VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSTGRADOS

MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: DISEÑO DE UN ESQUEMA METODOLÓGICO PARA EVALUAR EL USO Y EJECUCIÓN DE LA NORMATIVA PCI-DSS EN UNA ENTIDAD BANCARIA

AUTOR: CARANQUI ROMERO, KLEBER GIOVANNY

DIRECTOR: CHIRIBOGA, GABRIEL

SANGOLQUÍ

2017

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**DISEÑO DE UN ESQUEMA METODOLÓGICO PARA EVALUAR EL USO Y EJECUCIÓN DE LA NORMATIVA PCI-DSS EN UNA ENTIDAD BANCARIA**" realizado por el señor **KLEBER GIOVANNY CARANQUI ROMERO**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor **KLEBER GIOVANNY CARANQUI ROMERO** para que lo sustente públicamente.

Quito, 21 de noviembre del 2017

RUBEN DARIO ARROYO CHANGO
DIRECTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORÍA DE RESPONSABILIDAD

Yo, **KLEBER GIOVANNY CARANQUI ROMERO**, con cédula de identidad N° 1711533198, declaro que este trabajo de titulación **"DISEÑO DE UN ESQUEMA METODOLÓGICO PARA EVALUAR EL USO Y EJECUCIÓN DE LA NORMATIVA PCI-DSS EN UNA ENTIDAD BANCARIA"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Quito, 21 de noviembre del 2017

KLEBER GIOVANNY CARANQUI ROMERO
C.C 1711533198

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORIZACIÓN

Yo, **KLEBER GIOVANNY CARANQUI ROMERO**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **"DISEÑO DE UN ESQUEMA METODOLÓGICO PARA EVALUAR EL USO Y EJECUCIÓN DE LA NORMATIVA PCI-DSS EN UNA ENTIDAD BANCARIA"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Quito, 21 de noviembre del 2017

KLEBER GIOVANNY CARANQUI ROMERO
C.C 1711533198

DEDICATORIA

Este trabajo va dedicado en especial a Dios por todas las bendiciones y pruebas, que ha puesto en mi vida, para hacerme fuerte y por los cuales he podido salir adelante.

A mi familia quienes con su amor, apoyo incondicional y paciencia han sido mi fortaleza y guía para no renunciar y seguir adelante en momentos de dificultad.

Y, a todas aquellas personas que estuvieron pendientes y que con sus palabras de aliento siempre me motivaron a cumplir con este objetivo, demostrando verdadera amistad y cariño.

Ing. Kleber Giovanny Caranqui Romero

AGRADECIMIENTO

Doy gracias a todas las personas que colaboraron de manera directa o indirecta en la realización de este trabajo, quienes han sido mi soporte y compañía durante todo el periodo de estudio, para poder llegar a la meta.

Un agradecimiento también para mis maestros y a la Universidad por el apoyo, respeto y el profesionalismo con que se trata a sus estudiantes

¡Agradecimientos a todos!
Ing. Kleber Giovanny Caranqui Romero

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICES DE TABLAS

RESUMEN

Visa, MasterCard, American Express, y otras asociaciones de tarjetas han definido la normalización de seguridad de datos Payment Card Industry Data Security Standard (PCI DSS) para proteger la información de los usuarios y de esta manera mitigar de alguna manera el riesgo de ataques bajo los diferentes escenarios utilizados por los delincuentes para realizar fraudes tecnológicos. El presente trabajo se plantea frente a las enormes pérdidas económicas producidas como consecuencia del creciente fraude por robo de datos de tarjetas de crédito a nivel mundial y a la obligación de todas aquellas empresas que procesan, almacenan o transmiten datos de tarjetas de crédito o débito de fortalecer los esquemas de seguridad que permitan garantizar la protección adecuada de la información mediante el diseño de modelos que permitan evaluar periódicamente el adecuado cumplimiento y aplicación de los estándares de control que exige la Norma PCI-DSS. Otros factores que incide en la prioridad de generar evaluaciones esta la necesidad de mantener la buena imagen y confianza con el clientes, así como también cumplir con la exigencia de las franquicia y evitar la aplicación de sanciones en el caso de no contar con la certificación PCI-DSS y sus respectivos esquemas de control.

PALABRAS CLAVES

- **PCI-DSS**
- **FRAUDE TECNOLÓGICO**
- **CUMPLIMIENTO DE NORMATIVA**
- **ESTÁNDAR DE CONTROL**

ABSTRACT

Visa, MasterCard, American Express and other card associations have defined data security standards Payment Card Industry Data Security Standard (PCI DSS) to protect user information and thus somehow mitigate the risk of attacks on the different scenarios used by criminals to make technological fraud. This thesis project arises against the enormous economic losses as a result of growing fraud for stealing credit card data globally and the obligation of all companies that process, store or transmit credit card data or debit to strengthen the security structures to ensure the adequate protection of information by designing models to periodically evaluate the implementation and application of appropriate control standards required by the PCI-DSS standard. Other factors that affects the priority of generating evaluations is the need to maintain the good image and confidence with customers and also meet the requirement of the franchise and avoid sanctions in the case of not having the PCI certification -DSS and respective control schemes.

KEYWORDS

- **PCI-DSS**
- **TECHNOLOGICAL FRAUD**
- **SANCTIONS**
- **PROTECTION OF INFORMATION**

CAPÍTULO I

INTRODUCCIÓN

En la actualidad la globalización de servicios bancarios y el crecimiento del delito informático en los canales electrónicos de la banca ha provocado la necesidad de implementar nuevos esquemas de seguridad en todas las organizaciones que procesan, almacenan o transmiten información de titulares de tarjetas de pago, mediante el Estándar de seguridad en la industria de tarjetas de pago por sus siglas en inglés (PCI DSS).

En base a los análisis de seguridades que realizan las instituciones bancarias, es posible conocer el estado actual de los niveles de seguridad con los que cuentan varias instituciones a nivel de Infraestructura, Redes, procesos de control, normas y procedimientos de seguridad, ente otros, sin embargo se requiere evaluar los requerimientos de seguridad para el manejo de información exigidas por la norma y adecuar su implementación en las instituciones buscando minimizar el impacto que puede provocar estos cambios, así también es posible evidenciar la necesidad de fortalecer las políticas de seguridad actuales con el propósito de mitigar el riesgo de acciones ilícitas internas o externas a la institución.

Entre los controles que normalmente se pueden implementar para mitigar posibles riesgos en los procesos de Tecnología tenemos los siguientes: Redes con zonas desmilitarizadas, Monitoreo y reglas para administración del firewall, Manejo de listas blancas y negras, Administración de consolas antivirus y antimalware, control de accesos seguros a sitios Web, Esquemas para manejo de llaves criptográficas entre otros.

Estas prácticas han permitido brindar niveles de seguridad aceptables y controlar las incursiones de la delincuencia tecnológica disminuyendo los

fraudes a los clientes. (Priscila Balcazar. CISA, 2010; David Acosta CISSP, 2015; PayPal, 2015; nakedsecurity, 2015; PCI-DSS, 2015; MasterCard, 2015; Discover, 2015)**.**

Aspectos Generales de la Norma PCI-DSS

La especificación de normalización de seguridad de datos Payment Card Industry Data Security Standard (PCI DSS) se ha creado por las principales marcas de tarjetas de crédito con la reciente incorporación de todas las tarjetas internacionales para proteger la información de los usuarios y luchar contra la suplantación y otros fraudes que se producen en Internet.

Visa, MasterCard, American Express, y otras asociaciones de tarjetas han definido un conjunto de obligaciones en relación con la seguridad de la información y que deben ser cumplidas por toda empresa que almacene, procese o transmitan datos de los tarjetahabientes.

La norma exige el cumplimiento de varios requisitos clasificados en 6 grupos cuyo objetivo es ayudar a las organizaciones a proteger de manera proactiva los datos de las cuentas de los clientes y refleja la mayoría de las mejores prácticas para proteger información sensible. La norma incluye requisitos para la administración de la seguridad, políticas, procedimientos, arquitectura de redes, diseño de software y otras medidas de protección críticas.

En base a lo expuesto existe una clara necesidad de generar guías para implementar y evaluar periódicamente la ejecución adecuada de controles de seguridad a los diferentes procesos que pretende normalizar PCI y de esta manera mantener procesos funcionales y basados en la realidad del negocio. (Bento, 2010; welivesecurity, 2015) (searchsecurity.techtarget, 2012; es.pcisecuritystandards.org, 2015).

1.1 JUSTIFICACIÓN E IMPORTANCIA

En la actualidad el crecimiento y cambio constante de la tecnología así como la globalización de los diferentes servicios bancarios ha producido que la delincuencia aproveche la gran oferta de tecnología en el mercado para mantener una constante especialización en su accionar.

Los organismos de control locales y globales así como las franquicias de negocio a nivel mundial frente a este crecimiento continuo de la complejidad de la seguridad de la información han presentado, con el fin de contribuir a elevar las seguridades de las instituciones financieras, una serie de normativas y directrices que obligan a las empresas a robustecer sus procesos y esquemas actuales de trabajo. Uno de las más importantes es el Payment Card Industry Data Security Standard (PCI DSS), que establece 6 categorías para los controles de TI con el fin de garantizarla seguridad y protección de los datos.

El presente proyecto de tesis se plantea frente a la obligación y la responsabilidad de todas aquellas empresas que procesan, almacenan o transmiten datos de tarjetas de crédito o débito de fortalecer los esquemas de seguridad que permitan garantizar la protección adecuada de la información mediante el diseño de modelos que permitan evaluar periódicamente el cumplimiento y ejecución de los estándares de control que exige la Norma PCI-DSS. (ATCA, 2015; Hernández, 2009; apuntesacercadetarjetasdecrditoydbito, 2010; a2secure, 2015; seguridaddeinformacionenlastel.blogspot.com, 2014)

1.2 PLANTEAMIENTO DEL PROBLEMA

Debido a las enormes pérdidas económicas producidas como consecuencia del creciente fraude por robo de datos de tarjetas de crédito a nivel mundial se creó la normativa PCI y la obligación de las instituciones bancarias de cumplirla por tal razón el presente proyecto tiene como propósito fundamental proporcionar un modelo para evaluar los requerimientos PCI de manera periódica y así aportar al mejoramiento continuo de las seguridades y manejo de la información de los clientes de tarjeta de crédito y débito así como también apoyar el fortalecimiento de las políticas para la gestión de seguridades, esta necesidad de contar con modelos de control, tal como se indica anteriormente se da frente al crecimiento del delito informático lo que obliga a robustecer los controles actuales ya que hasta el momento no se veía necesario implementar niveles adicionales de seguridad, otros factores que incide en la prioridad de generar evaluaciones esta la necesidad de mantener la buena imagen y confianza con el clientes, así como también cumplir con la exigencia de las franquicia quienes han informado de una fecha límite de cumplimiento y la aplicación de sanciones en el caso de no contar con la certificación PCI-DSS y sus respectivos esquemas de control. (www.forbes.com.mx, 2015; Martínez, 2015; Ing Mario Ron, 2014; www.eluniverso.com, 2013; www.telegrafo.com.ec, 2013; ecommerce, 2015).

1.3 FORMULACIÓN DEL PROBLEMA

El problema actual se basa en el manejo simple de la información considerada como crítica en una institución financiera permitiendo accesos no adecuado a los datos privados, por lo que es importante contar con modelos de evaluación para conocer el estado actual de los procesos tecnológicos del banco y verificar el cumplimiento de la normativa, otro de los problemas es el conocimiento limitado sobre la participación del área de Auditoría en este proceso, así como también el verdadero alcance de PCI en

el ambiente actual de la organización. Auditoría cumple un papel importante en la permanencia de la certificación, por tal razón se busca elaborar un modelo que permita a este departamento ejecutar revisiones prácticas y concretas sobre los requisitos que propone PCI-DSS y de esta manera evaluar el correcto cumplimiento sin perder el rumbo durante su ejecución. (www.sbs.gob.ec, 2015; www.paymentmedia.com, 2012; www.eluniverso.com, 2013; www.forbes.com.mx, 2015; SOPHOS, 2015).

1.4 OBJETIVO GENERAL

Diseñar una guía que, mediante la ejecución de controles permita evaluar el nivel de implementación de la normativa PCI-DSS en una entidad bancaria y de esta manera contribuir al proceso de certificación, fortalecimiento de los esquemas de seguridad y mantenimiento de la imagen corporativa en el mercado financiero.

1.5 OBJETIVOS ESPECÍFICOS

- Definir el alcance de la revisión a la normativa PCI-DSS (PCI DSS –Payment Card Industry's Data Security Standards) en la entidad bancaria.
- Diseñar un modelo que permita realizar evaluaciones de cumplimiento a los procesos basados en las exigencias de la norma PCI y criterios de COBIT 4.1.
- Levantar información y evaluar en forma preventiva los procesos y áreas que participan en el proceso de certificación.
- Organizar la información y emitir un informe coherente con recomendaciones en base a las evaluaciones realizadas.

CAPÍTULO II

MARCO TEÓRICO

PCI DSS, en su idioma nativo (Inglés): Payment Card Industry Data Security Standard, significa Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.

Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran a estos medios de pago.

En el año 2005 y luego de las enormes pérdidas económicas producidas como consecuencia del creciente robo de datos de tarjetas de crédito y fraudes a nivel mundial, el Concilio de la Industria de Tarjetas de Pago conformado por las marcas más importantes (Visa International, MasterCard Worldwide, American Express, JCB y Discover Financial Services) desarrollo y adopto los estándares PCI DSS (Payment Card Industry Data Security Standards) estándares de Seguridad de Datos de la Industria de las Tarjetas de Pago, y a partir de ese momentos aquellas compañías que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o arriesgan la pérdida de sus permisos para procesar las tarjetas de crédito y débito (Perdida de franquicias), enfrentar auditorías rigurosas o pagos de multas por lo que los Comerciantes y proveedores de servicios de tarjetas de crédito y débito deben validar su cumplimiento al estándar en forma periódica. (www.procard.com.py, 2014; Bancard, 2004)

El proceso de certificación se maneja de acuerdo al siguiente flujo:

Figura 1. Proceso general para certificación en la Normativa PCI DSS 2.0

Fuente: (Avisortech, 2015)

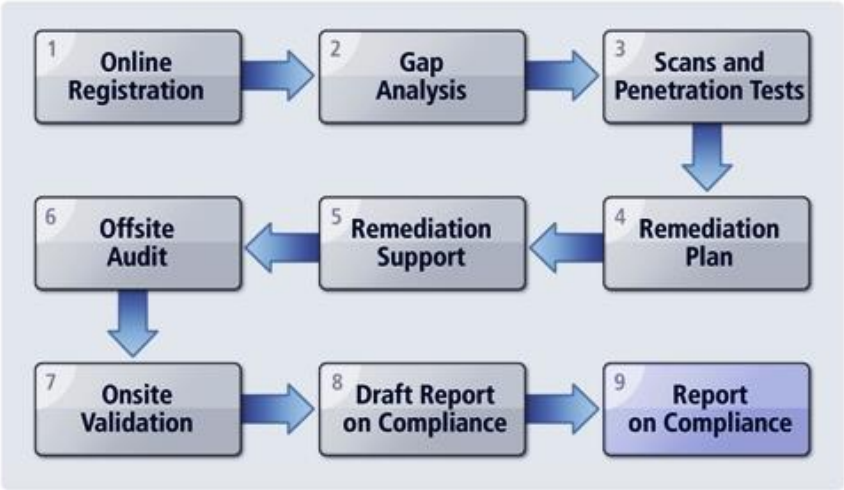


Figura 2. Metodología estándar de Certificación PCI

Fuente: (controlcase, 2015)

Esta validación es realizada por auditores autorizados Qualified Security Assessor (QSAs). Sólo a las compañías que procesan menos de 80,000 transacciones por año se les permite realizar un auto evaluación utilizando

un cuestionario provisto por el Consorcio del PCI. (www.pcisecuritystandards.org, 2014; Torres, 2010; isecauditors, 2015).

2.1 QUÉ ES PCI-DSS

PCI-DSS es un conjunto de prácticas orientadas a las seguridades de red y empresariales que deben ser observados y aplicados con la finalidad de garantizar la seguridad de la información, disminuyendo el riesgo de compromiso de esta información mediante un manejo adecuado de los datos de las tarjetas de pago.

El PCI-DSS es además un acuerdo contractual que describe en detalle cómo deben ser manejados los datos sensibles de las tarjetas de pago. La norma describe claramente lo que debe hacer en forma de “Cumplimiento de Requisitos” y la forma de demostrarlo en forma de “Requerimientos de validación”.

El cumplimiento de PCI DSS permite:

- Mayor seguridad para las compras por internet, al reducir el fraude online
- Impedir el robo y el uso no autorizado de tarjetas de crédito y débito
- Proteger a los consumidores y a los negocios ante actividades fraudulentas
- Garantizar que los comerciantes almacenan, procesan y transmiten los datos de tarjetas de forma segura
- Evitar los daños en la reputación y los costos financieros asociados a un fallo en la seguridad de los datos

Requisitos de Cumplimiento

La norma PCI DSS se compone de un conjunto de doce requisitos de cumplimiento general en torno a seis objetivos principales conocidos como “objetivos de control”.

Cada uno de los doce requerimientos incluye una serie de controles de cumplimiento que juntos permiten crear un programa eficiente de seguridad orientado a la protección de números de tarjetas de pago y otros datos sensibles.

El cumplimiento de la normativa PCI DSS es responsabilidad ineludible, de todos los negocios que manejan información de titulares de tarjeta incluyendo comercios, comercio electrónico, venta por correo, venta por teléfono, procesadores de pagos, bancos y proveedores de servicios.

Este estándar ha sido diseñado principalmente para el establecimiento de un programa de seguridad en sentido de línea base para las organizaciones. Como tal es recomendable que todas las organizaciones que manejan datos de Tarjetas de Pago, observen y apliquen el estándar.

En el Ecuador, la empresa Banred, la más grande procesadora da tarjetas de crédito, ha decidido adoptar al estándar de seguridad e implantarlo en la organización como parte de una estrategia para el endurecimiento de la plataforma tecnológica, además proponerlo e impulsarlo entre las instituciones miembros de la red de cajeros ATM con la finalidad de fortalecer en forma general a todos los socios.

Descripción de los requisitos:

El estándar tiene 6 grupos, en los que se definen 12 requisitos (5) para construir una infraestructura confiable para el procesado de transacciones mediante tarjetas de pago. Los requisitos son elementales, y son de fácil adopción para cualquier Entidad que se proponga cumplir con los estándares:

1. Construir y mantener una infraestructura segura

Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos de titulares de tarjetas.

Requisito 2: No emplear configuraciones por defecto en los elementos de protección.

2. Proteger los datos de los titulares

Requisito 3: Proteger los datos de titulares de tarjeta almacenados.

Requisito 4: Cifrar las transmisiones de datos de titulares de tarjeta en redes abiertas y públicas.

3. Mantener un programa de gestión de las vulnerabilidades

Requisito 5: Emplear y actualizar periódicamente el software antivirus.

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.

4. Implementar medidas fuertes de control de acceso

Requisito 7: Restringir el acceso a los datos de titulares al ámbito de lo estrictamente necesario para ofrecer el servicio.

Requisito 8: Asignar un identificador único a cada persona con acceso a equipos de proceso.

Requisito 9: Restringir la seguridad física para acceder a los datos de titulares.

5. Monitorizar y someter a pruebas regulares las redes

Requisito 10: Monitorizar y hacer seguimiento a todos los recursos de red y a los datos de titulares.

Requisito 11: Probar regularmente la seguridad de los sistemas y procesos.

6. Mantener una Política de Seguridad de la Información

Requisito 12: Mantener una política que cubra la seguridad de la información.

Los requisitos que exige la Norma de seguridad PCI a primera vista pueden parecer simples, pero son una base importante en la formalización de las practicas que las organizaciones vienen realizando, por ejemplo: “Contar con una política de seguridad de la información”, de esa manera no tiene el peso necesario, pero su efectividad mejora si a la política se incluye, se revisa, actualiza y se vigila su cumplimiento en periodos determinados.

Finalmente, con el cumplimiento total de estar norma de seguridad se puede decir que este es un marco bien objetivo de poder tener una visión global de los requisitos mínimos que ayudarían a una empresa a mitigar los riesgos de TI y del negocio. (Visa, 2015; pcisecuritystandards.org, 2015; searchsecurity.techtarget, 2012; www.403labs.com, 2015) .

2.2 MODELO COBIT 4.1

El Marco de referencia COBIT se publicó por primera vez en abril de 1996. Su última actualización – COBIT 4.1 centra su esfuerzo al cumplimiento reglamentario, ayudando a las organizaciones a incrementar el valor de Tecnología, destacando los vínculos entre los objetivos del negocio y TI.

Este marco de trabajo es la base para diferentes entes reguladores a nivel mundial, con la finalidad de lograr que las entidades reguladas optimicen sus inversiones de TI y administren adecuadamente sus riesgos tecnológicos.

COBIT 4.1 es un marco mundial aprobado que asegura que las áreas de tecnología estén alineadas con los objetivos de negocio, sus recursos sean usados responsablemente y sus riesgos administrados de forma apropiada.

Ayuda a las organizaciones a reducir riesgos en el manejo de las Tecnologías e incrementar el valor derivado de su uso. Las actualizaciones en COBIT 4.1 incluyen: avances en la medición del desempeño; mejores objetivos de control; y una excelente alineación entre objetivos de negocio y de TI.

Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT.

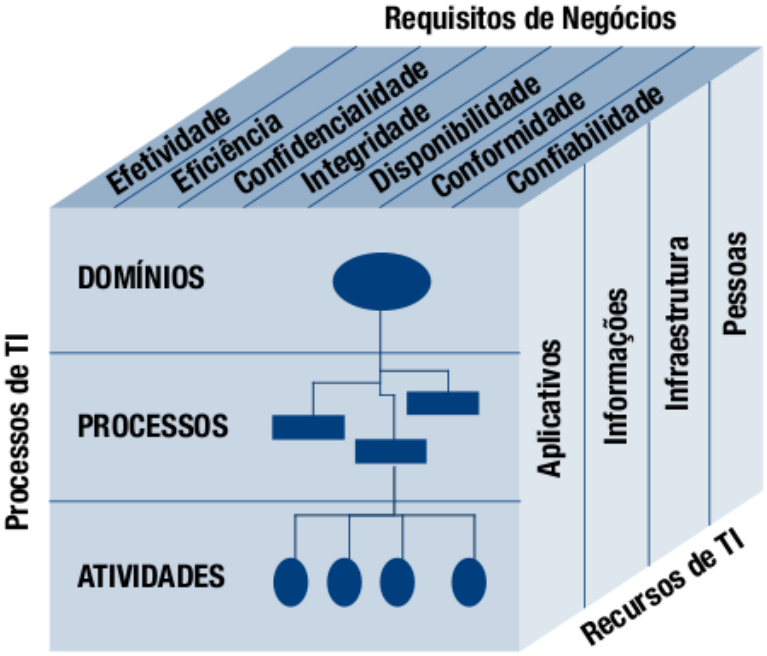


Figura 3. Modelo del marco de trabajo COBIT

Fuente: (COBIT, 2007)

COBIT es el único marco administrativo que comprende el ciclo de vida completo de la inversión en TI. Considera los logros en los objetivos de negocio, asegura alineación de las TI con el negocio y mejora la eficiencia y efectividad, afirma Roger Debreceny, Jefe del Comité de Manejo de COBIT del ITGI. COBIT 4.1 está creado como una guía práctica para administradores alrededor del mundo que lo utilizan para perfeccionar el gobierno de TI en sus organizaciones, así que ha sido probado y validado.

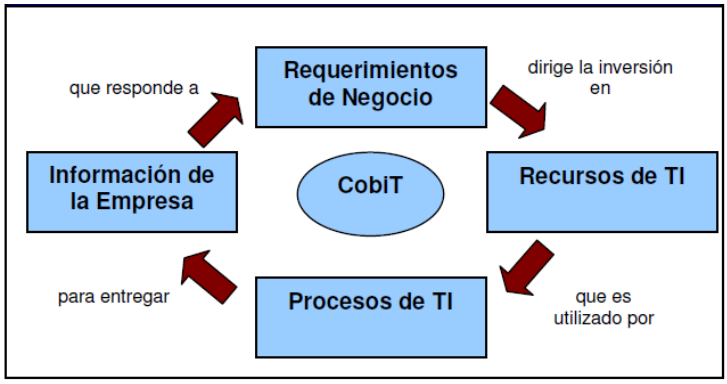


Figura 4. Flujo básico de COBIT

Fuente: (COBIT, 2007)

Beneficios

COBIT se ha convertido en el integrador de la mejores prácticas de TI y el marco de trabajo global de gobierno de TI, debido a su conjunción con otros estándares como ITIL, COSO, ISO 20000, ISO 9000, ISO 25999, ISO 27001, PRINCE2, TOGAF, entre otros y su constante actualización. La estructura de procesos de COBIT, en conjunción con su alto nivel y su enfoque "orientado al negocio" provee una visión de punta a punta de TI, que ayuda a las organizaciones a obtener el mayor valor posible de sus inversiones de TI.

Por algunos de los beneficios que se pueden obtener con el Cobit son:

- Mejor alineación basada en una focalización sobre el negocio.
- Visión comprensible de TI para su administración.
- Clara definición de propiedad y responsabilidades.
- Aceptabilidad general con terceros y entes reguladores.
- Entendimiento compartido entre todos los interesados basados en un lenguaje común.

COBIT apoya la gobernanza de TI, proporcionando un marco para garantizar que:

- TI esté alineada con el negocio
- Se permita las empresas maximizar sus beneficios
- Los recursos de TI se utilicen de manera responsable
- Riesgos de TI se gestionan adecuadamente

CONTENIDO (MARCO DE REFERNCIA COBIT 4.1)

En el Marco de referencia COBIT 4.1 los productos se encuentran definidos en tres niveles, los mismos que dan soporte a:

- Administración y consejos ejecutivos.
- Administración del negocio y de Tecnología de Información.
- Profesionales de gobierno, aseguramiento, control y seguridad.

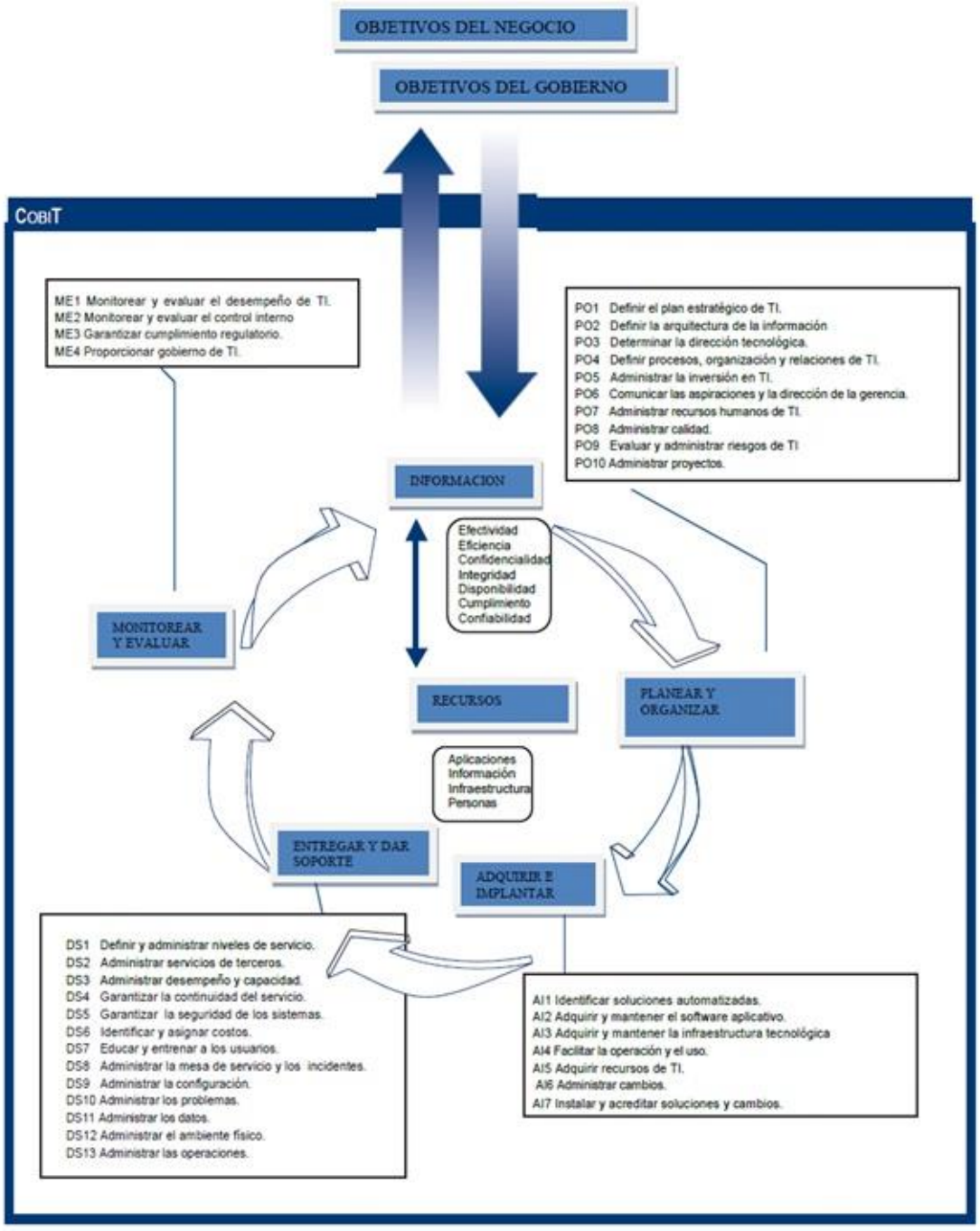


Figura 5. Principio básico de COBIT

Fuente: (COBIT, 2007)

Marco Referencial COBIT 4.1

El Marco Referencial COBIT, explica como los procesos de TI deben entregar la información, que el negocio requiere, para alcanzar sus objetivos, proporcionando al propietario de los procesos del negocio, herramientas que faciliten el cumplimiento de esta responsabilidad.

El Marco Referencial, permite también definir; si la información procesada para cumplir con los objetivos del negocio se está adaptando a los criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad), así como también define cuales de los recursos de TI (sistemas de aplicación, tecnología, instalaciones, datos) son importantes para apoyar a los objetivos del negocio.

Figura 6. Alineación de procesos y recursos de TI con el negocio

Fuente: (gobiernotic, 2006)

Dominios

Para lograr un gobierno de TI efectivo, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios (plan, construir, ejecutar y Monitorear). Estos dominios se llaman:

- Planear y Organizar (PO) – Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- Adquirir e Implementar (AI) – Proporciona las soluciones y las pasa para convertirlas en servicios.
- Entregar y Dar Soporte (DS) – Recibe las soluciones y las hace utilizables por los usuarios finales.
- Monitorear y Evaluar (ME) -Monitorear todos los procesos para asegurar que se sigue la dirección provista.

Figura 8 – Los Cuatro Dominios Interrelacionados de COBIT

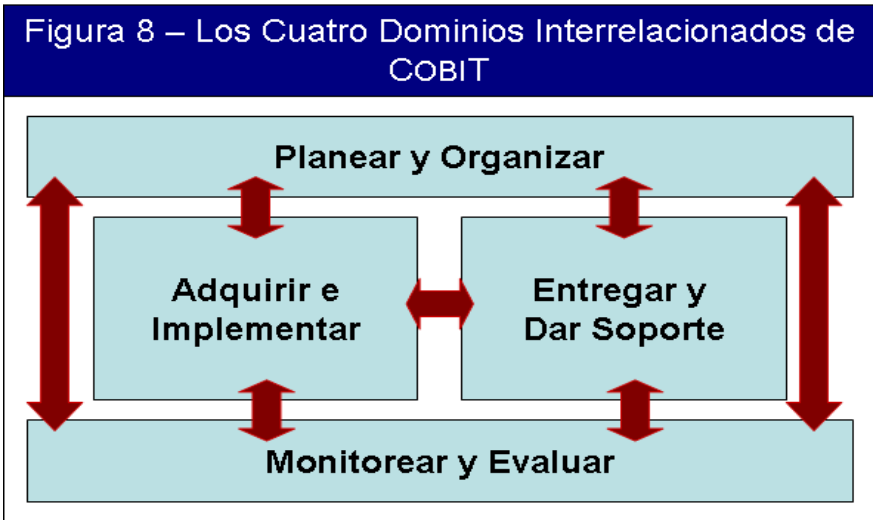


Figura 7. Interrelación de los cuatro dominios de COBIT

Fuente: (COBIT, 2007)

Planificación y Organización (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?

- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

Adquirir e Implementar (AI)

Las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

- ¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
- ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios no afectarán a las operaciones actuales del negocio?

Entregar y dar soporte (DS)

Este dominio cubre la entrega de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos. Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?

- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

Monitorear y Evaluar (ME)

Todos los procesos de TI deben evaluarse de forma regular en cuanto a su calidad y cumplimiento de los requerimientos de control. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?
  (www.isaca.org, Cobit, 2014)

2.3 RELACIÓN PCI DSS v2.0 y COBIT 4.1

Los beneficios que entrega el mapeo PCI DSS v2.0 con COBIT 4.1 se resumen en lo siguiente:

- Un sistema único de control al implementar PCI DSS puede gestionar, medir y presentar pruebas de satisfacer varios requisitos de cumplimiento y la gobernanza.

- La adhesión a los estándares de las organizaciones puede cumplir con varios estándares de la industria para proteger los datos de tarjetas de crédito y puede aumentar la eficiencia operativa.

- El aumento de rendimiento en cada requisito de PCI DSS y la adecuada asignación de los controles de COBIT previo a una evaluación del objetivo que se desea alcanzar, permite el aumento de la eficiencia y el desempeño del programa de seguridad.

Si bien el cumplimiento con PCI DSS es obligatorio para las organizaciones que procesan las transacciones financieras a través de tarjetas de pago, su alcance de seguridad se limita a la protección de datos de los tarjetahabientes. Sin embargo COBIT se convierte en un integrador de las mejores prácticas y un marco general para el gobierno de TI, lo cual complementa la eficacia de la aplicación y control de la norma.

Tabla 1.

Mapeo de los Requerimientos de PCI DSS 2.0 Vs Cobit 4.1.

PCI DSS v2.0 Vs COBIT 4.1		
Numero de Requisito	**PCI DSS v2.0 Requerimientos de Control**	**COBIT 4.1 Objetivos de Control/Procesos**
1	Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas	AI2.5 Configuración y Software Aplicativo Adquirido
		AI3.2 Protección y Disponibilidad del Recurso de Infraestructura
		DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
		DS5.7 Protección de la Tecnología de Seguridad
		DS5.10 Seguridad de la Red
		DS13.3 Monitoreo de la Infraestructura de TI
2	No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores	DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
		DS5.7 Protección de la Tecnología de Seguridad
		PO2.3 Esquema de Clasificación de Datos
		DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
3	Proteja los datos del titular de la tarjeta que fueron almacenados	DS5.8 Administración de Llaves Criptográficas
		DS11.2 Acuerdos de Almacenamiento y Conservación
		DS11.4 Eliminación
		DS11.6 Requerimientos de Seguridad para la Administración de Datos
		DS5.1 Administración de la Seguridad de TI
		DS5.7 Protección de la Tecnología de Seguridad
4	Cifrar la transmisión de los datos del titular de la tarjeta	DS5.8 Administración de Llaves Criptográficas
		DS5.10 Seguridad de la Red
		DS11.6 Requerimientos de Seguridad para la Administración de Datos
		DS5.9 Prevención, Detección y Corrección de Software Malicioso
		PO8.3 Estándares de Desarrollo y de Adquisición

CONTINÚA ⟶

5	Utilice y actualice regularmente el software o los programas antivirus	PO9.3 Identificación de Eventos
6	Desarrolle y mantenga sistemas y aplicaciones seguras	PO9.4 Evaluación de Riesgos de TI
		AI3.3 Mantenimiento de la Infraestructura
		AI3.4 Ambiente de Prueba de Factibilidad
		AI6.1 Estándares y Procedimientos para Cambios
		AI6.2 Evaluación de Impacto, Priorización y Autorización
		AI7.3 Plan de Implantación
		AI7.4 Ambiente de Prueba
		AI7.6 Pruebas de Cambios
		AI7.8 Promoción a Producción
		DS5.9 Prevención, Detección y Corrección de Software Malicioso
7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber del negocio.	DS5.3 Administración de Identidad
		DS5.4 Administración de Cuentas del Usuario.
8	Asignar una ID exclusiva a cada persona que tenga acceso por computadora	PO2.3 Esquema de Clasificación de Datos
		PO7.8 Cambios y Terminación de Trabajo
9	Restringir el acceso físico a los datos del titular de la tarjeta	DS5.3 Administración de Identidad
		DS5.4 Administración de Cuentas del Usuario
		DS5.7 Protección de la Tecnología de Seguridad
		PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
		DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
10	Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de	DS5.4 Administración de Cuentas del Usuario
		DS11.2 Acuerdos de Almacenamiento y Conservación
		DS11.3 Sistema de Administración de Librerías de Medios
		DS11.4 Eliminación

CONTINÚA ⟶

	las tarjetas	DS11.6 Requerimientos de Seguridad para la Administración de Datos
		DS12.2 Medidas de Seguridad Física
		DS12.3 Acceso Físico
		DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
		DS13.3 Monitoreo de la Infraestructura de TI
11	Pruebe con regularidad los sistemas y procesos de seguridad.	PO9.3 Identificación de Eventos
		DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
		DS5.6 Definición de Incidente de Seguridad
		ME1.2 Definición y Recolección de Datos de Monitoreo
		ME1.3 Método de Monitoreo
		ME1.4 Evaluación del Desempeño
		ME2.1 Monitoreo del Marco de Trabajo de Control Interno
		ME2.2 Revisiones de Auditoría
		ME2.3 Excepciones de Control
		ME2.4 Control de Auto Evaluación
		ME2.7 Acciones Correctivas
		PC5 Políticas, Planes y Procedimientos
		PO2.3 Esquema de Clasificación de Datos
12	Mantenga una política que aborde la seguridad de la información para todo el personal.	PO4.3 IT Comité Directivo de TI
		PO4.4 Ubicación Organizacional de la Función de TI
		PO4.6 Establecimiento de Roles y Responsabilidades
		PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
		PO4.9 Propiedad de Datos y de Sistemas
		PO6.1 Ambiente de Políticas y de Control
		PO6.3 IT Administración de Políticas para TI
		PO6.4 Implantación de Políticas de TI
		PO6.5 Comunicación de los Objetivos y la Dirección de TI
		PO7.1 Reclutamiento y Retención del Personal
		PO7.3 Asignación de Roles

CONTINÚA ⟶

		PO7.4 Entrenamiento del Personal de TI
		PO7.6 Procedimientos de Investigación del Personal
		PO9 Evaluar y Administrar los Riesgos de TI.
		DS5.1 Administración de la Seguridad de TI
		DS5.2 Plan de Seguridad de TI
		DS5.3 Administración de Identidad
		ME2.1 Monitoreo del Marco de Trabajo de Control Interno
		ME2.2 Revisiones de Auditoría
		ME2.4 Control de Auto Evaluación

(www.isaca.org, Mapping PCI DSS v2.0 to COBIT 4.1 , 2011)

La seguridad de la información siempre será un reto para todas las organizaciones por lo que el cumplimiento de PCI DSS v2.0, junto con los controles de COBIT 4.1, permitirán a la empresa trabajar de manera eficiente con el cumplimiento y gestión de TI, ya que PCI se centra en el área de cumplimiento y COBIT 4.1 proporciona la gobernanza global.

2.4 ANTECEDENTES DEL ESTADO DEL ARTE

PCI-DSS es una normativa que recoge los requisitos y procedimientos de seguridad para manejo de datos que deben seguir aquellas compañías que trabajen con transacciones de tarjetas de pago. La última actualización fue en Octubre de 2010, versión que da mayor flexibilidad, comprensión y facilidad en su implantación. Su vigencia efectiva es a partir del 1 Enero de 2011, sin embargo las organizaciones tienen un año para cumplir con la actualización.

En el Ecuador, la implementación de la normativa PCI-DSS se encuentra en una etapa inicial, son muy pocas las instituciones que han iniciado este proceso y otras pocas que han logrado ya obtener la certificación en el 2011,

por lo que es el momento adecuado para plantear modelos que permitan una adecuada evaluación a la aplicación de la norma.

El beneficio que obtienen las empresas que implementan y cumplen con los requisitos PCI-DSS es sufrir menos violaciones a su información así como también un status más elevado dentro del mercado financiero mejorando su imagen frente a los clientes y las franquicias.

Según la empresa Imperva, compañía con experiencia en la protección de datos y sitios web, y distribuido en el mercado ibérico por Exclusive Networks, junto al Instituto Ponemon, ha dado a conocer los resultados de su segundo estudio relativo al impacto del Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS -Payment Card Industry's Data Security Standards).

Según cita la fuente News Letter E. Security (09/05/2011)en su ***"Informe sobre Tendencias de Cumplimento PCI DSS*** -realizado en 2011 a 670 profesionales de multinacionales norteamericanas especializadas en seguridad TI- revela cómo el cumplimiento con PCI-DSS tiene un impacto positivo en la seguridad y protección de datos de las empresas.

CUMPLIMIENTO DEL ESTÁNDAR: una buena medida para reducir violaciones

Según el estudio, el 64% de las empresas que reconocen acatar el estándar PCI-DSS confirma no haber sufrido transgresiones relativas a los datos asociados a sus tarjetas de crédito en los últimos dos años, mientras que sólo el 38 % de las compañías que no cumplen pudieron afirmar lo mismo.

Cuando se trata de violaciones de datos globales (incidentes generales o relativos a la información contenida en la tarjeta de crédito), el 63% de las

organizaciones que se encuentran en conformidad con el estándar no padeció más que una única violación de sus datos, en comparación con el 22% de las compañías que no lo acogen. Cabe destacar también que el 26% de las empresas que no lo ejecutan fueron víctimas de más de cinco delitos en el mismo período de tiempo.

Una percepción cínica sobre PCI-DSS A pesar de que la evidencia indica lo contrario, el 88% de los encuestados confirma no estar de acuerdo con que el cumplimiento de PCI-DSS pueda encerrar un efecto positivo en lo relativo al número de transgresiones experimentadas, y sólo el 39% cita la mejora en la seguridad de los datos como una de las propuestas de valor -contenida en PCI DSS- para los negocios.

De hecho, únicamente el 33% cree que el gasto destinado a cumplir con PCI-DSS queda cubierto por el beneficio que supone para la organización. El cumplimiento aumenta, a pesar de todo.

El informe también recoge que dos tercios de los encuestados han logrado el cumplimiento sustancial con PCI-DSS. Esta cifra contrasta con la obtenida en el Estudio sobre Tendencias de Cumplimiento PCI DSS de 2009, cuando el número de participantes que confirmaba este hecho correspondía únicamente a la mitad de los profesionales preguntados, mientras que aproximadamente el 25% de los encuestados afirmaba que no había alcanzado nivel de cumplimiento alguno. En 2011, únicamente el 16% de las organizaciones sondeadas testifica no haberlo hecho.” (http://saladeprensabg.com, 2012; www.imperva.com, 2015) (www.portal.banred.fin.ec; E.Security, 2011; Arbesú, 2012).

Control Interno

Es un proceso, efectuado por la administración y diseñado para identificar los eventos potenciales que pueden afectar la entidad, y para

administrar los riesgos que se encuentran dentro de su apetito por el riesgo, a fin de proveer seguridad razonable en relación con el logro de los objetivos de la entidad en tres categorías de objetivos. (Malica, 2012)

Objetivos del Control Interno:

- Proteger los activos y salvaguardar los bienes de la institución.
- Verificar la razonabilidad y confiabilidad de los informes contables y administrativos.
- Promover la adhesión a las políticas administrativas establecidas.
- Lograr el cumplimiento de las metas y objetivos programados.
- Conseguir efectividad y eficiencia de las operaciones.
- Conseguir suficiencia y confiabilidad de la información financiera.

Componentes y elementos del control interno:

Filosofía de la gestión de riesgos.

La filosofía de la gestión de riesgos de una organización es el conjunto de creencias y actitudes compartidas que caracterizan el modo en que la entidad contempla el riesgo en sus actividades cotidianas. Dicha filosofía queda reflejada prácticamente en todo el que hacer de la dirección al gestionar la entidad y se plasma en las declaraciones sobre políticas, las comunicaciones verbales y escritas y la toma de decisiones. Tanto si la dirección pone su énfasis en las políticas escritas, normas de conducta, indicadores de rendimiento e informes de excepción, como si prefiere operar más informalmente mediante contactos personales con los directivos claves, lo críticamente importante es que desde ella se potencie la filosofía, no sólo con palabras, sino con acciones diarias.

El punto de partida de nuestro programa de gestión de riesgos es una estrategia de gestión que respete las necesidades y aspiraciones de todos aquellos con quienes se mantiene alguna relación. Dicho programa proporciona un modelo interactivo de información del riesgo, que facilita el

flujo de información y hace hincapié en la comunicación a través de toda la organización. Este modelo proporciona información acerca de las necesidades y expectativas de los grupos de interés, con el fin de mejorar continuamente nuestra estrategia de riesgo a escala empresarial. (www.gestiopolis.com, 2014; fccea.unicauca.edu.co, 2003; Mexico, 2004)

Evaluación de riesgos.

La evaluación de riesgos permite a una entidad considerar la amplitud con que los eventos potenciales impactan en la consecución de sus objetivos. La dirección evalúa estos acontecimientos desde una doble perspectiva –probabilidad e impacto y normalmente usa una combinación de métodos cualitativos y cuantitativos. Los impactos positivos y negativos de los eventos potenciales deben examinarse, individualmente o por categoría, en toda la entidad. Los riesgos se evalúan con un doble enfoque: riesgo inherente y riesgo residual.

Dentro de los métodos cualitativos se mencionan los siguientes: clasificación de riesgos y el uso de cuestionarios; y técnicas cuantitativas, tales como técnicas probabilísticas de valor en riesgo, valor de mercado en riesgo, distribuciones de pérdidas y análisis retrospectivo; y técnicas no probabilísticas tales como análisis de sensibilidad, análisis de escenarios, pruebas de tolerancia a situaciones límite. (MAZA, 2015; González, 2014; Carlosama, 2015).

Riesgo inherente y residual.

El riesgo inherente Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se haga a su interior.

El riesgo residual refleja el riesgo remanente una vez que se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.

Estas acciones pueden incluir las estrategias de diversificación relativas a las concentraciones de clientes, productos u otras, las políticas y procedimientos que establezcan límites, autorizaciones y otros protocolos, el personal de supervisión para revisar medidas de rendimiento e implantar acciones al respecto o la automatización de criterios para estandarizar y acelerar la toma de decisiones recurrentes y la aprobación de transacciones. Además, pueden reducir la probabilidad de ocurrencia de un posible evento, su impacto o ambos conceptos a la vez.

Probabilidad e impacto.

Al estimar la probabilidad e impacto de posibles eventos, ya sea sobre la base del efecto inherente o residual, se debe aplicar alguna forma de medición.

Medición nominal

Es la forma más sencilla de medición e implica el agrupamiento de eventos por categorías, tales como la económica, tecnológica o medioambiental, sin situar a un acontecimiento por encima de otro. Los números asignados en la medición nominal sólo tienen una función de identificación y los elementos no pueden ser ordenados, clasificados ni agregados.
(http://www.auditool.org, 2014; http://wwwisis.ufg.edu.sv, 2012).

2.5 MARCO CONCEPTUAL

Los clientes esperan que los negocios y las instituciones financieras protejan los datos de las tarjetas de crédito y débito. PCI DSS no garantiza que no vaya a haber una filtración de datos, pero anima a que los negocios

utilicen los datos de sus clientes de manera sensata. En el año 2006, un grupo de cinco instituciones financieras, preocupados por el aumento de los índices de fraudes con tarjetas, crearon un programa de seguridad para datos y así fundaron un consejo conocido como PCI Security Standards Council. Este grupo está conformado por las principales marcas de tarjetas como son: Visa, Master Card, JCB International, Discover Financial Services y American Express.

Las penalizaciones por no cumplir con PCI DSS van desde un aumento en las auditorías de seguridad, hasta un número ilimitado de multas, o incluso la pérdida total de la capacidad de procesar transacciones de tarjetas. Por supuesto, la reputación de tu negocio también corre peligro si hay una filtración de datos.

¿Cómo puedo cumplir con PCI DSS?

Hay cuatro niveles de cumplimiento de PCI DSS. El nivel que tu negocio necesite dependerá de dos factores principales:

- Su volumen de transacciones.
- El modo en que procese información de transacciones.

El PCI Security Standards Council reconoce a Asesores de Seguridad Cualificados (QSA) que pueden expedir tu certificado PCI DSS. Puede que tu banco adquirente tenga también un QSA recomendado.

La idea de generar un modelo de evaluación interna se basa en la necesidad de apoyar al proceso de implementación de soluciones a las brechas de seguridad que podrían surgir como resultado de los análisis iníciales y de esta manera contar con sistemas seguros para el manejo de información de titulares de tarjetas.

El crecimiento constante de la tecnología va de la mano con la especialización de la delincuencia lo que obliga a buscar nuevos

mecanismos de control y parte de estos nuevos mecanismos es la normativa PCI-DSS, creada por las principales marcas de tarjetas de crédito a nivel mundial como resultado de un análisis donde se pudo ver que los esfuerzos individuales que realizaba cada marca no era suficiente, por lo que tomaron la decisión de unirse y conjugar en un solo concepto las mejores prácticas de seguridad con un alcance a varios niveles.

Así nace el estándar PCI-DSS (Payment Card Industry –Data Security Standard).Y consiste en una serie de prácticas de seguridad que exigen el cumplimiento de 12 requerimientos de seguridad agrupados en 6 categorías que son:

Tabla 2.
Categoría de Cumplimiento de la normativa PCI DSS

CATEGORIAS DE CUMPLIMIENTO PARA PCI-DSS
Crear y mantener redes con adecuados niveles de seguridad
Protección de la información del tarjetahabiente
Generar pruebas de vulnerabilidades periódicas
Implementar mejoras al control de acceso
Monitorear y realizar pruebas de acceso a la red de manera regular
Crear, mejorar y mantener políticas de seguridad de la información.

(COBIT, 2007)

La normativa PCI DSS versión 2.0 se aplica a todas aquellas instituciones financieras que procesan, guardan o trasmiten datos de tarjetas de crédito o débito, el no hacerlo representa la posibilidad de arriesgar la facultad para procesar transacciones de estas tarjetas (Retiro de las franquicias), enfrentar auditorías rigurosas y llegar a pagos de multas Los Comerciantes y proveedores de servicios de tarjetas, están en la obligación de validar su cumplimiento al estándar en forma periódica.

El presente trabajo pretende generar y poner a disposición una guía clara y práctica de evaluación que permita realizar levantar información de los diferentes procesos que intervienen en temas de seguridad según la normativa PCI-DSS y que se ajusten a la realidad de las instituciones bancarias que emitan, procesen o trasmitan información de tarjetas de crédito o débito. (Sia, 2014; strategoscs, 2015; Jimenez, 2011).

CAPÍTULO III

METODOLOGÍA DE INVESTIGACIÓN

Por la naturaleza de la investigación se ha definido aplicar una metodología de trabajo mediante el uso de técnicas de investigación como la observación, encuestas y cuestionarios, mismo que serán aplicados a los actores directos en el proceso de certificación.

Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información.

El alcance de la investigación se da en base a la normativa PCI-DSS y COBIT 4.1, mediante criterios que muestran cómo orientar la tecnología de la información hacia el negocio; y su evaluación periódica de calidad y suficiencia.

Como primera actividad se espera recoger, agrupar y evaluar evidencias, para determinar si la infraestructura y procedimientos actuales cumplen con lo dispuesto en la normativa y, principalmente si lleva a cabo eficazmente los objetivos de la organización, utilizando eficientemente los recursos.

La ejecución de esta investigación será en una entidad bancaria, para lo cual se debe realizar una revisión a los controles establecidos dentro de la institución, aplicando el modelo COBIT, al final se espera obtener recomendaciones en base a las falencias detectadas, las cuales nos permitirán generar la guía de Auditoria más competente y que pueda ser aplicada de la mejor manera.

Durante la auditoría, se debe recopilar información útil y necesaria, misma que luego de analizarla, permita obtener conclusiones y sus

respectivas recomendaciones para el mejoramiento de la organización. La obtención de información o evidencias, se puede realizar combinando uno o más de los siguientes procedimientos:

- Indagar y confirmar
- Inspeccionar
- Observar
- Recolectar y analizar evidencia.

Productos a Entregar

Definir la metodología para ejecutar evaluaciones de la normativa PCI-DSS, que es el objetivo principal de este trabajo y de acuerdo a las evaluaciones ejecutadas se prevé entregar recomendaciones que permitan controlar los niveles de riesgo y las debilidades que esto pueda provocar dentro de las instituciones.

3.1.1 DISEÑO METODOLÒGICO

Tipo de Investigación

En base a la naturaleza del trabajo que se desea desarrollar se ha tomado en consideración varios tipos de investigación que apoyaran a cumplir este fin, los que se detallan a continuación:

Investigación Exploratoria.- No intenta dar explicación respecto del problema, sino sólo recoger e identificar antecedentes generales, temas y tópicos respecto del problema investigado, sugerencias de aspectos relacionados que deberían examinarse en profundidad en futuras investigaciones. Su objetivo es documentar ciertas experiencias, examinar temas o problemas poco estudiados o que no han sido abordadas antes. Por lo general investigan tendencias, identifican relaciones potenciales entre variables y establecen el “tono” de investigaciones posteriores más rigurosas.

Investigación Documental.- se realiza apoyándose en fuentes de carácter documental, esto es, en documentos de cualquier índole, tomando como recursos varias bibliografías relacionadas con el tema, en muchos archivos. (uovirtua, 2014; MaweLearn, 2010)

3.1.2 IDENTIFICACIÓN DE COMPONENTES QUE INTERVIENEN EN EL PROCESO INVESTIGATIVO.

De acuerdo al objetivo de la investigación, dentro de la institución mediante un análisis inicial a los componentes y procesos tecnológicos e ha logrado identificar las áreas más críticas en el proceso de evaluación y que son:

- Tecnología
- Desarrollo
- Seguridad de la Información
- Tarjeta de Crédito y Débito y
- Distribución.

Estas áreas deberán recibir capacitación inicial y una explicación sobre los objetivos de la evaluación, sin embargo el alcance del presente trabajo estará centrada en las áreas de Tecnología, Desarrollo y Seguridad de la Información.

3.1.3 MÉTODOS DE INVESTIGACIÒN

Se utilizará los siguientes métodos investigativos, mismos que ayudarán a la obtención de resultados confiables:

Método Inductivo

Este método obtiene conclusiones generales a partir de premisas particulares. Se trata del método científico más usual, en el que pueden

distinguirse cuatro pasos esenciales: la observación de los hechos para su registro; la clasificación y el estudio de estos hechos; la derivación inductiva que parte de los hechos y permite llegar a una generalización; y la contrastación, siempre y cuando se tome en consideración los siguientes parámetros:

- Observación
- Comparación y,
- Generalización.

Este permite identificar los aspectos indispensables para conseguir una información que permitirá toma de decisiones posteriores.

Figura 8. Explicación gráfica del flujo que aplica el método inductivo

Fuente: (Rangel, 2013)

Método Deductivo

Este método es uno de los más conocidos ya que permite que las afirmaciones de carácter general tengan relación con las afirmaciones particulares.

Método de Observación Directa

Mantiene una relación con hechos y fenómenos que trata de indagar o investigar aspectos inherentes a la Observación. Descripción, Interpretación, Comparación y Generalización de los resultados. (RANGEL, 2014; Rangel, 2013).

TECNICAS DE INVESTIGACIÓN

La auditoría informática, se basa en una serie de análisis que se realizan con tres métodos base escogidos para la realización de este trabajo:

- Encuestas de evaluación
- Simulaciones y pruebas de los procesos
- Entrevistas

Además existen otros métodos, como son:

Matrices de Investigación de Campo

Son instrumentos elaborados para ser utilizado como base de datos para la organización del trabajo del Auditor.

Observación Directa

Es una técnica que permite captar la realidad del proceso analizado y puede ser de dos tipos. No participante, es aquella en que el auditor observa externamente el proceso sin interferir y, participante, es aquella en la que el auditor participa en los procesos.

Entrevistas

Es una técnica útil donde el audito se va a encontrar con reacciones defensivas e incluso hostiles. Una forma de controlar estos factores de tensión, está en adoptar una postura amigable donde el éxito de la entrevista, depende de factores como: la experiencia y los conocimientos del auditor y la buena predisposición del auditado.

Checklist

El checklist es una técnica muy utilizada en el campo de la auditoría informática. No es más que una lista de comprobación o cuestionario, que sigue pautas determinadas, dependiendo de que estemos evaluando o qué objetivos se desean alcanzar. (Andrés Naveda Paredes, 2013).

3.1.4 EVALUACIÓN DE RESULTADOS

Luego de llevar a cabo la revisión de la documentación en el área de Tecnología y, de ejecutar el análisis respectivo, de acuerdo a la Guía de Auditoría de COBIT y PCI-DSS, se podrán obtener conclusiones que permitan generar recomendaciones. Resultados que se presentarán en un informe de auditoría.

Una vez analizada y conocida de la situación actual de la entidad y, definido el enfoque de auditoría a ser utilizado, así como los responsables de la parte tecnológica y del negocio; en esta etapa se realizarán las siguientes actividades:

- Definir el plan de pruebas para cada una de las actividades de control, señaladas en el enfoque de la auditoría.
- Determinar la documentación necesaria, para probar cada actividad de control identificada en el enfoque de auditoría.
- Planificar encuestas, checklist, hojas de evaluación y entrevistas con los encargados del Área de Sistemas, o cualquier otro documento que permita más a detalle los procesos y procedimientos existentes en la entidad y solicitar la documentación que respalde la información.
- Realizar el respectivo análisis y documentación de la información obtenida, y emitir una conclusión para cada actividad de control.
- Diseñar y elaborar el informe de auditoría, donde por cada Objetivo de Control se detallará:

- Criterio
- Condición
- Causa
- Efecto
- Conclusiones
- Recomendaciones

- Elaborar las guías de auditoría que permitirán evaluar las futuras condiciones de los componentes que intervienen en el proceso de cumplimiento a la normativa PCI-DSS
- Identificación de los componentes que intervienen en el proceso investigativo.
- Detalle general de cómo interpretar los resultados obtenidos.

CAPÍTULO IV

4.1 LEVANTAMIENTO DEL ESTADO ACTUAL DE LA INSTITUCIÓN COMO BASE PARA LA GENERACIÓN DEL MODELO DE EVALUACIÓN.

En base a los resultados de un estudio interno de la institución respecto a la situación actual frente a los diferentes campos donde PCI actúa, fue posible definir 5 grandes proyectos con los cuales se busca cubrir las exigencias de la norma PCI.

Los proyectos definidos son:

1. Control centralizado de manejo de información sensitiva.
2. Administración de la configuración de los sistemas de información.
3. Manejo de incidentes
4. Desarrollo seguro
5. Cumplimiento Normativo.

En base al análisis de salud actual de la institución, se han definido los requisitos mínimos necesarios de la Norma PCI que se deben cumplir, detalle que se presenta a continuación.

Tabla 3.
Propuesta De Trabajo Para Implementar Un Esquema De Control De Información Sensitiva

IMPLEMENTAR UN ESQUEMA DE CONTROL CENTRALIZADO PARA El MANEJO DE INFORMACIÓN SENSITIVA. (PAN) **Levantar información por donde fluyen datos sensibles de tarjetahabientes y de esta manera Implementar controles de acceso a la información.**	**REQUISITOS PCI**
Levantar flujo de datos del Personal Account Number (PAN) o numero principal de la tarjeta y establecer controles:	
- Levantar detalle del esquema a utilizar para retención y disposición de datos del tarjetahabiente (límites de almacenamiento, tiempo de permanencia, eliminación etc).	* 3.1.1.a / 3.1.1.b / 3.1.1.c / 3.1.1.d / 3.1.1.e
- Evaluar e implementar controles para encriptación de la información en todos los flujos que almacenen información del PAN	* 3.4.1 / 3.4.a / 3.4.b / 3.4.c
- Controles para restringir conexiones a internet y evitar entrada o salida de tráfico	* 1.3.3 / 1.3.5
- Controles para restringir el envío del PAN no cifrado por medios tecnológicos de mensajería.	* 4.2.a / 4.2.b
- Metodología para aplicar el cifrado de disco y seguridad en el manejo de llaves criptográficas.	* 3.4.1.b
- Adquisición de herramientas para Gestión de la mensajería y su contenido.	* 3.6.a / 3.6.b 3.6.1 / 3.6.2 / 3.6.3 / 3.6.4 / 3.6.5 / 3.6.5.a / 3.6.5.b / 3.6.5.c / 3.6.6 / 3.6.7 3.6.8
- Revisar que los datos de producción no sean utilizadas en ambiente de Testing (PAN)	* 6.4.3
- Mantener un proceso de borrado seguro que permita verificar que la información es irrecuperable.	* 3.2.b
- Ocultamiento o enmascarar el PAN en el flujo de Datos	* 3.3
- Documentar y ejecutar los procesos de evaluación de Riesgo tecnológico al flujo de Tarjeta de Crédito y vulnerabilidades al menos 1 vez al año	* 12.1.2.a / 12.1.2.b

*** Requisitos que contiene la norma PCI a ser implementados**

Tabla 4.
Propuesta De Trabajo Para Implementar Un Esquema De Administración de la Configuración (Hardening).

IMPLEMENTAR UN ESQUEMA DE ADMINISTRACIÓN DE LA CONFIGURACIÓN DE TECNOLOGIA DE LA INFORMACION (Hardening). **Robustecer procedimientos que contengan la información necesaria sobre las configuraciones óptimas de hardware y software (redes, firewall procesos), de acuerdo a las mejores prácticas (Hardening).**	**REQUISITOS PCI**
- Validar la existencia de procedimientos que contengan las configuraciones básicas necesarias para los componentes tecnológicos, control de cambios, así como evaluar el conocimiento de los administradores sobre estas configuraciones	* 2.2.3 / 6.4.5a / 6.4.5.1
- Desarrollar normas de configuración para todos los componentes de sistemas, basados en las mejores prácticas y Hardening	* 2.2.a / 2.2.b / 2.2.c / 2.2.d / 2.2.2.a / 2.2.2.b
- Evaluar la implementación de herramientas para monitoreo de integridad de archivos así como también sus esquemas de notificaciones en caso de esta información sea modificada.	* 11.5.a / 11.5.b
- Implementar sistemas de sincronización de tiempos en todos los componentes tecnológicos.	* 10.4.a / 10.4.1.a / 10.4.1.b / 10.4.2.a / 10.4.2.b / 10.4.3
- Implementar un esquema de manejo de parches de seguridad así como también un esquema de notificaciones que permita dar seguimiento al ciclo de vida de los parches.	* 6.1.b / 6.5.6
- Mantener un control de históricos y llaves únicas en la administración de contraseñas (ATM).	* 8.5.12.a
- Implementar procedimientos para pruebas de seguridad y funcionalidad de las aplicaciones basadas en buenas prácticas (OWASP)	* 6.4.5.3.a / 6.4.5.3.b
- Implementar y mantener procedimientos para desinstalación de aplicaciones y restauración de versiones (rollback).	* 6.4.5.4
- Implementar procedimientos para la ejecución de escaneos periódicos en busca de software malicioso.	* 5.2.c

CONTINÚA ⟶

- Implementar cifrado sólido a todo acceso administrativo que no sea de consola, así como validar que comandos de conexión no autorizados estén habilitados	* 2.3.a / 2.3.b / 2.3.c / 8.4.a
- Evaluar y actualizar las políticas de administración de cuentas y parámetros de seguridad para claves. (Caducidad, históricos, intentos fallidos, asignación de cuentas, log´s etc.).	* 8.5.8.a / 8.5.9.a / 8.5.10.a / 8.5.13.a
- Implementar pistas de auditoría a toda actividad por parte de usuarios con privilegios administrativos y de acceso a información del tarjetahabiente por parte del personal.	* 10.2.1 / 10.2.2
- Es necesario contemplar logs de acceso a los servidores de almacenamiento de pistas y rastros de auditoría.	* 10.2.3 / 10.2.4 / 10.2.5 / 10.2.6 / 10.2.7 / 10.3.1 / 10.3.2 / 10.3.2 / 10.3.3 / 10.3.4 / 10.3.5 / 10.3.6
- Manejo de Seguridades para los segmentos Inalámbricos - Wireless.	* 1.2.3 / 1.1.5 1 / 1.6 2.1.1.a / 2.1.b / 4.1.1/ 11.1
- Evaluar un esquema de bloqueo de puertos no usados mediante la habilitación port security basado en direcciones MAC o NAC autentificación de conexiones en puertos mediante 802.1x	* 11.1.a / 11.1.b / 11.1.c / 11.1.d / 9.1.2
- Implementar un IPS o IDS de red con interface y capacidad suficiente para monitorear los segmentos de servidores internos y actualizar las firmas de IPS actual.	* 11.4.a / 11.4.c
- Revisar las políticas y restricciones de Conexiones Remotas.	* 12.3.10 / 12.3.10.a / 12.3.10.b
- Habilitar mecanismos antispoofing en el firewall, normativa para revisión periódica (semestral) las regla de firewall.	* 1.3.4 / 1.1.6.a / 1.1.6.b
- Implementar un firewall de aplicaciones web.	* 6.6
- Completar la política y elaborar el procedimiento de destrucción de información o disposición final del tarjetahabiente (nist800-88).	* 9.10 / 9.10.1.b / 9.10.2
- Modificar programas de grabación de llamadas para eliminar tonos de PIN Digital (Tonos en las grabaciones).	* 3.2.3
- Crear la política para control de acceso para medios magnéticos removibles y cifrados, incluir manejo de llaves criptográficas.	* 3.4.1.c / 3.5.1 / 3.5.2.a / 3.5.2.b
- Habilitar complejidad de contraseña en las políticas de dominio.	* 8.5.11
- Disminuir el tiempo de bloqueo de las pantallas de Windows por inactividad.	* 8.5.15

CONTINÚA ⟶

- Desarrollar una política para distribución contralada de medios que contengan información en general.	* 9.7

* Requisitos que contienes la norma PCI a ser implementados

Tabla 5.

Propuesta De Trabajo Para Implementar Un Monitoreo Integral para Manejo de Incidentes.

IMPLEMENTAR CONSOLA DE MONITOREO PARA MANEJO DE INCIDENTES **Se debe implementar un esquema centralizado de monitoreo para Log's en todos los elementos de sistemas y red, así como también un adecuado esquema de trabajo para manejo de incidentes relacionado con seguridad y tecnología.**	**REQUISITOS PCI**
- Evaluar e implementar una herramienta que permita el monitoreo de incidentes y pistas de auditoria	* 10.1 / 10.5.1 / 10.5.2 / 10.5.3 / 10.5.4 / 10.5.5 / 12.2
- Proponer planes de acción para robustecer las seguridades, manejo de incidentes y proteger las pistas de auditoría, mediante un monitoreo integral NIST 800-61.	* 12.9.5 / 12.9.6
- Generar políticas y revisar que el plan de respuesta ante incidentes abarque la supervisión y la respuesta a las alertas por acceso no autorizados a puntos inalámbricos e incluya a los responsable de cada proceso.	* 11.1 / 12.9.1.b / 12.9.2 / 12.9.3 / 12.9.4 / 10.6.a / 10.6.b / 10.7.a / 10.7.b

*** Requisitos que contienes la norma PCI a ser implementados**

Tabla 6.

Propuesta De Trabajo Para Implementar Una Metodología de Desarrollo Seguro.

IMPLEMENTAR METODOLOGÍAS DE DESARROLLO SEGURO DE SOFTWARE **Implementar esquemas orientados al desarrollo seguro mediante la aplicación de mejores prácticas de la industria, así también es necesario incorporar seguridad de la información en todo el ciclo de vida del desarrollo.**	**REQUISITOS PCI**
- Revisar y evaluar los procesos de desarrollo e implementar estándares de desarrollo seguro para todas aplicaciones incluido aplicaciones Web	* 6.3.b / 6.3.c / 6.3.2.a / 6.3.2.b / 6.5.a / 6.5.b / 6.5.1 / 6.5.2 / 6.5.3 / 6.5.4 / 6.5.5 / 6.5.7 / 6.5.8 / 6.5.9 / 6.3.a

*** Requisitos que contienes la norma PCI a ser implementados**

Tabla 7.

Propuesta De Trabajo Para Implementar Normativas y Procedimientos.

CUMPLIMIENTO DE NORMATIVAS RELACIONADAS AL MANEJO SEGURO DE TI. **Implementar modelos de evaluación a los componentes, procesos y software personalizado del sistema, mismos que deben ser probados con frecuencia para garantizar que los controles de seguridad ofrezcan entornos dinámicos, se debe incluir análisis internos y externos de vulnerabilidades de red en periodos trimestrales.**	**REQUISITOS PCI**
- Implementar un programa para supervisar el estado de cumplimiento del a normativa PCI-DSS	* 12.8.4
- Establecer políticas y un programa Trimestral para análisis de vulnerabilidades	* 6.6 / 11.2.1.a / 11.2.1.b / 11.2.1.c / 11.2.2.b / 11.2.2.c / 11.2.3.a / 11.2.3.b / 11.2.3.c / 11.3 / 11.3.b / 11.3.c / 11.3.1 /

CONTINÚA ⟶

	11.3.2 / 11.5.a / 5.2.b
- Desarrollar políticas para guiar y normar PCI dentro del GFP	* 12.1.1
- Validar y actualizar las políticas y normas de configuración de los componentes de red, estas deben incluir descripción de grupos, roles y responsabilidades para la administración.	* 1.1.4
- Verificar la existencia de controles de seguridad física para cada sala informática, centro de datos y todo entorno que maneje sistemas con información de titulares de tarjetas, (control de acceso lógico y físico)	* 9.1.1 / 9.1.1.c
- Verificar registro de visita para mantener pistas de auditoría física y validar que contenga como mínimo: nombre del visitante, empresa, quien autorizó el ingreso. Estos registros se deben mantener al menos 3 meses.	* 9.4.a / 9.4.b
- Evaluar la política y procedimiento para el ingreso físico de visitantes y la asignación de placas de identificación.	* 9.2.a / 9.2.c / 9.3.2.a / 9.3.2.b
- Verificar el proceso de almacenamiento de los medios de copias de seguridad, debe ser un lugar externo con las seguridades adecuadas, esta revisión se realizará por lo menos una vez al año.	* 9.5 / 9.5.b
- Validar y de ser necesario robustecer los programas de concientización sobre seguridad a todos los empleados por lo menos una vez al año	* 12.6.a / 12.6.1.b
ADQUIRIR E IMPLEMENTAR HERRAMIENTAS DE SCANEO, ACCESOS A LAS REDES Y FIREWALLS	

*** Requisitos que contienes la norma PCI a ser implementados**

4.2 PROPUESTA DE EVALUACIÓN

En base a los resultados obtenidos en el análisis del estado actual de la institución, se ha desarrollado un modelo que, mediante el uso de una matriz de evaluación y un cuestionario se tenga la posibilidad de mantener un control permanente sobre el cumplimiento de la norma PCI-DSS, así como también en base a la información levantada poder emitir un informe como resultado final al proceso.

4.3 MODELO PROPUESTO PARA EVALUACIÓN

La matriz de evaluación se presenta dividida en 7 secciones, cuya finalidad es realizar una evaluación integral combinando los requisitos de PCI, Objetivos de control de Cobit, los factores del riesgo operativo y calificando el Riesgo Inherente y residual, con lo cual se obtendrán todos los argumentos necesarios para definir un nivel de madurez a cada proceso evaluado y emitir las recomendaciones más adecuadas al proceso.

MATRIZ PROPUESTA PARA EVALUAR CUMPLIMIENTO DE LA NORMATIVA PCI-DSS

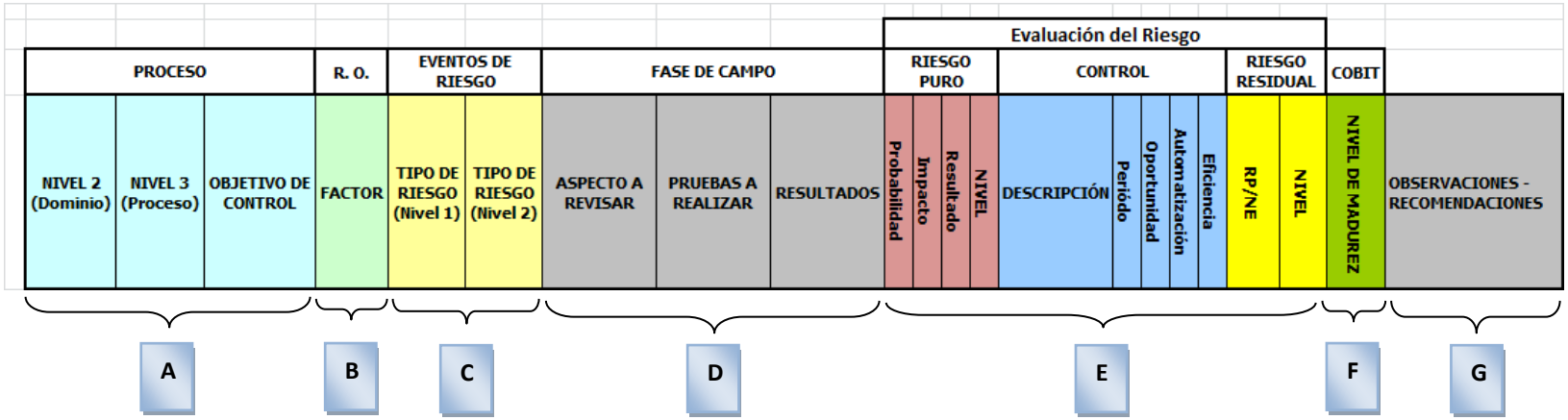


Figura 9. Modelo de la Matriz de Evaluación

Los campos que componen la matriz son:

A. Procesos
B. Riesgo Operativo
C. Eventos de Riesgo
D. Fase de Campo
    - Aspectos a revisar
    - Pruebas a realizar
    - Resultados
E. Evaluación del Riesgo
    - Riesgo Puro
    - Control
    - Riesgo residual
F. Cobit (Nivel de madurez)
G. Observaciones y Recomendaciones

4.4 METODOLOGIA PROPUESTA PAR LA EVALUACIÓN DE LA NORMA PCI - DSS

A continuación se presenta de manera detallada el uso de cada una de las 7 secciones que componen la matriz de evaluación propuesta, con lo cual se busca consolidar la información revisada y obtener un resultado que permita conocer el estado actual de cada proceso evaluado y sus respectivas recomendaciones en el caso que sea necesario.

A. PROCESOS

Los procesos a evaluar se basaran en el marco referencial de COBIT 4.1 y sus 4 cuatro dominios, mismos que se ingresaran en los 3 primeros campos como se muestra en la gráfica.

Tabla 8.

Componentes De La Primera Sección De La Matriz De Evaluación.

PROCESO		
NIVEL 2 (Dominio)	**NIVEL 3 (Proceso)**	**OBJETIVO DE CONTROL**

Dónde:

NIVEL 2 (Dominio): Se elegirá uno de los cuatro dominios de Cobit 4.1 para cada proceso evaluado.

Tabla 9.

Detalle General De Los Dominios de Cobit.

DOMINIOS COBIT
PO - Planear y Organizar
AI - Adquirir e Implementar
DS - Entregar y Dar soporte
ME - Monitorear y Evaluar

NIVEL 3 (Proceso): Se elegirá uno de los procesos de COBIT en base al dominio elegido en el campo anterior.

OBJETIVO DE CONTROL: Se elegirá el objetivo de control que más se ajuste a la necesidad de la revisión.

B. RIESGO OPERATIVO

En este campo se elige uno de los 4 factores del riesgo el cual permitirá guiar hacia donde orientar la evaluación y las posibles propuestas de mejora:

Tabla 10.

Componentes De La Segunda Sección De La Matriz De Evaluación Relacionado con Riesgo Operativo.

Riesgo Operativo
FACTOR DEL RIESGO

Dónde: los 4 factores de riesgo son

Tabla 11.

Detalle de los 4 Factores de Riesgo.

FACTORES DEL RIESGO
Proceso
Personas
Tecnología de la Información
Eventos Externos

Factor de Riesgo	Tipo de Evento
Personas	Fraude Interno
	Prácticas Laborales y Seguridad del Ambiente de Trabajo
	Prácticas relacionadas con los Clientes, los Productos y el Negocio
Sistemas	Interrupción del Negocio por fallas en la Tecnlogía de Información
Procesos	Ejecución, Entrega y Gestión de Procesos
Eventos Externos	Fraude Externo
	Daños a los Activos Físicos

C. EVENTOS DEL RIESGO

Se registrarán en los siguientes campos.

Tabla 12.

Componentes De La Tercera Sección De La Matriz De Evaluación Relacionado con los Eventos de Riesgo.

EVENTOS DE RIESGO	
TIPO DE RIESGO (Nivel 1)	**TIPO DE RIESGO (Nivel 2)**

Dónde:

- **TIPO RIESGO (NIVEL 1)**:

  Cada actividad será calificada en función de los 7 eventos de riesgo

Tabla 13.

Detalle General de los componentes de los eventos de riesgo

EVENTOS DE RIESGO (NIVEL 1)	
DEF.PRO	Deficiencias en ejecución y gestión de procesos y en las relaciones con proveedores y terceros
FRA.INT	Fraude interno
REL.LAB	Relaciones laborales y seguridad en el trabajo
PRACT	Practicas relacionadas con clientes, productos, negocio.
INT.NEG	Interrupciones en el negocio por fallas en los sistemas TICs.
FRA.EXT	Fraude externo
DAN.ACT	Daños a activos físicos

Para lo cual se debe tomar en cuenta las siguientes definiciones:

Fraude Interno

Pérdidas derivadas de: actuaciones encaminadas a defraudar, apropiarse de bienes indebidamente, o soslayar regulaciones, leyes o políticas empresariales, en las que se encuentre implicada una parte interna de la empresa.

Fraude Externo

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero

Relaciones laborales y seguridad en el trabajo

Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones.

Prácticas relacionadas con clientes, los productos y el negocio

Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto

Daños en Activos Físicos

Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales.

Deficiencias En La Ejecución De Los Procesos

Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

TIPO RIESGO (NIVEL 2):

Este nivel se asignará cumpliendo aspectos relacionados a los siguientes términos:

- Actividades no autorizadas:
    - Operaciones no reveladas (intencionalmente)
    - Operaciones no autorizadas (con pérdida pecuniaria)

- Hurto y Fraude:
    - Depósitos sin valor, falsificación, extorsión,
    - Malversación, robo, apropiación indebida de activos.

- Seguridad de la información:
    - Daños por ataques informáticos, robo de información

- Relaciones laborales:
    - Cuestiones relativas a remuneración, prestaciones
    - Sociales, extinción de contratos.

- Higiene y seguridad del trabajo:
    - Responsabilidad en general (resbalones, etc.)
    - Indemnización a los trabajadores

- Discriminación:
    - Separación de actividades

- Adecuación, divulgación de información y confianza
    - Abusos de confianza / incumplimiento de pautas
    - Aspectos de adecuación / divulgación de información

- Prácticas empresariales o de mercado improcedentes:
    - Manipulación del mercado
    - Abuso de información privilegiada - Blanqueo de dinero

- Productos defectuosos:
    - Error de los modelos

- Selección, patrocinio y riesgos:
    - Superación de los límites de riesgo frente a clientes

- Actividades de asesoramiento:
    - Litigios sobre resultados de las actividades de asesoramiento

- Desastres y otros:
    - Pérdidas por desastres naturales

- Acontecimientos:
    - Pérdidas humanas por causas externas (terrorismo, vandalismo)
- Sistemas:
    - Hardware, software,
    - Telecomunicaciones

- Recepción, ejecución y mantenimiento de operaciones:
    - Comunicación defectuosa
    - Errores de introducción de datos, mantenimiento o descarga

- Informes:
    - Incumplimiento de la obligación de informar bajo criterios de confianza, integridad y a tiempo.

- Documentación:
    - Inexistencia de autorizaciones / Documentos jurídicos inexistentes

- Gestión de cuentas de clientes:
    - Acceso no autorizado a cuentas
- Contrapartes comerciales:
    - Otros litigios con contrapartes distintas de clientes

- Distribuidores y proveedores Subcontratación:
    - Litigios con distribuidores

DETALLE DEL RIESGO:

En esta sección se definirá los posibles riesgos que se generen del proceso analizado.

D. FASE DE CAMPO

Aspectos a revisar: En este campo se realiza una descripción pequeña y general sobre el proceso a revisar.

Pruebas a realizar: Se realiza una descripción de las actividades a realizar para evaluar el proceso.

Resultados: Se registra la información obtenida en el proceso de investigación de campo.

Tabla 14.

Componentes De La Cuarta Sección De La Matriz De Evaluación Relacionado con la Fase Campo.

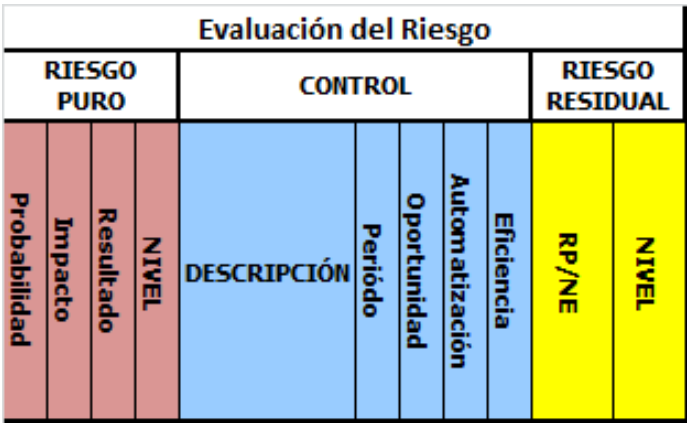
FASE DE CAMPO		
ASPECTO A REVISAR	**PRUEBAS A REALIZAR**	**RESULTADOS**

E. EVALUACIÓN DEL RIESGO

La evaluación del riesgo se basa en los principios generales del Riesgo Operativo y también en la normativa de riesgo Operativo de la Superintendencia de Bancos de Ecuador, evaluación que se debe realizar en los siguientes campos.

Tabla 15.

Componentes De La Quinta Sección De La Matriz De Evaluación Relacionado con la Evaluación del Riesgo Puro y Residual.



Dónde:

Riesgo puro: Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Probabilidad: Es la posibilidad de que el riesgo en evaluación ocurra.

Impacto: Son los efectos potenciales sobre los procesos evaluados.

Valor: Es un cálculo automático

Nivel: despliega un nivel de riesgo en base al valor obtenido del cálculo Probabilidad vs Impacto.

Descripción: Se registra el tipo de control con el que cuenta el proceso evaluado.

Periodo: Indica los periodos de tiempo en que se aplican los controles, en caso de que estos existan.

Oportunidad: Muestra el estado y efectividad de aplicación actual del control revisado y que valor da al monitoreo.

Nivel de automatización: Indica el nivel de evolución que tiene el control.

Nivel de eficiencia: calculo automático en base a los parámetros del control.

Riesgo residual: Son aquellos que representan la mayor probabilidad de ocurrencia y magnitud de impacto, después de considerar el efecto de los controles y los medios de mitigación

Es importante tomar en cuenta la información que se presenta a continuación, ya que esta permitirá tener un panorama más claro y amplio al momento de evaluar los controles. Se basan en situaciones particulares para cada evento dentro de la organización.

EVALUACIÓN DEL RIESGO

Descripción De La Sección Del Riesgo Puro

Guía para evaluar la Probabilidad

Tabla 16.

Detalle de Conceptos Relacionado con la Evaluación de la Probabilidad.

PROBABILIDAD	1 - Muy Improbable	2 - Improbable	3 - Moderado	4 - Probable	5 - Casi certeza
Frecuencia de ocurrencia	El evento es teóricamente posible pero nunca ha ocurrido en nuestra entidad	El evento ha ocurrido una vez durante el año	El evento se ha repetido hasta en tres meses durante el año	El evento se ha repetido hasta en seis meses durante el año	El evento se ha repetido en más de 6 meses durante el año
Posibilidad	Puede ocurrir en circunstancias excepcionales	Insignificante probabilidad de que el evento ocurra	Alguna posibilidad de que el evento ocurra	Posiblemente ocurra varias veces	Seguramente ocurrirá.
Probabilidad	Riesgo cuya probabilidad es muy baja. 1% al 25% de seguridad de que se presente	Riesgo cuya probabilidad de ocurrencia es baja. 26% al 50% de seguridad de que se presente	Riesgo cuya probabilidad es media. 51% al 75% de seguridad que se presente	Riesgo cuya probabilidad de ocurrencia es alta. 75% al 95% de seguridad de que se presente	Riesgo cuya probabilidad de ocurrencia es muy alta. La seguridad de que se presente tiende al 100%. Se tiene plena seguridad de que se presente

Guía para evaluar el Impacto

Tabla 17.

Detalle de Conceptos Relacionado con la Evaluación del Impacto.

IMPACTO	1 - No significativo	2 – Menor	3 - Moderado	4 - Mayor	5 - Extremo
Percepción de la magnitud de las pérdidas	Perdida o daño insignificante en el sector	Pérdida o daño menor en el sector	Pérdida significativa inusual en el sector	Pérdida o daño mayor inaceptable en el sector	Pérdida catastrófica en el sector
Necesidad de intervención por parte del organismo regulador	No hay reclamos de clientes ante el organismo regulador	Las quejas de clientes ante el organismo regulador van en aumento	Gran número de reclamos de los clientes ante el organismo regulador	Se abre investigación por parte del organismo regulador, hay sanciones	Obliga a intervención del organismo regulador, hay sanciones
Continuidad del negocio				El evento obliga a la activación de planes de continuidad	Los servicios del Banco dejan de funcionar por un período importante de tiempo o por tiempo indeterminado. Se puede

CONTINÚA ⟶

					producir la quiebra del Banco
Afectación al patrimonio	No se afecta el valor de las acciones	No afecta el valor de las acciones	Potencial pérdida del valor de las acciones. Pérdida importante en el patrimonio	Hay pérdida en el valor de las acciones. Daño significativo al patrimonio	Pérdida significativa en el valor de las acciones. Gran pérdida patrimonial
Objetivos	No afecta al logro de objetivos	Impacto menor en los objetivos es fácilmente remediable	Algunos de los objetivos son afectados	Algunos objetivos importantes no pueden ser alcanzados	La mayoría de los objetivos no se puede alcanzar
Esfuerzo de la Gerencia	Un evento cuyo impacto puede ser absorbido a través de las actividades normales directamente por los involucrados	Un evento cuyo impacto puede ser absorbido pero con el esfuerzo de la Gerencia responsable	Evento significativo puede ser manejado bajo circunstancias normales, puede requerir involucramiento de la alta gerencia	Un evento crítico que si es adecuadamente manejado puede ser sobrellevado, requiere una cantidad importante de tiempo de alta dirección e investigar y	Un evento desastroso con potencial a llevar una rápida reestructuración de la gerencia, de la

CONTINÚA ⟶

				corregir los daños	organización y de sus objetivos
Reputación e imagen	El evento solo es de conocimiento de los ejecutivos directamente involucrados. Sin efecto negativo en la imagen	El evento es de conocimiento general de la empresa. Leve efecto negativo en la imagen	El evento es de conocimiento a nivel local. Importante deterioro de la imagen	El evento es de conocimiento a nivel nacional. Deterioro significativo de la imagen	El evento de conocimiento a nivel internacional. Imagen completamente deteriorada
Afectación al recurso humano	Evento que no ocasionó lesiones con incapacidad hasta de 3 días	Evento que ocasionó incapacidad de 3 días a 1 mes.	Evento que ocasionó incapacidad de 1 mes hasta 3 meses	Evento que ocasionó incapacidad de 3 a 6 meses	Evento que ocasionó pérdida de vidas humanas o incapacidad permanente.

Interpretación de resultados de la evaluación del Riesgo Puro.

Tabla 18.

Detalle de la Valoración del Riesgo Puro

VALORACION RIESGO PURO					
IMPACTO / PROBABILIDAD	1 NO SIGNIFICATIVO	2 MENOR	3 MODERADO	4 MAYOR	5 EXTREMO
5 CASI CERTEZA	A	A	E	E	E
4 PROBABLE	M	A	A	E	E
3 MODERADO	B	M	A	E	E
2 IMPROBABLE	B	B	M	A	E
1 MUY IMPROBABLE	B	B	M	A	A

Dónde:

E = extremo

A = alto

M = medio

B = bajo

SECCION CONTROLES:

La información que se presenta en la tabla 20 hace referencia a los conceptos aplicados en cada uno de los criterios utilizados para evaluar los controles de cada evaluación.

Tabla 19.

Detalle de la Valoración del Control en los Campos de la Periodicidad, Oportunidad y Automatización.

VALORACION CONTROLES	
PERIODICIDAD	**DESCRIPCION**
PERMANENTE (PE)	Controles claves aplicados durante todo el proceso, es decir en cada operación
PERIODICO (PD)	Controles claves aplicados en forma constante solo cuando ha transcurrido un período específico de tiempo
OCASIONAL (OC)	Controles claves que se aplican solo en forma ocasional en un proceso

OPORTUNIDAD	DESCRIPCION
PREVENTIVO (PV)	Controles claves que actúan antes o al inicio del proceso
CORRECTIVO (CR)	Controles claves que actúan durante el proceso y que permiten corregir las deficiencias
DETECTIVO (DT)	Controles claves que solo actúan una vez que el proceso ha terminado

AUTOMATIZACION	DESCRIPCION
AUTOMATIZADO AL 100% (AT)	Controles claves incorporados en el proceso, cuya aplicación es completamente informatizada. Están incorporados en los sistemas
SEMI AUTOMATIZADO (SA)	Controles claves incorporados en el proceso, cuya aplicación es principalmente aplicada mediante sistemas informatizados
MANUAL (MA)	Controles claves incorporados en el proceso, cuya aplicación no considera uso de sistemas informatizados.

SECCION RIESGO RESIDUAL

Refleja el riesgo remanente una vez que se han evaluado los controles sobre el proceso evaluado, resultados que se muestran de manera automática

en base a los pesos dados en el riesgo puro y controles y que se interpretan en base a la siguiente tabla.

Tabla 20.

Detalle de Valores para Interpretación de los Resultados del Riesgo Residual.

INDICADOR DE EXPOSICION	VALOR	NIVEL DE EXPOSICION
NIVEL DE RIESGO RESIDUAL / NIVEL DE EFICIENCIA DEL CONTROL	8.0 - 25.0	EXTREMO
	4.0 - 7.99	ALTO
	3.0 - 3.99	MEDIO
	0.2 - 2.99	BAJO

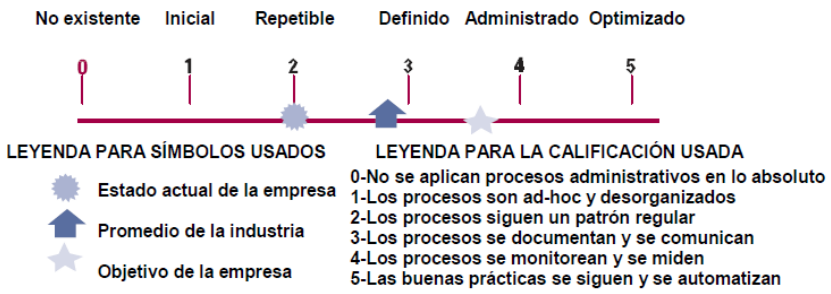
F. NIVEL DE MADUREZ

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Para la calificación del nivel de madurez se utiliza los criterios de Cobit 4.1.

Tabla 21.

Detalle de la Valoración del Nivel de Madurez según Cobit.

COBIT
NIVEL DE MADUREZ
3



Fuente: (COBIT, 2007)

G. OBSERVACIONES Y RECOMENDACIONES

En esta sección se debe registrar todos los hallazgos encontrados durante la evaluación así como también las posibles recomendaciones que se incluirán en el informe final.

4.4.1 GUÍA PARA INTERPRETACIÓN DE RESULTADOS

Posterior a la aplicación y evaluación de los procesos en el modelo propuesto, el auditor o evaluador tendrá la capacidad de obtener resultados mediante gráficas de diferentes tipos, mismos que permitirán interpretar la información de una manera interactiva y ágil, entre los resultados tenemos:

- Por nivel de riesgo
- Por factor de riesgo
- Por tipo de riesgo

Resultados Por Nivel de Riesgo:

1. **Por nivel de riesgo**

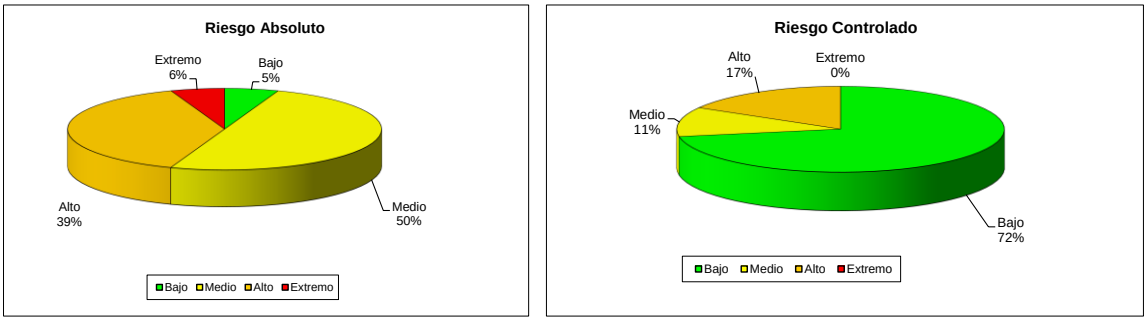


Figura 10. Resultados de la Matriz de Evaluación por su nivel de riesgo

Interpretación: las gráficas muestran el porcentaje de los riesgos agrupados por el nivel, con lo cual su puede validar rápidamente que tan

eficientes fueron los controles, resultado que se re refleja en el riesgo controlado. Así tenemos que en el riesgo absoluto tenemos un 6% del total evaluado en un riesgo externo sin embargo luego de evaluar el proceso y sus controles se pueden ver como desparecen los riesgos extremos.

Resultados Por Factor de Riesgo:

2. Por factor de riesgo

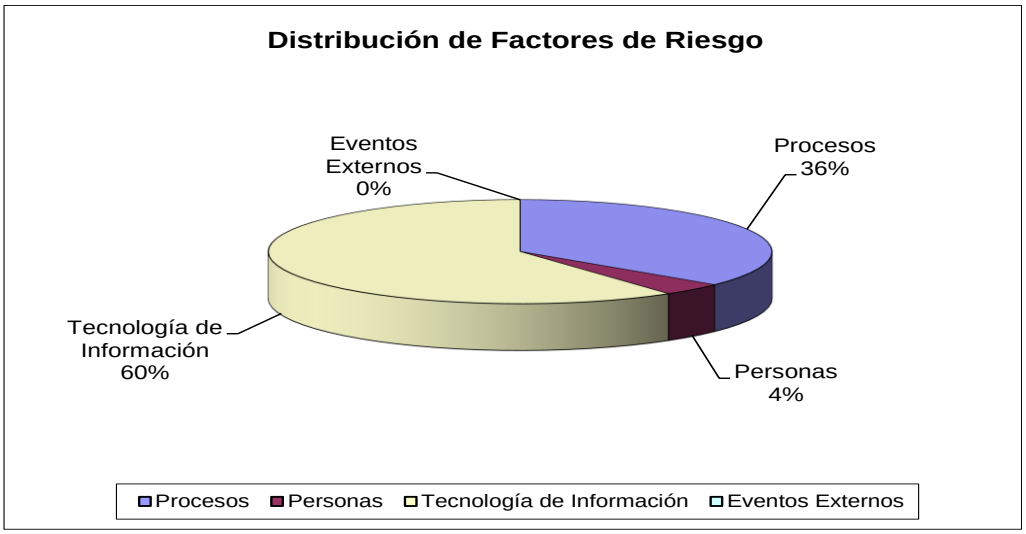


Figura 11. Resultados de la Matriz de Evaluación por Factores de Riesgo

Interpretación: la gráfica muestra de manera agrupada en cuál de los 4 factores de riesgo se concentra las deficiencias evaluadas. Así tenemos que las deficiencias del proceso evaluado se concentran en el factor tecnología con un 60%.

Resultados Por Tipo de Riesgo:

3. Por tipo de riesgo

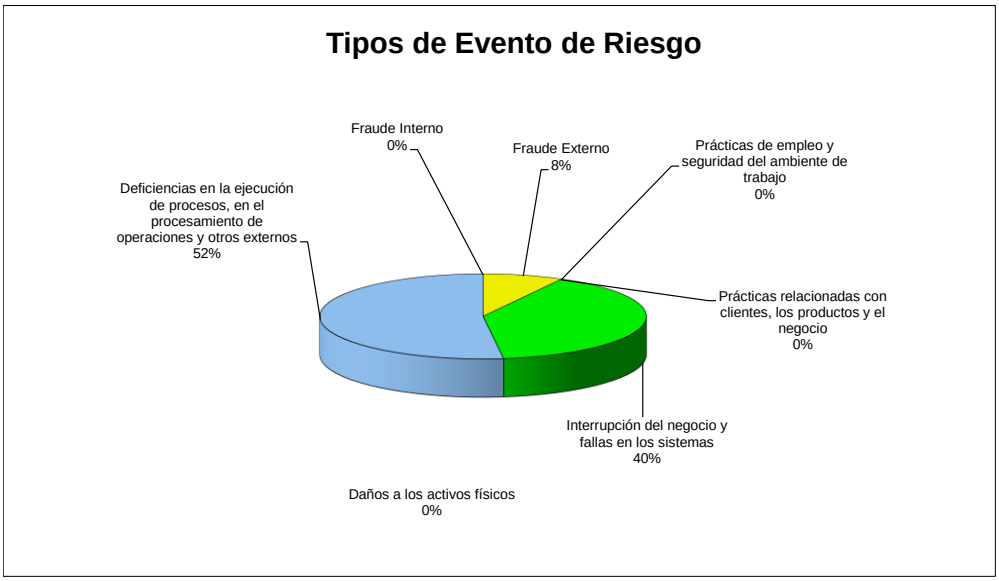


Figura 12. Resultados de la Matriz de Evaluación por Tipos de Riesgo

Interpretación: la gráfica muestra los resultados obtenidos de la sección Tipo de riesgo (Nivel 1) que se encuentra en el campo 3 de la matriz de evaluación.

4.5 APLICACIÓN PRÁCTICA DE LA MATRIZ DE EVALUACIÓN SOBRE UN PROCESO PARA MEDIR NIVEL DE EFECTIVIDAD.

A continuación se presenta la matriz de evaluación propuesta en un proceso real (Revisión Al Manejo De Monitoreo Centralizado Y Manejo De Incidentes) mediante la aplicación de técnicas de investigación para el levantamiento de información y Cobit 4.1 para su respectiva evaluación.

4.6 INTERPRETACIÓN DE RESULTADOS Y PRESENTACIÓN DE INFORME FINAL DE AUDITORIA.

Los resultados obtenidos de la matriz de evaluación en el proceso (Revisión Al Manejo De Monitoreo Centralizado Y Manejo De Incidentes) son los siguientes.

Por Nivel De Riesgo

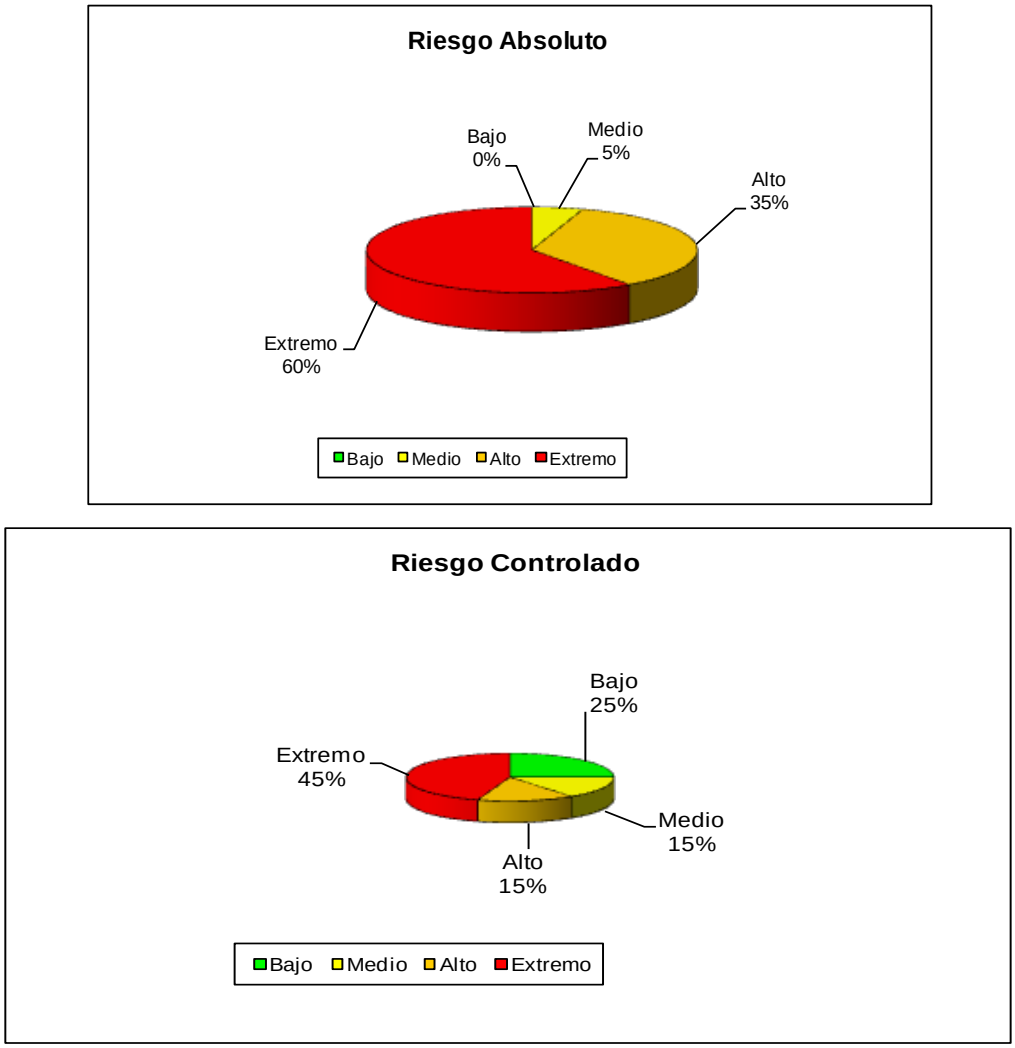


Figura 13. Resultados de la Matriz de Evaluación por Nivel de Riesgo

Interpretación: Estas graficas permiten validar rápidamente que tan eficientes fueron los controles implementados en el proceso evaluado, resultado que se refleja en el riesgo controlado. Así tenemos que los resultados mostrados en el riesgo controlado son favorables ya que se puede ver claramente un incremento en los niveles medio y bajo aspecto que indica la existencia de controles, sin embargo el porcentaje del riesgo absoluto a nivel extremo sigue alto por lo que es necesario centrar esfuerzos en disminuir este particular.

Por Factor De Riesgo

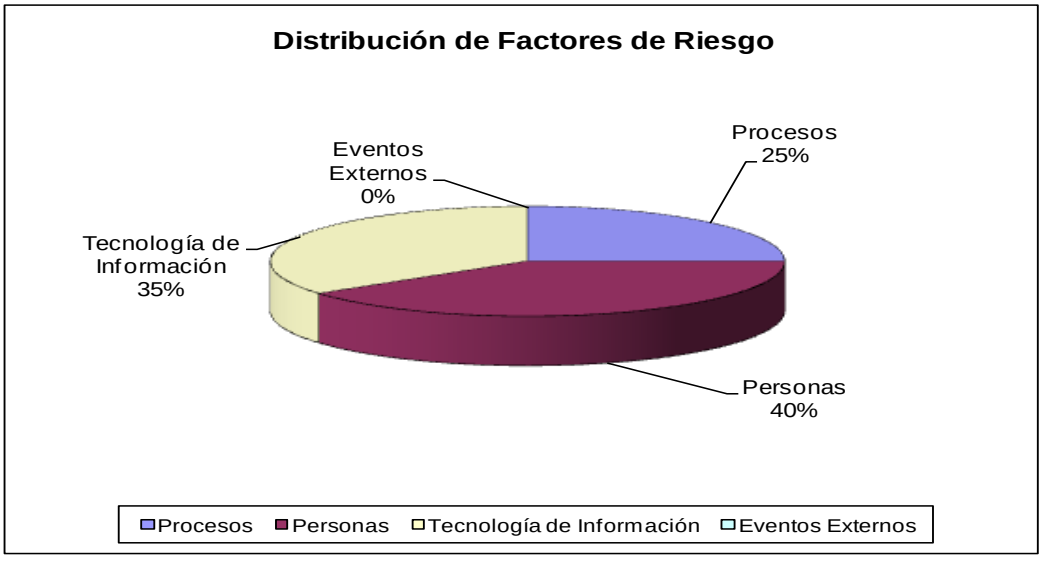


Figura 14. Resultados de la Matriz de Evaluación por Factor de Riesgo

Interpretación: de acuerdo a la información revisada se puede ver claramente que las deficiencias encontradas en este proceso se dan principalmente por falta de controles a nivel de personal, procesos que no están definidos claramente y al nivel de tecnología con la que cuenta actualmente la institución, la cual aún no está preparada para soportar la implementación de lo que requiere PCI.

Por Evento De Riesgo

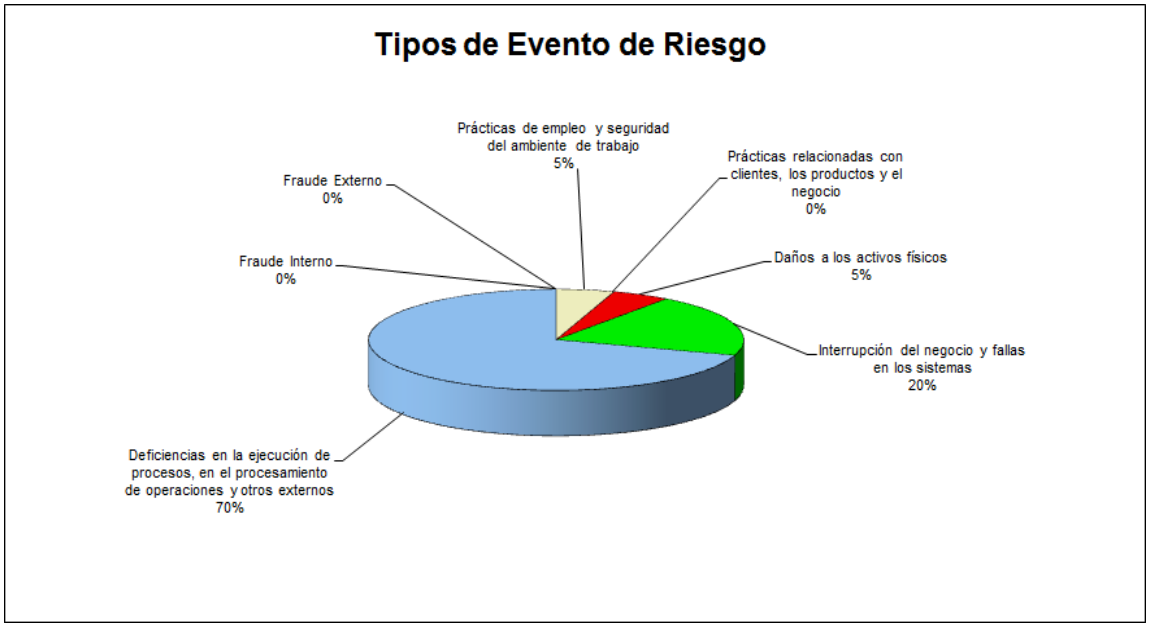


Figura 15. Resultados de la Matriz de Evaluación por Evento de Riesgo

Interpretación: Esta gráfica muestra claramente que la deficiencia en la ejecución de procesos y la posible interrupción del negocio por fallas en los sistemas son los principales eventos que se podrían presentar actualmente al no contar con lo requerido con PCI – DSS, aspectos que se tienen que ir cubriendo conforme avance el proyecto y las implementaciones de seguridad.

4.6.1 PRESENTACIÓN DEL INFORME

La parte final de la evaluación es presentación de un informe formal de auditoria que permita recoger los hallazgos y las recomendaciones que se levantaron de acuerdo a los resultados de la matriz de evaluación.

CAPÍTULO V

5.1 CONCLUSIONES Y RECOMENDACIONES

De acuerdo al análisis realizado en el presente documento, se derivan las siguientes conclusiones y recomendaciones, mismas que es importante tomar en cuenta para una mejor implementación de los controles.

CONCLUSIONES

- Es imperativo tener claro el alcance de la normativa de acuerdo al giro del negocio y el alcance sobre qué aspectos se desea dar atención.
- La administración de la organización debe exigir implementar controles de seguimiento periódicos al cumplimiento de la normativa PCI-DSS a las diferentes áreas de control.
- Establecer políticas que normen la ejecución de revisiones de cumplimiento y la difusión de los resultados encontrados.

RECOMENDACIONES

- Las instituciones deberán solicitar asesoría profesional para entender la normativa y como esta se aplica a cada uno de los negocios y sus ambientes
- Como parte de las buenas practicas la institución deberá ejecutar un análisis preliminar de cumplimiento de la normativa, lo cual permitirá conocer el estado actual de la empresa y manejar un horizonte real frente a las brechas encontradas
- La institución debe generar las políticas y procedimientos necesarios que permitan normar todas las actividades de Seguridad que permitan mantener la certificación PCI-DSS.

BIBLIOGRAFÍA

a2secure. (2015). *a2secure*. Obtenido de http://www.a2secure.com/es/pci/faq

Andrés Naveda Paredes, E. G. (2013). *EVALUACIÓN TÉCNICA INFORMÁTICA DEL SISTEMA DEINFORMACIÓN DE LA CORPORACIÓN HOLDINGDINE S.A. (MATRIZ), UTILIZANDO EL ESTÁNDAR INTERNACIONAL COBIT.* Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/5239/2/T-ESPE-033151-A.pdf

apuntesacercadetarjetasdecrditoydbito. (2010). *Estándar PCI*. Obtenido de http://apuntesacercadetarjetasdecrditoydbito.blogspot.com/2010/09/el-estandar-pci-dss-obligatorio-en.html

Arbesú, L. P. (2012). *Pcworld*. Obtenido de http://www.pcworld.com.mx/Articulos/25950.htm

ATCA. (2015). *Integrar Seguridades con PCI*. Obtenido de www.isecauditors.com/sites/default/files/files/como-integrar-PCI-DSS_Pedro_Sanchez-ATCA.pdf

Avisortech. (2015). *Auditoría y certificación PCI DSS*. Obtenido de http://www.avisortech.com/pci_dss_compliance.htm

Bancard. (2004). *Política.* Obtenido de https://www.bancard.com.py/institucional/jsp/subpage2.jsp?pagid=1&subpagid=86

Bento, A. (2010). *Las normas PCI DSS protegerán al ciudadano del uso indebido de su tarjeta*. Obtenido de http://www.redseguridad.com/tecnologia/certificaciones-y-formacion/las-normas-pci-dss-protegeran-al-ciudadano-del-uso-indebido-de-su-tarjeta

Carlosama, D. (2015). *FACTORES DEL CONTROL INTERNO.* Obtenido de https://prezi.com/-t3bui1d8ejv/factores-del-control-interno/

COBIT. (2007). Marco de Referencia COBIT 4.1. En *COBIT 4.1* (pág. 29).

controlcase. (2015). *Certificación y Cumplimiento PCI*. Obtenido de http://www.controlcase.com/es/pci_certification.html

David Acosta CISSP, C. C. (2015). *PCI hispano*. Obtenido de http://www.pcihispano.com/pci-dss-y-pa-dss-v3-0-disponibles-en-espanol/

Discover. (2015). *Fraud & Security*. Obtenido de http://www.discovernetwork.com/merchants/fraud-protection/

E.Security, N. (2011). *Las empresas que cumplen con los requerimientos PCI DSS sufren menos violaciones de datos*. Obtenido de http://seguridad-informacion.blogspot.com/2011/05/las-empresas-que-cumplen-con-los.html

ecommerce. (2015). *PCI - Información Sensible*. Obtenido de http://www.ecommerce.com.do/que-es-pci-dss/

es.pcisecuritystandards.org. (2015). *cerca del PCI Security Standards Council*. Obtenido de https://es.pcisecuritystandards.org/minisite/en/about.php

fccea.unicauca.edu.co. (2003). *COMPONENTES DEL CONTROL INTERNO.* Obtenido de http://fccea.unicauca.edu.co/old/tgarf/tgarfse88.html

gobiernotic. (2006). *La madurez como prerrequisito para IT Governance*. Obtenido de http://www.gobiernotic.es/2006/10/la-madurez-como-prerrequisito-para-it.html

González, J. (2014). *Gestión del Riesgo.* Obtenido de https://prezi.com/ywwu7oscvaug/coso-ii-salon-215/

Hernández, A. (2009). *Seguridad de Datos en Tarjetas de Pago*. Obtenido de http://www.revistadintel.es/Revista1/DocsNum29/Normas/Hernandez.pdf

http://saladeprensabg.com. (2012). *Banco de Guayaquil primer banco en recibir certificación PCI-DSS.* Obtenido de http://saladeprensabg.com/boletin/banco-de-guayaquil-primer-banco-en-recibir-certificacion-pci-dss/

http://www.auditool.org. (2014). *http://www.auditool.org.* Obtenido de http://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual

http://wwwisis.ufg.edu.sv. (2012). *http://wwwisis.ufg.edu.sv.* Obtenido de http://wwwisis.ufg.edu.sv/wwwisis/documentos/TEFLIP/657.458-M722m/files/assets/downloads/page0071.pdf

Ing Mario Ron, I. W. (2014). *ANALISIS FORENSE A PAQUETES DE DATOS EN LA RED LAN DE LA UNIVERSIDAD TECNOLOGIA EQUINOCCIAL COMO APORTE AL CUMPLIMIENTO DE LAS NORMAS PCI-DSS.* Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/9038/1/AC-MEVAST-ESPE-048298.pdf

isecauditors. (2015). *Implantación y Certificación PCI.* Obtenido de http://www.isecauditors.com/implantacion-pci-dss

Jimenez, J. J. (2011). *OWASP y el cumplimiento normativo PCI.* Obtenido de http://es.slideshare.net/jjriderwul4/infosecure-2011-owasp-y-cumplimiento-normativo-pcidss-y-padss

Malica, w. -C. (2012). *El sistema de control interno y su importancia en la auditoría.* Obtenido de http://www.facpce.org.ar:8080/iponline/el-sistema-de-control-interno-y-su-importancia-en-la-auditoria/

Martínez, E. (2015). *www.elfinanciero.com.mx*. Obtenido de 5 mil fraudes al día flagelan a usuarios: http://www.elfinanciero.com.mx/economia/mil-fraudes-al-dia-flagelan-a-usuarios-de-tarjetas-de-credito.html

MasterCard. (2015). *ite Data Protection and PCI*. Obtenido de http://www.mastercard.com/us/sdp/

MaweLearn. (2010). *TIPO DE INVESTIGACIÓN.* Obtenido de https://mawelearn.wordpress.com/category/metodologia-de-investigacion/

MAZA, G. P. (2015). *DISEÑO DEL SISTEMA DE CONTROL INTERNO MEDIANTE EL METODO COSO II PARA PRONTOCASA CONSTRUCCIONES CIA LTDA.* Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/7763/1/UPS-CT004619.pdf

Mexico, C. d. (2004). *Control Interno.* Obtenido de http://www.ccpm.org.mx/avisos/boletines/boletinauditoria3.pdf

nakedsecurity. (2015). *Fundamentos de seguridad: ¿Qué es PCI DSS?* Obtenido de https://nakedsecurity.sophos.com/es/2014/03/17/security-essentials-what-is-pci-dss/

PayPal. (2015). *Cumplimiento PCI DSS: Pagos en el sitio Web*. Obtenido de https://www.paypal.com/ec/cgi-bin/webscr?cmd=xpt/Marketing/merchant/PCIComplianceDSS-outside

PCI, I. a. (2012). *securityartwork*. Obtenido de http://www.securityartwork.es/2012/12/17/introduction-to-pci-dss-payment-card-industry-data-security-standard/

PCI-DSS. (2015). *PCI SSC Data Security Standards Overview*. Obtenido de https://es.pcisecuritystandards.org/security_standards/

pcisecuritystandards.org. (2015). *PCI-DSS.* Obtenido de https://es.pcisecuritystandards.org

Priscila Balcazar. CISA, C. y. (2010). *Todo Sobre PCI*. Obtenido de http://www.magazcitum.com.mx/?p=590#.VbbZs-N5Ntk

Rangel, N. I. (2013). *Juicios Deductivos e Inductivos, Metodos de Investigación.* Obtenido de https://sites.google.com/site/fisicacbtis162/home/juicios-deductivos-e-inductivos-metodos-de-investigacion-cientifico-y-cientifico-experimental

RANGEL, N. I. (2014). *sites.google.com.* Obtenido de JUICIOS DEDUCTIVOS E INDUCTIVOS, METODOS DE INVESTIGACION: https://sites.google.com/site/fisicacbtis162/home/juicios-deductivos-e-inductivos-metodos-de-investigacion-cientifico-y-cientifico-experimental

searchsecurity.techtarget. (2012). *PCI Security Standards Council*. Obtenido de http://searchsecurity.techtarget.com/definition/PCI-Security-Standards-Council

seguridaddeinformacionenlastel.blogspot.com. (2014). *PCI Security Standards Council* . Obtenido de http://seguridaddeinformacionenlastel.blogspot.com/p/pci-security-standards-council.html

Sia. (2014). *Conformidad con PCI DSS.* Obtenido de http://www.sia.es/images/06-Folleto%20Comercial%20-%20Servicios%20PCI-DSS_v2.1.pdf

SOPHOS. (2015). *Control y cumplimiento del estándar PCI .* Obtenido de https://www.sophos.com/es-es/security-news-trends/security-trends/pci-compliance.aspx

strategoscs. (2015). *La Norma de Seguridad de la Industria de Tarjetas de Pago – PCI DSS y Reglamento de Tarjetas de Débito y Crédito.* Obtenido de http://strategoscs.com/pci-dss/pci-dss-reglamento-de-tarjetas-de-credito-y-debito/

Torres, M. Á. (2010). *http://www.isecauditors.com.* Obtenido de http://www.isecauditors.com/sites/default/isecauditors.com/files//files/SIC92_pci-dss%20v2-maduracion-estandar.pdf

uovirtua. (2014). *DISEÑO DE LA INVESTIGACIÓN.* Obtenido de http://www.uovirtual.com.mx/licenciatura/lecturas/metder/15.pdf

Visa. (2015). *PCI-DSS*. Obtenido de https://www.visaeurope.com/receiving-payments/security/

welivesecurity. (2015). *El consejo de PCI actualiza los estándares de cifrado*. Obtenido de http://www.welivesecurity.com/la-es/2015/07/02/consejo-pci-actualiza-estandares-cifrado/

www.403labs.com. (2015). *Salvaguarde los datos de tarjetas de pago correctamente.* Obtenido de http://www.403labs.com/es/compliance/pcidss

www.eluniverso.com. (2013). *Bancos pagaron a clientes en 2 mil casos de fraude virtual.* Obtenido de http://www.eluniverso.com/noticias/2013/11/26/nota/1821096/bancos-pagaron-clientes-2-mil-casos-fraude-virtual

www.forbes.com.mx. (2015). *40% de las tarjetas de crédito son víctimas de fraude*. Obtenido de http://www.forbes.com.mx/40-de-las-tarjetas-de-credito-son-victimas-de-fraude/

www.gestiopolis.com. (2014). *Gobierno Corporativo (Corporate Governance) y Administración de riesgo empresarial o E.R.M.* Obtenido de http://www.gestiopolis.com/gobierno-corporativo-corporate-governance-administracion-riesgo-empresarial-erm/

www.imperva.com. (2015). *PCI DSS Compliance.* Obtenido de http://www.imperva.com/Resources/PCIDSS

www.isaca.org. (2011). *Mapeo PCI-DSS vs Cobit 4.1.* Obtenido de http://www.isaca.org/Journal/archives/2011/Volume-2/Pages/Mapping-PCI-DSS-v20-With-COBIT41.aspx

www.isaca.org. (2011). *Mapping PCI DSS v2.0 to COBIT 4.1 .* Obtenido de http://www.isaca.org/knowledge-center/documents/mapping-pci-dss-v2.0-with-cobit-4.1.pdf

www.isaca.org. (2014). *Cobit.* Obtenido de http://www.isaca.org/spanish/Pages/default.aspx

www.paymentmedia.com. (2012). *Credimatic- Empresa Certificada PCI.* Obtenido de http://www.paymentmedia.com/news-219-guillermo-vela-gerente-general-de-credimatic.html

www.pcisecuritystandards.org. (2014). *QSA Companies.* Obtenido de www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

www.portal.banred.fin.ec. (s.f.). *BANRED - PCI.* Obtenido de http://www.portal.banred.fin.ec/images/stories/banred_noticias/Seguridad/itn-012011-004pcidss.pdf

www.procard.com.py. (2014). *Certificación PCI.* Obtenido de https://www.procard.com.py/contenido.php?id=33

www.sbs.gob.ec. (2015). *SBS aclara sobre el manejo de Tarjetas de Crédito .* Obtenido de http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=4144&vp_tip=1&vp_imp=1

www.telegrafo.com.ec. (2013). *Instituciones financieras deben mitigar el riesgo de fraude informático.* Obtenido de http://www.telegrafo.com.ec/economia/item/tarjetas-de-credito-deben-llevar-chip.html.