METODOLOGÍA DE AUDITORÍA PARA VERIFICAR EL NIVEL DE CUMPLIMIENTO DEL PROCESO DE DESARROLLO DE SOFTWARE FRENTE A LOS REQUISITOS DE LA NORMA PCI DSS EN LA COMPAÑÍA ABPS

JAVIER ALFONSO SARMIENTO PIÑEROS

RICHARD MAURICIO SANABRIA BELLO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN

BOGOTÁ D.C – 2018

METODOLOGÍA DE AUDITORÍA PARA VERIFICAR EL NIVEL DE CUMPLIMIENTO DEL PROCESO DE DESARROLLO DE SOFTWARE FRENTE A LOS REQUISITOS DE LA NORMA PCI DSS EN LA COMPAÑÍA ABPS

JAVIER ALFONSO SARMIENTO PIÑEROS

RICHARD MAURICIO SANABRIA BELLO

Trabajo de grado para obtener el título de especialista en auditoría de Sistemas de información.

ASESOR: JUAN CARLOS BLANCO

INGENIERO DE SISTEMAS

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN

BOGOTÁ D.C – 2018

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D.C., junio de 2018.

Agradecimientos

Damos agradecimiento a nuestros maestros y a nuestro coordinador de la Especialización de Auditoria de Sistemas de Información Jaime Fernando Pérez González, por sus recomendaciones, enseñanzas y valiosos aportes, relacionados con nuestro proyecto.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

ABPS desea incursionar en la prestación de servicios al sector financiero por lo que actualmente está interesada en verificar el nivel de cumplimiento de uno de sus procesos más importantes como lo es el desarrollo de software, para lo que requiere identificar los requisitos de la norma PCI DSS que debe cumplir, al realizar esta verificación de cumplimiento lograra identificar las fortalezas y debilidades del proceso.

El desarrollo de una metodología de auditoria que permita identificar y mantener el nivel de cumplimiento de la norma PCI DSS al interior de ABPS busca asegurar que su proceso de desarrollo de software cumpla con los estándares exigidos por el mercado frente a la adecuada construcción de las aplicaciones que se utilizaran para prestar servicios a clientes del sector financiero que así lo requieran.

Para asegurar el cumplimiento de cada uno de los requisitos de la norma se hace necesario llevar a cabo verificaciones periódicas al proceso frente a la adecuada ejecución de cada uno de los controles solicitados, por lo que la implementación de la guía de verificación de cumplimiento será un instrumento muy importante que le permitirá al auditor contar con una herramienta adecuada para validar cada uno de los requisitos exigidos y determinar el nivel de cumplimiento que tiene el proceso frente a dichos requisitos.

Todo esto con el propósito de identificar a tiempo las posibles fallas que se puedan estar cometiendo y que pongan en riesgo las operaciones del negocio, de esta manera se podrán implementar en el proceso de desarrollo de software los planes de mejoramiento requeridos que permitan asegurar la adecuada prestación de los servicios ofrecidos.

Palabras clave:

Auditoria, Gestión de Riesgo, Metodología de Auditoria, PCI DSS, Seguridad de la Información

ABSTRACT

ABPS wants to venture into the provision of services to the financial sector so it is currently interested in verifying the level of compliance with one of its most important processes such as software development, for which it requires identifying the requirements of the PCI DSS standard that it must comply with, when carrying out this verification of compliance, it will be able to identify the strengths and weaknesses of the process.

The development of an audit methodology that allows to identify and maintain the level of compliance with the PCI DSS standard within ABPS seeks to ensure that its software development process complies with the standards required by the market against the proper construction of applications. that will be used to provide services to clients of the financial sector that require it.

To ensure compliance with each of the requirements of the standard it is necessary to carry out periodic checks on the process against the proper execution of each of the requested controls, so that the implementation of the compliance verification guide will be a very important instrument that will allow the auditor to have an adequate tool to validate each of the requirements and determine the level of compliance that the process has with respect to these requirements.

All this with the purpose of identifying in time the possible failures that may be committing and that put at risk the operations of the business, in this way the improvement plans required to ensure the adequate can be implemented in the software development process. provision of the services offered.

Keywords:

Audit, Risk Management, Audit Methodology, PCI DSS, Security of the Information

INTRODUCCIÓN

Actualmente las organizaciones que proveen servicios de tecnología requieren disponer de una gestión de servicios efectiva para cumplir las necesidades de sus clientes, pero también las internas. Para estas organizaciones no solo es suficiente invertir en tecnología. También se debe considerar la calidad de los servicios que proporcionan a sus clientes, donde cada vez se hace más importante e indispensable poseer sistemas de seguridad de la información adecuados, donde se hace necesaria una correcta gestión de estos sistemas (Mesquida, 2009).

Toda organización tiene objetivos, por lo general relacionados con el mercado, los negocios y servicios en tecnología, que requieren afinar sus procesos de operaciones hasta las políticas de uso de recursos, que sean definidos a un nivel general y de manera confiable. Si bien gran parte de la información se vincula con computadoras y redes, hay otra parte que no se representa en forma de bits, sino por ejemplo en papeles, en la memoria de las personas, en el conocimiento y experiencia de la organización misma, en la madurez de sus procesos entre otros. En ambos casos, la información debe ser protegida de manera diferente y aquí entra en juego un SGSI[1] (Pacheco, 2010).

ABPS es una empresa que se dedica a prestar servicios de Contact Center, por lo que cuenta con diferentes clientes públicos y privados. Como promesa de valor se compromete a implementar

[1] Sistema de Gestión de la Seguridad de la Información (en inglés: information security management system, ISMS)

y mantener controles que le permitan garantizar el adecuado aseguramiento de la información que se transmite, procesa y gestiona al interior de sus procesos.

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) o PCI DSS fue 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 evitar los fraudes que involucran tarjetas de pago débito y crédito.

Las 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[2]. Los Comerciantes y proveedores de servicios de tarjetas de crédito y débito, deben validar su cumplimiento al estándar en forma periódica. Esta validación es realizada por auditores autorizados Qualified Security Assessor (QSAs).

Para proveer y gestionar de forma eficaz los servicios ofrecidos, resulta determinante definir y adoptar un conjunto de buenas prácticas. En este sentido, desde hace seis años se encuentra certificada en la norma ISO 27001:2013 por lo que se diseñaron e implementaron, metodologías, normas, políticas, procedimientos, controles y buenas prácticas que permiten mantener la confidencialidad, integridad y disponibilidad de la información de manejo interno en la compañía y la de sus clientes.

A través de las auditorias ABPS tiene la oportunidad para identificar si sus procesos actualmente se están desarrollando de manera adecuada de acuerdo a los estándares de eficiencia

[2] In Data Leaks, Culprits Often Are Mom, Pop - WSJ.com

y eficacia exigidos por diferentes normas que son requeridas por múltiples clientes en el mercado nacional e internacional con el propósito de asegurar la calidad en la gestión de sus procesos bajo la implementación de diferentes estándares que les permitan controlar la adecuada prestación del servicio a sus clientes.

ABPS actualmente quiere certificarse en la norma PCI DSS y desea conocer el nivel de cumplimiento que tiene el proceso de desarrollo de software frente a esta norma, con el propósito de llevar a cabo los cambios que requiera el proceso para dar cumplimiento al estándar y de esta manera llevar a cabo el desarrollo seguro de aplicaciones realizadas para los clientes que demanden contar con un servicio certificado bajo esta norma, todo esto con el objetivo de incursionar en el sector financiero para lograr buscar nuevas oportunidades de negocio.

El presente documento en su apartado “Desarrollo” contiene una revisión detallada de los requisitos que debe satisfacer el proceso de desarrollo de software de ABPS frente a la norma PCI DSS, partiendo de un análisis y valoración de riesgos, que permite identificar aquellos que representan un mayor impacto para la organización.

Paso seguido, se propone el diseño y aplicación de una guía de auditoria que permita determinar el nivel de cumplimiento que tiene el proceso para llevar a cabo el desarrollo seguro de aplicaciones solicitadas por clientes del sector financiero.

1 GENERALIDADES DEL TRABAJO DE GRADO

1.1 LÍNEA DE INVESTIGACIÓN

Por el contexto en el que se desarrolla este trabajo de investigación el cual parte de la necesidad y oportunidad de establecer y conocer el nivel de cumplimiento del proceso de desarrollo de software de ABPS frente al estándar PCI DSS mediante el diseño de una metodología de auditoria, se determina que la anterior temática se relaciona con la línea de investigación de "software inteligente y convergencia tecnológica" avalada por la Universidad Católica de Colombia, toda vez que al realizar este estudio permitirá que ABPS pueda analizar, gestionar, proteger y mejorar las condiciones actuales en materia de desarrollo de software para clientes del sector financiero.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 Antecedentes del problema

ABPS se dedica a prestar servicios de Contact Center, por lo que cuenta con diferentes clientes públicos y privados. Como promesa de valor se compromete con sus clientes a implementar y mantener controles que le permitan garantizar el adecuado aseguramiento de la información que se transmite, procesa y gestiona al interior de sus procesos, de igual forma para los diferentes sistemas de información dispuestos para atender los requerimientos de sus clientes y de la compañía.

Actualmente la compañía quiere certificarse en la norma PCI DSS, esta norma es un estándar de seguridad de datos para la industria de tarjeta de pago, esto con el propósito de atraer nuevos clientes del sector financiero, para lograr este objetivo debe realizar un esfuerzo significativo en el mejoramiento de su proceso de desarrollo de software el cual juega un papel muy importante a la hora de llevar a cabo el desarrollo de aplicaciones hechas a la medida para los clientes del sector financiero.

Teniendo en cuenta las características del negocio, los requerimientos de los clientes y el fortalecimiento de uno de sus procesos más importantes, como es el de desarrollo de software, se hace necesario evaluar, analizar y determinar el nivel de cumplimiento de este proceso frente a los requisitos exigidos por la norma PCI DSS dado que si la compañía desea incursionar en el sector financiero debe estar preparada para afrontar este nuevo reto que le exigirá fortalecer sus procesos más importantes para brindar un mejor servicio a sus clientes con estándares de calidad y seguridad internacionales lo que le permitirá incursionar en nuevos mercados y fidelizar los clientes actuales.

1.2.2 Pregunta de investigación

¿Cómo es posible identificar el nivel de cumplimiento del proceso de desarrollo de software frente a los requisitos de la norma PCI DSS?

1.3 JUSTIFICACIÓN

Frente a lo expuesto en el planteamiento del problema y la estructuración de la pregunta de investigación y con el objeto de dar respuesta a la misma, es viable la realización de este proyecto, debido a que la compañía busca incursionar en el sector financiero por lo que se hace necesario fortalecer el proceso de desarrollo de software por lo que se debe conocer el nivel de cumplimiento del proceso frente a los requisitos de la norma PCI DSS.

Para la revisión y evaluación del nivel de cumplimiento según la norma PCI DSS la cual es obligatoria para cada uno de los proveedores que prestan servicios al sector financiero, mercado en el cual desea incursionar ABPS. Se propone la metodología de auditoria contenida en este documento, la cual como aspecto diferenciador hace un especial énfasis en el análisis y valoración de los riesgos, y deja de lado el enfoque enteramente de control interno.

Tabla 1-1. Matriz de comparación paradigmas de auditoria. Fuente: Técnicas y herramientas asistidas por computador – la auditoria continua vs la auditoria tradicional

CARACTERISTICAS	PARADIGMA TRADICIONAL	NUEVO PARADIGMA
Foco de la auditoria interna	Control interno.	Riesgos del negocio
Respuesta de la auditoria interna	Reactiva, después de los hechos, discontinua, observadora de las iniciativas del plan estratégico.	Proactiva, en tiempo real, monitoreo continuo, participante de los planes estratégicos.
Evaluación de riesgos	Factores de Riesgo.	Planeamiento de escenarios.
Pruebas de auditoria	Controles importantes.	Riesgos importantes.
Métodos de auditoria	Énfasis en las pruebas de control.	Énfasis en la importancia y el alcance del cubrimiento de los riesgos del negocio.
Recomendaciones de auditoría	Control interno: fortalecimiento, costo / beneficio, eficiencia / eficacia.	Gestión de riesgos: evitar / diversificar el riesgo, compartir / transferir el riesgo, controlar / aceptar el riesgo.
Informes de auditoría	Centrados en los controles funcionales.	Centrados en los riesgos de los procesos.

Papel del auditor interno en la organización	Función de evaluación independiente.	Integración de la gestión de riesgos al gobierno de la organización.

Actualmente la Gerencia de Tecnología (Figura 1), se encuentra soportada por 4 procesos, de los cuales el proceso que vamos a evaluar es el desarrollo de software, como se muestra en la Figura 1., proceso que está a cargo de la dirección de desarrollo de aplicaciones, quien tiene a su cargo dos jefaturas, una se encarga del desarrollo de aplicaciones administrativas que tiene a cargo 4 ingenieros de desarrollo de software y otra que se encarga del desarrollo de aplicaciones operativas para clientes que tiene a cargo 23 ingenieros de software, a continuación, se da a conocer el organigrama actual de la Gerencia de Tecnología de la compañía, que tiene a cargo el proceso de desarrollo de software:

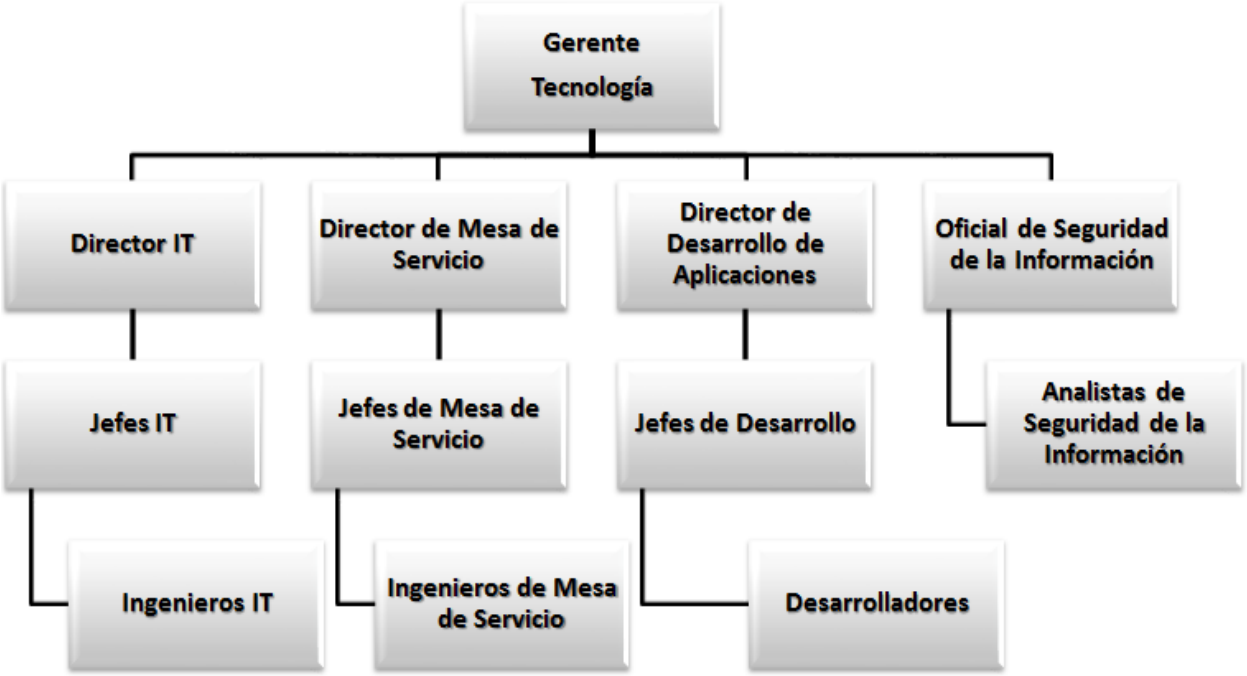

Figura 1-1. Organigrama Gerencia de Tecnología. Fuente: Elaboración propia

1.4 OBJETIVOS

1.4.1 Objetivo general

Diseñar una metodología de auditoria para verificar el nivel de cumplimiento de la norma PCI DSS en el proceso de desarrollo de software en la compañía ABPS.

1.4.2 Objetivos específicos

Identificar los requerimientos de cumplimiento asociados a la norma PCI DSS para el proceso de desarrollo de software.

Realizar un análisis de riesgos al proceso de desarrollo de software en relación con los requisitos aplicables de la norma PCI DSS.

Elaborar una guía de auditoria que permita verificar el nivel de cumplimiento del proceso de desarrollo de software frente a la norma PCI DSS.

2 MARCOS DE REFERENCIA

2.1 OWASP (PROYECTO DE SEGURIDAD DE APLICACIONES WEB ABIERTAS).

Es un proyecto apoyado por la fundación OWASP[3], su actividad principal es la identificación y supresión de las causas que llevan a que un producto de software sea inseguro o vulnerable.

En la comunidad OWASP se cuentan instituciones educativas y particulares de diversos puntos en todo el mundo; su objetivo es la producción de artículos, documentación, metodologías y herramientas tecnológicas que luego son liberadas para que cualquier persona u organización pueda hacer uso de ellas.

Algunos de los productos más exitosos del proyecto son las guías OWASP, útiles en la medida en que proveen una base de conocimiento para la seguridad y estabilidad de aplicaciones. La referencia de escritorio en seguridad de aplicaciones OWASP[4], desarrollo OWASP[5], de pruebas OWASP[6] y de revisión de código OWASP[7], son cuatro guías que funcionan de manera conjunta con parámetros bien definidos para identificar las posibles vulnerabilidades a las que se expone un producto de software en la web.

[3] Organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP.

[4] Contiene las definiciones básicas de todos los principios importantes de seguridad, agentes de amenaza, ataques, vulnerabilidades y contramedidas entre otros.

[5] Enmarca todos los controles de seguridad que los desarrolladores de software deben utilizar.

[6] Trata los procedimientos y herramienta para probar la seguridad de las aplicaciones.

[7] Es útil para verificar el funcionamiento de las aplicaciones enfocada en el código fuente.

2.2 LA SEGURIDAD INFORMÁTICA

Partiendo del concepto de seguridad de la información, es necesario hablar sobre el tratamiento específico que se da a la información por medios computacionales, limitando su concepto dentro de este medio.

La seguridad informática persigue un adecuado tratamiento de la información en medios computacionales o físicos, gestionado mediante políticas y herramientas que permitan cumplir con los principios de la información en función de los objetivos a los que esta sirve en cualquier organización[8].

La seguridad informática tiene como objetivo asegurar la información usando distintas técnicas que permitan gestionar los riesgos a la que es sometida, normalmente acompañada de investigación exhaustiva en estos casos, evitando la degradación causada por distintos eventos tales como ataques, errores o mala gestión.

Dicha degradación también recae en consecuencias negativas para la organización que la maneja, tales como perdidas económicas, sanciones penales, o pérdida de la credibilidad. Es por ello, que se debe hablar en contexto de la necesidad de una adecuada política de seguridad informática, que complemente a las que existen en cuanto a la seguridad en la información, teniendo en cuenta la gestión de riesgos[9].

La gestión de riesgos en la seguridad informática es una necesidad debido al número de ataques que se han producido en los últimos años contra organizaciones de distinto tipo[10], el uso de distintas técnicas y conocimientos han hecho que esta práctica no solo aumente los riesgos para

[8] Tomado de “http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm”

[9] La gestión de riesgos definida como se encuentra en la norma ISO 31000:2009

[10] Tomado de “http://www.imaginar.org/iicd/index_archivos/TUS5/introduccion.pdf”, página 4

cualquier organización, así como también que se aumente el número de regulaciones para contrarrestar incidentes, en consecuencia, el fortalecimiento del marco normativo.

2.2.1 PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información cuenta con tres principios básicos[11]:

Confidencialidad: La información, mediante mecanismos de control de acceso, debe ser accesible solo a personas o grupos autorizados, la información adquiere un carácter de confidencialidad alto cuando la compañía posee gran ventaja competitiva cuya divulgación afectaría gravemente el interés no solo de esta, sino también de sus clientes, especialmente cuando esta información posee datos que les pertenecen a este último grupo.

Integridad: Se debe garantizar que la información permanezca siempre inalterada bajo cualquier circunstancia excepto el contexto de uso de la misma, permitiendo una alta fiabilidad en los datos.

Disponibilidad: Se deben establece medidas que permita acceso a la información a la cual se está autorizado en todo momento, en especial en entornos críticos donde la información se debe encontrar disponible en tiempo real.

2.3 PCI - DSS

Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar

[11] Tomado de “http://www.imaginar.org/iicd/index_archivos/TUS5/introduccion.pdf”, página 11

la adopción de medidas de seguridad uniformes a nivel mundial. La PCI DSS proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas.

La PCI DSS se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios. La PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD)[12].

[12]https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3-2_es-LA.pdf

3 METODOLOGÍA

La estructura de la metodología que se propone ha sido diseñada tomando como guía las fases que tiene implícita una auditoría de gestión. Sin embargo, se incluye una parte muy importante que es la identificación y valoración de los riesgos, que servirán para enfocar el trabajo de auditoria en aquellos riesgos que representen un impacto significativo para la organización. A continuación, se describen las fases e instrumentos usados en el desarrollo del proyecto.

3.1 FASE DE ANÁLISIS DEL CONTEXTO

El propósito de esta fase es la identificación de los factores tanto externos como internos que influyen en los objetivos que persigue la organización, así como las dinámicas y flujos de información.

Lo anterior mediante la revisión de las fuentes documentales aplicables, que permiten validar la información y las evidencias obtenidas en las fases posteriores de esta metodología.

3.1.1 Contexto externo

Tabla 3-1. Matriz de análisis del contexto externo. Fuente: Elaboración propia

ABPS **ANALISIS DE RIESGOS** **CONTEXTO EXTERNO**		
REFERENCIAS DE CONSULTA		
FUENTE	**NOMBRE DOCUMENTO, CONTENIDO Y/O DESCRPCION**	
	NACIONAL	**INTERNACIONAL**
Elaborado por:	Fecha:	
Revisado por:	Fecha:	

3.1.2 Contexto interno

Tabla 3-2. Matriz de análisis del contexto interno. Fuente: Elaboración propia

ABPS ANALISIS DE RIESGOS CONTEXTO INTERNO	
REFERENCIAS DE CONSULTA	
FUENTE INTERNA	**CONTENIDO Y/O DESCRIPCION**
Elaborado por:	Fecha:
Revisado por:	Fecha:

3.2 FASE DE ANÁLISIS DE RIESGOS

El propósito de esta fase es la identificación y valoración de los riesgos asociados a los eventos que pueden presentarse en la ejecución de las actividades del proceso de desarrollo de software de la organización.

3.2.1 Identificación de actividades

Tomando como fuente principal la documentación decantada del análisis del contexto interno. Se procede a la identificación de las actividades pertenecientes al proceso mediante la aplicación del siguiente instrumento.

Tabla 3-3. Matriz de identificación de actividades. Fuente: Elaboración propia

ABPS ANALISIS DE RIESGOS IDENTIFICACION DE ACTIVIDADES		
PROCESO DESARROLLO DE SOFTWARE		
CODIGO	**NOMBRE DE LA ACTIVIDAD**	**DESCRIPCION**
Elaborado por:	Fecha:	
Revisado por:	Fecha:	

3.2.2 Identificación de eventos

Los eventos son identificados mediante revisión de aquellos factores críticos que se encuentran fuera del rango o límite establecido, durante la ejecución de las actividades que componen el proceso de desarrollo de software de ABPS. Se sistematizan haciendo uso del siguiente instrumento.

Tabla 3-4. Matriz de identificación de eventos. Fuente: Elaboración propia

ABPS **ANÁLISIS DE RIESGOS** **PROCESO DE DESARROLLO DE SOFTWARE** **IDENTIFICACIÓN DE EVENTOS** **ACTIVIDAD XXXXXXXXX**		
CÓDIGO	**NOMBRE DEL EVENTO**	**DESCRIPCIÓN**
Elaborado por:	Fecha:	
Revisado por:	Fecha:	

3.2.3 Identificación de riesgos

Los riesgos identificados en cada actividad se sistematizan en el siguiente instrumento.

Tabla 3-5. Matriz de identificación de riesgos. Fuente: Elaboración propia

ABPS **ANÁLISIS DE RIESGOS** **PROCESO DESARROLLO DE SOFTWARE** **IDENTIFICACIÓN DE RIEGOS** **ACTIVIDAD XXXXXX**		
CÓDIGO	**NOMBRE DEL RIESGO**	**DESCRIPCIÓN**
Elaborado por:	Fecha:	
Revisado por:	Fecha:	

3.2.4 Valoración del riesgo

Tabla 3-6. Consecuencia asociada al riesgo. Fuente: Elaboración propia

CONSECUENCIA	
CATEGORIA	**PESO**
CATASTROFICA	5
MAYOR	4
MODERADA	3
MENOR	2
INSIGNIFICANTE	1

Tabla 3-7. Probabilidad asociada al riesgo. Fuente: Elaboración propia

PROBABILIDAD	
CATEGORIA	**PESO**
SIEMPRE	5
MUY PROBABLE	4
MODERADA	3
IMPROBABLE	2
CASI NUNCA	1

Tabla 3-8. Severidad del riesgo. Fuente: Elaboración propia

SEVERIDAD DEL RIESGO		
CONVENCIÓN	**CRITERIOS Y PARAMETROS**	
	BAJO	0-6
	MEDIO	7-18
	ALTO	19-25

Tabla 3-9. Matriz consecuencia del riesgo VS probabilidad. Fuente: Elaboración propia

		PROBABILIDAD				
		1	2	3	4	5
CONSECUENCIA	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Finalmente se propone realizar la valoración del riesgo haciendo uso de la siguiente matriz la cual permitirá determinar procedimientos y a su vez los requisitos que deben ser priorizados por presentar riesgos significativos.

Tabla 3-10. Matriz clasificación de riesgos

PROCESO DE DESARROLLO DE SOFTWARE ABPS				CONSECUENCIA		PROBABILIDAD		VALORACIÓN	
CÓDIGO	ACTIVIDAD	CÓDIGO	NOMBRE DEL RIESGO	CATEGORÍA	PESO	CATEGORÍA	PESO	PESO	SEVERIDAD DEL RIESGO

3.3 FASE DE AUDITORIA

3.3.1 Planificación

En esta fase se establece la forma como se abordará la auditoria al proceso de desarrollo de software de la organización, para lo cual se generará un plan de la auditoria que tenga en cuenta la realización de una evaluación preliminar de los riesgos relevantes identificados y valorados en la fase anterior de esta metodología. Los objetivos del trabajo de auditoria se enfocarán en los resultados de esta evaluación. Los siguientes son los principales puntos a tener en cuenta:

- Establecer los objetivos y alcance de la auditoria.
- Determinar la disponibilidad y acceso a las instalaciones, programas, sistemas y datos del proceso de desarrollo de la organización.
- Definir los procedimientos a implementar (muestreo, cálculos).
- Determinar los recursos necesarios en cuanto a personal, CAATT[13], instalaciones entre otras.

PLAN DE AUDITORÍA			ABPS
Código: FX XXX XXXXXX	Versión: 00	Fecha: 19/04/2018	Pág.: 1 de 1

Fecha diligenciamiento	

Norma(s) a auditar	

Alcance de la auditoría	
Objetivo Auditoría	
Sede(s)	
Criterios de auditoría	
Equipo Auditor	

ID	ACTIVIDADES	Auditado	Auditor	Hora	
				Inicio	Fin
Día 1: (DD/MM/AAAAA)					
	(Proceso/Área/Campaña a ser auditado)				
	Día N: (DD/MM/AAAAA)				
	(Proceso/Área/Campaña a ser auditado)				

Figura 3-2. Plan de Auditoria. Fuente: Elaboración propia

[13] Técnicas y herramientas de auditoria asistidas por computador

3.3.2 Ejecución

Es la fase en la cual se recolectan las evidencias de la auditoria como soporte de los hallazgos encontrados, tomando como referencia el plan de la auditoria diseñado en la planeación. En esta fase es donde se aplican las técnicas tradicionales de la auditoria y las CAATT.

- Preparar las CAATT y procedimientos de prueba y controles.
- Revisar los controles definidos en los aplicativos / sistemas que contribuyan a la integridad de las pruebas de auditoria.
- Establecer la magnitud de las pruebas para asegurar que la verificación no afecte el software en operación.

3.3.3 Informe

Fase en la cual se comunican los resultados de la auditoria mediante un informe, el cual es construido tomando como insumo las evidencias recolectadas en la etapa anterior, para proceder a la identificación de hallazgos y las respectivas recomendaciones.

- Describir los resultados obtenidos
- Describir el proceso de análisis de auditoria realizado sobre los resultados.
- Relacionar los hallazgos de auditoria.
- Construir las conclusiones de auditoria
- Elaborar las recomendaciones de auditoria.

INFORME DE AUDITORÍA INTERNA			ABPS
Código: FX XXX XXXX	Versión: 00	Fecha: 19/04/2018	Pág. 1 de 1

ID		Fecha	Fecha	Normas Auditadas	Norma
Alcance de Auditoría					
Objetivo de la Auditoria					
Sede(s)					
Criterios de Auditoria					
Auditor(es)					
Procesos/Áreas/Proyectos Auditados					
Personal Auditado (Nombre y Cargo)					

OPORTUNIDADES DE MEJORA
Fortalezas:
N/A
Observaciones:
N/A

NO CONFORMIDADES	REFERENCIA/NUMERAL
N/A	N/A
N/A	N/A

CONCLUSIONES DE AUDITORÍA

Figura 3-3. Informe de Auditoria. Fuente: Elaboración propia

3.3.4 Seguimiento

En la cual se establecen los compromisos para dar tratamiento a los hallazgos de auditoria encontrados, además de la periodicidad con la cual van a ser validados. Se construirá un instrumento para realizar el respectivo seguimiento que permita vigilar y asegurar que las acciones que se han acordado cumplir se están ejecutando de acuerdo con lo establecido.

ACCIONES CORRECTIVAS			ABPS
CÓDIGO: FX XXX XXXXXX	VERSIÓN: 00	FECHA: 19/04/2018	Pág: 1 de 1

Proceso/subproceso/campaña		Fecha	
Detectada por			
Fuente de detección			
Responsable del plan de acción (aceptación)			

1. Descripción del Hallazgo:

Tipo de acción	○ Correctiva

2. Análisis de Causas

Método	

Desarrollo del Análisis

Causa raíz:

3. Acción(es) Tomada(s)

Corrección (Si aplica)	

Plan de Acción			
Id.	Actividad (Qué y cómo lo va a hacer + mejora esperada –si aplica–)	Fecha entrega	Responsable

4. Evaluación de la Mejora

4.1 Seguimiento (Cumplimiento Plan de Acción)

Id.	Fecha de seguimiento	Observación	Ejecutado (S/N)

4.2 Cierre del plan

Fecha cierre de ejecución del plan		Cerrada por	

Figura 3-4. Informe de Auditoria. Fuente: Elaboración propia

4 DESARROLLO

Durante la reunión de apertura realizada con la dirección de desarrollo de aplicaciones se informó que no se autorizaba a este equipo de trabajo para tomar fotografías, ni para copiar parcial o totalmente ningún tipo de documento de los que se presentaron para soportar cada una de las tareas que se ejecutan al interior del proceso de desarrollo de software, por esta razón únicamente se relacionó el nombre de los documentos que soportan cada una de las tareas ejecutadas al interior del proceso de desarrollo de software, únicamente se autorizó el retiro de la información recolectada en las entrevistas realizadas y en las verificaciones en sitio llevadas a cabo, lo anterior teniendo en cuenta que los formularios diligenciados para el levantamiento de dicha información fueron aportados por este equipo de trabajo.

4.1 IDENTIFICACIÓN REQUERIMIENTOS

El levantamiento de información se efectuó mediante la verificación de los doce requisitos que componen la norma PCI DSS V3.2 y su anexo A como se muestra en la siguiente tabla:

Tabla 4-11. Descripción General PCI DSS Fuente: Elaboración propia

DESCRIPCIÓN GENERAL PCI DSS	
Desarrollar y mantener sistemas y aplicaciones seguros	
1	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta.
2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	
3	Proteja los datos del titular de la tarjeta que fueron almacenados
4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	
5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
6	Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	
7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.

8	Identificar y autenticar el acceso a los componentes del sistema.
9	Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	
10	Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta
11	Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	
12	Mantener una política que aborde la seguridad de la información para todo el personal

Se llevó a cabo una verificación de los 470 controles que componen la norma, se identificó que el proceso de desarrollo de software debe dar cumplimiento al requisito seis el cual se describe a continuación:

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros.

Las personas sin escrúpulos utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches. Todos los sistemas deben contar con los parches de software correctos para evitar que personas malintencionadas o software maliciosos usen, de manera indebida, o pongan en riesgo los datos del titular de la tarjeta.

Nota: Los parches de software adecuados son aquéllos que se evaluaron y probaron para confirmar que no crean conflicto con las configuraciones de seguridad existentes. En el caso de las aplicaciones desarrolladas internamente por la institución, es posible evitar numerosas vulnerabilidades mediante la utilización de procesos estándares de desarrollo de sistemas y técnicas de codificación segura. [14] (PCI DSS V3.2).

[14] PCI DSS V3.2

Dentro del requisito seis se identificaron 24 controles que aplican directamente al proceso de desarrollo de software de ABPS y los cuales se relacionan en el Anexo 1 “Controles aplicables de PCI DSS V3.2 al proceso de Desarrollo de Software de ABPS”.

Es importante tener presente que el nivel de cumplimiento de cada uno de los requisitos que forman parte de la norma PCI DSS se determina en la valoración de dos criterios “Cumple” o “No Cumple” esto con el propósito de obtener el ROC (Report on Compliance).

4.2 ANÁLISIS DE RIESGOS

En esta fase se realizó el estudio de las actividades, eventos y riesgos asociados al proceso de desarrollo de software de ABPS, que fueron objeto de la investigación.

Para recolectar la información se aplicó la observación directa mediante visitas programadas y entrevistas aplicadas a los profesionales encargados del proceso con el fin de garantizar acceso a la documentación necesaria para poder elaborar el análisis de riesgos que se encuentra en el Anexo 2 “Metodología Gestión de Riesgos ABPS”.

4.3 GUÍA DE AUDITORIA

Teniendo en cuenta el nivel de cumplimiento que debe tener el proceso de desarrollo de software frente al requisito seis “Desarrollar y mantener sistemas y aplicaciones seguros.” de la norma PCI DSS a continuación se define el modelo de guía de auditoria a implementar para verificar el cumplimiento requerido por el estándar y el cual se relaciona en el Anexo 3 “Guía de auditoria PCI DSS Requisito 6”.

GUÍA DE AUDITORIA PARA LLEVAR A CABO LA VERIFICACIÓN DE CUMPLIMIENTO DE LA NORMA PCI DSS PARA EL PROCESO DE DESARROLLO DE SOFTWARE						
CÓDIGO: F1 PCI DSS Requisito 6			VERSIÓN: 00			FECHA: 07/05/2018
FECHA			Hora			
NORMA PARA AUDITAR			PCI DSS Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros.			
ÁREA/PROCESO/PROYECTO AUDITADO			Desarrollo de Software			
AUDITOR(ES)						
AUDITADO(S)						
ID						
No.	NUMERAL	REQUISITOS	PROCESO DE PRUEBA	CUMPLE SI	CUMPLE NO	HALLAZGO

Figura 4-5. Guía de Auditoria. Fuente: Elaboración propia

A continuación, se dan a conocer los resultados obtenidos después de llevar a cabo la entrevista de verificación de cumplimiento del requisito 6 de la norma PCI DSS al interior del proceso de desarrollo de software de ABPS.

Se validó el cumplimiento de los 24 controles que componen el requisito 6 de la norma PCI DSS y se identificó que el proceso de desarrollo de software tiene un 96% de cumplimiento frente a la totalidad de los controles del requisito 6 de la norma PCI DSS, es importante tener presente que se debe trabajar para remediar el 4% restante de los controles que no se encuentran en cumplimiento, esto con el propósito de obtener el 100% de cumplimiento de cada uno de los controles solicitados.

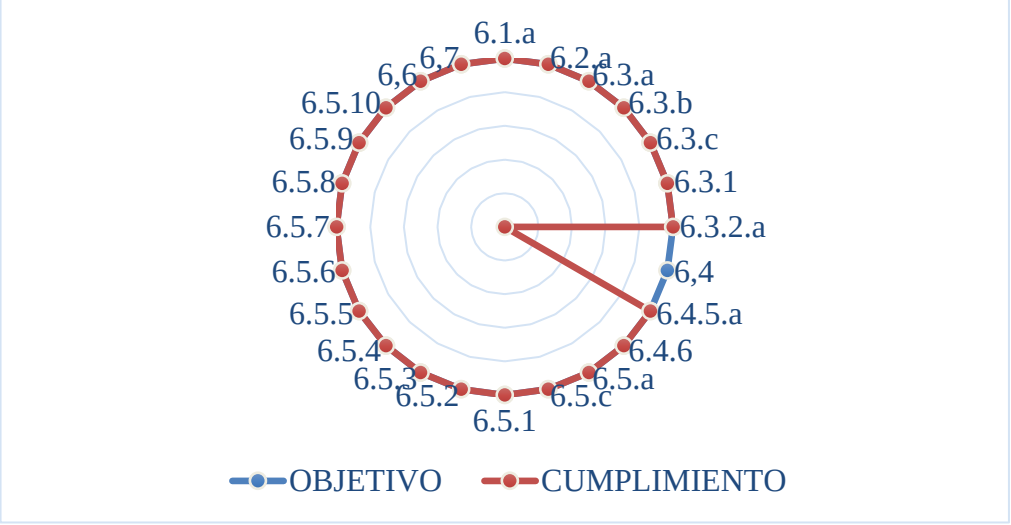

Figura 4-6. Nivel de Cumplimiento Requisito 6 PCI DSS: Elaboración propia

5 CONCLUSIONES Y RECOMENDACIONES

Teniendo en cuenta los resultados obtenidos podemos concluir que el proceso de desarrollo de software de ABPS no se encuentra en cumplimiento con el requisito 6 de la norma PCI DSS.

Se identifico que para el proceso de desarrollo de software de ABPS es aplicable el requisito 6 de la norma PCI DSS el cual contiene 24 controles aplicables al proceso, de los cuales se evidencio un nivel de cumplimiento del 96% de igual forma se identificaron debilidades en el 4% frente al total de controles aplicables al proceso de desarrollo de software.

Los resultados presentados no son aceptables de acuerdo con el cumplimiento que se debe tener frente a la norma PCI DSS toda vez que se evidencio que el proceso de desarrollo de software está incumpliendo el 4% del total de los controles que le aplican por lo que no se encuentra en cumplimiento de acuerdo con lo definido por la norma.

ABPS debe tomar acciones oportunas frente a las debilidades identificadas en el 4% de los controles que no se están cumpliendo, se sugiere implementar controles compensatorios que permitan colocar en cumplimiento las diferentes actividades que se ejecutan a diario al interior del proceso de desarrollo de software con el propósito de dar cumplimiento a la totalidad de controles solicitados por la norma PCI DSS en su requisito 6.

Se recomienda que esta metodología se aplique como un punto de partida que sirva de referencia a futuras revisiones y evaluaciones de cada uno de los procesos más críticos que soportan las operaciones del negocio de ABPS, con el objetivo de identificar el nivel de cumplimiento que tienen cada uno de dichos procesos frente a los requisitos de la norma PCI DSS.

BIBLIOGRAFÍA

- Tamayo J. A., & Valencia J. V., (2016). Técnicas y herramientas de auditoria asistidas por computador. La auditoría continua frente a la auditoría tradicional 84-85.

- Amutio, M., Candau, J., & Mañas, J. (2012). MAGERIT–Versión 3.0. Metodología De Análisis y Gestión De Riesgos De Los Sistemas De Información. Libro I-Método, 22-45.

- Mesquida, A. L., Mas, A., & Amengual, E. (2009). La madurez de los servicios TI. Innovación, Calidad e Ingeniería del Software, 5(2), 77.

- Bernal Montañés, R., & Coltell Simón, Ó. (1996). Auditoría de los sistemas de información.

REFERENCIAS ELECTRÓNICAS

- THE OPEN WEB APPLICATION SECURITY PROJECT, “About The Open Web Application Security Project”, [consulta: 2 de marzo de 2018], Disponible en: *https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project.*

ANEXOS

Anexo 1. Controles Aplicables PCI DSS V3.2 Desarrollo de Software de ABPS.

Anexo 2. Metodología Gestión de Riesgos ABPS

Anexo 3. Guía de auditoria PCI DSS Requisito 6

Anexo 4 Plan de Auditoria

Anexo 5 Informe Auditoría Interna

Anexo 6 Acciones Correctivas