REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO

ESPECIALIZACIÓN EN PLANIFICACIÓN,
DESARROLLO Y GESTIÓN DE PROYECTOS

FORMULACIÓN DE ESTRATEGIAS PARA IMPLANTAR EL ESTANDAR DE SEGURIDAD DE DATOS EN LA INDUSTRIA DE TARJETAS DE PAGO (PCI-DSS) DE BANCARIBE BANCO UNIVERSAL

Trabajo Especial de Grado, para optar al Título de Especialista en Planificación, Desarrollo y Gestión de Proyectos, presentado por:

Arroyo Higuera, Nailet Carolina, CI: 13.354.574

Asesorado por:

Guillén Guédez, Ana Julia

Sarache, Xarifa

Caracas, Marzo **de** 2017

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO

ESPECIALIZACIÓN EN PLANIFICACIÓN, DESARROLLO Y GESTIÓN DE PROYECTOS

FORMULACIÓN DE ESTRATEGIAS PARA IMPLANTAR EL ESTANDAR DE SEGURIDAD DE DATOS EN LA INDUSTRIA DE TARJETAS DE PAGO (PCI-DSS) DE BANCARIBE BANCO UNIVERSAL

Trabajo Especial de Grado, para optar al Título de Especialista en Planificación, Desarrollo y Gestión de Proyectos, presentado por:

Arroyo Higuera, Nailet Carolina, CI: 13.354.574

Asesorado por:

Guillén Guédez, Ana Julia

Sarache, Xarifa

Caracas, Marzo **de 2017**

Señores:

Universidad Monteávila
Comité de Estudios de Postgrado
Especialización en Planificación, Desarrollo y Gestión de Proyectos

Atención: Profesora Geraldine Cardozo

Referencia: **Aprobación de Asesoría**

Por medio de la presente le informo que he revisado el borrador final del Trabajo Especial de Grado de la Ciudadana: **Arroyo Higuera, Nailet Carolina**, titular de la Cédula de Identidad N° 13354574; cuyo título tentativo es: **"Formulación de Estrategias para Implantar el Estándar de Seguridad de Datos en la Industria de Tarjetas de Pago (PCI-DSS) de Bancaribe"**, la cual cumple con los requisitos vigentes de esta casa de estudio para asignarles jurado y su respectiva presentación.

A los 9 días del mes de Marzo del 2017

Guillén Guédez, Ana Julia

Caracas, 07-03-2017

Señores
Universidad Monteávila
Comité de Estudios de Postgrado.
Especialización en Planificación, Desarrollo y Gestión de Proyectos
Presente.

Estimados el siguiente es con la finalidad de solicitar de su apoyo en la valoración de la propuesta de trabajo de grado de la Ing. Nailet Arroyo, titular de la Cédula de Identidad: 13.354.574, cuyo título es “FORMULACIÓN DE ESTRATEGIAS PARA IMPLANTAR EL ESTANDAR DE SEGURIDAD DE DATOS EN LA INDUSTRIA DE TARJETAS DE PAGO (PCI-DSS) DE BANCARIBE “. Actualmente deseamos cubrir esa necesidad.

Víctor Mendoza
Gerencia de Gestión de Riesgo
V.P. de Seguridad de la Información
Teléfono: 58 (212) 954.59.07

REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO
ESPECIALIZACIÓN EN PLANIFICACIÓN, DESARROLLO Y GESTIÓN DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

FORMULACIÓN DE ESTRATEGIAS PARA IMPLANTAR EL ESTANDAR DE SEGURIDAD DE DATOS EN LA INDUSTRIA DE TARJETAS DE PAGO (PCI-DSS) DE BANCARIBE

Autora: Arroyo Higuera, Nailet Carolina
Asesor: Guillén Guédez, Ana Julia
Año: 2017

RESUMEN

La implementación del estándar de seguridad de datos en la industria de tarjetas de pago de una institución bancaria, son normativas que permiten aumentar la seguridad en los sistemas de procesamiento de la información de las transacciones, con ello se incrementa la confianza de los clientes y por consiguiente su fidelidad y aumento de las ventas del negocio. Sin embargo hay interrogantes que debieron plantearse estas organizaciones, ¿Cuánto costará realizar la implementación del estándar?, ¿Cuánto tiempo se invertirá para implementarlo?, ¿Será beneficioso para la organización implementar dicho estándar? El presente trabajo de investigación presentó una propuesta de Plan de implementación para un proyecto de formulación de estrategias para implantar el estándar de seguridad de datos en la industria de tarjetas de pago, específicamente la versión 3.2 del estándar PCI-DSS, en el mismo se toman en cuenta las Mejores Prácticas de la Gerencia de Proyectos. Las bases teóricas se enmarcaron en los fundamentos para la dirección de proyectos de PMI, la ISO21500:2012. Normas sobre dirección e ISO 9000:2015 Sistemas de Gestión de la Calidad. La investigación fue de tipo Aplicada su diseño documental y de campo, enfocada a la recolección y análisis de datos en una sola fase temporal, con la finalidad de desarrollar un Plan de implementación del estándar de seguridad de datos en la industria de tarjetas de pago de pago (PCI-DSS), el cual sirvió de modelo a aquellas instituciones bancarias que deseen apostar por la certificación PCI-DSS. Se utilizaron como referencias destacadas el Estándar PCI-DSS y las Buenas Prácticas en Gerencia de Proyectos. El plan de implementación permitió una orientación estandarizada de planificación lo cual garantizó un buen control del cronograma del proyecto de acuerdo a los procesos de planificación propuestos en el PMI.

Palabras Clave: Plan de implementación, PCI-DSS, Proyecto, Institución Bancaria, Buenas Prácticas, Gerencia de Proyectos.

Línea de Trabajo: Definición y Desarrollo de Proyectos.

Nomenclatura UNESCO: (53) Ciencias Económicas, (5311) Organización y Dirección de Empresas, (531106) Gestión Financiera

INDICE GENERAL

INDICE DE FIGURAS

Figura **Página**

INDICE DE TABLAS

Tabla **Página**

LISTA DE ACRONIMOS Y SIGLAS

Siglas	Significado
CAV	Card Authentication Value (valor de autenticación de la tarjeta) (tarjetas de pago JCB)
CAV2	Card Authentication Value 2 (valor de autenticación de la tarjeta) (tarjetas de pago JCB).
CID	Card Identification Number (número de identificación de la tarjeta) (tarjetas de pago American Express y Discover).
CSC	Card Security Code (código de seguridad de la tarjeta) (tarjetas de pago American Express).
CVC2	Card Validation Code 2 (código de validación de la tarjeta 2) (tarjetas de pago MasterCard).
CVV	Card Verification Value (valor de verificación de la tarjeta) (tarjetas de pago Visa y Discover).
CVV2	Card Verification Value 2 (valor de verificación de la tarjeta) (tarjetas de pago Visa).
DSS	Acrónimo de “Data Security Standard” (Estándar de seguridad de datos).
EDT/WBS	Estructura Desagregada de Trabajo/Work Breakdown Structure.
PA-DSS	Acrónimo de “Data Security Standard- Payment Application” (Estándar de Seguridad de Datos para las aplicaciones de pago).
PA-QSA	Acrónimo de “Payment Application Qualified Security Assesor” (Asesor de seguridad certificado para las aplicaciones de pago), una empresa calificada por las PCI-SSC para realizar evaluaciones de aplicaciones de pago de acuerdo con las PA-DSS.
PAN	El número de cuenta principal (PAN) es el factor que define la aplicabilidad de los requisitos de las PCI-DSS y las PA-DSS. Los requisitos de las PCI- DSS se aplican si se almacena, procesa o transmite un número de cuenta principal (PAN). Si no se almacena, procesa ni transmite el PAN, no se aplicarán las PCI-DSS ni las PA-DSS.
PCI-DSS	Acrónimo de “Payment Card Industry-Data Security Standard” (Norma de seguridad de datos de la industria de tarjetas de pago).
PCI-PTS	Acrónimo de “Payment Card Industry-Pin Transaction Security” (Industria de Tarjetas de Pago-Seguridad de Transacciones con PIN).
PCI -SSC	Acrónimo de “Security Standards Council” (Consejo de Normas de seguridad-Industria de tarjetas de pago).
PIN	Acrónimo de “Personal Identification Number” (Número de Identificación Personal). Contraseña numérica que conocen solo el usuario y un sistema para autenticar al usuario en el sistema. El usuario tan solo obtiene acceso si su PIN coincide con el PIN del sistema.
POI	Acrónimo de “Point of Interaction” (Punto de Interacción).
PMI	Project Management Institute.
QSA	Acrónimo de “Qualified Security Assessor” (Asesor de Seguridad Certificado). Los QSA están calificados por las PCI-SSC para realizar evaluaciones en el lugar.
SIAR LC/FT	Acrónimo de “Sistema Integral de Administración de Riesgos de Legitimación de Capitales y Financiamiento al Terrorismo”.
TEG	Trabajo Especial de Grado.
UNIF	Acrónimo de “Unidad Nacional de Inteligencia Financiera”

INTRODUCCIÓN

Las instituciones bancarias que procesan, almacenan o gestionan la información de los titulares de las tarjetas de crédito o débito deben garantizar la seguridad de estos datos sensibles debido a que su filtración podría conllevar el hackeo o fraude de la información. Con el fin de combatir el fraude se creó el estándar de seguridad de datos para la industria de tarjetas de pago, destinado a la formulación, mejora, almacenamiento, difusión y la aplicación constante de las normas de seguridad para la protección de datos, de esta manera se deben asegurar que las transacciones de sus clientes se realicen en un entorno seguro.

Para ello es fundamental el cumplimiento de la normativa PCI-DSS cuyo fin es combatir el fraude de los datos de los titulares de las tarjetas y cuentas. La implementación de dicho estándar en las organizaciones traen consigo una cantidad de costos tanto en moneda, como en tiempo y el recurso humano a invertir para adecuarse a la normativa, es ahí cuando cobra importancia tratar el tema de implementación como un “Proyecto”.

El presente trabajo basado en un enfoque de proyectos, planteó un camino para minimizar los riesgos que puedan presentársele a las instituciones bancarias que tomen la decisión de implementar el estándar PCI-DSS. Cuyo objetivo es proponer un proyecto de formulación de estrategias para implantar el estándar PCI-DSS en Bancaribe. Este documento está estructurado por capítulos, en el Capítulo I se presenta el planteamiento de la investigación, interrogante y sistematización, posteriormente se establecen los objetivos de la misma y por último se justifica la problemática tratada.

En el Capítulo II se establecen los antecedentes de la investigación, bases teóricas, bases legales compuestas por leyes nacionales e internacionales. En el

capítulo III, se establece el marco metodológico, se detalla el tipo de investigación, las técnicas y herramientas de recolección de datos, las fases de la investigación, Operacionalización de las variables y aspectos éticos. En el capítulo IV, se describe el Marco referencial de la institución bancaria Bancaribe Banco Universal. En el capítulo V, se desarrollan los objetivos de la investigación y se describen los resultados por cada objetivo específico.

En el capítulo VI, se analizan los resultados de la investigación, en el capítulo VII, se detallan las lecciones aprendidas. Finalmente se presenta el capítulo VIII, se describen las conclusiones por cada objetivo y se detallan las recomendaciones relacionadas al objetivo general y por ultimo las Referencias Bibliográficas.

CAPITULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1. PLANTEAMIENTO DE LA INVESTIGACIÓN

En la actualidad el avance tecnológico le ha permitido a las instituciones financieras ofrecer a sus clientes nuevos servicios bancarios, como es el caso de la banca en línea y la banca móvil, permitiéndoles realizar transacciones y consultas a través de Internet. Sin embargo a la par de los servicios, también incrementa la delincuencia (ciberdelito), dado que esta última se encarga de desarrollar nuevas tecnologías para realizar robos. Es una obligación para los bancos implantar sistemas de protección sobre toda la información sensible y confidencial que posee de sus tarjetahabientes.

De los anteriores párrafos se desprende que servicios agregados de los bancos, tales como banca electrónica y móvil, compras online, entre otros, implican el manejo de dinero electrónico, siendo por lo tanto común el uso de tarjetas de crédito y debito, que le permiten al cliente realizar compras, sin tener el dinero físico con él. Las instituciones financieras han buscado mecanismos de control que permitan disminuir los riesgos tanto financieros como operacionales y por ende los siniestros fraudulentos, tal es el caso de las empresas emisoras de tarjetas de crédito.

Las empresas emisoras de tarjetas han diseñado normas, procedimientos y adecuaciones de sistemas, para que las instituciones que emitan tarjetas localmente, mantengan estándares de control que contribuyan a minimizar y eliminar este flagelo que tanto afecta a los entes involucrados. En este sentido se considera que a pesar de todos los mecanismos diseñados y establecidos por las autoridades respectivas, las instituciones financieras siguen presentando el

problema del fraude financiero, especialmente el cometido con tarjetas de crédito ya que estas representan un medio de pago para la clientela de los bancos.

Bancaribe no escapa del fenomeno de fraudes con tarjetas de credito que afecta al sistema financiero venezolano. A través del cumplimiento de normas externas, ha clasificado los fraudes en externos e internos para atacar e identificar las debilidades de control. Como parte de los fraudes externos se encuentran los puntos de venta, cuya información viaja automáticamente al sistema central del banco, cada vez que un tarjetahabiente efectúa alguna transacción en los comercios afiliados, repercutiendo esta incidencia en dedicar tiempo a las investigaciones correspondientes.

Como consecuencia de lo anteriormente expresado, las instituciones financieras en concordancia con requerimientos de las diferentes franquicias y entidades reguladoras del sistema financiero, han desarrollado diferentes sistemas de monitoreo de prevención y control para detectar las transacciones presumiblemente falsas. En base a este señalamiento se requiere formular las estrategias para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) en Bancaribe a través de un plan de implementación.

2. INTERROGANTE Y SISTEMIZACIÓN DE LA INVESTIGACIÓN

a. Interrogante de la Investigación

Sobre la base de lo expuesto anteriormente se formula la siguiente interrogante: ¿Cómo debe implantarse un estándar de seguridad de datos en la industria de tarjetas de pago en una institución financiera venezolana aplicando las Buenas Prácticas de la Gerencia de Proyectos?

b. Sistemización de la Investigación

Del Planteamiento de la investigación surgen las siguientes interrogantes:

¿Cuáles son los requisitos que exige el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal?
¿Cuáles son los riesgos por incumplimiento del estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal?
¿Cuáles son las alternativas para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe a través del proyecto "Implementación del Estándar (PCI-DSS)", basado en la Buenas Prácticas de la Gerencia de Proyectos?

3. OBJETIVOS DE LA INVESTIGACIÓN

a. Objetivo General:

Formular la propuesta para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal.

b. Objetivos Específicos

- Determinar los requisitos que exige el estándar de seguridad de datos para la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal.
- Identificar los riesgos por incumplimiento del estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal.
- Evaluar las alternativas para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal.

4. JUSTIFICACIÓN E IMPORTANCIA

En el mercado bancario dentro de la sección de seguridad de la información para la industria de tarjetas de pago, PCI *Security Standards Council*, ofrece las normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS), las cuales se desarrollaron para fomentar y mejorar la seguridad de los datos del

titular de la tarjeta y facilitar la adopción de medidas de seguridad. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los tarjetahabientes. Las PCI DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago.

Entre las entidades que participan se incluyen comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicios, como también todas las demás entidades que almacenan, procesan o transmiten datos del titular de la tarjeta o información de autenticación confidenciales. El estándar PCI-DSS hace hincapié en su protección, esto es con el fin de evitar la usurpación de identidad en el mundo digital y con ella la obtención de información financiera, entre otras. Por ello no solo se debe proteger la información confidencial y sensible, sino todo lo referido a Identificación Personal.

Aplicar el estándar PCI-DSS le permite a las instituciones financieras, reducir el fraude relacionado con las tarjetas de crédito e incrementar la seguridad, lo que brinda confiabilidad y continuidad del negocio, dado que por lo general los tarjetahabientes demandan que el banco al que le confían su dinero, sea líder en seguridad, de tal forma que sus finanzas no se vean afectadas o comprometidas. Bancaribe como institución que procesa, guarda y/o transmite datos de tarjetas debe cumplir con el estándar PCI-DSS, de lo contrario se arriesgaría a perder sus permisos para procesar las tarjetas de crédito.

La investigadora incursiona en la incorporación de la Dirección de Proyectos en la formulación de estrategias para implantar el estándar de seguridad de datos en la industria de tarjetas de pago de la institución bancaria, a través de un proyecto de plan de implementación.

5. ALCANCE Y DELIMITACIÓN DE LA INVESTIGACIÓN

El alcance de este proyecto de investigación llega hasta la formulación de las estrategias para implantar el estándar de seguridad de datos en la industria de tarjetas de pago PCI-DSS en una institución bancaria en Venezuela y no así hasta su aplicación.

CAPITULO II. MARCO TEÓRICO

1. ANTECEDENTES

En relación a la problemática planteada, se tomaron como referencia un conjunto de estudios previos relacionados con el tema objeto de la investigación, que dan soporte bibliográfico y referencial en el desarrollo del mismo.

Beissel (2014). "*Supporting PCI DSS 3.0 Compliance With COBIT 5*". El objetivo de PCI DSS es proteger la confidencialidad de los datos. Confidencialidad, como parte de la tríada de la seguridad de información que incluye la integridad y disponibilidad, es uno de los principales objetivos de seguridad de la información. Las empresas que almacenan, procesan o transmiten datos de titulares de tarjetas o datos de autenticación deben cumplir con requisitos de seguridad de PCI DSS. Mediante el uso de COBIT 5, estas empresas pueden cubrir los requisitos de seguridad PCI DSS que permiten procesos de COBIT 5. Con este artículo se evidencia la importancia de proteger la información de tarjetahabientes.
Palabras clave: COBIT, PCI DSS, Confidencialidad.

Willey, L & White, B (2013), "*Teaching Case. Do you take credit cards? Security and compliance for the credit card Payment Industry*". Un estudio de las pequeñas empresas, mostraron que menos de la mitad acepta tarjetas de crédito. Una razón para no aceptarlas implica la percepción de que el cumplimiento de los requisitos de seguridad de tarjetas de crédito es complicado y costoso. El caso de enseñanza explica los requisitos de cumplimiento de PCI-DSS, lo cual permite a los estudiantes familiarizarse con los temas de seguridad,

en el mundo de pequeñas empresas. La relación de este artículo con el tema de investigación es que el cumplimiento de las normas PCI lo deben cumplir todas las pequeñas empresas procesadoras de Tarjetas de crédito.

Palabras Clave: Requisitos de seguridad, caso de enseñanza, pequeñas empresas, PCI-DSS.

Dennis y Goldman (2013). "*Journal of Internet Law. Data Security Laws and The Cybersecurity Debate*". El incumplimiento de las leyes de seguridad de datos de estado o de las normas PCI podría dar lugar a acciones reguladoras bajo los estatutos del Estado de Nevada. La ley de ciberseguridad de 2012, que crearía "requisitos de desempeño de ciberseguridad" y amenaza cibernética compartiendo estándares entre el sector privado, las empresas operativas, las infraestructuras críticas (por ejemplo, energía); la seguridad de los datos, ley de notificación de incumplimiento de 2012, exigiría a las empresas a mantener medidas para proteger información personal y establecer una ley de notificación de incumplimiento. Este artículo complementa el marco teórico de esta investigación.

Palabras clave: Ciberseguridad, amenaza cibernética, Normas PCI.

TELKOMNIKA (2011), "*Implementing the Payment Card Industry (PCI) Data Security Standard (DSS)".* El incumplimiento de PCI puede dar lugar a multas sustanciales pero lo más importante, una pérdida potencial de negocio. Una razón para el incumplimiento puede ser la cantidad de requisitos. Desde un nivel superior sólo hay 12 requisitos básicos y cada requisito tiene una serie de sub-requisitos resultando en un total de 214 temas a tratar. El aporte de este artículo con este trabajo, es que la implementación del estándar de seguridad de datos para la industria de tarjetas de pago, es un trabajo complejo que requiere de personal altamente capacitado y con amplios conocimientos de seguridad para su implementación.

Palabras Clave: Credit card, data security standards, payment card industry, primary account number.

Zambrano (2011), “Elementos de Seguridad E-Business en la Banca Nacional para Prevenir el Fraude en Medios de Pago Electrónicos” Para Optar al Título de Especialista en Gerencia y Tecnología de las Telecomunicaciones. Tuvo como finalidad analizar el gran problema del comercio electrónico en Venezuela, el cual no es confiable ni seguro, ya que a través de este se realizan grandes cantidades de fraudes. Este trabajo concluye que los proyectos de seguridad de la información avalados por estándares de la industria poseen una inversión considerable para ser ejecutados. Este trabajo aportó a la investigación, la estrecha relación entre el estándar ISO/IEC 27001:2005 con las normas PCI-DSS. Adicionalmente, muestra la interacción de seguridad que debe tener un usuario o cliente de una entidad autorizadora de medios de pago, con los métodos de comercio electrónico.

Palabras clave: ISO/IEC 27001:2005, PCI-DSS, Medios de Pago.

Martínez (2010), “Formulación del Plan de Ejecución (PEP) del Proyecto Ampliación del Estacionamiento del Centro Comercial Valle Arriba Market Center” Para Optar al Título de Especialista en Gerencia de Proyectos. Esta investigación usó la técnica de investigación documental, a través de la consulta de material bibliográfico, planos y procedimientos. Como conclusión el área del conocimiento que alcanzó una menor valoración, cercana al nivel 2 (procesos comunes) fue la gerencia de la calidad. Como recomendación, la organización debe planificar e iniciar un proyecto de elaboración de manuales de procedimiento, formularios y listas de chequeo para la planificación y el control de los proyectos. La relación de este trabajo con el objeto de estudio, se basa específicamente en un aporte conceptual importante para estructurar las bases teóricas así como el marco metodológico.

Palabras clave: PEP, PMBOK, Gerencia de la Calidad

2. BASES TEÓRICAS

En este capítulo se exponen los antecedentes tomados como referencia para la realización de este trabajo de investigación, los conceptos y las referencias teóricas que apoyan la investigación, los fundamentos teóricos que permiten aclarar los conceptos relativos a Implementación del estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) y serán complementados con los conceptos sobre la gerencia de proyectos, los procesos que la conforman y las áreas del conocimiento que serán aplicados específicamente según los objetivos planteados.

A continuación se exponen los conceptos fundamentales que soportan la investigación.

Proyecto:

Un proyecto es un esfuerzo temporal que se lleva a cabo para diseñar un producto, servicio o resultado único. La naturaleza temporal de los proyectos implica que un proyecto tiene un principio y un final definidos. El final se alcanza cuando se logran los objetivos del proyecto, cuando se termina el proyecto porque sus objetivos no se cumplirán o no pueden ser cumplidos, o cuando ya no existe la necesidad que dio origen al proyecto. (PMI, 2013, p. 3).

La definición de ISO 21500:2012 Orientación sobre la Gestión de Proyectos es “conjunto único de procesos que consta de actividades coordinadas y controladas, con fechas de inicio y fin, que se llevan a cabo para lograr objetivos del proyecto.

Gerencia o Dirección de Proyectos:

> La dirección de proyectos es la aplicación de conocimientos, habilidades herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo, Se logra mediante la aplicación e integración adecuada de los 47 procesos de la dirección de proyectos agrupados de manera lógica, categorizados en cinco Grupos de Procesos… (PMI, 2013. p.5).

Ciclo de Vida de un Proyecto: El PMI (2013) define el Ciclo de Vida de un Proyecto como el progreso continuo a través de una serie de etapas de desarrollo, es lo que se debe hacer para producir entregables de un proyecto. En la Tabla Nº1 se enumeran las principales diferencias entre los Ciclos de Vida de Proyecto impulsados por planes y los impulsados por cambios.

Tabla 1: Diferencias entre tipos de Ciclos de Vida de Proyectos

CICLOS DE VIDA IMPULSADOS POR PLANES	CICLOS DE VIDA IMPULSADOS POR CAMBIOS
Ciclos de vida predictivos, tradicionales o en cascada	Ciclos de vida interactivos, incrementales o adaptables (ágiles)
Alcance, cronograma y costos se determinan en las primeras etapas del ciclo de vida del proyecto	Los ciclos de vida incrementales e interactivos incluyen la planificación anticipada del alcance, para permitir estimados de tiempo y costos. Los ciclos de vida adaptables incluyen tiempos y costos fijos, el alcance se define en líneas generales y se perfecciona a medida que los proyectos avanzan

Fuente: PMI (2013)

Procesos de la Dirección de Proyectos: De acuerdo con el PMI (2013), la Dirección de Proyectos se logra mediante la aplicación e integración adecuada de los 47 procesos de la dirección de proyectos agrupados en 5 grupos de procesos.

Grupos de Procesos de la Dirección de Proyectos: A continuación se presentan los cinco grupos de la Dirección de Proyectos descritos por el PMI (2013) e ISO 21500 (2012), con sus procesos, objetivos, entradas, salidas y las áreas del conocimiento que en ellos intervienen.

- **Grupo de Inicio**

Tabla 2: Resumen de Procesos de Inicio PMI

Procesos	1. Desarrollar el Acta de Constitución del Proyecto (GI) 2. Identificar interesados (GIN)
Objetivos	1. Alinear expectativas de los interesados con el propósito del proyecto 2. Darle a los interesados visibilidad sobre el alcance y los objetivos 3. Mostrar como la participación de los interesados en el proyecto pueden asegurar el logro de sus expectativas
Entradas	Caso del negocio, descripción del producto (lo que se supone que debe hacer el proyecto), el aporte que hace el Proyecto al Plan estratégico de la compañía, lista de interesados, restricciones del proyecto, acuerdos pertinentes, estándares de la industria, tendencias del mercado, sistema de control de cambios de la compañía, procesos y procedimientos de la organización, relaciones previas con el patrocinador del proyecto, plantillas de proyectos anteriores, estimaciones históricas, Estructura de Desglose de Trabajo (EDT/WBS) históricas, lecciones aprendidas de proyectos anteriores, situación actual de la empresa, comprensión del futuro de la empresa, comprensión de la cultura de la compañía, lista de posibles miembros del equipo
Salidas	Acta de Constitución del Proyecto y Registro de Interesados del Proyecto
Área del Conocimiento	1. Gestión de Integración (GI) 2. Gestión de los Interesados (GIN)

Fuente: PMI (2013)

Tabla 3: Resumen de Procesos de Inicio ISO 21500

Procesos	1. Desarrollar el Acta de Constitución del Proyecto (I) 2. Identificar las partes interesadas (PI) 3. Establecer el equipo del Proyecto (R)
Entradas	Casos de Negocio, Proyecto nuevo, Contado, Enunciado de trabajo, Documentación de Fase previa,
Salidas	Acta de Constitución del Proyecto
Grupos de Materia	Integración (I) Parte Interesada (PI) Recurso (R)

Fuente: ISO 21500 (2012)

- **Grupo de Planificación**

Tabla 4: Resumen de Procesos de Planificación PMI

Procesos	1. Desarrollar el Plan para la Dirección del Proyecto (GI) 2. Planificar la Gestión del Alcance (GA) 3. Recopilar Requisitos (GA) 4. Definir el Alcance (GA) 5. Crear la EDT (GA) 6. Planificar la Gestión del Cronograma (GT) 7. Definir las Actividades (GT) 8. Secuenciar las Actividades (GT) 9. Estimar los Recursos de las Actividades (GT) 10. Estimar la Duración de las Actividades (GT) 11. Desarrollar el Cronograma (GT) 12. Planificar la Gestión de los Costos (GC) 13. Estimar los Costos (GC) 14. Determinar el presupuesto (GC) 15. Planificar la Gestión de la Calidad (GCA) 16. Planificar la Gestión de los Recursos Humanos (GRH) 17. Planificar la Gestión de las Comunicaciones (GCO) 18. Planificar la Gestión de los Riesgos (GR) 19. Identificar los Riesgos (GR) 20. Realizar análisis cualitativo de Riesgos (GR) 21. Realizar análisis cuantitativo de Riesgos (GR) 22. Planificar respuesta a los Riesgos (GR) 23. Planificar la Gestión de Adquisiciones (GAD) 24. Planificar la Gestión de Interesados (GIN)
Objetivos	1. Establecer el alcance total del esfuerzo 2. Definir y refinar los objetivos 3. Desarrollar la línea de acción requerida para alcanzar dichos objetivos
Entradas	Acta de Constitución del Proyecto, registro de interesados, factores ambientales de la empresa, activos de los procesos de la organización
Salidas	Plan para la Dirección de Proyectos y documentos del Proyecto
Áreas del conocimiento	1. Gestión de Integración (GI) 2. Gestión del Alcance (GA) 3. Gestión del Tiempo (GT) 4. Gestión de los Costos (GC) 5. Gestión de la Calidad (GCA) 6. Gestión de los Recursos Humano (GRH) 7. Gestión de las Comunicaciones (GCO) 8. Gestión de los Riesgos (GR) 9. Gestión de las Adquisiciones (GAD) 10. Gestión de Interesados (GIN)

Fuente: PMI (2013)

Tabla 5: Resumen de Procesos de Planificación ISO 21500

Procesos	Desarrollar los Planes del Proyecto (I) Definir el Alcance (A) Crear la Estructura de Desglose de Trabajo (A) Definir las Actividades (A) Estimar los Recursos (R) Definir la Organización del Proyecto (R) Secuenciar las actividades (T) Estimar la duración de las Actividades (T) Desarrollar el cronograma (T) Estimar los costos (C) Desarrollar el presupuesto (C) Identificar los Riesgos (RI) Evaluar los Riesgos (RI) Planificar la Calidad (CAL) Planificar las Adquisiciones (AD) Planificar las Comunicaciones (CO)
Entradas	Acta de Constitución del Proyecto, Registro de Partes Interesadas, Cambios Aprobados, Lecciones Aprendidas de Proyectos Previos
Salidas	Planes de Proyecto, Registro de Riesgos, para la Dirección de Proyectos y documentos del Proyecto
Grupos de Materia	Integración (I) Alcance (A) Recursos (R) Tiempo (T) Costo (C) Riesgo (RI) Calidad (CAL) Adquisiciones(AD) Comunicación (CO)

Fuente: ISO 21500 (2012)

- **Grupo de Ejecución (PMI) e Implementación (ISO)**

Tabla 6: Resumen de Procesos de Ejecución PMI

Procesos	Dirigir y Gestionar el Trabajo del Proyecto (GI) Realizar el Aseguramiento de la Calidad (GCA) Adquirir el equipo del Proyecto (GRH) Desarrollar el Equipo del Proyecto (GRH) Dirigir el Equipo del Proyecto (GRH) Gestionar las Comunicaciones (GC) Efectuar las Adquisiciones (GAD) Gestionar la Participación de los Interesados (GIN)
Objetivo	Completar el trabajo definido en el plan para la dirección del proyecto a fin de cumplir con las especificaciones del mismo
Entradas	Última revisión del Plan para la Dirección de Proyecto, factores ambientales de la empresa, activos de los procesos de la organización, métricas de calidad, mediciones de control de calidad, registros de interesados, estrategias de gestión de interesados, registro de incidentes, criterios de selección de proveedores, lista de vendedores calificados, documentos de la adquisición, documentos del proyecto, decisiones de hacer o comprar
Salidas	Entregables, trabajo del proyecto terminado, objetivos del proyecto cumplidos, información sobre el desempeño del trabajo, actualizaciones del Plan para la Dirección del Proyecto, actualizaciones a los documentos del proyecto, solicitudes de cambio, asignación de personal al proyecto, calendario de recursos, evaluaciones de desempeño del equipo, actualizaciones a los factores ambientales de la empresa, actualizaciones de los activos de los procesos de la empresa, solicitudes de cambio, vendedores seleccionados, adjudicación del contrato de adquisición
Áreas del conocimiento	Gestión de la Integración (GI) Gestión de la Calidad (GCA) Gestión de los Recursos Humanos (GRH) Gestión de las Comunicaciones (GC) Efectuar las adquisiciones (GAD) Gestión de los Interesados (GIN)

Fuente: PMI (2013)

Tabla 7: Resumen de Procesos de Implementación ISO 21500

Procesos	Dirigir el Trabajo del Proyecto (I) Gestionar las partes interesadas (PI) Desarrollar el equipo del Proyecto (I) Tratar los riesgos (RI) Realizar el Aseguramiento de la Calidad (CA) Seleccionar los proveedores (AD) Distribuir la información (CO)
Entradas	Planes de proyecto, Registro de riesgos, Cambios aprobados, Informes de Progreso
Salidas	Lecciones aprendidas, Cambios requeridos, Registro de problemas, Datos de progreso
Grupos de Materia	Integración (I) Parte Interesada (PI) Recurso (R) Riesgo (RI) Calidad (CA) Adquisiciones (AD) Comunicación (CO)

Fuente: ISO (2012)

- **Grupo de Monitoreo y Control**

Tabla 8: Resumen de Procesos de Monitoreo y Control PMI

Procesos	Monitorear y Controlar el Trabajo del Proyecto (GI) Realizar el Control Integrado de Cambios (GI) Validar el Alcance (GA) Controlar el Alcance (GA) Controlar el Cronograma (GT) Controlar los Costos (GC) Controlar la Calidad (GCA) Controlar las Comunicaciones (GCO) Controlar los Riesgos (GR) Controlar las Adquisiciones (GAD) Controlar la Participación de los Interesados (GIN)
Objetivo	Rastrear, analizar y dirigir el progreso y desempeño del proyecto, para identificar áreas en las que el plan requiera cambios y para iniciar los cambios correspondientes
Entradas	Plan para la Dirección de Proyecto, Informes de desempeño del proyecto, factores ambientales de la empresa, activos de los procesos de la organización, documentación de requisitos, matriz de rastreabilidad de requisitos, entregables, información sobre el desempeño del trabajo, activos de los procesos de la organización, cronograma del proyecto, registros de financiamiento del proyecto, métricas de calidad, listas de control de calidad, solicitudes de cambio aprobadas, registro de riesgos, documentos de la adquisición, contrato
Salidas	Solicitudes de cambio, actualizaciones del Plan para la Dirección del Proyecto, actualizaciones de documentos del proyecto, actualizaciones al estado de solicitudes de cambio, entregables aceptados, mediciones de desempeño del trabajo, actualizaciones de los activos de los procesos de la organización, proyecciones del presupuesto, mediciones de control de calidad, cambios validados, entregables validados, informes de desempeño, actualizaciones al registro de riesgos
Áreas del conocimiento	Gestión de la Integración (GI) Gestión del Alcance (GA) Gestión del Tiempo Gestión de los Costos Gestión de la Calidad (GCA) Gestión de las Comunicaciones (GCO) Gestión de los Riesgos (GR) Gestión de las Adquisiciones (GAD) Gestión de los Interesados (GIN)

Fuente: PMI (2013)

Tabla 9: Resumen de Procesos de Control ISO 21500

Procesos	Controlar el Trabajo del Proyecto (I) Controlar los cambios (I) Definir las actividades (A) Controlar los recursos (R) Gestionar el equipo del Proyecto (R) Controlar el cronograma (T) Controlar los Costos (C) Controlar los Riesgos (RI) Realizar control de Calidad (CA) Administrar los Contratos (AD) Gestionar las Comunicaciones (CO)
Entradas	Planes de Proyecto, Registro de Riesgos, Cambios requeridos, Registros de problemas, Datos de progreso.
Salidas	Cambios aprobados, Informes de progreso, Informes de Avance, Informes de finalización, Acciones correctivas.
Grupos de Materia	Integración (I) Alcance (A) Recursos (R) Tiempo (T) Costo (C) Riesgo (RI) Calidad (CA) Adquisiciones (AD) Comunicación (CO)

Fuente: ISO (2012)

- **Grupo de Procesos de Cierre**

Tabla 10: Resumen de Procesos de Cierre PMI

Procesos	Cerrar Proyecto o Fase (GI) Cerrar las Adquisiciones (GAD)
Objetivo	Finalizar todas las actividades a través de todos los grupos de procesos de la Dirección de Proyectos, a fin de completar formalmente el proceso, una fase del mismo u otras obligaciones contractuales
Entradas	Fase de proyecto completada, proyecto completado, adquisiciones completadas
Salidas	Cierre del Proyecto
Áreas del conocimiento	Gestión de la Integración Gestión de las Adquisiciones

Fuente: PMI (2013)

Tabla 11: Resumen de Procesos de Cierre ISO 21500

Procesos	Cerrar la Fase del Proyecto o Proyecto (I) Recopilar las Lecciones Aprendidas (I)
Entradas	Informes de Avance, Informes de Finalización del Proyecto, Registro de Problemas, Lecciones Aprendidas
Salidas	Informes de Cierre de Proyecto o Fase del Proyecto
Grupos de Materia	Integración

Fuente: ISO (2012)

Áreas de Conocimiento de la Gerencia de Proyectos:

Según el PMI (2013) en su publicación internacional PMBOK, los 47 procesos de la gerencia de proyectos se agrupan a su vez en diez Áreas de Conocimiento las cuales representan un conjunto completo de conceptos, términos y actividades que conforman un ámbito profesional, un ámbito de la dirección de proyectos o un área de especialización. Dichas áreas se utilizan en la mayoría de los proyectos por los equipos de proyecto. Las definiciones que se presentan a continuación corresponden a las contenidas en los términos del PMI (2013).

- **Gestión de la Integración del Proyecto:** Conjunto de actividades para identificar, definir, combinar, unificar y coordinar las diversas actividades de dirección del proyecto. Los procesos de la Gestión de la Integración son:

1. Desarrollar el Acta de Constitución del Proyecto
2. Desarrollar el Plan para la Dirección de Proyectos
3. Dirigir y gestionar el Trabajo del Proyecto
4. Monitorear y controlar el trabajo del Proyecto
5. Realizar el Control Integrado de Cambios
6. Cerrar el Proyecto o Fase.

- **Gestión del Alcance del Proyecto:** Procesos requeridos para garantizar que el proyecto incluye todo el trabajo necesario para completarlo con éxito. Los procesos de la Gestión del Alcance son:

1. Planificar la Gestión del Alcance
2. Recopilar los Requisitos
3. Definir el Alcance
4. Crear la EDT
5. Validar el Alcance
6. Controlar el Alcance

- **Gestión del Tiempo del Proyecto:** Conjunto de actividades requeridas para administrar la finalización del proyecto a tiempo. Los procesos de la Gestión del Tiempo son:

1. Planificar la Gestión del Cronograma
2. Definir las Actividades
3. Secuenciar las Actividades
4. Estimar los Recursos de las Actividades
5. Estimar la Duración de las Actividades
6. Desarrollar el Cronograma
7. Controlar el Cronograma

- **Gestión de los Costos del Proyecto:** Procesos involucrados en planificar, estimar, presupuestar, financiar, obtener financiamiento, gestionar y controlar los costos de modo que se complete el proyecto dentro del presupuesto aprobado. Los procesos de la Gestión de los Costos son:

1. Planificar la Gestión de los Costos
2. Estimar los costos
3. Determinar el presupuesto
4. Controlar los costos

- **Gestión de la Calidad del Proyecto:** Procesos y actividades de la organización ejecutante que determinan responsabilidades, objetivos y políticas de calidad a fin de que el proyecto satisfaga las necesidades requeridas. Los procesos de la Gestión de la Calidad son:

    1. Planificar la Gestión de la Calidad
    2. Realizar el Aseguramiento de la Calidad
    3. Controlar la Calidad

- **Gestión de los Recursos Humanos del Proyecto:** Conjunto de actividades que organizan, gestionan y conducen el equipo del proyecto. Los procesos de la Gestión de los Recursos Humanos son:

    1. Planificar la Gestión de los Recursos Humanos
    2. Adquirir el equipo del Proyecto
    3. Desarrollar el equipo del Proyecto
    4. Dirigir el equipo del Proyecto

- **Gestión de las Comunicaciones del Proyecto:** Conjunto de actividades requeridas para garantizar que la planificación, recopilación, creación, distribución, almacenamiento, recuperación, gestión, control, monitoreo y disposición final de la información del proyecto sean oportunos y adecuados. Los procesos de la Gestión de las Comunicaciones son:

    1. Planificar la Gestión de las Comunicaciones
    2. Gestionar las Comunicaciones
    3. Controlar las Comunicaciones

- **Gestión de los Riesgos del Proyecto:** Conjunto de actividades para llevar a cabo la planificación de la gestión de riesgos, así como la identificación, análisis,

planificación de respuesta y control de los riesgos de un proyecto. Los procesos de la Gestión de Riesgos son:

1. Planificar la Gestión de los Riesgos
2. Identificar los Riesgos
3. Realizar análisis cualitativo de los riesgos
4. Realizar análisis cuantitativo de los riesgos
5. Planificar la respuesta a los Riesgos
6. Controlar los Riesgos

- **Gestión de las Adquisiciones del Proyecto:** Conjunto de actividades necesarias para la compra o adquisición de los productos, servicios o resultados requeridos por fuera del equipo del proyecto. Los procesos de la Gestión de las Adquisiciones son:

1. Planificar la Gestión de Adquisiciones
2. Efectuar las Adquisiciones
3. Controlar las Adquisiciones
4. Cerrar las Adquisiciones

- **Gestión de los Interesados del Proyecto:** Incluye las actividades necesarias para identificar a las personas, grupos u organizaciones que pueden afectar o ser afectadas por el proyecto. Los procesos de la Gestión de Interesados son:

1. Identificar los Interesados
2. Planificar la Gestión de interesados
3. Gestionar la Participación de los Interesados
4. Controlar la participación de los Interesados

Calidad: La definición de Calidad de la norma ISO 9000:2015 Sistemas de Gestión de la Calidad Fundamentos y Vocabulario es: "…el grado en el que un conjunto de características inherentes de un objeto cumple con los requisitos" (Organismo Internacional de Normalización, 2015).De acuerdo con la Norma ISO 9000:2015 el Sistema de Gestión de la Calidad (SGC) comprende las actividades mediante las que la organización identifica sus objetivos y determina los procesos y recursos requeridos para lograr los resultados deseados. (Organismo Internacional de Normalización, 2015).

La certificación de un SGC es un proceso mediante el cual un organismo acreditado, otorga el reconocimiento oficial (con un certificado) de que un SGC cumple con los requisitos de un estándar. ISO 9001 es estándar de Sistemas de Gestión de la Calidad reconocido internacionalmente, basado en los principios de Gestión de Calidad están resumidos en las Tablas N° 13, 14, 15, 16,17, 18 y 19. La versión de la norma ISO 9001:2015 publicada el 23 de septiembre del 2015, tiene una estructura de alto nivel que incorpora el ciclo Planificar-Hacer-Verificar-Actuar (Ciclo de Deming) y el pensamiento basado en riesgos.

Tabla 12: Resumen de Enfoque al Cliente

Declaración	Es cumplir los requisitos del cliente y tratar de exceder las expectativas del cliente
Base Racional	1. El éxito sostenido se alcanza cuando una organización atrae y conserva la confianza de los clientes 2. Cada aspecto de la interacción del cliente proporciona una oportunidad de crear más valor para el cliente 3. Entender necesidades actuales y futuras de clientes y partes interesadas contribuye al éxito sostenido de la organización
Beneficios Clave	1. Incremento del valor para el cliente 2. Incremento de la satisfacción del cliente 3. Mejora de la fidelización del cliente 4. Incremento de la repetición del negocio 5. Incremento de la reputación de la organización 6. Ampliación de la base de los clientes 7. Incremento de las ganancias y la cuota de mercado
Acciones Posibles	1. Reconocer a clientes directos e indirectos como aquellos que reciben valor de la organización 2. Entender las necesidades y expectativas actuales y futuras de clientes 3. Relacionar los objetivos de la organización con las necesidades y expectativas de los cliente 4. Relacionar objetivos de la organización con las necesidades y expectativas del cliente 5. Comunicar las necesidades y expectativas del cliente a través de la organización 6. Planificar, diseñar, desarrollar, producir, entregar y dar soporte a los productos y servicios para cumplir las necesidades y expectativas del cliente 7. Medir y realizar el seguimiento de la satisfacción del cliente y tomar las acciones adecuadas 8. Determinar y tomar las acciones sobre necesidades y expectativas de las partes interesadas que puedan afectar la satisfacción del cliente 9. Gestionar de manera activa las relaciones con los clientes para lograr el éxito sostenido

Fuente: ISO 9000:2015

Tabla 13: Resumen de Liderazgo

Declaración	Los líderes en todos los niveles establecen la unidad de propósito y la dirección y crean condiciones en las que las personas se implican en el logro de los objetivos de la calidad de la organización
Base Racional	La creación de la unidad de propósito y la dirección y gestión de las personas permiten a una organización alinear sus estrategias, políticas, procesos y recursos para lograr sus objetivos
Beneficios Clave	1 Aumento de la eficacia y eficiencia al cumplir los objetivos de la calidad de la organización 2 Mejora en la coordinación de los procesos de la organización 3 Mejora en la comunicación de los altos niveles y funciones de la organización 4 Desarrollo y mejora de la capacidad de la organización y de sus personas para entregar los resultados deseados
Acciones Posibles	1 Comunicar en toda la organización la misión, visión, la estrategia, las políticas y los procesos de la organización 2 Crear y mantener los valores compartidos, la imparcialidad y los modelos éticos para el comportamiento en todos los niveles de la organización 3 Establecer una cultura de la confianza y la integridad 4 Fomentar un compromiso con la calidad en toda la organización 5 Asegurarse de que los líderes en todos los niveles son ejemplos positivos para las personas de la organización 6 Proporcionar a las personas los recursos, la formación, y la autoridad requerida para actuar con responsabilidad y obligación de rendir cuentas 7 Inspirar, fomentar y reconocer la contribución de las personas

Fuente: ISO 9000:2015

Tabla 14: Compromiso de las Personas

Declaración	Las personas competentes empoderadas y comprometidas en toda la organización son esenciales para aumentar la capacidad de la organización para generar y proporcionar valor
Base Racional	Para gestionar una organización de manera eficaz y eficiente, es importante respetar e implicar activamente a todas las personas en todos los niveles. El reconocimiento, el empoderamiento y la mejora de la competencia facilitan el compromiso de las personas en el logro de los objetivos de la calidad de la organización
Beneficios Clave	1 Mejora de la comprensión de los objetivos de la calidad de la organización por parte de las personas de la organización y aumento de la motivación para lograrlos 2 Aumento de la participación activa de las personas en las actividades de mejora 3 Aumento en el desarrollo, iniciativa y creatividad de las personas 4 Aumento de la satisfacción de las personas 5 Aumento de la confianza y colaboración en toda la organización 6 Aumento de la atención a los valores compartidos y a la cultura de la organización
Acciones Posibles	1 Comunicarse con las personas para promover la comprensión de la importancia de su contribución individual 2 Promover la colaboración en toda la organización 3 Facilitar el diálogo abierto y que se compartan los conocimientos y la experiencia 4 Empoderar a las personas para determinar las restricciones que afectan el desempeño y para tomar iniciativas sin temor 5 Reconocer y agradecer la contribución, el aprendizaje y las mejoras de las personas 6 Posibilitar la autoevaluación del desempeño frente a objetivos personales 7 Realizar encuestas para evaluar la satisfacción de las personas, comunicar los resultados y tomar las acciones adecuadas

Fuente: ISO 9000:2015

Tabla 15: Enfoque a Procesos

Declaración	Se alcanzan resultados coherentes y previsibles de manera más eficaz y eficiente cuando las actividades se entienden y gestionan como procesos interrelacionados que funcionan como un sistema coherente
Base Racional	El SGC consta de procesos interrelacionados. Entender como este sistema produce los resultados permite a una organización optimizar el sistema y su desempeño
Beneficios Clave	1 Aumento de la capacidad para centrar esfuerzos en los procesos clave y en las oportunidades de mejora 2 Resultados coherentes y previsibles mediante un sistema de procesos alineados 3 Optimización del desempeño mediante la gestión eficaz del proceso, el uso eficiente de los recursos y la reducción de las barreras interdisciplinarias 4 Posibilidad de que la organización proporcione confianza a las partes interesadas en lo relativo a su coherencia, eficacia y eficiencia
Acciones Posibles	1 Definir los objetivos del sistema y de los procesos necesarios para lograrlos 2 Establecer la autoridad, la responsabilidad y la obligación de rendir cuentas para la gestión de los procesos 3 Entender las capacidades de la organización y determinar las restricciones de recursos antes de actuar 4 Determinar las interdependencias del proceso y analizar el efecto de las modificaciones a los procesos individuales sobre el sistema con un todo 5 Gestionar los procesos y sus interrelaciones como un sistema para lograr los objetivos de la calidad de la organización de una manera eficaz y eficiente 6 Asegurarse de que la información necesaria está disponible para operar y mejorar los procesos y para realizar el seguimiento, analizar y evaluar el desempeño del sistema global 7 Gestionar los riesgos que pueden afectar a las salidas de los procesos y a los resultados globales del SGC

Fuente: ISO 9000:2015

Tabla 16: Resumen de Mejora

Declaración	Las organizaciones con éxito tienen un enfoque continuo hacia la mejora
Base Racional	La mejora es esencial para que una organización mantenga los niveles actuales de desempeño, reacciones a los cambios en sus condiciones internas y externas y cree nuevas oportunidades
Beneficios Clave	Mejora del desempeño del proceso, de las capacidades de la organización y de la satisfacción del cliente Mejora del enfoque en la investigación y la determinación de la causa raíz, seguido de la prevención y de las acciones correctivas Aumento de la capacidad de anticiparse y reaccionar a los riesgos y oportunidades internas y externas Mayor atención tanto a la mejora progresiva como a la mejora abrupta Mejor uso del aprendizaje para la mejora Aumento de la promoción de la innovación
Acciones Posibles	1 Promover el establecimiento de objetivos de mejora en todos los niveles de la organización 2 Educar y formar a las personas en todos los niveles sobre cómo aplicar herramientas básicas y metodologías para lograr objetivos de mejora 3 Asegurarse de que las personas son competentes para promover y completar los proyectos de mejora exitosamente 4 Desarrollar y desplegar procesos para implementar los proyectos de mejora en toda la organización 5 Realizar seguimiento, revisar y auditar la planificación, la implementación, la finalización y los resultados de los proyectos de mejora 6 Integrar las consideraciones de la mejora en el desarrollo de productos, servicios y procesos nuevos o modificados 7 Reconocer y admitir la mejora

Fuente: ISO 9000:2015

Tabla 17: Toma de decisiones basada en la evidencia

Declaración	Las decisiones basadas en el análisis y la evaluación de datos e información tiene mayor probabilidad de producir los resultados deseados
Base Racional	La toma de decisiones puede ser un proceso complejo y siempre implica cierta incertidumbre, con frecuencia implica múltiples tipos y fuentes de entradas, así como la interpretación que pueda ser subjetiva. Es importante entender las relaciones de causa y efecto y las consecuencias potenciales no previstas. El análisis de los hechos, las evidencias y los datos conduce a una mayor objetividad y confianza en la toma de decisiones
Beneficios Clave	1 Mejora de los procesos de toma de decisiones 2 Mejora de la evaluación de desempeño del proceso y de la capacidad de lograr objetivos 3 Mejora de la eficacia y eficiencia operativas 4 Aumento de la capacidad de revisar, cuestionar y cambiar opiniones y las decisiones 5 Aumento de la capacidad de demostrar la eficacia de las decisiones previas
Acciones Posibles	1 Determinar, medir y hacer el seguimiento de los indicadores clave para mostrar el desempeño de la organización 2 Poner a disposición de las personas pertinentes todos los datos necesarios 3 Asegurarse de que los datos y la información son suficientemente precisos, fiables y seguros 4 Analizar y evaluar los datos y la información utilizando métodos adecuados 5 Asegurarse de que las personas son competentes para analizar y evaluar los datos según sea necesario 6 Tomar decisiones y tomar acciones basadas en la evidencia, equilibrando la experiencia y la intuición

Fuente: ISO 9000:2015

Tabla 18: Gestión de las Relaciones

Declaración	Para el éxito sostenido, las organizaciones gestionan sus relaciones con las partes interesadas pertinentes, tales como los proveedores
Base Racional	Las partes interesadas pertinentes influyen en el desempeño de la organización. Es más probable lograr el éxito sostenido cuando la organización gestiona las relaciones con sus partes interesadas para optimizar el impacto de su desempeño. Es particularmente importante la gestión de las relaciones con la red de proveedores y socios
Beneficios Clave	1 Aumento del desempeño de la organización y de sus partes interesadas pertinentes respondiendo a las oportunidades y restricciones relacionadas con cada parte interesada 2 Entendimiento común de los objetivos y los valores entre las partes interesadas 3 Aumento de la capacidad de crear valor para las partes interesadas compartiendo los recursos y la competencia y gestionando los riesgos relativos a la calidad 4 Una cadena de suministro bien gestionada que proporciona un flujo estable de productos y servicios
Acciones Posibles	1 Determinar las partes interesadas pertinentes 2 Determinar y priorizar las relaciones con las partes interesadas que es necesario gestionar 3 Establecer relaciones que equilibren las ganancias a corto plazo con las consideraciones a largo plazo 4 Reunir y compartir la información, la experiencia y los recursos con las partes interesadas pertinentes 5 Medir el desempeño y proporcionar retroalimentación del desempeño a las partes interesadas, para aumentar las iniciativas de mejora 6 Establecer actividades de desarrollo y mejora colaborativas con los proveedores, los socios y otras partes interesadas 7 Fomentar y reconocer las mejoras y los logros de proveedores y socios

Fuente: ISO 9000:2015

Seguridad de la Información: Según Maiwald (2003), la seguridad de la información se define como las “medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso de conocimientos, hechos, datos o capacidades”.(p.4). Según la ISO/IEC 27000-2014, la seguridad de información se define como “Preservación de la confidencialidad, integridad y disponibilidad de la información. Además, otras propiedades, como autenticidad, responsabilidad, no repudio y confiabilidad, también pueden estar involucradas”. (p.4).

La seguridad de la información ayuda a identificar los riesgos y las amenazas a las que están expuestas las organizaciones, en qué medida las pueden afectar y cómo se pueden minimizar. Además permite establecer pautas y procedimientos en caso que se produzca algún desastre. Al mismo tiempo, resulta oportuno mencionar que muchas veces los fallos de seguridad son ocasionados por la errónea percepción de que si la seguridad física está razonablemente asegurada, no tiene por qué haber problemas. O que protegiendo únicamente las aplicaciones y las bases de datos ya está garantizada la seguridad.

Con esos supuestos se dejan desprotegidas muchas áreas de la organización, muchos activos de información que pueden ser fácilmente dañados o destruidos, ya que no se han tenido en cuenta todos los aspectos de la seguridad de la información: la seguridad física, la seguridad lógica y las medidas organizativas. (INTECO, 2010).

Estándares de seguridad de la información para la industria de tarjetas de pago:

Se debe analizar la implementación del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS), el cual tiene como objetivo principal mejorar el nivel de seguridad que promueve un entorno seguro de pago, permitiendo encontrar una solución que satisfaga el escenario expuesto en el planteamiento del problema. Evidentemente las normas se rigen a nivel mundial. De este modo el estándar garantiza la existencia de un marco global consistente para la protección de los datos de cuentas bancarias, tarjetas, transacciones y datos de autenticación. (PCI-DSS, V3.2, 2.016)

Es por ello que se aplica a las entidades que participan en los procesos de las tarjetas de pago (comerciantes, instituciones financieras, entidades adquirientes, entidades emisoras, proveedores de servicios y otros) y en general, a toda organización que almacene, procese o transmita datos de cuentas, siendo el número de cuenta (*Primary Account Number, PAN*) el factor que determina la

aplicabilidad. Por consiguiente el estándar incluye los requisitos mencionados a continuación: Administración de Seguridad, Arquitectura de Redes, Diseño de Sotware, Políticas, Procedimientos y otras medidas de protección.

Es importante mencionar, que para poder obtener la certificación se debe cumplir con los requisitos mencionados. En la actualidad PCI-DSS es gestionado, revisado y actualizado por el *PCI Security Standards Council*. A continuación, se observa en la siguiente figura (1), los estandares de seguridad para la industria de tarjetas de pago. (PCI-DSS, V3.2, 2.016)

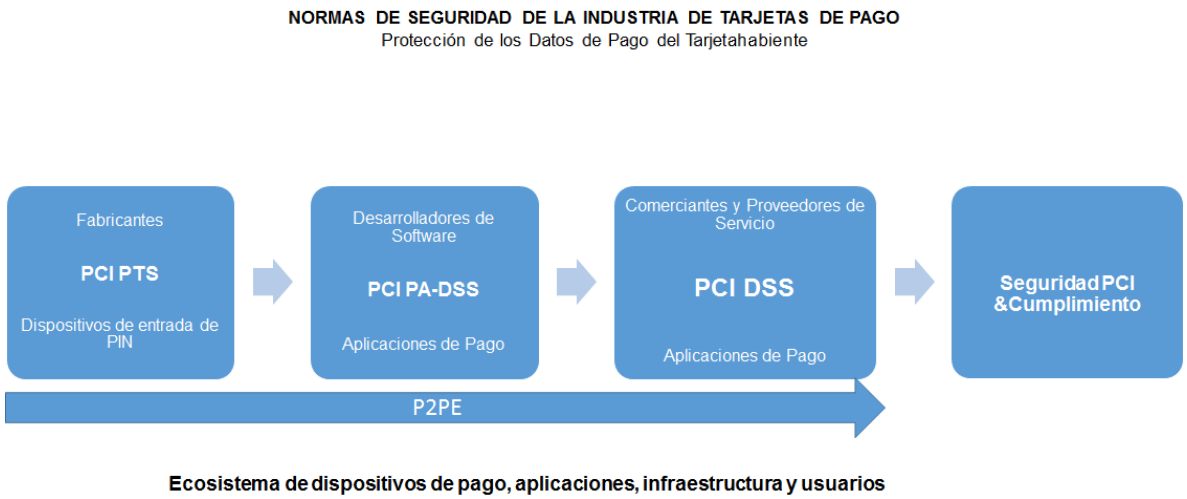

Figura 1: Estándares de Seguridad Industria de Tarjetas de Pago
Fuente: PCI Security Standards Council. V.3.1 (2.013)

El Estándar define los datos de titulares de tarjetas y datos confidenciales de autenticación, como se detalla a continuación:

Tabla 19: Elementos de Datos de: Titulares y Confidenciales de autenticación

Datos de los Tarjetahabientes	Datos confidenciales de autenticación
Número de cuenta principal (PAN)	Los datos completos de la pista (datos de banda magnética, o su equivalente en un chip).
Nombre del titular	Números CAV2/CVC2/CVV2/CID
Fecha de expiración	Pins/bloqueos de PIN
Código de servicio	

Fuente: PCI-DSS, V3.2, 2.016

Tipos de Tarjetas

Según el PCI Security Standards Council, cuando se habla de tarjetas de pago, se debe distinguir entre las tarjetas de debito y de crédito: La tarjeta de crédito es un documento que permite a su titular o beneficiario, adquirir bienes o servicios en establecimientos comerciales, difirendo su pago a crédito. Estos créditos pueden o no incluir tarifas, costos de emisión, costo de estados de cuenta, intereses y comisiones. Mientras que la tarjeta de débito es un documento usado para retirar dinero de un cajero automático y también para realizar pagos de los consumos realizados en locales comerciales. (PCI-DSS, V3.2, 2.016).

Mecanismos de seguridad de las tarjetas de pago

La información confidencial de los datos de autenticación de los tarjetahabientes consta en la banda magnética, código o valor de validación de la tarjeta, y datos del PIN. Estos son los datos que se requieren para que una persona malintencionada pueda generar tarjetas de pago falsas y crear transacciones fraudulentas. En la figura (2) se muestra el reverso y el frente de una tarjeta con la ubicación de los datos del titular de la misma y los datos confidenciales de autenticación. (PCI-DSS, V.3.2, 2.016).

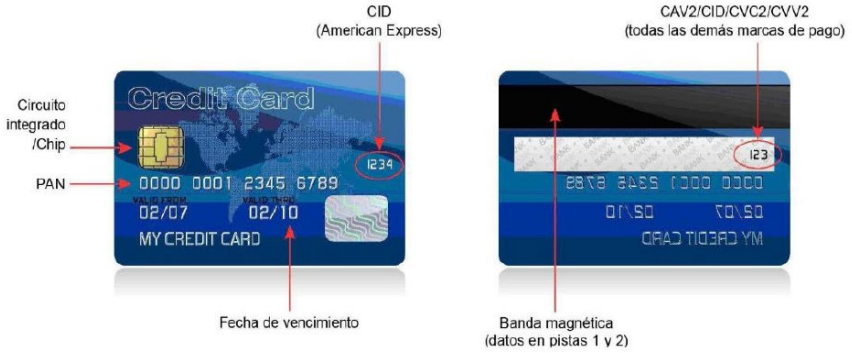

Figura 2: Datos de la Tarjeta
Fuente: PCI Security Standards Council. V.3.1 (2.013)

Norma PCI-DSS:

PCI-DSS es un estándar de seguridad de datos y su objetivo es proteger los datos de titulares de tarjetas, sus requisitos deberán aplicarse en cualquier sistema servidor y/o de la red que contiene este tipo de datos, la norma define controles homogéneos para que las organizaciones puedan implementar contramedidas de manera sistemática y auditables La adopción de dichos controles está enfocada a la protección de los datos del tarjetahabiente, existe información que de acuerdo a lo establecido por la norma puede ser almacenada, como lo es: PAN, nombre del titular, código de servicio y fecha de vencimiento de la tarjeta. (PCI-DSS, 2.016).

Del mismo modo los datos confidenciales de la banda magnética como los códigos de validación y el PIN/PINBLOCK. (Ver tabla 21), no pueden ser almacenados bajo ninguna circunstancia, esto con el fin de reducir el fraude relacionado con tarjetas. (PCI-DSS, 2016).

Tabla 20: Datos de Almacenamiento permitido y no permitido.

		Elemento de datos	Almacenamiento permitido	Hace que los datos de la cuenta almacenado no se puedan leer, según el requisito 3.4
Datos de la cuenta	Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Si	Si
		Nombre del titular de la tarjeta	Si	No
		Código de servicio	Si	No
		Fecha de vencimiento	Si	No
	Datos confidenciales de autenticación	Datos completos de la banda magnética	No	No se pueden almacenar según requisito 3.2
		CAV2/CVC2/CVV2/CID	No	No se pueden almacenar según requisito 3.2
		PIN/Bloqueo de PIN	No	No se pueden almacenar según requisito 3.2

Fuente: Adaptado de (PCI-DSS, V3.2, 2.016)

El estandar PCI-DSS incluye doce (12) requisitos orientados a la creación de políticas, procedimientos y procesos de seguridad de información, se da una descripción general de los doce (12) requisitos. (Ver tabla 22).

Tabla 21: Estándar de seguridad de datos PCI-DSS.

Estándar de Seguridad de Datos de la industria de tarjetas de Pago (PCI-DSS): Descripción general de alto nivel.	
Requisito	**Descripción**
Desarrolle y mantenga redes y sistemas seguros	1.- Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. 2.- No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	3.- Proteja los datos del titular de la tarjeta que fueron almacenados. 4.- Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	5.- Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. 6.- Desarrollar y mantener sistemas y aplicaciones seguros.
Implementar medidas solidas de control de acceso	7.- Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. 8.- Identificar y autenticar el acceso a los componentes del sistema. 9.- Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10.- Rastree y supervise todos los accesos a los recursos de red y a los datos de titular de la tarjeta. 11.- Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	12.- Mantener una política que aborde la seguridad de la información para todo el personal.

Fuente: Adaptado de (PCI-DSS, V3.2, 2.016)

A continuación, se muestra el historial de versiones del Estándar de seguridad de datos para la industria de tarjetas de pago: (Ver tabla 22).

Tabla 22: Historial de Versiones (PCI-DSS).

Versión	Descripción	Fecha
1.0	Se publica la primera versión	Diciembre 2.004
1.1	Se incluyeron mejoras del requerimiento 6.6 para la protección de servidores web publicados en internet.	Septiembre 2.006
1.2	Se reorganiza el estándar incluyendo nuevas columnas que permiten el seguimiento del cumplimiento. Se adicionan controles para el aseguramiento de redes inalámbricas y antivirus.	Octubre 2.008
1.2.1	Se trató como una versión intermedia que corregía algunos errores tipográficos de la versión 1.2.	Julio 2.009
2.0	Se eliminan los formularios de cumplimiento del documento del estándar, que se convierten en formatos independientes. Igualmente, se aclaró que el número de cuenta principal (PAN) es el factor que define la aplicación de PCI DSS.	Octubre 2.010
3.0	Dentro de los cambios se encontraban la necesidad de definir un diagrama de flujo de datos, un inventario de activos en el entorno, se reforzaron los controles vinculados con contraseñas y se estipuló la necesidad de establecer una metodología de pruebas de penetración, así como el reforzamiento de controles de segmentación.	Noviembre 2.013
3.1	Debido a las vulnerabilidades de los protocolos SSL y TLS que estaban siendo explotadas activamente por usuarios maliciosos, se publica la versión 3.1, en donde se excluye a SSL (todas las versiones) y TLS (1.0 y 1.1 bajo algunas excepciones) del concepto de criptografía robusta.	Abril 2.015
3.2	Entre los cambios más significativos se encuentran la realización semestral de pruebas de penetración si se emplea segmentación en el entorno, la definición de responsabilidades de cumplimiento de PCI DSS por parte de la dirección y la revisión trimestral de la aplicación de procedimientos y políticas por parte del personal.	Abril 2.016

Fuente: Adaptado de (PCI-DSS, V3.2, 2.016)

3. BASES LEGALES

Existen diversas leyes y normativas relativas a la Seguridad de la Información y al uso de las tecnologías de la información (TI) que aplican a todo tipo de organizaciones. A continuación se presentan las leyes nacionales y normas internacionales, que tienen correspondencia con la presente investigación.

Constitución Bolivariana de Venezuela: Según gaceta oficial de la República Bolivariana de Venezuela, 5.908. (Extraordinaria), febrero 19, 2.009, regula en su Título VI de manera programática y general el sistema socio económico de la nación. El artículo 117 consagra, entre otros aspectos, que todas las personas tendrán derecho a disponer de bienes y servicios de calidad; así como, a una información adecuada y no engañosa sobre el contenido y características de los productos y servicios que consumen. Visto que este Ente Regulador, debe velar por un desarrollo armónico y ordenado de la red de distribución de los servicios bancarios a los fines que éstos cubran racionalmente las expectativas de crecimiento de la demanda de tales servicios.

Ley del Banco Central de Venezuela: Según artículo 51, de la Gaceta Oficial de la República Bolivariana de Venezuela, 5.606, octubre 18, 2.002. Los bancos e instituciones financieras están en la obligación de suministrar al Banco Central de Venezuela los informes que le sean requeridos sobre su estado financiero o sobre cualquiera de sus operaciones.

Ley General de Bancos y Otras Instituciones Financieras: Según decreto N° 1.526, noviembre 03, 2.001. En su artículo 43**,** "atención a los clientes y depositantes", los bancos, entidades de ahorro y préstamo, y demás instituciones financieras deben mantener sistemas de seguridad adecuados a fin de evitar la comisión de delitos que afecten los depósitos del público; así como brindar atención y oportuna respuesta, tanto a los clientes como a los depositantes que denunciaren cargos no reconocidos u omisiones presentadas en sus cuentas.

Ley de Reforma Parcial de la Ley de Instituciones del Sector Bancario: Según Gaceta Oficial Nº 39.627. Marzo 02, 2011. Decreto Nº 8.079. En su artículo l97, "apropiación de información de los clientes" quien a través de la manipulación informática o mecanismo similar, se apodere o altere documentos, cartas, mensajes de correo electrónico o cualquier otro documento o efecto personal remitido por un banco, institución financiera o casa de cambio, a un cliente o usuario de dicho ente, será penado con prisión de ocho a diez años.

SUDEBAN, Normas relativas a la protección de los usuarios y usuarias de los servicios financieros: Según resolución 083.11, Gaceta Oficial Nº 39.635. Marzo 15, 2011. Artículo 13: Las Instituciones estarán en la obligación de proteger los datos personales de sus clientes. Al respecto, deben administrar la información que reposa en sus archivos y sistemas con la debida confidencialidad, imparcialidad y respeto.

SUDEBAN, Normas para una adecuada administración integral de riesgos: Según resolución 136.03, mayo 29, 2.003. Artículo 3: La administración integral de riesgos debe asegurar la homogeneidad de las herramientas, estructuras organizativas, procesos y sistemas adecuados a la dimensión de la institución financiera; que permita facilitar la gestión global de todos los riesgos que se asuman en cualquier actividad o área geográfica.

Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN): Según resolución 119-10, marzo 09, 2.010. En su artículo 115:"Deberes y obligaciones de las empresas emisoras y operadoras de tarjetas de crédito". No están obligadas a implementar el SIAR LC/FT, pero deberán nombrar un Oficial de Cumplimiento de prevención y control de LC/FT, que adicionalmente a sus funciones exclusivas dentro de la empresa, sirva de enlace para colaborar con la UNIF cuando le sea requerida información a petición de los organismos competentes.

Ley Orgánica de Ciencia, Tecnología e Innovación: Promulgada en Gaceta Oficial Nro. 38.242 de fecha 03 de Agosto de 2005.

Titulo 1: Disposiciones fundamentales

Artículo 1: Objeto del Decreto-Ley: El presente Decreto-Ley tiene por objeto desarrollar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela, organizar el Sistema Nacional de Ciencia, Tecnología e Innovación, definir los lineamientos que orientarán las políticas y estrategias para la actividad científica, tecnológica y de innovación, con la implantación de mecanismos institucionales y operativos para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para la generación, uso y circulación del conocimiento y de impulsar el desarrollo nacional.

Ley cuyo objetivo fundamental de estructurar el Sistema Nacional de Ciencia, Tecnología e Innovación (SNCTI). En este Sistema se integran las instituciones, organismos, entidades y organizaciones universitarias estadales del sector público y privado para que realicen actividades vinculadas al desarrollo científico, tecnológico e innovativo, y adelanten la formación del personal que hace vida en los diferentes entes que lo conforman.

Ley Orgánica de Telecomunicaciones: Promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001 por Decreto N° 1.024 - 10 de febrero de 2001

Título I. Disposiciones Generales.

Artículo 1.- Esta Ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a fin de garantizar el derecho humano de las personas a la comunicación y a la realización de las actividades económicas de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes.

Se excluye del objeto de esta Ley la regulación del contenido de las transmisiones y comunicaciones cursadas a través de los distintos medios de

telecomunicaciones, la cual se regirá por las disposiciones constitucionales, legales y reglamentarias correspondientes.
Ley que da soporte legal al área de las telecomunicaciones, regulando la transferencia de información entre los diferentes organismos, incluyendo las redes de datos.

Ley Especial Contra los Delitos Informáticos: Promulgada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001 por la Asamblea Nacional.
Título I. Disposiciones Generales.
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.
Este instrumento legal concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Cuyo objetivo es proteger los sistemas que utilicen tecnologías de información, así como prevenir y sancionar los delitos cometidos contra o mediante el uso de tales tecnologías.

Ley Sobre Mensajes De Datos y Firmas Electrónicas: Promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001, por Decreto N° 1.024 – 10 de febrero de 2001.
Capítulo I. Objeto y Aplicabilidad Del Decreto -Ley
Artículo 1°: El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas. La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

Esta ley sienta las bases para la regulación del comercio electrónico. Apoyando las transacciones a través de formatos digitales, las transferencias de datos entre organizaciones, el establecimiento de redes inter empresariales, así como la comunicación efectiva entre organismos públicos y privados.

Estándares Internacionales

Payment Card Industry Data Security Standard (PCI-DSS). Normas de seguridad de datos de la industria de tarjetas de pago (PCI-DSS): Se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. Las PCI-DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI-DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicios, como también todas las demás entidades que almacenan, procesan o transmiten CHD (datos del titular de la tarjeta) o SAD (datos de autenticación confidenciales). (PCI Consejo de Normas de Seguridad. En un vistazo, panorama de las Normas, 2010).

ISO/IEC 27000:2014 Tecnología de Información, Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información-Requerimientos. Aprobado y publicado como estándar internacional el 15 de enero de 2014, por la Organización Internacional de Estándares y la Comisión Electrónica Internacional.

ISO 21500:2012 Guía de Dirección de Proyectos. Publicado el año 2012 por el Organismo Internacional de Normalización. Proporciona una guía para la gestión de proyectos y puede ser utilizado por cualquier tipo de organización, incluidas las organizaciones públicas, privadas u organizaciones comunitarias, y para cualquier tipo de proyecto, independientemente de la complejidad, tamaño o duración.

CAPITULO III. MARCO METODOLÓGICO

1. TIPO DE INVESTIGACIÓN

En este capitulo se presentó la metodología que se seguió para dar respuesta al problema planteado, por medio de procedimientos específicos que incluyen las técnicas de observación y recolección de datos. Esta tarea consistió en hacer operativos los conceptos y elementos del objeto que se estudió. Según Balestrini (2006), una vez que fue formulado y definido el problema se procede a describir el tipo de investigación, el cual debe ser el más adecuado y apropiado según los objetivos establecidos. La presente investigación fue basada en el concepto de Investigación Aplicada.

Esto se define en base los siguientes conceptos desarrollados por Tamayo y Tamayo (2009): La investigación aplicada “depende de sus descubrimientos y aportes teóricos, y busca confrontar la teoría con la realidad. Se refiere a resultados inmediatos y se halla interesada en el perfeccionamiento de los individuos implicados en el proceso de la investigación” (p. 43). Consiste en el estudio y aplicación sobre problemas concretos, en circunstancias y características concretas. Además afirma que este tipo de investigación, está orientada a la aplicación inmediata de teorías ya establecidas y no al desarrollo de éstas.

2. DISEÑO DE LA INVESTIGACIÓN

El diseño de investigación aplicado fue de tipo Documental y de Campo, ya que fueron evaluados los registros y documentos existentes para sacar conclusiones, diagnosticar y proponer soluciones (Investigación Documental); al mismo tiempo, fueron recopilados datos a través de entrevistas, juicio de expertos y reuniones

con el personal involucrado en el área de seguridad de información y de proyectos (Investigación de Campo).

3. UNIDAD DE ANALISIS

La unidad de análisis se refiere a qué o quienes se estudia, esto a su vez depende del planteamiento de la investigación y su alcance (Hernandez, Fernández, & Baptista, 2010, p. 172).

En esta investigación, la unidad de análisis en la que fue desarrollada la investigación, fue en la Vicepresidencia de Seguridad de la Información de Bancaribe.

4. TECNICAS Y HERRAMIENTAS DE RECOLECCIÓN E INTERPRETACIÓN

Esta sección describe las herramientas que fueron empleadas para el desarrollo de la presente investigación, técnicas e instrumentos de recolección de datos necesarios para el logro de los objetivos. Utilizando como referencia (Hernandez, Fernández, & Baptista, 2010) se presentan a continuación dichas herramientas de análisis y recolección:

Revisión Bibliográfica: La revisión bibliográfica fue un procedimiento estructurado cuyo objetivo es la localización y recuperación de información relevante, dando como ventaja marcar pautas teóricas sobre el tema, facilitando el entendimiento del mismo. En el caso de esta investigación fue utilizada para la búsqueda de datos históricos, información relacionada a la implementación del estándar de seguridad de datos en las aplicaciones de pago en instituciones bancarias, así como información para desarrollar las bases teóricas.

Entrevistas Estructuradas y No estructuradas: Cuando se realizan preguntas de acuerdo a las respuestas que vayan surgiendo durante la entrevista, con preguntas abiertas y sin orden preestablecido, adquiriendo característica de conversación, se trata de una entrevista no estructurada.

A diferencia de esta, una entrevista estructurada se caracteriza por el empleo de preguntas predefinidas e invariables, es decir, el entrevistador formula las cuestiones tal cual están escritas y el entrevistado tiene que contestarlas según las opciones o alternativas de respuesta; la secuencia y la redacción de las preguntas es prefijada y deja poca libertad al entrevistador para introducir modificaciones; poseen valor psicométrico puesto que permiten comparación de respuestas entre situaciones e individuos.

La entrevista según Balestrini (2006) “es una forma específica de interacción social que tiene por objeto recolectar datos para una investigación.” (p. 123).

Ambas entrevistas se llevaron a cabo, con el fin de orientar la información al desarrollo de elaboración de estrategias, realizando al mismo tiempo en toda oportunidad pertinente, preguntas que surjan en el transcurso de cada consulta.

Juicio de Expertos: Según (Hernandez, Fernández, & Baptista, 2010) “Toda medición o instrumento de recolección de datos debe reunir tres requisitos esenciales: confiabilidad, validez y objetividad.” (p.200) Por tanto, estas tres son cualidades esenciales que deben estar presentes en todos los instrumentos utilizados para la recogida de datos. El Juicio de experto consiste en permitir la participación de personas profesionales y especializadas en un área determinada de interés para la investigación, que tienen la capacidad de emitir sus criterios con respecto a un proyecto, gracias a su amplio conocimiento en el tema pueden suministrar información precisa, acertada, y aportar importantes evaluaciones sobre el mismo.

Para llevar a cabo esta técnica, se contó con las diversas opiniones de los expertos seleccionados como muestra de estudio, los cuales ofrecieron mayor autenticidad.

Reuniones: Las reuniones fueron una herramienta para obtener información bastante efectiva, y tuvo como objetivo agrupar una cantidad de personas con conocimiento en el área de estudio, que intercambiaron información sobre un objetivo en común para llegar a ciertos acuerdos. Se comprobó que cuando se juntan diferentes personas que aportan conocimientos, habilidades y experiencias,

se obtuvo un resultado superior a la suma de las aportaciones de las personas pensando individualmente.

En el caso de este estudio, se tomó la muestra junto a expertos involucrados a proyectos dentro de la Vicepresidencia de seguridad de la información, se convocaron reuniones organizadas y bien estructuradas, que fueron dirigidas al diseño y estrategias para la elaboración de estrategias para implementación del estándar de seguridad de datos en las aplicaciones de pago.

5. FASES DE LA INVESTIGACIÓN

Se definió con anterioridad en el Diseño de la Investigación y las técnicas a utilizar en el análisis y recolección de datos, a la ejecución de dicha recolección, análisis y el procesamiento de la información. Para ello, el desarrollo del presente estudio se realizó bajo un conjunto de fases consecutivas, que se presentan a continuación:

Fase I: Inicio de la investigación. Esta fase comprendió la investigación documental que sirvió de base para el planteamiento del problema, definición de objetivo general y objetivos específicos, marco teórico, marco metodológico, antecedentes.

Fase II: Planificación de la investigación: La segunda fase consistió en establecer las políticas, procedimientos y la documentación necesaria para planificar, desarrollar, gestionar, ejecutar y controlar el cronograma del proyecto. Una vez estudiado profundamente el problema, se adoptó un enfoque más claro para atacarlo. La planificación del cronograma como bien lo señala el PMI (2013), se realizó utilizando el juicio de expertos y reuniones, junto con una buena capacidad de análisis de datos, para concretar la base para el plan. Por supuesto, el *software* más apropiado para presentar la información fue el Project 2013 ©.

Fase III: Ejecución de la investigación: Esta etapa será la más larga en tiempo, y haciendo uso de las técnicas descritas en el punto 4 serán respondidas las interrogantes planteadas en los puntos 2 a y b, y en consecuencia se cumplirá con lo establecido en los objetivos específicos de la investigación.

Fase IV: Cierre de la investigación: La última fase corresponde a la evaluación, conclusiones y recomendaciones del proceso investigativo y a la entrega final del Trabajo Especial de Grado (TEG).

Estructura Desagregada de Trabajo: En la figura 3 se presenta la Estructura Desagregada de Trabajo (EDT/WBS) que se utilizará en esta investigación.

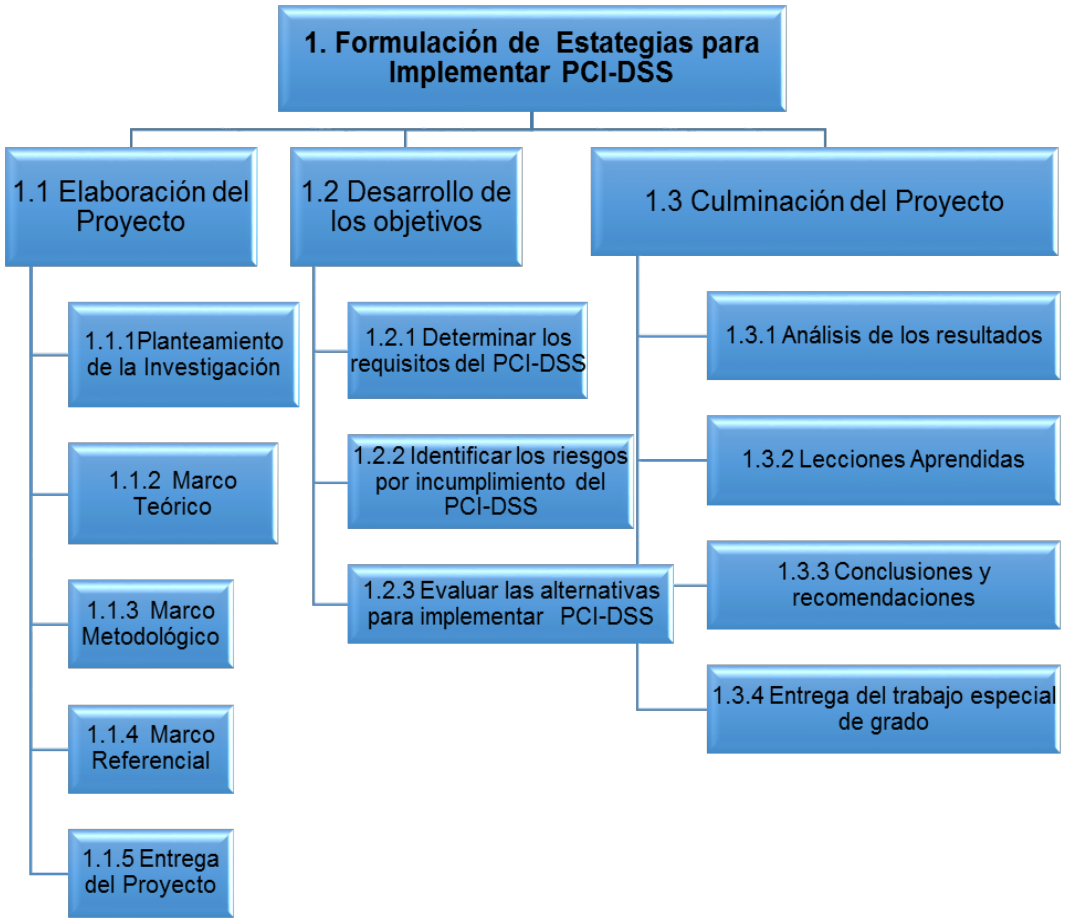

Figura 3: EDT/WBS Trabajo Especial de Grado
FUENTE: Adaptación PMI (2013)

Procedimiento por Objetivos: A continuación se presenta el procedimiento que será aplicado a cada uno de los objetivos específicos planteados en esta investigación y cuyo fin último será formular las estrategias para implementar el estándar de seguridad de datos en la industria de tarjetas de pago de Bancaribe.

Objetivo 1. Determinar los requisitos que exige el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe.

Actividades:

- Revisión de los requisitos que exige el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe.

Técnicas y herramientas: Consulta de expertos, revisión documental.

Entregable: Requisitos exigidos por el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS).

Objetivo 2. Identificar los riesgos por incumplimiento del estándar PCI-DSS.

Actividades:

- Evaluación de los riesgos.
- Realización de entrevistas a los expertos.
- Análisis de la información recopilada
- Redacción del informe de análisis

Técnicas y Herramientas: Entrevistas, revisión documental, evaluación e impacto de riesgos, matriz de probabilidad e impacto, categorización de riesgos, evaluación de la urgencia de los riesgos, estrategias para riesgos positivos y negativos.

Entregable: Informe sobre los riesgos detectados por incumplimiento del estándar PCI-DSS.

Objetivo 3. Evaluar las alternativas para implantar el estándar PCI-DSS.

Actividades:

- Revisión de las áreas del conocimiento según el PMI que apliquen a la investigación.

- Elaboración de las alternativas para implementar el estándar PCI-DSS.

Técnicas y Herramientas: Juicio de expertos, revisión documental.

Entregable: Cronograma de actividades con las alternativas formuladas.

6. OPERACIONALIZACIÓN DE LAS VARIABLES:

A continuación la tabla N° 23 presenta de manera resumida la operacionalización de las variables.

Tabla 23: Operacionalización de las Variables

EVENTO	SINERGIA	VARIABLE	INDICADOR	TÉCNICAS / HERRAMIENTAS	FUENTE
Formular la propuesta para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal.	Determinación de los requisitos exigidos por el estándar PCI-DSS.	Requisitos	Informe de Requisitos	Consulta de expertos Revisión documental	PCI-DSS Información de campo Bases académicas
	Identificación de los riesgos por incumplimiento del estándar PCI DSS	Riesgos	Informe sobre los riesgos detectados	Entrevistas Revisión documental Evaluación e impacto de riesgos Matriz de probabilidad e impacto Categorización de riesgos Evaluación de la urgencia de los riesgos Estrategias para riesgos positivos y negativos	Bases académicas Información de campo PMI(2013)
	Evaluar las alternativas para el proyecto “Plan de Implementación para implantar el estándar de seguridad de datos en la industria de tarjetas de pago de Bancaribe”	Alcance Tiempo Costos Calidad Riesgos Involucrados	Alternativas de Implantación	Juicio de expertos Revisión documental	Bases académicas Información de campo PMI(2013)

7. ASPECTOS ETICOS DE LA INVESTIGACIÓN

Los Aspectos Éticos para esta investigación se sostienen de dos códigos específicos, el primero el Código de Ética Profesional del CIV (1.996) y en segundo lugar el Código de ética y conducta profesional del PMI (2.006).

Código de Ética Profesional del CIV **(1.996),** donde se considera "contrario a la ética" (p. 1) para profesionales de la ingeniería, las siguientes situaciones:

- "Actuar en cualquier forma que tienda a menoscabar el honor, la responsabilidad y aquellas virtudes de honestidad, integridad y veracidad que deben servir de base a un ejercicio cabal de la profesión." (p. 1).
- "Descuidar el mantenimiento y mejora de sus conocimientos técnicos, desmereciendo así la confianza que al ejercicio profesional concede la sociedad." (p. 1).
- "Atentar contra la reputación o los legítimos intereses de otros profesionales, o intentar atribuir injustificadamente la comisión de errores profesionales a otros colegas." (p. 2).
- "Utilizar estudios, proyectos, planos, informes u otros documentos, que no sean el dominio público, sin la autorización de sus autores y/o propietarios." (p. 2).
- "Revelar datos reservados de índole técnico, financiero o profesionales, así como divulgar sin la debida autorización, procedimientos, procesos o características de equipos protegido por patentes o contratos que establezcan las obligaciones de guardas de secreto profesional. Así como utilizar programas, discos, cintas u otros medios de información, que no sea de dominio público, sin la debida autorización de sus autores y/o propietarios, o utilizar sin autorización de códigos de acceso de otras personas, en provecho propio." (p.2).

Código de Ética y Conducta Profesional del PMI **(2.006),** donde destacan las siguientes expectativas entre profesionales de la Gerencia de Proyectos:

- "Únicamente aceptamos aquellas asignaciones que se condicen con nuestros antecedentes, experiencia, habilidades y preparación profesional." (p. 3).

- “Cumplimos los compromisos que se asumen: hacer lo que se dice que se va a hacer.” (p. 3).
- “Cuando cometemos errores u omisiones, se responsabilizan por ellos y los corrigen de inmediato.” (p. 3).
- “Protegemos la información confidencial o de propiedad exclusiva que se les haya confiado.” (p. 3).
- “Nos informamos sobre las normas y costumbres de los demás, y evitar involucrarse en comportamientos que ellos podrían considerar irrespetuosos.” (p. 4).
- “Escuchamos los puntos de vista de los demás y procurar comprenderlos.” (p. 4).
- “Nos comportamos de manera profesional, incluso cuando no se es correspondido de la misma forma.” (p. 4).
- “No nos aprovechamos de nuestra experiencia o posición para influir en las decisiones o los actos de otras personas a fin de obtener beneficios personales a costa de ellas.” (p. 4).
- “Respetamos los derechos de propiedad de los demás.” (p. 4).
- “Demostramos transparencia en el proceso de toma de decisiones.” (p. 5).
- “Revisar constantemente los criterios de imparcialidad y objetividad, y realizar las acciones correctivas pertinentes.” (p. 5).
- “Brindar acceso equitativo a la información a quienes están autorizados a contar con dicha información.” (p. 5).
- “Procuramos que haya igualdad de acceso a oportunidades para aquellos candidatos que sean idóneos.” (p. 5).

CAPITULO IV. MARCO REFERENCIAL

Reseña Institucional Bancaribe Banco Universal

La información sobre la historia del Banco se obtuvo del documento digital: Un Poco de Historia 1954-2014. Bancaribe. PDF interno, publicado en la biblioteca virtual. De igual manera, la visión, misión y valores se obtuvo del documento digital: marco filosófico Bancaribe. PDF interno, publicado en la biblioteca virtual. Y el organigrama fue elaborado con información publicada en la intranet del banco.

Historia:

Un miércoles 03 de Noviembre de 1954, en Puerto Cabello, Nazri David Dao, mejor conocido como N.D.Dao, vio cómo se concretaba el sueño de años: un Banco que realmente atendiera las necesidades de los porteños. La Junta promotora del Banco del Caribe pasó meses vendiendo acciones para reunir el capital necesario para su fundación. La primera oficina estuvo en Puerto Cabello, rápidamente comenzó su expansión estableciendo agencias en: Barquisimeto, Morón, Barinas, Valencia, Maracay, Guanare, San Felipe.

En 1958 que traslada su sede frente a la Plaza España en Caracas. En los años sesenta las computadoras comenzaban a marcar los destinos de las empresas del mundo. Entonces el Banco quiso dar un salto hacia la innovación tecnológica y comenzó a utilizar la computadora 360 de IBM que nos permitió tener nuestros sistemas en línea. Luego se incorporaron las oficinas el interior del país, a través de terminales del tipo IBM 1060 que las interconectaba con el computador central ubicado en la capital.

Entre 1974 y 1981 inauguramos 24 oficinas en el interior del país y en 1977 el Banco decide traspasar las fronteras nacionales y fundar el primer Banco en Curazao, The Caribbean American Bank N.V, hoy Bancaribe Curazao Bank, con el objetivo de internacionalizar al grupo

financiero. En la madrugada del martes 26 de marzo de 1984 fallece ND Dao, nuestro fundador. Si bien su ausencia se sintió en el Banco, paso a ser presidido por Edgar Alberto Dao (hijo mayor de ND) quien tenía cinco años desempeñándose como suplente del Presidente.

A finales de los años 80, el Banco emprendió la reingeniería de procesos para adaptarse a las condiciones del entorno y ser más competitivos. En paralelo a la reingeniería, el Banco trabajó en la fundación, junto con otros bancos, del primer sistema interconectado de cajeros automáticos del país, Suiche 7B y del primer centro operador de tarjetas de crédito, Consorcio Credicard. La década de los 90, se caracterizó por ser la de mayor apertura de oficinas, abrimos 41 oficinas y 13 PABs (Puntos de Atención Bancaribe).

El crecimiento nos impulsó a convertirnos en 1997 en Banco Universal, para lo que se fusionaron: El Fondo de Activos Líquidos del Caribe, la Sociedad Financiera del Caribe y el Banco de Inversiones del Caribe para brindar financiamiento a mediano y largo plazo; así en 1997 se formaliza la alianza estratégica con el Scotiabank, banco Canadiense de amplia trayectoria y fuerte presencia en Latinoamérica. Además firmamos un acuerdo de corresponsalía e intercambio comercial con la Caixa de Galicia.

En 1999, junto con varias organizaciones no gubernamentales, Bancaribe creó al Banco de la Gente Emprendedora, Bangente, única institución de microfinanzas venezolana que, a través de la inclusión financiera, contribuye a cambiar la vida de los microempresarios populares de distintos sectores económicos del país. Tras 15 años de fundada, Bangente ha otorgado cerca de 550 mil créditos. Siguiendo la práctica de velar por los intereses de los clientes, se aprobó la creación de la Oficina del Defensor del Cliente y Usuario Bancaribe.

Se implementó en 2001, como un servicio autónomo. Fue la única en el país hasta que en 2011 Sudeban instruyó que fuera creada en todos los bancos. En el 2004 la evolución del Banco continúa avanzando y el Dr.

Edgar A. Dao decide retirarse de la Presidencia para poner en manos de un banquero honorable y de amplia experticia, el Dr. Miguel Ignacio Purroy, el rumbo de la institución. En el 2006 cambiamos nuestra identidad de marca a Bancaribe, en el 2009 mudamos la sede principal a una torre ubicada en el centro financiero de Caracas: El Rosal.

Al cumplir una década al frente de Bancaribe, el Dr. Miguel Purroy se retira de la Presidencia y le sucede el Dr. Arturo Ganteaume, banquero de renombre y con una clara visión de negocios, quien comienza a dirigir el destino el Banco a partir del 60 aniversario de la institución.

Misión de Bancaribe Banco Universal

Estamos en el negocio de intermediación y distribución de soluciones financieras integrales, para satisfacer oportunamente las necesidades y expectativas de nuestros clientes, construyendo relaciones cercanas y duraderas que generan afinidad y lealtad con la organización.

Visión de Bancaribe Banco Universal

Ser reconocidos como una institución financiera innovadora, sólida y confiable, comprometida con la excelencia y el alto desempeño, lugar de referencia para trabajar y crecer, que contribuye al desarrollo y bienestar de los trabajadores y del país.

Valores de Bancaribe Banco Universal

Vocación de servicio:

Tenemos la mejor disposición para cuidar los intereses y satisfacer las necesidades de nuestros clientes y compañeros de trabajo, para lo cual buscamos crear relaciones cercanas y permanentes.

Espíritu de Equipo:

Nos comprometemos de manera conjunta para lograr las metas empresariales y sociales. A través de la comunión de creencias, valores y propósitos formamos parte de una gran familia en la que reinan actitudes de apoyo mutuo, compenetración, generosidad y lealtad.

Excelencia:

Desarrollamos y mejoramos de manera continua los procesos para incorporar las mejores prácticas de negocio y consolidar una organización de alto desempeño, basada en calidad, agilidad, flexibilidad y eficiencia.

Creatividad e Innovación:

Fomentamos la generación de ideas y propiciamos espacios para la reinvención constante de la organización en procura de alcanzar nuestra misión y visión.

Reconocimiento:

Valoramos el aporte individual y colectivo de nuestro capital humano, cuyos conocimientos, habilidades y conductas construyen día a día el éxito permanente de la Institución.

Respeto:

Basamos nuestras relaciones internas y externas en un trato equitativo, justo, considerado y respetuoso de la individualidad y de los derechos de los demás.

Confianza:

Fomentamos relaciones fundamentadas en la integridad de nuestra gente, en la transparencia de nuestras prácticas de negocio, en la solidez de nuestra institución y en la puesta en acción de valores como la equidad, la honestidad y la solidaridad. Buscamos siempre construir alianzas de beneficio mutuo.

Crecimiento personal y profesional:

Valoramos y promovemos las oportunidades de desarrollo y satisfacción personal, mediante la generación de espacios y actividades que permitan a nuestra gente desplegar todo su potencial humano y profesional.

Transparencia:

Actuamos con altos estándares éticos enmarcados en un modelo de Gobierno Corporativo, que nos permite dejar a la vista nuestras acciones y resultados.

Responsabilidad Social:

Somos un Banco comprometido con el desarrollo sostenible del país, expresado a través del equilibrio entre el crecimiento económico, el bienestar social y la protección del medio ambiente. Apoyamos las iniciativas sociales, educativas y culturales de las comunidades y procuramos el bienestar de nuestros trabajadores.

Organigrama de Bancaribe Banco Universal

A continuación se presenta el organigrama de la VP de Seguridad de Información, específicamente la Gerencia de Gestión de Riesgo, quien es la asignada a realizar el presente trabajo de investigación. (Ver figura 4).

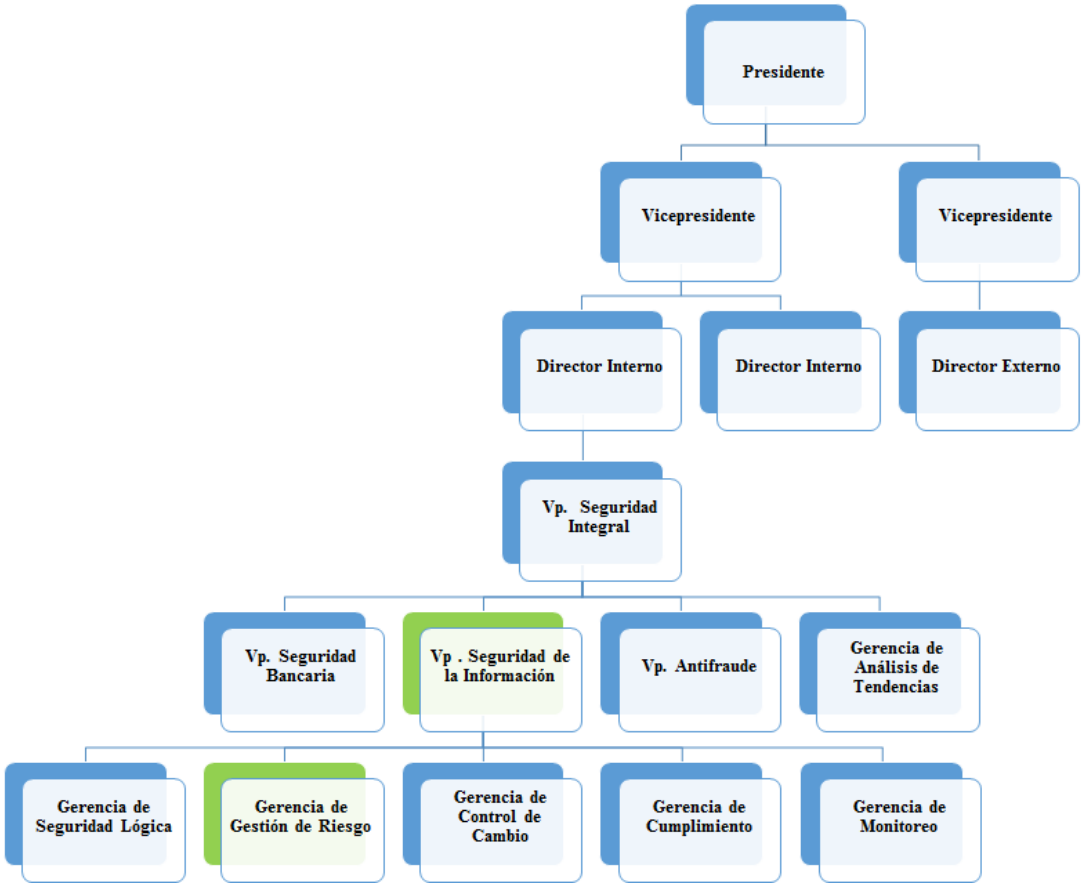

Figura 4: Organigrama Bancaribe Banco Universal/VP Seguridad Integral
Fuente: Intranet Bancaribe 2.016

Hitos Históricos de Bancaribe Banco Universal:

Tabla 24: Hitos históricos de Bancaribe

Año	Hito
1954	Inicio de operaciones en Puerto Cabello.
1955	Se inauguran oficinas en Barquisimeto y Barinas.
1956	Se inauguran dos oficinas en Valencia, dos en Morón y otra más en Puerto Cabello.
1957	Se inauguran nuevas sucursales en las principales ciudades del Centro y Los Llanos del país: San Felipe, Valle de la Pascua, Maracay, Calabozo, San Fernando de Apure, Punto Fijo, Guacara, El Tocuyo, Chivacoa y Guanare.
1958	Abre la primera oficina en Caracas.
1963	Se traslada la sede principal a Caracas.
1977	Se funda a Bancaribe Curaçao Bank, N. V.,el primer banco venezolano off shore ubicado en Curaçao.
1988	Participa en la creación del primer sistema de interconexión de cajeros automáticos en el país, Suiche 7B, y en la fundación del Consorcio Credicard, primer centro operador de tarjetas de crédito del país.
1994	Conjuntamente y a partes iguales con American International Group, participa en el capital de las empresas Seguros Venezuela, S.A. y C. A. Seguros American International.
1996	Emprende, conjuntamente con dos organizaciones locales no gubernamentales y varios entes multilaterales, la creación de Bangente.
1997	Se transforma en Banco Universal mediante la fusión con el Banco de Inversión del Caribe y el Fondo de Activos Líquidos del Caribe. Scotia International Limited, empresa del Grupo Financiero Scotiabank, se incorpora como un importante accionista de Bancaribe. Establece una asociación estratégica con Caixa Galicia, una de las más acreditadas e importantes instituciones financieras de España. Recibe la calificación de la Superintendencia de Bancos y Otras Instituciones Financieras (Sudeban) como una empresa de inversión mixta. Inscribe su capital en el Registro Nacional de Valores y se inicia la cotización de sus acciones en la Bolsa de Valores de Caracas.
1999	Bangente inicia sus operaciones. Crea la Oficina del Defensor del Cliente y Usuario Bancaribe.
2001	Adopta los principios de Wolsfberg (para la prevención del blanqueo del dinero en banca de corresponsales).
2003	Incorpora las mejores prácticas de Gobierno Corporativo, mediante una reforma estatutaria.
2006	Adopta nueva marca e imagen: Bancaribe. Establece un nuevo Modelo de Actuación Comercial.
2009	Estrena su nueva sede principal en la urbanización El Rosal, Chacao, Caracas.
2010	Incorpora la tecnología Chip EMV a sus medios de pago, convirtiéndose en el primer banco en hacerlo con la tarjeta de crédito MasterCard en Venezuela.
2011	Incorpora nuevos productos a su oferta y potencia sus canales de distribución al inaugurar cuatro nuevas oficinas, remodelar otras cinco e instalar 81 cajeros automáticos de última generación.
2012	Logra ubicarse como el banco privado con mayor crecimiento en su segmento.

Fuente: http://www.bancaribe.com.ve/informacion-vital/la-institucion/historia

Red de Agencias Bancarias en Venezuela:

Figura 5: Red de Agencias Bancaribe Banco Universal
Fuente: Pagina Web Bancaribe 2.016 (http://www.bancaribe.com.ve/informacion-vital/canales/oficinas)

CAPITULO V. DESARROLLO DE LOS OBJETIVOS DE LA INVESTIGACIÓN

El presente capítulo presenta los resultados de la investigación, detallando las actividades realizadas para alcanzar cada uno de los objetivos planteados, usando las herramientas de recolección de datos descritas en el Marco Metodológico de este Trabajo Especial de Grado.

Objetivo 1: Determinar los requisitos que exige el estándar de seguridad de datos para la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal

A continuación se detallan los requisitos que exige el estándar de seguridad de datos para la industria de tarjetas de pago, para ello se utilizó el cuestionario de auditoria de la ISO 9001:2015, lo cual constituye el primer objetivo específico de la presente investigación. Ver tabla 25.

Tabla 25: Instrumento de determinación de requerimientos según ISO 9001:2015

			Cumple			
Item	Nro ISO	Requisito	Si	No	Parcialmente	Observaciones
Contexto de la Organización						
1	1.1	El banco se encuentra certificado PCI				
2	1.2	Cantidad de aplicaciones de pago que procesan, almacenan o transmiten datos de titulares de tarjeta				
3	1.3	Las aplicaciones de pago están certificadas PCI-DSS				
4	1.4	Las aplicaciones de pago cumplen los requisitos exigidos en el estándar PCI-DSS				
Control de la Información documentada						
5	2.1	Tiene documentado los procesos de medios de pago junto con los mapas de los flujos relacionados con información de tarjetahabiente				
6	2.2	La infraestructura tecnológica que soporta los procesos de medios de pago está documentada				
Determinación del alcance de los requisitos						
7	3.1	Posee canales de banca o ventas virtuales, para operaciones con tarjeta crédito y débito				
8	3.2	Posee canales de Banca Móvil para servicios que involucren tarjetas débito o crédito				
9	3.3	Tiene proveedores de servicio a los cuales su organización le entrega, le comparte o le permite acceder a Datos de Tarjetahabiente				
Política de seguridad y riesgos						
10	4.1	Existe una política y procedimientos de seguridad de la información				
11	4.2	Ha realizado evaluación de riesgos a los activos de información de los procesos relacionados con información de tarjetahabiente				

Una vez aplicado el instrumento de determinación de requerimientos según ISO 9001:2015 se describen los resultados, en la siguiente tabla:

Tabla 26: Resultados de requerimientos según ISO 9001:2015

			Cumple			
Item	Nro ISO	Requisito	Si	No	Parcialmente	Observaciones
Contexto de la Organización						
1	1.1	El banco se encuentra certificado PCI		x		
2	1.2	Cantidad de aplicaciones de pago que procesan, almacenan o transmiten datos de titulares de tarjeta			x	Son dos (2) aplicaciones de pago
3	1.3	Las aplicaciones de pago están certificada PCI-DSS	x			La otra aplicación está en proceso de certificación
4	1.4	Las aplicaciones de pago cumplen los requisitos exigidos en el estándar PCI-DSS	x			La otra aplicación cumple parcialmente
Control de la Información documentada						
5	2.1	Tiene documentado los procesos de medios de pago junto con los mapas de los flujos relacionados con información de tarjetahabiente			x	Falta actualizar algunos documentos
6	2.2	La infraestructura tecnológica que soporta los procesos de medios de pago está documentada	x			
Determinación del alcance de los requisitos						
7	3.1	Posee canales de banca o ventas virtuales, para operaciones con tarjeta crédito y débito	x			
8	3.2	Posee canales de Banca Móvil para servicios que involucren tarjetas débito o crédito	x			
9	3.3	Tiene proveedores de servicio a los cuales su organización le entrega, le comparte o le permite acceder a Datos de Tarjetahabiente	x			Un solo proveedor de servicio
Política de seguridad y riesgos						
10	4.1	Existe una política y procedimientos de seguridad de la información	x			
11	4.2	Ha realizado evaluación de riesgos a los activos de información de los procesos relacionados con información de tarjetahabiente	x			La evaluación de riesgo se hizo hace más de un año

A continuación se presentan los resultados de cumplimiento de los requisitos exigidos por el estándar de seguridad de datos para la industria de tarjetas de

pago (PCI-DSS), producto de la revisión de la documentación publicada en la Vicepresidencia de Seguridad de la Información, conjunto a las reuniones con los expertos involucrados:

Contexto de la organización: El banco no se encuentra certificado PCI, cuenta con dos (2) aplicaciones de pago que procesan, almacenan o transmiten datos de titulares de tarjeta. De las dos (2) aplicaciones de pago, una (1) está certificada PCI y la otra se encuentra en proceso de certificación. La aplicación que está certificada PCI cumple con todos los requisitos exigidos por el estándar (PA-DSS) y la otra aplicación cumple parcialmente dichos requisitos.

Control de la información documentada: Los procesos de medio de pago se encuentran documentados, junto con los mapas de los flujos relacionados con información de tarjetahabiente, sin embargo no están actualizados. La infraestructura tecnológica que soporta los procesos de medios de pago está documentada y actualizada.

Determinación del alcance de los requisitos: El banco posee canales de banca o ventas virtuales y canales de banca móvil, para operaciones con tarjeta crédito y débito, los cuales formarán parte de la implementación del estándar PCI-DSS. En la actualidad el banco, tiene un (1) proveedor de servicio a los cuales su organización le entrega, le comparte o le permite acceder a Datos de Tarjetahabiente, es importante mencionar que dicho proveedor está certificado PCI.

Políticas de seguridad y riesgo: En la institución bancaria, existe una política y procedimientos de seguridad de la información, por el cual se rige la organización. En el banco se realizó la evaluación de riesgos a los activos de información de los procesos relacionados con información de tarjetahabiente, hace más de un año.

En base a los resultados del cuestionario, se presenta la matriz DAFO de Bancaribe.

Tabla 27: Matriz DAFO de Bancaribe

Fortalezas	Oportunidades
Buen posicionamiento en el mercado nacional	Identificar riesgos que afecten la seguridad de la información de los tarjetahabientes
Goza de la confianza de los clientes, socios y accionistas	Facilitar el gbierno corporativo del banco
Fluidez economica garantizada	Incrementar la confianza de los clientes, socios y accionistas
Personal de seguridad capacitado y comprometido	Proteger la imagen y reputación del banco
Disponibilidad de recursos: tecnicos, humanos y economicos	
Debilidades	**Amenazas**
Falta de personal certificado QSA	Fuga de talento por la situación del país
Carga laboral en el personal de tecnologia	Tasa de inflación en el país variable
Limitaciones en el presupuesto del banco	Persona de tecnología con poca experiencia
Escaza atención a las necesidades de tecnologia	Cambios politicos en el país que afecten las regulaciones bancarias

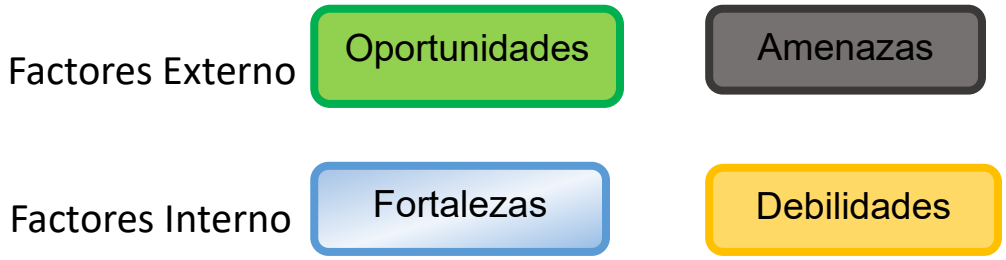

Figura 6: Matriz DAFO
Fuente: Seguridad de la Información (Bancaribe 2017)

A continuacion se señalan las estrategias que se pueden extraer del analisis CAME:

Tabla 28: Análisis CAME de Bancaribe

Factores		Fortalezas	Debilidades
Internos	Externos		
Oportunidades		Estrategia Ofensiva (FO)	Estrategia de Reorientación (DO)
		Campañas de captación de nuevos clientes	Desarrollo de sistemas de fidelización de clientes
		Aprovechar los recursos del banco para invertir en tecnologia de vanguardia	Realizar campañas de incentivos para el personal capacitado y comprometido
		Seguimiento de los riesgos que afecten la seguridad de los tarjetahabientes	Equilibrar las cargas de trabajo en el personal de tecnología
Amenazas		Estrategia Defensiva (FA)	Estrategia de Supervivencia (DA)
		Buscar alianzas con empresas outsorcing de personal de TI	Implementar planes de formación para el personal de TI y Seguridad del banco
		Afrontar subidas de precios por la situación país	Explorar nuevas tecnologías
		Capacitar al personal constantemente	Lanzar productos innovadores al mercado

Una vez analizada la matriz CAME, se procede a priorizar las estrategias de acuerdo a su impacto y prioridad y se establece su plan de acción. Como se observa en la siguiente tabla.

Tabla 29: Priorización de Estrategias CAME de Bancaribe

Estrategia	Impacto	Prioridad de Atención	Acción
Seguimiento de los riesgos que afecten la seguridad de los tarjetahabientes	Alto	Muy alta	Realizar planes de mitigación de los riesgos a corto plazo
Aprovechar los recursos del banco para invertir en tecnologia de vanguardia	Medio	Medio	Invertir en infraestructura tecnologica
Desarrollo de sistemas de fidelización de clientes	Medio	Medio	Realizar campañas e incentivos dirigida a los clientes del banco
Campañas de captación de nuevos clientes	Medio	Medio	Establecer alianzas con empresas para aperturas de cuentas nomina a sus empleados
Implementar planes de formación para el personal de TI y Seguridad del banco	Medio	Medio	Implementar planes de capacitación para los empleados de TI y Seguridad
Realizar campañas de incentivos para el personal capacitado y comprometido	Bajo	Bajo	En conjunto con capital humano y en base a los resultados de las evaluaciones, incentivar con bonos adicionales al personal capacitado y comprometido
Buscar alianzas con empresas outsorcing de personal de TI	Bajo	Bajo	Mantener las que se tienen actualmente y buscar nuevas empresas
Equilibrar las cargas de trabajo en el personal de tecnología	Bajo	Bajo	Medir las capacidades de los recursos en base a la cantidad de trabajo asignado
Lanzar productos innovadores al mercado	Bajo	Bajo	Desarrollar nuevos productos que los diferencien de la competencia
Afrontar subidas de precios por la situación país	Bajo	Bajo	Mantener buenas relaciones con los proveedores
Capacitar al personal constantemente	Bajo	Bajo	Realizar adiestramientos frecuentemente al personal
Explorar nuevas tecnologías	Bajo	Bajo	Innovar con aplicaciones en la nube

Objetivo 2: Identificar los riesgos por incumplimiento del estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal.

Una vez identificados los requisitos exigidos por el estándar, se utilizó la metodología de administración de riesgo de seguridad de información (MARSI), la cual es propia de la VP de seguridad de información del banco. Se aplicaron como herramientas de recolección de datos: el juicio con los expertos, las reuniones, entre otros.

Tabla 30: Matriz de Riesgo

ID	Descripción del Riesgo	Tipo de Riesgo	Probabilidad (P)	Impacto (I)	Criticidad (C)
1.1	Imposibilidad de trabajar con un adquiriente. En caso que un comercio no cumpla con el estándar, dicho adquiriente puede finalizarle su servicio al banco	Reputacional	Baja	Alto	Medio
1.2	Pago de multas en caso de fraudes: Dichas multas pueden ser impuestas por las marcas de pago y por los adquirientes.	Legal	Media	Alto	Alto
1.3	Pago de indemnizaciones a clientes afectados por fraude relacionado a PCI	Financiero	Baja	Alto	Medio
1.4	Costos asociados de una investigación forense, que debe ser ejecutada por un Investigador forense certificado por la industria de tarjetas de pago(PCI-PFI) únicamente	Financiero	Alta	Alto	Alto
1.5	Problemas derivados de mala prensa y pérdida de imagen de cara a clientes	Reputacional	Baja	Alto	Medio
1.6	Costos asociados a la implementación de los controles de PCI DSS de forma correctiva después de un incidente de seguridad, siempre serán mucho más altos que si se implementan de forma preventiva.	Financiero	Alta	Alto	Alto
1.7	Posibilidad de problemas legales derivados del incumplimiento colateral de otras leyes o normativas	Legal	Baja	Medio	Medio
1.8	Prohibición de procesamiento de tarjetas de crédito Mastercard o Visa	Reputacional	Baja	Alto	Alto
1.9	Prohibición de procesamiento de tarjetas internacionales y/o nacionales	Reputacional	Baja	Alto	Alto

Tipos de Riesgo
Financieros
Legal
Reputacional
Operacional
Tecnológico
Riesgo de Mercado y Liquidez
Riesgo de Crédito

Figura 7: Tipos de Riesgo
Fuente: Seguridad de la Información

	Riesgo Alto. Requiere medidas preventivas urgentes. Se requiere monitoreo constante.
	Riesgo Medio. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo durante el proyecto.
	Riesgo Bajo. Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo.

Figura 8: Leyenda
Fuente: Seguridad de la Información

Mapa de Calor

Anexo se reflejan los mapas de calor, resultado de la matriz de riesgo

Mapa de Calor		Impacto		
		Bajo	**Medio**	**Alto**
Probabilidad	**Baja**	Bajo	Medio	Alto
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Alto

Mapa de Calor		Impacto		
		Bajo	**Medio**	**Alto**
Probabilidad	**Bajo**			
	Medio		4	
	Alto			5

Figura 9: Mapa de calor
Fuente: Seguridad de la Información

Analisis cualitativo de riesgos: Se empleó una matriz de probabilidad e impacto adaptada a las condiciones del banco. Dicha matriz considera dos variables: la probabilidad de ocurrencia del evento no deseado y el impacto potenial asociado al mismo. La combinacion de ambas variables permitirá establecer el nivel de riesgo. A continuacion, en la figura 10 se muestran los criterios de probabilidad de ocurrencia utilizados.

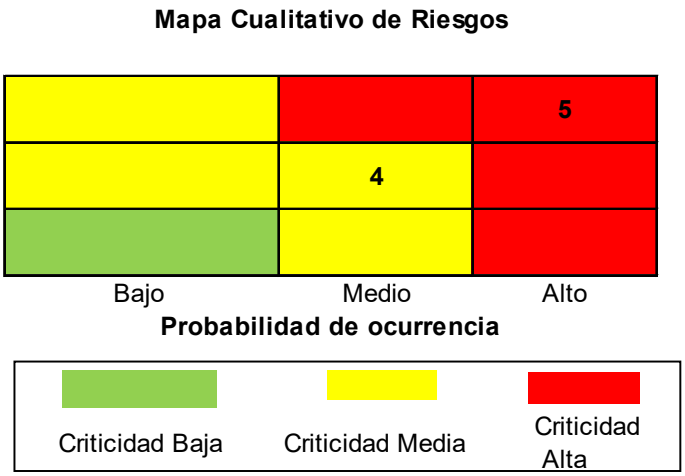

Figura 10: Mapa cualitativo de riesgos
Fuente: Seguridad de la Información

A continuación se presentan los resultados de los riesgos por incumplimiento del estándar de seguridad de datos para la industria de tarjetas de pago (PCI-DSS):

- Los riesgos de criticidad alta deben ser atendidos de manera urgente. Se debe elaborar un plan de acción para mitigarlos. En este caso son cinco (5) riesgos.

- Los riesgos de criticidad media deben ser atendidos luego de atender los de criticidad alta. Se debe elaborar un plan de acción para mitigarlos. En este caso son cinco (4) riesgos.

Para elaborar el plan de mitigación de los riesgos detectados, se utilizarán las estrategias presentadas en la tabla nro. 30:

Tabla 31: Estrategia de Mitigación de Riesgo

ID	Descripción del Riesgo	P	I	C	Estrategia	Responsable	Fecha
1.1	Imposibilidad de trabajar con un adquiriente. En caso que un comercio no cumpla con el estándar, dicho adquiriente puede finalizarle su servicio al banco	Baja	Alto	Medio	Incentivar a los adquirientes para que cumplan con la certificación PCI	VP Medios de Pago	En marcha
1.2	Pago de multas en caso de fraude: Dichas multas pueden ser impuestas por las marcas de pago y por los adquirientes.	Media	Alto	Alto	Negociar con las marcas de pago y adquirientes	Consultoría Jurídica	Cuando sea necesario
1.3	Pago de indemnizaciones a clientes afectados por fraude relacionado a PCI	Baja	Alto	Medio	Negociar con el cliente para no afectar la reputación del banco	Consultoría Jurídica	Cuando sea necesario
1.4	Costos asociados de una investigación forense, que debe ser ejecutada por un Investigador forense certificado por la industria de tarjetas de pago(PCI-PFI) únicamente	Alta	Alto	Alto	Asumir los costos ocasionados por la investigación y hacer las remediaciones pertinentes	VP Medios de Pago	Cuando sea necesario
1.5	Problemas derivados de mala prensa y pérdida de imagen de cara a clientes	Baja	Alto	Medio	Campañas informativas	VP Mercadeo	A través del proyecto
1.6	Costos asociados a la implementación de los controles de PCI-DSS de forma correctiva después de un incidente de seguridad, siempre serán mucho más altos que si se implementan de forma preventiva.	Alta	Alto	Alto	Asumir los costos de implementación necesarios	VP Tecnología	A través del proyecto
1.7	Posibilidad de problemas legales derivados del incumplimiento colateral de otras leyes o normativas	Baja	Medio	Medio	Negociar con las franquicias mientras el banco se certifica PCI	Consultoría Jurídica	A través del proyecto
1.8	Prohibición de procesamiento de tarjetas de crédito Mastercard o Visa	Baja	Alto	Alto	Negociar con las franquicias mientras el banco se certifica PCI	Consultoría Jurídica	A través del proyecto
1.9	Prohibición de procesamiento de tarjetas internacionales y/o nacionales	Baja	Alto	Alto	Negociar con las franquicias mientras el banco se certifica PCI	Consultoría Jurídica	A través del proyecto

Objetivo 3: Evaluar las alternativas para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS) de Bancaribe Banco Universal.

Una vez identificados los requisitos exigidos por el estándar de seguridad de datos para la industria de tarjetas de pago e identificados los riesgos por no cumplimento de dicho estándar, se presenta un análisis de alto nivel de las posibles alternativas que podrían emplearse para cerrar la brecha entre la situación actual del banco y lo que se propone en este trabajo, que es el plan de implementación para implantar el estándar PCI DSS en la institución bancaria.

Identificación de Alternativas: A continuación se enumeran las posibles alternativas identificadas para el análisis:

Alternativa 1- El banco puede considerar no hacer nada para implementar el estándar de seguridad de datos de la industria de tarjetas de pago y de esta manera seguiría operando bajo la situación actual.

Alternativa 2 – Realizar la evaluación PCI, con los recursos internos del banco y guiándose por los cuestionarios y toda la documentación publicada en la página web oficial del Consejo de Normas de seguridad-Industria de tarjetas de pago, en este caso el banco no obtendría la certificación PCI por no contratar un asesor de seguridad certificado para ello.

Alternativa 3 - Realizar la evaluación PCI, el proceso de remediación y por último la certificación. Para ello se requiere contratar una empresa certificada por el Consejo de Normas de seguridad-Industria de tarjetas de pago, la cual cuenta con asesores certificados de seguridad para implantar el estándar PCI-DSS y proceder con la certificación del banco.

Comparación de Alternativas: A continuación se comparan las alternativas propuestas resumiendo los beneficios, desventajas, costos y riesgos, en la siguiente tabla:

Tabla 32: Comparación de Alternativas

Criterios	Alternativa 1	Alternativa 2	Alternativa 3
Beneficios: Junta directiva Medios de Pago	Impulsar otros proyectos relacionados al negocio. Disponibilidad de recursos para apoyar proyectos de negocio.	Ahorrar dinero por no contratar personal certificado. Conocer las vulnerabilidades a las que está expuesto el banco.	Mejora de la imagen de la marca del banco Concientización de los empleados sobre la importancia de proteger los datos de la tarjeta
Desventajas Junta directiva Medios de Pago	Debe aceptar los riesgos a los que está expuesto el banco por no estar certificado PCI.	Retrabajo por no contar con la asesoría de un asesor experto y certificado PCI.	En el país no existen asesores certificados (QSA) por lo que debe contratar una empresa extranjera.
Costos: Directos	No involucra costos.	Los costos estarían asociados a la remediación.	Los costos son en moneda extranjera por la contratación del QSA.
Riesgos: Costos de mitigación	No involucra costos.	Los costos estarían asociados al proceso de remediación para mitigar los riesgos.	Los costos estarían asociados al proceso de remediación y certificación para mitigar los riesgos.

Alternativa Recomendada: En base a la comparación de alternativas, se considera que la mejor alternativa es la numero 3. Al implementar esta solución se estarían mitigando todos los riesgos descritos en la matriz de riesgo. Sin embargo es importante destacar que sería la opción más costosa para el banco, sin embargo los beneficios para la organización a largo plazo contribuyen a recuperar lo gastado en el proyecto.

Estrategia de implementación: De acuerdo a la alternativa recomendada anteriormente, se creará un proyecto de plan de implementación para implantar el estándar de seguridad de datos en la industria de tarjetas de pago para una institución bancaria, el cual se detallará en el siguiente capítulo, análisis de resultados.

En la figura anexa, se visualiza el Canvas modelo de negocio, donde se observan los socios clave: Empresas Certificadas PCI, Empresas de Tecnología, Consorcio Credicard y la Junta Directiva. Entre las actividades clave se mencionan las siguientes: Ejecutar procesos de evaluación, remediación y certificación PCI. Sus recursos más importantes son: Humanos, tecnológicos y financieros. Como propuesta de valor más destacada se tiene: Mitigación de riesgos, controles de seguridad más robustos y mejora de la imagen de la marca del banco. La relación con los clientes se realiza a través de la red de agencias, canales electrónicos y pagina web del banco.

Sus clientes están segmentados en persona natural y jurídica. La estructura de costos está compuesta por los siguientes gastos: Recursos contratados y capacitación del personal. Para finalizar el flujo de ingresos está compuesto por captación de nuevos clientes y mejoras en la plataforma tecnológica.

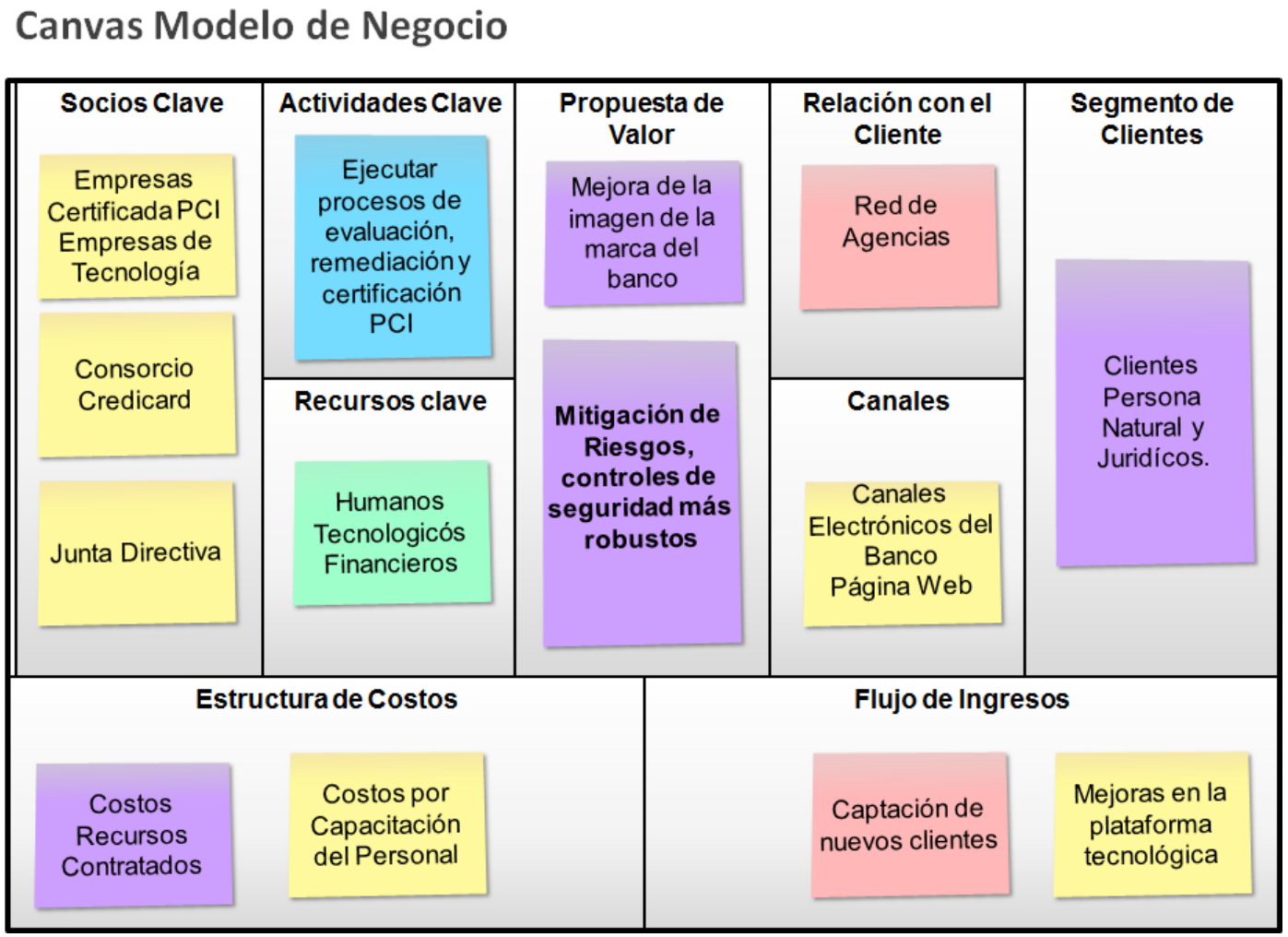

Figura 11: Canvas Modelo de Negocio

CAPITULO VI. ANALISIS DE LOS RESULTADOS

El plan de implementación diseñado permite a los líderes de proyectos, una orientación estandarizada de planificación, garantizando un buen control del cronograma de los proyectos e impulsando el uso de una metodología en lugar de procesos empíricos. La metodología empleada, las herramientas y técnicas de recolección de datos recomendadas por los autores, fueron acertadas y contribuyeron a determinar el cumplimiento de los procesos de planificación propuestos en el PMI (2013), todo esto permitió obtener valiosos aportes y de factible aplicación para Bancaribe.

A continuación de describe el plan de implementación para implantar el estándar de seguridad de datos en la industria de tarjetas de pago de Bancaribe Banco Universal.

Título del proyecto: Plan de implementación para implantar el estándar de seguridad de datos en la industria de tarjetas de pago para Bancaribe Banco Universal.

Términos y abreviaturas: Se listan los términos o abreviaturas que se utilizarán en el plan de implementación.

Tabla 33: Términos y abreviaturas

Término	Significado
PCI-DSS	Acrónimo de “Payment Card Industry Data Security Standard” (Estándar de seguridad de datos-Industria de tarjetas de pago)
PCI-QSA	Acrónimo de “Payment Application Qualified Security Assesor” (Asesor de seguridad certificado para las aplicaciones de pago).
PCI-PFI	Acrónimo de “Payment Card Industry- Forensic Investigator” (Investigador forense certificado por la industria de tarjetas de pago).
PCI-SSC	Acrónimo de “Security Standards Council” (Consejo de Normas de seguridad-Industria de tarjetas de pago).

Propósito del plan de implementación: El Plan de Implementación detalla los cronogramas de implementación de alto nivel, los recursos requeridos, los detalles de la implementación y el apoyo posterior.

Plan de Recursos: Se enumeran los recursos necesarios para las etapas de implementación.

Tabla 34: Plan de recursos

Recurso	Responsabilidad
Gerente de Proyecto (PMO)	Dirige las actividades del proyecto y garantizar que se cumplan las expectativas del cliente
Líder de proyecto (Contratado)	Dirige las actividades del proyecto y garantiza que se cumplan las expectativas del cliente
Consultor de Seguridad de Información (Contratado certificado PCI QSA)	Responsable por el desarrollo del proceso de certificación PCI.
Líder funcional de seguridad	Coordina las actividades que serán ejecutadas por los consultores de seguridad
Consultor de Seguridad de Información	Asegura se cumplan las políticas y controles de seguridad de información del banco.
Líder Técnico	Controla y dirige todas las actividades inherentes al proyecto relacionadas con tecnología y sistemas.
Líder funcional de medios de pago	Establece lineamientos y gestiona la planificación y control del proyecto, estimación y control de costo, análisis de riesgo y control de desviación.
Líder funcional de canales electrónicos	Establece lineamientos y gestiona la planificación y control del proyecto, estimación y control de costo, análisis de riesgo y control de desviación.
Líder de Procesos	Asegura la actualización y distribución de la información, bajo su custodia, inherente al proyecto.
Líder de Infraestructura	Apoya en suministrar información requerida sobre la infraestructura tecnológica
Líder de Calidad TI	Encargado de ejecutar y coordinar el proceso de remediación en conjunto con el líder técnico

Estructura desagregada de trabajo (EDT): A continuación se presenta la estructura desagregada de trabajo.

Tabla 35: Estructura desagregada de trabajo (EDT)

EDT	ID	NOMBRE DE TAREA	DESCRIPCIÓN
1	**1**	**Plan de Implementación para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS)en Bancaribe**	
1.1	**2**	**Grupo de Procesos de Inicio**	
1.1.1	3	Elaborar Acta de Constitución del Proyecto	Realizar entrevistas no estructuradas con el solicitante del proyecto
1.1.2	4	Identificar los Interesados del Proyecto	Validar con el Líder Técnico y PMO quienes serían los interesados del proyecto
1.1.3	5	Registrar Matriz con los Interesados del Proyecto	Documentar matriz con los interesados identificados
1.2	6	Hito: Fin Grupo de Procesos de Inicio	Evento que indica el cierre de Grupos de Procesos de Inicio
1.3	**7**	**Grupo de Procesos de Planificación**	
1.3.1	8	Levantar Información sobre los controles requeridos por PCI DSS	Realizar entrevistas no estructuradas con los involucrados del proyecto con el fin de entender los requisitos exigidos por la norma PCI, solicitar a cada unidad su plan de actividades
1.3.2	9	Definir Alcance de la Evaluación de PCI	Aplicar reuniones con todos los involucrados para la definición del alcance y EDT
1.3.3	10	Elaborar Estructura Desagregada de Trabajo (EDT)	
1.3.4	11	Realizar el Cronograma de Actividades	Desarrollar el cronograma de actividades del proyecto (Actividades, Secuenciación, Duración, Recursos)
1.3.5	12	Preparar Plan de Comunicación	Realizar el Plan de Comunicación que irá en la presentación de Kickoff
1.3.6	13	Levantar Riesgos	Levantar los riesgos del proyecto con todo el equipo

EDT	ID	NOMBRE DE TAREA	DESCRIPCIÓN
1.3.7	14	Realizar Presentación de Kickoff	La presentación de kickoff debe contener: Objetivo y Alcance, Antecedentes, Situación Actual Propuesta, Entregables, Beneficios, Involucrados Cronograma Macro, Plan de Comunicación Riesgos, Próximos Pasos
1.3.8	15	Presentar Kickoff	Presentar a todos los involucrados la presentación de kickoff del proyecto
1.3.9	16	Hito: Presentación de Kickoff Realizada	Primer entregable Presentación de Kickoff
1.3.10	17	Solicitar Línea Base	Realizar la solicitud formal de línea base a la oficina de proyectos (PMO)
1.3.11	18	Hito: Fin Grupo de Procesos de Planificación	Evento que indica el fin de la fase Planificación
1.4	**19**	**Grupo de Procesos de Ejecución**	
1.4.1	20	Elaborar cuestionario de evaluación PCI	Elaborar cuestionario de evaluación PCI de acuerdo a la guía de auditoria de PCI DSS v3.2
1.4.2	21	Realizar Evaluación PCI	Realizar la evaluación de acuerdo a la guía de auditoria de PCI DSS v. 3.2
1.4.3	22	Realizar GAP Análisis PCI DSS	Este servicio busca identificar y medir las diferencias existentes entre los requerimientos establecidos por PCI y lo entregado por los sistemas de seguridad de la información del banco.
1.4.4	23	Revisar documentación de procesos relacionados con tarjetas de crédito	Revisar documentación
1.4.5	24	Observar procesos, operaciones y configuraciones de los componentes del sistema	Observar procesos, operaciones y configuraciones de los componentes del sistema
1.4.6	25	Presentar recomendaciones para los controles no establecidos	Realizar una presentación a nivel gerencia mostrando los principales hallazgos y recomendaciones

EDT	ID	NOMBRE DE TAREA	DESCRIPCIÓN
1.4.7	26	Realizar Informe de recomendaciones	Realizar informe de recomendaciones de los controles no establecidos
1.4.8	27	Generar reporte del GAP Análisis PCI	Generar reporte del Gap análisis PCI DSS
1.4.9	28	Hito Informe de Gap Análisis PCI	Segundo Entregable Informe de Gap análisis
1.4.10	29	Hito Fin de evaluación PCI	Evento que indica el fin de evaluación PCI
1.4.11	30	Realizar proceso de remediación	Evento que indica el inicio del proceso de remediación. Consiste en resolver las situaciones encontradas en el gap análisis
1.4.12	31	Elaborar las tareas de remediación	Elaborar las tareas de remediación para los controles no establecidos detectados en el gap análisis
1.4.13	32	Ejecutar tareas de remediación	Ejecutar tareas de remediación
1.4.14	33	Hito Tareas de remediación ejecutadas	Evento que indica que han sido realizadas las tareas de remediación
1.4.15	34	Hito Fin Grupo de Procesos de Ejecución	Evento que indica el fin de la fase Ejecución
1.5	**35**	**Grupo de Procesos de certificación PCI**	
1.5.1	36	Realizar la evaluación PCI de acuerdo a las guías de auditoria de PCI DSS	Evento que indica la evaluación PCI
1.5.2	37	Generar reporte de cumplimiento PCI	Generar reporte de cumplimiento PCI DSS
1.5.3	38	Hito Reporte de cumplimiento generado	Tercer Entregable Reporte de cumplimiento PCI
1.6	39	Hito Fin Grupo de procesos de certificación PCI	Evento que indica el fin de la fase de certificación

EDT	ID	NOMBRE DE TAREA	DESCRIPCIÓN
1.7	40	**Grupo de Procesos de Cierre**	
1.7.1	41	Solicitar Cierre del Proyecto	Enviar correo electrónico con la conformidad del solicitante a la oficina de proyectos para que realicen el cierre administrativo del proyecto
1.7.2	42	Hito Fin Cierre del Proyecto	Evento que indica el Cierre del proyecto
1.8	43	Hito 025: Fin del Proyecto	Evento que indica el fin del proyecto

Elaboración del Cronograma: Se elabora la programación del proyecto, para tal fin se empleó el software MS Project 2013 en la elaboración del cronograma mostrado en la figura 12. El contenido del cronograma se basa en cada una de las actividades identificadas para la consecución del proyecto, por lo que se requiere haber cumplido a cabalidad los procesos anteriores. Se estableció como fecha de inicio del proyecto el día 27 de febrero de 2017, resultando como fecha de culminación del proyecto el día 13 de septiembre de 2017. Para el desarrollo del plan de implementación, se fijó como jornada laboral lunes a viernes de 8:00 am a 5:00 pm.

A continuación se anexa el diagrama de Gantt del proyecto.

	EDT	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
1	1	**Plan de Implementación para implantar el estándar de seguridad de datos en la industria de tarjetas de pago (PCI-DSS)en Bancaribe**	142,5 días	27 feb	13 sep	
2	1.1	Grupo de Procesos de Inicio	6 días	27 feb	06 mar	
3	1.1.1	Elaborar acta de constitución del proyecto	2 días	27 feb	28 feb	Gerente de Proyecto;Líder funcional de seguridad
4	1.1.2	Identificar los Interesados del Proyecto	2 días	01 mar	02 mar	Gerente de Proyecto;Líder funcional de seguridad
5	1.1.3	Registrar matriz con los interesados del proyecto	2 días	03 mar	06 mar	Gerente de Proyecto;Líder funcional de seguridad
6	1.2	Hito Fin Grupo de Procesos de Inicio	0 días	06 mar	06 mar	
7	1.3	Grupo de procesos de planificación	36,5 días	07 mar	26 abr	
8	1.3.1	Levantar información sobre los controles requeridos por PCI DSS	10 días	07 mar	20 mar	Líder de Proyecto Contratado;Líder funcional de seguridad
9	1.3.2	Definir alcance de la evaluación de PCI	5 días	21 mar	27 mar	Gerente de Proyecto;Líder funcional de seguridad
10	1.3.3	Elaborar estructura desagregada de trabajo EDT	5 días	28 mar	03 abr	Gerente de Proyecto;Líder funcional de seguridad
11	1.3.4	Realizar el cronograma de actividades	5 días	04 abr	10 abr	Gerente de Proyecto
12	1.3.5	Preparar plan de comunicación	3 días	11 abr	13 abr	Gerente de Proyecto;Líder funcional de seguridad
13	1.3.6	Levantar riesgos	3 días	14 abr	18 abr	Gerente de Proyecto;Líder funcional de seguridad
14	1.3.7	Realizar presentación de kickoff	3 días	19 abr	21 abr	Gerente de Proyecto;Líder funcional de seguridad
15	1.3.8	Presentar kickoff	0,5 días	24 abr	24 abr	Gerente de Proyecto;Líder funcional de seguridad
16	1.3.9	Hito Presentación de kickoff realizada	0 días	24 abr	24 abr	
17	1.3.10	Solicitar linea base	2 días	24 abr	26 abr	Gerente de Proyecto
18	1.3.11	Hito Fin grupo de procesos de planificación	0 días	26 abr	26 abr	
19	1.4	Grupo de procesos de ejecución	85 días	26 abr	23 ago	
20	1.4.1	Elaborar cuestionario de evaluación PCI	7 días	26 abr	05 may	Lider de Proyecto Contratado;Líder funcional de seguridad; Consultor de Seguridad de Información ;Consultor de Seguridad
21	1.4.2	Realizar evaluación PCI	15 días	05 may	26 may	Consultor de Seguridad de Información ; Consultor de Seguridad de Información (Contratado certificado
22	1.4.3	Realizar gap análisis PCI DSS	7 días	26 may	06 jun	Líder Técnico;Consultor de Seguridad de Información (Contrata Consultor de Seguridad de Información ;Líder funcional de segu
23	1.4.4	Revisar documentación de procesos relacionados con tarjetas de crédito	10 días	06 jun	20 jun	Consultor de Seguridad de Información ; Consultor de Seguridad de Información (Contratado certificado
24	1.4.5	Observar procesos, operaciones y configuraciones de los componentes de sistema	10 días	20 jun	04 jul	Líder de Infraestructura;Consultor de Seguridad de Información Consultor de Seguridad de Información (Contratado certificado Líder Técnico
25	1.4.6	Presentar recomendaciones para los controles no establecidos	1 día	04 jul	05 jul	Consultor de Seguridad de Información (Contratado certificado Lider de Proyecto Contratado
26	1.4.7	Realizar informe de recomendaciones	3 días	05 jul	10 jul	Consultor de Seguridad de Información (Contratado certificado Lider de Proyecto Contratado
27	1.4.8	Generar reporte del gap análisis PCI	3 días	10 jul	13 jul	Lider de Proyecto Contratado; Consultor de Seguridad de Información (Contratado certificado
28	1.4.9	Hito Informe de gap análisis PCI	0 días	13 jul	13 jul	
29	1.4.10	Hito Fin de evaluación PCI	0 días	13 jul	13 jul	
30	1.4.11	Realizar proceso de remediación	10 días	13 jul	27 jul	Consultor de Seguridad de Información ; Consultor de Seguridad de Información (Contratado certificado
31	1.4.12	Elaborar las tareas de remediación	4 días	27 jul	02 ago	Consultor de Seguridad de Información ; Consultor de Seguridad de Información (Contratado certificado
32	1.4.13	Ejecutar tareas de remediación	15 días	02 ago	23 ago	Consultor de Seguridad de Información ;Líder Técnico;Líder
33	1.4.14	Hito Tareas de remediación ejecutadas	0 días	23 ago	23 ago	
34	1.4.15	Hito Fin grupo de procesos de ejecución	0 días	23 ago	23 ago	
35	1.5	Grupo de Procesos de Certificación PCI	12 días	23 ago	08 sep	
36	1.5.1	Realizar evaluación PCI	10 días	23 ago	06 sep	Consultor de Seguridad de Información (Contratado certificado Consultor de Seguridad de Información
37	1.5.2	Generar reporte de cumplimiento PCI	2 días	06 sep	08 sep	Consultor de Seguridad de Información (Contratado certificado Lider de Proyecto Contratado
38	1.5.3	Hito Reporte de cumplimiento elaborado	0 días	08 sep	08 sep	
39	1.6	Hito Fin grupo de procesos de certificación PCI	0 días	08 sep	08 sep	
40	1.7	Grupo de procesos de cierre	3 días	08 sep	13 sep	
41	1.7.1	Solicitar cierre de proyecto	3 días	08 sep	13 sep	Gerente de Proyecto;Líder funcional de seguridad
42	1.7.2	Hito Fin cierre del proyecto	0 días	13 sep	13 sep	
43	1.8	Hito Fin de grupo de procesos de cierre	0 días	13 sep	13 sep	

Figura 12. Diagrama de Gantt

Nomenclatura de identificación de recursos: Se establece una nomenclatura para identificar a los recursos en el plan de comunicación.

Tabla 36: Nomenclatura de identificación de recursos

ID	Nombre del recurso	Nivel de Canal de Comunicación
GPY	Gerente de Proyecto	Central
LPC	Líder de proyecto contratado	Central
QSA	Consultor de seguridad de información (Contratado Certificado PCI QSA)	Lateral
CSI	Consultor de seguridad de información	Lateral
LTI	Líder Técnico	Lateral
LMP	Líder funcional de medios de pago	Lateral
LCE	Líder funcional de canales electrónicos	Lateral
LPR	Líder de procesos	Lateral
LIF	Líder de infraestructura	Abajo
LCT	Líder de calidad TI	Abajo
LFS	Líder funcional de seguridad	Central

Plan de Comunicación: Se organizó en base a las necesidades de información y comunicación de los interesados para asegurarse de hacer llegar la información correcta a la persona indicada. En tabla anexa se describe la metodología comunicacional que será utilizada en el proyecto. Se construirá un repositorio (sitio web) en la herramienta colaborativa del banco, disponible para publicar toda la información del proyecto.

Tabla 37: Plan de comunicación

Id del Recurso	Prioridad	Frecuencia	Tipo de comunicación	Responsable de elaborar comunicación	Forma de entrega
GPY-LFS- LTI-LPC-LMP-LCE	Alta	Mensual	Minuta seguimiento mensual	Gerente de Proyecto	Formal, digital, publicada en el sitio web del proyecto
Todo el equipo	Media	Semanal	Minuta seguimiento semanal	Gerente de proyecto	Formal, digital, publicada en el sitio web del proyecto
Todo el equipo	Alta	Única	Presentación kickoff	Gerente de proyecto	Formal, digital, publicada en el sitio web del proyecto
LFS-GPY-LTI-QSA-CSI	Alta	Única	Reporte Gap análisis PCI	Líder de proyecto contratado	Formal, impreso, digital, publicada en el sitio web del proyecto
LFS-GPY-LTI-QSA-CSI	Alta	Única	Reporte de cumplimiento PCI	Líder de proyecto contratado	Formal, impreso, digital, publicada en el sitio web del proyecto
Todo el equipo	Alta	Única	Presentación de cierre de proyecto	Gerente de proyecto	Formal, digital, publicada en el sitio web del proyecto
Todo el equipo	Media	Única	Matriz de riesgo del proyecto	Gerente de proyecto	Formal, digital, publicada en el sitio web del proyecto
Todo el equipo	Media	A demanda	Necesidades de información	Involucrados	Informal, digital por correo, publicada en el sitio web del proyecto
GPY-LFS- LTI-LPC-LMP-LCE	Alta	Mensual	Control de presupuesto	Gerente de proyecto	Formal, digital, publicada en el sitio web del proyecto

Plan de Aseguramiento de Calidad

A continuación se detalla el plan de aseguramiento de Calidad, de los principales entregables del proyecto:

Tabla 38: Plan de Aseguramiento de la calidad

EDT	Requerimiento	Especificación	Actividad	Cronograma	Responsable
1.2	Fin grupo de procesos de inicio	Revisión de documentos: acta de constitución del proyecto, matriz de interesados	Reporte de proyecto	06-03	Gerente del proyecto
1.3.9	Presentación del kickoff	Presentación de kickoff a los interesados del proyecto	Reporte de proyecto	24-04	Gerente del proyecto
1.3.11	Fin grupo de procesos de planificación	Revisión de documentos: alcance del proyecto, EDT, cronograma, plan de comunicación y matriz de riesgo.	Reporte de proyecto	26-04	Gerente del proyecto
1.4.9	Informe de Gap Análisis	Revisión de informé de gap análisis	Reporte de proyecto	13-07	Gerente del proyecto
1.4.10	Informe de recomendaciones	Revisión de informé de recomendaciones	Reporte de proyecto	13-07	Gerente del proyecto
1.4.14	Tareas de remediación ejecutadas	Revisión de las actividades de remediación	Reporte de proyecto	23-08	Gerente del proyecto
1.4.15	Fin grupo de procesos de ejecución	Revisión de documentos de procesos de remediación	Reporte de proyecto	23-08	Gerente del proyecto
1.5.3	Reporte de cumplimiento	Revisión del reporte de cumplimiento PCI	Reporte de proyecto	08-09	Gerente del proyecto
1.6	Fin grupo de procesos de certificación PCI	Revisión y publicación de documentación generada	Reporte de proyecto	08-09	Gerente del proyecto
1.7.2	Cierre de proyecto	Revisión de documentación asociada al cierre técnico y administrativo del proyecto	Reporte de proyecto	13-09	Gerente del proyecto
1.8	Fin grupo de procesos de cierre	Revisión y publicación de toda la documentación asociada al cierre proyecto	Reporte de proyecto	13-09	Gerente del proyecto

CAPITULO VII. LECCIONES APRENDIDAS

✓ Lo primero al iniciar un proyecto es tener conciencia del aporte del mismo al negocio, así como del entorno, oportunidades, amenazas, restricciones, ver cómo podemos gestionarlos para tener un proyecto exitoso.

✓ Es importante identificar, definir, combinar, unificar y coordinar los diversos procesos y actividades de dirección de proyecto.

✓ Asegurarse que el proyecto incluye todo el trabajo requerido para ser completado con éxito, por ello es muy importante definir el alcance del mismo, por lo cual se debe lograr la aceptación de todas las partes interesadas, sobre qué es exactamente lo que el proyecto va a producir y mantener ese acuerdo durante todo el ciclo de vida del proyecto.

✓ La gestión del tiempo, el desarrollo y control del cronograma garantizan el éxito del proyecto y la satisfacción del cliente.

✓ Definir responsabilidades, objetivos y políticas de calidad, de esta manera se garantiza que los entregables sean los esperados por el cliente.

✓ Tener en cuenta a todos los grupos o personas que tienen algún interés en el proyecto, para ello es vital la matriz de interesados así como la gestión de equipo de trabajo.

✓ Aplicar las habilidades de comunicación en forma efectiva, lo cual permite construir una asociación con los clientes del proyecto y satisfacer las necesidades de información de todas las partes afectadas de una manera precisa, completa y oportuna.

✓ El proyecto debe tener una adecuada gestión del presupuesto de esta manera se administran las proyecciones de calendario y presupuesto con precisión durante todo el ciclo de vida del proyecto.

✓ Establecer y gestionar los compromisos del proyecto, para hacer un seguimiento adecuado a los acuerdos contraídos, ya sea en términos de alcance,

horario y presupuesto acordados, o en términos de entregables previamente aceptados, y para manejar las variaciones de los compromisos.

✓ Manejo adecuado de la documentación del proyecto y accesibilidad a la misma, cuyo propósito es recopilar, almacenar y administrar datos generados por y sobre el proyecto, y para capturar datos históricos en el repositorio para su uso o análisis futuro.

✓ Planificar la gestión de riesgos, así como la identificación, análisis, planificación de respuesta y control de los mismos.

✓ La gestión de adquisiciones permite una adecuada obtención de los productos, servicios o resultados requeridos por el equipo del proyecto.

CAPITULO VIII. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

- La identificación de los requisitos exigidos por el estándar de seguridad de datos, sirvió de referencia para conocer cuál es el nivel de cumplimiento del banco en relación a la certificación PCI.

- Se pudo conocer la situación actual del banco en relación a la certificación y cumplimiento de la normativa.

- La matriz de riesgo por no cumplimento del estándar PCI DSS, nos mostró la importancia para el banco de certificarse, de esta manera se estarían aplicando los mecanismos de protección necesarios para salvaguardar la seguridad de los datos confidenciales de los clientes del banco y mitigando los riesgos. Asimismo se definieron las estrategias de mitigación de los mismos en base a la criticidad y el impacto.

- Al evaluar las alternativas para implantar el estándar de seguridad de datos, nos dimos cuenta que la implantación del mismo muy costosa y requiere de personal altamente capacitado no disponible en Venezuela, sin embargo trae como resultado gestionar de forma segura las operaciones del banco, garantizando la máxima seguridad de la información sensible y confidencial de sus clientes y prestigio para la institución.

- En cuanto a los objetivos específicos, todos fueron logrados, se determinaron los requisitos exigidos por el estándar de seguridad de datos; el cual permitió identificar la situación actual del banco en relación al cumplimiento del estándar PCI-DSS, luego se identificaron los riesgos a los que está expuesto el banco por incumplimiento del estándar de seguridad de datos para la industria de tarjetas de pago.

RECOMENDACIONES:

- Al formular la propuesta a través del plan de implementación para implantar el estándar de seguridad de datos de la industria de tarjetas de pago, es recomendable actualizar el cronograma del proyecto en la medida que se desarrolle; la planificación como proceso dinámico necesita de retroalimentación para poder medir los resultados de una manera más confiable.

- El plan de implementación debe contar con reuniones presenciales (semanales o quincenales), para detectar desviaciones y corregir de inmediato en la medida que sea posible, dejando los acuerdos y decisiones registradas en minuta.

- En busca de optimizar los tiempos de las actividades, es importante tener en cuenta las diferentes técnicas de aceleración de proyectos, con especial atención a las actividades que conforman la ruta crítica, puesto que son más vulnerables en cuanto al impacto en el proyecto si llegan a retrasarse.

- Para un mejor desempeño y fluidez del proyecto, se recomienda balancear las cargas de los recursos, lo que permitirá detectar posibles desviaciones y tomar las correcciones necesarias.

Referencias Bibliográficas

Asamblea Nacional de la República Bolivariana de Venezuela . (30 de Octubre de 2001). Ley especial contra Los Delitos Informáticos . Gaceta Oficial Nro. 37313.

Asamblea Nacional de la República Bolivariana de Venezuela. (28 de Febrero de 2001). *Ley Orgánica de Telecomunicaciones*. Caracas, Venezuela: Gaceta Oficial No.37.148.

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

Asamblea Nacional de la República Bolivariana de Venezuela. (18 de Octubre de 2002). Ley del Banco Central de Venezuela . Caracas, Venezuela: Gaceta Oficial Nº 5.606.

Asamblea Nacional de la República Bolivariana de Venezuela. (03 de Agosto de 2005). *Ley Orgánica de Ciencia, Tecnología e Innovación*. Caracas, Venezuela: Gaceta Oficial N° 38.242 .

Asamblea Nacional de la República Bolivariana de Venezuela. (19 de Febrero de 2009). Constitución Bolivariana . Caracas, Venezuela: Gaceta Oficial Nº 5.908.

Asamblea Nacional de la República Bolivariana de Venezuela. (02 de Marzo de 2011). *Ley de Reforma Parcial de la Ley de Instituciones del Sector Bancario*. Caracas, Venezuela: Gaceta Oficial Nº 39.627.

Balestrini, M. (2006). *Como se Elabora el Proyecto de Investigación.* Caracas: Venezuela (7ma ed.).

Bancaribe. (2014). *Mi Banco. Análisis fundacional*. Obtenido de http://intranetbc.tpr.bancaribe

Beissel, S. (2014). Supporting PCI DSS 3.0 Compliance With COBIT 5. *IT Governance Institute (ITGI). The Information Systems Audit & Control Association (ISACA)*.

Colegio de Ingenieros de Venezuela. (1996). *Código de Ética Profesional*. Obtenido de http://www.civ.net.ve/uploaded_pdf/cep.pdf

Consejo de Normas de seguridad. (Abril de 2016). *Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS). Requisitos y procedimientos de evaluación de seguridad.* Obtenido de https://www.pcisecuritystandards.org/pci_security/

Consejo de Ministros de la República Bolivariana de venezuela. (03 de Noviembre de 2001). Ley General de Bancos y otras Instituciones Financieras. Caracas, Venezuela: Decreto N° 1.526.

Dennis, C., & Goldman, D. (2013). Journal of Internet Law. *Data Security Laws and The Cybersecurity Debate*, Volumen 17. Number 2. Editado por DLA PIPER.

Hernandez, R., Fernández, C., & Baptista, P. (2010). *Metodología de la Investigación.* México DF: Mc Graw Hill.

Instituto de Manejo de Proyectos (PMI). (2013). Guía de los Fundamentos de la Dirección de Proyectos (Guía del PMBOK®). *5ta. Ed*. Pennsylvania, Estados Unidos.

Instituto Nacional de Tecnologías de la Comunicación (INTECO). (Mayo de 2010). *Manual Curso de Sistemas de gestión de la seguridad de la información según la norma UNE ISO IEC 27001 .* Obtenido de https://formacion-online.inteco.es/index.php

Maiwald, E. (2003). *Fundamentos de Seguridad de Redes* (2da. ed.). México D.F. México: Mc.Graw Hill.

Martínez, R. (Noviembre de 2010). Formulación del plan de ejecución (PEP) del proyecto ampliación del estacionamiento del Centro Comercial Valle Arriba Market Center. *Universidad Católica Andrés Bello, Dirección de Postgrado*. Caracas, Venezuela.

Ministerio de Ciencia y Tecnología. (10 de Febrero de 2001). *Ley Sobre Mensajes de Datos y Firmas Electrónicas* . Caracas, Venezuela: Decreto N° 1.024. Gaceta Oficial N° 37.148.

Organización Internacional de Normalización (ISO). (Septiembre de 2012). ISO 21500:2012. *Orientación sobre la dirección de proyectos*. Ginebra, Suiza.

Organización Internacional de Normalización (ISO). (Enero de 2014). ISO/IEC 27000:2014. *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos*. Ginebra, Suiza.

Organización Internacional de Normalización (ISO). (2015). *ISO 9000:2015 Sistema de Gestión de la Calidad Fundamentos y Vocabularios.* Madrid: Asociación Española de Normalización y Certificación.

Organización Internacional de Normalización (ISO). (23 de Septiembre de 2015). ISO 9001:2015. *Sistemas de gestión de la calidad - Requisitos*. Ginebra, Suiza.

PCI Consejo de Normas de Seguridad. (2010). *Estándares de Seguridad para la Industria de Tarjetas de Pago. En un vistazo panorama de las normas.* Obtenido de https://www.pcisecuritystandards.org/document_library

PCI Consejo de Normas de Seguridad. (2013). *PCI DSS- Guía de referencia rápida. Descripción del estándar de seguridad de datos de la industria de tarjetas de pago.* Obtenido de https://www.pcisecuritystandards.org/document_library

Project Management Institute. (2006). *Código de ética y conducta profesional del PMI.* Caracas.

Superintendencia de las Instituciones del Sector Bancario de Venezuela (SUDEBAN). (2010). 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. Caracas, Venezuela: Resolución 119-10.

Superintendencia de las Instituciones del Sector Bancario de Venezuela (SUDEBAN). (2011). Normas Relativas a la Protección de los Usuarios y Usuarias de los Servicios Financieros. Caracas, Venezuela: Resolución N° 083.1.

Superintendencia de las Instituciones del Sector Bancario de Venezuela (SUDEBAN). (2011). Normas Relativas a la Protección de los Usuarios y Usuarias de los Servicios Financieros. Caracas, Venezuela: Resolución N° 083.11.

Superintendencia de las Instituciones del Sector Bancario de Venezuela (SUDEBAN). (29 de Mayo de 2003). Normas para una Adecuada Administración Integral de Riesgos. Caracas, Venezuela: Gaceta Oficial N° 37.703.

Tamayo, & Tamayo, M. (2009). *El Proceso de la Investigación Científica.* (3era. ed.). (E. Limusa, Ed.) México, D.F. (México).

Universidad Ahmad Dahlan, Departamento de Ingeniería Eléctrica. (2011). Implementación del Estándar de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI). *Telecomunicaciones Informática Electrónica y Control (TELKOMNIKA)*.

Willey, L., & White, B. (2013). Caso de enseñanza. ¿Aceptan tarjetas de crédito? Seguridad y cumplimiento de la industria de pagos de tarjetas de crédito. *Diario de la educación de sistemas de información*.

Zambrano, R. (2011). Elementos de Seguridad E-Business en la Banca Nacional para prevenir el fraude en medios de pago electrónicos. *Universidad Metropolitana. Dirección de Postgrado del área de estudios de Ingeria.* . Caracas, Venezuela.