UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
AREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTIÓN
POSTGRADO EN GERENCIA DE PROYECTOS

DISEÑO DE UN PLAN PARA LA IMPLEMENTACIÓN DE LA NORMA DE LA INDUSTRIA DE TARJETAS DE PAGO EN ENTIDADES BANCARIAS VENEZOLANAS

Presentado por:
Erika Fabiola Lazzarin Montalti

Para optar al título de:
ESPECIALISTA EN GERENCIA DE PROYECTOS

Asesor:
Rodríguez López, Nelson Antonio

Caracas, Octubre de 2011

AAU2677

UNIVERSIDAD CATOLICA ANDRES BELLO
Urb. Montalbán - La Vega - Apartado 29068
Teléfono: 407-42-68 y 407-42-69 Fax: 407-43-52
Estudios de Postgrado

ACTA DE EVALUACIÓN DE TRABAJO ESPECIAL DE GRADO ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS

Nosotros, **Profesores Nelson Rodríguez (Asesor) y Ámbar Ambrosetti**, designados por el Consejo Área de **Ciencias Administrativas y de Gestión** el día **trece** de **julio** de **dos mil once**, para conocer y evaluar en nuestra condición de jurado del Trabajo Especial de Grado "**DISEÑO DE UN PLAN PARA LA IMPLEMENTACIÓN DE LA NORMA DE LA INDUSTRIA DE TARJETAS DE PAGO EN ENTIDADES BANCARIAS VENEZOLANAS**" presentado por el estudiante ***Erika Lazzarin Montalti***, C.I. N° **15.782.544**, Exp. N° 96550, para optar al título de *Especialista en* ***Gerencia de Proyectos.***

Declaramos que:

Hemos leído el ejemplar del Trabajo Especial de Grado que nos fue entregado con anterioridad por la Dirección del Programa.

Reunidos el día **trece** de **octubre** de **dos mil once** en la sede de los Estudios de Postgrado de la Universidad Católica Andrés Bello, previa lectura y estudio del mencionado trabajo, hemos decidido **convocar al estudiante con el fin de responder las preguntas que le formule el jurado. Hechas por nuestra parte las preguntas y aclaratorias correspondientes, se consideró** formalizar el siguiente dictamen:

APROBADO

Hemos acordado calificar el Trabajo Especial de Grado de ***Erika Lazzarin Montalti*** con **dieciocho (18)** puntos.

En fe de lo cual, nosotros los miembros del jurado designado, firmamos la presente acta en Caracas, a los **nueve** días del mes de **noviembre** de **dos mil once.**

Nombre y firmas del jurado evaluador:

Nelson Rodríguez
C.I. 3.246.033

Ámbar Ambrosetti
C.I. 15.027.129

Secretaría Ejecutiva: 1ª. emisión de cuatro ejemplares de un mismo tenor.

ACEPTACIÓN DEL TUTOR

Por la presente hago constar que he leído el Trabajo Especial de Grado, presentado por la ciudadana Erika Fabiola Lazzarin Montalti, para optar al grado de Especialista en Gerencia de Proyectos, cuyo título es “Diseño de un Plan para la Implementación de la Norma de la Industria de Tarjetas de Pago en entidades bancarias venezolanas”; y manifiesto que cumple con los requisitos exigidos por la Dirección de Estudios de Postgrado de la Universidad Católica Andrés Bello y que por lo tanto, lo considero apto para ser evaluado por el jurado que se decida designar a tal fin.

En la ciudad de Caracas, a los catorce días del mes de octubre de 2011.

MSc. Nelson Antonio. Rodríguez López
C.I. N° 3.246.033

DEDICATORIA

A mi Madre, por lo maravillosa y perseverante que es.

AGRADECIMIENTOS

A Dios y la Virgen del Valle.

A mi mamá y a mi hermano Carlos por su amor y apoyo.

A mi esposo Gustavo Peña, por siempre darme su amor y apoyo en tantos momentos de mi vida.

A Leslie Chiquito y a Domingo Matos quienes fueron mis compañeros y amigos a lo largo de la carrera y compartimos logros y fracasos.

A todos los profesores que me apoyaron a lo largo de la elaboración del presente trabajo de grado y a lo largo de la carrera, muy especialmente a Ana Julia Guillén y a Nelson Rodríguez.

A William González, que me apoyó muchísimo con sus conocimientos en la Norma de la Industria de Tarjetas de Pago.

A los compañeros de las entidades bancarias quienes brindaron aportes fundamentales para el desarrollo del Trabajo Especial de Grado.

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTIÓN
POSTGRADO EN GERENCIA DE PROYECTOS

DISEÑO DE UN PLAN PARA LA IMPLEMENTACIÓN DE LA NORMA DE LA INDUSTRIA DE TARJETAS DE PAGO EN ENTIDADES BANCARIAS VENEZOLANAS

Autor: Erika Fabiola Lazzarin Montalti
Asesor: Nelson Rodríguez., MSc
Año: 2011

RESUMEN

En el país se ha producido un crecimiento exponencial en las transacciones con tarjetas de crédito en los últimos años, si bien este fenómeno ha generado un crecimiento de clientes, comercios, instituciones bancarias y la industria de las tarjetas de pago, ha traído como consecuencia un incremento en transacciones fraudulentas producto de defraudadores ocasionales o profesionales que han evolucionado sus técnicas con el transcurso de los años. Esta situación ha generado pérdidas millonarias a la industria de la tarjeta de pago y a la banca. A raíz de lo anteriormente expuesto, las empresas que conforman la Industria de las tarjetas de pago formaron un organismo independiente denominado Consejo para el Estándar de Seguridad en la Industria de las Tarjetas de Pago, o PCI SSC (Payment Card Industry Security Standards Council) por sus acrónimo en inglés, con el objetivo de elaborar una norma que permita a las organizaciones que procesan, almacenen y transmitan datos asociados a las tarjetas de crédito crear políticas para el aseguramiento de los datos con la finalidad de prevenir los fraudes. De acuerdo a lo expresado, a través del presente Trabajo Especial de Grado (TEG) se desarrollarán políticas para dar respuesta a los riesgos por medio de estrategias de control y mitigación, dando foco a los de mayor criticidad a menor criticidad, determinados por medio de un instrumento de recolección de datos que permitirá conocer la tendencia de la banca venezolana. Estos objetivos serán realizados a través de una metodología de tipo de investigación científica, conformada por un diseño de investigación de fuente primaria de campo y fuente secundaria bibliográfica. Se desarrollará el diseño de un plan para la implementación de políticas para el cumplimiento de la noma en entidades bancarias venezolanas en aras de dar respuesta a los riesgos detectados.

Palabras clave: Industria de Tarjetas de Pago, Gestión de Riesgos, Entidades Bancarias Venezolanas.

Línea de Trabajo: Gestión de Riesgos en Proyectos.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Figura **Pág.**

ÍNDICE DE TABLAS

Tabla **Pág.**

INTRODUCCIÓN

El fraude mediante tarjetas de crédito ha sufrido un incremento significativo en los últimos años, principalmente por el robo de información por parte de individuos, organizaciones delictivas o empleados deshonestos.

Las compañías que manejan el negocio de las tarjetas de crédito para el almacenamiento, procesamiento o transmisión de la data, están expuestas a múltiples amenazas por las consecuencias que se producen por transacciones fraudulentas tales como: multas por parte de las marcas de la industria de tarjetas de pago, pérdidas financieras y la credibilidad ante los clientes.

El presente TEG está estructurado en ocho (8) capítulos, que consisten en el desarrollo de un plan para el diseño de las mejores prácticas alineadas con la norma de la industria de tarjetas de pago establecida en el 2006, para mitigar y controlar los riesgos asociados a tarjetas de crédito en entidades bancarias venezolanas, establecida en el año 2006 por la Industria de las Tarjetas de Pago, la cual está conformada por doce requerimientos.

Por otro lado, el presente TEG estará focalizado en las técnicas y herramientas descritas en la Gestión del Riesgo del Project Management Institute para lograr los objetivos planteados.

- **Capítulo I - Propuesta del Proyecto**: está compuesto del planteamiento del problema, que indica las razones por las cuales se dio inicio a este proyecto, destacando los objetivos que deben cumplirse, la justificación del proyecto y las limitaciones del mismo.

- **Capítulo II - Marco Teórico:** conformado por los antecedentes de la investigación, además de mencionar las bases teóricas que se siguen en el desarrollo del proyecto con la finalidad de ubicar su entorno.

- **Capítulo III - Marco Metodológico**: destaca los aspectos como el tipo de investigación que se realizó, así como el diseño de la misma, las fuentes de información utilizadas, el método empleado para la recolección de datos aplicado a una muestra determinada dentro de una población seleccionada y finalmente el procesamiento de dichos datos.

- **Capítulo IV - Ventana de Mercado:** ubica el tipo de ambiente en el cual se desarrolla este proyecto, y que a la larga será el que haga uso de los resultados del estudio.

- **Capitulo V - Análisis Resultados**: muestra los resultados obtenidos a través de la herramienta del cuestionario, que arrojaron la moda, media y mediana de loes riesgos presentados en las entidades bancarias venezolanas.

- **Capítulo VI - Desarrollo del Plan:** con el estudio de los resultados, y con la información obtenida, proveniente de los capítulos anteriormente mencionados, se desarrolla el plan propuesto de actividades.

- **Capítulo VII - Evaluación del Proyecto:** se evalúa los objetivos plasmados y la explicación de cómo fueron alcanzados los mismos a través del desarrollo del TEG.

- **Conclusiones y Recomendaciones**: una vez concluida la investigación se procede a concluir sobre los aspectos más relevantes de la misma; así como las sugerencias obtenidas.

El producto final del presente Trabajo Especial de Grado, es el diseño de un Plan de para la implementación de la norma de la Industria de Tarjetas de Pago, en donde se determinaron las tendencias de los riesgos asociados a tarjetas de crédito en la banca venezolana, y se desarrollarán políticas para dar respuesta a los mismos, que no solo permitirán el fortalecimiento de la entidad bancaria en sí a nivel de seguridad, sino que repercute en los procesos de negocio.

CAPITULO I

PROPUESTA DE LA INVESTIGACIÓN

1.1. Planteamiento del Problema

A nivel mundial se ha producido un crecimiento acelerado de la industria de las tarjetas de crédito en los últimos sesenta años, si bien se han generado resultados positivos, ha traído como consecuencia el incremento en transacciones fraudulentas producto de defraudadores ocasionales o profesionales que han ido evolucionando sus técnicas con el transcurso de los años. Esta situación ha generado pérdidas millonarias a la industria de tarjetas de pago y a la banca venezolana.

Es por ello que en septiembre del 2006 Visa, Master Card, American Express, Discover y JCB formaron un organismo independiente denominado Consejo para el Estándar de Seguridad en la Industria de las Tarjetas de Pago, o como sus siglas en inglés PCI SSC (Payment Card Industry Security Standards Council) con el objetivo de elaborar una norma que permita a las organizaciones que procesan, almacenen y transmitan datos de titulares de tarjetas crear políticas para el aseguramiento de los datos con la finalidad de prevenir los fraudes.

Actualmente en Venezuela el cumplimiento de la norma PCI no es obligatoria, sin embargo, las empresas de tarjetas de crédito instan a las instituciones bancarias a tomar las acciones correctivas pertinentes para el cumplimiento del estándar con la finalidad de minimizar el fraude.

A través de este Trabajo Especial de Grado se desarrollará un plan basándose en la norma de la industria de pago focalizado en el área de

conocimiento de la gestión de riesgos del PMBOK que permita a la banca venezolana fortalecer las brechas detectadas a través de estrategias de control y mitigación.

Con los resultados obtenidos las instituciones financieras contarán con la descripción detallada de herramientas que fortalecerán la seguridad de la información, trayendo como beneficio la confianza de sus tarjetahabientes, así como pérdidas económicas por concepto de multas debido al incumplimiento de normas de seguridad en la realización de transacciones.

De lo anteriormente planteado, se deriva la necesidad de desarrollar el diseño de un plan para la Implementación de la Norma de la Industria de las Tarjetas de Pago para la banca venezolana, donde se realice un análisis en la gestión de riesgos.

Para abordar esta iniciativa, en esta investigación, se plantean las siguientes interrogantes:

¿El área de la seguridad de la información en las diferentes entidades bancarias públicas y privadas conoce qué es la Industria de las Tarjetas de Pago?

¿Las entidades bancarias están poniendo en práctica los doce requerimientos en que se basa la norma de la Industria de Tarjeta de Pago?

¿Existe dentro de la organización una óptima gestión de riesgos que se base en normas desarrolladas por líderes de la industria en el área de la seguridad de la información, que conlleve a acciones asertivas en la planificación de inversiones de tecnología como en la optimización de los procesos?

Una vez conocidas estas interrogantes, y a manera de resumen, el presente TEG tendrá como finalidad responder a dichas inquietudes planteadas, y cómo objetivo fundamental que los resultados obtenidos, conclusiones, recomendaciones y lecciones aprendidas sirvan como herramientas para el fortalecimiento de la seguridad de la información en ambientes de tarjetas de crédito.

1.2. Justificación e Importancia de la Investigación

Para la banca venezolana resulta de suma importancia la seguridad de la información que conlleva el manejo de las transacciones con tarjetas de crédito. La gestión del riesgo forma parte de los procesos de negocio, sin embargo, el cómo se maneja esta incertidumbre es un factor que puede diferenciar a dos bancos a través una ventaja competitiva de imagen para sus clientes, así como desaceleración del crecimiento, producto de las pérdidas financieras.

Adicionalmente, en la actualidad la Superintendencia de las Instituciones del Sector Bancario, es un organismo que vela por los clientes de los diferentes bancos a través de normativas dentro de las cuales está el manejo de la seguridad de los datos, por tanto, este estudio permitirá a la banca aplicar un plan para minimizar los riesgos negativos.

A través de las conclusiones y lecciones aprendidas derivados del presente Trabajo Especial de Grado, las entidades bancarias podrán obtener como beneficio:

- Conocer un instrumento que permita detectar debilidades de acuerdo a los requerimientos de PCI.
- Priorizar los riesgos detectados.

- Conocer la probabilidad e impacto.
- Aplicar técnicas y estrategias para el control y la mitigación de los riesgos, de acuerdo a las recomendaciones descritas en los requisitos de la norma de la industria de pago.
- La implementación de un plan para la gestión de riesgos acorde a PCI.

1.3. Objetivo General

Diseñar un plan para la implementación de la norma de la Industria de Tarjetas de Pago en entidades bancarias venezolanas.

1.4. Objetivos Específicos

- Identificar y describir los requisitos de la norma de la Industria de Tarjetas de Pago.

- Priorizar los riesgos que pueden generarse ante las brechas de seguridad, de acuerdo a la clasificación de los requisitos de la norma de la Industria de Tarjetas de Pago.

- Definir estrategias para el control y mitigación de riesgos asociados por el no cumplimiento de los requerimientos de la Industria de Tarjetas de Pago.

- Caracterizar los elementos teóricos, técnicos, conclusiones y lecciones aprendidas.

- Elaborar un plan para la implementación de la norma de la industria de tarjetas de pago.

1.5. Alcance de la Investigación

El presente Trabajo Especial de Grado se encuentra enmarcado en la norma de seguridad de datos establecida en el año 2006 por la Industria de las Tarjetas de Pago, la cual está conformada por doce requerimientos.

Adicionalmente el estudio se enfoca en entidades bancarias venezolanas públicas o privadas que almacenen, procesen o trasmitan datos de tarjetas de crédito.

Por otro lado, el Presente Trabajo Especial de Grado estará focalizado en las técnicas y herramientas descritas en la Gestión del Riesgo del Project Management Institute para lograr los objetivos planteados.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes de la Investigación

Para desarrollar los objetivos planteados en el Trabajo Especial de Grado se consultaron estudios asociados a la tecnología de la información con la finalidad de enriquecer los conocimientos y metodología que serán aplicados, los cuales se presentan a continuación:

Palacios. J. (2008)***. Evaluación del desarrollo de los fundamentos teóricos de seguridad de la información en la banca comercial y universal de Venezuela.*** Trabajo Especial de Grado realizado para optar por el Título de Magíster en Gerencia de Sistemas de Información no publicado Universidad Católica Andrés Bello, Caracas.

El Trabajo Especial de Grado aporta una visión globalizada de los fundamentos más importantes y característicos que conforman la seguridad de la información, específicamente para el área de la banca que es objeto de nuestro estudio.

Pellegrino. A. (2004). ***Efectos del fraude electrónico mediante tarjetas de débito y crédito en la banca venezolana, período comprendido 2003, primer trimestre 2004.*** Trabajo Especial de Grado para optar por el Título de Especialista en Instituciones Financieras. Mención Análisis y Gestión de las Instituciones Financieras no publicado. Universidad Católica Andrés Bello, Caracas.

Este Trabajo Especial de Grado, permitió conocer cuáles son los efectos del fraude electrónico en la banca venezolana, los riesgos que pueden ocasionarse, así como las prácticas que se implementaron hace seis años como entrada para el plan de la gestión de los riesgos.

Fermín. N. (2010). ***Desarrollo de un plan de gestión de proyecto para la implementación del sistema de gestión de seguridad de la información.*** Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Este Trabajo Especial de Grado ofrece un significativo aporte ya que es cónsono con el área de la seguridad de la información. Adicionalmente, está enfocado en una implementación, por lo que servirá como apoyo para la metodología del estudio en cuestión.

Pérez. H. (2007). ***Los fraudes con tarjetas de crédito y sus efectos financieros en el BBVA Banco Provincial***. Trabajo Especial de Grado para optar por el Título de Especialista en Instituciones Financieras. Mención Análisis y Gestión de las Instituciones Financieras no publicado. Universidad Católica Andrés Bello, Caracas.

Este Trabajo Especial de Grado, ofrece un enfoque de suma importancia, ya que enriquece la presente investigación con los efectos financieros que se producen por los fraudes con las tarjetas de crédito en una entidad bancaria de importante trayectoria como lo es el BBVA Banco Provincial. Esta información será de mucha utilidad para la Gestión de Riesgos que será desarrollada así como se evidenciarán las políticas con que cuenta un banco que se encuentra a nivel mundial, por lo que cuenta con una madurez en el área de la seguridad de la información.

Rivas. A. (2010). ***Diseño de un Plan para la Implementación de Proyectos de Servicios de Tecnología De Información Caso: Virtualización De Almacenamiento De Datos.*** Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Presentó como Objetivo General: Diseñar un plan para la implementación de proyectos de servicios de virtualización de almacenamiento de datos.

Y como Objetivos Específicos: Realizar un diagnóstico de las herramientas que se utilizan para implantar proyectos en el área de virtualización de almacenamiento de datos. Analizar las áreas de conocimiento del Project Management Institute involucradas en la implantación de proyectos sobre virtualización de almacenamiento de datos. Estructurar los elementos conceptuales, técnicos y de lecciones aprendidas en un plan que sirva de apoyo a los especialistas de informática en la implantación de proyectos de virtualización de almacenamiento de datos.

Este Trabajo Especial de Grado se enfoca en realizar un estudio exhaustivo para conocer cuáles son las mejores prácticas para el diseño de servicios de virtualización para el almacenamiento de datos. Está orientado hacia el área de la tecnología de la información y aporta a la presente investigación herramientas para la elaboración del presente estudio ya que está enmarcado en el área de la tecnología.

Rolingsón. J. (2004). ***Propuesta metodológica para la implantación y mejora de la gestión de riesgos en organizaciones de proyectos.*** Trabajo Especial de Grado realizado para optar por el Título de Especialista

en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Presentó como Objetivo General: Desarrollar una propuesta metodológica para la implantación de la gestión de riesgos en organizaciones de proyectos, que permita su desarrollo estructurado en función a las necesidades propias de la organización.

Y como Objetivos Específicos: Seleccionar, evaluar y adaptar un modelo de madurez de gerencia de riesgos como marco de referencia del nivel de desarrollo alcanzado por una organización de proyectos. Proponer un plan de implementación genérico, que permita evolucionar hacia nuevos niveles de desarrollo de la gestión de riesgos de acuerdo a la estrategia deseada de la organización. Identificar y proponer algunas herramientas de soporte al proceso de implantación.

Este Trabajo Especial de Grado ofrece un aporte importante hacia la gestión de los riesgos que forma parte esencial de los objetivos propuestos. Esta área de conocimiento suele ser una de las áreas más complejas en la gerencia de proyectos, y este estudio ofrece una orientación en cómo abordarlo.

Cavalieri. I. (2007). ***Metodología para la gestión de riesgos de los proyectos de la empresa de ingeniería TEENS CONSULTORES.*** Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Presentó como Objetivo General: Proponer una metodología para la Gestión de Riesgos de la Empresa “Teens Consultores”.

Y como Objetivos Específicos: Caracterizar los proyectos que maneja la empresa. Identificar los Riesgos de los Proyectos de la Empresa. Caracterizar los riesgos de la empresa. Evaluar la gestión actual de riesgo de los proyectos. Desarrollar una metodología para la gestión.

Este Trabajo Especial de Grado nos permite conocer como aplicar las herramientas y técnicas de la gestión de riesgos que es fundamental para este estudio.

Ordoñez. V. (2007). ***Diseño De Un Sistema De Gestión Por Procesos Para Sincrudos De Oriente Sincor, C. A.*** Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Presentó como Objetivo General: Diseñar un sistema de gestión por procesos para Sincrudos de Oriente Sincor, C. A., como plataforma al sistema de gestión de la calidad de su negocio de mejoramiento de crudo; enfocado en el cumplimiento de los requisitos de la Norma ISO 9001:2000.

Y como Objetivos Específicos: Diseñar los mapas y matrices de estructuración de procesos que permitan la identificación de los procesos, visualización de la desagregación, secuencia e interacción de los mismos; así como, sus aspectos claves de control. Formular mejoras para la optimización de los procesos del negocio de mejoramiento de crudo de Sincrudos de Oriente Sincor, C. A. Formular un plan de acción, en base a la estructura de procesos, para el desarrollo de la documentación e implementación del sistema de gestión de la calidad de Sincrudos de Oriente Sincor, C. A.

Este Trabajo Especial de Grado está relacionado con la optimización de los procesos de Sincrudos de Oriente Sincor, C. A., con respecto a la norma ISO 9001:2000, si bien esta norma está relacionada con el área de conocimiento de la calidad, nos orienta en como formular soluciones para una empresa.

Los siguientes artículos electrónicos fueron utilizados como antecedentes para la investigación:

R.A., C. (2009). TARJETA DE CRÉDITO. Este artículo permite conocer la historia y origen de las tarjetas de crédito, un punto importante para el Trabajo Especial de Grado.

Industria de Tarjetas de Pago (PCI). (2009). Normas de seguridad de datos. El artículo es uno de los aportes más importante para el Trabajo Especial de Grado, ya que en él se describen los requerimientos de la norma de la Industria de Tarjeta de Pago.

Angarita. Guillermo. (2009). Payment Card Industry Digital Security Standards “PCI DSS”. El artículo fue realizado por un especialista certificado por la Industria de Tarjetas de Pago, para realizar las evaluaciones y certificaciones a las empresas, es muy importante porque ofrece una visión de acuerdo a la experiencia del autor, de los factores más destacados de la norma y sus características.

2.2. Fundamentos Teóricos

2.2.1. Historia de la Banca Venezolana

El Banco Nacional fue creado en 1841 a través de la participación del Estado, el mismo quebró y fue suplantado en 1850 por el Congreso

Constitucional. Posteriormente se crea el Banco de los Trabajadores de Venezuela cuyo capital era originario del gobierno y por el interés de que se fusionaran otros bancos a nivel nacional.

En 1889 se crea el Banco Maracaibo y en 1890 se crea el Banco Caracas, sin embargo la banca venezolana se inicia en 1916 cuando es fundado el Banco Comercial de Maracaibo y el Royal Bank of Canadá. Posteriormente en 1917 se establece el National City Bank.

En Venezuela los comerciantes ejercían funciones de Banco ya que guardaban depósitos de los agricultores hasta 1933.

En los años veinte se impulsó significativamente el crecimiento de la banca venezolana a raíz del sector petrolero, se creó el Banco Holandés Unido, el Venezolano de Crédito, Mercantil y Agrícola. Debido a este crecimiento los créditos de la banca venezolana aumentaron siete veces y los depósitos de diez. Luego a finales de dicha década se crean los bancos Agrícola, Pecuario y el Obrero.

Debido al crecimiento bancario en nuestro país se incrementan y mejoran significativamente los servicios, a su vez reduciendo los costos e incrementando las ganancias.

A finales de la década de los veinte, hubo una crisis en las instituciones financieras en nuestro país, afortunadamente ningún banco llegó a la quiebra a diferencia de países de norte América o Europa.

En 1936 se establece en nuestro país el Banco de Londres y en 1937 se funda el Banco Industrial de Venezuela, en el año 1939 ocurre el Banco Central de Venezuela.

2.2.2. Banca Venezolana

De acuerdo con Muci y Martín (2004), el sector bancario financiero es aquel que se encarga en promover servicios de transacción a sus clientes, consiste en promover transacciones entre los clientes actuando como intermediarios, ya que toman dinero prestado en aras de crear un beneficio entre los inversionistas y la inversión final.

El sector bancario es la figura que se encarga de ofrecer servicios financieros como un intermediario en virtud de generar beneficios, la banca influye de manera determinante al crecimiento económico de un país.

De acuerdo con el autor Maza (1995), los beneficios que otorgan los intermediarios bancarios son:

- Promover el ahorro nacional.
- Ser eje operativo del sistema de pagos.
- Brindar servicios financieros al sector real de la economía, procurando el desarrollo económico y el bienestar social del país.
- Canalizar el ahorro hacia la inversión productiva.
- Apoyar a los servicios públicos y privados.
- Facilitar las relaciones financieras con el exterior.
- Distribuir fondos a nivel nacional.
- Diseñar instrumentos de pago innovadores.
- Garantizar la liquidez, la rentabilidad y la solvencia del sistema económico del país.

2.2.3. La Banca y la Seguridad de la Información

En Venezuela en el transcurso de los años se ha incrementado significativamente la importancia de la seguridad de la información, haciendo principal énfasis al sector bancario.

Se define como la seguridad de la información a aquellos patrones frente a la cual una compañía toma decisiones de protección de la información con base en sus objetivos y propósito. El proceso de toma de decisiones requiere la definición de una política y de un plan de acción para alcanzar los objetivos de seguridad de la información. La estrategia permite definir los procesos y estructuras requeridos para los criterios de confidencialidad, integridad y disponibilidad de los datos a través de estándares y normas creados por empresas u organismos de acuerdo a las mejores prácticas.

2.2.3.1. Marco Jurídico de la seguridad de la información venezolana

A continuación se presenta el marco jurídico que ha sido creado en Venezuela con la finalidad de regular a la banca venezolana con el objetivo de ofrecer a sus ahorristas seguridad en sus transacciones.

De acuerdo con Medina, Flores y Ojeda (2009), en el año 2000 se promulga la Superintendencia de Bancos y otras Instituciones Financieras, SUDEBAN, siendo un organismo autónomo, adscrito al Ministerio de Finanzas, en donde expone en su artículo 213 que velará por la inspección, supervisión, vigilancia, regulación y control de los bancos, entidades de ahorro y préstamo, otras instituciones financieras, casas de cambio, operadores cambiarios fronterizos, empresas emisoras y operadoras de tarjetas de crédito.

Como se mencionó anteriormente, en Venezuela se han creado leyes relativas a la banca y a la seguridad de la información, tales como: la Ley General de Bancos y otras Instituciones Financieras (2000), Ley Orgánica de Ciencia, Tecnología e Innovación (2005), la Ley sobre Mensajes de Datos y Firmas Electrónicas (2001) y la Ley Especial sobre Delitos Informáticos (2001).

A continuación se realizará una breve descripción de las mismas:

Ley General de Bancos

La Ley General de Bancos y otras Instituciones Financieras, manifiesta en sus artículos 233, 234, 251 y 252, que la información bancaria debe manejarse de manera confidencial por los organismos que la posean, y adicionalmente debe ser suministrada de la misma manera por los entes de control que la ameriten, por lo que se hace necesario que sea administrada de manera segura.

Adicionalmente, dicha ley en sus artículos 444, 445, 446 y 447, señala que quien utilice los medios informáticos o mecanismos similares para apoderarse, manipular o alterar papeles, cartas, mensajes de correo electrónico o cualquier otro documento que repose en los archivos electrónicos de un banco, entidad de ahorro y préstamo, institución financiera o casa de cambio, perjudicando el funcionamiento de las empresas regidas por este Decreto Ley o a sus clientes, será penado con prisión de ocho (8) a diez (10) años.

Ley Orgánica de Ciencia, Tecnología e Innovación

La Ley Orgánica de Ciencia, Tecnología e Innovación (2005) manifiesta en su artículo 3 que forman parte del Sistema Nacional de Ciencia Tecnología e Innovación, las instituciones públicas o privadas que generen, desarrollen conocimientos científicos, tecnológicos y procesos de innovación, así como las personas que se dediquen a la planificación, administración, ejecución y aplicación de actividades que posibiliten la vinculación efectiva entre la ciencia, la tecnología y la sociedad (tal es el caso de las entidades del sector bancario).

Adicionalmente, dicha ley en su artículo 4, expresa la necesidad de estimular la capacidad de innovación tecnológica del sector productivo, empresarial y académico, tanto público como privado, a través de mecanismos que permitan la inversión de recursos financieros para el desarrollo de las actividades científicas, tecnológicas y de innovación.

La Ley sobre Mensajes de Datos y Firmas Electrónicas

En su artículo 1, manifiesta que se otorga y reconoce la eficacia y el 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 (tal es el caso de las operaciones electrónicas efectuadas por parte de las entidades del sector bancario).

La ley en su artículo 7, expresa que cuando se requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un Mensaje de Datos si se ha conservado su

integridad y cuando la información contenida en dicho Mensaje de Datos esté disponible. A tales efectos, la ley establece que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación.

En el artículo 27 de dicha ley se expresa que la Superintendencia de Servicios de Certificación Electrónica (adscrita al Ministerio de Ciencia y Tecnología) podrá adoptar las medidas preventivas o correctivas necesarias para garantizar la confiabilidad de los servicios prestados por los Proveedores de Servicios de Certificación, por lo que, podrá ordenar, entre otras medidas, el uso de estándares o prácticas internacionalmente aceptadas para la prestación de los servicios de certificación electrónica, o que el proveedor se abstenga de realizar cualquier actividad que ponga en peligro la integridad y la seguridad del dato o el buen uso del servicio de los sistemas de información (tal es el caso de los sistemas de información y la plataforma tecnológica que soporta las operaciones de las entidades del sector bancario).

La Ley Especial contra Delitos Informáticos

Expresa en su artículo 1 que es objeto de protección integral 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 (tal es el caso de los sistemas de información y la plataforma tecnológica que soporta las operaciones de las entidades del sector bancario).

Adicionalmente dicha ley en sus artículos del 13 al 26, expresan que serán aplicadas sanciones para aquellos que a través del uso de tecnologías de

información, accedan, intercepten, interfieran, manipulen o usen de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, con prisión de dos (2) a seis (6) años y multa de doscientas (200) a seiscientas (600) unidades tributarias.

2.2.4. Tarjetas De Crédito

El concepto de realizar operaciones a crédito se inició en Europa, sin embargo, fue en Estados Unidos en 1924 que tomó auge cuando la empresa de provisión de gasolina General Petroleum Corporation puso en funcionamiento la primera tarjeta de crédito, posteriormente en 1929 La American Telephone & Telegraph.

En 1940 se restringe su uso debido a la segunda guerra mundial, no obstante este sistema era poco práctico debido a que cada tarjeta solo podía ser usada en los establecimientos de la empresa emisora, hasta 1949 que Frank X. McNamara, un banquero norteamericano crea Diners Club, la primera empresa independiente en donde una sola tarjeta podría usarse en diversos comercios.

En los años siguientes se iniciaron nuevas empresas tales como American Express, la compañía hotelera Hilton, Bank Americard (posteriormente VISA), Master Charge que luego cambió a Mastercard.

2.2.4.1. Datos que componen las Tarjetas de Crédito

A continuación se describe los datos que componen las tarjetas de crédito, las cuales son utilizadas para la conformación exitosa de las transacciones.

Chip: posee un microprocesador y posiblemente una memoria en la que se pueden almacenar aplicaciones y datos.

Número de Cuenta Primario: es el número de la tarjeta de pago (crédito o débito) que identifica al emisor y la cuenta del tarjetahabiente.

Figura 1. Componentes de la Tarjeta de Crédito
Fuente: Industria de Tarjetas de Pago. (2009)

Código de Validación de la Tarjeta: número de tres dígitos ubicado en la parte posterior derecha de la tarjeta para proveedores como Discover, JCB, MasterCard y Visa y denominado (CAV2, CID, CVC2 Y CVV2) respectivamente. Para el caso de American Express, el mismo es un código de cuatro dígitos ubicado en la parte delantera de la tarjeta denominado CID.

Este código es utilizado para la verificación de transacciones cuyo cliente no se encuentra físicamente tales como: Internet, correo, fax o vía telefónica. Debido al aumento de los fraudes a tarjetas de créditos por estas vías, actualmente es obligatorio proporcionar este código.

Banda Magnética: es la banca oscura presente en la parte posterior de la tarjeta, en ella se presentan los datos codificados para la autorización de una transacción cuando el cliente se encuentra presente. Estos datos también pueden ser encontrados en el Chip, en caso que el banco haya implementado esta tecnología.

Figura 2. Componentes del Reverso de la Tarjeta de Crédito
Fuente: Industria de Tarjetas de Pago. (2009)

2.2.5. Industria de las Tarjetas de Pago

En septiembre del 2006 Visa, Master Card, American Express, Discover y JCB formaron un organismo independiente denominado Consejo para el Estándar de Seguridad en la Industria de las Tarjetas de Pago, o como sus siglas en inglés PCI SSC (Payment Card Industry Security Standards Council) con el objetivo de elaborar una norma que permita a las organizaciones que procesan, almacenan y transmitan datos de titulares de tarjetas crear políticas para el aseguramiento de los datos con la finalidad de prevenir los fraudes.

La norma de la Industria de las Tarjetas de Pago se dividen en:

- **PCI PED:** aplica a dispositivos de entrada y define las características que deben contar los mismos.

- **PCI PA-DSS:** aplica a vendedores de software que desarrollan aplicaciones que almacenan, procesan o transmitan números de tarjetas de crédito.

- **PCI DSS:** aplica a cualquier entidad que almacene, procese o transmita número de tarjetas de crédito.

Para este Trabajo Especial de Grado se trabajará en el último caso, para aquellas entidades que aplican, almacenen o procesen números de tarjetas de pago.

Los actores involucrados se describen a continuación:

Figura 3. Participantes Industria de Tarjeta de Pago

2.2.5.1. Requisitos para el cumplimiento de la norma de la Industria de las Tarjetas de Pago

De acuerdo a los estándares de la Industria de las Tarjetas de Pago (2009), a continuación se describen cuáles con los doce requerimientos exigidos para el cumplimiento de la misma:

- Requisito 1: Desarrollar y mantener una red segura.
- Requisito 2: No usar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.

- Requisito 3: Se deben proteger los datos del titular de las tarjetas de crédito que son almacenados.

- Requisito 4: Codificar la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.

- Requisito 5: Utilización y actualización de antivirus.

- Requisito 6: Desarrollar, mantener sistemas y aplicaciones seguras.

- Requisito 7: Restringir el acceso a los datos de los titulares de las tarjetas conforme a la necesidad de conocer de la empresa.

- Requisito 8: Asignar una ID única a cada persona que tenga acceso a equipos.

- Requisito 9: Restringir el acceso físico a datos de titulares de tarjetas.

- Requisito 10: Rastrear y supervise todo acceso a los recursos de red y datos de titulares de tarjetas.

- Requisito 11: Probar con regularidad los sistemas y procesos de seguridad.

- Requisito 12: Mantener una política que aborde la seguridad de la información para empleados y contratistas.

2.2.6. La Gerencia de Proyectos: un enfoque al desarrollo de un plan el área de la seguridad de la información

Se define como Gerencia de Proyectos, de acuerdo a la Guía de los Fundamentos de la Dirección de Proyectos (PMBOK), “a la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades de un proyecto para satisfacer los requisitos de dicho proyecto”; siendo Proyecto, “un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único” (Project Management Institute, 2008, pg 11).

Para el desarrollo del TEG relacionado con la seguridad de la información para transacciones con tarjetas de crédito, al área de conocimiento que aportará los conocimientos para el desarrollo del mismo es la gestión de riesgos.

- **Gerencia del Riesgo:** de acuerdo al Project Management Institute en el PMBOK (2008), indica que la gestión de los riesgos son los procesos involucrados para llevar la planificación de la gestión, identificación, análisis y planificación de la respuesta a los riesgos con la finalidad de minimizar el impacto producido por aquellos eventos negativos.

  El Trabajo Especial de Grado aborda el diseño de un plan para la implementación de las buenas prácticas establecidas por las principales empresas de pago a nivel mundial para minimizar los riesgos detectados en la banca venezolana a la exposición de data sensible por transacciones con tarjetas de crédito.

CAPITULO III

MARCO METODOLÓGICO

Este capítulo está referido al contexto operativo de la investigación a través del cual se fijan los lineamientos y procedimientos que se llevaron a cabo para el diseño de un plan para la implementación de la norma de la Industria de Tarjeta de Pago en entidades bancarias venezolanas, objetivo de este TEG. En este sentido se describen el tipo y diseño de investigación, unidad de análisis, población y muestra, las técnicas e instrumentos de recolección de datos, así como las técnicas para procesamiento y análisis de datos para el logro de los objetivos planteados.

3.1. Tipo de Investigación

Valarino, Yáber, y Cemborain (2010, p.66) cita a Hernández, Fernández y Baptista (2003), quien conceptualiza la investigación como "un conjunto de procesos sistemáticos y empíricos que se aplican al estudio de un fenómeno: es dinámica, cambiante y evolutiva". Por otro lado, Valarino, y cols. (2010), sostienen que la investigación científica tiene como objetivo principal generar o comprender nuevos conocimientos que puedan eventualmente formalizarse en forma de teorías o modelos. Se cumplen dos propósitos fundamentales: producir conocimientos y teorías (básica, pura o científica) y resolver problemas prácticos (investigación aplicada).

De acuerdo a lo descrito anteriormente, el tipo de investigación empleada en el presente TEG es investigación aplicada, en virtud de que se realiza fuera de un laboratorio y se basa en la investigación científica.

3.2. Diseño de Investigación

En función de la formulación de los objetivos generales y específicos, el TEG está enmarcado dentro del diseño de investigación de campo, conceptualizado por Arias (2006, p.31) como "… la recolección de datos directamente de los sujetos investigados o de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna, es decir, el investigador obtiene la información pero no altera las condiciones existentes". Adicionalmente, existen fuentes secundarias provenientes de documentación bibliográfica.

Ello se justifica ya que durante la investigación la fuente de información primaria, se constituye por los resultados obtenidos a través de cuestionarios a especialistas y gerentes del área de seguridad de información en entidades bancarias venezolanas.

Por tanto, considerando que no existe la manipulación de variables, se enmarcó como no experimental y de acuerdo a la perspectiva de temporalidad, transeccional, ya que los datos se obtuvieron en un período de tres semanas contadas a partir de la entrega de los cuestionarios hasta la recepción de la totalidad de los mismos.

3.3. Unidad de Análisis

De acuerdo con Hernández, Fernández y Baptista (2003, p.117), la unidad de análisis son los elementos que "van a ser medidos". Es este sentido, corresponde a los riesgos de la seguridad de los datos asociados a las transacciones con tarjetas de crédito en la banca venezolana.

3.4. Población y Muestra

De acuerdo con Arias (2006), la población en estudio u objetivo consiste en el conjunto de elementos para el cual serán válidas las conclusiones de la investigación y están delimitadas por el problema y los objetivos del proyecto.

La población del presente Trabajo Especial de Grado se conformó por treinta y tres entidades bancarias venezolanas, de las cuales once son públicas y veintidós privadas, las cuales se presentan a continuación (Tabla 1):

Tabla 1. Listado de Bancos

Nombre Banco	Público	Privado
Banco Bicentenario, C.A, Banco Universal.	1	
Banco Agrícola de Venezuela, C.A, Banco Universal.	1	
Banco Caroní, C.A. Banco Universal		1
Banco de Venezuela, S.A. Banco Universal	1	
Bancaribe C.A., Banco Universal		1
Banco del Tesoro, C.A. Banco Universal	1	
Banco Exterior, C.A. Banco Universal		1
Banco Internacional de Desarrollo, C.A. Banco Universal		1
Banco Nacional de Crédito, C.A. Banco Universal		1
Banco Occidental De Descuento, Banco Universal, C.A.		1
Banco Provincial, S.A. Banco Universal		1
Banco Sofitasa Banco Universal, C.A.		1
Banesco Banco Universal, C.A		1
BFC Fondo Común, C.A.,		1
Banco Universal Citibank, N.A., Banco Universal.		1
Corp Banca, C.A. Banco Universal		1
Del Sur Banco Universal, C.A. Mercantil, C.A.		1
Banco Universal Venezolano De Crédito, S.A., Banco Universal		1
Banco Activo, C.A. Banco Universal		1
Banco Del Pueblo Soberano, Banco Comercial	1	
The Royal Bank Of Scotland, N.V.		1
Banco de Exportación y Comercio, C.A. Banco Comercial	1	
Banco Guayana, C.A.		1
Banco Plaza, C.A.		1
Banplus Banco Comercial, C.A.		1
Banco de Comercio Exterior (Bancoex)	1	
Banco Industrial de Venezuela, C.A.	1	
Banco Nacional de Vivienda Y Hábitat	1	
Bancamiga, Banco De Desarrollo	1	
Banco de Desarrollo Económico y Social de Venezuela (Bandes)	1	
Banco de la Gente Emprendedora (Bangente), C.A.		1
Bancrecer, S.A. Banco De Desarrollo		1
Mi Banco. Banco De Desarrollo		1
	11	**22**

Fuente: Superintendencia de las Instituciones del Sector Bancario (2010)

“La muestra es un subconjunto representativo y finito que se extrae de la población accesible”, (Arias, 2006, pág. 83), por tanto, a partir de la población se procedió a delimitar el número de unidades que la integran para que resultaran más accesibles.

La muestra objeto de estudio está conformada por especialistas y gerentes del área de seguridad de la información, cuatro para entidades públicas y siete (7) para entidades privadas para un total de once individuos. Estos participantes fueron elegidos en base a un muestreo intencional u opinático; de acuerdo con Arias (2006), es la selección de los elementos con base a criterios o juicios del investigador, los mismos fueron elegidos de acuerdo a la accesibilidad, acuerdos de confidencialidad y fines académicos debido a la criticidad de la información que se maneja.

3.5. Técnicas e instrumentos de recolección de datos

La recolección de información se realizó haciendo uso de la modalidad de encuesta escrita denominada cuestionario, que consiste en responder una serie de preguntas y se caracteriza por ser autoadministrado, es decir, se responde sin la presencia, asesoría o influencia del encuestador.

En el encabezado del instrumento se incorporó un breve instructivo en donde se plantearon los objetivos, la confidencialidad, así como definición de escalas.

El instrumento se estructuró en base a dieciocho preguntas, (véase apéndice A), las mismas fueron planteadas en forma cerrada, es decir, en donde se presentan opciones de respuestas claras tales como: si, no y con escalas de medición: insignificante, menor, moderado, importante, extremo, que fueron

definidas en el instructivo y en donde el encuestado seleccionaría aquella que más se adecue.

Adicionalmente, fueron incorporadas preguntas abiertas en donde existe la libertad de que el encuestado exponga su criterio sin opciones preestablecidas.

Al realizarse el diseño se contempló que las interrogantes y las opciones de respuestas fueran expuestas de forma clara, con la finalidad de evitar ambigüedades ya que las mismas representaban una fuente de suma importancia para recabar los datos requeridos para el cumplimiento de los objetivos.

Por otro lado el instrumento fue revisado y validado en base a dos criterios fundamentales:

- **Técnicas de cuestionario:** fue revisado y validado por un sociólogo, quien cuenta con la pericia para verificar que la estructura fuera la adecuada para recopilar la información propuesta.

- **Contenido:** fue revisado y validado por un asesor de seguridad certificado por el PCI Security Standards Council.

3.6. Técnicas para procesamiento y análisis de datos

La información que se obtuvo, a través de los cuestionarios realizados, fue la fuente que permitió el desarrollo del plan para la implementación de la norma de tarjetas de pago en entidades bancarias venezolanas.

De acuerdo con Valarino, y cols. (2010), para el procesamiento de los datos se utilizó la estadística descriptiva que consiste en el análisis y la representación de los datos. Al analizarse los resultados obtenidos a través del cuestionario se obtuvieron medidas de tendencia central, tales como la moda, medianas o medias. Estos valores fueron representados en forma de barras y en tablas.

3.6.1. Estructura Desagregada de Trabajo

La estructura desagregada de trabajo se presenta con la finalidad de realizar un desglose en componentes para el desarrollo del TEG y sirva de apoyo para el cumplimiento de los objetivos planteados.

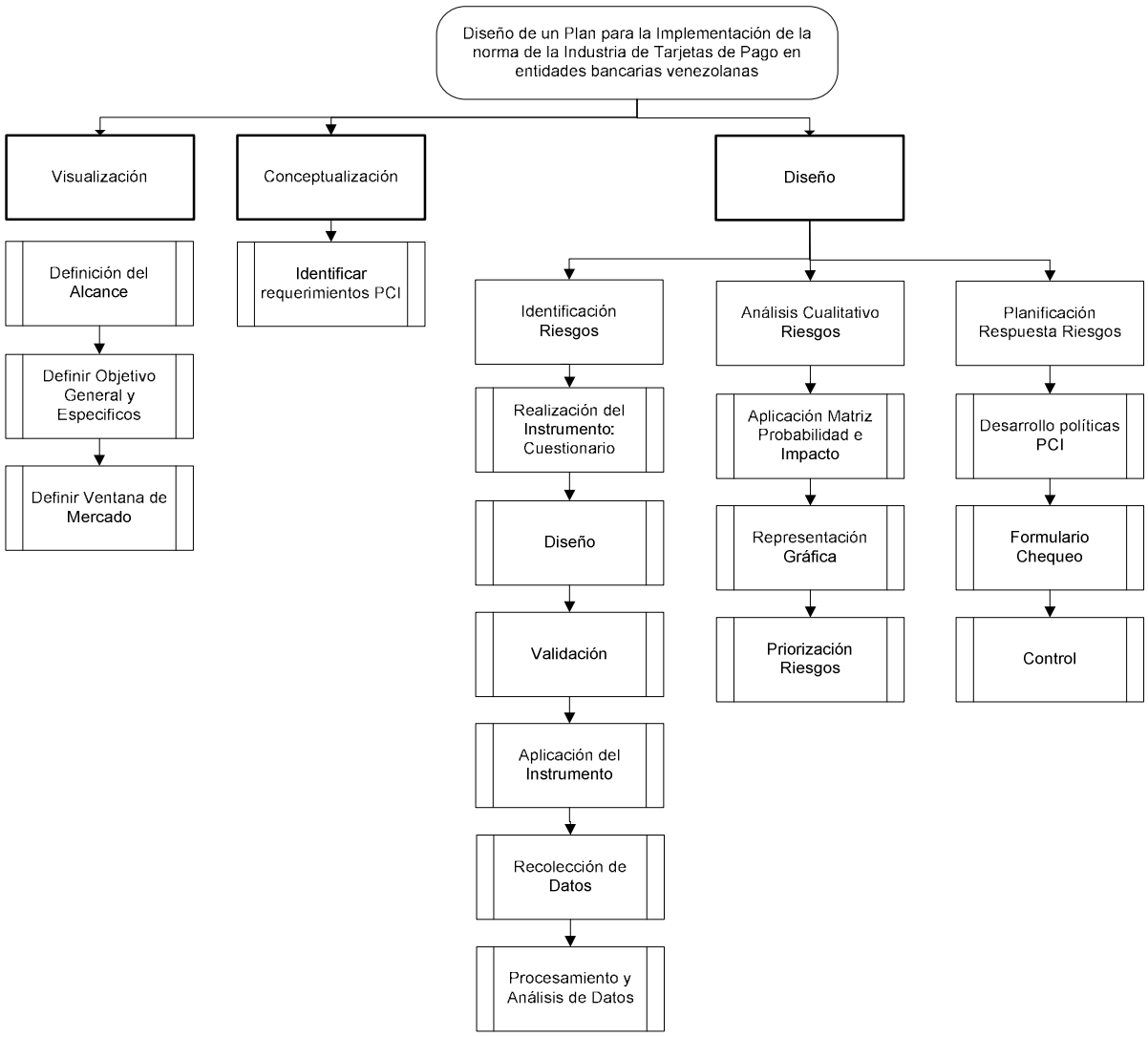

Figura 4. Estructura Desagregada de Trabajo

Los componentes principales para el diseño del plan están conformados por tres procesos fundamentales de la gestión de riesgos:

- Identificación de Riesgos.
- Análisis Cualitativo de Riesgos.
- Planificación de Respuesta a los Riesgos.

3.6.1.1. Identificación de Riesgos

Consistió en el proceso mediante el cual se determinaron los riesgos que pueden afectar a la banca venezolana.

La herramienta y técnica utilizada fue de analizar y describir cuáles son los requisitos que componen la norma de la industria de la tarjeta de pago, con la finalidad de comprender los lineamientos y buenas prácticas descritas en la misma para así conocer las brechas en la seguridad de la información que se derivan por el no cumplimiento, lo que se traduce en riesgos para la organización.

Los riesgos fueron descritos en dieciocho interrogantes en el instrumento explicado en el apartado de las técnicas y recolección de datos, se contemplaron aspectos que traen efectos negativos por las amenazas que conllevan, no fue foco de estudio oportunidades que podrían generarse.

3.6.1.2. Análisis Cualitativo

Para el análisis cualitativo se utilizaron métodos para priorizar los riesgos identificados, con el objeto de que el plan sea desarrollado de forma efectiva, enfocándose en los de mayor a menor criticidad.

La evaluación de la prioridad de los riesgos identificados se realizó a través de la construcción de una matriz de probabilidad e impacto que consistió en:

Definición de escala de impacto:

La escala de impacto de riesgos se desarrolló con la finalidad de reflejar la severidad de sus efectos con los objetivos del proyecto, es decir, la

erradicación de la exposición de información sensible en las entidades bancarias.

El impacto se desarrolló a través de una escala ordinal, en donde los valores fueron ordenados por rango:

- Insignificante: 5.
- Menor: 10.
- Moderado: 20.
- Importante 40.
- Extremo 80.

Estos rangos se determinaron con el apoyo de los gerentes y especialistas de las entidades bancarias encuestados a través de tormentas de ideas, si bien determinar una escala puede ser subjetivo ya que se utiliza el juicio basado en la experiencia, se realizó una homologación de criterios en virtud de que la escala reflejara el impacto por la exposición de data sensible para las organizaciones.

Tabla 2. Escala de Impacto para la Organización

Escala de Impacto para la Organización

	Insignificante 5	**Menor** 10	**Moderado** 20	**Importante** 40	**Extremo** 80
Exposición de Información sensible asociado a tarjetas de crédito	Riesgo mínimo de exposición de información sensible	Riesgo bajo de exposición de información sensible	Riesgo medio de exposición de información sensible	Riesgo alto de exposición de información sensible	Riesgo eminente de exposición de información sensible

Definición de la probabilidad de ocurrencia:

Posteriormente se determinó la escala de probabilidad de ocurrencia de los riesgos se suscitaron en la organización en el último año. La misma se

desarrolló empleando la técnica tormentas de ideas con especialistas y gerentes de las entidades bancarias que brindaron la información de acuerdo a lo suscitado en sus organizaciones, un mínimo número de incidencias hasta situaciones poco frecuentes de eventos ocurridos entre seis a más ocasiones.

- Nunca: 10%.
- Una vez en el último año: 30%.
- Cuatro a cinco veces en el último año: 70%.
- Seis a más veces en el año: 90%.

Tabla 3. Escala de Probabilidad e Impacto

Matriz de Probabilidad e Impacto						
Probabilidad		**Impacto (Amenazas)**				
Rango	**%**	**Insignificante**	**Menor**	**Moderado**	**Importante**	**Extremo**
		5	**10**	**20**	**40**	**80**
Nunca	**10%**	0.5	1	2	4	8
Una vez en el último año	**30%**	1.5	**3**	6	12	24
Dos a Tres veces en el último año	**50%**	2.5	5	**10**	20	40
Cuatro a Cinco veces en el último año	**70%**	3.5	7	14	28	56
Seis a más veces en el año	**90%**	4.5	9	18	36	72

Para cada riesgo expresado a través del instrumento, en caso de que el encuestado haya respondido que afirmativamente el evento haya ocurrido en su organización, en aras de otorgarle un valor acorde al impacto que el mismo originó y la ocurrencia del mismo en el último año para determinar la priorización de los riesgos, se realizó la multiplicación de las escalas tal como se evidencia en la tabla 4.

En el capítulo de análisis de resultados se podrá observar por medio de tablas, los resultados de cada encuestado, así como las medias aritméticas para cada riesgo.

A través de la obtención de las medias, se realizó la priorización de los riesgos en forma ascendente, en donde de mayor a menor puntaje representa la criticidad por concepto de exposición de data sensible asociada a tarjetas de crédito en la banca venezolana, con esta información el plan de desarrolló a través de desarrollo de políticas basadas en la norma de la industria de tarjetas de pago para mitigar y controlar los mismos.

3.6.1.3. Análisis Cuantitativo

No fue realizado un análisis cuantitativo para la presente investigación, debido a la dificultad de obtener información financiera producto de pérdidas asociadas por concepto de exposición sensible de tarjetas de crédito, por su naturaleza confidencial.

3.6.1.4. Planificación de Respuesta a los Riesgos

Al ser descritos y analizados los procesos de, identificación, análisis cualitativo de riesgos se cuenta con la priorización de los mismos clasificados de mayor a menor criticidad para las entidades bancarias venezolanas.

Para dar respuesta a los riesgos detectados se desarrollaron políticas de seguridad de información basadas en los requerimientos y buenas prácticas recomendadas por la industria de pago para el cumplimiento de la norma.

Por otro lado, se desarrolló un formulario de chequeo que refleja para cada una de las políticas desarrolladas el estatus de cumplimiento, fecha para la remediación y las acciones para que cada entidad bancaria haga uso del mismo para realizar una planificación interna en aras de cumplir con todas las políticas.

3.7. Operacionalización de los Objetivos

De acuerdo con Arias (2006, P63), la operacionalización de los objetivos o variables se usa en los procesos de investigación para transformar a los objetivos de conceptos abstractos a términos concretos, tangibles y cuantificables.

A continuación se presenta un resumen de la operacionalización de los objetivos:

Tabla 4. Operacionalización de los Objetivos

Eventos	Sinergias	Indicios	Técnicas	Instrumentos	Fuente
Identificar y describir los requisitos de la norma de la Industria de Tarjetas de Pago	Conjunto de buenas prácticas para la mitigación de riesgos asociados a la seguridad de la información de acuerdo a la norma PCI.	Doce requisitos que conforman la norma de la industria de tarjetas de pago, plenamente identificados	Análisis y estructuración de la información obtenida	Documental	Bibliográfica
Priorizar los riesgos que pueden generarse ante las brechas de seguridad, de acuerdo a la clasificación de los requisitos de la norma de la Industria de Tarjetas de Pago	Utilización de la metodología descrita para la gestión de riesgos.	Listado de riesgos de mayor a menor puntaje obtenido de acuerdo a la ocurrencia e impacto para la organización	Método Cualitativo	Tablas y gráficos	Personal especializado del área de seguridad de la información
Definir estrategias para el control y mitigación de riesgos asociados por el no cumplimiento de los requerimientos de la Industria de Tarjetas de Pago.	Utilización de la metodología descrita para la gestión de riesgos.	Plan de respuesta a los riesgos detectados en la banca venezolana de acuerdo a PCI.	Método de gestión de riesgos	Documental. Cuestionario.	Personal especializado del área de seguridad de la información Bibliográfica
Caracterizar los elementos teóricos, técnicos, conclusiones y lecciones aprendidas	Documento que contiene los aspectos clave del plan para el diseño de implementación de la norma PCI.	Documento que contiene las mejores prácticas para el diseño de un plan para la implementación de la norma de la industria de tarjetas de pago	Análisis y estructuración de la información obtenida.	Documental. Cuestionario.	Personal especializado del área de seguridad de la información
Elaborar un plan para la implementación de la norma de la industria de tarjetas de pago	Análisis de riesgos, priorización, control y mitigación para estructurar pautas para diseñar un plan que se adecue a una entidad bancaria.	Técnicas y herramientas para diseñar un plan adecuado a las necesidades de una entidad bancaria.	Análisis y Estructuración de un plan para identificar los riesgos, priorizarlos, definir estrategias de control y mitigación	Documental	Bibliográfica

3.8. Códigos de Ética

Los datos obtenidos a través del cuestionario aplicado a las diferentes entidades bancarias pertenecientes a la muestra, fueron estrictamente confidenciales y con fines académicos ya que dicha información es sumamente crítica para la organización.

Los códigos de ética bajo los cuales está regido este TEG son los siguientes:

- Código de Ética vigente del Colegio de Ingenieros de Venezuela.

- Responsabilidad Social y Profesional del Código de Ética del Project Management Institute (PMI).

- Código de ética personal relacionado con la moral, buenas costumbres y respeto.

3.9. Viabilidad de la Investigación

Para la aplicación del instrumento se contaba un listado de especialistas y gerentes del área de seguridad de la información del área bancaria, lo que facilitó el proceso de selección de personas clave, su contacto, así como la explicación de los objetivos del cuestionario y su carácter confidencial.

Debido a que este proceso fue realizado en la ciudad de Caracas, no implicó gastos de viáticos, por otro lado, el equipamiento o licenciamiento de software estaban disponibles dentro de los recursos del investigador. Adicionalmente, se contó con múltiples fuentes bibliográficas y la colaboración de asesores en el área.

CAPITULO IV

VENTANA DE MERCADO

4.1. Sistema Bancario Venezolano

El sistema bancario consiste en un conjunto de instituciones que permiten el desarrollo de todas aquellas transacciones entre personas, empresas y organizaciones que impliquen el uso de dinero.

El sistema bancario venezolano está integrado de la siguiente manera: Banca comercial y universal, Banco hipotecario, Banca de Inversión, Banca de desarrollo, Entidades de ahorro y préstamo, entre otros.

El 3 de noviembre de 2001, bajo Decreto No. 1.526 se promulga La Ley General de Bancos y otras Instituciones Financieras, se autorizaba a la Superintendencia de Bancos y Otras Instituciones Financieras a inspeccionar, vigilar y fiscalizar a los bancos y las demás instituciones de crédito.

A continuación se describen las funciones de las principales instituciones que velan por la seguridad de los usuarios y de las entidades bancarias:

Superintendencia de las Instituciones del Sector Bancario (SUDEBAN)

Según la Ley de Instituciones de Sector Bancario, la Superintendencia de Bancos debe ejercer inspección, supervisión, vigilancia, regulación y control de los Bancos Universales, Comerciales, con Leyes Especiales, de Inversión, Hipotecarios, Sociedades de Capitalización, Casas de Cambio, Almacenes Generales de Depósito, Oficinas de Representación de Bancos Extranjeros,

Arrendadoras Financieras, Fondos de Activos Líquidos y Entidades de Ahorro y Préstamo, con el objetivo de determinar la correcta realización de sus actividades a fin de evitar crisis bancarias y permitir el sano y eficiente funcionamiento del Sistema Financiero venezolano.

Comisión Bancaria Nacional (CBN):

La comisión bancaria nacional tiene como funciones:

- Estudiar las condiciones bancarias, económicas del país y enviar informes con sus conclusiones y recomendaciones a la Superintendencia de Bancos y al Banco Central de Venezuela.

- Responder las consultas que le sean realizadas a la Superintendencia de Bancos y el Banco Central de Venezuela.

- Estudiar, coordinar y mejorar las prácticas bancarias y velar que sean cumplidas a los fines de que se brinde un servicio óptimo al usuario del sistema bancario nacional.

- Estudiar las disposiciones y medidas que dicten el Ejecutivo Nacional, la Superintendencia de Bancos y el Banco Central de Venezuela.

- Informar a la Superintendencia de Bancos los casos de desacato o desatención por parte de sus miembros a las prácticas bancarias identificadas y mejoradas por el Consejo, a los fines de que ésta pueda imponer los correctivos correspondientes.

Fondo de Garantía de Depósitos y Protección Bancaria (FOGADE)

El objetivo es el de garantizar los depósitos del público mantenidos en bancos, entidades de ahorro y préstamo y demás instituciones financieras, regidas por la Ley General de Bancos y Otras Instituciones Financieras.

Adicionalmente, posee las funciones de liquidador de bancos, entidades de ahorro, préstamo y otras instituciones tanto financieras como no financieras, todo ello conforme a lo establecido por el Ordenamiento Jurídico vigente, a fin de contribuir con la confianza y estabilidad en el Sistema Financiero Nacional.

4.2. Leyes venezolanas

Lo expuesto anteriormente se enmarca en el sistema bancario nacional, no obstante el TEG se enfoca en un estudio de las transacciones con las tarjetas de crédito, por tanto, mencionamos:

La Asamblea Nacional de la República Bolivariana de Venezuela decretó en La Gaceta Oficial Nº 39.021 del 22 de septiembre de 2008:

"La presente Ley tiene por objeto regular, todos los aspectos vinculados con el sistema y operadores, de tarjetas de crédito, débito, prepagadas; y demás tarjetas, de financiamiento o pago electrónico, así como su financiamiento y las relaciones entre el emisor, el o la tarjetahabiente y los negocios afiliados al sistema, con el fin de garantizar el respeto y protección de los derechos de los usuarios y las usuarias de dichos instrumentos de pago, obligando al emisor de tales instrumentos a otorgar información adecuada y no engañosa a los y las tarjetahabientes; asimismo a resolver las controversias que se puedan presentar por su uso, conforme a lo previsto en la Constitución de la República Bolivariana de Venezuela y la ley".

La ley de tarjetas de créditos y débito tenía como objetivo principal la regulación de las relaciones jurídicas entre el emisor de la tarjeta de crédito o débito y los usuarios de las mismas, en la actualidad regula todos los aspectos que surgen de la relación entre emisores de tarjetas y sus usuarios o tarjetahabientes.

Se entiende como emisor a las instituciones financieras que otorgan el crédito al usuario y esto conlleva a un conjunto de obligaciones que de determinarse su incumplimiento les acarrea sanciones administrativas de índole económico y en algunos casos a las personas naturales que laboran en las mismas de acuerdo a los supuestos previstos en la misma Ley.

Para los casos en que el emisor sea una institución financiera debe solicitar a la Superintendencia de Bancos y otras Instituciones Financieras (SUDEBAN) la autorización para emisiones de las tarjetas respectivas.

Corresponde a esta Superintendencia autorizar, supervisar, inspeccionar, controlar y regular el ejercicio de la actividad que realizan las instituciones que conforman el sector bancario, así como, instruir la corrección de las fallas que se detecten en la ejecución de sus actividades y sancionar las conductas desviadas al marco legal vigente. Todo ello con el fin de garantizar y defender los derechos e intereses de los usuarios y usuarias del sector bancario nacional y del público en general.

4.3. La banca y PCI

Ante el crecimiento exponencial de la banca pública y privada y del uso de tarjetas de crédito, la certificación PCI es en la actualidad es uno de de los

requisitos más importantes que tendrá el sector bancario tanto en Venezuela como en el mundo entero.

PCI reúne las mejores prácticas desarrolladas por las industrias de tarjetas de pago para garantizar la seguridad de datos sensibles, que surge ante la creciente ocurrencia de brechas e incidentes de seguridad relacionados con las tarjetas crédito, ya sea que se trate del acceso, uso, exposición, alteración o destrucción no autorizada de información sensible relacionada a los sistemas o datos de las entidades emisoras de tarjetas de crédito.

Esta información se sustenta con la resolución No. 64110 emitida por la Superintendencia de Bancos y Otras Instituciones de fecha 23 de diciembre de 2010 en donde se presenta en el artículo 30:

"La gestión de seguridad, contingencias y comunicaciones deben estar en concordancia con lo establecido en:

- La circular No. SBIF-DSB-IO-GGT GRT-01907 de fecha 30 de enero de 2008, contentiva de la Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica Virtual y en Línea para los Entes Sometidos al Control Regulación Vigilancia y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras.

De igual forma podrán tener como referencia:

- El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS por sus siglas en inglés)".

Por lo anteriormente expuesto el desarrollo del TEG se enfoca en el desarrollo de un plan para la implementación de la norma basándose en la metodología de gestión de riesgos del PMI, lo que se traduce en fortalecer la estructura y los procesos de las instituciones bancarias para mitigar efectos negativos como las sanciones establecidas por la SUDEBAN, así como cumplir con sistemas de alerta temprana para generar reportes que serán remitidos y analizados por la SUDEBAN, con el objeto de que este Organismo emita al sector Bancario la normativa prudencial que considere pertinente, a los fines de prevenir la emisión de actos fraudulentos que puedan convertirse en prácticas reiteradas.

CAPITULO V

ANÁLISIS DE RESULTADOS

En virtud del logro de los objetivos planteados en el presente TEG se aplicó la técnica de recolección de datos del cuestionario, a una muestra de once (11) especialistas o gerentes de entidades bancarias a nivel nacional.

El cuestionario fue diseñado tal como se mencionó en el marco metodológico para identificar, analizar cualitativamente y priorizar los riesgos a los cuales están expuestos las entidades financieras nacionales de acuerdo a la norma de la industria de tarjetas de pago.

Para cada interrogante se presentará gráficamente la porción que los encuestados hayan respondido afirmativa o negativamente, debido a que este TEG se enfoca en los riesgos negativos, en los casos en donde se haya respondido que hubo incidencias de exposición de data sensible en su organización, se presenta adicionalmente la ocurrencia y el impacto del mismo en el último año, así como el valor obtenido a través de la aplicación de la matriz de probabilidad e impacto descrita en el marco metodológico en el apartado de análisis cualitativo.

Al ser analizados los resultados obtenidos para cada interrogante y las escalas, a través de las mismas se priorizaron los riesgos de mayor a menor criticidad, con la finalidad de que el plan sea desarrollado en aras de cumplir con uno de los objetivos específicos del presente TEG, de desarrollar estrategias de control y mitigación de acuerdo a las necesidades detectadas en Venezuela. A continuación se presentan los resultados obtenidos de acuerdo a los riesgos identificados:

6.1. Identificación de Riesgos

A continuación se ahondará en los riesgos identificados a través del instrumento de recolección de datos:

5.1.1. Identificación de Sistemas

La primera interrogante planteada en el instrumento consistió: **¿En su organización se tienen identificados todos los sistemas que almacenan, transmitan o procesan información relacionada con tarjetas de crédito?**

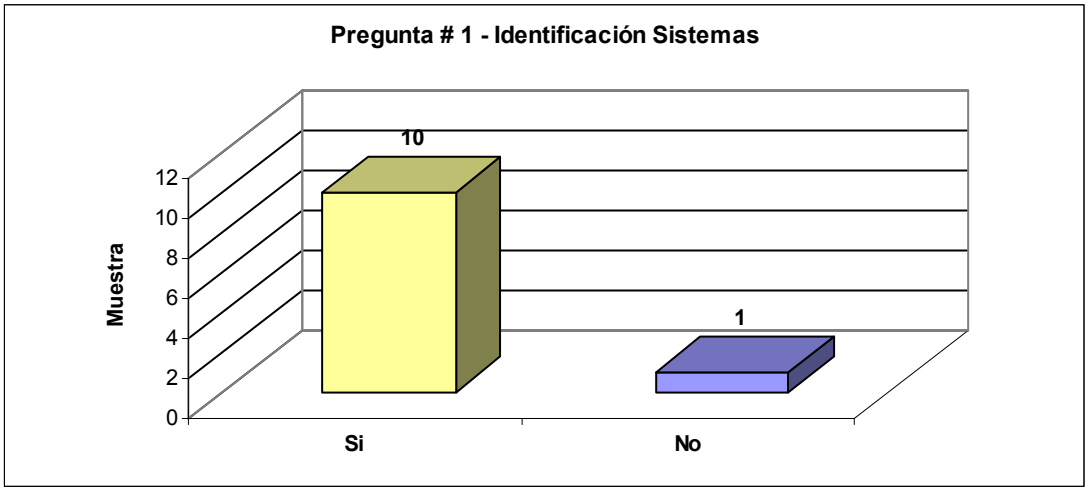

Figura 5. Identificación Sistemas

Para la pregunta número uno tal como se observa en la figura 5, del total de la muestra de once entidades bancarias, diez encuestados que representan el 91%, considera que en su organización están plenamente identificados los sistemas y componentes que almacenan, transmitan o procesan información relacionada con tarjetas de crédito, mientras que existe un entrevistado que contestó lo contrario, lo cual representa el 9%.

Debido a que este estudio está enmarcado en los riesgos negativos, se procedió a evaluar la probabilidad e impacto para el caso en donde no están identificados los sistemas.

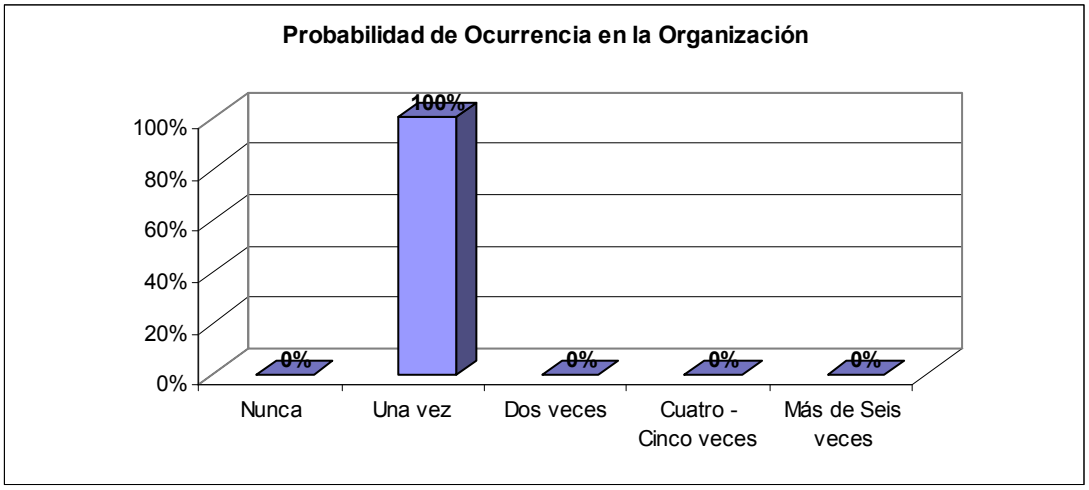

Figura 5.1 Probabilidad Ocurrencia en la Organización

La figura 5.1 muestra que el entrevistado respondió que en la organización este evento tuvo una ocurrencia en un 100% de una vez en el último año, adicionalmente, el impacto por exposición de data sensible fue insignificante, tal como se observa en la figura 5.2.

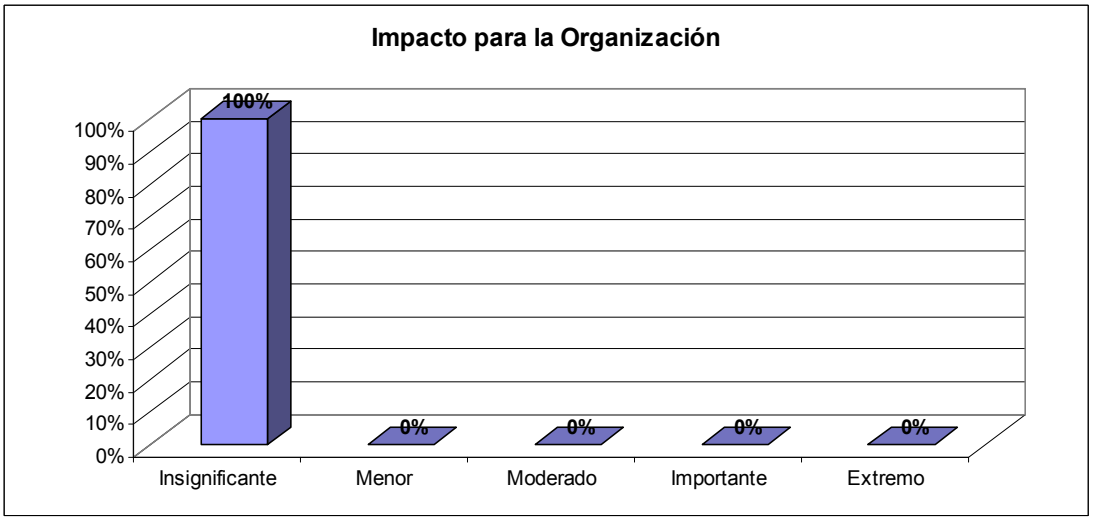

Figura 5.2 Impacto para la Organización

En conclusión, el entrevistado que expresó que esta incidencia se había suscitado en su entidad bancaria, tal como se observa en la tabla 5, su respuesta fue que había ocurrido en una ocasión en el último año, por tanto, se obtuvo una probabilidad de 30%, así como el impacto fue insignificante que representa 5 en la escala definida, al hacer uso de la matriz de probabilidad e impacto, al realizar la multiplicación se obtiene como resultado **1.50**, tal como se muestra a continuación:

Tabla 5. Escala Probabilidad e Impacto. Identificación de Sistemas

Entrevistado	Probabilidad	Impacto	Calificación
E1	30%	5	1.5
			1.50

5.1.2. División Lógica

La segunda pregunta planteada en el instrumento consistió:

¿En su organización existe una división lógica de los componentes asociados al almacenamiento, transmisión o procesamiento de la información sensible asociada a las tarjetas de crédito con el resto de la plataforma?

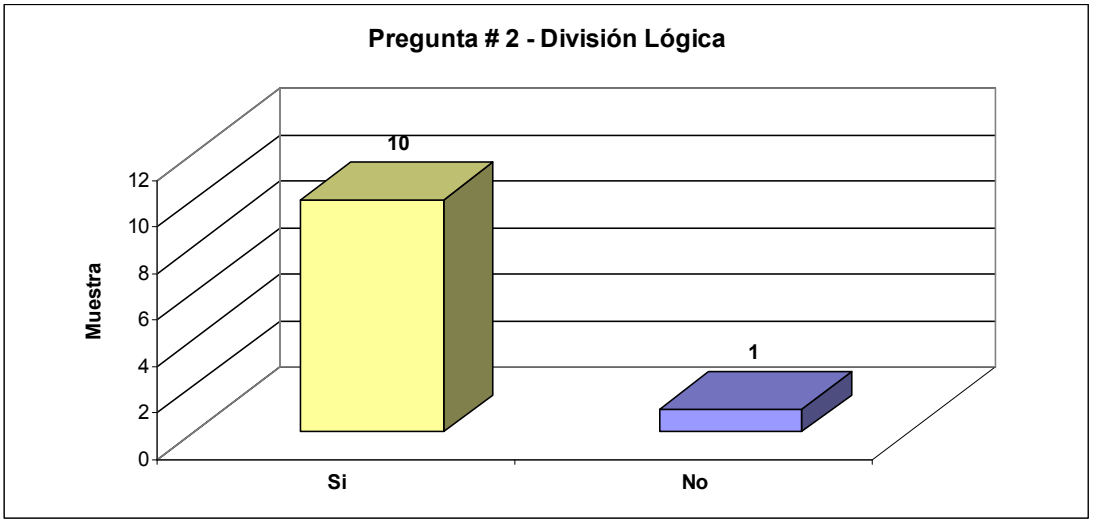

Figura 6. División Lógica

Para la pregunta número dos tal como se observa en la figura 6, del total de la muestra de once entidades bancarias, diez encuestados que representan el 91%, considera que en su organización no hay ausencia en la división lógica de los componentes que almacenan, tramitan o procesen datos de tarjetas de crédito, mientras que existe un entrevistado que contestó lo contrario, lo cual representa el 9%.

Debido a que este estudio está enmarcado en los riesgos negativos, se procedió a evaluar la probabilidad e impacto para el caso en donde no existe ausencia en la división lógica.

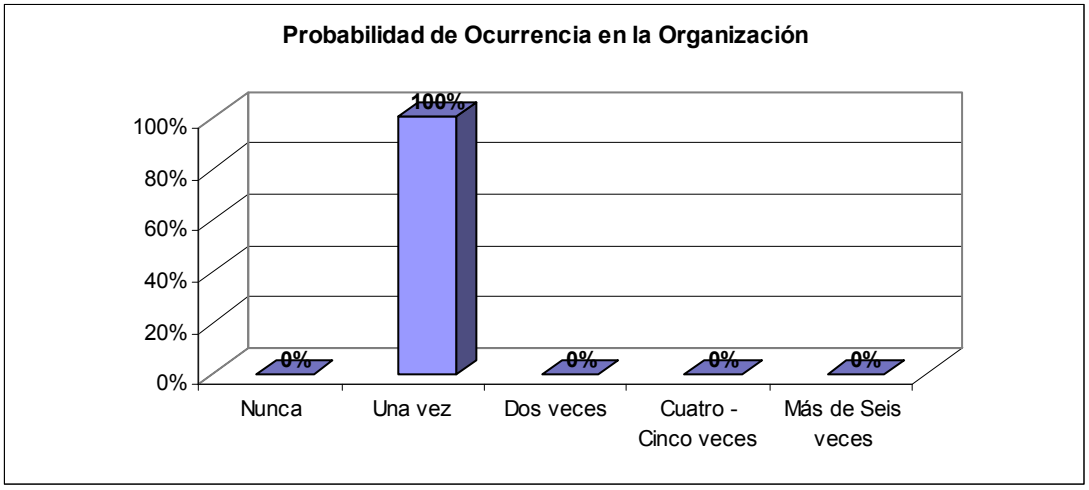

Figura 6.1 Probabilidad Ocurrencia en la Organización

La figura 6.1 muestra que el entrevistado respondió que en la organización este evento tuvo una ocurrencia en un 100% de una vez en el último año, adicionalmente, el impacto de exposición de data sensible fue insignificante, tal como se observa en la figura 6.2.

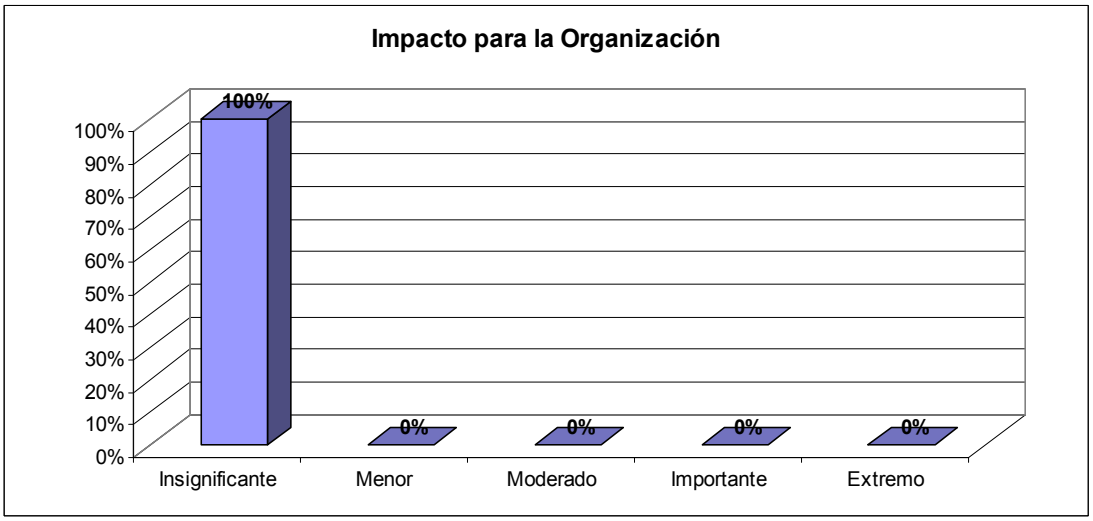

Figura 6.2 Impacto

En conclusión, el entrevistado que expresó que esta incidencia se había suscitado en su entidad bancaria, tal como se observa en la tabla 6, su

respuesta fue que había ocurrido una vez en el último año, por tanto, se obtuvo una probabilidad de 30%, así como el impacto fue insignificante que representa 5 en la escala definida, al hacer uso de la matriz de probabilidad e impacto, al realizar la multiplicación se obtiene como resultado **1.50**, tal como se muestra a continuación:

Tabla 6. Escala Probabilidad e Impacto. División Lógica

Entrevistado	Probabilidad	Impacto	Calificación
E1	30%	5	1.5
			1.50

5.1.3. Cortafuegos

A continuación se presenta la tercera interrogante:

¿Usted considera que existe ausencia o debilidad en la configuración o actualización del cortafuego que protege áreas sensibles de su organización?

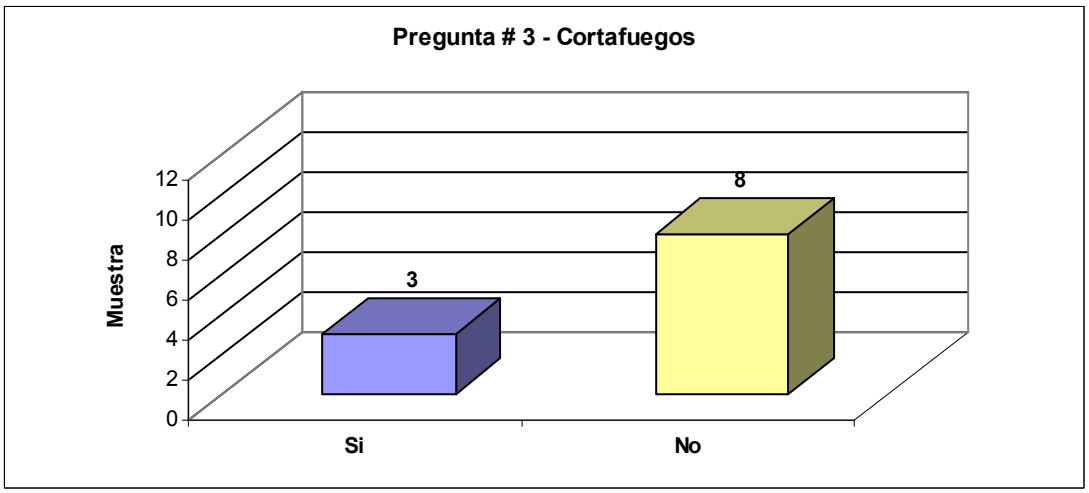

Figura 7. Cortafuegos

Para la pregunta número tres tal como se observa en la figura 7, del total de la muestra de once entidades bancarias, ocho encuestados que representan el 73%, exponen que no existe ausencia o debilidad en la configuración o actualización del cortafuego que protege áreas sensibles de su organización, mientras que existen tres entrevistados que respondieron lo contrario, lo cual representa el 27%.

Debido a que este estudio está enmarcado en los riesgos negativos, se procedió a evaluar la probabilidad e impacto para el caso en donde no existe ausencia en la división lógica.

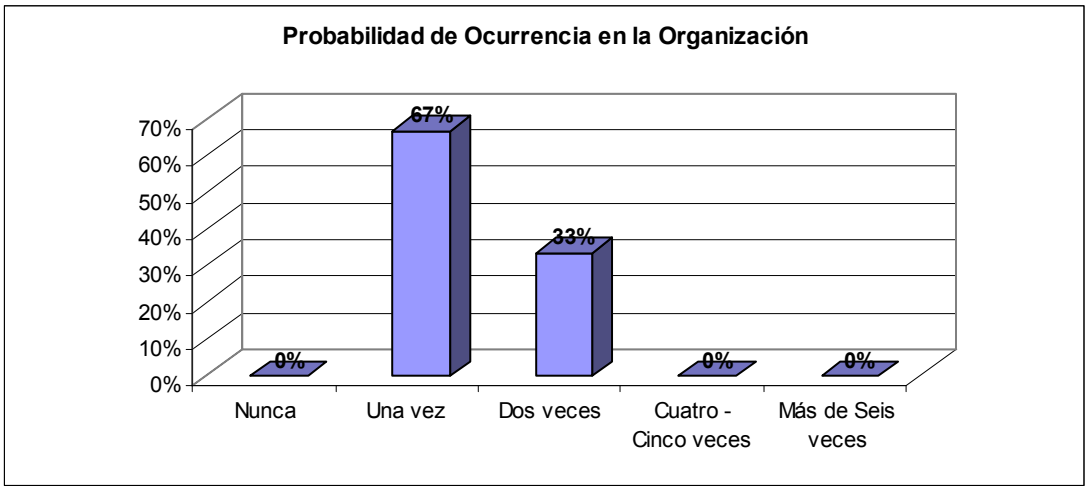

Figura 7.1 Probabilidad Ocurrencia

La figura 7.1 muestra que de los ocho entrevistados respondieron que en la organización este evento tuvo una ocurrencia en un 67% de una vez y de 33% en dos oportunidades en el último año, adicionalmente, el impacto de exposición de data sensible fue en un 33% insignificante, 33% menor y 33% de moderado, tal como se observa en la figura 7.2.

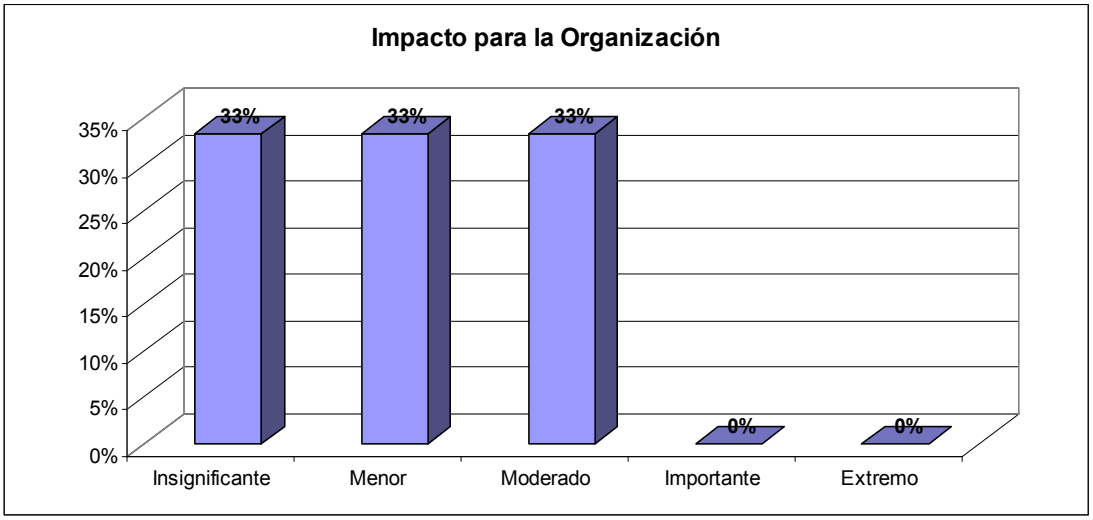

Figura 7.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 7, expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 7. Escala Probabilidad e Impacto. Cortafuegos

Entrevistado	Probabilidad	Impacto	Calificación
E1	30%	10	3
E2	10%	5	0.5
E3	10%	20	2
			1.83

La media de las calificaciones obtenidas para el riesgo identificado es de **1.83**.

5.1.4. Uso contraseñas predeterminadas

La cuarta interrogante planteada consistió:

¿Usted considera que en su organización se hace uso de contraseñas estándares fijadas por los proveedores de componentes de hardware o software, es decir, no se realizan cambios luego de adquirir el componente?

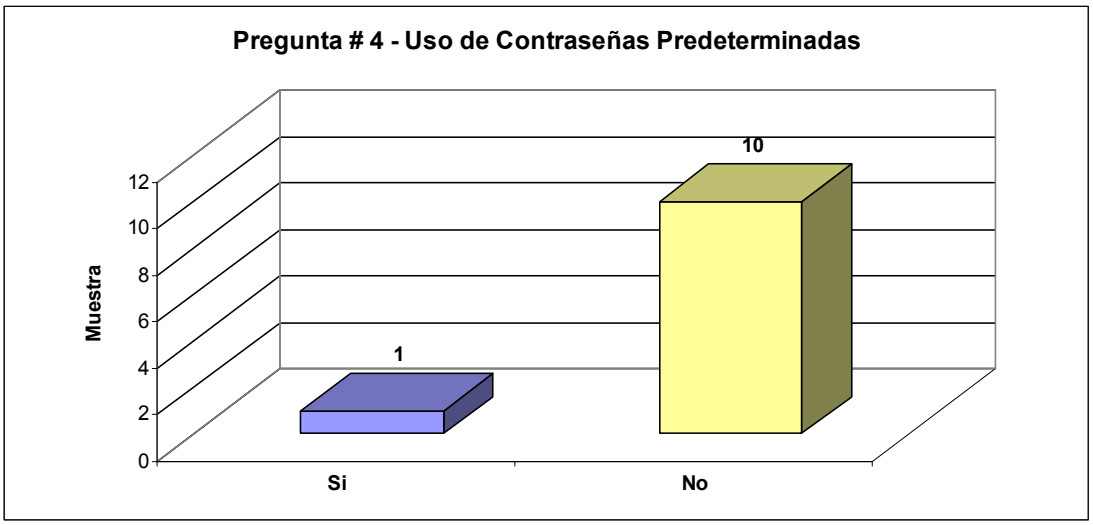

Figura 8. Contraseñas Predeterminadas

Para la pregunta número cuatro tal como se observa en la figura 8, del total de la muestra de once entidades bancarias, diez encuestados que representan el 91%, describen que en su organización se han usado contraseñas estándares fijadas por los proveedores de componentes de hardware o software, es decir, que no se actualizan las contraseñas y quedan las predeterminadas por el fabricante.

Por otro lado, un entrevistado que contestó lo contrario, lo cual representa el 9%.

Se procede a realizar el análisis para la porción de los entrevistados que expresaron que hubo exposición de data sensible en su organización.

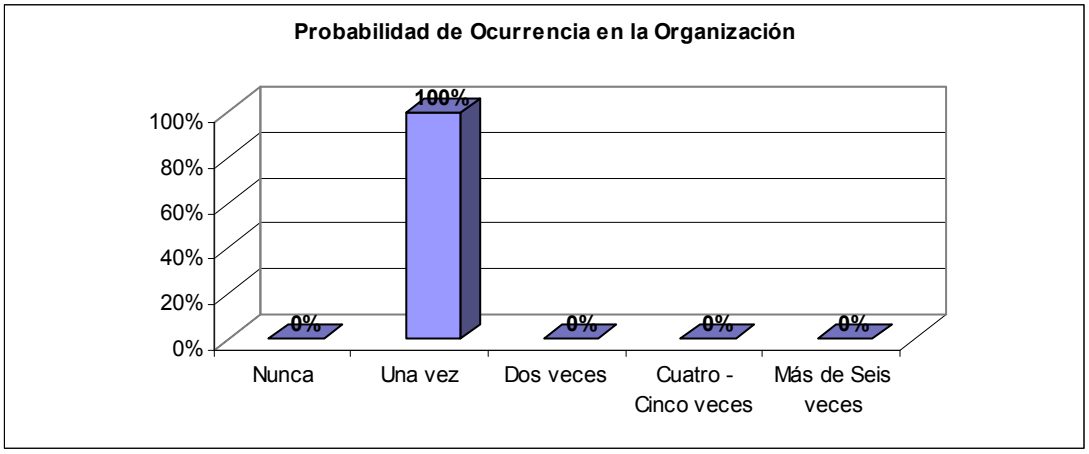

Figura 8.1 Probabilidad Ocurrencia

La figura 8.1 muestra que el entrevistado respondió que en la organización este evento tuvo una ocurrencia en un 100% de una vez en el último año, adicionalmente, el impacto de exposición de data sensible fue insignificante, tal como se observa en la figura 8.2.

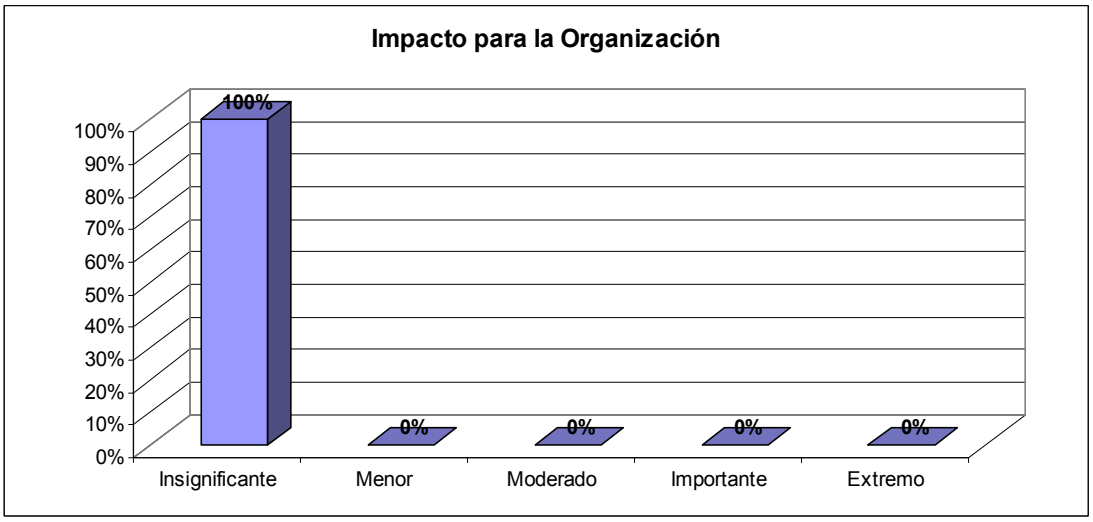

Figura 8.2. Impacto

En conclusión, el entrevistado que expresó que esta incidencia se había suscitado en su entidad bancaria, tal como se observa en la tabla 8, su respuesta fue que había ocurrido una vez en el último año, por tanto, se

obtuvo una probabilidad de 30%, así como el impacto fue insignificante que representa 5 en la escala definida, al hacer uso de la matriz de probabilidad e impacto, al realizar la multiplicación se obtiene como resultado **1.50**, tal como se muestra a continuación:

Tabla 8. Escala Probabilidad e Impacto. Contraseñas Predeterminadas

Entrevistado	Probabilidad	Impacto	Calificación
E1	30%	5	1.5
			1.5

5.1.5. Mecanismos de Cifrado, Truncamiento, Ocultamiento y Refundición

La interrogante planteada número cinco en el instrumento es:

¿En su organización se realizan mecanismos de cifrado, truncamiento, ocultamiento y refundición de la data sensible asociada a las tarjetas de crédito?

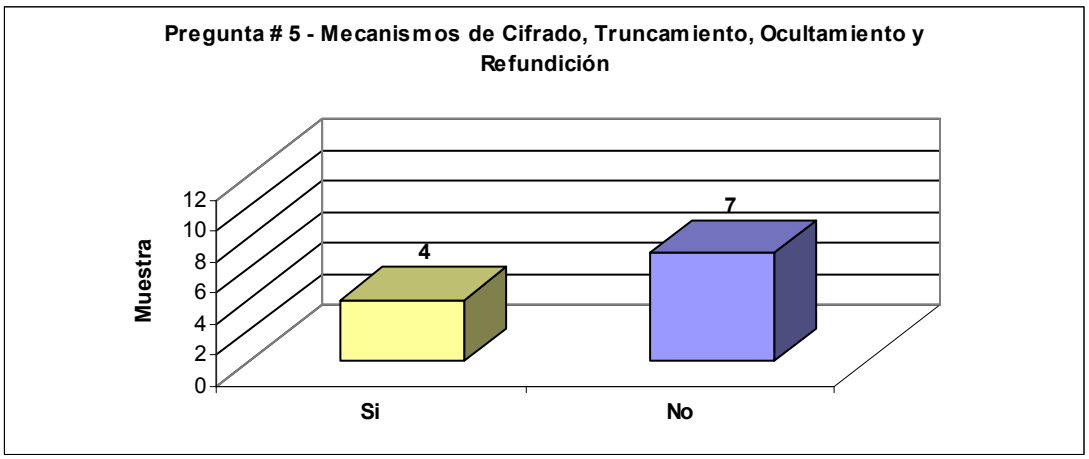

Figura 9. Mecanismo Cifrado

Para la pregunta número cinco tal como se observa en la figura 9, del total de la muestra de once entidades bancarias, cuatro de los encuestados que

representan el 36%, considera que en su organización hacen uso de mecanismos de cifrado, truncamiento, ocultamiento y refundición, mientras, mientras que siete contestaron lo contrario, lo cual representa el 64%.

Se procedió a evaluar la probabilidad e impacto para el caso en donde no se están haciendo uso de mecanismos apropiadamente.

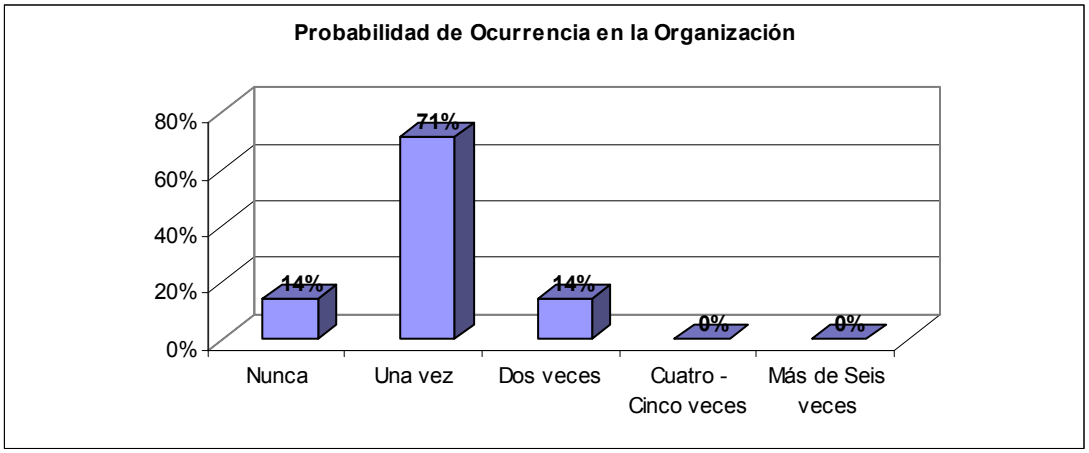

Figura 9.1 Probabilidad Ocurrencia

La figura 9.1 muestra que de los siete entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 14%, un 71% de una vez y de 14% en dos oportunidades, adicionalmente, el impacto de exposición de data sensible fue en un 14% insignificante, 43% menor y 43% de moderado, tal como se observa en la figura 9.2.

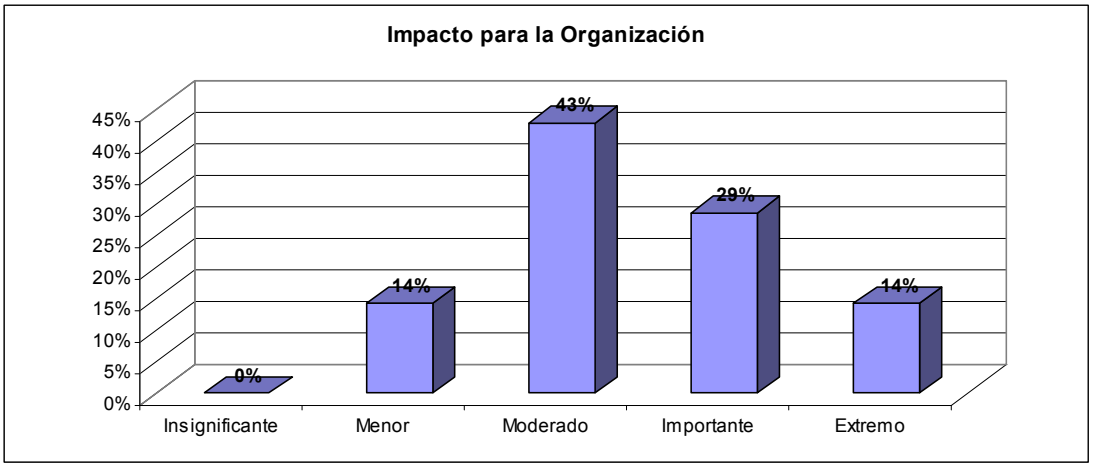

Figura 9.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 9, expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 9. Escala Probabilidad e Impacto. Mecanismos de Cifrado

Entrevistado	Probabilidad	Impacto	Calificación
E1	30%	40	12
E2	30%	20	6
E3	30%	80	24
E4	30%	20	6
E5	30%	40	12
E6	10%	10	1
E7	50%	20	10
			10.14

La media de las calificaciones obtenidas para el riesgo identificado es de **10.14.**

5.1.6. Protección Claves Criptográficas

La interrogante número seis del instrumento consistió:

¿Considera usted que en su organización se protegen adecuadamente las claves criptográficas utilizadas para el cifrado de datos sensibles?

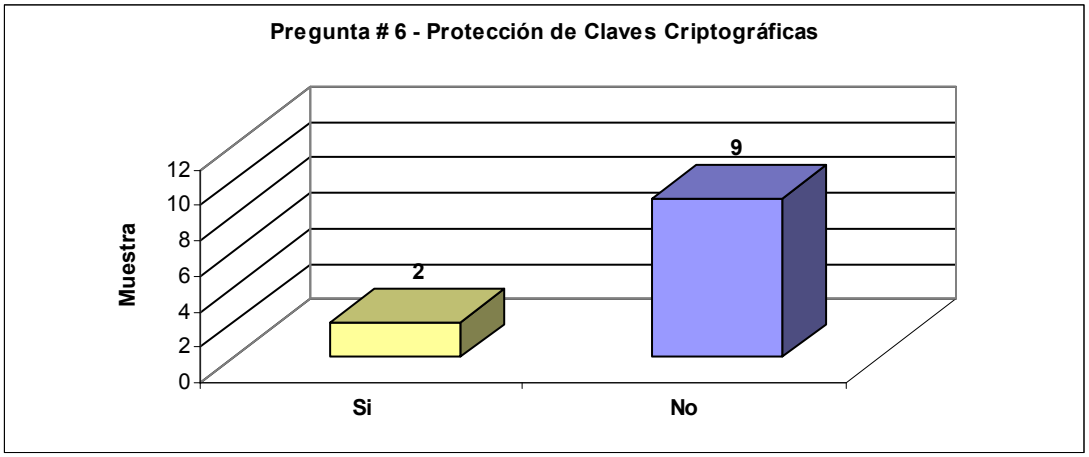

Figura 10. Protección Claves Criptográficas

Para la pregunta número seis tal como se observa en la figura 10, del total de la muestra de once entidades bancarias, dos de los encuestados que representan el 18%, considera que en su organización existe una protección adecuada de claves criptográficas, mientras, que nueve contestaron lo contrario, lo cual representa el 82%.

Se procedió a evaluar la probabilidad e impacto para el caso en donde no se está haciendo una protección adecuada.

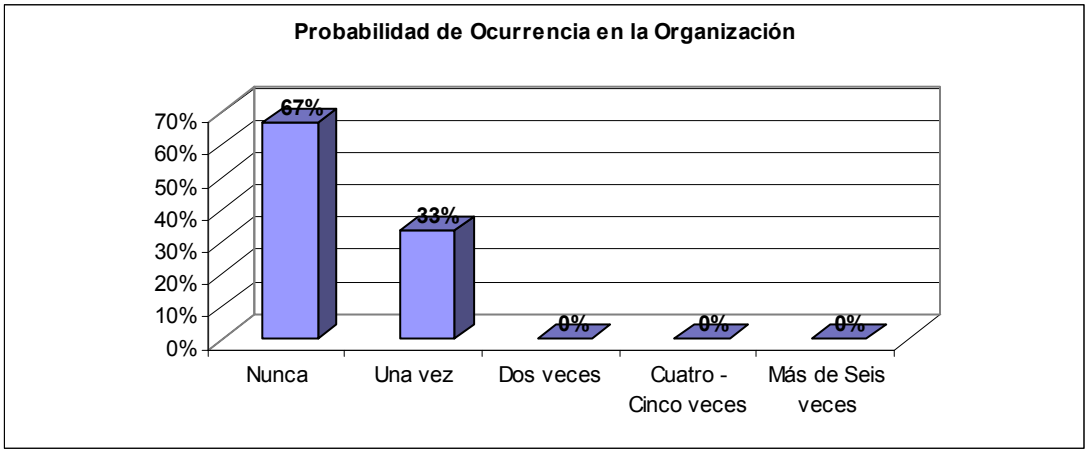

Figura 10.1 Probabilidad Ocurrencia

La figura 10.1 muestra que de los nueve entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 67% y un 33% una vez, adicionalmente, el impacto de exposición de data sensible fue en un 22% menor, 33% moderado, 33% importante y un 11% extremo tal como se observa en la figura 10.2.

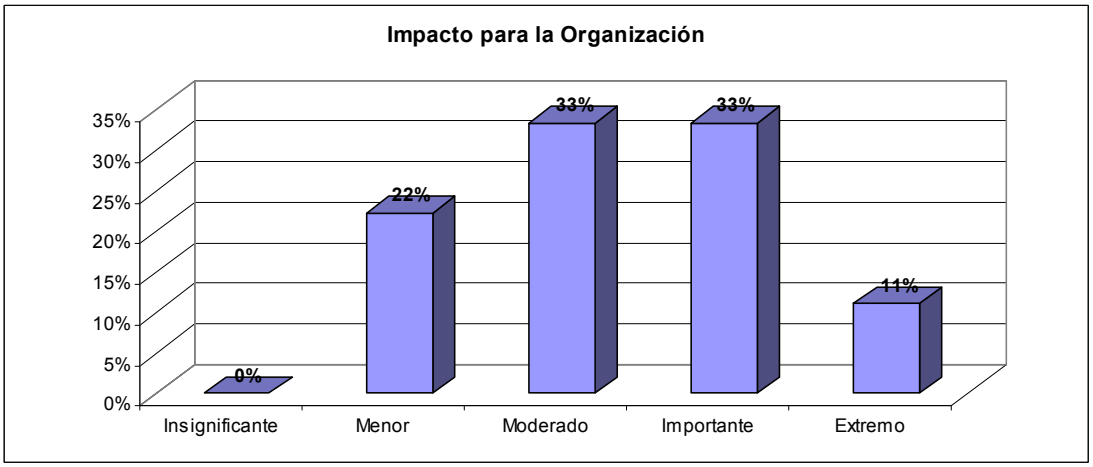

Figura 10.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 10,

expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 10. Escala Probabilidad e Impacto. Protección Claves Criptográficas

Entrevistado	Probabilidad	Impacto	Calificación
E1	10%	40	4
E2	30%	10	3
E3	10%	40	4
E4	10%	80	8
E5	10%	20	2
E6	10%	10	1
E7	10%	40	4
E8	30%	20	6
E9	30%	20	6
			4.22

La media de las calificaciones obtenidas para el riesgo identificado es de **4.22.**

5.1.7. Transmisión de Data Sensible

La interrogante número siete del instrumento consistió:

¿Considera usted que existe ausencia o debilidad en la codificación de data sensible asociada a las tarjetas de crédito al momento de transmisión a través de redes públicas?

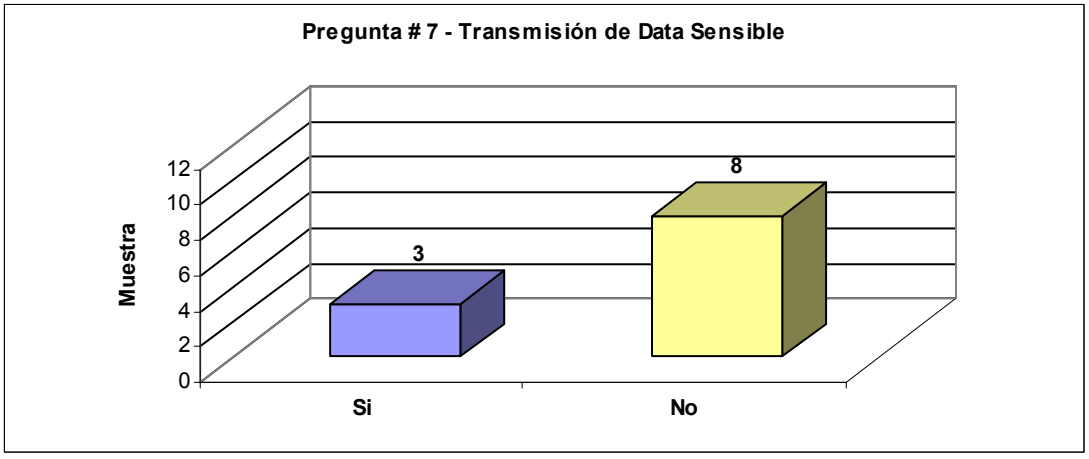

Figura 11. Transmisión de Data Sensible

Para la pregunta número siete tal como se observa en la figura 11, del total de la muestra de once entidades bancarias, tres de los encuestados que representan un 27%, considera que en su organización existe ausencia o debilidad de data sensible al ser transmitidas a través de redes públicas, mientras, que ocho contestaron lo contrario, lo cual representa el 73%.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

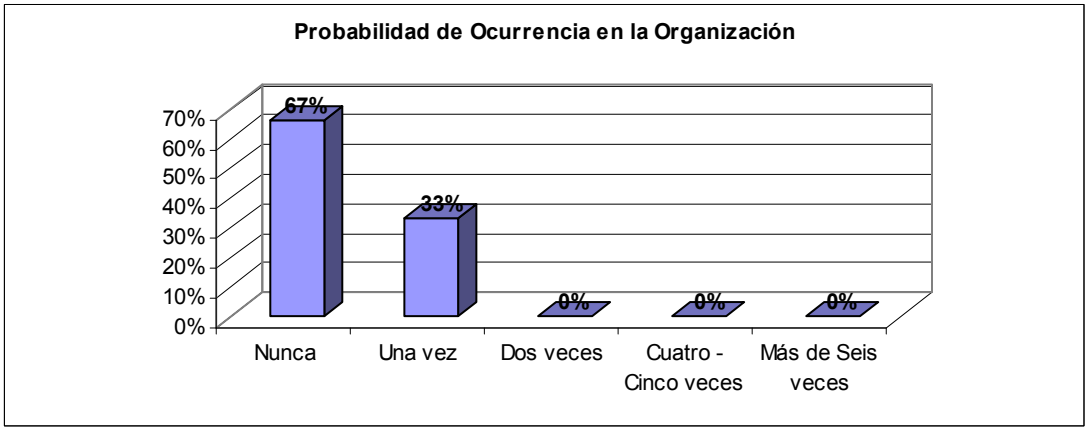

Figura 11.1 Probabilidad Ocurrencia

La figura 11.1 muestra que de los ocho entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 67% y un 33%, una vez, adicionalmente, el impacto de exposición de data sensible fue en un 33% insignificante, y un 67% menor tal como se observa en la figura 11.2.

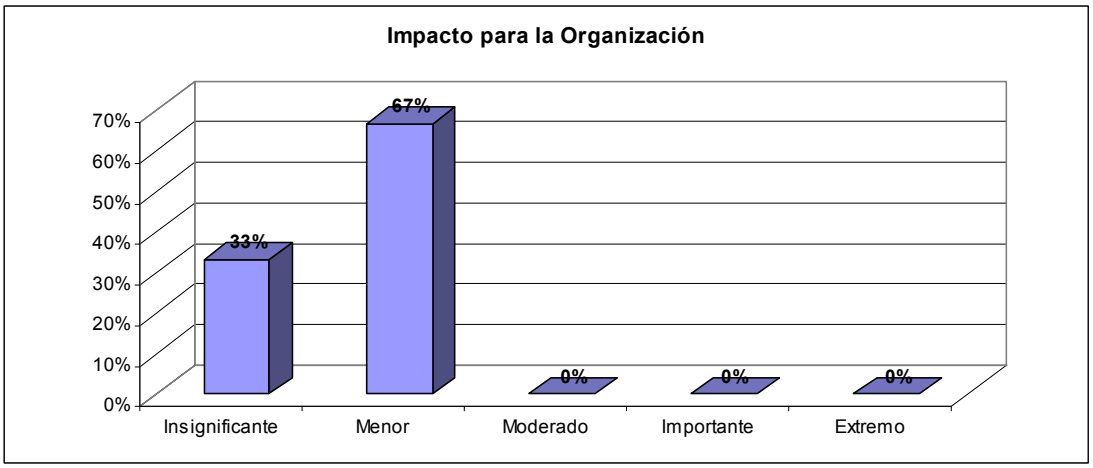

Figura 11.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 11, expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 11. Escala Probabilidad e Impacto. Transmisión Data Sensible

Entrevistado	Probabilidad	Impacto	Calificación
E1	10%	5	0.5
E2	30%	20	6
E3	10%	20	2
			2.83

5.1.8. Antivirus

La interrogante número ocho del instrumento consistió:

¿Considera usted que existen debilidades en la protección de su data sensible debido a la falta de antivirus o de la actualización oportuna de los mismos?

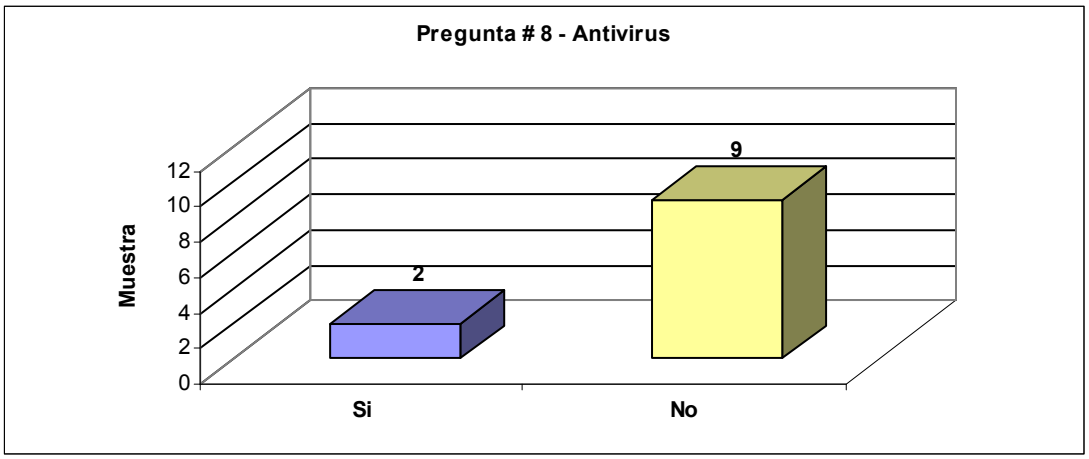

Figura 12. Antivirus

Para la pregunta número ocho tal como se observa en la figura 12, del total de la muestra de once entidades bancarias, dos de los encuestados que representan un 18%, dos de los encuestados que representan un 18%, considera que en su organización existe ausencia o debilidad en la protección de data sensible debido a la falta de antivirus o de la actualización de los mismos, mientras que nueve contestaron lo contrario, lo cual representa el 82%.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

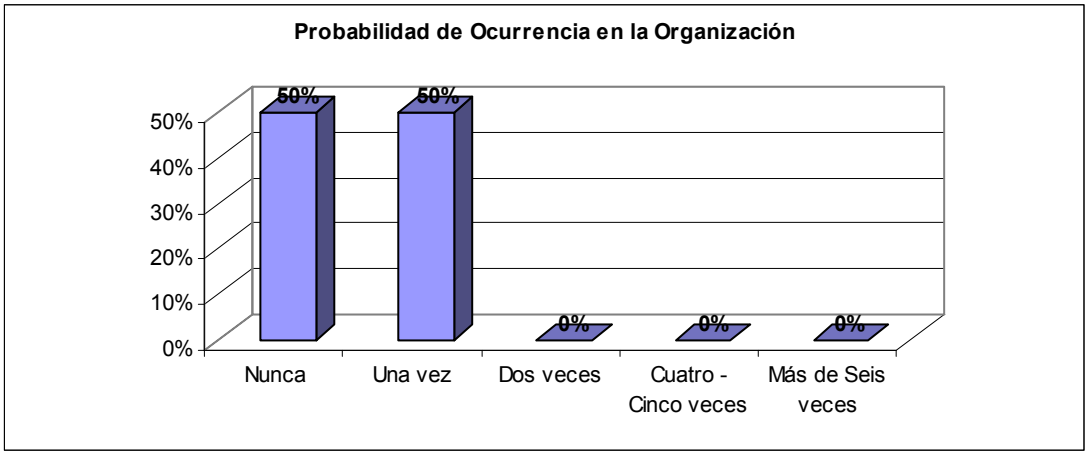

Figura 12.1 Probabilidad Ocurrencia

La figura 12.1 muestra que de los nueve entrevistados respondieron que en la organización este evento no se suscitó en el último año en 50% y un 50% una vez, adicionalmente, que el impacto de exposición de data sensible fue en un 100% menor, tal como se observa en la figura 12.2.

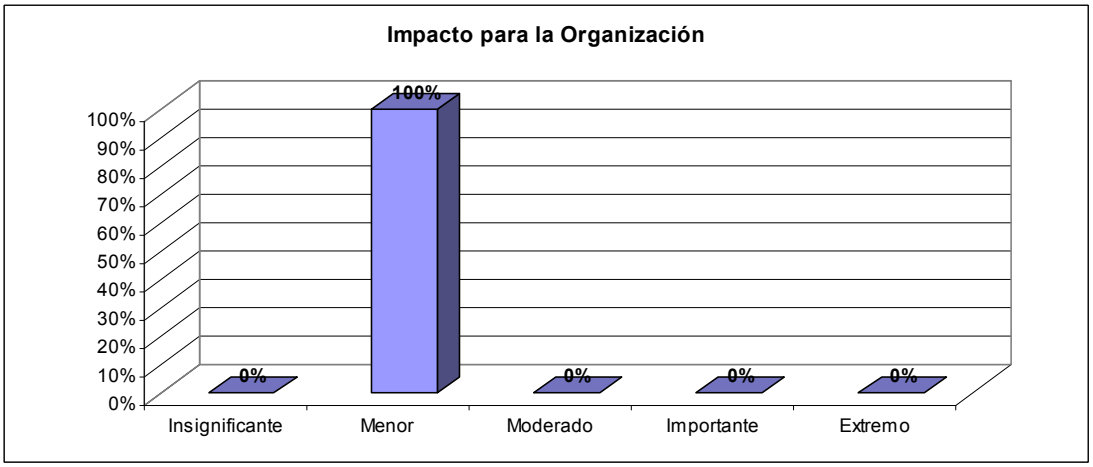

Figura 12.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 12, expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 12. Escala Probabilidad e Impacto. Antivirus

Entrevistado	Probabilidad	Impacto	Calificación
E1	10%	10	1
E2	30%	10	3
			2.00

La media de las calificaciones obtenidas para el riesgo identificado es de **2.00.**

5.1.9. Actualización de Parches

La interrogante número nueve del instrumento consistió:

¿En su organización cuentan con políticas de actualizaciones de parches de seguridad?

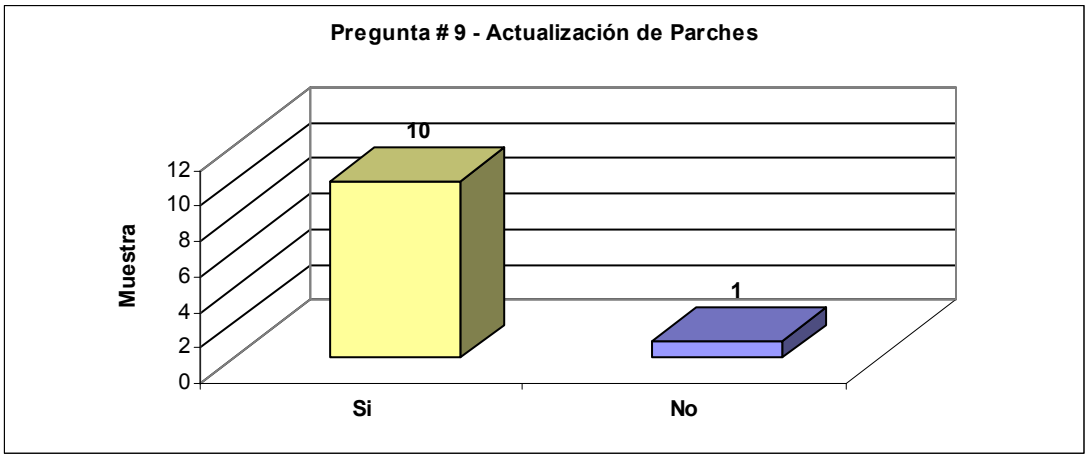

Figura 13. Actualización de Parches

Para la pregunta número nueve tal como se observa en la figura 13, del total de la muestra de once entidades bancarias, diez de los encuestados que representan un 91% considera que en su organización no existen debilidades relacionadas con la actualización de parches, mientras que uno contestó lo contrario, lo cual representa el 9%.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

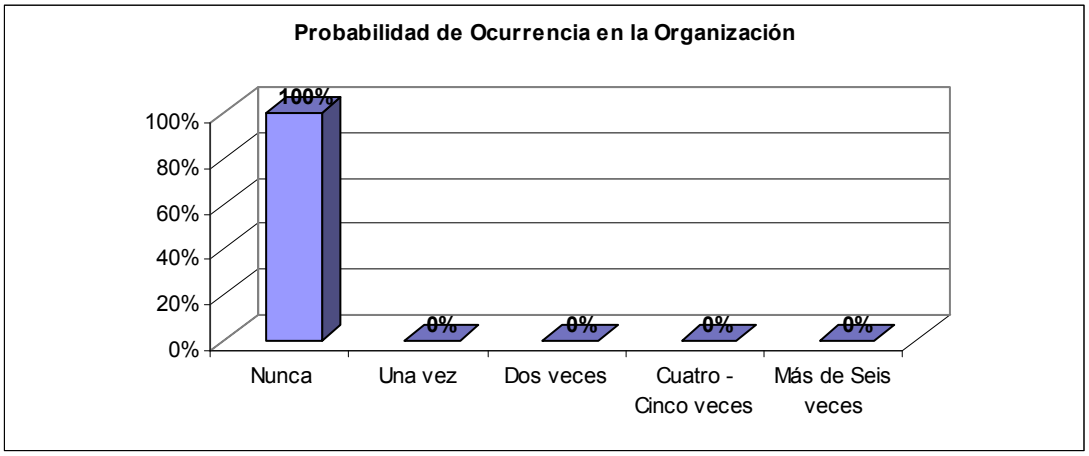

Figura 13.1 Probabilidad Ocurrencia

La figura 13.1 muestra que el entrevistado que respondió que en la organización este evento no se suscitó en el último año en un 100%, adicionalmente, que el impacto de exposición de data sensible fue en un 100% insignificante, tal como se observa en la figura 13.2.

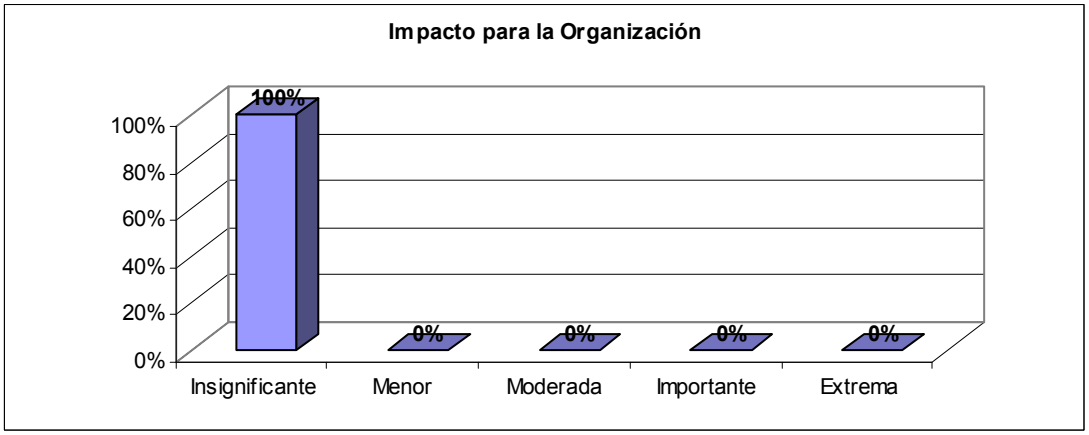

Figura 13.2 Impacto

En conclusión, el entrevistado que expresó que esta incidencia se había suscitado en su entidad bancaria, tal como se observa en la tabla 13, su respuesta fue que no había ocurrido el último año, por tanto, se obtuvo una probabilidad de 10%, así como el impacto fue insignificante que representa 5 en la escala definida, al hacer uso de la matriz de probabilidad e impacto, al realizar la multiplicación se obtiene como resultado **0.50**, tal como se muestra a continuación:

Tabla 13. Escala Probabilidad e Impacto. Actualización de Parches

Entrevistado	Probabilidad	Impacto	Calificación
E1	10%	5	0.5
			0.50

La media de las calificaciones obtenidas para el riesgo identificado es de **0.50.**

5.1.10. Mitigación Brechas de Seguridad

La interrogante número diez del instrumento consistió:

¿En el caso que la organización desarrolle sus propias aplicaciones, se aplican mecanismos que mitiguen las brechas de seguridad producidas por vulnerabilidades que no fueron detectadas antes de pasar al ambiente de producción?

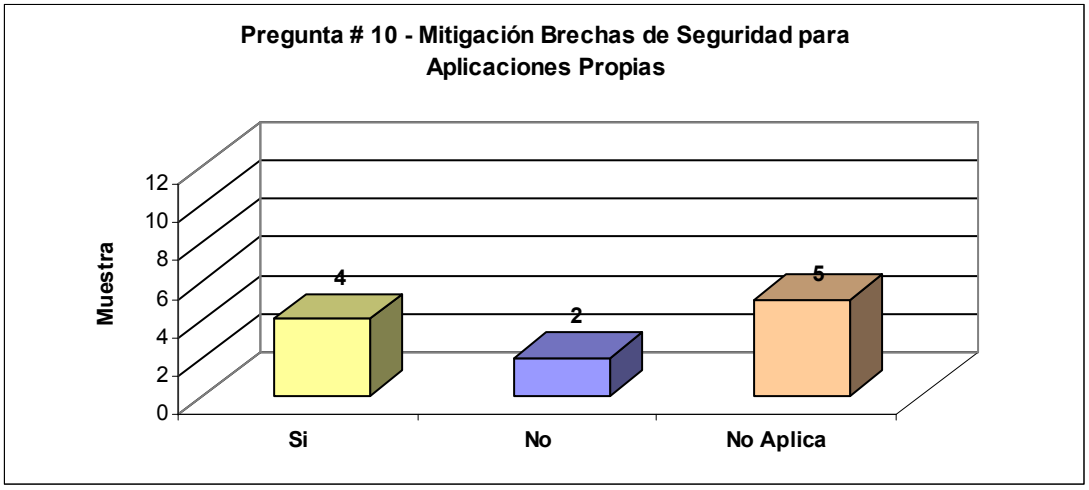

Figura 14. Mitigación Brechas Seguridad

Para la pregunta número diez tal como se observa en la figura 14, del total de la muestra de once entidades bancarias, cuatro encuestados que representan un 36%, considera que en su organización no existe debilidad en la mitigación de brechas se seguridad producto del desarrollo de aplicaciones propias, mientras que cuatro que representa un 36% expresan que se existen deficiencias, así como un 45% no aplica esta interrogante.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

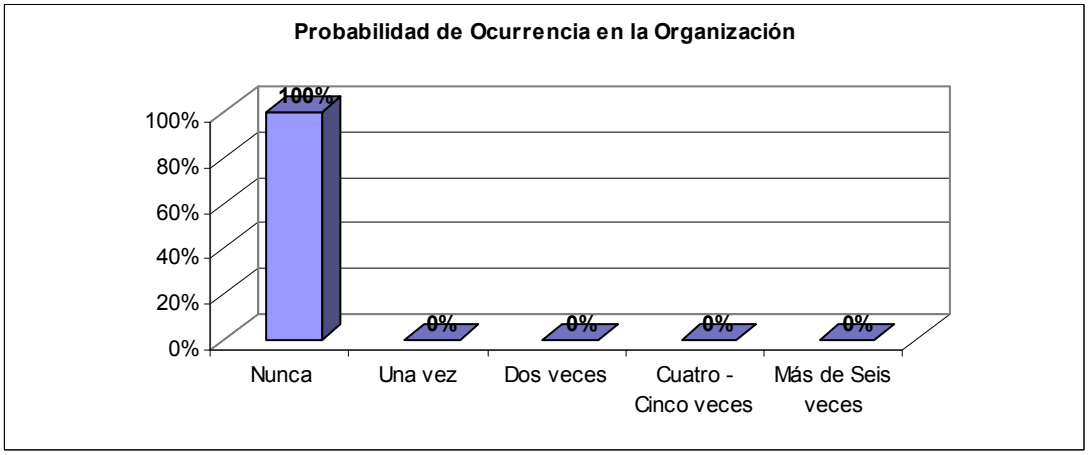

Figura 14.1 Probabilidad Ocurrencia

La figura 14.1 muestra que los entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 100%, adicionalmente, el impacto de exposición de data sensible fue en un 100% insignificante, tal como se observa en la figura 14.2.

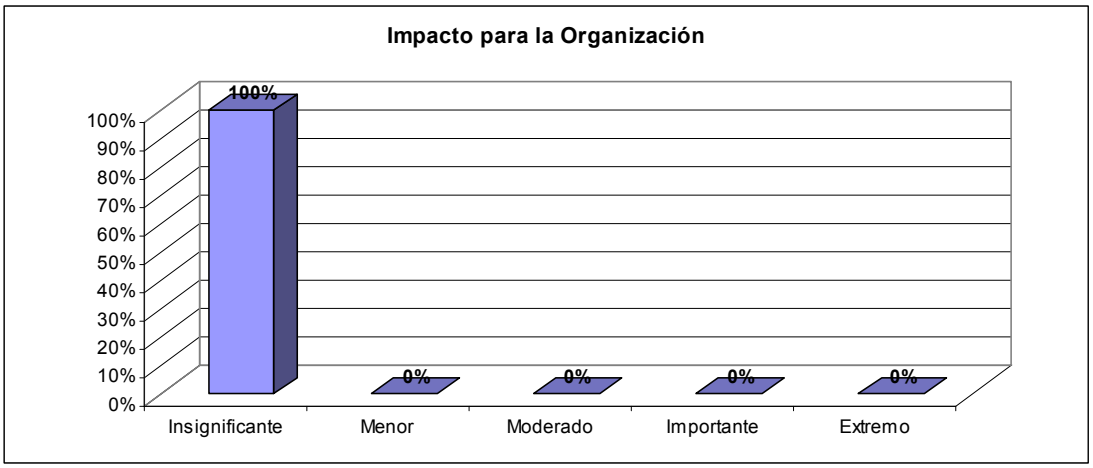

Figura 14.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 12, expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 14. Escala Probabilidad e Impacto. Mitigación Brechas Seguridad

Entrevistado	Probabilidad	Impacto	Calificación
E1	10%	5	0.5
E2	10%	5	0.5
			0.50

La media de las calificaciones obtenidas para el riesgo identificado es de **0.50.**

5.1.11. Definición de Permisos

La interrogante número once del instrumento consistió:

¿Considera que en su organización existe una detallada definición de permisos de acuerdo a roles y responsabilidades a la data sensible asociada a las tarjetas de crédito?

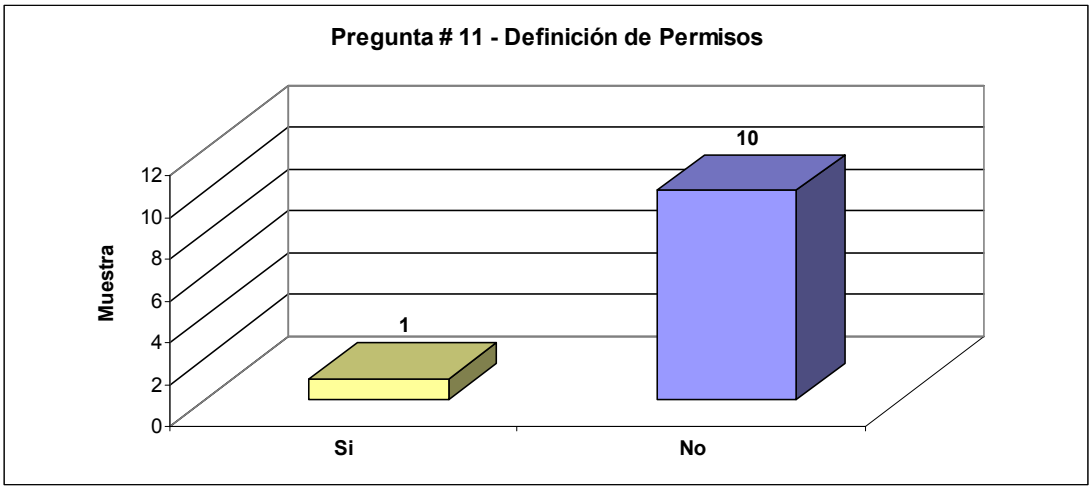

Figura 15. Definición de Permisos

Para la pregunta número once tal como se observa en la figura 15, del total de la muestra de once entidades bancarias, un encuestado que representa el 9%, considera que en su organización no existe debilidad en la definición de permisos de acuerdo a los roles y responsabilidades, mientras que diez que representa un 91% expresan que existen deficiencias.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

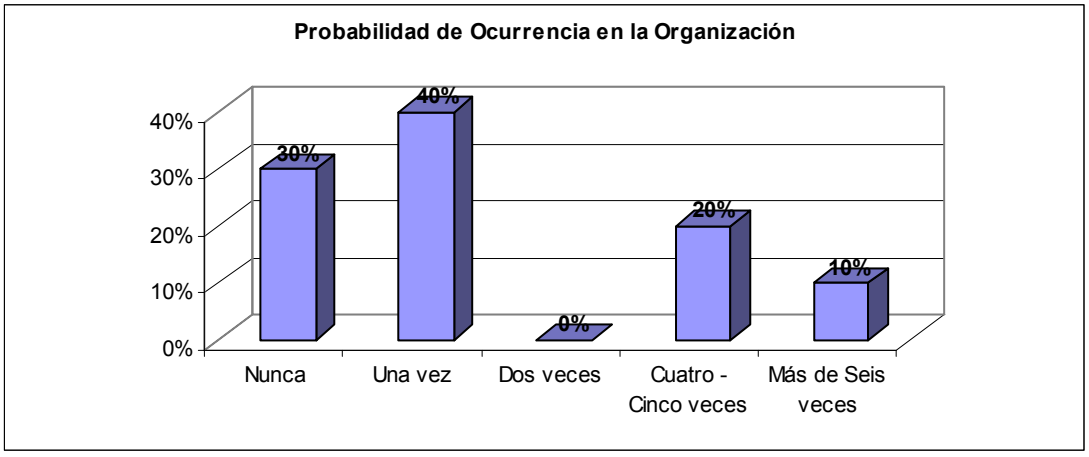

Figura 15.1 Probabilidad Ocurrencia

La figura 15.1 muestra que los entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 30%, 40% una vez, 20% entre cuatro y seis veces y un 10% más de seis veces, adicionalmente, el impacto de exposición de data sensible fue en un 10% insignificante, 30% menos, 20% moderado, 30% importante y 10% extremo, tal como se observa en la figura 15.2.

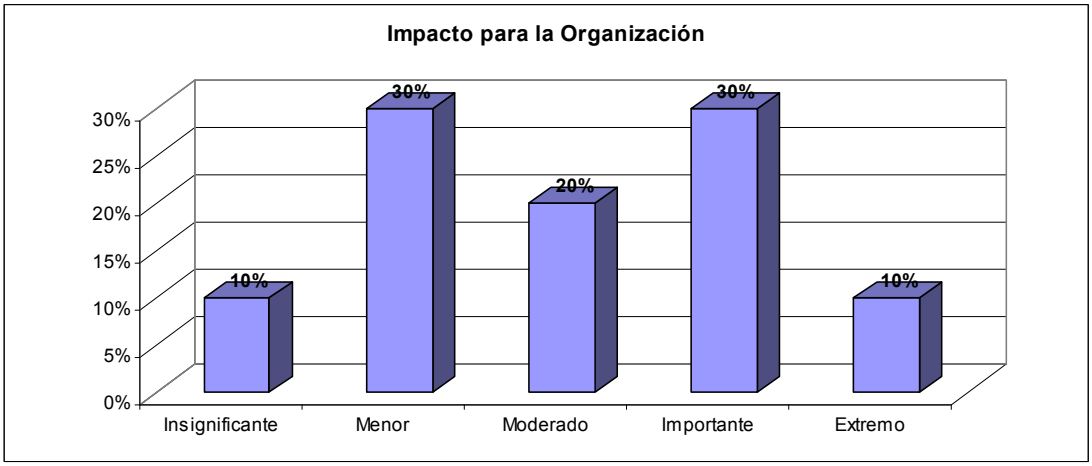

Figura 15.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 12,

expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 15. Escala Probabilidad e Impacto. Roles y Responsabilidades

Entrevistado	Probabilidad	Impacto	Calificación
E1	10%	20	2
E2	30%	10	3
E3	10%	40	4
E4	10%	80	8
E5	30%	20	6
E6	70%	10	7
E7	30%	40	12
E8	70%	5	3.5
E9	30%	40	12
E10	90%	10	9
			6.65

La media de las calificaciones obtenidas para el riesgo identificado es de **6.65.**

5.1.12. Uso de Credenciales Genéricas

La interrogante número doce del instrumento consistió:

¿En su organización se utilizan credenciales genéricas, es decir, se utilice un mismo usuario para un grupo de personas?

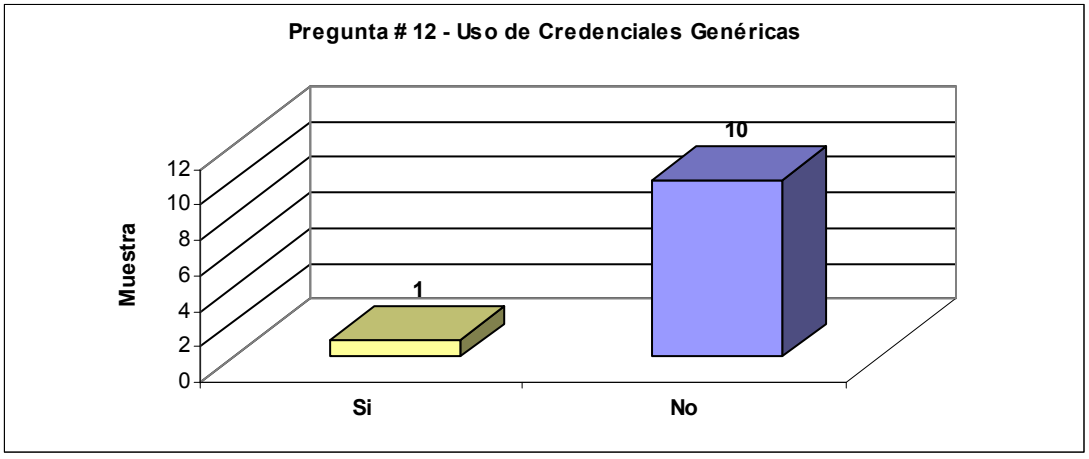

Figura 16. Uso Credenciales Genéricas

Para la pregunta número doce tal como se observa en la figura 16, del total de la muestra de once entidades bancarias, diez encuestados que representan el 91%, consideran que en su organización no hacen uso de credenciales genéricas, mientras que uno que representa un 9% expresa que lo contrario.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

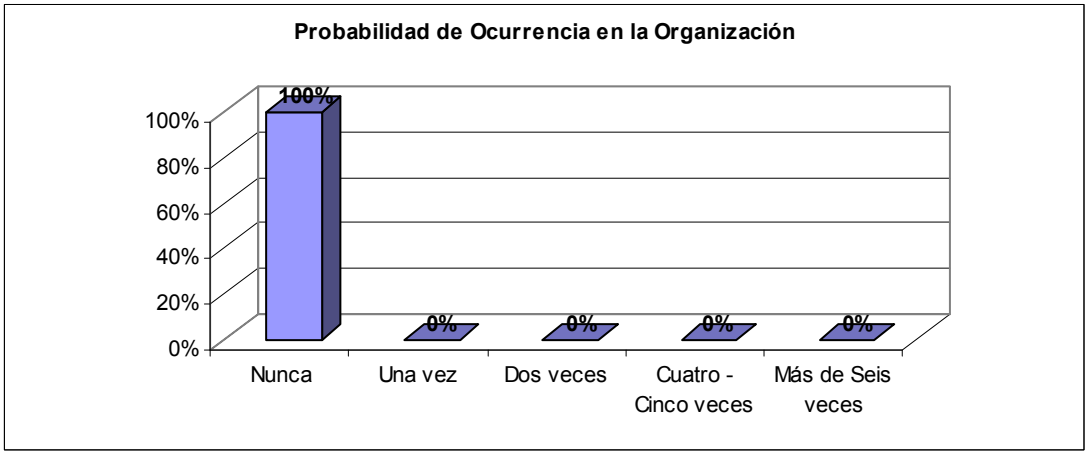

Figura 16.1 Probabilidad Ocurrencia

La figura 16.1 muestra que los entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 100%, adicionalmente, el impacto de exposición de data sensible fue en un 100% insignificante, tal como se observa en la figura 16.2.

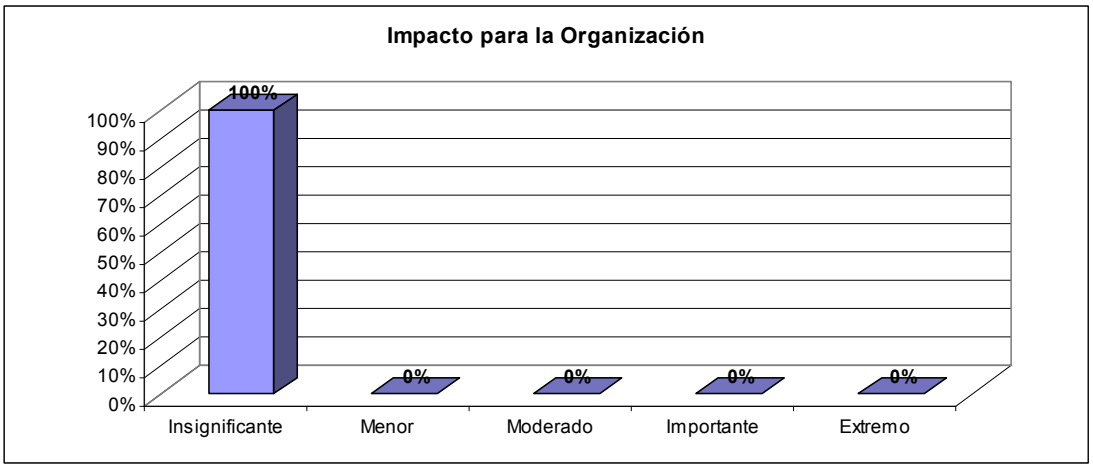

Figura 16.2 Impacto

En conclusión, el entrevistado que expresó que esta incidencia se había suscitado en su entidad bancaria, tal como se observa en la tabla 16, su respuesta fue que no había ocurrido en el último año, por tanto, se obtuvo una probabilidad de 10%, así como el impacto fue insignificante que representa 5 en la escala definida, al hacer uso de la matriz de probabilidad e impacto, al realizar la multiplicación se obtiene como resultado **0.50**, tal como se muestra a continuación:

Tabla 16. Escala Probabilidad e Impacto. Uso Credenciales Genéricas

Entrevistado	Probabilidad	Impacto	Escala
E1	10%	5	0.5
			0.50

5.1.13. Seguridad Física

¿En su organización cuentan con controles de seguridad física, tales como: cámaras de video vigilancia, control de acceso, donde se proteja el ingreso de personas no autorizadas a los componentes en donde se encuentran almacenados los datos sensibles de la organización?

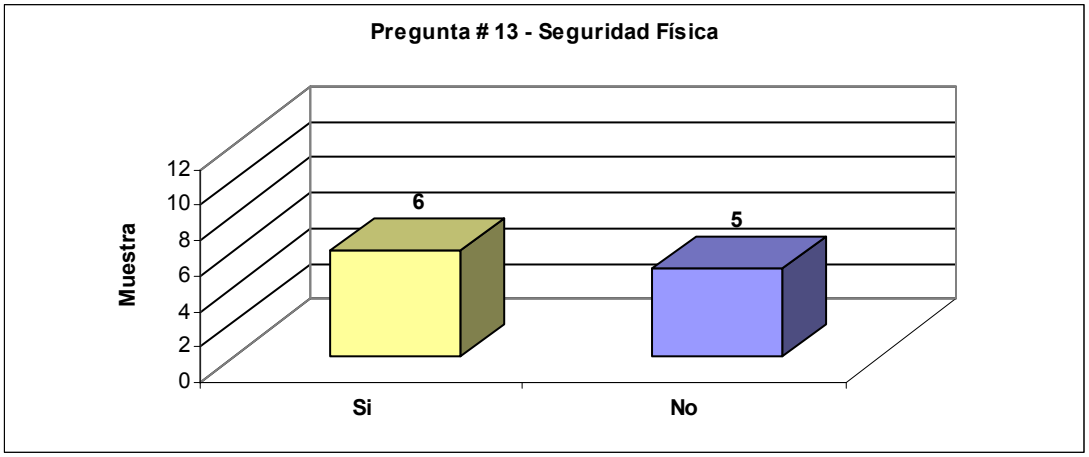

Figura 17. Seguridad Física

Para la pregunta número trece tal como se observa en la figura 17, del total de la muestra de once entidades bancarias, seis encuestados que representan el 55%, consideran que en su organización no existen debilidades en la seguridad física, mientras que cinco que representan un 45% expresa que lo contrario.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

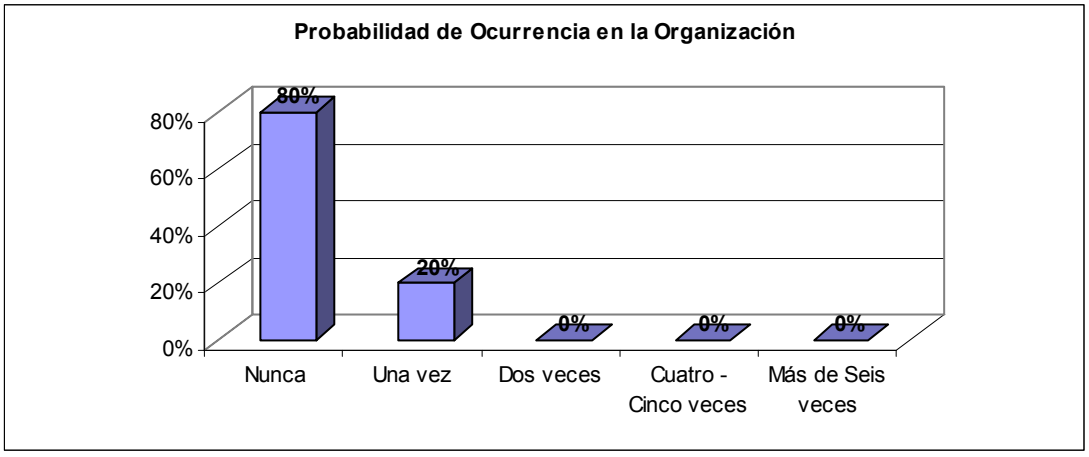

Figura 17.1 Probabilidad Ocurrencia

La figura 17.1 muestra que los entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 80% y en un 20% en una oportunidad, adicionalmente, el impacto de exposición de data sensible fue en un 20% insignificante, 20% menor, 40% Moderado y un 20% importante, tal como se observa en la figura 17.2.

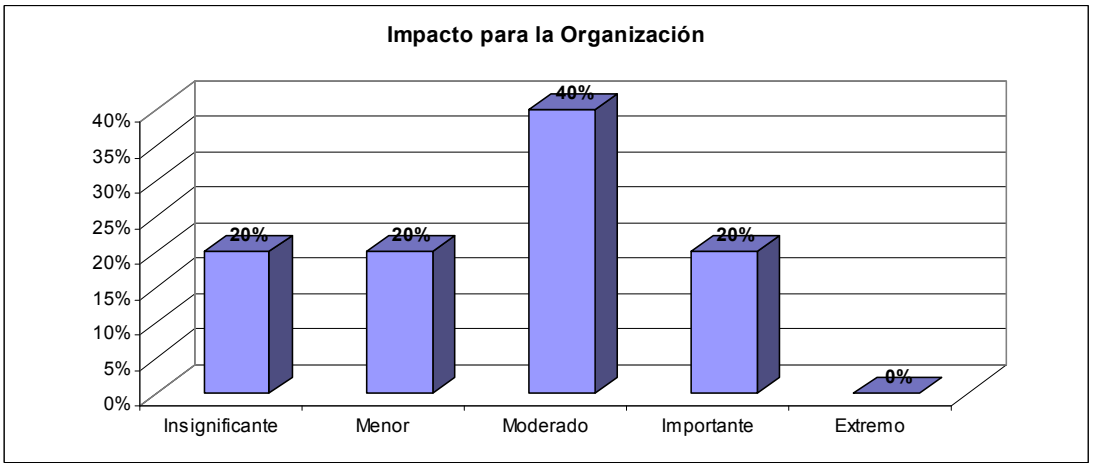

Figura 17.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 17,

expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 17. Escala Probabilidad e Impacto. Seguridad Física

Entrevistado	Probabilidad	Impacto	Calificación
E1	10%	20	2
E2	10%	40	4
E3	30%	10	3
E4	10%	5	0.5
E5	10%	20	2
			2.30

La media de las calificaciones obtenidas para el riesgo identificado es de **2.30.**

5.1.14. Detección y Registro

La interrogante número catorce del instrumento consistió:

¿En su organización cuentan con herramientas que tengan la capacidad de detectar y registrar cualquier acceso a información sensible de los tarjetahabientes?

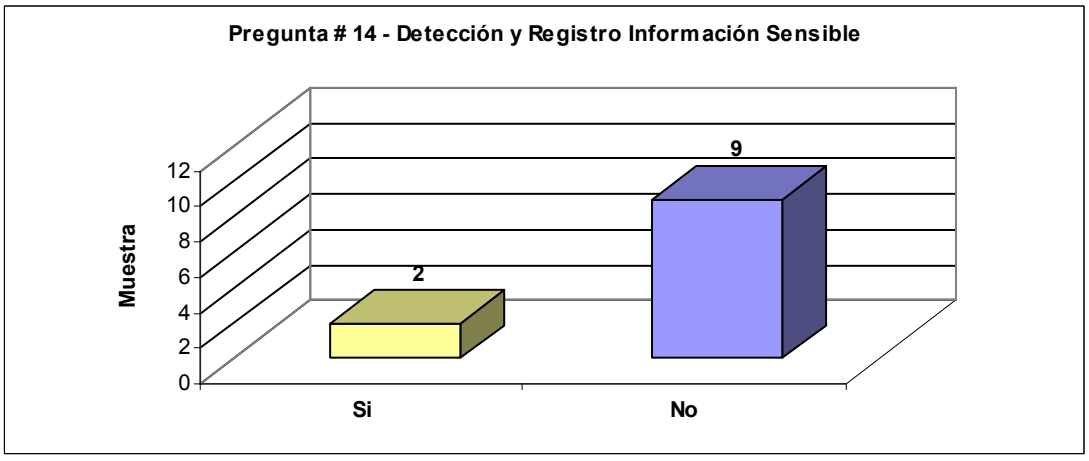

Figura 18. Detección y Registro

Para la pregunta número catorce tal como se observa en la figura 18, del total de la muestra de once entidades bancarias, dos encuestados que representan el 18%, consideran que en su organización no existen debilidades en cuanto a herramientas que tengan la capacidad de detectar y registrar cualquier acceso a información sensible de los tarjetahabientes, mientras que nueve que representan un 82% expresa que lo contrario.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

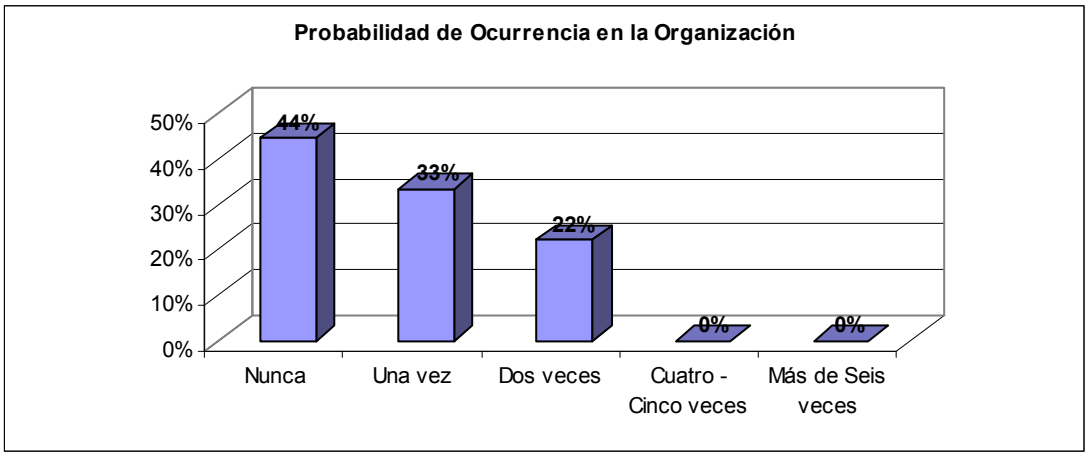

Figura 18.1 Probabilidad Ocurrencia

La figura 18.1 muestra que los entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 44%, en un 33% en una oportunidad y 22% en dos ocasiones, adicionalmente, el impacto de exposición de data sensible fue en un 22% insignificante, 11% menor, 56% moderado y 11% importante, tal como se observa en la figura 18.2.

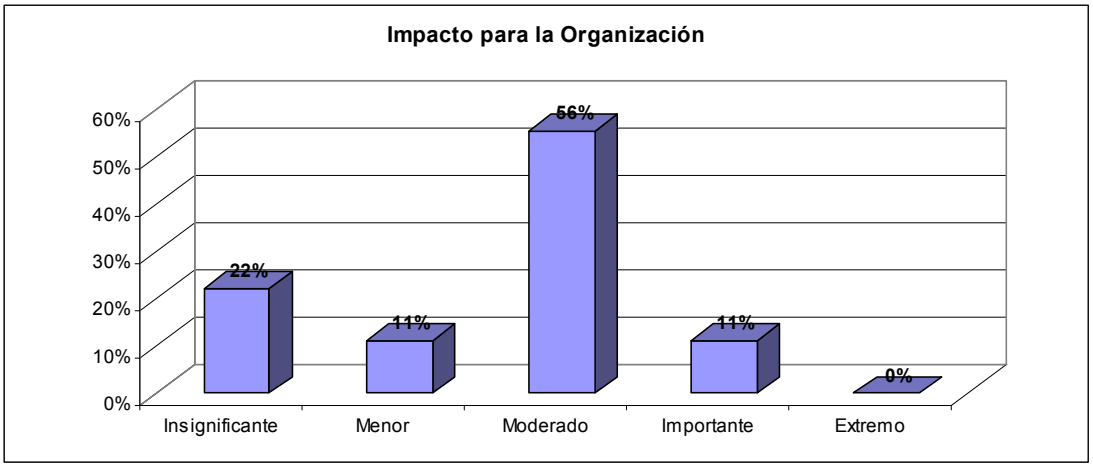

Figura 18.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 18, expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 18. Escala Probabilidad e Impacto. Detección y Registro

Entrevistado	Probabilidad	Impacto	Escala
E1	30%	5	2
E2	30%	10	4
E3	50%	40	20
E4	10%	5	0.5
E5	10%	20	2
E6	30%	20	6
E7	10%	20	2
E8	50%	20	10
E9	10%	20	2
			5.39

La media de las calificaciones obtenidas para el riesgo identificado es de **5.39.**

5.1.15. Prueba dispositivos inalámbricos

La interrogante número quince del instrumento consistió:

¿En la organización se realizan pruebas para identificar los todos los dispositivos inalámbricos en uso?

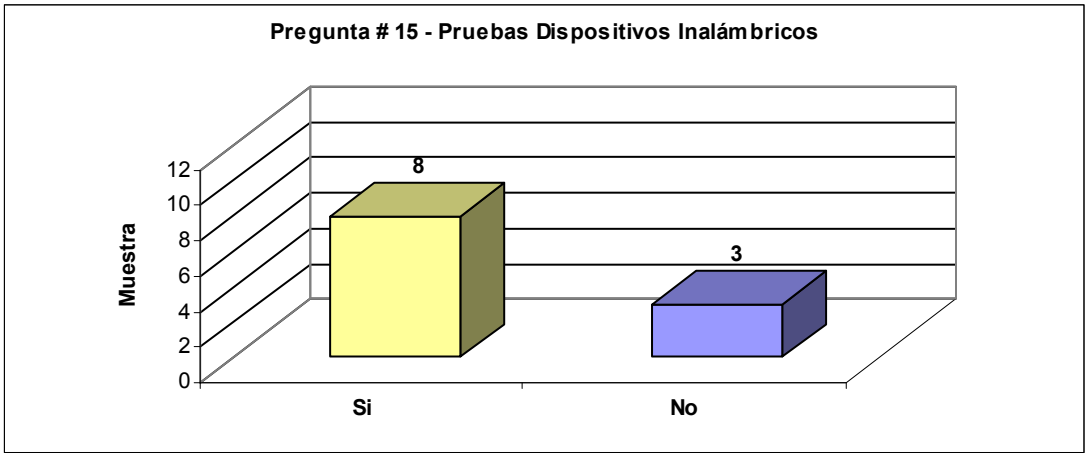

Figura 19. Pruebas Dispositivos Inalámbricos

Para la pregunta número quince tal como se observa en la figura 19, del total de la muestra de once entidades bancarias, tres encuestados que representan el 27%, consideran que en su organización no existen debilidades relacionadas con las pruebas de dispositivos inalámbricos en uso, mientras que ocho que representan un 27% expresa que lo contrario.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

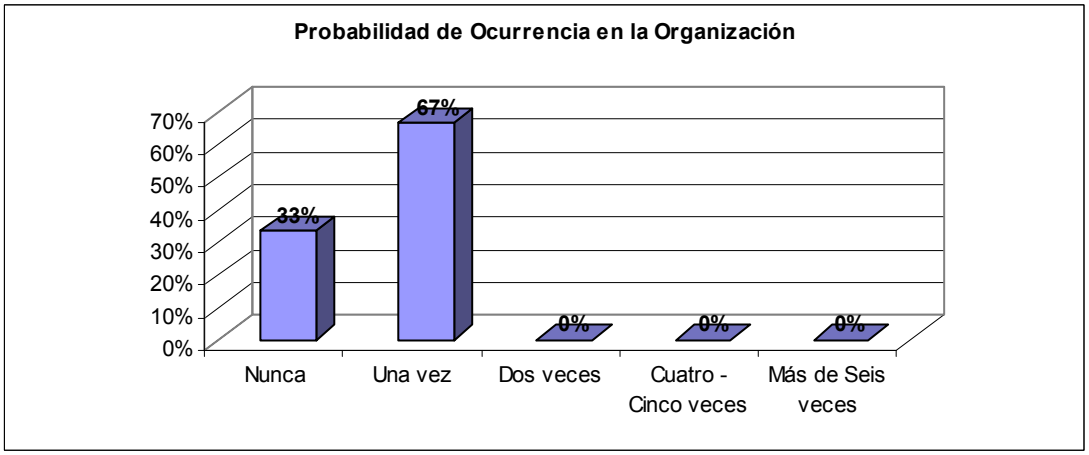

Figura 19.1 Probabilidad Ocurrencia

La figura 19.1 muestra que los entrevistados respondieron que en la organización este evento no se suscitó en el último año en un 33% y en un 67% en una oportunidad, adicionalmente, el impacto de exposición de data sensible fue en un 33% insignificante, 33% menor y 33% moderado, tal como se observa en la figura 19.2.

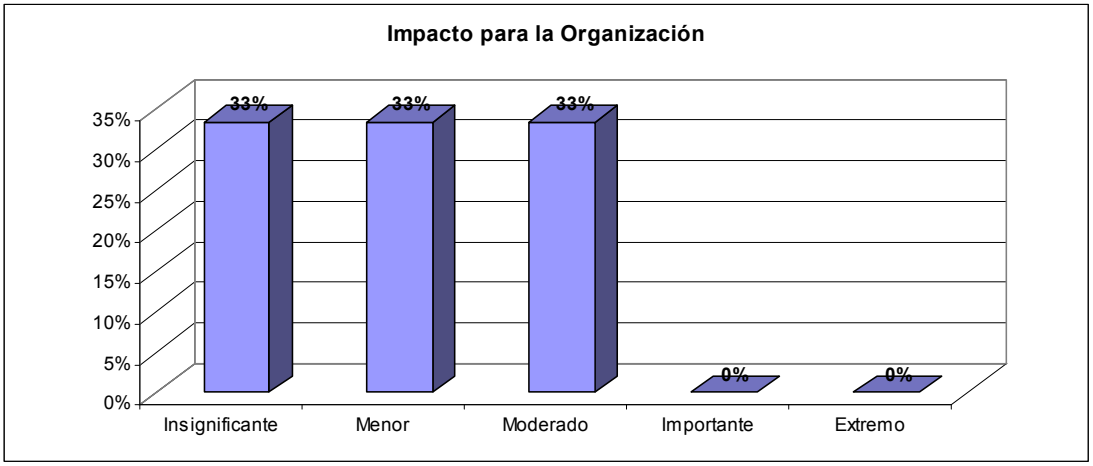

Figura 19.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 19, expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 19. Escala Probabilidad e Impacto. Pruebas Inalámbricas

Entrevistado	Probabilidad	Impacto	Escala
E1	10%	20	2
E2	30%	10	3
E3	30%	5	1.5
			2.17

La media de las calificaciones obtenidas para el riesgo identificado es de **2.17.**

5.1.16. Análisis interno y externo de vulnerabilidades

La interrogante número dieciséis del instrumento consistió:

¿En su organización se realizan análisis internos y externos de las vulnerabilidades de la red?

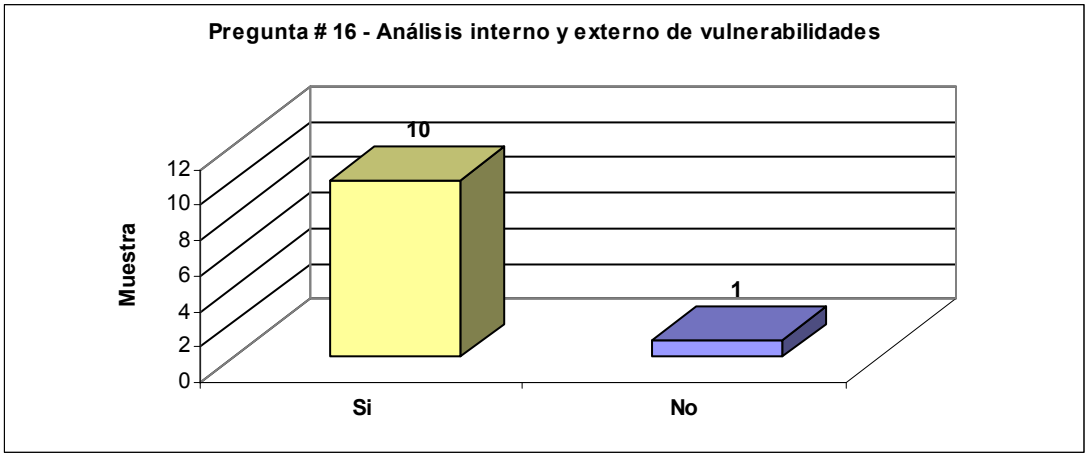

Figura 20. Análisis interno y externo de vulnerabilidades

Para la pregunta número dieciséis tal como se observa en la figura 20, del total de la muestra de once entidades bancarias, diez encuestados que representan el 91%, considera que en su organización existen debilidades en el análisis interno y externo de vulnerabilidades, mientras que uno que representa un 9% expresa que lo contrario.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

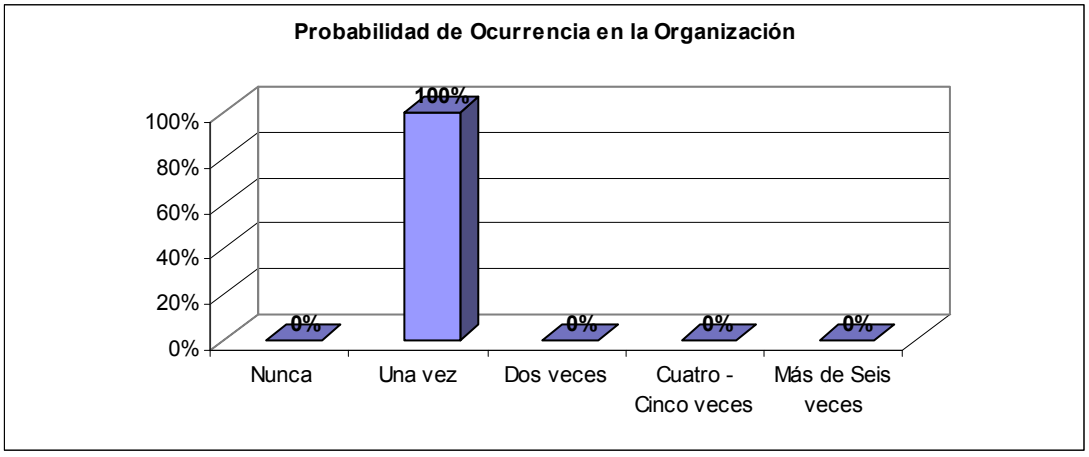

Figura 20.1 Probabilidad Ocurrencia

La figura 20.1 muestra que el entrevistados respondió que en la organización este evento se suscitó en un 100% en una oportunidad, adicionalmente, el impacto de exposición de data sensible fue en un 100% menor, tal como se observa en la figura 20.2.

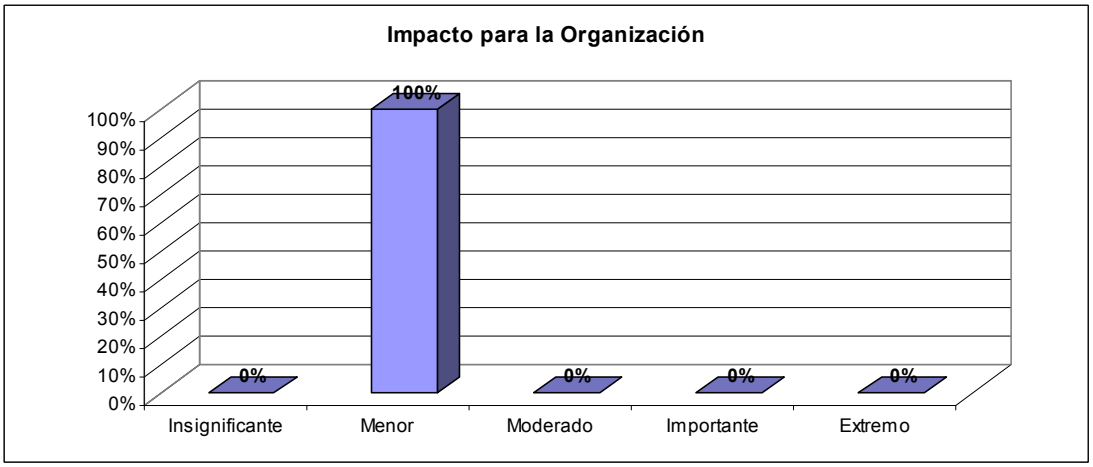

Figura 20.2 Impacto

En conclusión, el entrevistado que expresó que esta incidencia se había suscitado en su entidad bancaria, tal como se observa en la tabla 20, su respuesta fue que había ocurrido una vez en el último año, por tanto, se obtuvo una probabilidad de 30%, así como el impacto fue menor que

representa 10 en la escala definida, al hacer uso de la matriz de probabilidad e impacto, al realizar la multiplicación se obtiene como resultado **3.50**, tal como se muestra a continuación:

Tabla 20. Escala Probabilidad e Impacto. Análisis vulnerabilidades

Entrevistado	Probabilidad	Impacto	Calificación
E1	30%	10	3
			3.00

5.1.17. Pruebas de Penetración

La interrogante número diecisiete del instrumento consistió:

¿En su organización se realizan pruebas de penetración internas y externas a la infraestructura o aplicaciones?

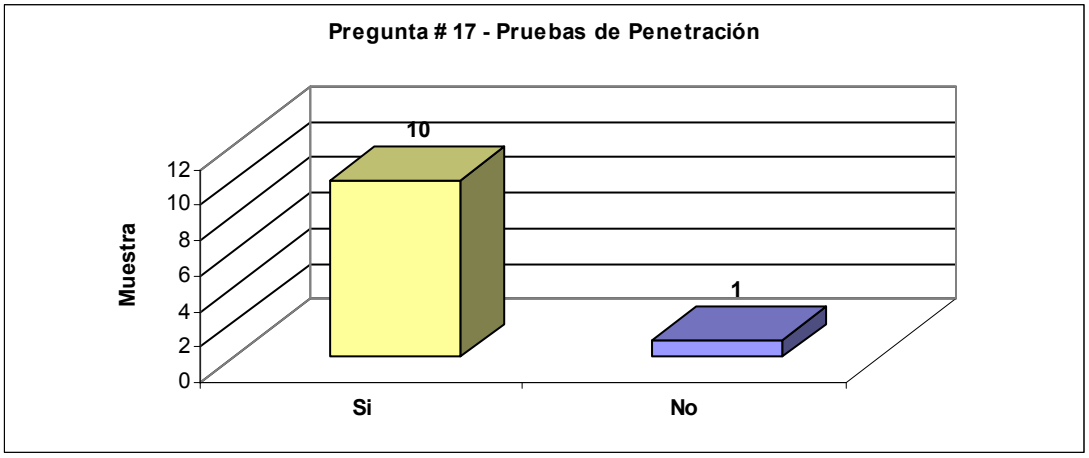

Figura 21. Pruebas de Penetración

Para la pregunta número diecisiete tal como se observa en la figura 21, del total de la muestra de once entidades bancarias, diez encuestados que representan el 91%, considera que en su organización existen debilidades en

las pruebas de penetración, mientras que uno que representa un 9% expresa que lo contrario.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

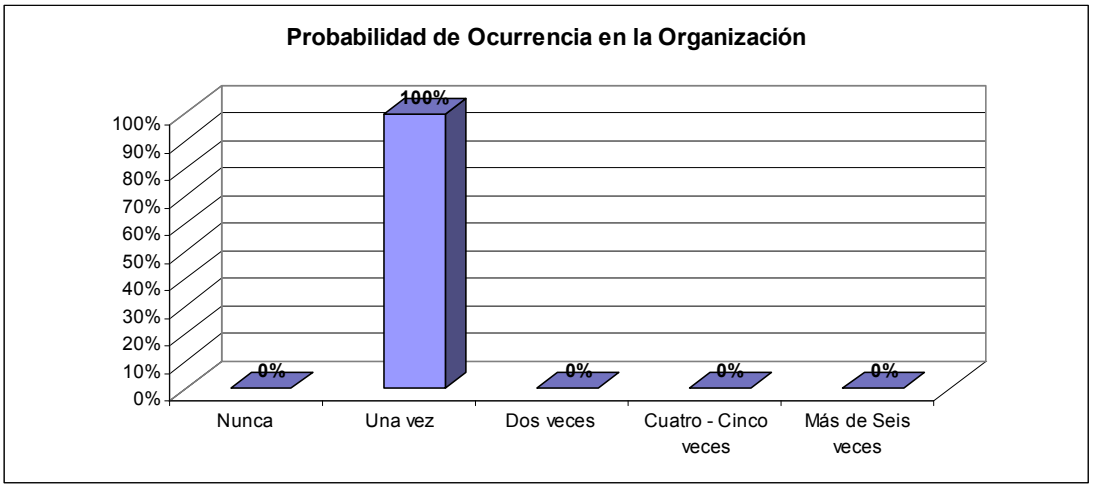

Figura 21.1 Probabilidad Ocurrencia

La figura 21.1 muestra que el entrevistados respondió que en la organización este evento se suscitó en un 100% en una oportunidad en el último año, adicionalmente, el impacto de exposición de data sensible fue en un 100% menor, tal como se observa en la figura 20.2.

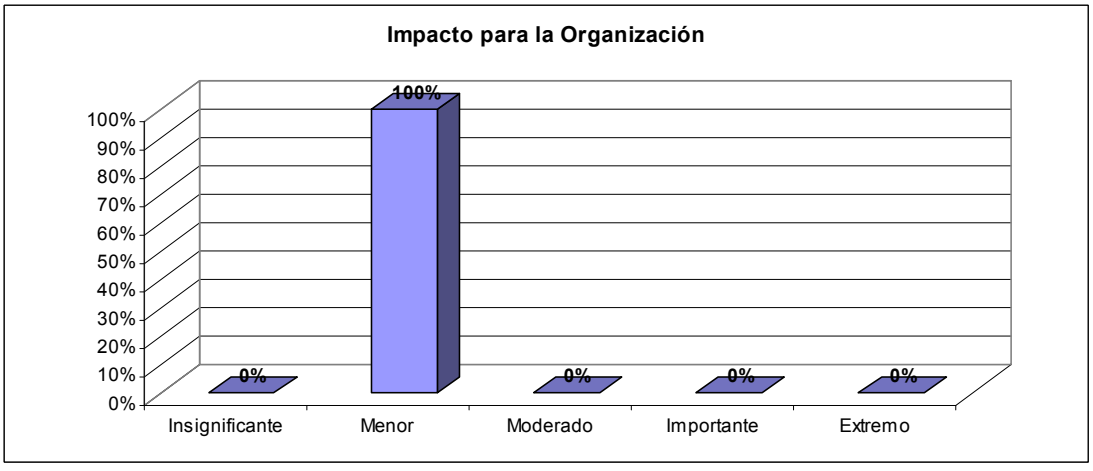

Figura 21.2 Impacto

En conclusión, el entrevistado que expresó que esta incidencia se había suscitado en su entidad bancaria, tal como se observa en la tabla 21, su respuesta fue que había ocurrido una vez en el último año, por tanto, se obtuvo una probabilidad de 30%, así como el impacto fue menor que representa 10 en la escala definida, al hacer uso de la matriz de probabilidad e impacto, al realizar la multiplicación se obtiene como resultado **3.00**, tal como se muestra a continuación:

Tabla 21. Escala Probabilidad e Impacto. Pruebas de Penetración

Entrevistado	Probabilidad	Impacto	Calificación
E1	30%	10	3
			3.00

5.1.18. Procesos de Comunicación

La interrogante número dieciocho del instrumento consistió:

¿Considera que existe debilidad en los procesos de comunicación y/o entrenamiento a los empleados acerca de la confidencialidad de los datos y su responsabilidad para la protección de los mismos?

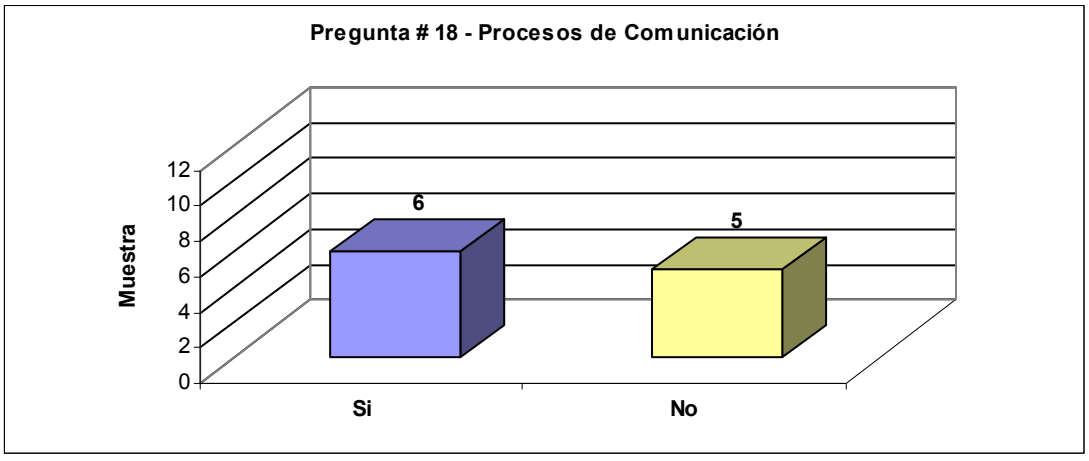

Figura 22. Procesos de Comunicación

Para la pregunta número dieciocho tal como se observa en la figura 19, del total de la muestra de once entidades bancarias, cinco encuestados que representan el 45%, consideran que en su organización no existen debilidades asociados a los procesos de comunicación y/o entrenamiento a los empleados acerca de la confidencialidad de los datos y su responsabilidad para la protección de los mismos, mientras que seis que representan un 55% expresa que lo contrario.

Se procedió a evaluar la probabilidad e impacto para el caso en donde existe exposición de data sensible.

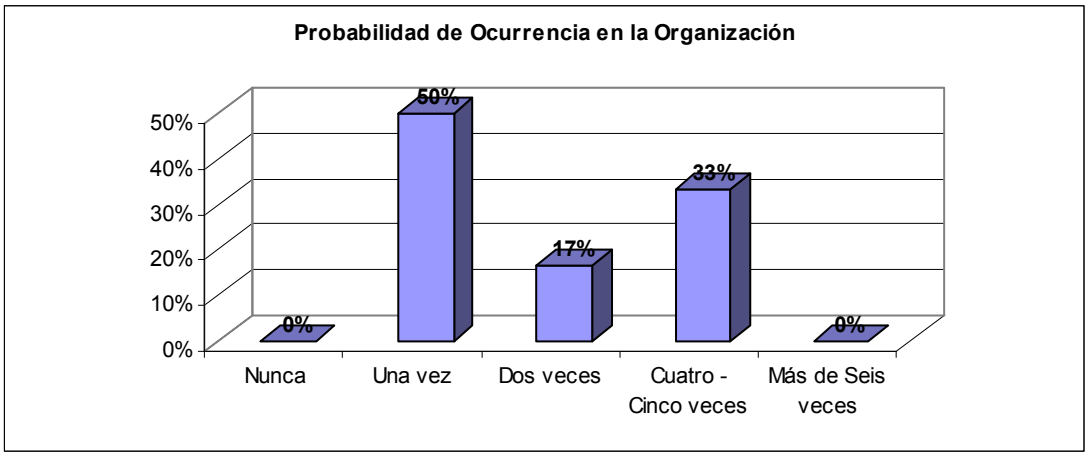

Figura 22.1 Probabilidad Ocurrencia

La figura 22.1 muestra que los entrevistados respondieron que en la organización este evento se suscitó en el último año en un 50% una vez, 33% dos ocasiones y 33% de cuatro a cinco, adicionalmente, el impacto de exposición de data sensible fue en un 50% insignificante, 17% menor, 17% moderado y 17% importante, tal como se observa en la figura 22.2.

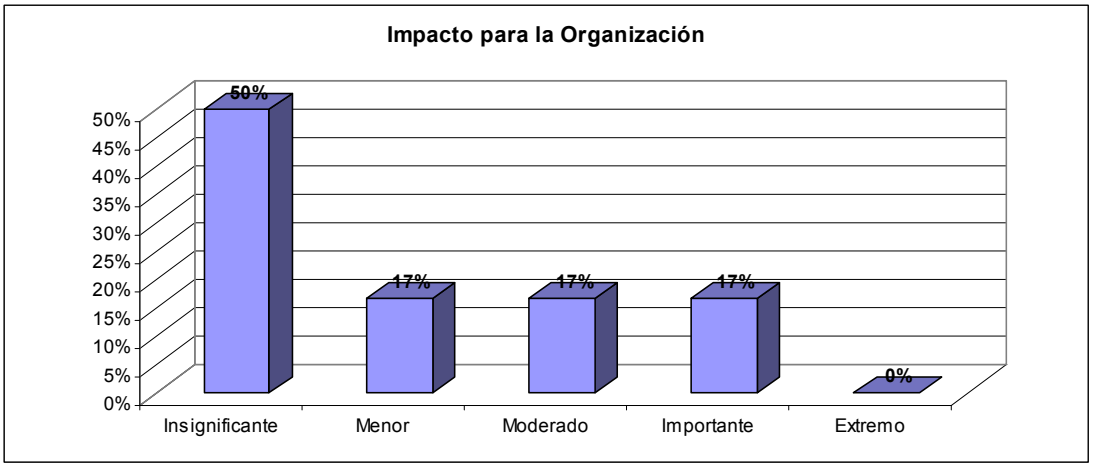

Figura 22.2 Impacto

En conclusión, para los entrevistados que expresaron que esta incidencia se suscitó en sus entidades bancarias tal como se observa en la tabla 18, expusieron las siguientes probabilidades de ocurrencia e impacto, dando como resultado la calificación:

Tabla 22. Escala Probabilidad e Impacto. Procesos de Comunicación

Entrevistado	Probabilidad	Impacto	Calificación
E1	30%	5	1.5
E2	70%	10	7
E3	30%	5	1.5
E4	50%	40	20
E5	30%	20	6
E6	70%	5	3.5
			7.90

5.2. Calificación de Riesgos Identificados

A continuación se presenta un resumen con las calificaciones de probabilidad de ocurrencia e impacto obtenidos para las entidades bancarias venezolanas:

Tabla 23. Calificación Probabilidad e Impacto Riesgos Obtenida

Pregunta Instrumento	Descripción del Riesgo	Calificación de Probabilidad e Impacto
1	Exposición de la organización bancaria por debilidad o ausencia en la identificación de los sistemas que almacenan, transmitan o procesen datos de tarjetas de crédito.	1.5
2	Exposición de la organización bancaria por ausencia en la división lógica de los componentes que almacenan, tramitan o procesen datos de tarjetas de crédito.	1.5
3	Exposición de la organización bancaria por ausencia o debilidad en los cortafuegos.	1.83
4	Exposición de la organización bancaria por uso de contraseñas predeterminadas.	1.5
5	Exposición de la organización bancaria por ausencia o debilidad en los mecanismos de cifrado, truncamiento, ocultamiento o refundición de data sensible.	10.14
6	Exposición de la organización bancaria por ausencia o debilidad en los mecanismos de protección adecuada de las claves criptográficas.	4.22
7	Exposición de la organización bancaria por debilidad o ausencia en la codificación de la información sensible a través de redes públicas.	2.83
8	Exposición de la organización bancaria por falta de antivirus o debilidad en la actualización del mismo.	2
9	Exposición de la organización bancaria por debilidad en los parches de seguridad.	0.5
10	Exposición de la organización bancaria por debilidad en la mitigación de brechas de seguridad en el desarrollo de aplicativos propios.	0.5
11	Exposición de la organización bancaria por debilidad en el detalle de los roles y responsabilidades	6.65
12	Exposición de la organización bancaria por uso de credenciales genéricas	0.5
13	Exposición de la organización bancaria por debilidad en la seguridad física.	2.3
14	Exposición de la organización bancaria por debilidad al detectar y/o registrar cualquier acceso a información sensible.	5.39
15	Exposición de la organización bancaria por debilidad en pruebas de dispositivos inalámbricos en uso.	2.17
16	Exposición de la organización bancaria al no realizarse pruebas internas y externas de vulnerabilidades en la red.	3
17	Exposición de la organización bancaria al no realizarse pruebas de penetración internas y externas a aplicaciones o infraestructura.	3
18	Exposición de la organización bancaria por debilidad en los procesos de comunicación y/o entrenamiento a los empleados acerca de la confidencialidad de los datos y su responsabilidad para la protección de los mismos	7.9

5.2. Calificación de Riesgos Identificados Priorizados

De acuerdo a las calificaciones obtenidas de los riesgos identificados y con la finalidad de elaborar un plan para la implementación de la norma de la industria de tarjeta de pago, a continuación de priorizan los riesgos detectados de manera de tomar acciones de control y mitigación, atendiendo al orden que representan mayor criticidad (probabilidad de ocurrencia e impacto).

Tabla 24. Calificación Probabilidad e Impacto Riesgos Priorizada

Pregunta Instrumento	Descripción del Riesgo	Calificación de Probabilidad e Impacto
5	Exposición de la organización bancaria por ausencia o debilidad en los mecanismos de cifrado, truncamiento, ocultamiento o refundición de data sensible.	10.14
18	Exposición de la organización bancaria por debilidad en los procesos de comunicación y/o entrenamiento a los empleados acerca de la confidencialidad de los datos y su responsabilidad para la protección de los mismos	7.9
11	Exposición de la organización bancaria por debilidad en el detalle de los roles y responsabilidades	6.65
14	Exposición de la organización bancaria por debilidad al detectar y/o registrar cualquier acceso a información sensible.	5.39
6	Exposición de la organización bancaria por ausencia o debilidad en los mecanismos de protección adecuada de las claves criptográficas.	4.22
16	Exposición de la organización bancaria al no realizarse pruebas internas y externas de vulnerabilidades en la red.	3
17	Exposición de la organización bancaria al no realizarse pruebas de penetración internas y externas a aplicaciones o infraestructura.	3
7	Exposición de la organización bancaria por debilidad o ausencia en la codificación de la información sensible a través de redes públicas.	2.83
13	Exposición de la organización bancaria por debilidad en la seguridad física.	2.3
15	Exposición de la organización bancaria por debilidad en pruebas de dispositivos inalámbricos en uso.	2.17
8	Exposición de la organización bancaria por falta de antivirus o debilidad en la actualización del mismo.	2
3	Exposición de la organización bancaria por ausencia o debilidad en los cortafuegos.	1.83
1	Exposición de la organización bancaria por debilidad o ausencia en la identificación de los sistemas que almacenan, transmitan o procesen datos de tarjetas de crédito.	1.5
2	Exposición de la organización bancaria por ausencia en la división lógica de los componentes que almacenan, tramitan o procesen datos de tarjetas de crédito.	1.5
4	Exposición de la organización bancaria por uso de contraseñas predeterminadas.	1.5
9	Exposición de la organización bancaria por debilidad en los parches de seguridad.	0.5
10	Exposición de la organización bancaria por debilidad en la mitigación de brechas de seguridad en el desarrollo de aplicativos propios.	0.5
12	Exposición de la organización bancaria por uso de credenciales genéricas	0.5

CAPITULO VI

PLAN PARA LA IMPLEMENTACIÓN DE LA NORMA DE LA INDUSTRIA DE TARJETAS DE PAGO EN ENTIDADES BANCARIAS VENEZOLANAS

El diseño del plan para la implementación de la norma de la industria de tarjeta de pago en entidades bancarias venezolanas está conformado por tres pilares fundamentales para su desarrollo exitoso: identificación de los riesgos, priorización de los riesgos a través del análisis cualitativo que fueron desarrollados en capítulos previos y por último el plan de respuesta a los riesgos detectados.

El proceso consistió en primera instancia en conocer y analizar la norma de la Industria de Tarjetas de Pago, este estudio arrojó que la misma posee tres vertientes: PED, para dispositivos de entrada tales como los puntos de venta, PA – DSS que aplica para vendedores de software y el DSS que aplica a cualquier entidad que almacene, procese o transmita número de tarjetas de crédito. Este estudio se enmarcó para el último escenario tal como se expuso en el capítulo de planteamiento del problema.

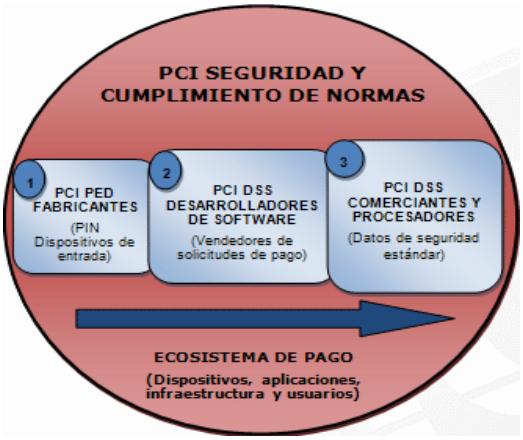

Figura 23. Vertientes Norma PCI
Fuente: IQ Seguridad en Medios de Pago. (2009)

Al estudiar la norma se conoció que la misma está compuesta por doce (12) requisitos que abarcan tanto el área técnica como los procesos del negocio, por tanto, se desarrolló un instrumento en donde se plasmaron interrogantes que fueron alineados en el contexto de cada política descrita por la Industria de Tarjetas de pago.

Como se ha mencionado anteriormente, el análisis de resultados que se realizó en el capítulo anterior fue enfocado en los eventos que conllevan consecuencias o impactos adversos, es decir, en riesgos negativos para la organización.

El desarrollo de las políticas consistió en estudiar y analizar cada uno de los requisitos que componen la norma y describir sus pautas en el TEG de forma exhaustiva, de manera de lograr el objeto principal de este estudio, que el mismo sea utilizado para la implementación de la norma en las entidades bancarias venezolanas.

En línea con lo expuesto anteriormente, el plan de respuesta de riesgos es el proceso de desarrollar estrategias de respuesta en función a su prioridad, a continuación se exponen las políticas de acuerdo a la norma de la industria de la norma de pago, de acuerdo a la criticidad obtenida en la tendencia de la banca nacional, a través del análisis cualitativo:

6.1. Política de mecanismos de cifrado, truncamiento, ocultamiento o refundición de data sensible

La exposición de la organización bancaria por ausencia o debilidad en los mecanismos de cifrado, truncamiento, ocultamiento o refundición de data sensible puede ser mitigada a través una serie de procedimientos que se describen a continuación:

Se deben obtener, evaluar las políticas y procedimientos de la empresa relativos a la retención y disposición de los datos, esto incluye los requisitos legales y reglamentarios en donde deben ser almacenados en el lapso de tiempo requerido. Además, de métodos automáticos para la eliminación de los datos luego de que este tiempo haya transcurrido.

No deben ser almacenados datos confidenciales de autentificación luego de recibir la autorización, aunque los mismos se encuentren cifrados tales como:

- Totalidad de la pista de la banda magnética, Chip o en algún otro dispositivo.

- Código de validación de las tarjetas (número de tres o cuatro dígitos) que se encuentra en el anverso o reverso de las tarjetas de crédito que se utiliza para verificar las transacciones de tarjetas ausentes.

- Número de identificación personal (PIN) ni el bloqueo del PIN cifrado.

- Se debe ocultar el PAN cuando aparece, solo pueden ser los primeros seis y los últimos cuatro dígitos. Adicionalmente cuando el PAN es almacenado debe ser de forma ilegible.

6.2. Política de procesos de comunicación

La exposición de datos sensible en la organización bancaria por debilidad en los procesos de comunicación o entrenamiento a los empleados acerca de la confidencialidad de los datos y su responsabilidad para la protección de los

mismos, es uno de los elementos principales para la implementación de medidas de seguridad de la información.

Para que los empleados se sientan comprometidos con la gestión de la seguridad, se les debe concienciar e informar a fin de que cumplan con las medidas establecidas por la organización en el desempeño habitual de sus funciones.

Es preciso instruir al personal de forma apropiada sobre seguridad y el uso correcto de los sistemas de información y sus recursos, así como sobre la importancia de la seguridad en el tratamiento de los datos en la organización.

Es importante que se definan campañas periódicas a los empleados para entrenamiento y evitar errores por desinformación, así como formarle el compromiso hacia la empresa.

Adicionalmente, se deben definir exigencias de confidencialidad y no divulgación de datos para todo el personal que dispone de acceso al sistema de información para el desarrollo de sus funciones, tanto para el personal contratado como para el personal externo. Estas exigencias se definirán formalmente en acuerdos de confidencialidad, que todo el personal deberá firmar como prueba de su recepción.

Esto permitirá que un empleado antes de ofrecer o comentar alguna información sensible asociada a tarjetas de crédito que pueda exponer al banco lo piense dos veces, ya que existe un contrato firmado en donde se pueden asumir medidas legales o disciplinarias.

6.3. Política de definición de roles y responsabilidades

Uno de los principales riesgos en la banca es el acceso de usuarios no autorizados (internos o externos) que puedan consultar información sensible de tarjetas de crédito.

Se deben definir las funciones y responsabilidades de seguridad para cada uno de los usuarios del sistema de información; para ello se aplicará el principio de establecer los mínimos privilegios necesarios para el desarrollo de dichas labores, de manera tal, que se le otorgue el acceso a la información de tarjetas de crédito de acuerdo a un rol específico.

Los sistemas de control de acceso deben abarcar todos los componentes del sistema, inicialmente estará predefinido en modo no permitir ningún acceso para que luego le sea otorgado a un empleado los privilegios de acuerdo a un cargo en específico.

El empleado debe ser informado de forma clara y precisa acerca de sus funciones y obligaciones en el tratamiento de los datos.

Cada proceso de seguridad debe identificar a un propietario y a los usuarios que participarán en el mismo, de esta forma se evitarán malentendidos acerca de las responsabilidades sobre los elementos del sistema de información.

Todas las funciones y responsabilidades deben comunicarse a los usuarios involucrados en su ejecución, de una forma clara y asegurando su recepción y entendimiento.

6.4. Política de registro de acceso a información sensible

Los mecanismos de registro y la posibilidad de rastrear las actividades del usuario son críticos para la prevención, detección o minimización del impacto de los riesgos de datos. La presencia de los registros en todos los entornos permite el rastreo, alertas y análisis cuando algo no funciona bien. La determinación de la causa de algún riesgo es muy difícil sin los registros de la actividad del sistema.

Deben implementarse los siguientes mecanismos:

- Se deben establecer procesos que vinculen todos los accesos a componentes del sistema a cada usuario en particular.

- De deben implementar auditorías automatizadas para todos los componentes del sistema a fin de reconstruir accesos a data sensible de tarjetas de crédito, personas con privilegios de administrador.

- Es importante que la reconstrucción de eventos cuente con una precisión en cuanto al tipo, fecha, hora y componentes relacionados al evento, así como si fuese exitoso o no.

Se debe tener especial cuidado en donde se almacene esta información de auditoría para evitar que haya acceso indebido y se realicen eliminaciones.

Se debe realizar una revisión de al menos una vez al día en busca de registros anormales.

Se debe mantener un histórico durante al menos un año y de los últimos tres meses disponible para posible análisis.

Con estas medidas se podrá realizar una traza en caso de un evento irregular y se permitirá tomar acciones correctivas de inmediato.

6.5. Política protección claves criptográficas

Se deben proteger las claves criptográficas que se utilizan para cifrar los datos de los titulares de tarjetas de acuerdo a las siguientes premisas:

- Se debe restringir el acceso a las claves al mínimo de personas posible.

- Se deben guardar de forma segura en el mínimo de ubicaciones y formas posibles.

- Se deben generar de forma sólida, tener una distribución y almacenamiento seguro.

- Los cambios de las claves se realizarán de forma periódica.

- Existir métodos seguros de destrucción de claves antiguas o en riesgo.

- Aplique mecanismos en donde las claves sean creadas entre varias personas y solo cada una de ellas conozca su porción de la clave para formar una completa.

6.6. Política pruebas vulnerabilidades a la red

Las pruebas de vulnerabilidad forman parte esencial de la seguridad de los datos ya que a través de la misma se detecta el nivel de exposición del sistema ante amenazas.

Se debe implementar una política de seguridad en donde se realicen análisis internos y externos de vulnerabilidades de red al menos trimestralmente y después de cada cambio significativo en la red (tales como: instalaciones de componentes del sistema, cambios en la topología de red, modificaciones en las normas del los cortafuegos, actualizaciones de productos).

Se deben inspeccionar los resultados de los últimos cuatro trimestres de los análisis de la red interna para verificar que se realicen las pruebas de seguridad periódicas de los dispositivos dentro del entorno de datos de los titulares de tarjetas. Es importante que en este proceso de análisis sea realizado hasta que se obtengan resultados aprobados, es decir que no hayan brechas en los análisis de vulnerabilidades realizados.

Es importante destacar que los análisis trimestrales de vulnerabilidades externas debe realizarlos un Proveedor Aprobado de Escaneo (ASV) certificado por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC).

6.7. Política pruebas penetración

Las pruebas de penetración son la estrategia más efectiva para evaluar tanto la competencia como las necesidades de los componentes del sistema bancario. Una prueba de penetración simula un ataque desde afuera y proporciona un riguroso examen de vulnerabilidades actuales y potenciales,

incluyendo fallas de software y hardware, configuraciones defectuosas del sistema, medidas de protección insuficientes.
Se debe implementar una política de seguridad en donde se realicen pruebas de penetración externas e internas al menos una vez al año y después de cualquier actualización o modificación significativa de infraestructuras o aplicaciones (como por ejemplo la actualización del sistema operativo, la adición de una subred al entorno, o la adición de un servidor Web al entorno). Estas pruebas de penetración deben incluir lo siguiente:

- Pruebas de penetración de cada de red.
- Pruebas de penetración de capa de aplicación.

Se deben examinar los resultados de la última prueba de penetración para verificar que dichas pruebas se realicen al menos anualmente y después de cualquier cambio significativo realizado en el entorno, este proceso debe ser realizado hasta que las vulnerabilidades detectadas se hayan corregido.

Se debe velar que la prueba se haya realizado con un recurso interno calificado o bien que la haya realizado un tercero capacitado.

6.8. Política codificación de la información sensible a través de redes públicas

La información que es confidencial debe ser codificada en su momento de transmisión, con la finalidad de fortalecer el entorno de los datos de los titulares de las tarjetas ante posibles delincuentes que deseen explotar estas vulnerabilidades.

Esta actividad puede ser realizada a través:

- Hacer uso de protocolos sólidos como SSL/TLS o IPSEC y de métodos criptográficos para que los datos y su transmisión sea seguro por medio de redes públicas.

- Cuando se ponga en práctica la transmisión de datos de manera inalámbrica, dicha arquitectura debe estar basada de acuerdo a las mejores prácticas de la industria para tecnologías inalámbricas, tales como IEEE 802.11i.

- Implementar criptografía y protocolos de seguridad sólidos como SSL/TLS o IPSEC para salvaguardar los datos confidenciales de los titulares de las tarjetas durante su transmisión a través de redes públicas abiertas tales como: inalámbricas, sistema global de comunicaciones móviles (GSM) y servicio de radio paquete general.

- No debe enviarse bajo ningún concepto las PAN de los clientes, si las mismas no se encuentran cifradas a través de tecnologías tales como: Chat, mensajería instantánea, correo electrónico.

6.9. Políticas de seguridad física

Se debe desarrollar y aplicar una política robusta de restricción de cualquier acceso físico a datos o sistemas que alojen datos de titulares de tarjetas, así como la eliminación de eliminación de sistemas o copias en papel.

Se deben implementar controles de entrada al banco para limitar y supervisar el acceso a sistemas en el entorno de datos de titulares de tarjetas.

Deben existir cámaras de video u otros mecanismos de control de acceso para supervisar el acceso físico de personas a áreas confidenciales, esta información debe ser almacenada al menos tres meses.

Debe haber restricciones de acceso físico a conexiones de red de acceso público, así como de puertas de enlace y dispositivos manuales.

Deben existir procedimientos para distinguir fácilmente a empleados y visitantes, hacer especial énfasis en donde haya datos de titulares de tarjetas.

Los visitantes deben contar con mecanismos de:

- Autorización previa al ingreso a áreas en las que se procesan o se conservan datos de titulares de tarjetas.
- Se le debe otorgar un carnet de identificación con vencimiento y que se identifiquen fácilmente que no pertenecen al banco.
- Se le debe solicitar la entrega del carnet físico antes de salir de las instalaciones del banco, así como llevar un registro de visitas.
- Estos registros deben ser almacenados al menos tres meses.

Los medios de copias de seguridad deben ser almacenados en un lugar seguro, preferiblemente externo al banco y el lugar debe ser revisado al menos una vez al año.

.

Se debe implementar un control exhaustivo de distribución de cualquier medio que contenga datos de tarjetas de crédito:

Clasificación de los medios en donde se puedan identificar los confidenciales.

Si son enviados por correo electrónico debe ser seguro y si son por otros medios deben rastrearse fácilmente.

Debe implementarse que políticas de aprobaciones gerenciales para cualquier distribución.

Cuando deban destruirse los medios por razones del banco o por motivos legales córtense las tiras, incinérense o utilice un medio que sea fiable para su destrucción.

6.10. Política pruebas dispositivos inalámbricos en uso

Es imprescindible la realización de pruebas para comprobar la presencia de puntos de acceso inalámbricos mediante el uso de un analizador inalámbrico al menos trimestralmente o la implementación de un sistema de detección de intrusiones (IDS)/sistema contra intrusos (IPS) inalámbrico para identificar todos los dispositivos inalámbricos en uso.

En caso de que se implemente un sistema de un IDS/IPS inalámbrico, se debe verificar que el mismo genere alertas al personal en caso de una irregularidad.

Debe generarse en caso de no existir un plan de respuesta en la organización en caso de que se detecten dispositivos inalámbricos no autorizados.

6.11. Política de antivirus

En la actualidad en Internet existen innumerables virus, troyanos, spywares y adwares, programas que se instalan en las computadoras y pueden propagarse a través de la red, deben implementarse políticas de seguridad haciendo uso de programas antivirus disminuimos significativamente la brecha de seguridad con las siguientes pautas:

- Implementar programas antivirus en todos aquellos sistemas que pueden ser atacados tales como: computadoras personales y servidores.

- Implementar programas antivirus que tengan la capacidad de detectar, eliminar y proteger los sistemas, así como actualizarse con las últimas novedades y generar reportes.

6.12. Política de cortafuegos

Los cortafuegos, o Firewall como se denomina en inglés, son dispositivos de hardware o de software que forman parte de las redes. Los cortafuegos son utilizados para que usuarios no autorizados tengan acceso a redes privadas a través de Internet. Los mismos controlan el tránsito de entrada y salida a las áreas más sensibles de la red confidencial de las empresas, evaluando y bloqueando las transmisiones que no cumplan los criterios definidos.

Los cortafuegos tienen la función de proteger el ingreso a los sistemas por medio de la Internet tales como: las computadoras de los empleados y su correo electrónico, comercio electrónico, redes inalámbricas, etc.

Este es el primer requisito que establece PCI, a continuación se describirá detalladamente los requerimientos que la conforman:

Se deben establecer estándares de configuración del firewall y del enrutador en donde exista un mecanismo formal en donde se aprueben y evalúen los cambios y las conexiones de red, esto debe plasmarse en diagramas en donde se evidencien los flujos de los datos de las tarjetas de crédito, la utilización de los servicios, protocolos, puertos permitidos, así como, descripción de las políticas de seguridad para el uso de puertos inseguros. Esta documentación debe ser revisada y actualizada al menos cada seis meses.

Deben existir cortafuegos entre las redes inalámbricas y el entorno de datos de los titulares de las tarjetas de crédito con la finalidad de negar o limitar el ingreso desde este medio.

No debe existir un acceso directo público entre Internet y todo componente del sistema que compone el entorno de los datos de los titulares de tarjetas.

Deben existir políticas de seguridad en donde cualquier computadora que tenga conectividad a Internet tenga instalado cortafuegos actualizados y que se actualicen con mucha regularidad.

6.13. Política identificación de los sistemas

Una política de suma importancia para la implementación exitosa de las normas de tarjetas de pago, es realizar un análisis de la organización, identificar los puntos en la cadena de valor donde se transmite, procesa o almacena información de tarjetas de crédito y definir el entorno que debe ser protegido.

Si en el banco no cuenta con una definición detallada se deben establecer mesas de trabajo con las diferentes unidades para luego hacer una unión de esa información para identificar de forma minuciosa el entorno.

6.14. Política división lógica

El entorno de los datos del titular de la tarjeta es la parte de la red que posee los datos del titular de la tarjeta o los datos confidenciales de autenticación, incluidos los componentes de la red, los servidores y las aplicaciones.

Los componentes de la red incluyen, a modo de ejemplo, cortafuegos, interruptores, routers, puntos de acceso inalámbricos, dispositivos de red y otros dispositivos de seguridad.

Los tipos de servidores incluyen, a modo de ejemplo: Web, base de datos, autenticación, correo electrónico, Proxy, protocolo de tiempo de red (NTP) y servidor de nombre de dominio (DNS).

Las aplicaciones incluyen todas las aplicaciones compradas y personalizadas, incluidas las aplicaciones internas y externas (Internet).

Sede ser desarrollada una política de adecuada segmentación de red, que aísla los sistemas que almacenan, procesan o transmiten datos del titular de la tarjeta de los que no lo hacen, esto ofrece la ventaja que se reduce el alcance del entorno de los datos del titular para la aplicación y cumplimiento de mecanismos de seguridad.

6.15. Política de no uso de contraseñas predeterminadas

Los componentes tanto de software como de hardware que conforman la tecnología de la información, poseen contraseñas estándar cuando parten de la fábrica. En muchas ocasiones por no tener una política rigurosa de seguridad, las contraseñas no son modificadas cuando son implementados en los sistemas de producción de las empresas. Las personas tanto internas como externas a las empresas que desean afectar los sistemas conocen las contraseñas y parámetros ya que son conocidas y pueden ser difundidas a través de Internet.

6.16. Política de parches de seguridad

Un parche es un código que se le aplica a un programa para realizar una mejora a un programa existente, optimizando un código, agregando funcionalidades y generando actualizaciones.

Los parches de seguridad son de vital importancia para proteger el entornos de los titulares de tarjetas de crédito, debido a que los proveedores están constantemente analizando posibles huecos de seguridad y proveen de las mejoras a sus clientes para que fortalezcan sus sistemas.

Adicionalmente, en el caso de que las empresas cuenten con un departamento de desarrollo de software personalizado, existen pautas que deben cumplirse rigurosamente para mitigar las vulnerabilidades de seguridad para que los programas entren en ambiente de producción, para el cumplimiento de la norma PCI:

- Los componentes de sistemas y software deben contar con los últimos parches de los proveedores en un lapso no mayor a un mes, para el logro de este objetivo se desarrolla un proceso de flujo de información

para la empresa, en donde se obtengan notificaciones de las últimas actualizaciones de los proveedores de sus componentes.

- Realizar pruebas de manejo de errores, almacenamiento criptográfico, comunicaciones seguras y control de acceso para validar que el programa, sus parches de seguridad y entorno de software cumplen a cabalidad con las políticas de seguridad antes de pasar al ambiente de producción.

6.17. Política desarrollo aplicativos propios

Para el caso de las empresas que desarrollen sus propias aplicaciones hay una serie de pautas basadas en las mejores prácticas para que sean implementados con las normativas de seguridad:

- Los ambientes de desarrollo y pruebas, deben estar separados al de producción.

- Bajo ningún concepto usar datos del entorno de tarjetas de pago para el ambiente de desarrollo, calidad o pruebas.

- Eliminar cualquier dato ficticio, identificador y contraseña que haya sido usado en los ambientes de desarrollo/calidad o pruebas antes de pasar a producción.

- Para el proceso de control de cambios se deben tomar las siguientes consideraciones:

    Documentar las incidencias.

Contar con las aprobaciones de los involucrados en el proceso: especialistas, gerentes del área.
Pruebas de funcionalidad operativa.
Procedimientos de desinstalación.

- Aplicaciones Web: las empresas al desarrollar aplicaciones Web tanto internas como externas serán realizadas bajo las prácticas de la OWASP.

  La OWASP, acrónimo de Open Web Application Security Project en inglés, Proyecto de seguridad de aplicaciones Web abiertas, es un organismo conformado por comunidades educativas, empresas de todo el mundo con el fin de investigar y determinar soluciones para hacer el software Web seguro. La OWASP trabaja en desarrollar herramientas, metodologías, documentación.

  La OWSP destaca que para el desarrollo de una aplicación Web seguro hay que analizar:

  Lenguaje de comandos entre distintos sitios (XSS).
  Errores de inyección tales como: SQL, LDAP y Xpath.
  Ejecución de archivos maliciosos
  Referencias inseguras a objetos directos.
  Falsificación de solicitudes entre distintos sitios (CSRF).
  Filtración de información y manejo inadecuado de errores.
  Autenticación y administración de sesión interrumpidas.
  Almacenamiento criptográfico inseguro.
  Comunicaciones inseguras.
  Omisión de restringir el acceso URL.

- Para aplicaciones Web públicas contar con un firewall que proteja el tráfico de información, así como desarrollar herramientas y métodos para la detección de vulnerabilidades.

6.18. Política de no uso de credenciales genéricas

Es fundamental que cada empleado cuente con una identificación única para el acceso, esto ofrece que cada persona sea responsable por la información que acceda y haya una trazabilidad.

Los identificadores grupales son muy perjudiciales para el negocio ya que si ocurriese algún tipo de fuga de información, no se podría constatar de quien fue.

Adicionalmente aplicar las siguientes políticas para el uso de las contraseñas:

- Asignación de identificadores únicos a cada empleado antes de tener acceso a cualquier componente del sistema.

- Incluir un método adicional al identificador único para la autentificación tales como: contraseñas, dispositivos token, tarjetas inteligentes, biometría o claves públicas.

- Incorporar una doble autentificación para el acceso remoto.

- Mantener ilegibles todas las contraseñas con encriptamiento durante la transmisión y almacenamiento.

- Mantenga un proceso para el mantenimiento de los identificadores y contraseñas.

- Usar mecanismos de validación de usuarios al reestablecer contraseñas.

- Establezca la primera contraseña del usuario y fije de manera obligatoria su modificación en el primer uso.

- Elimine inmediatamente cualquier acceso de usuario que ya no se encuentre en la compañía o no tenga privilegios para el uso del mismo.

- En un lapso de máximo noventa días aquellas cuentas que no estén activas serán inhabilitadas.

- Mantenga una red de comunicación a todos los empleados acerca de las políticas de contraseñas-

- Activar las cuentas que utilizan los proveedores para el mantenimiento de los sistemas solo por el tiempo que hagan uso de las mismas.

- Establecer que las contraseñas de los usuarios caduquen al menos cada noventa días.

- Solicitar que la contraseña de los usuarios sea de al menos siete caracteres y que contenga caracteres tanto numéricos como alfabéticos.

- No permitir repeticiones de contraseñas de al menos las cuatro anteriores.

- Limitar los intentos erróneos a seis, luego bloquear el usuario.

- Establecer una duración mínima de bloqueo de treinta minutos o hasta que el administrador habilite la ID del usuario.

- Solicitar la clave al usuario si su actividad ha cesado por más de quince minutos.

- Debe existir una estricta política de autenticación a bases de datos que formen parte del entorno de tarjetas de crédito.

6.19. Plan de control cumplimiento

En el apartado anterior fueron desarrolladas las políticas de acuerdo a la tendencia de la banca nacional y en base a la norma de la industria de tarjeta de pago para los riesgos detectados de mayor a menor criticidad.

Si bien este plan es desarrollado de forma genérica para cualquier entidad nacional, a continuación se presenta un formulario (Ver Tabla 25), para que cualquier institución financiera logre plasmar su situación actual, es decir, si está cumpliendo o no con la política, en caso de ser negativo se debe a acordar con las unidades involucradas la fecha para la recuperación, y cuáles son las acciones que van en concordancia con las descritas en las políticas desarrolladas.

En el chequeo se debe plasmar:

- **Estado de Cumplimiento:** para cada política se plasmará si el banco cumple o no con la misma en su totalidad.

- **Unidades responsables:** se debe plasmar cual o cuales unidades o personas serán las responsables de que la política sea cumplida en el tiempo establecido.

- **Fecha para la Recuperación:** se debe establecer una fecha clara y realista del tiempo planificado para que la política sea implementada**.**

- **Acciones:** se detallan las acciones a ser realizadas.

Tabla 25. Formulario de Cumplimiento

Descripción de la Política de la Norma de la Industria de Tarjeta de Pago	**Estado de Cumplimiento**	**Unidades Responsable**	**Acciones**	**Fecha para la Recuperación**
Política de mecanismos de cifrado, truncamiento, ocultamiento o refundición de data sensible	□ Si □ No			
Política de procesos de comunicación	□ Si □ No			
Política de definición de roles y responsabilidades	□ Si □ No			
Política de registro de acceso a información sensible	□ Si □ No			
Política protección claves criptográficas	□ Si □ No			
Política pruebas vulnerabilidades a la red	□ Si □ No			
Política pruebas penetración	□ Si □ No			
Política codificación de la información sensible a través de redes públicas.	□ Si □ No			
Políticas de seguridad física	□ Si □ No			
Política pruebas dispositivos inalámbricos en uso	□ Si □ No			
Política de antivirus	□ Si □ No			
Política de cortafuegos	□ Si □ No			
Política identificación de los sistemas	□ Si □ No			
Política división lógica	□ Si □ No			
Política de no uso de contraseñas predeterminadas	□ Si □ No			
Política de parches de seguridad	□ Si □ No			
Política desarrollo aplicativos propios	□ Si □ No			
Política de no uso de credenciales genéricas	□ Si □ No			

6.20. Procesos de implementación de la norma PCI

A continuación se presenta el proceso para la implementación y cumplimiento de la norma PCI:

Se aplica el formulario de chequeo y se determinan las acciones, responsables, y fechas de cumplimiento. Adicionalmente, se fija una fecha de chequeo o revisión en donde las unidades involucradas acuerden que se lograría la aplicación en su totalidad de las políticas.

En ese instante existen dos posibles escenarios:

- Se desarrollaron y aplicaron todas las políticas anteriormente descritas. En ese caso, el banco puede optar a que el estatus sea avalado por PCI. Este proceso consiste en que se realice la evaluación por un consultor externo que es certificado por la Industria de Tarjetas de Pago. Es posible que el banco conozca su estatus de cumplimiento, más no certificado para este caso es necesario que sea realizado por alguien externo.

- No se cumplieron las fechas programadas para el cumplimiento de las políticas, en ese caso se procede a aplicar el formulario de chequeo, se establecen nuevamente las acciones, responsables, fechas de cumplimiento y próximo punto de chequeo.

6.21. Elaboración del plan para Implementación de la Norma de la Industria de Tarjetas de Pago

La implantación de la norma de la industria de tarjetas de pago puede convertirse en una ardua tarea. Definir el ámbito de la implantación, así como

el tiempo y esfuerzos requeridos, puede ayudar a las entidades bancarias a diseñar un proceso de tecnología de información de conformidad más efectivo.

En función del tamaño de la organización, la naturaleza de sus actividades y la madurez de sus procesos, la implantación de la norma puede implicar una inversión considerable de recursos que requiere del compromiso de la alta gerencia.

Adicionalmente, y debido al énfasis de la norma en la seguridad de los datos asociados a tarjetas de crédito, en muchas ocasiones se percibe el estándar únicamente dentro del dominio de la tecnología y recomiendan, con frecuencia, a los departamentos de TI cumplir con los requisitos del estándar desconociendo la cantidad de tiempo y recursos que se requieren para lograr la conformidad. Con objeto de garantizar la aceptación de la gerencia y el éxito, es vital realizar unos análisis iniciales y una planificación.

Dado que las diferentes unidades de las entidades bancarias están en la mejor posición para aportar valor a los procesos de tecnología de información de la organización, pueden ayudar a los departamentos de TI a preparar los pilares de una estrategia eficiente y efectiva de implantación de la norma PCI durante la fase de planificación inicial. Esto ayudará a las compañías a garantizar que sus procesos estén mejor alineados con los requisitos del estándar y asegurar la conformidad a largo plazo.

Implantar PCI puede llevar tiempo y consumir recursos no previstos, especialmente si las organizaciones no disponen de un plan de acción para implantación al inicio del proceso de conformidad. Con objeto de intensificar los esfuerzos en la conformidad es necesario identificar sus objetivos principales de negocio y el ámbito para la implantación.

Se debe trabajar en definir los niveles de madurez de conformidad actuales y analizar el retorno de inversión (ROI) del proceso. Estos pasos pueden ser realizados por un equipo formado por miembros los miembros que se hayan designado para la implementación del estándar.

Con base al diagnóstico realizado, a continuación aspectos a ser considerados:

Identificación de los objetivos de negocio

Los planes para la adopción de PCI deben ser respaldados por un análisis específico de negocio que comprende la enumeración de los objetivos principales de negocio y la garantía de lograr el consenso entre los participantes más relevantes de la compañía. Los objetivos de negocio pueden derivarse de la misión de la compañía, el plan estratégico y objetivos TI actuales, y pueden incluir:

- La garantía de la gestión eficaz del riesgo, que identifique los activos de información y efectúe evaluaciones precisas del riesgo.

- La preservación de las ventajas competitivas de la compañía, si la industria en su conjunto hace uso de información sensible para los negocios.

- La preservación de la reputación y buen nombre del banco entre los líderes de la industria.

- El aporte de confianza que se proporciona a clientes y socios, concerniente al compromiso de la organización para la protección de los datos.

- El aumento de ingresos de la compañía, beneficio y ahorro en las áreas donde los controles de protección resulten efectivos.

- También se debe enfatizar la conformidad con las obligaciones contractuales con las industrias de tarjetas de pago (Visa, Master Card, American Express, Discover y JCB) lo cual podría considerarse otro objetivo de negocio clave.

Determinar los niveles de madurez

Cuando se realiza la evaluación de madurez a través del instrumento, se debe determinar si el equipo de implantación está respondiendo a las interrogantes en conocimiento de:

Procesos de negocio y flujos de información claramente definidos y documentados

Las unidades involucradas deben estar en conocimiento de los procesos del negocio y de los flujos de información existentes en la entidad bancaria, de lo contrario, no se posee la información clara para responder el instrumento de manera de determinar el punto de partida para la implementación de la norma.

Inventario de activos de información

Todos los activos que puedan repercutir en la seguridad de la organización deben estar incluidos en un inventario. Los activos habitualmente incluyen software, hardware, documentos, informes, bases de datos, aplicaciones y sus propietarios.

Debe mantenerse un inventario estructurado que incluya activos particulares o grupos de activos disponibles, su ubicación, uso y propietario. El inventario debe ser actualizado regularmente para garantizar que se utiliza información precisa para la conformidad de implementación de la norma.

Clasificación de los activos de información

Los activos de información deben ser clasificados en función de su importancia desde el punto de vista de la organización y nivel de impacto, y si su confidencialidad, disponibilidad e integridad pudieran estar comprometidas.

Análisis del retorno de inversión

Realizar un análisis de los tiempos y costos estimados para la implantación de las brechas detectadas, impulsa la implementación de las políticas que no se encuentran en cumplimiento. Por otro lado, es importante mencionar que cuanto más tiempo se espere para obtener la certificación, mayor es esfuerzo del personal interno, esto se debe a que la implementación llega a ser inclusive más crítica cuando es conducida por las necesidades del mercado o por la presión de la Industria de Tarjetas de Pago.

Las actividades anteriormente descritas son sumamente importantes tomar en consideración en el momento que las entidades bancarias venezolanas deciden implementar la norma, actualmente la misma no es obligatoria, no obstante, se deben tomar las previsiones correspondientes para que al momento que lo sea, la implementación sea aún más compleja debido a los costos y el tiempo.

CAPITULO VII

EVALUACIÓN DEL PROYECTO

En el presente Trabajo Especial de Grado, se definieron cinco (5) objetivos específicos para que en conjunto se cumpliese el objetivo general de diseño de un plan para la implementación de la norma de la Industria de Tarjetas de Pago en entidades bancarias venezolanas.

Cada uno fue cumplido en 100% mediante la ejecución de las actividades originalmente planteadas.

El primer objetivo consistió en:

- **Identificar y describir los requisitos de la norma de la Industria de Tarjetas de Pago.**

Este objetivo fue cumplido en un cien por ciento, la identificación y descripción de los requisitos de la norma de la industria de tarjetas de tarjeta de pago se realizó durante la fase de levantamiento de información a través de fuentes bibliográficas.

La identificación y descripción de los requisitos fue crucial para el diseño y realización del instrumento utilizado para la recolección de los datos, ya que el cuestionario se desarrolló con el objetivo de identificar y detectar los riesgos presentes en la banca venezolana relacionados con las brechas de seguridad de datos en tarjetas de crédito.

El segundo objetivo consistió en:

- **Priorizar los riesgos que pueden generarse ante las brechas de seguridad, de acuerdo a la clasificación de los requisitos de la norma de la Industria de Tarjetas de Pago.**

Al ser determinados los riesgos a través de la identificación y descripción de la norma explicada en el objetivo anterior, se procedió a priorizar los riesgos, este proceso consistió en la recolección de los datos obtenidos a través de especialistas y gerentes de las diferentes entidades bancarias a las cuales se le aplicó el instrumento que se diseño para tal fin.

Esta información recabada consistió en determinar si en la entidad bancaria habían brechas de seguridad asociadas a tarjetas de crédito, éstas fueron plasmadas en dieciocho interrogantes; en caso de ser afirmativo se debía indicar la ocurrencia del evento en el último año en la organización, así como el impacto que se había sufrido por exposición de data sensible.

Las respuestas de cada entrevistado se analizaron cualitativamente a través de la aplicación de una matriz de probabilidad e impacto, para cada riesgo se obtuvo el promedio de los resultados objetivos, lo que originó una ponderación de mayor a menor criticidad.

Por lo anteriormente expuesto, los riesgos fueron priorizados satisfactoriamente.

El tercer objetivo consistió en:

- **Definir estrategias para el control y mitigación de riesgos asociados por el no cumplimiento de los requerimientos de la Industria de Tarjetas de Pago.**

Al ser priorizados los riesgos tal como se explicó en el objetivo anterior, se cuenta con un esquema para definir estrategias de control y mitigación de riesgos, atendiendo a los que cuentan con mayor incidencia en la banca a aquellos menores.

Para cada uno de los riesgos detectados, se desarrollaron políticas para dar respuesta a los mismos y así ser mitigados.

Las políticas estuvieron conformadas por actividades relacionadas tanto por cambios en la arquitectura de la institución bancaria, así como en los procesos de negocio, por lo que se ahonda en herramientas de suma importancia no solo para el cumplimiento de la norma, sino para el fortalecimiento de la seguridad en la banca.

Adicionalmente, se realizó un formulario de mucha utilidad para elaborar un plan de control de cumplimiento, el mismo consistió en plasmar para cada política en caso de que existiesen puntos de mejora a realizar, cuales son las personas responsables, fecha estimada para el cumplimiento y acciones a tomar.

El proceso para el cumplimiento de la norma PCI, consistió en que la entidad bancaria aplica el formulario y en caso que haya políticas por establecer, se fija una fecha de revisión con las unidades correspondientes para tener un punto de chequeo y determinar si se corrigieron las brechas detectadas.

Si en ese punto de chequeo todas las políticas se implementaron satisfactoriamente, la entidad bancaria está plenamente preparada para que un consultor externo certifique que cumple PCI, en caso de no ser así, se deberán establecer nuevamente los puntos de mejora, responsables y acciones.

El cuarto objetivo consistió en:

- **Caracterizar los elementos teóricos, técnicos, conclusiones y lecciones aprendidas.**

Para el desarrollo del Trabajo Especial de Grado hubo dos vertientes primordiales:

Investigación Teórica: para el desarrollo del Trabajo Especial de Grado fueron imprescindibles las fuentes bibliográficas para la culminación exitosa el mismo, está conformado por el planteamiento del problema, justificación, alcance, objetivos generales y específicos que fueron explicados en el capítulo I, fundamentos teóricos y antecedentes de la investigación que se evidencian en el capítulo II, el marco metodológico que se detalla en el presente capítulo y la ventana de mercado que se ahonda en el capítulo IV.

Investigación de Campo: estuvo conformada por la determinación del universo, población y posterior muestra a ser estudiada. Al contar con la delimitación objeto del estudio, se procedió a diseñar y validar el instrumento, se realizó la recolección y análisis de los datos para el desarrollo del plan.

Posterior al análisis de los resultados, en el desarrollo del plan se caracterizaron elementos teóricos y técnicos de la norma de la industria de tarjeta de pago en el plan de respuesta a los riesgos desarrollada a través de políticas.

En el capítulo próximo se ahondarán en las conclusiones y recomendaciones del presente TEG; como lecciones aprendidas durante el desarrollo tenemos:

- La implementación de la norma no solo corresponde a los departamentos de TI, la seguridad de la información no solo atañe a las unidades de tecnología de información, sino que existen cambios organizacionales y gestión de recursos humanos, por tanto es un esfuerzo de toda la entidad bancaria para el éxito.

- La implementación de la norma no dura unas pocas semanas, es posible que las políticas que haya de implementar para el cumplimiento lleve tiempo porque se deben realizar una serie de cambios tanto a nivel de tecnología como en la cultura organizacional.

- La implementación de la norma no culmina con el análisis de la situación actual de la entidad bancaria y la implementación de las políticas, es de suma importancia una revisión constante, así como de mantenerse al tanto de las tendencias fraudulentas, así como la tecnología avanza a pasos agigantados las actividades fraudulentas también.

- Al ser aplicado el instrumento en las diferentes entidades bancarias a nivel nacional, uno de los riesgos detectados con mayor criticidad estuvo relacionado con los procesos de comunicación, esto lleva como lección aprendida que este factor es uno de los más delicados y en ocasiones no se le da la importancia que tiene. Deben ser desarrollados y fortalecidos los canales a los empleados y fortalecer la identificación con la organización.

- **Elaborar un plan para la implementación de la norma de la industria de tarjetas de pago.**

La fase del desarrollo del plan estuvo conformada por tres fases fundamentales, la identificación, priorización de los riesgos y la definición de estrategias para el control y mitigación de riesgos asociados por el no cumplimiento de los requerimientos de la Industria de Tarjetas de Pago.

La fases mencionadas fueron descritas en los primeros tres objetivos, adicionalmente el plan se conformó por las actividades que deben ser aplicadas en la fase inicial para una exitosa implementación de la norma.

La implantación de la norma PCI, requiere una cuidadosa reflexión, planificación y coordinación que asegure una adaptación cómoda. La decisión acerca de cuando implementar el plan, puede verse influida por un número de factores que incluyen los distintos objetivos de negocio, los niveles actuales de madurez TI y esfuerzos para la conformidad, aceptación y concienciación de los usuarios, necesidades de los clientes u obligaciones contractuales y la capacidad de la organización de adaptación al cambio y adopción de los procesos internos.

Por lo anteriormente expuesto se cumplieron exitosamente todos los objetivos planteados en el Trabajo Especial de Grado.

CAPITULO VIII

CONCLUSIONES Y RECOMENDACIONES

7.1. Conclusiones

El presente Trabajo Especial de Grado se centró en el diseño de un plan para la implementación de la norma de la Industria de Tarjetas de Pago, como se expuso en la importancia para la investigación, resulta vital que las entidades bancarias venezolanas tomen acciones tempranas para cumplir las políticas descritas en la norma, no solo porque la misma próximamente será de carácter obligatorio sino que permite el fortalecimiento de la gestión de riesgos para la organización.

Las fuentes bibliográficas constituyeron un aporte de suma importancia, ya que a través de las mismas se estudiaron y desarrollaron herramientas relacionadas a la norma de la industria de tarjetas de pago y la gestión de riesgos del PMI, puntos focales del Trabajo Especial de Grado.

El instrumento de recolección de datos constituyó un pilar fundamental, ya que a través del mismo se obtuvieron las tendencias de la banca nacional en cuanto a los riesgos asociados a la seguridad de los datos de tarjetas de crédito, esto fue posible a través del análisis cualitativo que constituyó una herramienta de la gestión de riesgos que permitió la priorización a través de matrices de probabilidad de ocurrencia y escala de impacto.

Por lo anteriormente expuesto, el desarrollo estuvo enmarcado en las políticas en donde los bancos están presentando mayor debilidad a menor debilidad.

Por otro lado, se desarrolló un formulario de cumplimiento de manera que el banco realice una autoevaluación para plasmar su situación actual y así pueda realizar una planificación que involucra el personal designado, fecha de recuperación y acciones a ser realizadas.

Por otro lado, las políticas fueron desarrolladas en linealidad con los requisitos expuestos en la norma de la industria de tarjetas de pago, lo que le facilitará al lector establecer una secuencia de actividades para el cumplimiento de todas y nada una de las políticas.

En conclusión, el diseño del plan para la implementación de la norma de la industria de tarjetas de pago resulta una herramienta de mucha utilidad para los especialistas y gerentes de las entidades bancarias, esto se debe a que se detalla concienzudamente las actividades que deben ser realizadas para que el objetivo final se cumpla a cabalidad, el cumplimiento de la norma.

7.2. Recomendaciones

Las recomendaciones derivadas del proyecto son:

- El plan para la implementación de la norma de la industria de tarjetas de pago debe darse a conocer, tanto entre las diferentes entidades bancarias como a los proveedores de tecnología de información para que incluyan las buenas prácticas derivadas entre sus políticas de ejecución.

- Debido a que la información que debe ser suministrada a través del instrumento resulta sumamente crítica y de carácter confidencial, mecanismos para realizar un análisis cuantitativo enfocado en el

impacto financiero para la organización, complementaría de forma significativa el estudio realizado.

- Es importante destacar que la implementación del plan conlleva no solo un esfuerzo de personal calificado de las entidades bancarias, sino que dependiendo del escenario deban contemplarse inversiones económicas significativas.

- Se sugiere que para posteriores investigaciones pueda incluirse la gestión de costos y de tiempo para que el plan tenga un mayor nivel de detalle en cuanto a esas áreas de conocimiento.

REFERENCIAS BIBLIOGRÁFICAS

Cavalieri. I. (2007). Metodología para la gestión de riesgos de los proyectos de la empresa de ingeniería TEENS CONSULTORES*.* Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Fermín. N. (2010). Desarrollo de un plan de gestión de proyecto para la implementación del sistema de gestión de seguridad de la información*.* Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Palacios. J. (2008)*.* Evaluación del desarrollo de los fundamentos teóricos de seguridad de la información en la banca comercial y universal de Venezuela*.* Trabajo Especial de Grado realizado para optar por el Título de Magíster en Gerencia de Sistemas de Información no publicado Universidad Católica Andrés Bello, Caracas.

Pellegrino. A. (2004). Efectos del fraude electrónico mediante tarjetas de débito y crédito en la banca venezolana, período comprendido 2003, primer trimestre 2004*.* Trabajo Especial de Grado para optar por el Título de Especialista en Instituciones Financieras. Mención Análisis y Gestión de las Instituciones Financieras no publicado. Universidad Católica Andrés Bello, Caracas.

Pérez. H. (2007). Los fraudes con tarjetas de crédito y sus efectos financieros en el BBVA Banco Provincial. Trabajo Especial de Grado para optar por el Título de Especialista en Instituciones Financieras. Mención Análisis y

Gestión de las Instituciones Financieras no publicado. Universidad Católica Andrés Bello, Caracas.

Rivas. A. (2010). Diseño de un Plan para la Implementación de Proyectos de Servicios de Tecnología De Información Caso: Virtualización De Almacenamiento De Datos. Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Rolingsón. J. (2004). Propuesta metodológica para la implantación y mejora de la gestión de riesgos en organizaciones de proyectos. Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Ordoñez. V. (2007). Diseño De Un Sistema De Gestión Por Procesos Para Sincrudos De Oriente Sincor, C. A. Trabajo Especial de Grado realizado para optar por el Título de Especialista en Gerencia de Proyectos no publicado Universidad Católica Andrés Bello, Caracas.

Fuentes Impresas:

Arias, F. (2006). *El Proyecto de investigación*. (5ta ed.). Caracas: Episteme.

Hernández, R.; Fernández, C. y Baptista, L. (2003). *Metodología de la Investigación*. (2da ed.). México: Mc Graw-Hill.

Ley Especial contra Delitos Informáticos. (2001). *Gaceta Oficial de la República Bolivariana de Venezuela*, 37313, Octubre, 2001.

Ley General de Bancos y otras Instituciones Financieras. (2000). *Gaceta Oficial de la República Bolivariana de Venezuela*, 1526, Noviembre, 2001.

Ley Orgánica de Ciencia, Tecnología e Innovación. (2005). *Gaceta Oficial de la República Bolivariana de Venezuela*, 37291, Julio, 2005.

Ley Sobre Mensajes de Datos y Firmas Electrónicas. *Gaceta Oficial de la República Bolivariana de Venezuela*, 1181, Enero, 2001.

Maza, D. (1995). *El Sistema Financiero Deseable*. (1ra ed.). Barquisimeto: Instituto de Estudios Jurídicos del Estado Lara.

Muci, G. y Martín, R. (2004). *Regulación Bancaria*. (1ra ed.). Caracas: Publicaciones UCAB.

Project Management Institute. (2008). *Guía de los Fundamentos de la Dirección de Proyectos*. (4ta ed). Estados Unidos de Norteamérica: PMI.

Valarino, E.; Yáber, G. y Cemborain, M. (2010). *Metodología de la Investigación Paso a Paso*. (1ra ed.). México: Trillas.

Fuentes Electrónicas:

IQ Seguridad en Medios de Pago. (2009). *PCI DSS*. Recuperado en Junio 22, 2011, de http://www.iqcol.com/services-pci.html

Colegio de Ingenieros de Venezuela. (2011). *Código de Ética Profesional*. Recuperado en Febrero 20, 2011, de http://www.fimp-civ.org.ve/index.asp?spg_id=47

Medina, A.; Flores, M. y Ojeda, J. (2009). *Seguridad de datos en tecnologías de información y comunicación en la banca venezolana. Marco jurídico y político*. Recuperado en Noviembre 10, 2010, de http://www.revistaespacios.com/a09v30n03/09300362.html

Project Management Institute. (2011). *Código de Ética y Conducta Profesional*. Recuperado en Febrero 20, 2011, de http://www.pmi.org/About-Us/Ethics/~/media/PDF/Ethics/ap_pmicodeofethics_SPA-Final.ashx

Superintendencia de Bancos y Otras Instituciones Financieras. (2010). *Resolución Número 64110*. Recuperado en Junio 25, 2011, de http://www.sudeban.gob.ve/uploads/UI/HW/UIHWw8oCrYguPdjhEq9BAQ/27-2-RES-641-10.pdf

Superintendencia de las Instituciones del Sector Bancario. (2010). *Directorio Bancario*. Recuperado en Febrero 25, 2011, de http://sudeban.gob.ve/webgui/pagina1

Tribunal Supremo de Justicia. (2008). *Gaceta Oficial N° 39.021.* Recuperado en Febrero 25, 2011, de http://www.tsj.gov.ve/gaceta/septiembre/220908/220908-39021-32.html

GLOSARIO DE TÉRMINOS, ACRÓNIMOS Y SIGLAS

Acrónimos y Siglas:

PCI: Industria de Tarjetas de Pago (Payment Card Industry).

PCI SSC: Consejo para el Estándar de Seguridad en la Industria de las Tarjetas de Pago (Payment Card Industry Security Standards Council).

PMI: Project Management Institute.

SUDEBAN: Superintendencia de las Instituciones del Sector Bancario.

TEG: Trabajo Especial de Grado.

TI: Tecnología de Información.

Glosario de Términos:

AES: método de cifrado por bloque.

Cortafuego: hardware, software, o ambos, que se utilizan para proteger los recursos de una red de los intrusos procedentes de otras redes.

DMZ: zona desmilitarizada es una red que se agrega entre una red privada y una red pública para proporcionar una capa de seguridad adicional.

DNS: domain Name System o Domain Name Server. Sistema que guarda información asociada con nombres de dominio en una base de datos distribuida en redes como Internet.

GSM: estándar para teléfonos móviles.

IDS/IPS: intrusion detection system/ intrusion prevention system, sistema de detección y prevención de intrusiones, utilizado para identificar y alertar sobre intentos de intrusión en un sistema o una red.

PAN: número de cuenta primario, es el número de la tarjeta de pago (crédito o débito) que identifica al emisor y la cuenta del tarjetahabiente. También se llama Número de Cuenta.

PIN: número de Identificación Personal.

SSL: estándar establecido en la industria que encripta el canal entre un navegador y un servidor de Web para asegurar la privacidad y confiabilidad de los datos transmitidos a través de éste.

APÉNDICE A - INSTRUMENTO

Instrumento para identificar, analizar cualitativamente y cuantitativamente riesgos en la seguridad de la información en entidades bancarias venezolanas

El objetivo del presente instrumento es de recopilar datos de riesgos producidos por brechas de seguridad de la información en entidades bancarias venezolanas, así como evaluar el impacto producido por la exposición de datos sensibles asociados a transacciones con tarjetas de crédito y la ocurrencia en la organización.

La información del encuestado y la entidad bancaria será estrictamente confidencial y solo serán usados los resultados con objetivos académicos para identificar, analizar cualitativamente los riesgos por cada pregunta, impacto y ocurrencia de forma global.

Una vez completado este cuestionario remítalo de manera electrónica a: Erika Lazzarin, erikalaz@gmail.com

La escala para el impacto producido para su organización sería:

- **Insignificante:** riesgo mínimo de exposición de información sensible.
- **Menor:** riesgo bajo de exposición de información sensible.
- **Moderado:** riesgo medio de exposición de información sensible.
- **Importante:** riesgo alto de exposición de información sensible.
- **Extremo:** riesgo eminente de exposición de información sensible

1. **¿En su organización se tienen identificados todos los sistemas que almacenan, transmitan o procesan información relacionada con tarjetas de crédito?**

   No ( )
   Si ( )

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

2. **¿En su organización existe una división lógica de los componentes asociados al almacenamiento, transmisión o procesamiento de la información sensible asociada a las tarjetas de crédito con el resto de la plataforma?**

   No ( )
   Si ( )

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

3. ¿Usted considera que existe ausencia o debilidad en la configuración o actualización del cortafuego que protege áreas sensibles de su organización?

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

4. ¿Usted considera que en su organización se hace uso de contraseñas estándares fijadas por los proveedores de componentes de hardware o software, es decir, no se realizan cambios luego de adquirir el componente?

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

5. ¿En su organización se realizan mecanismos de cifrado, truncamiento, ocultamiento y refundición de la data sensible asociada a las tarjetas de crédito?

No ( )
Si ( )

En caso de ser afirmativo ¿Podría mencionar los mecanismos más relevantes?

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

6. ¿Considera usted que en su organización se protegen adecuadamente las claves criptográficas utilizadas para el cifrado de datos sensibles?

No ( )
Si ( )

En caso de ser afirmativo, ¿Podría mencionar los mecanismos más relevantes?

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

7. **¿Considera usted que existe ausencia o debilidad en la codificación de data sensible asociada a las tarjetas de crédito al momento de transmisión a través de redes públicas?**

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

8. **¿Considera usted que existen debilidades en la protección de su data sensible debido a la falta de antivirus o de la actualización oportuna de los mismos?**

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.

Comentarios Adicionales:

---

9. **¿En su organización cuentan con políticas de actualizaciones de parches de seguridad?**

No ( )
Si ( )

En caso de ser afirmativo, indicar: ¿Con qué regularidad se actualizan los parches críticos de seguridad?

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

10. ¿En el caso que la organización desarrolle sus propias aplicaciones, se aplican mecanismos que mitiguen las brechas de seguridad producidas por vulnerabilidades que no fueron detectadas antes de pasar al ambiente de producción?

No ( )
Si ( )
No Aplica ( )

En caso de ser afirmativo, ¿Podría mencionar los mecanismos más relevantes?

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

11. ¿Considera que en su organización existe una detallada definición de permisos de acuerdo a roles y responsabilidades a la data sensible asociada a las tarjetas de crédito?

No ( )
Si ( )

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

12. ¿En su organización se utilizan credenciales genéricas, es decir, se utiliza un mismo usuario para un grupo de personas?

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?:
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

13. ¿En su organización cuentan con controles de seguridad física, tales como: cámaras de video vigilancia, control de acceso, donde se proteja el ingreso de personas no autorizadas a los componentes en donde se encuentran almacenados los datos sensibles de la organización?

No ( )
Si ( )

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?:
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

14. ¿En su organización cuentan con herramientas que tengan la capacidad de detectar y registrar cualquier acceso a información sensible de los tarjetahabientes?

No ( )
Si ( )

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

15. ¿En la organización se realizan pruebas para identificar los todos los dispositivos inalámbricos en uso?

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente la frecuencia anual:

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

16. ¿En su organización se realizan análisis internos y externos de las vulnerabilidades de la red?

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente la frecuencia anual:

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

17. ¿En su organización se realizan pruebas de penetración internas y externas a la infraestructura o aplicaciones?

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente la frecuencia anual:

En caso de ser negativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

---

18. ¿Considera que existe debilidad en los procesos de comunicación y/o entrenamiento a los empleados acerca de la confidencialidad de los datos y su responsabilidad para la protección de los mismos?

No ( )
Si ( )

En caso de ser afirmativo, indicar adicionalmente:

¿Cómo calificaría el impacto para la Organización?
( ) Insignificante
( ) Menor
( ) Moderado
( ) Importante
( ) Extremo

¿Con qué frecuencia sucede este evento en la organización?
( ) Nunca
( ) Una vez en el último año.
( ) Dos a tres veces en el último año.
( ) Cuatro a cinco veces en el último año.
( ) Seis a más veces en el último año.

Comentarios Adicionales:

A continuación por favor podría comentar de acuerdo a su experiencia, ¿Cuál es la tendencia y de qué tipo son los fraudes a los que la banca venezolana se ha visto enfrentada?

Muchas gracias por su colaboración.