obtener asistencia al reclamo.				
2.4.12. Se cuentan con procesos, mecanismos y sistemas asociados al bloqueo preventivo de acceso a la banca por Internet, ATM y POS.	8	80%	2	20%
2.4.13. Existen mecanismos y sistemas utilizados para la detección de fallas de dispensación de efectivo en ATMs. y comprobación del reintegro del monto comprometido se hace de manera inmediata, incluyendo, la revisión de las tablas de error.	8	80%	2	20%
2.4.14. Existen reportes y estadísticas asociados a los eventos por fallas de dispensación de efectivo en ATMs.	7	70%	3	30%
2.4.15. Se cuenta con sistema de monitoreo de Seguridad y Antifraude.	8	80%	2	20%
2.4.16. Se realiza un estudio establecido por la UAIR en el cual se reflejan los montos máximos diarios para retiro por cada canal, y se evalúan los parámetros establecidos en los sistemas de banca electrónica, a fin de determinar la homogeneidad en los montos.	7	70%	3	30%

Alcance Nº 3

Aplicación del escáner para determinar vulnerabilidades

Tabla 7. Aplicación del escáner para determinar vulnerabilidades.

Alternativas	Se cumple	FR	No se cumple	FR
3.1. Se cuenta actualmente con herramientas tecnológicas para la detección de vulnerabilidades en los canales electrónicos de la Institución.	3	30%	7	70%
3.2. Cuenta con un cronograma de actividades para la revisión, detección y análisis de vulnerabilidades en los canales electrónicos de la institución.	2	20%	8	80%
3.3. Se realizan plan o ejecución con las actividades a realizar para mitigar el riesgo asociado a las vulnerabilidades detectadas en los canales electrónicos de la	3	30%	7	70%

Institución.				
3.4. Se realiza control y seguimiento a los casos de vulnerabilidades identificadas.	4	40%	6	60%
3.5. Cuenta con algún instrumento que permita medir la eficiencia y eficacia con la que se realiza el proceso de detección de vulnerabilidades. (Revisión, detección, análisis, control y seguimiento)	3	30%	7	70%

Fuente: Elaboración propia.

Alcance Nº 4.

Análisis de riesgo de las vulnerabilidades.

Tabla 8. Análisis de riesgo de las vulnerabilidades.

Alternativas	Se cumple	FR	No se cumple	FR
4.1. Se cuenta con una gestión de Seguridad de la Información basada en una metodología de Análisis de Riesgo de la organización que produzca resultados comparables y reproducibles.	3	30%	7	70%
4.2. Se mantiene un histórico de las vulnerabilidades detectadas en el tiempo.	3	30%	7	70%
4.3. Se realiza un control y seguimiento a los casos de vulnerabilidades resueltos.	2	20%	8	80%
4.4. Se cuenta con una base de datos de vulnerabilidades detectadas que sirva como apoyo para la debida gestión de las incidencias asociadas a la seguridad lógica.	4	40%	6	60%
4.5. Se cuenta con un inventario de equipos críticos de la red objetivo a los cuales se les aplicará el escaneo de vulnerabilidades.	5	50%	5	50%
4.6. Dentro del inventario se evalúan todos los servicios y puertos activos de cada uno de los equipos encontrados como críticos para la red objetivo.	4	40%	6	60%
4.7. Se tiene un listado ordenado de equipos críticos de acuerdo a su nivel riesgo en alto, medio o bajo.	3	30%	7	70%
4.8. Se atienden los casos de vulnerabilidades de acuerdo al nivel de	4	40%	6	60%

riesgo que estos representen.				

Fuente: Elaboración propia.

Alcance Nº 5.

Presentación del informe de análisis de riesgo con las recomendaciones.

Tabla 9. Presentación del informe de análisis de riesgo con las recomendaciones.

Alternativas	Se cumple	FR	No se cumple	FR
5.1. Existen Roles y Responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información.	4	40%	6	60%
5.2. Se realiza un informe del análisis de riesgo periódicamente.	3	30%	7	70%
5.3. Se realizan recomendaciones para mitigar los riesgos detectados.	6	60%	4	40%
5.4. El informe presentado se encuentra formalizado por la máxima autoridad de TI y el área de seguridad de la Información.	4	40%	6	60%
5.5. Existe un área encargada de centralizar y evaluar todos los informes generados.	2	20%	8	80%

Fuente: Elaboración propia.

Anexo F
[Tabla Mejores Prácticas]

Tabla 10. Tabla de Mapeo de ITIL v3 e ISO/IEC 27002 con los Objetivos de Control de COBIT 4.1

Id_Control	Objetivo de Control COBIT 4.1	Áreas clave	Información de soporte ITIL V3	Información de soporte ISO/IEC 27002:2005
1	PO1.1 Gestión del valor de TI	Caso de negocio • Asignación presupuestal • Obtención de beneficios • Evaluación de caso de negocio	SS 3.1 Creación de valor • SS 3.4 Estructuras del servicio • SS 4.4 Preparar la ejecución • SS 5.1 Gestión financiera • SS 5.2 Retorno sobre la inversión • SS 5.3 Gestión del portafolio de servicios • SS 5.4 Métodos de gestión del portafolio de servicios	
2	PO1.2 Alineación de TI con el negocio	• Alineamiento de TI con la estrategia del negocio • Involucramiento bi-direccional y recíproco en el plan estratégico	• SS 2.1 ¿Qué es gestión del servicio? • SS 2.3 El proceso de negocio • SS 2.4 Principios de la gestión del servicio	
3	PO1.3 Evaluación del desempeño y la capacidad actual	• Línea base del desempeño actual • Evaluación de la contribución del negocio, funcionalidad, estabilidad, complejidad, costos, fortalezas y debilidades	• SS 4.4 Preparar la ejecución • CSI 5.2 Evaluaciones	
4	PO1.4 Plan estratégico de TI	• Definición de objetivos de TI	• SS 3.3 Tipos de proveedor de	

		• Contribución a los objetivos de la empresa, presupuestos, financiación, compras y estrategia de adquisición	servicio • SS 3.5 Fundamentos de la estrategia del servicio • SS 4.1 Definir el mercado • SS 4.2 Desarrollar las ofertas • SS 4.3 Desarrollar activos estratégicos • SS 4.4 Preparar la ejecución • SS 5.5 Gestión de la demanda • SS 6.5 Estrategia de sourcing	
5	PO1.5 Planes tácticos de TI	• Iniciativas de TI • Requerimientos de recursos • Monitoreo y gestión del logro de beneficios	• SS 4.4 Preparar la ejecución • SS 7.1 Implementación a través del ciclo de vida • SS 7.2 Estrategia y diseño • SS 7.3 Estrategia y transiciones • SS 7.4 Estrategia y operaciones	
6	PO1.6 Gestión del portafolio de TI	• Definiendo, priorizando y gestionando programas • Clarificando el alcance y los resultados del esfuerzo • Asignando el rol de la rendición de cuentas • Asignando recursos y financiamiento	• SS 2.5 El ciclo de vida del servicio • SS 3.4 Estructuras del servicio • SS 4.2 Desarrollar las ofertas • SS 4.3 Desarrollar activos estratégicos • SS 5.3 Gestión del portafolio de servicios • SS 5.4 Métodos de	

			gestión del portafolio de servicios • SS 5.5 Gestión de la demanda • SD 3.4 Identificar y documentar los requisitos y drivers del negocio • SD 3.6.1 Diseño de soluciones de servicios • SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios	
7	PO2.1 Modelo de arquitectura de información empresarial	Análisis de soporte a las decisiones • Mantenimiento del modelo de arquitectura de información • Modelo corporativo de datos	• SD 3.6 Aspectos de diseño • SD 3.6.3 Diseño de la arquitectura tecnológica • SD 3.9 Arquitectura orientada al servicio • SD 3.10 Gestión de servicio al negocio • SD 5.2 Gestión de los datos y la información • ST 4.7 Gestión del conocimiento	
8	PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	• Diccionario corporativo de datos • Comprensión general de los datos	• SD 5.2 Gestión de los datos y la información • SD 7 Consideraciones tecnológicas	• 7.1.1 Inventario de activos • 11.1.1 Políticas de control de acceso
9	PO2.3 Esquema de	• Clases de información	• SD 5.2 Gestión de los	• 7.2.1

	clasificación de datos	• Propietarios • Retención • Reglas de acceso • Niveles de seguridad para cada clase de información	datos y la información	Lineamientos para la clasificación • 10.7.1 Gestión de medios removibles • 10.8.1 Políticas y procedimientos para el intercambio de información • 10.8.2 Acuerdos de intercambio • 11.1.1 Políticas de control de acceso
10	PO2.4 Gestión de integridad	• Integridad y consistencia de los datos	• SD 5.2 Gestión de los datos y la información • ST 4.7 Gestión del conocimiento	
11	PO3.1 Planeamiento de la orientación tecnológica	• Tecnologías disponibles • Habilitación de la estrategia de TI • Arquitectura de sistemas • Dirección tecnológica • Estrategias de migración	• SS 8 Estrategia y tecnología	• 5.1.2 Revisión de la política de seguridad de la información • 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio • 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
12	PO3.2 Plan de infraestructura	• Plan de infraestructura	• SD 3.6.3 Diseño de la arquitectura	

	tecnológica	tecnológica • Orientación sobre adquisiciones • Economías de escala • Interoperabilidad de plataformas	tecnológica	
13	PO3.3 Monitoreo de tendencias y regulaciones futuras	• Sector del negocio, industria, tecnología, infraestructura, las tendencias legales y reglamentarias	• SS 2.4 Principios de la gestión del servicio • SD 4.3.5.7 Modelamiento y tendencias	• 6.1.1 Compromiso de la gerencia con la seguridad de la información
14	PO3.4 Estándares tecnológicos	• Fórum tecnológico • Estándares y directrices de productos		• 10.3.2 Aceptación del sistema • 10.8.2 Acuerdos de intercambio • 11.7.2 Teletrabajo
15	PO3.5 Consejo de arquitectura de TI	Estándares y directrices de arquitectura tecnológica		• 6.1.1 Compromiso de la gerencia con la seguridad de la información
16	PO4.1 Marco de trabajo de procesos de TI	• Estructura y relaciones del proceso de TI • Propiedad de los procesos • Integración con los procesos del negocio, la gestión del portafolio de la empresa y los procesos de cambio	• SS 2.6 Funciones y procesos a través del ciclo de vida • SS 3.4 Estructuras del servicio • SS 7.1 Implementación a través del ciclo de vida • SS 9.1 Complejidad • SS 9.2 Coordinación y control • SS 9.3 Preservando valor • SS 9.4 Efectividad en mediciones • SD 2.4.2 Alcance • SD 3.6.3 Diseño de la arquitectura	

			tecnológica • SD 3.6.4 Diseño de procesos • SD 3.6.5 Diseño de sistemas de medición y métricas • SD 4 Procesos del diseño del servicio • SD 6.1 Análisis de roles funcionales • SD 6.2 Análisis de actividades • SD 6.3 Habilidades y atributos • SD 6.4 Roles y responsabilidades • SD 8 Implementar el diseño del servicio • SD Apéndice C Plantillas de documentación de procesos (ejemplo) • ST 3.2.7 Establecer controles y disciplinas eficaces • ST 4 Procesos de transición del servicio • ST 6.1 Roles genéricos • ST 8 Implementar la transición del servicio • SO 2.3 Funciones y procesos a través del ciclo de vida	

			• SO 4 Procesos de operación del servicio • SO 4.6 Actividades operativas del proceso cubiertas en otras fases del ciclo de vida • SO 6 Organización para la operación del servicio • SO 8 Implementar la operación del servicio • CSI 3.11 Marcos, modelos, estándares y sistemas de calidad • CSI 4 Procesos de mejora continua del servicio • CSI 4.1.1 Integración con el resto de etapas del ciclo de vida y los procesos de gestión del servicio • CSI 5.2 Evaluaciones • CSI 5.5 El ciclo Deming CSI 8 Implementar la mejora continua del servicio	
17	PO4.2 Comité estratégico de TI	• Comité de dirección • Gobierno de TI • Dirección estratégica • Revisión de las inversiones	• SD 2.4.2 Alcance	
18	PO4.2 Comité estratégico de TI	• Comité de dirección • Gobierno de TI • Dirección estratégica • Revisión de las inversiones	• SD 2.4.2 Alcance	
19	PO4.3 Comité directivo de TI	• Priorización del programa de inversiones y el seguimiento de estado de proyectos • Resolución de recursos • Servicios de monitoreo		• 6.1.1 Compromiso de la gerencia con la seguridad de la información • 6.1.4 Proceso de autorización para las instalaciones de procesamiento de información

20	PO4.4 Ubicación organizacional de la función de TI	• Significado de negocio de TI • Líneas de reporte del CIO	• SS 6.1 Desarrollo organizacional • SO 3.2.4 Organizaciones reactivas versus proactivas	• 6.1.1 Compromiso de la gerencia con la seguridad de la información • 6.1.2 Coordinación para la seguridad de la información • 6.1.3 Asignación de las responsabilidades para la seguridad de la información • 6.1.4 Proceso de autorización para las instalaciones de procesamiento
21	PO4.5 Estructura organizacional de TI	• Alineamiento organizacional con las necesidades del negocio	• SS 2.6 Funciones y procesos a través del ciclo de vida • SS 6.1 Desarrollo organizacional • SS 6.2 Departamentalización organizacional • SS 6.3 Diseño organizacional • SS 6.5 Estrategia de sourcing • SS Apéndice B2 Gerentes de producto • SD 6.3 Habilidades y atributos • ST 4.2.6.8 Consejo consultivo de cambios • ST 6.2 Contexto organizacional para la transición de servicios • ST 6.3 Modelos organizacionales para apoyar la transición de servicios • SO 3.1 Funciones, grupos, equipos, departamentos y divisiones • SO 3.2 Obtener balance en la operación del servicio • SO 3.3 Prestación del servicio • SO 6.1 Funciones • SO 6.2 Mesa de servicios • SO 6.3 Gestión técnica • SO 6.4 Gestión de operaciones de TI • SO 6.5 Gestión de aplicaciones • SO 6.7 Estructuras organizacionales de operación	• 6.1.1 Compromiso de la gerencia con la seguridad de la información • 6.1.2 Coordinación para la seguridad de la información

22	PO4.6 Establecer roles y responsabilidades	• Roles y responsabilidades explícitos. • Clara rendición de cuentas y autorizaciones de usuario final	• **SS 2.6 Funciones y procesos a través del ciclo de vida** • **SD 6.2 Análisis de actividades** • **SD 6.4 Roles y responsabilidades** • **ST 6.3 Modelos organizacionales para apoyar la transición de servicios** • **SO 6.6 Roles y responsabilidades en la operación del servicio • CSI 6 Organización para la mejora continua del servicio**	• *6.1.2 Coordinación para la seguridad de la información* • *6.1.3 Asignación de las responsabilidades para la seguridad de la información* • *6.1.5 Acuerdos de confidencialidad* • *8.1.1 Roles y responsabilidades* • *8.1.2 Verificación* • *8.1.3 Términos y condiciones del empleo* • *8.2.2 Educación, entrenamiento y concientización en seguridad de información* • *15.1.4 Protección de datos y privacidad de la información personal*
23	PO4.7 Responsabilidades para el aseguramiento de la calidad de TI (QA)	• Responsabilidad, experiencia e implementación de control de calidad según los requisitos de la organización	• *CSI 6 Organización para la mejora continua del servicio*	
24	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	• Propiedad de riesgos de TI en el negocio • Roles para gestionar riesgos críticos • Gestión de la seguridad y los riesgos en toda la empresa • Seguridad específica de sistemas • Dirección del apetito de riesgo y la aceptación del riesgo residual	• *SD 6.4 Roles y responsabilidades*	• **6.1.1 Compromiso de la gerencia con la seguridad de la información** • **6.1.2 Coordinación para la seguridad de la información** • **6.1.3 Asignación de las responsabilidades para la seguridad de la información** • **8.1.1 Roles y responsabilidades** • **8.2.1 Responsabilidades de la Gerencia** • **8.2.3 Procesos disciplinarios** • **15.1.1 Identificación de legislación aplicable** • **15.1.2 Derechos**

				de propiedad intelectual • **15.1.3 Protección de registros organizacionales** • **15.1.4 Protección de datos y privacidad de la información personal** • **15.1.6 Regulación de controles criptográficos** • **15.2.1 Cumplimiento con políticas y estándares de seguridad**
25	PO4.9 Propiedad de los datos y sistemas	• Habilitación de la propiedad de los datos • Toma de decisiones sobre la clasificación de información	• *SO 6.3 Gestión técnica*	• *6.1.3 Asignación de las responsabilidades para la seguridad de la información* • *6.1.4 Proceso de autorización para las instalaciones de procesamiento de información* • *7.1.2 Propiedad de los activos* • *9.2.5 Seguridad de los equipos fuera de las instalaciones*
26	PO4.10 Supervisión	• Roles y responsabilidades • Revisión de los indicadores clave de desempeño (KPIs)		• *6.1.2 Coordinación para la seguridad de la información* • *6.1.3 Asignación de las responsabilidades para la seguridad de la información* • *7.1.3 Uso aceptable de activos* • *8.2.1 Responsabilidades de la Gerencia*
27	PO4.11 Segregación de funciones	• Ejecución apropiada de roles y responsabilidades • Evitar el compromiso de procesos críticos	• *ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado* • *SO 5.13 Gestión de seguridad de la información y la operación del servicio*	• *8.2.1 Responsabilidades de la Gerencia* • *10.1.3 Segregación de funciones* • *10.1.4 Separación de los entornos de desarrollo, pruebas y*

				producción • *10.6.1 Controles de red*
28	PO4.12 Personal de TI	• Número y competencia; evaluación de requerimientos	• *SO 6.2 Mesa de servicios*	
29	PO4.13 Personal clave de TI	• Roles clave definidos • Minimizar dependencia del staff		
30	PO4.14 Políticas y procedimientos para el personal contratado	• Conocimiento y cumplimiento de políticas • Activos de información protegidos		• *6.1.5 Acuerdos de confidencialidad* • *6.2.1 Identificación de riesgos relacionados con terceros* • *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *9.1.5 Trabajo en áreas seguras* • *15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información*
31	PO4.15 Relaciones	• Coordinación óptima • Comunicaciones y coordinación	• *SD 4.2.5.9 Desarrollar contratos y relaciones*	• *6.1.6 Relación con las autoridades* • *6.1.7 Relación con grupos de interés especial*
32	PO5.1 Marco de trabajo para la gestión financiera	• Gestión de portafolio • Gestión de inversiones y costos de los activos de TI	• *SS 3.1 Creación de valor* • *SS 5.1 Gestión financiera* • *SS 5.2 Retorno sobre la inversión* • *SS Apéndice A Valor presente de una anualidad*	
33	PO5.2 Priorización dentro del presupuesto de TI	• Asignación de recursos de TI • Optimización del ROI	• *SS 5.2 Retorno sobre la inversión* • *SS 5.3 Gestión del portafolio de servicios* • *SS 5.4 Métodos de gestión del portafolio de servicios*	
34	PO5.3 Proceso presupuestal	• Proceso presupuestal • Asegurar que el presupuesto esté alineado con el portafolio de inversiones de programas y servicios • Revisión y aprobación del presupuesto	• **SS 5.2 Retorno sobre la inversión**	• *5.1.2 Revisión de la política de seguridad de la información*
35	PO5.4 Gestión de costos de TI	• Comparación de costos con el presupuesto	• **SS 5.1 Gestión financiera (esp.**	• *5.1.2 Revisión de la política de seguridad*

		• Reporte de costos • Remediación de las desviaciones de costos respecto del plan	**5.1.2.7)**	*de la información* • *13.2.2 Aprendiendo de los incidentes de seguridad de información*
36	PO5.5 Gestión de beneficios	• Monitoreo y análisis de beneficios • Mejora de la contribución de TI • Mantenimiento de los casos de negocio	• *SS 2.2 ¿Qué son los servicios?* • *SS 5.1 Gestión financiera* • *SS 5.2 Retorno sobre la inversión* • *ST 4.4.5.10 Revisar y cerrar la transición del servicio* • *ST 4.4.5.8 Soporte temprano*	
37	PO6.1 Política y entorno de control de TI	• Filosofía de gestión y estilo de operación • Integridad, ética, competencias, rendir cuentas y responsabilidad • Cultura de entrega de valor y gestión de riesgos	• *SS 6.4 Cultura organizacional*	• *5.1.1 Documento de la política de seguridad de la información* • *13.2.1 Responsabilidades y procedimientos*
38	PO6.2 Riesgo corporativo y marco de referencia del control interno de TI	• Promulgar y controlar las políticas • Alineamiento con el control y el riesgo de la empresa		• **5.1.1 Documento de la política de seguridad de la información** • **6.2.2 Considerar la seguridad al tratar con los clientes** • **7.1.3 Uso aceptable de activos** • **8.2.2 Educación, entrenamiento y concientización en seguridad de información** • **8.3.2 Devolución de activos** • **9.1.5 Trabajo en áreas seguras** • **9.2.7 Eliminar la propiedad** • **10.7.3 Procedimientos para el manejo de la información** • **10.8.1 Políticas y procedimientos**

				para el intercambio de información • **10.9.3 Información de dominio público** • **11.1.1 Políticas de control de acceso** • **11.3.1 Uso de contraseñas** • **11.3.2 Equipos desatendidos de usuario** • **11.3.3 Políticas de escritorios y pantallas limpias** • **11.7.1 Computación móvil y las comunicaciones** • **11.7.2 Teletrabajo** • **12.3.1 Políticas de uso de controles criptográficos** • **15.1.2 Derechos de propiedad intelectual** • **15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información** • **15.2.1 Cumplimiento con políticas y estándares de seguridad**
39	PO6.3 Gestión de políticas de TI	• Creación de políticas • Política propuesta, roles y responsabilidades		• *5.1.1 Documento de la política de seguridad de la información* • *5.1.2 Revisión de la política de seguridad de la información* • *6.1.1 Compromiso de la gerencia con la seguridad de la información* • *8.1.1 Roles y responsabilidades*
41	PO6.4 Implantación de políticas, estándares y	• Distribución y aplicación de las políticas al staff		• *6.1.1 Compromiso de la gerencia con la seguridad de la*

	procedimientos			*información* • *6.1.8 Revisión independiente de la seguridad de la información* • *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
42	PO6.5 Comunicación de los objetivos y de la dirección de TI	• Conciencia y comprensión de los objetivos de TI y del negocio	• *ST 5.1 Gestión de las comunicaciones y el compromiso* • *SO 3.6 Comunicaciones*	• *5.1.1 Documento de la política de seguridad de la información* • *6.1.1 Compromiso de la gerencia con la seguridad de la información* • *6.1.2 Coordinación para la seguridad de la información*
43	PO7.1 Reclutamiento y retención del personal	• Una política corporativa basada en prácticas de reclutamiento y promoción del personal • Habilidades mapeadas hacia los objetivos organizacionales		• *8.1.1 Roles y responsabilidades* • *8.1.2 Verificación* • *8.1.3 Términos y condiciones del empleo*
44	PO7.2 Competencias del personal	• Definición de las competencias básicas • Verificación de competencias		• *8.1.1 Roles y responsabilidades* • *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
45	PO7.3 Asignación de roles	• Roles y responsabilidades definidas • Nivel de supervisión adecuado		• *8.1.1 Roles y responsabilidades* • *8.1.3 Términos y condiciones del empleo* • *8.2.1 Responsabilidades de la Gerencia*
46	PO7.4 Entrenamiento del personal de TI	• Inducción organizacional y entrenamiento continuo para elevar los niveles de habilidad técnica y gerencial	• *SD 6.3 Habilidades y atributos*	• *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
47	PO7.5 Dependencia	• Abordar la disponibilidad de recursos para las		

	de individuos	funciones clave • Captura del conocimiento • Plan de sucesión		
48	PO7.6 Verificación de antecedentes del personal	• Acreditaciones de seguridad según la criticidad de la posición		• *8.1.2 Verificación*
49	PO7.7 Evaluación del desempeño del empleado	• Evaluación del desempeño reforzada por un sistema de recompensas		• *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
50	PO7.8 Cambios y ceses en los puestos de trabajo	• Transferencia y reasignación del conocimiento a fin de minimizar riesgos		• *8.2.3 Procesos disciplinarios* • *8.3.1 Responsabilidades en el cese* • *8.3.2 Devolución de activos* • *8.3.3 Eliminación de privilegios de acceso*
51	PO8.1 Sistema de administración de calidad	• Enfoque estándar alineado a los requisitos del negocio que cubren los requisitos y criterios de calidad • Las políticas y los métodos para detectar y corregir casos de no conformidades de calidad	• *SS 7.5 Estrategia y mejora* • *ST 4.4.5.3 Construcción y pruebas*	
52	PO8.2 Estándares y prácticas de calidad	• Estándares y procedimientos para implementar un sistema de gestión de calidad	• *SS 7.5 Estrategia y mejora* • *ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado* • *ST 4.5 Validación del servicio y pruebas (ITIL se enfoca en la transición y en las pruebas continuas del servicio)* • *CSI Apéndice A Guía complementaria*	
52	PO8.3 Estándares para desarrollos y adquisiciones	• Estándares del ciclo de vida para entregables	• *SS 6.5 Estrategia de sourcing* • *SD 3.5 Actividades de diseño* • *SD 3.6 Aspectos de diseño* • *SD 3.9 Arquitectura orientada al servicio* • *SD 3.11 Modelos para el diseño de los servicios* • *SD 5.3 Gestión de aplicaciones*	• **6.1.5 Acuerdos de confidencialidad** • **6.2.3 Considerar la seguridad en los acuerdos con terceros** • **12.5.5 Outsourcing de desarrollo de software**

			• *SD 7 Consideraciones tecnológicas* • *ST 3.2.3 Adopción de estándares y de un marco de trabajo común* • *ST 4.1.4 Políticas, principios y conceptos básicos* • *ST 4.1.5.1 Estrategia de transición*	
53	PO8.4 Enfoque en el cliente de TI	• Sistema de gestión de la calidad orientado al cliente • Roles y responsabilidades para la resolución de conflictos	• **SS 5.5 Gestión de la demanda** • **SD 4.2.5.4 Comparar, medir y mejorar la satisfacción del cliente** • **ST 3.2.6 Establecer y mantener relaciones con los interesados**	
54	PO8.5 Mejora continua	• Los procesos de comunicación promueven la mejora continua	• **SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio** • **SO 5.14 Mejora de las actividades operativas** • **CSI 1 Introducción a la mejora continua del servicio (CSI)** • **CSI 2 Gestión del servicio como una práctica** • **CSI 3 Principios de CSI** • **CSI 4.1 El proceso de mejora de los siete pasos** • **CSI 4.1.1 Integración con el resto de etapas del ciclo de vida y los procesos de gestión de servicio** • **CSI 4.4 Retorno sobre la inversión debido al CSI** • **CSI 4.5 Aspectos del negocio en CSI** • **CSI 5 Métodos y técnicas en CSI** • **CSI 5.1 Métodos y técnicas** • **CSI 5.5 El ciclo Deming** • **CSI 5.6 CSI y otros procesos de gestión del servicio** • **CSI 5.7 Resumen** • **CSI 6 Organización para la mejora continua del servicio** • **CSI 8 Implementar la mejora continua del**	

			servicio • **CSI 9 Desafíos, factores críticos de éxito y riesgos**	
55	PO8.6 Medición, monitoreo y revisión de la calidad	• Monitoreo del cumplimiento con el sistema de gestión de calidad; valor del sistema de gestión de calidad	• **CSI 5.2 Evaluaciones** • **CSI 5.3 Benchmarking** • **CSI 5.4 Marcos de medición y reporte**	
56	PO9.1 Marco de trabajo de gestión de riesgos	• Alineamiento al marco de riesgo empresarial	• *SS 9.5 Riesgos* • *SD 4.5.5.1 Etapa 1 – Inicio*	• **14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio** • **14.1.2 Continuidad del negocio y evaluación de riesgos**
57	PO9.2 Establecimiento del contexto del riesgo	• Contextos interno y externo; metas de cada evaluación	• *SS 9.5 Riesgos* • *SD 4.5.5.1 Etapa 1 – Inicio* • *SD 4.5.5.2 Etapa 2 – Requisitos y estrategia*	• **14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio** • **14.1.2 Continuidad del negocio y evaluación de riesgos**
58	PO9.3 Identificación de eventos	• Amenazas importantes que exploten vulnerabilidades tienen impacto negativo en el negocio • Registro de riesgos	• *SS 9.5 Riesgos* • *SD 4.5.5.2 Etapa 2 – Requisitos y estrategia* • *ST 9 Desafíos, factores críticos de éxito y riesgos* • *CSI 5.6.3 Gestión de continuidad de servicios de TI*	• **13.1.1 Reporte de eventos de seguridad de información** • **13.1.2 Reporte de debilidades de seguridad**
59	PO9.4 Evaluación de riesgos de TI	• Probabilidad e impacto de todos los riesgos identificados • Evaluación cualitativa y cuantitativa • Riesgos residual e inherente	• *SS 9.5 Riesgos* • *SD 4.5.5.2 Etapa 2 – Requisitos y estrategia* • *SD 8.1 Análisis de impacto en el negocio (sin detalle)* • *ST 4.6 Evaluación*	• **5.1.2 Revisión de la política de seguridad de la información** • **14.1.2 Continuidad del negocio y evaluación de riesgos**
60	PO9.5 Respuesta a los riesgos	• Controles económicamente efectivos que mitiguen la exposición • Estrategias de gestión del riesgo en términos de evitar, mitigar o aceptar	• *SS 9.5 Riesgos* • *SD 4.5.5.3 Etapa 3- Implementación* • *ST 4.6 Evaluación*	

61	PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos	• Priorización y planeamiento de las respuestas al riesgo • Costos, beneficios y responsabilidades • Monitoreo de desviaciones	• *SS 9.5 Riesgos* • *SD 4.5.5.4 Etapa 4 – Operación continua*	
62	PO10.1 Marco de trabajo para la gestión de programas	• Identificar, definir, evaluar, priorizar, seleccionar, iniciar, gestionar y controlar todos los programas de inversión de los proyectos • Coordinación, interdependencia, conflictos con los recursos		
63	PO10.2 Marco de trabajo para la gestión de proyectos	• Alcance y límites de la gestión de proyectos y el método a adoptarse		
64	PO10.3 Enfoque de gestión de proyectos	• Dimensionar la propuesta con el tamaño, complejidad y requerimientos de cada proyecto • Estructura de gobierno del proyecto • Patrocinadores del proyecto	• *ST 3.2 Políticas para la transición del servicio*	
65	PO10.4 Compromiso de los interesados	• Compromiso y participación de los interesados	• *ST 3.2.6 Establecer y mantener relaciones con los interesados* • *ST 3.2.12 Asegurar una participación temprana en el ciclo de vida del servicio*	
66	PO10.5 Declaración de alcance del proyecto	• Aprobación de la naturaleza y el alcance del proyecto	• *SD 3.4 Identificar y documentar los requerimientos y drivers del negocio* • *SD 3.5 Actividades de diseño*	
67	PO10.6 Inicio de las fases del proyecto	• Aprobación del inicio de cada etapa • Programar decisiones de gobierno		
68	PO10.7 Plan integrado del proyecto	• Plan integrado que cubra el negocio y los recursos de TI • Actividades e interdependencias entre proyectos	• *SD Apéndice D Diseñar y planificar documentos y sus contenidos*	
69	PO10.8 Recursos del proyecto	• Responsabilidades, relaciones, autoridades y criterios de desempeño del		

		equipo de proyecto • Planificación de aprovisionamiento de recursos		
70	PO10.9 Gestión de riesgos del proyecto	• Proceso sistemático para planificar, indentificar, analizar, monitorear, controlar y responder ante riesgos		
71	PO10.10 Plan de calidad del proyecto	• Plan y sistema de gestión de calidad definidos y consensuados		
72	PO10.11 Control de cambios del proyecto	• Sistema de control de cambios para cada proyecto (costo, cronograma, alcance, calidad)	• **ST 3.2.10 Anticipar y gestionar correcciones de curso**	
73	PO10.12 Planeamiento del proyecto y métodos de aseguramiento	• Tareas de aseguramiento requeridas para apoyar la acreditación		
74	PO10.13 Medición del desempeño, reporte y monitoreo del proyecto	• Medir el desempeño del proyecto contra criterios clave • Evaluar desviaciones, recomendar e implementar acciones correctivas		
75	PO10.14 Cierre del proyecto	• Revisión del cumplimiento de resultados y beneficios por parte de los directivos del proyecto • Comunicar acciones resaltantes y documentar lecciones aprendidas		
76	AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio	• Identificar, priorizar y especificar los requerimientos para todas las iniciativas relacionadas con los programas de inversión	• **SS 7.5 Estrategia y mejora** • **SS 8.1 Automatización del servicio** • **SD 3.2 Diseño balanceado** • **SD 3.3 Identificación de requerimientos de servicios** • **SD 3.4 Identificar y documentar los requisitos y drivers del**	• *8.2.2 Educación, entrenamiento y concientización en seguridad de información* • *12.1.1 Análisis y especificación de los requisitos de seguridad* • *10.3.2 Aceptación del sistema*

			negocio • **SD 3.5 Actividades de diseño** • **SD 3.6.1 Diseño de soluciones de servicios** • **SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios** • **SD 3.6.3 Diseño de la arquitectura tecnológica** • **SD 3.6.4 Diseño de procesos** • **SD 3.6.5 Diseño de sistemas de medición y métricas** • **SD 3.8 Limitaciones del diseño** • **SD 3.9 Arquitectura orientada al servicio** • **SD 4.3.5.8 Dimensionamiento de aplicaciones** • **SD Apéndice D Diseñar y planificar documentos y sus contenidos** • **ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio**	
77	AI 1.2 Reporte de análisis de riesgos	• Análisis de todas las amenazas significativas y vulnerabilidades potenciales que afecten los requerimientos	• *SD 2.4.2 Alcance* • *SD 3.6 Aspectos de diseño* • *SD 4.5.5.2 Etapa 2 – Requisitos y estrategia*	• *11.6.2 Aislamiento de sistemas sensitivos* • *12.1.1 Análisis y especificación de los requisitos de seguridad*
78	AI1.3 Estudio de factibilidad y formulación de cursos alternativos de acción	• Soluciones alternativas que satisfagan los requerimientos del negocio, evaluados por el negocio y por TI	• *SD 3.6.1 Diseño de soluciones de servicios* • *SD 3.7.1 Evaluación de soluciones alternativas* • *ST 3.2.4 Maximizar la reutilización de procesos y sistemas establecidos*	
79	AI1.4 Requerimientos, decisión de factibilidad y aprobación	• Aprobación de requerimientos, opciones factibles, soluciones y la propuesta de adquisición por parte del patrocinador del proyecto	• *SD 3.6.1 Diseño de soluciones de servicios*	• *6.1.4 Proceso de autorización para las instalaciones de procesamiento de información* • *10.3.2 Aceptación del sistema*
80	AI2.1 Diseño a alto nivel	• Traducción de los requerimientos del negocio a diseño de alto nivel para la	• *SD 3.6.1 Diseño de soluciones de servicios* • *SD 3.6.3 Diseño de la*	

		adquisición • Alineamiento con la dirección tecnológica y la arquitectura de información	*arquitectura tecnológica*	
81	AI2.2 Diseño detallado	• Diseño técnico y requerimientos de la aplicación • Criterio para la aceptación	• *SS 8.2 Interfaces del servicio* • *SD 4.2.5.2 Requisitos acordados y documentados de los nuevos servicios; definir los requisitos de los niveles de servicios* • *SD 5.3 Gestión de aplicaciones*	
82	AI2.3 Control y auditabilidad de las aplicaciones	• Controles de negocio con aplicaciones automatizad para procesos exactos, completos, autorizados y auditables		• **10.10.1 Logs de auditoría** • **10.10.5 Logs de fallas** • **12.2.1 Validación de datos de entrada** • **12.2.2 Control de procesamiento interno** • **12.2.3 Integridad de mensajes** • **12.2.4 Validación de datos de salida** • **13.2.3 Recolección de evidencia** • **15.3.1 Controles de auditoría de sistemas de información** • **15.3.2 Protección de herramientas de auditoría de sistemas de información**
83	AI2.4 Seguridad y disponibilidad de las aplicaciones	• Definición de requerimientos de seguridad y disponibilidad	• *SD 3.6.1 Diseño de soluciones de servicios* • *SO 4.4.5.11 Errores detectados en el entorno de desarollo*	• **6.1.4 Proceso de autorización para las instalaciones de procesamiento de información** • **7.2.1 Lineamientos para la clasificación** • **10.3.2 Aceptación del sistema** • **11.6.2 Aislamiento de**

				sistemas sensitivos • **12.1.1 Análisis y especificación de los requisitos de seguridad** • **12.2.3 Integridad de mensajes** • **12.3.1 Política de uso de controles criptográficos** • **12.4.3 Control de acceso al código fuente de los programas** • **12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo** • **12.5.4 Fuga de información** • **15.3.2 Protección de herramientas de auditoría de sistemas de información**
84	AI2.5 Configuración e implementación de software de aplicación adquirido	• Configuración de los paquetes de software adquiridos		• *12.5.3 Restricciones en los cambios a los paquetes de software*
85	AI2.6 Actualizaciones importantes en sistemas existentes	• Aplicación de procesos similares de desarrollo cuando se realicen cambios mayores		• *12.5.1 Procedimientos de control de cambios*
86	AI2.7 Desarrollo de software aplicativo	• Desarrollar funcionalidad según diseño, estándares y requisitos de aseguramiento de calidad • Requisitos legales y contractuales seguidos por desarrolladores de los proveedores	• *SD 3.7.3 Desarrollar la solución del* *servicio*	• *12.5.5 Outsourcing de desarrollo de software*
87	AI2.8 Aseguramiento de la calidad del software	• Política y plan de aseguramiento de calidad (QA).		• *10.3.2 Aceptación del sistema*
88	AI2.9 Gestión de los requisitos de las	• Seguimiento de todos los requerimientos a	• *ST 3.2.6 Establecer y mantener relaciones con los interesados*	

	aplicaciones	través del proceso de gestión de cambios	• *ST 3.2.10 Anticipar y gestionar correcciones de curso*	
89	AI2.10 Mantenimiento del software aplicativo	• Estrategia y plan para el mantenimiento del software		
90	AI3.1 Plan de adquisición de infraestructura tecnológica	• Plan de adquisición, implementación y mantenimiento para la infraestructura, en línea con las necesidades del negocio y la dirección tecnológica	• *SD 3.6.3 Diseño de la arquitectura tecnológica*	
91	AI3.2 Protección y disponibilidad de la infraestructura	• Protección de recursos utilizando mediciones de seguridad y auditablidad • Uso de infraestructura sensitiva	• *SD 4.6.5.1 Controles de seguridad* • *SO 5.4 Gestión y soporte de servidores*	• *12.1.1 Análisis y especificación de los requisitos de seguridad*
92	AI3.3 Mantenimiento de la infraestructura	• Control de cambios, gestión de parches ,estrategias de actualización y requerimientos de seguridad	• **SO 5.4 Gestión y soporte de servidores** • **SO 5.5 Gestión de redes** • **SO 5.7 Administración de bases de datos** • **SO 5.8 Gestión de servicios de directorio** • **SO 5.9 Soporte de estaciones de trabajo** • **SO 5.10 Gestión de middleware** • **SO 5.11 Gestión Internet/web**	• *9.1.5 Trabajo en áreas seguras* • *9.2.4 Mantenimiento de equipos* • *12.4.2 Protección de los datos de prueba de sistema* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo* • *12.6.1 Control de vulnerabilidades técnicas*
93	AI3.4 Ambiente de prueba de factibilidad	• Entornos de desarrollo y pruebas; pruebas de factibilidad e integración	• *ST 4.4.5.1 Planificación* • *ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue* • *ST 4.4.5.3 Construcción y pruebas* • *ST 4.5.5.7 Limpieza y cierre de las pruebas* • *ST 4.5.7 Gestión de información*	• *10.1.4 Separación de los entornos de desarrollo, pruebas y producción*
94	AI4.1 Planificación de soluciones operacionales	• Identificación y planificación de todos los aspectos técnicos, operacionales y de uso de la solución	• **SD 3.6.1 Diseño de soluciones de servicios** • **ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio** • **ST 3.2.9 Planificar la**	

			liberación y el despliegue de paquetes • **ST 4.4.5.1 Planificación** • **ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue** • **ST 4.4.5.5 Planificar y preparar el despliegue**	
95	AI4.2 Transferencia de conocimiento a la gestión del negocio	• Facilitar la propiedad, entrega, calidad y el control interno de la solución	• *ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio* • *ST 4.7 Gestión del conocimiento*	
96	AI4.3 Transferencia de conocimiento a los usuarios finales	• Conocimiento y habilidades del usuario final como parte del proceso de negocio	• **ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones** • **ST 4.4.5.8 Soporte temprano** • **ST 4.7 Gestión del conocimiento**	
97	AI4.4 Transferencia de conocimiento al personal de operaciones y soporte	• Conocimiento y habilidades para facilitar la operación y el soporte de los sistemas y la infraestructura	• **ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones** • **ST 4.4.5.5 Planificar y preparar el despliegue** • **ST 3.7 Documentación** • **ST 4.4.5.11 Errores detectados en el entorno de desarrollo** • **SO 4.6.6 Gestión de conocimiento (actividades operativas)**	• *10.1.1 Procedimientos operativos documentados* • *10.3.2 Aceptación del sistema* • *10.7.4 Seguridad de la documentación de sistemas* • *13.2.2 Aprendiendo de los incidentes de seguridad de información*
98	AI5.1 Control de adquisiciones	• Estándares y procedimientos alineados con el proceso de adquisiciones de la empresa	• *SD 3.7.2 Adquisición de la solución elegida*	• *6.1.5 Acuerdos de confidencialidad*
99	AI5.2 Gestión de contratos de proveedores	• Inicio de contrato y gestión del ciclo de vida	• *SD 4.2.5.9 Desarrollar contratos y relaciones* • *SD 4.7.5.3 Nuevos proveedores y contratos*	• *6.1.5 Acuerdos de confidencialidad* • *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *10.8.2 Acuerdos de intercambio* • *12.5.5 Outsourcing de desarrollo de software*
100	AI5.3 Selección de proveedores	• Proceso de selección justo y formal • Mejor ajuste viable	• **SD 3.7.1 Evaluación de soluciones alternativas**	

		de los requerimientos	• **SD 4.7.5.3 Nuevos proveedores y contratos** • **SD Apéndice I Ejemplo de una declaración de requerimiento y/o una invitación a ofertar**	
	AI5.4 Adquisición de recursos TI	• Protección de los intereses de la empresa en los contratos • Derechos y obligaciones de todas las partes	• **SD 3.7.2 Adquisición de la solución elegida.**	
101	AI6.1 Estándares y procedimientos para cambios	• Procedimientos formales de gestión de cambios • Enfoque estandarizado	• **SD 3.2 Diseño balanceado** • **SD 3.7 Actividades subsiguientes del diseño** • **ST 3.2 Políticas para la transición del servicio** • **ST 3.2.1 Definir e implementar una política formal para la transición del servicio** • **ST 3.2.2 Implementar todos los cambios a los servicios a través de la transición del servicio** • **ST 3.2.7 Establecer controles y disciplinas eficaces** • **ST 4.1 Planificación y soporte para la transición** • **ST 4.1.4 Políticas, principios y conceptos básicos** • **ST 4.2 Gestión de cambios**	• *10.1.2 Gestión de cambios* • *12.5.3 Restricciones en los cambios a los paquetes de software*
102	AI6.1 Estándares y procedimientos para cambios (cont.)		• **ST 4.2.6.1 Procedimiento de cambio normal** • **ST 5 Actividades comunes de operación en la transición del servicio** • **ST 6 Organización para la transición del servicio** • **ST 6.3 Modelos organizacionales para apoyar la transición de servicios** • **ST 6.4 Relación de la transición del servicio con otras etapas del ciclo de vida** • **SO 4.6.1 Gestión de cambios (actividades**	

			operativas)	
103	AI6.2 Evaluación de impacto, priorización y autorización	• Evaluar impacto, categorizar, priorizar y autorizar	• **ST 4.2.6.2 Crear y registrar la solicitud de cambio** • **ST 4.2.6.3 Revisar la solicitud de cambio** • **ST 4.2.6.4 Valorar y evaluar el cambio** • **ST 4.2.6.5 Autorizar el cambio** • **ST 4.2.6.6 Coordinar la implementación del cambio** • **ST 4.2.6.8 Consejo consultivo de cambios** • **ST 4.6 Evaluación** • **SO 4.3.5.1 Selección por menú** • **SO 4.3.5.2 Aprobación financiera** • **SO 4.3.5.3 Otras aprobaciones**	• *10.1.2 Gestión de cambios* • *12.5.1 Procedimientos de control de cambios* • *12.5.3 Restricciones en los cambios a los paquetes de software* • *12.6.1 Control de vulnerabilidades técnicas*
104	AI6.3 Cambios de emergencia	• Proceso para definir, escalar, probar, documentar, evaluar y autorizar cambios de emergencia	• **ST 4.2.6.9 Cambios de emergencia**	• *10.1.2 Gestión de cambios* • *11.5.4 Uso de utilitarios del sistema* • *12.5.1 Procedimiento de control de cambios* • *12.5.3 Restricciones en los cambios a los paquetes de software* • *12.6.1 Control de vulnerabilidades técnicas*
105	AI6.4 Seguimiento y reporte de estado de los cambios	• Seguimiento y reporte de todos los cambios (rechazados, aprobados, en curso y concluidos)	• **ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado** • **ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio** • **ST 4.1.5.3 Planificar y coordinar la transición del servicio** • **ST 4.1.6 Brindar soporte al proceso de transición**	• *10.1.2 Gestión de cambios*
106	AI6.5 Cierre y documentación del cambio	• Implementación de cambios y actualizaciones de la documentación	• **ST 4.2.6.4 Valorar y evaluar el cambio** • **ST 4.2.6.7 Revisar y cerrar el registro del cambio** • **ST 4.4.5.10 Revisar y cerrar la transición del servicio** • **ST 4.4.5.9 Revisar y**	• *10.1.2 Gestión de cambios*

			cerrar un despliegue • **SO 4.3.5.5 Cierre**	
107	AI7.1 Entrenamiento	• Entrenamiento de usuarios en operaciones de acuerdo con el plan de implementación	• **ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue**	• *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
108	AI7.2 Plan de pruebas	• Plan de prueba con definición de roles y responsabilidades	• **ST 4.5.5.1 Gestión de pruebas y validación** • **ST 4.5.5.2 Planificar y diseñar pruebas** • **ST 4.5.5.3 Verificar el plan y el diseño de pruebas** • **ST 4.5.5.4 Preparar el entorno de pruebas**	• *12.5.1 Procedimientos de control de cambios* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo*
109	AI7.3 Plan de implementación	• Plan de implementación que incluye estrategias de retirada y retroceso	• **ST 3.2.9 Planificar la liberación y el despliegue de paquetes** • **ST 4.1.5.2 Preparación para la transición del servicio** • **ST 4.4.5.2 Preparación para la contrucción, pruebas y despliegue** • **ST 4.4.5.3 Construcción y pruebas** • **ST 4.4.5.4 Pruebas y pilotos del servicio** • **ST 4.4.5.5 Planificar y preparar el despliegue**	
110	AI7.4 Ambiente de prueba	• Ambientes de prueba seguros, basados en condiciones de operación	• *ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio* • *ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue* • *ST 4.4.5.3 Construcción y pruebas* • *ST 4.4.5.4 Pruebas y pilotos del servicio*	• *10.1.4 Separación de los entornos de desarrollo, pruebas y producción* • *12.4.3 Control de acceso al código fuente de los programas* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo*
111	AI7.5 Conversión de datos y sistemas	• Conversión de datos y migración de infraestructura		
112	AI7.6 Pruebas de cambios	• Pruebas independientes de los cambios previas a la migración	• *ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio* • *ST 4.4.5.4 Pruebas y pilotos del servicio* • *ST 4.5.5.5 Ejecutar pruebas* • *ST 4.5.5.6 Evaluar*	• *6.1.4 Proceso de autorización para las instalaciones de procesamiento de información* • *12.4.3 Control de acceso al código fuente de los programas*

			criterios de fin de pruebas y reportar	• *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo*
113	AI7.7 Pruebas de aceptación final	• Los dueños de los procesos de negocios y los interesados evalúan los resultados de las pruebas	• *ST 4.4.5.4 Pruebas y pilotos del servicio* • *ST 4.5.5.5 Ejecutar pruebas* • *ST 4.5.5.6 Evaluar criterios de salida y reportar*	• *10.3.2 Aceptación del sistema* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo* • *12.5.4 Fuga de información*
114	AI7.8 Promoción a producción	• Traspaso controlado a operaciones, distribución de software, procesamiento paralelo	• **ST 4.4.5.5 Planificar y preparar el despliegue** • **ST 4.4.5.6 Realizar transferencia, despliegue y retiros** • **SO 4.3.5.4 Cumplimiento**	
115	AI7.9 Revisión posterior a la implementación	• Evaluar si se lograron los objetivos y beneficios • Plan de acción para abordar los problemas	• **ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado** • **ST 4.1.5.3 Planear y coordinar la transición del servicio** • **ST 4.4.5.10 Revisar y cerrar la transición del servicio** • **ST 4.4.5.7 Verificar despliegue** • **ST 4.4.5.9 Revisar y cerrar un despliegue** • **ST 4.6 Evaluación** • **SO 4.3.5.5 Cierre**	
116	DS1 Marco de gestión de niveles de servicio	• Proceso formal de gestión de niveles de servicio y alineación continua con los requerimientos del negocio • Facilitar el entendimiento común entre el cliente y el proveedor	• **SS 2.6 Funciones y procesos a través del ciclo de vida** • **SS 4.3 Desarrollar activos estratégicos** • **SS 4.4 Preparar la ejecución** • **SS 7.2 Estrategia y diseño** • **SS 7.3 Estrategia y transiciones** • **SS 7.5 Estrategia y mejora** • **SD 4.2.5.1 Diseñar marcos ANS** • **SD 4.2.5.9 Desarrollar contratos y relaciones**	• *10.2.1 Entrega de servicios*
117	DS1.2 Definiciones de los servicios	• Servicios definidos basados en las características del servicio y los requerimientos del negocio en un	• **SS 4.2 Desarrollar las ofertas** • **SS 4.3 Desarrollar activos estratégicos** • **SS 5.4 Métodos de gestión del portafolio**	• *10.2.1 Entrega de servicios*

		catálogo de servicios	**de servicios** • **SS 5.5 Gestión de la demanda** • **SS 7.2 Estrategia y diseño** • **SS 7.3 Estrategia y transiciones** • **SS 7.4 Estrategia y operaciones** • **SS 7.5 Estrategia y mejora** • **SS 8.2 Interfaces del servicio** • **SD 3 Principios de diseño de servicio** • **SD 3.1 Metas** • **SD 3.2 Diseño balanceado** • **SD 3.4 Identificar y documentar los requisitos y drivers del negocio** • **SD 3.5 Actividades de diseño** • **SD 3.6 Aspectos de diseño** • **SD 4.1 Gestión del catálogo de servicios**	
118	DS1.3 Acuerdos de niveles de servicio (ANS)	• Definir los ANS basándose en los requerimientos del cliente y las capacidades de TI • Métricas, roles y responsabilidades de los servicios	• **SD 4.2.5.2 Requisitos acordados y documentados de los nuevos servicios; definir los requisitos de los niveles de servicios** • **SD Apéndice F Ejemplos de ANS y Acuerdos de niveles de operación**	• *10.2.1 Entrega de servicios*
119	DS1.4 Acuerdos de niveles de operación	• Definición de la entrega técnica para soportar los ANS	• **SD 4.2.5.5 Examinar y revisar los acuerdos suscritos y el alcance del servicio** • **SD Apéndice F Ejemplos de ANS y Acuerdos de niveles de operación**	
120	DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	• Monitoreo continuo del desempeño del servicio	• **SS 5.3 Gestión del portafolio de servicios** • **SD 4.2.5.3 Monitorear el desempeño del servicio contra el ANS** • **SD 4.2.5.6 Generar reportes del servicio** • **SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio**	• *10.2.2 Monitoreo y revisión de los servicios de terceros* • *10.2.3 Gestión de cambios a los servicios de terceros*

			• **SD 4.2.5.10 Reclamos y reconocimientos** • **SD 4.3.8 Gestión de la información** • **CSI 4.2 Reportes del servicio** • **CSI 4.3 Mediciones del servicio**	
121	DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos	• Revisión periódica de los ANS y mejorar los contratos para mayor efectividad y vigencia	• **SD 4.2.5.4 Comparar, medir y mejorar la satisfacción del cliente** • **SD 4.2.5.5 Examinar y revisar los acuerdos suscritos y el alcance del servicio** • **SD 4.2.5.8 Examinar y revisar los ANS, alcance del servicio y los acuerdos suscritos**	
122	DS2.1 Identificación de todas las relaciones con proveedores	• Categorizar los servicios según el tipo de proveedor, significancia y criticidad	• **SS 7.3 Estrategia y transiciones** • **SD 4.7.5.1 Evaluación de nuevos proveedores y contratos**	• *6.2.1 Identificación de riesgos relacionados con terceros*
123	DS2.2 Gestión de relaciones con proveedores	• Enlace respecto a temas del cliente y el proveedor • Confianza y transparencia	• **SD 4.2.5.9 Desarrollar contratos y relaciones** • **SD 4.7.5.2 Clasificación de proveedores y mantenimiento de la base de datos de proveedores y contratos** • **SD 4.7.5.4 Gestión y desempeño de proveedores y contratos** • **SD 4.7.5.5 Renovación y/o término de contratos**	• *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *10.2.3 Gestión de cambios a los servicios de terceros* • *15.1.4 Protección de datos y privacidad de la información personal*
124	DS2.3 Gestión de riesgos de proveedores	• Identificación de riesgo, conformidad contractual y viabilidad de proveedores	• **SD 4.7.5.3 Nuevos proveedores y contratos** • **SD 4.7.5.5 Renovación y/o término de contratos**	• *6.2.1 Identificación de riesgos relacionados con terceros* • *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *8.1.2 Verificación* • *8.1.3 Términos y condiciones del empleo* • *10.2.3 Gestión de cambios a los servicios de terceros* • *10.8.2 Acuerdos de intercambio*
125	DS2.4 Monitoreo del desempeño de	• Satisfacer los requerimientos del	• **SD 4.7.5.4 Gestión y desempeño de**	• *6.2.3 Considerar la seguridad en los*

	proveedores	negocio, adhesión a los contratos y desempeño competitivo	**proveedores y contratos**	*acuerdos con terceros* • *10.2.1 Entrega de servicios* • *10.2.2 Monitoreo y revisión de los servicios de terceros* • *12.4.2 Protección de los datos de prueba del sistema* • *12.5.5 Outsourcing de desarrollo de software*
126	DS3.1 Planeamiento del desempeño y la capacidad	• Asegurar que las capacidades y los desempeños cumplen con los ANS	• **SD 4.3.5.1 Gestión de la capacidad para el negocio** • **SD Apéndice J Contenido típico de un plan de capacidad** • **CSI 5.6.2 Gestión de la capacidad**	• *10.3.1 Gestión de la capacidad*
127	DS3.2 Capacidad y desempeño actual	• Evaluación de los desempeños y capacidades actuales	• **SD 4.3.5.2 Gestión de la capacidad del servicio** • **SD 4.3.5.3 Gestión de la capacidad de los componentes** • **SO 4.1.5.2 Notificación de eventos** • **SO 4.1.5.3 Detección de eventos** • **SO 5.4 Gestión y soporte de servidores** • **CSI 4.3 Mediciones del servicio**	• *10.3.1 Gestión de la capacidad*
128	DS3.3 Capacidad y desempeño futuro	• Pronóstico de requerimientos de recursos • Tendencias de las cargas de trabajo	• **SD 4.3.5.1 Gestión de la capacidad para el negocio** • **SD 4.3.5.2 Gestión de la capacidad del servicio** • **SD 4.3.5.3 Gestión de la capacidad de los componentes** • **SD 4.3.5.7 Modelamiento y tendencias** • **SD 4.3.8 Gestión de la información**	• *10.3.1 Gestión de la capacidad*
129	DS3.4 Disponibilidad de recursos de TI	• Provisión de recursos, contingencias, tolerancia a fallas y priorización de recursos	• **SD 4.3.5.3 Gestión de la capacidad de los componentes** • **SD 4.3.5.4 Actividades de soporte de la gestión de capacidad** • **SD 4.4 Gestión de la disponibilidad** • **SD 4.4.5.1 Actividades**	

			reactivas de la gestión de la disponibilidad • **SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad** • **SO 4.6.5 Gestión de la disponibilidad (actividades operativas)** • **CSI 5.6.1 Gestión de la disponibilidad**	
130	DS3.5 *Monitoreo* y reporte	• Mantenimiento y afinamiento de performance y capacidad; reporte de la disponibilidad de servicio al negocio	• **SD 4.3.5.4 Actividades de soporte de la gestión de la capacidad** • **SD 4.3.5.5 Gestión y control de umbrales** • **SD 4.3.5.6 Gestión de la demanda** • **SD 4.4.5.1 Actividades reactivas de la gestión de la disponibilidad**	
131	DS4.1 Marco de trabajo de continuidad de TI	• Enfoque consistente y corporativo a la gestión de continuidad	• *SD 4.5 Gestión de continuidad de servicios de TI* • *SD 4.5.5.1 Etapa 1 – Inicio* • *CSI 5.6.3 Gestión de continuidad de servicios de TI*	• **6.1.6 Relación con las autoridades** • **6.1.7 Relación con grupos de interés especial** • **14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio** • **14.1.2 Continuidad del negocio y evaluación de riesgos** • **14.1.4 Marco de planificación de continuidad del negocio**
132	DS4.2 Planes de continuidad de TI	• Planes individuales de continuidad • Análisis de impacto en el negocio • Resiliencia, procesamiento alternativo y recuperación	• **SD 4.5.5.2 Etapa 2 – Requisitos y estrategia** • **SD 4.5.5.3 Etapa 3 – Implementación** • **SD Apéndice K Contenido típico de un plan de recuperación**	• *6.1.6 Relación con las autoridades* • *6.1.7 Relación con grupos de interés especial* • *14.1.3 Desarrollar e implementar planes de continuidad que incluyan la seguridad de la información*
133	DS4.3 Recursos críticos de TI	• Centrarse en la infraestructura crítica, resiliencia y priorización	• *SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad* • *SD 4.5.5.4 Etapa 4 –*	• *14.1.1 Incluir la seguridad de información en el proceso de*

		• Respuesta para diferentes períodos de tiempo	*Operación continua*	*gestión de continuidad del negocio* • *14.1.2 Continuidad del negocio y evaluación de riesgos*
134	DS4.4 Mantenimiento del plan de continuidad de TI	• Control de cambios para reflejar los requerimientos cambiantes del negocio	**• SD 4.5.5.4 Etapa 4 – Operación** **continua**	**• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio**
135	DS4.5 Pruebas del plan de continuidad de TI	• Pruebas regulares • Implementación del plan de acción	• **SD 4.5.5.3 Etapa 3 – Implementación** • **SD 4.5.5.4 Etapa 4 – Operación continua**	**• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio**
136	DS4.6 Entrenamiento en el plan de continuidad de TI	• Entrenamiento regular para todas las partes involucradas	• **SD 4.5.5.3 Etapa 3 – Implementación** • **SD 4.5.5.4 Etapa 4 – Operación continua**	**• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio**
137	DS4.7 Distribución del plan de continuidad de TI	• Distribución segura y adecuada a todas las partes autorizadas	• **SD 4.5.5.3 Etapa 3 – Implementación** • **SD 4.5.5.4 Etapa 4 – Operación continua**	**• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio**
138	DS4.8 Recuperación y reanudación de los servicios de TI	• Planificación del período cuando TI se esté recuperando y reanudando servicios • Entendimiento del negocio y soporte a la inversión	• **SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad** • **SD 4.5.5.4 Etapa 4 – Operación continua**	• *14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio* • *14.1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la información*
139	DS4.9 Almacenamiento externo de respaldos	• Almacenamiento externo de los medios críticos; documentación y recursos necesarios, en colaboración con los dueños de los procesos de negocio	• **SD 4.5.5.2 Etapa 2 – Requisitos y estrategia** • **SO 5.2.3 Respaldo y restauración**	• *10.5.1 Respaldo de la información*
140	DS4.10 Revisión	• Evaluación regular de	• *SD 4.5.5.3 Etapa 3 – Implementación*	• *14.1.5 Pruebas,*

	postreanudación	los planes	• *SD 4.5.5.4 Etapa 4 – Operación continua*	*mantenimiento y revaluación de los planes de continuidad del negocio*
141	DS5.1 Gestión de la seguridad de TI	• Ubicar la gestión de seguridad a alto nivel para cumplir con las necesidades del negocio	• *SD 4.6 Gestión de seguridad de la información* • *SO 5.13 Gestión de seguridad de la información y la operación del servicio*	• **6.1.1 Compromiso de la gerencia con la seguridad de la información** • **6.1.2 Coordinación para la seguridad de la información** • **6.2.3 Considerar la seguridad en los acuerdos con terceros** • **8.2.2 Educación, entrenamiento y concientización en seguridad de información**
142	DS5.2 Plan de Seguridad de TI	• Traducción de requerimientos de negocio, riesgo y cumplimiento en un plan de seguridad	• *SD 4.6.4 Políticas, principios y conceptos básicos* • *SD 4.6.5.1 Controles de seguridad (cobertura a alto nivel, sin detalle)*	• **5.1.1 Documento de la política de seguridad de la información** • **5.1.2 Revisión de la política de seguridad de la información • 6.1.2 Coordinación para la seguridad de la información** • **6.1.5 Acuerdos de confidencialidad** • **8.2.2 Educación, entrenamiento y concientización en seguridad de información** • **11.1.1 Políticas de control de acceso** • **11.7.1 Computación móvil y las comunicaciones** • **11.7.2 Teletrabajo**
143	DS5.3 Gestión de identidad	• Identificación de todos los usuarios (internos, externos y	• *SO 4.5 Gestión de acceso*	• **5.1.1 Documento de la política de seguridad de la información**

		temporales) y su actividad		• **5.1.2 Revisión de la política de seguridad de la información** • **6.1.2 Coordinación para la seguridad de la información** • **6.1.5 Acuerdos de confidencialidad** • **8.2.2 Educación, entrenamiento y concientización en seguridad de información** • **11.1.1 Políticas de control de acceso** • **11.7.1 Computación móvil y las comunicaciones** • **11.7.2 Teletrabajo**
144	DS5.4 Gestión de cuentas de usuario	• Gestión del ciclo de vida de las cuentas de usuario y privilegios de acceso	• *SO 4.5 Gestión de acceso* • *SO 4.5.5.1 Peticiones de acceso* • *SO 4.5.5.2 Verificación* • *SO 4.5.5.3 Habilitar privilegios* • *SO 4.5.5.4 Monitorear el estado de la identidad* • *SO 4.5.5.5 Registro y seguimiento de accesos* • *SO 4.5.5.6 Eliminar o restringir privilegios*	• **6.1.5 Acuerdos de confidencialidad** • **6.2.1 Identificación de riesgos relacionados con terceros** • **6.2.2 Considerar la seguridad al tratar con los clientes** • **8.1.1 Roles y responsabilidades** • **8.3.1 Responsabilidades en el cese** • **8.3.3 Eliminación de privilegios de acceso** • **10.1.3 Segregación de funciones** • **11.1.1 Políticas de control de acceso** • **11.2.1 Registro de usuarios** • **11.2.2 Gestión de privilegios** • **11.2.4 Revisión de derechos de acceso de usuarios** • **11.3.1 Uso de**

				contraseñas • **11.5.1 Procedimientos seguros de inicio de sesión** • **11.5.3 Sistema de gestión de contraseñas** • **11.6.1 Restricción de acceso a la información**
145	DS5.5 Pruebas, vigilancia y monitoreo de la seguridad	• Pruebas proactivas de la implementación de seguridad • Acreditación oportuna • Reporte oportuno de eventos inusuales	• *SO 4.5.5.6 Eliminar o restringir privilegios* • *SO 5.13 Gestión de seguridad de la información y la operación del servicio*	• **6.1.8 Revisión independiente de la seguridad de la información** • **10.10.2 Monitoreo del uso del sistema** • **10.10.3 Protección de logs** • **10.10.4 Logs de administrador y de operador** • **12.6.1 Control de vulnerabilidades técnicas** • **13.1.2 Reporte de debilidades de seguridad** • **15.2.2 Verificación de cumplimiento técnico** • **15.3.1 Controles de auditoría de sistemas de información**
146	DS5.6 Definición de incidente de seguridad	• Definición y clasificación de las características de los incidentes de seguridad	• **SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle)** • **SD 4.6.5.2 Gestión de brechas de seguridad e incidentes**	• **8.2.3 Procesos disciplinarios** • **13.1.1 Reporte de eventos de seguridad de información** • **13.1.2 Reporte de debilidades de seguridad** • **13.2.1 Responsabilidades y procedimientos** • **13.2.3 Recolección de evidencia**
147	DS5.7 Protección de la tecnología de seguridad	• Resistencia a la manipulación	• *SO 5.4 Gestión y soporte de servidores*	• **6.1.4 Proceso de autorización para las instalaciones de**

				procesamiento de información • **9.1.6 Áreas de acceso público, despacho y recepción** • **9.2.1 Ubicación y protección de equipos** • **9.2.3 Seguridad del cableado** • **10.6.2 Seguridad de los servicios de red** • **10.7.4 Seguridad de la documentación de sistemas** • **10.10.1 Logs de auditoría** • **10.10.3 Protección de logs** • **10.10.4 Logs de administrador y de operador** • **10.10.5 Logs de fallas** • **10.10.6 Sincronización de relojes** • **11.3.2 Equipos desatendidos de usuario** • **11.3.3 Políticas de escritorios y pantallas limpias** • **11.4.3 Identificación de equipos en redes** • **11.4.4 Protección de puertos de configuración y diagnóstico remoto**
148	DS5.7 Protección de la tecnología de seguridad (cont.)			• **11.5.1 Procedimientos seguros de inicio de sesión** • **11.5.4 Uso de utilitarios del sistema** • **11.5.5 Período de inactividad de sesión** • **11.5.6 Limitación del tiempo de conexión** • **11.6.2**

				Aislamiento de sistemas sensitivos • **11.7.1 Computación móvil y las comunicaciones** • **11.7.2 Teletrabajo** • **12.4.1 Control del software de operaciones** • **12.6.1 Control de vulnerabilidades técnicas** • **13.1.2 Reporte de debilidades de seguridad** • **13.2.3 Recolección de evidencia** • **15.2.2 Verificación de cumplimiento técnico** • **15.3.2 Protección de las herramientas de auditoría de sistemas**
149	DS5.8 Gestión de llaves criptográficas	• Gestión del ciclo de vida de llaves criptográficas		• **10.8.4 Mensajería electrónica** • **12.2.3 Integridad de mensajes** • **12.3.1 Política de uso de controles criptográficos** • **12.3.2 Gestión de llaves** • **15.1.6 Regulación de controles criptográficos**
150	DS5.9 Prevención, detección y corrección de software malicioso	• Parches de actualización, control de virus y protección de malware		• **10.4.1 Controles contra código malicioso** • **10.4.2 Controles contra código móvil**
151	DS5.10 Seguridad de la red	• Controles para autorizar acceso y flujos de información desde y hacia las redes	• *SO 5.5 Gestión de redes*	• **6.2.1 Identificación de riesgos relacionados con terceros** • **10.6.1 Controles de red** • **10.6.2 Seguridad de los servicios de red** • **11.4.1 Política de uso de los servicios de red** • **11.4.2**

				Autenticación de usuarios para conexiones externas • **11.4.3 Identificación de equipos en redes** • **11.4.4 Protección de puertos de configuración y diagnóstico remoto** • **11.4.5 Segregación en redes** • **11.4.6 Control de conexiones en la red** • **11.4.7 Control de enrutamiento en la red** • **11.6.2 Aislamiento de sistemas sensitivos**
152	DS5.11 Intercambio de datos sensitivos	• Ruta confiable y controles de autenticación, constancia de recepción y no repudio		• **6.2.1 Identificación de riesgos relacionados con terceros** • **10.6.1 Controles de red** • **10.6.2 Seguridad de los servicios de red** • **11.4.1 Política de uso de los servicios de red** • **11.4.2 Autenticación de usuarios para conexiones externas** • **11.4.3 Identificación de equipos en redes** • **11.4.4 Protección de puertos de configuración y diagnóstico remoto** • **11.4.5 Segregación en redes** • **11.4.6 Control de conexiones en la red** • **11.4.7 Control de enrutamiento en la red** • **11.6.2**

				Aislamiento de sistemas sensitivos
153	DS6.1 Definición de servicios	• Identificación de todos los costos vinculados con los servicios de TI y a los procesos asociados	• **SS 5.1 Gestión financiera** • **SD 4.1 Gestión del catálogo de servicios**	
154	DS6.2 Contabilización de TI	• Asignación de costos según el modelos de costos de la empresa	• **SS 5.1 Gestión financiera**	
155	DS6.3 Modelamiento de costos y cargos	• Modelos de costeo de TI basados en definiciones de servicio y procesos de devolución	• **SS 5.1 Gestión financiera** • **SS 7.2 Estrategia y diseño**	
156	DS6.4 Mantenimiento del modelo de costos	• Revisión regular y comparación del modelo de costo/recarga	• **SS 5.1 Gestión financiera**	
157	DS7.1 Identificación de necesidades de educación y formación	• Programa de formación para cada grupo de empleados	• *SO 5.13 Gestión de seguridad de la información y la operación del servicio* • *SO 5.14 Mejora de las actividades operativas*	• **8.2.2 Educación, entrenamiento y concientización en seguridad de información**
158	DS7.2 Brindar educación y entrenamiento	• Identificar y nombrar instructores • Cronograma de entrenamiento		• *8.2.2 Educación, entrenamiento y concientización en seguridad de información*
159	DS7.3 Evaluación del entrenamiento recibido	• Evaluar la entrega del entrenamiento y mejoras futuras		
160	DS8.1 Mesa de servicios	• Interface de usuario • Gestión de llamadas • Clasificación y priorización de incidentes basadas en servicios y ANS	• **SO 4.1 Gestión de eventos** • **SO 4.2 Gestión de incidentes** • **SO 6.2 Mesa de servicios**	• *14.1.4 Marco de planeamiento de continuidad del negocio*
161	DS8.2 Registro de consultas de clientes	• Registro y seguimiento de todas las llamadas, incidentes, solicitudes de servicio y necesidades de información	• **SO 4.1.5.3 Detección de eventos** • **SO 4.1.5.4 Filtrado de eventos** • **SO 4.1.5.5 Significado de los eventos** • **SO 4.1.5.6 Correlación de eventos** • **SO 4.1.5.7 Trigger** • **SO 4.2.5.1 Identificación de incidentes**	• *13.1.1 Reporte de eventos de seguridad de información* • *13.1.2 Se pueden agregar los reportes de debilidades de seguridad ya que se relacionan con la identificación de eventos* • *13.2.1 Responsabilidades*

			• **SO 4.2.5.2 Log de incidentes** • **SO 4.2.5.3 Clasificación de incidentes** • **SO 4.2.5.4 Priorización de incidentes** • **SO 4.2.5.5 Diagnóstico inicial** • **SO 4.3.5.1 Selección por menú**	*y procedimientos* • *13.2.3 Recolección de evidencia*
162	DS8.3Escalamiento de incidentes	• Escalamiento de incidentes de acuerdo a los límites en los ANS	• **SO 4.1.5.8 Selección de respuestas** • **SO 4.2.5.6 Escalamiento de incidentes** • **SO 4.2.5.7 Investigación y diagnóstico** • **SO 4.2.5.8 Resolución y recuperación** • **SO 5.9 Soporte de estaciones de trabajo**	• *13.1.2 Se pueden agregar los reportes de debilidades de seguridad ya que se relacionan con la identificación de eventos* • *13.2.3 Recolección de evidencia* • *14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio* • *14.1.4 Marco de planificación de continuidad del negocio*
163	DS8.4 Cierre de incidentes	• Registro de los incidentes resueltos y no resueltos	• **SO 4.1.5.10 Cerrar eventos** • **SO 4.2.5.9 Cierre de incidentes**	• *13.2.2 Aprendiendo de los incidentes de seguridad de información* • *13.2.3 Recolección de evidencia*
164	DS8.5 Reportes y análisis de tendencias	• Reportes de desempeño de servicio y tendencias de los problemas recurrentes	• **SO 4.1.5.9 Revisar acciones** • **CSI 4.3 Mediciones del servicio (aproximada)**	• *13.2.2 Aprendiendo de los incidentes de seguridad de información*
165	DS9.1 Repositorio y línea base de configuración	• Registrar ítems de configuración, monitorear y registrar todos los activos, implementar una línea de base para cada sistema y servicio como punto de control de recuperación de cambios	• **SS 8.2 Interfaces del servicio** • **ST 4.1.5.2 Preparación para la transición del servicio** • **ST 4.3.5.2 Gestión y planificación**	• *7.2.2 Etiquetado y manejo de la información* • *12.4.1 Control del software de operaciones* • *12.4.2 Protección de los datos de prueba de sistema*
166	DS9.2 Identificación y mantenimiento de	• Procedimientos de configuración que	• **ST 4.1.5.2 Preparación para la transición del**	• *7.1.1 Inventario de activos*

	elementos de la configuración	soporten el registro de todos los cambios en la base de datos de configuración	**servicio** • **ST 4.3.5.3 Identificación de la configuración** • **ST 4.3.5.4 Control de la configuración** • **ST 4.3.5.5 Contabilización y registro de estados**	• *7.1.2 Propiedad de los activos* • *7.2.2 Etiquetado y manejo de la información* • *10.7.4 Seguridad de la documentación de sistemas* • *11.4.3 Identificación de equipos en redes* • *12.4.2 Protección de los datos de prueba de sistema* • *12.5.3 Restricciones en los cambios a los paquetes de software* • *12.6.1 Control de vulnerabilidades técnicas* • *15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información*
167	DS9.3 Revisión de integridad de la configuración	• Revisión periódica de la integridad de los datos de configuración • Control de software licenciado y software no autorizado	• **ST 4.3.5.6 Auditoría y verificación** • **SO 5.4 Gestión y soporte de servidores** • **SO 7 Consideraciones de tecnología (especialmente para licenciamiento, mencionado en SO 7.1.4)**	• *7.1.1 Inventario de activos* • *10.7.4 Seguridad de la documentación de sistemas* • *12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo* • *15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información*
168	DS10.1 Identificación y clasificación de problemas	• Clasificación de problemas; asignación al personal de soporte	• **SO 4.4.5.1 Detección de problemas** • **SO 4.4.5.3 Clasificación de problemas** • **SO 4.4.5.4 Priorización de problemas** • **SO Apéndice C Kepner y Tregoe** • **SO Apéndice D Diagramas de Ishikawa**	• *13.2.2 Aprendiendo de los incidentes de seguridad de información*
169	DS10.2 Seguimiento y resolución de problemas	• Pistas de auditoría, seguimiento y análisis de causa raíz de todos los	• **SO 4.4.5.2 Log de problemas** • **SO 4.4.5.5 Investigación y**	• *13.2.2 Aprendiendo de los incidentes*

		problemas • Inicio de soluciones para abordar las causas de origen	**diagnóstico de problemas** • **SO 4.4.5.6 Soluciones provisionales** • **SO 4.4.5.7 Registro de errores conocidos** • **SO 4.4.5.8 Resolución de problemas**	*de seguridad de información*
170	DS10.3 Cierre de problemas	• Procedimientos de cierre después de la eliminación del error o enfoques alternos	• **SO 4.4.5.9 Cierre de problemas** • **SO 4.4.5.10 Revisión de problemas mayores**	
171	DS10.4 Integración de la gestión de configuración, incidentes y problemas	• Integración para habilitar una gestión efectiva de problemas		
172	DS11.1 Requerimientos del negocio para la gestión de datos	• Diseño de formulario de entrada • Minimizando errores u omisiones • Procedimientos de manejo de errores	• *SD 5.2 Gestión de los datos y la información*	• *10.8.1 Políticas y procedimientos para el intercambio de información*
173	DS11.2 Acuerdos para el almacenamiento y la conservación	• Preparación de documentos • Segregación de funciones	• **SD 5.2 Gestión de los datos y la información** • **SO 5.6 Almacenamiento y archivo**	• *10.5.1 Respaldo de la información* • *10.7.1 Gestión de medios removibles* • *15.1.3 Protección de registros organizacionales*
174	DS11.3 Sistema de gestión de librería de medios	• Integridad y exactitud		• **10.7.1 Gestión de medios removibles** • **10.7.2 Eliminación de medios** • **12.4.3 Control de acceso al código fuente de los programas**
175	DS11.4 Eliminación	• Detección, reporte y corrección		• **9.2.6 Eliminación o reutilización segura de equipos** • **10.7.1 Gestión de medios removibles** • **10.7.2 Eliminación de medios**
176	DS11.5 Respaldo y restauración	• Requisitos legales • Mecanismos de recuperación y reconstrucción	• **SO 5.2.3 Respaldo y restauración**	• **10.5.1 Respaldo de la información**
177	DS11.6 Requisitos de seguridad para la gestión de datos	• Ingreso de datos por personal autorizado	• *SD 5.2 Gestión de los datos y la información*	• **10.5.1 Respaldo de la información** • **10.7.3 Procedimientos**

				para el manejo de la información • **10.8.3 Medios de almacenamiento físico en tránsito** • **10.8.4 Mensajería electrónica** • **12.4.2 Protección de datos de prueba de sistema** • **12.4.3 Control de acceso al código fuente de los programas**
178	DS12.1 Selección y diseño del centro de datos	• Selección de sitio basada en estrategia tecnológica, riesgo y requerimientos legales y regulatorios		• **9.1.1 Perímetro de seguridad física** • **9.1.3 Seguridad de oficinas, salas e instalaciones** • **9.1.6 Áreas de acceso público, despacho y recepción**
179	DS12.2 Medidas de seguridad física	• Aseguramiento de la ubicación, incluyendo protección para acceso no autorizado, riesgos naturales e interrupciones de energía	• *SO Apéndice E Descripción detallada de la gestión de las instalaciones*	• **9.1.1 Perímetro de seguridad física • 9.1.2 Controles físicos de ingreso** • **9.1.3 Seguridad de oficinas, salas e instalaciones** • **9.2.5 Seguridad de los equipos fuera de las instalaciones** • **9.2.7 Eliminar la propiedad**
180	DS12.3 Acceso físico	• Acceso controlado a los locales	• *SO Apéndice E Descripción detallada de la gestión de las instalaciones* • *SO Apéndice F Controles de acceso físico*	• **6.2.1 Identificación de riesgos relacionados con terceros** • **9.1.2 Controles físicos de ingreso** • **9.1.5 Trabajo en áreas seguras** • **9.1.6 Áreas de acceso público, despacho y recepción** • **9.2.5 Seguridad de los equipos fuera de las instalaciones**
181	DS12.4 Protección contra factores	• Monitoreo y control de factores	• **SO Apéndice E Descripción detallada de la gestión de las**	• **9.1.4 Protección contra amenazas externas y**

	ambientales	ambientales	**instalaciones**	**ambientales** • **9.2.1 Ubicación y protección de equipos** • **9.2.2 Servicios de soporte** • **9.2.3 Seguridad del cableado**
182	DS12.5 Gestión de instalaciones físicas	• Gestión de instalaciones de conformidad a los requerimientos de negocio, legales y regulatorios	• **SO 5.12 Gestión del centro de datos e instalaciones**	• *9.2.2 Servicios de soporte* • *9.2.4 Mantenimiento de equipos*
183	DS13.1 Procedimientos e instrucciones de operación	• Procedimientos y familiaridad con tareas operativas	• **SO 3.7 Documentación** • **SO 5 Actividades comunes de la operación del servicio** • **SO Apéndice B Comunicaciones en la operación de servicio**	• *10.1.1 Procedimientos operativos documentados* • *10.7.4 Seguridad de la documentación de sistemas*
184	DS13.2 Programación de tareas	• Organización de programación de tareas para maximizar el rendimiento y la utilización para cumplir los ANS	• **SD 4.3.5.5 Gestión y control de umbrales** • **SD 4.3.5.6 Gestión de la demanda** • **SD 5.2.2 Programación de tareas** • **SO 5.3 Gestión de mainframe**	
185	DS13.3 Monitoreo de la infraestructura de TI	• Infraestructura de monitoreo para eventos críticos • Registro de logs para permitir revisión	• **SD 4.3.5.4 Actividades de soporte de la gestión de capacidad** • **SD 4.3.5.5 Gestión y control de umbrales** • **SO 4.1 Gestión de eventos** • **SO 4.1.5.1 Ocurrencia de eventos** • **SO 4.1.5.9 Revisar acciones** • **SO 5.2.1 Gestión de consola / Puente de operaciones**	
186	DS13.4 Documentos sensitivos y dispositivos de salida	• Salvaguardas físicas para activos sensitivas e instrumentos negociables	• *SO 5.2.4 Datos electrónicos e impresos*	
187	DS13.5 Mantenimiento preventivo del hardware	• Mantenimiento para reducir el impacto de fallas	• *SO 5.3 Gestión de mainframe* • *SO 5.4 Gestión y soporte de servidores*	• *9.2.4 Mantenimiento de equipos*
188	ME1.1 Enfoque del monitoreo	• Marco de monitoreo general • Integración con el	• **SD 8.5 Mediciones del diseño de servicio** • **ST 4.5.5.1 Gestión de**	

		enfoque corporativo	**pruebas y validación** • **SO 3.5 Operación saludable** • **CSI 4.1 El proceso de mejora de los siete pasos** • **CSI 4.1a Paso Uno – Definir lo que se debe medir** • **CSI 4.1b Paso Dos – Definir lo que se puede medir** • **CSI 4.1.1 Integración con el resto de etapas del ciclo de vida y los procesos de gestión de servicio** • **CSI 4.1.2 Métricas y mediciones** • **CSI 4.3 Mediciones del servicio** • **CSI 4.4 Retorno sobre la inversión debido al CSI** • **CSI 4.5 Aspectos del negocio en CSI** • **CSI 5.1 Métodos y técnicas** • **CSI 5.2 Evaluaciones**	
189	ME1.2 Definición y recolección de datos de monitoreo	• Conjunto balanceado de objetivos aprobado por los interesados • Comparativas, disponibilidad y recolección de datos medibles	• **SD 4.2.5.10 Reclamos y reconocimientos** • **CSI 4.1c Paso Tres – Recopilación de datos** • **CSI 4.1d Paso Cuatro – Procesar los datos**	• *10.10.2 Monitoreo del uso del sistema*
190	ME1.3 Método de monitoreo	• Método para capturar y reportar resultados	• **ST 4.5.5.2 Planificar y diseñar pruebas** • **ST 4.5.5.3 Verificar el plan y el diseño de pruebas** • **ST 4.5.5.4 Preparar el entorno de pruebas** • **CSI 4.1b Paso Dos – Defina lo que se puede medir** • **CSI 4.1f Paso Seis – Presentar y utilizar la información** • **CSI 5.4 Marcos de medición y reporte**	
191	ME1.4 Evaluación del desempeño	• Revisión de desempeño contra objetivos • Acciones correctivas • Análisis de causas raíz	• **SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio** • **CSI 3 Principios de**	

			mejora continua de servicios • **CSI 4.1e Paso Cinco – Analizar los datos** • **CSI 5.3 Benchmarking** • **CSI 8 Implementar la mejora continua del servicio**	
192	ME1.5 Reportes al Consejo Directivos y a ejecutivos	• Reportes de la contribución de TI al negocio por los portafolios y programas de servicios e inversión	• *CSI 4.1f Paso Seis – Presentar y utilizar la información* • *CSI 4.2 Reportes del servicio*	
193	ME1.6 Acciones correctivas	• Seguimiento y correcciones a todos los problemas de desempeño	• **CSI 4.1g Paso Siete – Implementar acciones correctivas**	
194	ME2.1 Monitoreo del marco de trabajo del control interno	• Revisión y mejoramiento continuo de controles internos		• *5.1.1 Documento de la política de seguridad de la información* • *15.2.1 Cumplimiento con políticas y estándares de seguridad.*
195	ME2.2 Revisiones de supervisión	• Revisión de los controles de revisión de la gerencia		• *5.1.2 Revisión de la política de seguridad de la información* • *6.1.8 Revisión independiente de la seguridad de la información* • *10.10.2 Monitoreo del uso del sistema* • *10.10.4 Logs de administrador y de operador* • *15.2.1 Cumplimiento con políticas y estándares de seguridad*
196	ME2.3 Excepciones de control	• Análisis de las excepciones de control y causas raíz		• *15.2.1 Cumplimiento con políticas y estándares de seguridad*
197	ME2.4 Autoevaluación de control	• Evaluación de la efectividad de los controles por medio de la auto evaluación		• *15.2.1 Cumplimiento con políticas y estándares de seguridad*

198	ME2.5 Aseguramiento del control interno	• Revisiones por terceros para brindar mayor garantía		• *5.1.2 Revisión de la política de seguridad de la información* • *6.1.8 Revisión independiente de la seguridad de la información* • *10.10.2 Monitoreo del uso del sistema* • *10.10.4 Logs de administrador y de operador* • *15.2.1 Cumplimiento con políticas y estándares de seguridad* • *15.2.2 Verificación de cumplimiento técnico* • *15.3.1 Controles de auditoría de sistemas de información*
199	ME2.6 Control interno para terceros	• Estado y conformidad de controles de proveedores externos		• *6.2.3 Considerar la seguridad en los acuerdos con terceros* • *10.2.2 Monitoreo y revisión de los servicios de terceros* • *15.2.1 Cumplimiento con políticas y estándares de seguridad*
200	ME2.7 Acciones correctivas	• Corrección de las excepciones de la evaluación de control		• *5.1.2 Revisión de la política de seguridad de la información* • *15.2.1 Cumplimiento con políticas y estándares de seguridad*
201	ME3.1 Identificación de los requisitos legales, regulatorios y de cumplimiento contractual	• Identificación continua de requerimientos de cumplimiento para su incorporación en las políticas y prácticas		• **6.1.6 Relación con las autoridades que tengan impacto potencial en TI** • **15.1.1 Identificación de legislación aplicable** • **15.1.2 Derechos de propiedad intelectual** • **15.1.4 Protección de datos y privacidad de la**

				información personal
202	ME3.2 Optimización de respuesta a requerimientos externos	• Revisión y ajuste de políticas y prácticas para asegurar el cumplimiento		
203	ME3.3 Evaluación del cumplimiento con requerimientos externos	• Confirmación del cumplimiento		• *6.1.6 Relación con las autoridades que tengan impacto potencial en TI* • *15.1.1 Identificación de legislación aplicable* • *15.1.2 Derechos de propiedad intelectual* • *15.1.4 Protección de datos y privacidad de la información personal*
204	ME3.4 Aseguramiento positivo del cumplimiento	• Reportar garantía de cumplimiento y confirmación de las acciones correctivas		• *6.1.6 Relación con las autoridades que tengan impacto potencial en TI* • *15.1.1 Identificación de legislación aplicable* • *15.1.2 Derechos de propiedad intelectual* • *15.1.4 Protección de datos y privacidad de la información personal*
205	ME3.5 Reportes integrados	• Reportes integrados de cumplimiento de la empresa		
206	ME4.1 Establecimiento de un marco de gobierno de TI	• Marco de gobierno de TI alineado al gobierno corporativo • Basado en procesos adecuados de TI y el modelo de control • Marco de confirmación que asegure el cumplimiento y la confirmación de la entrega de la estrategia corporativa para TI	• *CSI 3.10 Gobierno* • *CSI Apéndice A Guía complementaria*	
207	ME4.2 Alineamiento	• Comprensión de la Dirección de la	• *SD 3.10 Gestión de*	

	estratégico	estrategia de TI, la dirección estratégica, confianza entre el negocio y TI, y la co-responsabilidad para decisiones estratégicas y realización de beneficios	*servicio al negocio*	
208	ME4.3 Entrega de valor	• Entrega del valor óptimo para apoyar la estrategia empresarial • Entender los resultados de negocio esperados; casos de negocio eficaces; gestión del ciclo de vida económico y realización de beneficios; ejecución de la gestión de portafolio, programas y proyectos; asignar propiedad de las inversiones	• *SS 3.1 Creación de valor*	
209	ME4.4 Gestión de recursos	• Evaluación regular para asegurar los recursos apropiados y el alineamiento con los objetivos vigentes y futuros		
210	ME4.5 Gestión de riesgos	• Apetito de riesgo; prácticas apropiadas de gestión de riesgo; responsabilidades implícitas de riesgos; evaluación regular y reportes transparentes de riesgo	• *SS 9.5 Riesgos*	
211	ME4.6 Medición del desempeño	• Confirmar que los objetivos han sido alcanzados; revisar cualquier acción correctiva; reporte del desempeño a la alta gerencia y habilitar revisión de los avances	• *SS 4.4 Preparar la ejecución* • *SS 9.4 Efectividad en mediciones* • *SD 3.6.5 Diseño de sistemas de medición y métricas* • *CSI 4.3 Mediciones del servicio*	
212	ME4.7 Aseguramiento independiente	• Obtener el aseguramiento independiente apropiado (interna o externa) de		• *5.1.2 Revisión de la política de seguridad de la información* • *6.1.8 Revisión independiente de*

		cumplimiento con los objetivos y con los requerimientos externos		*la seguridad de la información* • *10.10.2 Monitoreo del uso del sistema*

Fuente: **IT Governance Institute 2008**

Anexo G
[Tabla de Normativas]

Tabla 11. Marco Legal

Id_Normativa	Id_Control	Num_Articulo	Descripción Artículo
NTI1	20	39a	En la estructura organizacional del Ente supervisado, debe existir un área de seguridad de la información independiente de las unidades de Tecnología de la Información, Auditoria de Sistemas y Riesgo, estableciéndose como mínimo las siguientes funciones: a. Definir y mantener actualizadas las políticas de seguridad de la información.
NTI1	37	39b	b. Aplicar y asegurar el cumplimiento de las políticas de seguridad de la información definidas.
NTI1	144	39c	c. Administrar el acceso a los sistemas operativos, bases de datos, aplicaciones, cortafuego, enrutadores, proxys, equipos computacionales y de telecomunicaciones empleados por el Ente supervisado, incluyendo aquellos administrados y custodiados por terceros.
NTI1	120	39d	d. Monitorear los procesos de control de cambio y pases a producción de los sistemas y aplicaciones productivas.
NTI1	143	39e	e. Realizar el control y seguimiento continuo a los accesos efectuados a los activos de información.
NTI1	1001	39f	f. Establecer políticas, normas y procedimientos que regulen, controlen y aseguren el seguimiento continuo de la utilización del correo electrónico e Internet y todas aquellas transacciones que son ejecutadas a través de los diferentes canales electrónicos empleados por los clientes.
NTI1	1002	44	El Ente supervisado debe establecer políticas y procedimientos para regular, controlar y monitorear la utilización y acceso al correo electrónico e Internet, así como, a los enrutadores, cortafuego (firewall) y proxys. De igual forma, deberá generar reportes de auditoría sobre intentos de violaciones a las redes o equipos, detección de posibles delitos informáticos que atentan contra la confidencialidad de los clientes, uso de utilitarios sensitivos y las actividades de los usuarios con atributos de administración y accesos especiales.
NTI1	150	46	Establecer dentro de su plataforma de red, aplicaciones que faculten la prevención, detección y eliminación de virus informáticos. El Ente supervisado, deberá asegurarse de la oportuna actualización de la base de datos de virus.
NTI1	169	49	Se deben mantener activos los registros o pistas de auditoría generadas por las aplicaciones y sistemas de misión crítica, particularmente en aquellos casos en los cuales exista modificación o alteración de la información almacenada en las

			bases de datos productivas. De igual forma, deberán asegurar el almacenamiento de los mencionados registros por un periodo de un (1) año. Por otra parte, las pistas de auditoría deberán ser revisadas por el área de seguridad de la información y auditoría de sistemas, para lo cual será necesario generar informes que reflejen posibles brechas o vulnerabilidades identificadas. Estos informes deberán generarse anualmente y deben ser entregados a esta Superintendencia, cuando así sea requerido.
NTI1	187	129	La unidad de seguridad de los activos de información del Ente supervisado, deberá establecer mecanismos de control que permitan alertar las fallas y minimizar las vulnerabilidades que la plataforma tecnológica que soporta los servicios de banca virtual pueda presentar, considerando como mínimo:
NTI1	1003	129a	a. Definición de controles de acceso lógicos a datos, sistemas, aplicaciones, software, utilitarios, líneas de comunicaciones, librerías, entre otros.
NTI1	92	129b	b. Existencia de mecanismos cortafuegos (firewalls) para mediar entre la red pública, Internet y la red privada del Ente supervisado, a fin de garantizar la no intromisión cuando estas se evidencien.
NTI1	1004	129c	c. Protección contra virus y monitoreo y acciones correctivas sobre cualquier actividad asociada a delitos informáticos en el ambiente de banca virtual y sus redes privadas de soporte (denegación del servicio, plagio, usurpación o adulteración de identidad, captura de información personal, financiera y privada del cliente, entre otros aspectos).
NTI1	1005	129d	d. Inhabilitación de servicios innecesarios en el servidor de aplicación de la banca virtual, tales como: Protocolo de Transferencia de Archivo (FTP - File Transfer Protocol), Telnet.
NTI1	1006	129e	e. Utilización de tecnologías de seguridad para implementar el servicio de la banca virtual, tales como: Infraestructura de Claves Públicas (PKI – Public Key Infraestructura), Protocolos SSL (Secure Sockets Layer), TLS (Transport Layer Security), IPSec, SET.
NTI1	185	129f	f. Uso de herramientas que permitan el monitoreo de los sistemas y las redes para detectar intrusos o prevenir ataques.
NTI1	149	129g	g. Manejo de precauciones para emplear los enlaces de telecomunicación a través de redes privadas virtuales y técnicas de encriptación relacionadas.
NTI1	1007	12h	h. Revisión periódica de la infraestructura y políticas de seguridad de la Institución con el fin de optimizar las mismas basadas en la propia experiencia de la Institución y sus cambios tecnológicos.

NTI1	180	129i	i. Reforzamiento de los controles de acceso físico.
NTI1	139	129j	j. Infraestructura apropiada para la ejecución de respaldos de la data, la cual debe ser probada periódicamente.
NTI1	138	129k	k. Mecanismos que garanticen la disponibilidad del servicio.
NTI1	168	129l	l. Planes apropiados de respuesta a incidentes que incluyan estrategias de comunicación que aseguren la continuidad del servicio y responsabilidad limitada asociada con interrupciones del servicio de banca virtual incluyendo aquellos originados desde sistemas externos.
NTI1	1008	129m	m. Definición e implantación de procedimientos y controles que brinden una adecuada seguridad en las aplicaciones de banca virtual: control de cambios y/o modificaciones, separación de ambientes de prueba.
NTI1	152	130	Se debe garantizar la autenticidad, la integridad, la confidencialidad y el no repudio o rechazo de las transacciones; así como, asegurar una adecuada segregación de responsabilidades y controles de autorización. En este sentido, se deben considerar como mínimo los siguientes aspectos:
NTI1	1009	131	El Ente supervisado debe tomar las medidas apropiadas para informar a los clientes del servicio de banca virtual sobre el manejo de la seguridad y privacidad de la información. Para tal propósito se deben aplicar, al menos, las siguientes medidas:
	1010	131a	a. Informar a los clientes, en forma clara, las políticas de seguridad empleadas por la Institución en su servicio de banca virtual.
	1011	131b	b. Instruir a los clientes sobre la necesidad de proteger su clave secreta, número de identificación personal y cualquier información bancaria y personal.
NTI2	1012	5	Las Instituciones Bancarias deberán utilizar factores de autenticación para verificar la identidad de sus clientes y la cualidad de éstos para realizar operaciones mediante la Banca Electrónica. Dichos factores de autenticación serán los siguientes: • Factor de autenticación categoría 1: Se compone de la información obtenida de la ficha del cliente y del uso de productos, servicios u operaciones efectuadas por éstos mediante los diversos canales. Esta información será utilizada mediante la aplicación de cuestionarios al cliente a través del servicio de IVR, Banca por Internet y la asistencia de operadores telefónicos. Para este tipo de factor las Instituciones Bancarias deberán: • Definir previamente los cuestionarios que serán aplicados para la identificación positiva de los clientes y modificar su contenido al menos una (1) vez al año.

			• Establecer generadores aleatorios de las preguntas de los cuestionarios. • Cuando intervenga el operador, éste no podrá consultar o conocer anticipadamente las respuestas para la identificación positiva del cliente, las cuales deben ser validadas con el uso de sistemas informáticos. • Factor de Autenticación Categoría 2: Se compone de contraseñas que sólo el cliente conoce e ingresa mediante un mecanismo o dispositivo de acceso, el cual debe cumplir con las siguientes características: • Su longitud mínima debe ser de: • Cuatro (4) caracteres para los servicios ofrecidos a través de cajeros automáticos, puntos de ventas, Banca Telefónica, servicio de IVR y Pago Móvil. • Ocho (8) caracteres para Banca por Internet y Banca Móvil. • Cuando el dispositivo de acceso lo permita, la composición de este factor de autenticación deberá incluir, a elección del cliente, al menos dos (2) de los siguientes tipos de caracteres: alfabéticos, numéricos y/o especiales. • Se debe validar el uso de las últimas cinco (5) contraseñas. • Su vencimiento no será superior a ciento ochenta (180) días; no obstante, las Instituciones Bancarias están en la obligación de ofrecer a sus clientes la posibilidad de realizar el cambio de las contraseñas cuando éstos lo requieran. • Transcurridos los 180 días de vigencia de la contraseña, al cliente se le permitirá la realización de transacciones si y solo si, el canal electrónico a utilizar no posibilita el cambio de esta. No obstante, la Institución Bancaria deberá notificar al cliente la obligación de realizar el cambio de la contraseña, a la brevedad posible. • En el caso de las contraseñas asignadas por las Instituciones Bancarias, para el acceso a la Banca Electrónica, se debe requerir en forma automática que el cliente la modifique inmediatamente después de iniciar la primera sesión.

			• Garantizar que la primera sesión se efectúe como máximo al siguiente día hábil bancario de la generación de la contraseña por parte de la Institución; en caso contrario, ésta debe ser inhabilitada automáticamente. • En ningún caso se podrá utilizar como contraseña, la siguiente información: • El identificador del cliente. • El nombre de la Institución. • Más de tres (3) caracteres iguales consecutivos numéricos o alfabéticos. • Fecha de nacimiento, nombres, apellidos y número telefónico, registrado por el cliente en la Institución. • Factor de Autenticación Categoría 3: Se compone de claves dinámicas de un único uso, generadas por dispositivos electrónicos o cualquier otro medio, las cuales deben cumplir con las siguientes características: • Contar con mecanismos que impidan su duplicación o alteración. • Una vez generada la clave dinámica, ésta tendrá vigencia: • Hasta dos (2) minutos, en el caso de que sean generados por Tokens. • Hasta el cierre de sesión, para los canales de Banca por Internet y Banca Móvil. • No ser conocida antes de su generación ni durante su uso, por los funcionarios, empleados, representantes o por terceros de la Institución. • Se podrán utilizar tablas aleatorias de contraseñas como factor de autenticación de esta categoría, siempre y cuando cumplan con las características listadas en este factor de autenticación. • Los reclamos derivados de estas operaciones deberán ser atendidos en el plazo establecido por el Decreto con Rango, Valor y Fuerza de Ley de Reforma Parcial de la Ley de Instituciones del Sector Bancario y las normas

			vigentes. • Factor de Autenticación Categoría 4: Se refiere a la utilización de firmas electrónicas certificadas debidamente emitidas a nombre del Cliente por un Proveedor de Servicios de Certificación (PSC). • Factor de Autenticación Categoría 5: Se compone de información del Cliente derivada de sus características Biométricas.
NTI2	1013	6	Los sistemas de Banca Electrónica de las Instituciones Bancarias deberán requerir a sus Clientes un factor para inicio de sesión más un segundo factor de autenticación de categorías 3, 4 ó 5 a que hace referencia el artículo 5 de las presentes normas.
NTI2	1014	7	Para las operaciones de pagos o transferencias electrónicas a terceros que no requieran la afiliación o registro de cuentas, se deberá utilizar el factor adicional, a que hace referencia el artículo anterior.
NTI2	1015	10	Para permitir el inicio de sesión a los Clientes a través de los servicios ofrecidos por la Banca por Internet, Banca Móvil u otro canal electrónico que así lo requiera, las Instituciones Bancarias deberán solicitar y validar al menos: • Un identificador de Cliente de por lo menos seis (6) caracteres. • Un factor de autenticación de las categorías 2, 3, 4 o 5. El identificador del Cliente deberá permitir unívocamente a las Instituciones Bancarias, determinar todas las operaciones realizadas por el propio Cliente mediante estos canales.
NTI2	1016	12	En la Banca por Internet, las Instituciones Bancarias deben proveer información al Cliente, de acuerdo con lo siguiente: • Elementos que identifiquen a la Institución, antes de ingresar todos los elementos de autenticación. Para ello, deberán usar certificados electrónicos (SSL) u otros mecanismos que permitan autenticar el sitio transaccional. Adicionalmente, podrán utilizar la siguiente información: - Aquella que el Cliente conozca y haya proporcionado a la Institución, o bien, que haya señalado para este fin, tales como nombres y apellidos, imágenes, entre otros. - La provista por los factores de autenticación de categoría 4 o 5.

NTI2	1017	14	Las Instituciones Bancarias podrán establecer métodos adicionales de autenticación a los previstos en esta norma para las transacciones realizadas en la Banca Electrónica.
NTI2	1018	15	Las Instituciones Bancarias deben establecer para cada canal electrónico, montos máximos diarios para las operaciones de pagos, transferencias y retiros, con base a estudios realizados por su Unidad de Administración Integral de Riesgo (UAIR), sin perjuicio de lo establecido en la legislación y las normas vigentes.
NTI2	1019	16	Las Instituciones Bancarias deberán generar comprobantes electrónicos para todas las operaciones realizadas en el servicio de Banca Electrónica. Se exceptúan las operaciones de consulta que se realicen a través de la Banca por Internet o Banca Móvil.
NTI2	148	17	Con respecto a la sesión del Cliente, las Instituciones Bancarias deben garantizar lo siguiente: • Finalizar la sesión en forma automática en los casos siguientes: - Cuando la inactividad alcance a tres (3) minutos en la Banca por Internet. - Cuando se detecten sesiones simultáneas. • Las Instituciones Bancarias que ofrezcan enlaces a empresas mediante su página web, deberán comunicar a sus Clientes que al momento de ingresar a éstos, su seguridad no depende ni es responsabilidad de dicha Institución.
NTI2	22	18	Las Instituciones Bancarias deberán informar a sus Clientes, mediante campañas educacionales, sobre el funcionamiento de los canales electrónicos que pongan al alcance de éstos, a fin de prevenir actos que pudieran derivar en operaciones irregulares o ilegales que afecten a los Clientes o a las propias Instituciones.
NTI2	177	21	Para las operaciones que se realicen a través de la Banca Electrónica, las Instituciones Bancarias deben implementar mecanismos de protección de datos en la transmisión y almacenamiento de la información, a fin de evitar que los datos sensibles sean conocidos por terceros no autorizados.
NTI2	1020	22	En ningún caso, las Instituciones Bancarias podrán transmitir las contraseñas de categoría 2 a que se refiere el artículo 5 de las presentes normas o números de identificación personal y de productos, a través de algún medio de comunicación electrónica.
NTI2	1021	25	Las Instituciones Bancarias deben notificar en forma inmediata a los Clientes a través de mensajes de texto (SMS) al teléfono móvil registrado, las alertas activadas por sus sistemas de monitoreo antifraude asociadas a las operaciones realizadas a través de los canales electrónicos de acuerdo a la evaluación del perfil transaccional del cliente. En caso que el Cliente no posea el mencionado dispositivo o manifieste no

			desear el servicio, la Institución podrá realizar la notificación por cualquier otro medio de comunicación electrónica. El mensaje deberá incluir al menos la siguiente información: fecha y hora de la transacción, monto de la operación, número de referencia de la transacción, nombre y número de teléfono de la Institución, canal utilizado y tipo de operación.
NTI2	1022	26	Las Instituciones Bancarias deberán establecer procesos y mecanismos automáticos para bloquear preventivamente el acceso a la Banca Electrónica, en los siguientes casos: • Cuando se intente ingresar al servicio utilizando información de autenticación incorrecta. En ningún caso, los intentos de acceso fallidos podrán exceder tres (3) intentos consecutivos. • Cuando los sistemas de monitoreo detecten comportamiento transaccional irregular o los sistemas de seguridad detecten un ataque informático que comprometa los datos sensibles. • Cuando existan situaciones que comprometan la seguridad de los sistemas de información y del Cliente.
NTI2	130	28	Las Instituciones Bancarias deben definir mecanismos de monitoreo y control para asegurar el adecuado funcionamiento de los canales electrónicos.

Fuente: Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras y Resolución 641.10 de Banca Electrónica.