Escuela de Ingeniería Informática

Herramienta para la identificación de riesgos y controles para la protección de datos de los clientes en la aplicación Retailer Transaction Settlement para la empresa Shell Global con base en el marco de referencia PCI-DSS

Trabajo final de graduación para optar al grado de Licenciatura en Ingeniería Informática

Elaborado por:

Mauricio Lizano Barahona

Profesor Tutor:

Lic. Pedro Leiva Chinchilla

San Jose, Costa Rica

Julio, 2019

DECLARACION JURADA

Yo, Mauricio Lizano Barahona, mayor, soltero, egresado de la Carrera de Ingeniería Informática, de la Universidad Hispanoamericana, vecino de Tibas, portador de la cédula 112020237, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi Proyecto de Graduación para optar al título de Licenciatura en Ingeniería Informática, juro solemnemente que mi trabajo de investigación: "Herramienta para la identificación de riesgos y controles para la protección de datos de los clientes en la aplicación Retailer Transaction Settlement para la empresa Shell Global con base en el marco de referencia PCI-DSS" es una obra original que ha respetado todo lo preceptuado por las Leyes Penales así como la Ley de Derechos de Autor y derechos Conexos, número 6683 de 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 de 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte: artículo 70°: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedo advertido que la Universidad Fidélitas se reserva del derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la Ciudad de San José el jueves 4 de junio de 2020.

Mauricio Lizano Barahona

Cedula

112020237

DEDICATORIA

A la mujer que limpiaba casas… mientras yo estudiaba.

Mauricio Lizano Barahona

AGRADECIMIENTO

Agradezco a mi hermana Maribel quien Dios ha puesto en nuestra familia para dar el ejemplo, subir la barra y cambiar nuestros parámetros y paradigmas.

A mi mamá, quien, con trabajo, dedicación y con mucho amor, nos ha mostrado el camino a seguir.

También a mis hermanos, que me ayudaron a forjar el carácter.

A mi papá, de quien aprendí a sonreír a pesar del aguacero.

A todas las personas que han ayudado, sin justificación alguna.

Pero sobre todo a mi Creador.

CARTA DE AUTORIZACION DEL TUTOR

Cartago, 5 de Junio del 2020

San José, 6 de junio de 2020
Sra. María Isabel Losilla Barrientos
Facultad de Ingeniería Informática
Universidad Hispanoamericana

Estimada señora directora:

Yo, Pedro Ignacio Leiva Chinchilla, mayor, casado, ingeniero, vecino de Cartago, portador de la cédula de identidad número 1-1394-0453, en mi condición de tutor del trabajo final de graduación titulado: HERRAMIENTA PARALA IDENTIFICACION DE RIESGOS Y CONTROLES PARA LA PROTECCION DE DATOS DE LOS CLIENTES EN LA APLICACIÓN RETAILER TRANSACTION SETTLEMENT PARA LA EMPRESA SHELL GLOBAL CON BASE EN EL MARC DE REFERENCIA PCI-DSS, propuesta por el estudiante Mauricio Lizano Barahona, manifiesto que de los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

A)	Original del tema	10%	8%
B)	Cumplimiento de entrega de avances	20%	9%
C)	Coherencia entre los objetivos, los instrumentos aplicados y los resultados de la investigación	30%	25%
D)	Relevancia de las conclusiones y recomendaciones	20%	15%
E)	Calidad, detalle del Marco Teórico	20%	23%
F)	TOTAL		80%

En virtud de la calificación obtenida, se avala el traspaso al proceso de lectura.

Atentamente,

Firmado digitalmente por PEDRO IGNACIO LEIVA CHINCHILLA (FIRMA)
Fecha: 2020.06.06 10:36:09 -06'00'

Ing. Pedro Ignacio Leiva Chinchilla

Tutor

CARTA DE LECTOR

San José, 10 de agosto de 2020

Universidad Hispanoamericana
Sede Llorente
Carrera de Ingeniería Informática

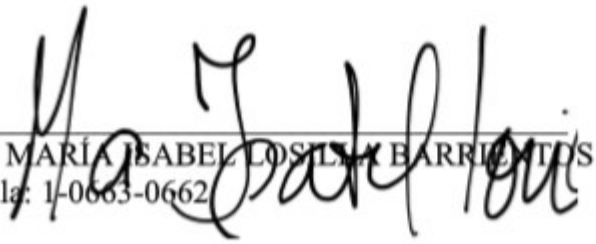
Estimado señor

El estudiante **LIZANO BARAHONA MAURICIO**, cédula de identidad 1-1202-0237, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado " **Herramienta para la identificación de riesgos y controles para la protección de datos de los clientes en la aplicación Retailer Transaction Settlement para la empresa Shell Global con base en el marco de referencia PCI-DSS**.", el cual ha elaborado para obtener su grado de LICENCIATURA.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.



ING. MARÍA ISABEL [illegible] BARRANTES M.R.I.
Cédula: 1-0663-0662

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 13 de Agosto del 2020

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Mauricio Lizano Barahona con número de identificación 1-1202-0237 autor (a) del trabajo de graduación titulado **" Herramienta para la identificación de riesgos y controles para la protección de datos de los clientes en la aplicación Retailer Transaction Settlement para la empresa Shell Global con base en el marco de referencia PCI-DSS."** presentado y aprobado en el año 2020 como requisito para optar por el título de Licenciatura; (SI) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Mauricio Lizano Barahona
1-1202-0237

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las "Condiciones de uso de estricto cumplimiento" de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

Tabla de Contenido

1 Capítulo I: Introducción 1
1.1 Antecedentes 2
1.1.1 Antecedentes del Contexto de la Empresa 2
1.2 Justificación del Proyecto 8
1.3 Definición del Problema 9
1.3.1 Problemática 9
1.3.2 Problema General 13
1.3.3 Problemas Específicos 13
1.4 Objetivos 14
1.4.1 Objetivo General 14
1.4.2 Objetivos Específicos 14
1.5 Alcance del Proyecto 15
1.5.1 Pilares estratégicos de la Herramienta 16
1.5.2 Exclusiones 17
1.6 Entregables del Proyecto 18
1.6.1 Entregables de la gestión del Proyecto 18
1.6.2 Entregables de Producto 18
1.7 Limitaciones del Proyecto 19
2 Capítulo II: Marco Teórico 20
2.1 Conceptos Básicos 20
2.1.1 Auditoría 20
2.1.2 Objetivos de la Auditoría 21

2.1.3 Etapas de Auditoría 22
2.1.4 Riesgo y control 24
2.1.5 Análisis de riesgos 24
2.1.6 Análisis de controles 25
2.1.7 Seguridad de la información 28
2.1.8 Seguridad física 31
2.1.9 Seguridad lógica 31
2.1.10 Capas de seguridad de la información 33
2.2 Cobit 5 35
2.2.1 Principios de Cobit 5 36
2.2.2 Procesos de gestión 38
2.2.3 Procesos de Gobierno 44
2.3 PCI-DSS 47
2.3.1 Aplicabilidad de las PCI DSS 47
2.3.2 Alcance de los requisitos de las PCI DSS 49
2.3.3 Normativa PCI DSS v3.2.1 50
2.3.4 Mejores prácticas para implementar las PCI-DSS 59
2.3.5 Controles de compensación 61
2.3.6 Ejemplo Requerimiento 3: Proteger los datos del Titular 63
2.4 ISO 27001 Information Segurity Management 65
2.4.1 Funcionamiento de la Norma ISO 27001 66
2.4.2 Ventajas de utilizar la norma ISO 27001 66
2.4.3 Gestión de seguridad de la información en una empresa 67
2.4.4 Estructura de la Norma ISO 27001 68
3 CAPÍTULO III: MARCO METODOLÓGICO 70

3.1 Tipo de Investigación 70
3.1.1 Clasificación de Dimensión Temporal 71
3.1.2 Clasificación según su profundidad 71
3.1.3 Clasificación según su enfoque 71
3.2 Alcance de la Investigación 73
3.3 Fuentes de Información 73
3.3.1 Fuentes de información primarias: 74
3.3.2 Fuentes de información secundarias: 74
3.4 Técnicas y herramientas de recolección de datos 75
3.4.1 Entrevistas 75
3.4.2 Revisión de Documentos 77
3.4.3 Variables de Investigación 77
3.4.4 Diseño de la Investigación 79
3.4.5 Matriz de coherencias 80
4 CAPÍTULO IV: ANALISIS DE LA INFORMACION 83
4.1 Recopilación y Análisis de Información 83
4.2 Revisión Documental y Artefactos 84
4.2.1 Manejo de Información en Medios Físicos 85
4.2.2 Manejo de eventos de seguridad 86
4.2.3 Manejo de llaves criptográficas 87
4.2.4 Procesos de “Onboarding” 88
4.3 Identificación de Mejoras y Recomendaciones 90
5 CAPÍTULO V: PROPUESTA DEL PROYECTO 92
5.1 Identificación y calificación cualitativa de riesgos inherentes 92
5.2 Identificación de controles para gestión eficaz de riesgos 94

5.3 Identificación y calificación de riesgos residuales 95
5.3.1 Criterios de evaluación de riesgos residuales 95
6 CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES 97
6.1 Conclusiones 97
6.2 Recomendaciones 100
Bibliografía 102
Apéndices 104
Apéndice A. Plantilla para las entrevistas 104
Apéndice B. Entrevistas realizadas a profesionales en auditoría 105
Apéndice B.01. Entrevista a un Gerente de Auditoría de Tecnología de la información 105
Apéndice B.02. Entrevista a un Gerente de Auditoría Interna 108
Apéndice B.03 Entrevista a un Auditor de tecnologia 111
Apéndice C. Entrevista Administrador de la cuenta 114
Apéndice E. Minutas de Entrevistas 125
Apéndice D. Plantilla Revision Documental 129
Apéndice D.1. Historial Revision Documental 129
Apéndice F. Herramienta de Gestión de Riesgos y Controles PCI 130
Apéndice F.1 Identificación y Calificación de Riesgos Inherentes 130
Apéndice F.2 Identificación de Controles Adecuados con referencia a Estándar PCI 131
Apéndice F.3 Identificación y Calificación de Riesgos Residuales 131
Anexos 132
Anexo 1. DXC Sanitization and Destruction Standard 132
Anexo 2. RCU Shell GRM Data Retention Schedule 139

Anexo 3. Notificación de Acceso Fallido 139
Anexo 4. RCU Shell Cryptographic Keys 140
Anexo 5. RCU Shell PCI DSS Awareness..... 142
Anexo 6. Confirmacion De Entrevista 143
Glosario..... 144

Tabla de Ilustraciones

Ilustración 1. Organigrama Empresarial Equipo de Aplicaciones. 5
Ilustración 2. Diagrama Causa - Problemática – Efecto. 12
Ilustración 3. Pilares de los alcances del Proyecto. 16
Ilustración 4. Principios de COBIT 5. 36
Ilustración 5. Gestion del riesgo segun ISO. 67
Ilustración 6. Tipos de Investigación. 71
Ilustración 7. Diseño de la Investigación. 80
Ilustración 8. Métodos de destrucción de datos basados en el tipo de medio. 85
Ilustración 9. Calendario de retención de datos. 86
Ilustración 10. Notificación de Acceso Fallido. 87
Ilustración 11. Consola de Administración de llaves (Vormetric). 88
Ilustración 12. Evidencia de entrenamiento a nuevos empleados. 89
Ilustración 13. Identificación de Riesgos Inherentes. 93
Ilustración 14. Medición cualitativa de riesgos Inherentes. 94
Ilustración 15. Identificación de controles PCI. 94
Ilustración 16. Plantilla de evaluación de riesgos residuales (efectividad de controles aplicados). 96
Ilustración 17. Plantilla de evaluación de riesgos residuales (probabilidad de materialización). 96

Índice de Tablas

Tabla 1. Descripción de puestos según el organigrama 7
Tabla 2. APO12 Apoyo de metas de TI. 40
Tabla 3. APO12 Objetivos y Metricas de Proceso. 40
Tabla 4. APO13 Apoyo de metas de TI. 42
Tabla 5. APO13 Objetivos y Metricas de Proceso. 42
Tabla 6. DSS06 Apoyo de metas de TI. 43
Tabla 7. DSS06 Objetivos y Metricas de Proceso. 44
Tabla 8, MEA02 Apoyo de metas de TI. 46
Tabla 9. MEA02 Objetivos y Metricas de Proceso. 46
Tabla 10. Datos de Cuentas. 48
Tabla 11. Datos no permitidos de almacenar 49
Tabla 12. Normativa de Seguridad PCI DSS. 58
Tabla 13. Herramientas según enfoque de la investigación. 75
Tabla 14. Definicion de Variables. Fuente: Creacion Propia 79
Tabla 15. Matrix de Coherencia. 82
Tabla 16. Tabla de Posibles Mejoras, ... 91

1 CAPÍTULO I: INTRODUCCIÓN

El auge de las tecnologías de la Información es uno de los grandes causantes del cambio que se ha visto en las actividades económicas durante las últimas décadas. Iniciando por el auge de los medios de pagos en comercios como también la posibilidad de hacer pagos a través de la internet. Es gracias a los avances de tecnología de la Información que se ha visto la necesidad de proteger y mantener control sobre la información sobre los medios de pago.

Siendo la comercialización de hidrocarburos una de las más grandes actividades comerciales de nuestros tiempos, los pagos y transacciones hechos diariamente se vuelven una prioridad en cuanto al procesamiento contable de las operaciones de negocios de Shell.

De esta manera Shell da un paso adelante en cuanto al compromiso que tiene en cuanto a la manutención y protección de la información de sus clientes. Sin embargo, se han visto retos difíciles de obstaculizar ya que la implementación de las mejores prácticas a las herramientas actuales lleva a cabo esfuerzos contantes que no han del todo sido eficientes.

En este documento se expondrá una propuesta de herramienta de diagnóstico para el cumplimiento de las mejores prácticas a través de correcta identificación de riesgos y los controles que realmente permiten a los administradores de la aplicación a mitigar y controlar de una manera constante el cumplimiento de las normas del estándar PCI-DSS.

La gestión incorrecta de riesgos ha hecho que en reiteradas ocasiones los procesos de auditoria encuentren hallazgos de incumplimiento con las normas que han requerido un esfuerzo constante de mitigación no siempre efectiva ya que muchas de las correcciones se han hecho posterior al momento en que las normas fueron incumplidas.

1.1 ANTECEDENTES

Para el desarrollo de esta investigación se considera importante brindar un contexto sobre la organización, a continuación, se describen elementos importantes sobre los retos y logros que han alcanzado, su estrategia: misión, visión. También se expone la filosofía que ha acompañado la compañía por más de un centenar de años.

1.1.1 Antecedentes del Contexto de la Empresa

El Grupo Royal Dutch Shell se creó en 1907 cuando la Compañía Shell Transport and Trading Company Ltd. fusionaron sus operaciones. La Royal Dutch Petroleum Company era una compañía holandesa fundada en 1890 por Jean Kessler, junto con Henri Deterding y Hugo Loudon, cuando un chárter real fue concedido por la reina Holandesa Wilhelmina a una pequeña compañía de exploración petrolífera conocida como "Royal Dutch". La Shell Transport and Trading Company era una compañía británica fundada en 1897 por Marcus Samuel y su hermano Samuel.

La Royal Dutch Shell es una empresa de hidrocarburos anglo-neerlandesa que tiene intereses en los sectores petrolífero y del gas natural, así como del refinado de gasolinas. Siendo la comercialización de hidrocarburos uno de los ejes central de las operaciones de la compañía, las operaciones relacionadas al control contable, reportes de ventas y transacciones es uno de los pilares de mayor afluencia. De la misma forma, las operaciones de tecnología de la información que soportan esta unidad de negocio son también de suma importancia dentro de la compañía.

En la última década, el mercado en el que se desenvuelve la empresa ha sido afectado, ya que el precio del producto ha sido determinado negativamente por factores externos a su demanda, haciendo que las compañías del sector petrolífero se vean en la necesidad de implementar medidas para mejorar sus esquemas de costos. En cuanto a la administración de tecnologías de la información ha habido tendencias marcadas tanto en los servicios de aplicaciones que se están migrando a países en donde la mano de obra intelectual y los costos operativos sean más eficientes.

1.1.1.1 Visión

Hacer la diferencia a través de nuestra gente, un equipo de profesionales dedicados, que valoran a nuestros clientes, cumplen nuestras promesas y contribuyendo al Desarrollo sostenible.

1.1.1.2 Misión

Comercializar y distribuir de manera segura los productos energéticos y petroquímicos al tiempo que ofrece servicios innovadores de valor agregado.

1.1.1.3 Valores de la Empresa

A continuación, se presentarán los valores organizacionales de la Empresa Shell.

En Shell, se comparten un conjunto de valores fundamentales: honestidad, integridad y respeto por las personas, que sustentan todo el trabajo que hacemos. Los Principios comerciales generales, el Código de conducta y el Manual de ética y cumplimiento de Shell ayudan a todos en Shell a actuar de acuerdo con estos valores y cumplir con las leyes y regulaciones pertinentes (Shell, 2019).

Los principios comerciales generales de Shell son fundamentales para la forma en que llevamos a cabo nuestros negocios y vivir de acuerdo con ellos es crucial para nuestro éxito continuo. Somos juzgados por cómo actuamos y cómo estamos a la altura de nuestros valores fundamentales de honestidad, integridad y respeto por las personas. Nuestros principios comerciales se basan en estos. Promueven la confianza, la apertura, el trabajo en equipo y la profesionalidad, así como el orgullo de lo que hacemos y cómo hacemos negocios (Shell, 2019).

Shell fue una de las primeras compañías globales en declarar y compartir nuestras creencias cuando publicamos nuestros Principios Generales de Negocios en 1976. Como parte de estos principios, nos comprometemos a contribuir al desarrollo sostenible, equilibrar intereses a corto y

largo plazo e integrar la economía, el medio ambiente y el medio ambiente. y consideraciones sociales en nuestra toma de decisiones (Shell, 2019).

Se espera que todos los empleados y contratistas de Shell, y aquellos en las empresas conjuntas que operamos, comprendan y se comporten continuamente de acuerdo con nuestros Principios comerciales. Esperamos que los proveedores y las empresas conjuntas que no operamos apliquen principios equivalentes (Shell, 2019).

1.1.1.4 Organigrama

A continuación, se presenta el organigrama empresarial con la intención de exponer la jerarquía del departamento de Tecnologías de Información quien es un equipo de Outsourcing de servicios de aplicaciones, el cual tiene presencia en la Gran Bretaña, India, Marruecos, Estados Unidos y Costa Rica. El equipo es el encargado de las mejoras a la aplicación, soporte operacional y soporte de Incidentes, así como también las implementaciones necesarias según las necesidades del negocio. El servicio que se da es 24/7 ya que las aplicaciones que se soportan dan servicios a diferentes países y tiene una prioridad de respuesta de servicio alta.

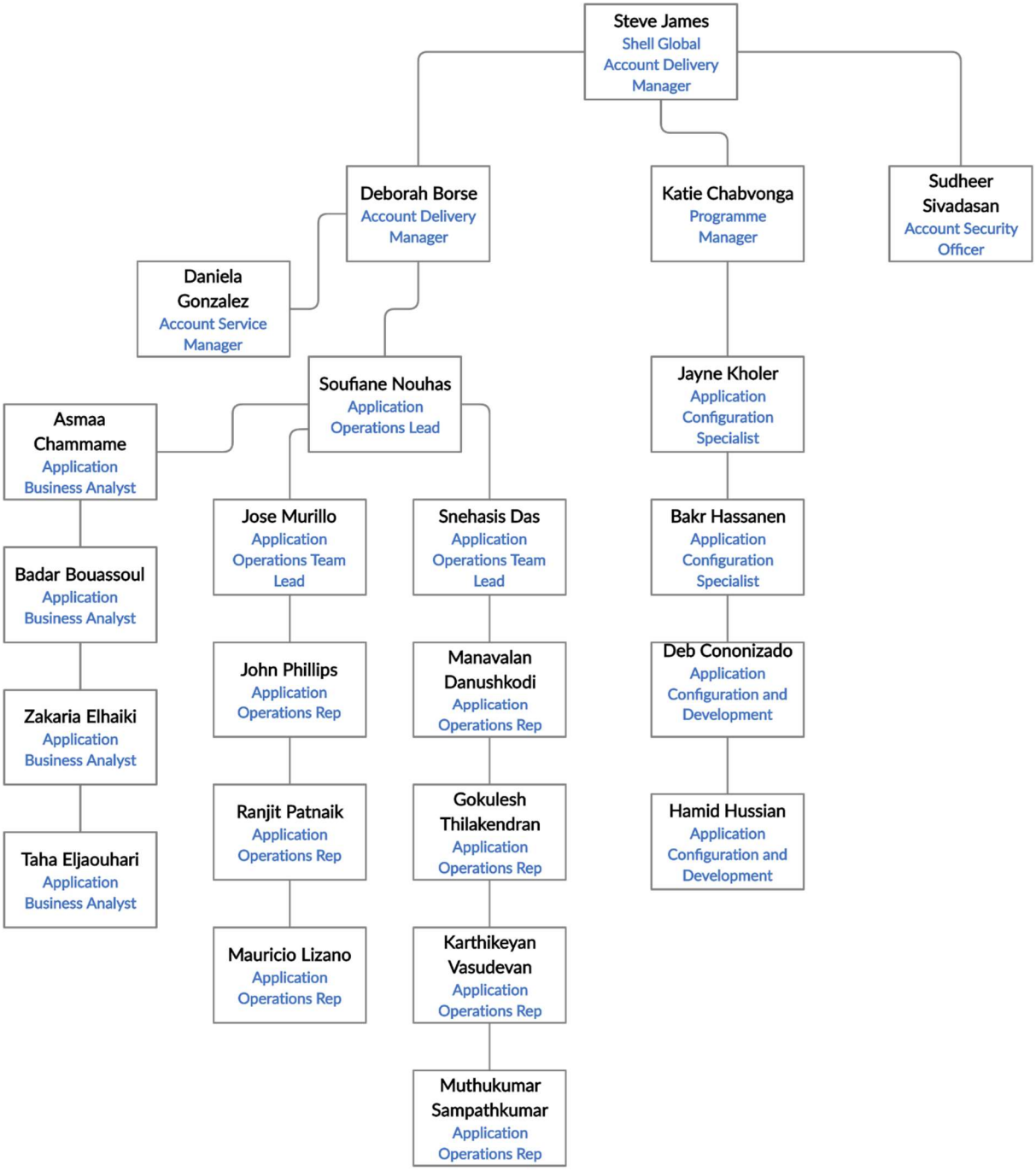


Ilustración 1. Organigrama Empresarial Equipo de Aplicaciones.

Fuente: Elaboración propia a partir de D, Borse (comunicación personal, 6 de Diciembre de 2019)

En la Figura 1 se puede apreciar el volumen de la fuerza de trabajo requerida para mantener las operaciones diarias de la aplicación, siendo un equipo que da un servicio "*Follow the sun*" de tal manera que siempre existen profesionales de TI asistiendo y revisando el buen funcionamiento de la aplicación.

1.1.1.5 Descripción de Puestos

En este apartado se muestra una representación detallada de los puestos mostrados en la figura 1, con el fin de exponer las diferentes funciones dentro del equipo de soporte a la aplicación en cuestión, además se proporciona una explicación del rol que involucra cada uno de los puestos dentro del proyecto.

A continuación, se presenta la tabla 1 con la descripción detallada para cada uno de los puestos representados en el organigrama del equipo de soporte a la aplicación en cuestión.

Funcionario	**Rol de soporte**	**Rol dentro del proyecto**
Steve James	Administración general del Proyecto	Coordinar y delegar funciones del proyecto
Deborah Deborse	Gerente la entrega de servicio de operaciones	Velar por el funcionamiento de las operaciones de la aplicación
Katie Chavvonga	Gerente del Programa	Velar por cumplimiento de los requerimientos del negocio
Jayne Kholer	Especialista de configuración de la aplicación	Encargada de la configuración de la aplicación
Bakr Hassanen	Especialista de configuración de la aplicación	Encargado de la configuración de la aplicación
Deb Cononizado	Desarrollo y configuración de la aplicación	Encargada de configuración y el funcionamiento del código de la aplicación
Hamid Hussian	Desarrollo y configuración de la aplicación	Encargado de configuración y el funcionamiento del código de la aplicación
Sudheer Sivadasan	Encargado de seguridad de la aplicación	Velar por el cumplimiento de seguridad y soporte a auditorias de la aplicación
Daniela Gonzalez	Gerente de servicio	Velar por el cumplimiento de acuerdos de servicio de la aplicación.
Soufiane Nouhas	Líder del equipo de operaciones	Gerenciar el buen funcionamiento de las operaciones de la aplicación como también el cumplimiento de servicios de la aplicación
Asmaa Chammame	Analista de negocio	Interceder por las necesidades de los usuarios según las capacidades de la aplicación

Funcionario	Rol de soporte	Rol dentro del proyecto
Badar Boussoul	Analista de negocio	Interceder por las necesidades de los usuarios según las capacidades de la aplicación
Zakaria Elhaiki	Analista de negocio	Interceder por las necesidades de los usuarios según las capacidades de la aplicación
Taha Elijaouhari	Analista de negocio	Interceder por las necesidades de los usuarios según las capacidades de la aplicación
Jose Murillo	Líder técnico de operaciones	Aseguramiento del buen funcionamiento de las operaciones de la aplicación
Snehasis Das	Líder técnico de operaciones	Aseguramiento del buen funcionamiento de las operaciones de la aplicación
John Phillips	Consultor de Operaciones técnicas de la aplicación	Consultado de operaciones técnicas diarias de la aplicación
Ranjit Patnaik	Consultor de Operaciones técnicas de la aplicación	Consultado de operaciones técnicas diarias de la aplicación
Mauricio Lizano	Consultor de Operaciones técnicas de la aplicación	Consultado de operaciones técnicas diarias de la aplicación
Manavalan Danushkodi	Consultor de Operaciones técnicas de la aplicación	Consultado de operaciones técnicas diarias de la aplicación
Gokulesh Thilakendran	Consultor de Operaciones técnicas de la aplicación	Consultado de operaciones técnicas diarias de la aplicación
Karthikeyan Vasudevan	Consultor de Operaciones técnicas de la aplicación	Consultado de operaciones técnicas diarias de la aplicación
Muthukumar Sampathkumar	Consultor de Operaciones técnicas de la aplicación	Consultado de operaciones técnicas diarias de la aplicación

Tabla 1. Descripción de puestos según el organigrama

Fuente: *Elaboración propia a partir de D, Borse (comunicación personal, 6 de diciembre de 2019)*

1.2 JUSTIFICACIÓN DEL PROYECTO

La administración de los riesgos relacionados con aplicaciones tecnológicas recae directamente en sus administradores, quienes deben asegurar un correcto y oportuno funcionamiento en un ambiente controlado, que además de proporcionar un servicio ininterrumpido, resguarde la seguridad de la información que contiene.

Este análisis surge de la necesidad de proveer de herramientas tácitas y eficaces, para la gestión de los riesgos tecnológicos que permita al administrador del sistema realizar un análisis profundo y a consecuencia determinar controles adecuados. Para demostrar el funcionamiento de la herramienta a presentar en este proyecto, se aplicará en una aplicación web, específicamente para el estándar PCI, en donde se procesan, mantienen y transfieren datos de tarjetas de pago con las mejores prácticas de la gestión.

En la actualidad la seguridad de la información para las industrias de tarjetas de pago es una actividad regulada mundialmente, la entidad PCI *Security Standards Concuil* ofrece el estándar PCI DSS (*Payment Card Industry – Data Security Standard* por sus siglas en Inglés) en donde se normaliza, una base bajo la cual se definen ciertas acciones como necesidades en el manejo de la información personal y numérica de las diferentes tarjetas de pago. Esto certifica a los sistemas informáticos donde se procesan, mantienen o transmiten datos de tarjetas y evita consecuencias legales que son aplicables globalmente.

La gestión y manejo de riesgos en cuanto al cumplimiento de estas normas de seguridad es uno de los principales pilares de los administradores de los sistemas informáticos, específicamente en este proyecto se planteará para aplicativos en donde se gestionan datos de tarjetas.

Por tal razón, es evidente la necesidad de contar con una herramienta sencilla para que el administrador de la aplicación pueda identificar, analizar y evaluar los riesgos y diseñar controles que los mitiguen adecuadamente. Con este trabajo se demostrará su importancia para la gestión de riesgos, en cuanto a seguridad de la información de tarjetas de pago en una aplicación web en donde se tramitan aprobaciones automáticas y manuales de conciliaciones y transacciones diarias para ocho países a nivel global.

1.3 DEFINICIÓN DEL PROBLEMA

A continuación, se describe la problemática actual con el fin de ofrecer un panorama general sobre cómo se gestiona el aseguramiento de la protección de la información crediticia y de las medidas tomadas hasta el momento para la mitigación de riesgos.

1.3.1 Problemática

El equipo de soporte de operaciones de la aplicación *Retailer Transaction Settlement Platform* (RTSP por sus siglas en inglés), es el encargado de velar por el buen funcionamiento de la aplicación en el ambiente de producción, como también encargado del procesamiento de scripts y generación de reportes fundamentales para las operaciones del negocio. En dichos scripts se genera información que es sumamente necesaria para Shell dado que se usa para operaciones contables y financieras de la empresa.

En términos generales, la función primordial del equipo es habilitar el funcionamiento de operaciones del negocio a través del soporte que se le brinda al procesamiento de información en los servidores de producción. Asimismo, como resguardar la integridad de la información.

Siendo la seguridad de los datos de métodos de pagos uno de los principales estandartes en los cuales el equipo hace esfuerzos constantes para mantener, procesar y administrar información sensitiva según las mejores prácticas del negocio.

En la entrevista realizada a la gerente de la cuenta Deborah Deborse, se explica que una de las operaciones críticas para el negocio de Shell son las liquidaciones de transacciones a minoristas, en donde diariamente de procesan miles de millones de dólares globalmente (Ver Anexo C). La información que se procesa en dichas operaciones contiene datos sensibles de medios de pago de los usuarios finales, de tal manera que el procesamiento y la tenencia de esta información es regulada y aunque existen esfuerzos permanentes por mantener certificaciones de seguridad, como también el cumplimiento de las mejores prácticas de la industria, siempre se tienen reportes de violación de estándares de seguridad (Ver Apéndice C).

El diseño de seguridad de la aplicación toma en cuenta la necesidad de resguardar la información, incluso cuenta con un módulo para enmascarar información sensible según el perfil de seguridad del usuario. No obstante, constantemente se reportan incidentes, en donde usuarios tienen acceso innecesario, ya sea porque se le asignó un perfil de seguridad inadecuado u otra razón. Adicionalmente, el enmascarado de información sensitiva hace un mapeo del perfil de seguridad con el objeto programado al cual se quiere proteger (Ver Apéndice C).

Los módulos de la aplicación permiten acciones que parecerían normales de operaciones propias del negocio, como la importación, exportación y descarga de reportes completos sin el control externo de quien hace uso de estas acciones y quien tiene acceso a la Información PCI (*Personal Credit Information* por sus siglas en Ingles). La aplicación también hace uso de funciones básicas programadas como "*mail to*". Esta es una operación necesaria para el negocio de Shell, sin embargo no se tienen evidencia de procesos de eliminación segura de información sensitiva, lo cual es una violación directa de las normas del estándar (Ver Apéndice C).

El aplicativo y las operaciones contables de la empresa han crecido, de manera tal que se han creado múltiples unidades de negocio y perfiles de seguridad, lo que complica el acceso que cada perfil tiene; adicionalmente, conlleva un mantenimiento adicional de actualizar la documentación y los objetos programables que procesan información sensible (Ver Apéndice C). Dicho mantenimiento no se hace con regularidad y se han visto incidentes donde algún objeto ha mostrado información sensible y no ha sido incluido para su enmascaramiento, en estos casos se ha hecho una corrección reactiva y no proactivamente.

Por otro lado, hay una cultura empresarial por parte de Shell de apoyarse de los equipos de TI, para proveerse de reportes e información sensitiva, ya sea por una falencia temporal del sistema o por un Incidente reportado. También se han visto estalaciones en los procesos de aprovisionamiento en donde alta gerencia de Shell ha sido indulgente con el proceso de aprovisionamiento y se ha permitido hacer uso de documentación desactualizada. Una vez más, queda evidenciado el deficiente diseño de seguridad, pero también se evidencia que la compañía no cuenta con la educación requerida, ni la cultura para el manejo de información sensitiva.

Repetidamente las auditorías ejecutadas, han evidenciado hallazgos enfocados a las restricciones de los distintos perfiles de seguridad, que han penalizado el servicio del proveedor según los contratos de nivel de servicio (SLA por sus siglas en ingles), sin encontrar la causa raíz del problema. Los esfuerzos de analistas de TI en mejoras del diseño de perfiles de seguridad han sido ineficientes en cumplir con soluciones alineadas con los estándares de calidad PCI y mejores prácticas del sector (Ver Apéndice C).

En la siguiente figura, se presenta un diagrama de Causa-Efecto para apoyar la idea de cuáles son las causas de la problemática.

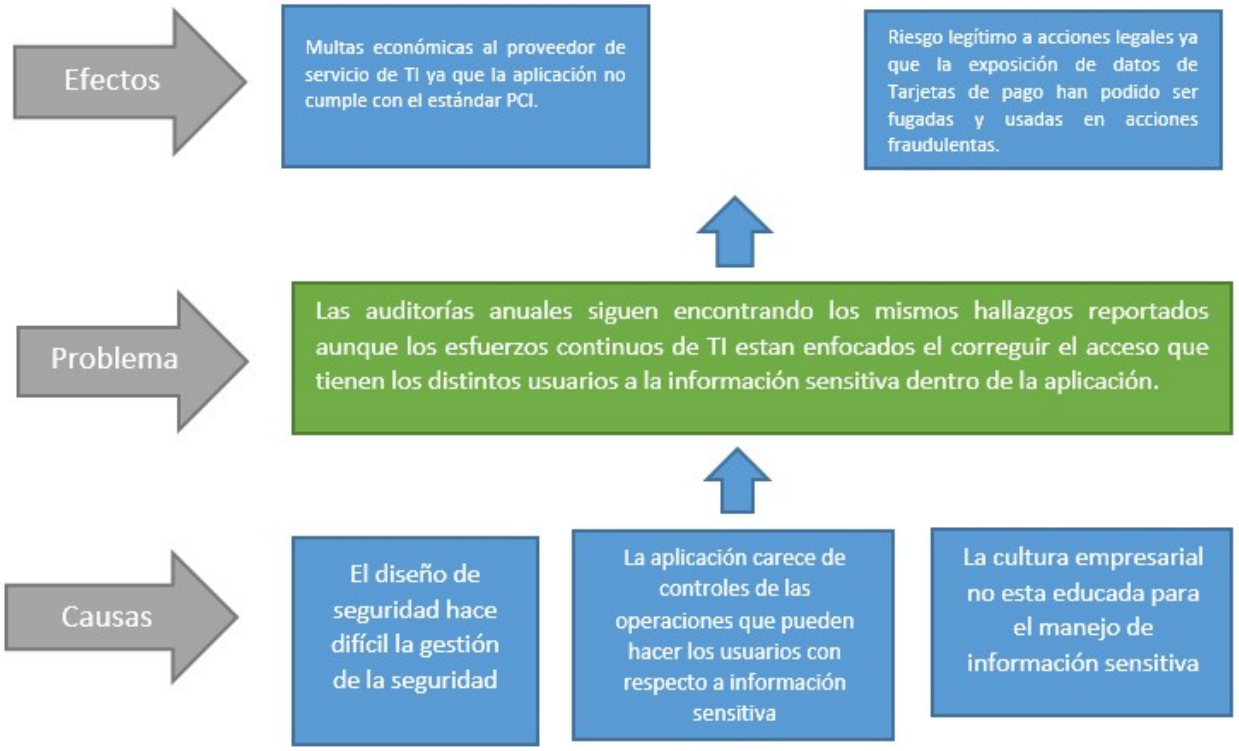


Ilustración 2. Diagrama Causa - Problemática – Efecto.

Fuente: Elaboración propia a partir de entrevista con D, Deborse (Ver Apéndice C)

1.3.2 Problema General

A continuación, se expone el problema general del proyecto.

¿Como identificar y analizar eficientemente los riesgos y gestionar controles precisos que permitan que las operaciones de la aplicación se den siempre dentro del marco referencial de las mejores prácticas de la industria PCI-DSS y Cobit? Los esfuerzos que se han hecho para asegurar el correcto manejo de información sensitiva han sido reactivos e ineficientes ya que se han evidenciado eventos de incumplimiento con la normativa

1.3.3 Problemas Específicos

En esta sección se presentan los problemas específicos que forman parte del proyecto.

a. ¿Existen instrumentos de referencia para que administradores de TI puedan llevar a cabo procesos de auditoría, asegurando el cumplimiento con las normas internacionales del correcto uso y manejo de información de tarjetas de pago?
b. ¿Como reconocer cuales exactamente son los riesgos inherentes que impactan negativamente el cumplimiento con la normativa?
c. ¿De qué manera evaluar y priorizar la mitigación de los riesgos encontrados y de esta manera poder agendar como pendientes necesarios en las mejoras de la aplicación?
d. ¿Es posible determinar los controles capaces y necesarios para la gestión eficaz de los riesgos encontrados en la aplicación?
e. ¿Como poder hacer una evaluación sobre de los riesgos residuales para conocer las repercusiones en el cumplimiento de la normativa?

1.4 OBJETIVOS

A continuación, se presenta el objetivo general y los objetivos específicos del proyecto.

1.4.1 Objetivo General

Crear una propuesta de implementación de una herramienta de referencia para identificar y analizar riesgos como también la gestión de controles oportunos durante el primer semestre del año 2020, usando como marco de referencia las mejores prácticas de la industria con el fin de asegurar el cumplimiento con los estándares PCI-DSS y Cobit.

1.4.2 Objetivos Específicos

a. Proponer una herramienta de referencia para procesos de auditoria con el fin de asegurar el cumplimiento de las mejores prácticas de la industria en cuanto al manejo de datos de pago y protección de identidad.
b. Identificar los riesgos inherentes en la aplicación a través de la propuesta de implementación de una herramienta que permita hacer una evaluación de fondo en la manera en que información sensitiva es administrada, con el fin de asegurar el cumplimiento con las mejores prácticas según la norma PCI-DSS y Cobit.
c. Valorar los riesgos identificados con base en un modelo cualitativo con escala de medición ordinal, para determinar su importancia dentro de las prioridades de gestión en alineamiento con el estándar.
d. Identificar los controles diseñados para gestionar eficazmente los riesgos encontrados y a su vez evaluar su efectividad en la mitigación de la vulnerabilidad de la información.
e. Valorar los riesgos residuales posteriores al proceso de gestión de controles, asimismo determinar sus repercusiones en cuanto al manejo de información sensitiva.

1.5 ALCANCE DEL PROYECTO

La propuesta de este proyecto se basa en la elaboración de una herramienta para la identificación de riesgos y gestión de riesgos para la aplicación *Retail Transaction Settlement Platform* para la empresa Shell global, alineado a las mejores prácticas de la industria según Cobit y el estándar PCI-DSS.

A su vez, la herramienta funciona como una guía de referencia para que equipos de administración de la aplicación mantenga sus operaciones normales siempre dentro del marco de referencia de las mejores prácticas y de la misma manera cumpla con requerimientos legales.

A continuación, en la Figura 3 se representan los ejes estratégicos principales para que la presente propuesta entregue el valor agregado en la administración de las aplicaciones siempre dentro las operaciones normales.

Ilustración 3. Pilares de los alcances del Proyecto.

Fuente: Elaboración propia

1.5.1 Pilares estratégicos de la Herramienta

Tal como se puede apreciar en la Figura 3, el alcance del proyecto se encuentra dividido en cuatro ejes estratégicos que son esperados para que la propuesta sea de valor para el aseguramiento de operaciones del equipo de soporte dentro del marco referente de las mejores prácticas en la industria. A continuación, se explicará el detalle de cada una de ellas.

1.5.1.1 Elaboración de la herramienta de referencia

Este es el primer pilar de donde se partirá para el desarrollo del presente proyecto, como es anteriormente mencionado en la problemática, el equipo de administradores de la aplicación no cuenta con una herramienta que ayude a identificar los riesgos como también sea eficiente en establecer los controles necesarios.

1.5.1.2 Identificación de riesgos Inherentes y Residuales

Este eje de la investigación cuenta con dos etapas, inicialmente se requiere establecer riesgos inherentes para posteriormente trabajar con controles que mitiguen estos mencionados. Posteriormente se requiere identificar los riesgos residuales ya que es para su valoración en las prioridades de gestión de los administradores de la aplicación.

1.5.1.3 Valoración de Riesgos

La valoración de riesgos es una etapa importante para el desarrollo del presente proyecto, su importancia en base cualitativa será de suma importancia para la determinación de prioridades de gestión.

1.5.1.4 Identificar los Controles necesarios

La identificación de controles eficaces es una de las etapas críticas del proyecto ya que de aquí se partirá una base para asegurar la eficiencia en el cumplimiento de con las mejores prácticas de la industria, de la misma manera se asegurarán que las operaciones de administración de la aplicación sean siempre dentro del marco de referencia de los estándares con los que se busca estar alineado.

1.5.2 Exclusiones

De la misma manera en que los pilares anteriormente mencionados representan las necesidades que satisfacen las necesidades del equipo de administración de la aplicación para el cumplimiento con las mejores prácticas. Existen aspectos que deben ser mencionados como exclusiones del proyecto ya que por la complejidad de su implementación quedan por fuera del alcance del presente proyecto.

Dichas exclusiones representan aspectos que no son contemplados en los entregables, no obstante, es importante considerar dichos aspectos que específicamente no forman parte del desarrollo del presente proyecto:

a. Queda excluido el proceso administrativo de aprobación de alta gerencia sobre la herramienta de referencia
b. Los riesgos Inherentes y residuales que serán tomados en cuenta para este proyecto son exclusivamente relacionados a aspectos que afecten el incumplimiento con la normativa de información sensitiva de medios de pago y de información de los clientes de la compañía.
c. La implementación de los controles identificados no es una de las actividades objetivo del presente proyecto

1.6 ENTREGABLES DEL PROYECTO

Los entregables del proyecto consta de la documentación final sobre el desarrollo del presente proyecto, en él se cuenta con documentación del progreso de la investigación tanto como los productos finales como consecuencia de dicho proyecto.

1.6.1 Entregables de la gestión del Proyecto

Los entregables de la gestión del proyecto corresponden a la documentación que se genera durante los avances del mismo, entre ellos se pueden mencionar los siguientes:

a. Minutas de reuniones
b. Cronograma del proyecto
c. Informes de avances semanales

1.6.2 Entregables de Producto

Los entregables de producto corresponden a la documentación final que se espera tener como consecuencia del presente proyecto. Entre estos podemos identificar la plantilla de análisis de riesgos inherentes como también riesgos residuales. Asimismo, la documentación para la valoración cualitativa de riesgos y finalmente la plantilla para la identificación de controles adecuados que mitiguen los riesgos encontrados.

1.7 LIMITACIONES DEL PROYECTO

A continuación, se presentan los factores que pueden limitar o restringir el desarrollo del presente proyecto. Seguidamente, se presenta las limitaciones identificadas:

a. La presente investigación se limita a hacer una propuesta de implementación de la herramienta, usando la aplicación web llamada *Retailer Transaction Settlement Platform* (RTSP por sus siglas en inglés) como ejemplo de implementación de la propuesta.
b. Este proyecto aportará una herramienta para un análisis de riesgos, no constituirá una auditoria completa a la aplicación.
c. Se identificarán los controles que mitigan los riesgos que se identifiquen, sin embargo, no aportara un rediseño de los controles.
d. La implementación de dichos controles no forma parte de los objetivos del presente proyecto.
e. Solamente se analizará la seguridad de la información relacionada a las tarjetas de pago.
f. La herramienta por desarrollar se utilizará para el análisis de riesgos en Tecnología de la Información, no incluye el análisis en otras áreas de la empresa.
g. La normativa que se tomara en cuenta para el cumplimiento en este proyecto es PCI – DSS.

2 CAPÍTULO II: MARCO TEÓRICO

El Marco Teórico describe en detalle los conceptos, antecedentes y marcos de referencia que serán usados en el presente proyecto con el fin de propiciar la comprensión de los contenidos de este documento en términos de los resultados y su respectivo análisis, como también la propuesta de solución planteada.

Las ideas, conceptos y estándares de mejores prácticas que se desarrollan en este capítulo representan la base teórica sobre la cual se fundamenta la presente investigación. Es por esta razón que se ha hecho una división conceptual según su naturaleza técnica dentro del área técnica en que se emplea.

Ahora bien, el marco teórico consta de cuatro secciones, en las cuales se abarca la totalidad del esquema conceptual propuesto para la presente investigación. Estas cuatro secciones corresponden a: Conceptos Básicos, Cobit 5, Estándar PCI-DSS, ISO/IEC 20000.

A continuación, se detallan cada una de estas secciones.

2.1 CONCEPTOS BÁSICOS

2.1.1 Auditoría

Según el Manual para la preparación para el examen CISA de la Asociación de Auditoria y Control de Sistemas de Información (ISACA), en su 26° edición, la auditoría de define de la siguiente forma:

> La auditoría de Tecnología de la información es el examen, la entrevista y/o la prueba formal de los sistemas de información para determinar si:
>
> - Los sistemas de información cumplen con las leyes, reglamentaciones y contratos aplicables y/o pautas de la industria.
> - Los datos e información de SI tienen niveles de confidencialidad, integridad y disponibilidad adecuados.
> - Las operaciones de SI se están realizando de forma eficiente y si se cumplen los objetivos de efectividad.
>
> (ISACA, 2017, p. 32)

2.1.1.1 Definición de control interno:

Para el desarrollo de este trabajo, es necesario conocer la definición de control interno, la cual se tomó de *Commitee of Sponsoring Organizations of the Treadway Commission*, que es la entidad que en forma oficial emite los pronunciamientos relacionados con control interno a nivel global.

COSO (1997) define Control Interno como "*proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:*

- *Eficacia y eficiencia de las operaciones.*
- *Fiabilidad de la información financiera.*
- *Cumplimiento de las leyes y normas aplicables."*

La definición anterior refleja ciertos conceptos fundamentales;

- El control interno es un proceso. Es un medio utilizado para la consecución de un fin, no es un fin en sí mismo.
- El control interno lo llevan a cabo las personas. No se trata solamente de manuales, políticas e impresos, sino de personas en cada nivel de la organización.
- El control interno sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la dirección y al consejo de administración de la entidad.
- El control interno está pensado para facilitar la consecución de objetivos en una o más de las diferentes categorías que, al mismo tiempo, se solapan.
  (COSO, 1997, pág. 16).

2.1.2 Objetivos de la Auditoría

Los objetivos de la auditoría se refieren a las metas específicas que deben cumplirse por parte de la auditoría. En contraste, un objetivo de control se refiere a cómo debe funcionar un control interno. Una auditoría incorpora por lo general varios objetivos de auditoría, que se centran

en validar que existen controles internos para minimizar los riesgos del negocio, y que éstos funcionen como se espera. (ISACA, 2017, p. 47)

2.1.3 Etapas de Auditoría

La ejecución de una auditoría de tecnología de la información puede organizarse en etapas y en cada una de ellas se llevan a cabo un conjunto de procedimientos documentados de auditoría diseñados para alcanzar los objetivos de auditoría. Sus componentes básicos son la planificación, la definición del alcance, los objetivos de la auditoría, y los programas de auditoría, que se basarán en el análisis de riesgos y controles.

Las fases de una auditoría típica se describen:

I. Sujeto de la auditoría: Identificar el área que será auditada.

II. Objetivo de la auditoría: Identificar el propósito de la auditoría. Por ejemplo, un objetivo podría ser determinar si los cambios del código fuente del programa ocurren en un ambiente bien definido y controlado.

III. Alcance de la auditoría: Identificar los sistemas, funciones o unidades específicos de la organización que serán incluidos en la revisión. Por ejemplo, en el caso anterior de los cambios del programa, el enunciado de alcance podría limitar la revisión a sólo un sistema de aplicación o a un período limitado.

IV. Planificación de preauditoria:
    a. Identificar las habilidades y los recursos técnicos necesarios.
    b. Identificar las fuentes de información para la prueba o examen, como diagramas de flujo funcionales, políticas, normas, procedimientos y papeles de trabajo anteriores a la auditoría.
    c. Identificar las localidades o instalaciones que serán auditadas.
    d. Desarrollar un plan de comunicaciones al comienzo de cada compromiso que describa con quién comunicarse, cuándo, con qué frecuencia y por qué motivos

V. Procedimientos de auditoría y pasos para la recolección de datos:
    a. Identificar y seleccionar el enfoque de auditoría, para verificar y comprobar los controles, Identificar una lista de individuos que serán entrevistados.
    b. Identificar y obtener las políticas, estándares y directrices departamentales para real izar la revisión.
    c. Desarrollar herramientas y metodología de auditoría para probar y verificar el control.

VI. Procedimientos para evaluar los resultados de la prueba o la revisión:
    a. Identificar métodos (incluyendo herramientas) para realizar la evaluación.
    b. Identificar criterios para evaluar la prueba (similar a una guía de prueba que use el auditor al realizar la evaluación).
    c. Identificar medios y recursos para confirmar que la evaluación fue precisa (y que se puede repetir, si corresponde).

VII. Procedimientos para las comunicaciones con la gerencia:
    a. Determinar la frecuencia de la comunicación.
    b. Preparar la documentación para el reporte final.

VIII. Preparación del reporte de auditoría:
    a. Revelar los procedimientos de seguimiento de la revisión.
    b. Revelar los procedimientos para evaluar/ probar la eficacia y efectividad operacional.
    c. Revelar los procedimientos para probar los controles.
    d. Revisar y evaluar la calidad de los documentos, las políticas y los procedimientos.

(ISACA, 2017, p. 49)

Un enfoque de auditoría basada en riesgos está dirigido al análisis de la gestión de los riesgos que los dueños de procesos y activos tecnológicos están llevando a cabo (actividades de control) para gestionar los riesgos inherentes a las actividades que realizan. En un enfoque de

auditoría basado en riesgos, los auditores de TI no se basan sólo en el riesgo, sino que también se basan en los controles y en el conocimiento de la empresa o del negocio. Este tipo de decisión sobre la evaluación del riesgo puede ayudar a relacionar el análisis de costo-beneficio del control con el riesgo conocido, permitiendo selecciones prácticas.

Según, ISACA, (2017), los riesgos del negocio son las preocupaciones sobre los probables efectos de un evento incierto en el logro de los objetivos establecidos. La naturaleza de los riesgos del negocio puede ser financiera, regulatoria u operativa, y puede también incluir riesgos derivados de tecnologías específicas. Por ejemplo, una compañía de aviación está sujeta a extensas regulaciones de seguridad y a cambios económicos, impactando ambos la continuidad de las operaciones de la compañía. En este contexto, la disponibilidad de servicios de TI y su confiabilidad es crítica.

2.1.4 Riesgo y control

Para que los sistemas de información concreten las metas de optimización de beneficios, riesgos y recursos, se debe abordar el riesgo que podría prevenir o inhibir la obtención de estas metas. Las organizaciones diseñan, desarrollan, implementan y monitorean sistemas de información a través de políticas, procedimientos, prácticas y estructuras organizativas para abordar estos tipos de riesgos. (ISACA, 2017, p. 41)

2.1.5 Análisis de riesgos

El análisis de riesgos es parte de la planificación de la auditoría y ayuda a identificar el riesgo y las vulnerabilidades para que auditoría de Tecnología de la información pueda determinar los controles necesarios para mitigar el riesgo:

Riesgos: efectos adversos que pudieran ocurrir a las operaciones de la organización (incluyendo misión, funciones, imagen, reputación), activos de la organización, individuos, otras organizaciones, debido al potencial para acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada de la información y/o de los sistemas de información. (ISACA, 2017, p. 41)

2.1.5.1 Gestión de riesgos: Principios y directrices para mitigar riesgos.

> La gestión de riesgos es el proceso de identificar las vulnerabilidades y las amenazas para los recursos de información utilizados por una organización para lograr los objetivos de negocio, y decidir qué contramedidas (protecciones o controles) tomar, si hubiera alguna, para reducir el riesgo a un nivel aceptable (es decir, riesgo residual), basándose en el valor del recurso de información para la organización. (ISACA, 2017, p. 101)

El proceso de evaluación del riesgo comienza identificando los objetivos del negocio, los activos de información y los sistemas o recursos de información subyacentes que generan/almacenan, usan o manipulan los activos clave (hardware, software, bases de datos, redes, instalaciones, personas, etc.) para lograr estos objetivos. Debido a que los riesgos de TI son dinámicos, es clave que la gerencia reconozca la necesidad de un proceso dinámico de gestión de riesgos de TI y que establezca un proceso de este tipo que respalde el proceso de gestión de riesgos del negocio. Después de que se identifican los activos de información sensible o crítica, se realiza una evaluación del riesgo para identificar las vulnerabilidades y amenazas y determinar la probabilidad de que ocurran, el impacto resultante y las medidas adicionales que mitigarían este impacto a un nivel aceptable para la dirección.

Luego, durante la etapa de mitigación de riesgos, se identifican los controles para mitigar los riesgos identificados. Estos controles son contramedidas para la mitigación de riesgos que buscan prevenir o reducir la probabilidad de que ocurra un evento de riesgo, detectar su ocurrencia, minimizar el impacto o transferir el riesgo a otra organización. La etapa final es el monitoreo de los niveles de desempeño de los riesgos gestionados.

2.1.6 Análisis de controles

Los controles normalmente son políticas, procedimientos, prácticas y estructuras organizacionales implementadas para reducir los riesgos para la organización. Son desarrollados para proveer una certeza razonable a la gerencia de que se alcanzarán los objetivos de negocio de la organización y de que se previenen o detectan y corrigen los eventos de riesgo. Las actividades de control interno y los procesos que las respaldan pueden ser manuales o manejados por recursos de información automatizados. El consejo de dirección y la alta dirección son responsables de establecer la cultura apropiada para facilitar un sistema efectivo y eficiente de control interno y de

monitorear continuamente la efectividad del sistema de control interno, aunque toda persona dentro de una organización debe participar en este proceso.

Los controles se clasifican en preventivos, detectivos o correctivos de acuerdo con su naturaleza y deben cumplir con los siguientes objetivos: eficacia, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Los objetivos de control se aplican a todos los controles, ya sean manuales, automatizados, o una combinación de ellos (por ejemplo, revisiones de registros de sistemas). Los objetivos de control en un entorno de SI no difieren de aquellos de un entorno manual; sin embargo, la manera en que se implementan estos controles puede ser diferente. Por lo tanto, se deben considerar los objetivos de control relevantes para los procesos específicos relacionados con SI. (ISACA, 2017, p. 43)

2.1.6.1 Controles generales

Los controles incluyen políticas, procedimientos y prácticas (tareas y actividades) que son establecidos por la gerencia para proveer una certeza razonable de que se alcanzarán objetivos específicos. Los controles generales son aplicables a todas las áreas de la organización, incluyendo infraestructura y servicios de soporte de TI. Los controles generales establecidos por ISACA (2017, p.46) incluyen:

- Políticas y procedimientos de seguridad de la organización para asegurar el uso adecuado de los activos.
- Políticas generales para el diseño y uso de documentos y registros (manuales/automatizados) adecuados para ayudar a asegurar el registro apropiado de las transacciones-pista de auditoría de transacciones.
- Procedimientos y prácticas para asegurar la protección adecuada en el acceso y el uso de activos e instalaciones.
- Políticas de seguridad física y lógica para todas las instalaciones, centros de datos y recursos de TI (por ejemplo, servidores e infraestructura de telecomunicaciones).

2.1.6.2 Controles específicos de Tecnología de la Información

Cada control general puede ser traducido a un control específico de SI, un sistema de información bien diseñado debería contar con controles para todas sus funciones sensitivas o críticas. Por ejemplo, el procedimiento general para asegurar, la adecuada custodia del acceso a los activos e instalaciones puede traducirse en un conjunto de procedimientos de control relacionado con sistemas de información, que abarque controles de acceso a los programas de computación, datos y equipos informáticos. En las auditorías de tecnología de la información debe entender los objetivos básicos de control que existen para todas las funciones. Los procedimientos de control de SI incluyen:

- Estrategia y dirección de las funciones de Tecnología de la Información.
- Organización general y gestión de las funciones de Tecnología de la Información Acceso a los recursos de Tecnología de la Información, incluyendo datos y programas.
- Metodologías de desarrollo de sistemas y control de cambios.
- Procedimientos de operaciones.
- Programación de sistemas y funciones de soporte técnico.
- Procedimientos de aseguramiento de calidad.
- Controles de acceso físico.
- Planificación de continuidad del negocio.
- Redes y comunicaciones
- Administración de la base de datos
- Protección y mecanismos de detección contra ataques internos y externos
- Seguridad

(ISACA, 2017, p. 46)

El establecimiento de la base para una gestión efectiva de la seguridad de la información es el factor más crítico en la protección de los activos de información y la privacidad. Los desarrollos recientes en el entorno actual, tales como el intercambio electrónico a través de los

proveedores de servicios y directamente con los clientes, el uso de mecanismos de acceso remoto y la exposición a riesgos de seguridad de alto impacto (por ejemplo, intrusiones, robo de identidad, virus, ataques de negación de servicios, , etc.) han elevado el perfil del riesgo de la información y de la privacidad y con esto la necesidad de gestionar con eficacia la seguridad de la información.

Los objetivos de seguridad para satisfacer los requerimientos del negocio de las organizaciones incluyen los siguientes:

- Asegurar la continua disponibilidad de los datos y sistemas de información.
- Asegurar la integridad de la información en sus sistemas informáticos (almacenada y en tránsito).
- Preservar la confidencialidad de los datos sensibles mientras están almacenados y en tránsito.
- Asegurar el cumplimiento de leyes, regulaciones y estándares aplicables.
- Asegurar el cumplimiento de los requerimientos de confianza depositada y con las obligaciones en relación con cualquier información relativa a una persona identificada o identificable (es decir, sujeto de datos) en conformidad con su política de privacidad o leyes y regulaciones de privacidad aplicables.
- Asegurar, que los datos sensibles están bien protegidos cuando se almacenan y cuando están en tránsito, en función de los requerimientos de la organización.

(ISACA, 2017, p. 46)

2.1.7 Seguridad de la información

Un sistema de gestión de seguridad de la información es un marco de políticas, procedimientos, directrices y recursos asociados para establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información para todos los tipos de organizaciones. Por ejemplo, la serie 27000 de estándares y directrices de la Organización Internacional de Normalización (ISO), que define el alcance y el vocabulario que se usa en todo el estándar de

seguridad de la información y proporciona un directorio de las publicaciones que conforman el estándar. (ISACA, 2017, p. 360)

2.1.7.1 Elementos clave de la gestión de seguridad de la información

Según ISACA, Pág. 360, existen 7 elementos clave que requieren ser gestionado con relación a la seguridad de la información, se detallan:

1. Liderazgo, compromiso y respaldo de la alta dirección: El compromiso y respaldo de la alta gerencia son importantes para el éxito en el establecimiento y la continuidad de un programa de gestión de la seguridad de la información.
2. Políticas y procedimientos: Establecer el marco de una política proporcionando una declaración concisa de directivas de la alta gerencia que trata el valor de los activos de información, la necesidad de seguridad y la importancia de definir una jerarquía de clases de activos confidenciales y críticos. Una vez que una política ha sido aprobada por el organismo de gobierno de la organización y por las funciones y las responsabilidades relacionadas, el programa de seguridad de la información será sustentado con lo siguiente:
   - Estándares para desarrollar niveles de seguridad mínimos
   - Criterios y métodos de medición
   - Directrices, prácticas y procedimientos específicos.
   - La política debe asegurar que se cumplan las leyes y regulaciones, deben estar actualizados y reflejar los objetivos del negocio, los estándares y las prácticas de seguridad.
3. Organización: Las responsabilidades para la protección de los activos individuales deben ser definidos claramente. La política de seguridad de la información debe proporcionar una orientación general sobre la asignación de funciones y responsabilidades de seguridad en la organización y también, donde sea necesario, orientación detallada para los sitios específicos, activos, servicios y procesos de seguridad relacionados, tales como la planificación de la recuperación y continuidad del negocio de TI.
4. Concienciación y formación en seguridad: Todos los empleados de una organización, y cuando corresponda, los usuarios externos deben recibir capacitación apropiada y

actualizaciones periódicas para promover la concienciación y el cumplimiento de las políticas y los procedimientos de seguridad que están por escrito. Para los nuevos empleados, esta capacitación debe ocurrir antes de que se otorgue acceso a la información o a los servicios. Los diferentes mecanismos disponibles para elevar la concienciación de seguridad incluyen los siguientes:

- Actualizaciones periódicas escritas de las políticas y procedimientos de seguridad que están por escrito
- Capacitación formal sobre seguridad de la información
- Programa interno de certificación para el personal relevante
- Declaraciones firmadas por los empleados comprometiéndose a acatar la política y los procedimientos de seguridad documentados, incluyendo la obligación de no divulgación.
- Uso de diferentes medios para la distribución de material relacionado con la seguridad (por ejemplo, boletín de noticias de la compañía, página Web, videos, etc.)
- Cumplimiento visible de las reglas sobre segundad y auditorías periódicas
- Ejercicios e incidentes simulados de seguridad

5. Gestión de riesgos: Se deben implementar procesos para identificar, evaluar, responder y mitigar el riesgo para los activos de información
6. Monitoreo y cumplimiento: Los auditores de SI están generalmente encargados de evaluar, periódicamente, la efectividad de los programas de seguridad de la organización. Para llevar a cabo esta tarea, estos deben entender y conocer los esquemas de protección, el marco de la seguridad y los aspectos relacionados incluyendo el cumplimiento de las leyes y regulaciones aplicables. Por ejemplo, estos aspectos pueden estar relacionados con la debida diligencia de la organización en cuanto a la seguridad y privacidad de información sensible, en particular cuando ésta se relaciona con industrias específicas (por ejemplo, las instituciones bancarias y "financieras, de salud).
7. Tratamiento y respuesta a incidentes: Un incidente de seguridad de computadoras es un evento que afecta adversamente el procesamiento del uso de computadoras. Esto incluye pérdida de confidencialidad de la información, causar inestabilidad de la integridad de la información, negación de servicio, acceso no autorizado a los sistemas, mal uso de los

sistemas de información, robo y daño a los sistemas. Otros incidentes incluyen ataques de virus e intrusiones por personas dentro o fuera de la compañía.

2.1.7.2 Roles y responsabilidades de la gestión de la seguridad de la información

De acuerdo con, (ISACA, 2017), la responsabilidad por gestionar la seguridad de la información cae en todos los niveles de la organización, y va desde la Dirección ejecutiva, el Comité de seguridad de la información (es óptimo que se implemente este órgano en las empresas), propietarios de procesos, Director de Seguridad de la información, colaboradores de la organización y terceos. Adicionalmente, la responsabilidad de rendir cuentas definidas y documentadas debe ser establecida y comunicada a todo el personal y gerencia de la organización.

2.1.8 Seguridad física

Según ISACA, (2017) los controles correspondientes a la seguridad física se dividen en tres categorías:

1. Controles físicos: se instalan para restringir físicamente el acceso a una instalación o hardware.
2. Técnicos: también conocidos como controles lógicos y se proporcionan mediante el uso de tecnología, equipos o dispositivos; por ejemplo: firewalls.
3. De gestión: Controles relacionados con la supervisión, los informes, los procedimientos y las operaciones de un proceso.

2.1.9 Seguridad lógica

Los controles de acceso lógico son los medios principales que se utilizan para gestionar y proteger los activos de información. Ellos establecen y sustancian las políticas y los procedimientos creados para proteger estos activos y están diseñados para reducir el riesgo hasta un nivel aceptable para una organización. Los auditores de SI necesitan entender esta relación. Al hacerlo, ellos deben poder analizar y evaluar la efectividad del control de acceso lógico para lograr

los objetivos de seguridad de la información y evitar las pérdidas resultantes de las exposiciones a riesgos. Estas exposiciones pueden tener como consecuencia desde inconvenientes menores hasta una paralización total de las funciones de la computadora. (ISACA, 2017, p. 379)

Algunas industrias cuentan con estándares que se pueden usar corno un punto de referencia para la seguridad, un ejemplo es el estándar de seguridad de la Industria de Tarjetas de Pagos (PCI/DSS), que se usa como estándar para todas las organizaciones que procesan tarjetas de pagos (por ejemplo, tarjetas de débito, tarjetas de crédito, etc.).

2.1.9.1 Exposiciones de acceso lógico

Las exposiciones se presentan debido a la explotación accidental o intencional de las debilidades de control de acceso lógico. La explotación intencionada de exposiciones técnicas puede conducir a crímenes informáticos. Sin embargo, no todos los crímenes informáticos explotan las exposiciones técnicas.

Las exposiciones técnicas son las actividades no autorizadas que interfieren con el procesamiento normal, por ejemplo, la implementación o modificación de datos y software bloqueando o haciendo uso indebido de los servicios de usuario, destruyendo los datos, comprometiendo la utilización del sistema, distrayendo los recursos de procesamiento o espiando el flujo de datos o las actividades de los usuarios ya sea en la red, la plataforma (SO), la base de datos o el nivel de aplicación. Las exposiciones técnicas incluyen:

- Vaciado o fuga de datos: implica extraer o efectuar un vaciado de información fuera de la computadora. Esto puede involucrar imprimir archivos en papel, o puede ser tan sencillo como robar los reportes y cintas de la computadora. A diferencia de la fuga de productos, la fuga de datos deja la copia original, de modo que puede pasar inadvertido.
- Intercepción de Líneas (*wiretapping)*: consiste en escuchar ilegalmente la información que es transmitida a través de las líneas de telecomunicación.
- Paralización o caída de la Computadora (*Computer Shut down)*: Se puede realizar a través de las terminales o de las microcomputadoras conectadas directamente (en línea) o remotamente (a través de Internet). Sólo las personas que conozcan un identificador de inicio de sesión (logon ID) de alto nivel pueden usualmente iniciar el proceso de cierre, pero esta medida de seguridad es efectiva sólo si están operando los controles apropiados

de seguridad de acceso para el ID de logon de alto nivel y para las conexiones de telecomunicaciones en la computadora. Algunos sistemas han demostrado ser vulnerables a cerrarse a sí mismos bajo ciertas condiciones de sobrecarga.
(ISACA, 2017, p. 379)

2.1.10 Capas de seguridad de la información

Según ISACA (2017) los activos de TI bajo la seguridad lógica pueden agruparse en cuatro capas: redes, plataformas, bases de datos y aplicaciones. Esto permite el concepto de seguridad en capas para Acceso al Sistema que proporciona un mayor alcance y granularidad de control de los recursos de información. Por ejemplo, las capas de red y de plataforma proporcionan un amplio control general sobre los usuarios que se autentican en los sistemas, en el software de sistemas y en la configuración de aplicaciones, conjuntos de datos (data sets), bibliotecas de carga, y cualquier biblioteca de conjuntos de datos de producción. Los controles de las bases de datos y de las aplicaciones. Por lo general, proporcionan un mayor grado de control sobre la actividad del usuario dentro de un proceso particular del negocio al controlar el acceso a registros, campos de datos específicos y transacciones.

Dados los riesgos potenciales de Internet, se pueden producir en varios niveles, deberá configurar medidas de seguridad que ofrezcan múltiples capas de defensa contra los riesgos. En general, cuando se conecte a Internet, no debe preguntarse si hay alguna posibilidad de que se produzcan intrusiones o ataques de denegación de servicio. Por el contrario, debe dar por sentado que sí se producirán problemas de seguridad. De esta forma, la mejor defensa será un ataque proactivo y deliberado. El uso de un enfoque por capas al planificar la estrategia de seguridad de Internet garantiza que el atacante que logre penetrar en una de las capas de defensa será detenido en una capa ulterior.

La estrategia de seguridad debe incluir medidas que ofrezcan protección en las siguientes capas del modelo informático de red tradicional. En general, debe planificar la seguridad desde el nivel más básico (seguridad del sistema) hasta el nivel más complejo (seguridad de transacciones).

2.1.10.1 Seguridad a nivel de sistema

Las medidas de seguridad del sistema representan la última línea de defensa contra un problema de seguridad relacionado con Internet. Por lo tanto, el primer paso de una estrategia de seguridad en Internet completa debe ser configurar debidamente la seguridad básica del sistema.

2.1.10.2 Seguridad a nivel de red

Las medidas de seguridad de la red controlan el acceso al sistema operativo y a otros sistemas de la red. Cuando se conecta la red a Internet, se deben tener implementadas las debidas medidas de seguridad adecuadas a nivel de la red para proteger los recursos internos de la red contra la intrusión y el acceso no autorizado. El medio más común para garantizar la seguridad de la red es un cortafuegos. El proveedor de servicios de Internet, puede proporcionar una parte importante del plan de seguridad de la red.

2.1.10.3 Seguridad a nivel de aplicaciones

Las medidas de seguridad a nivel de aplicaciones controlan cómo pueden interaccionar los usuarios con las aplicaciones concretas. En general, se tendrá que configurar valores de seguridad para cada una de las aplicaciones que se utilicen. Sin embargo, conviene prestar atención especial al configurar la seguridad de las aplicaciones y los servicios que utilizará de Internet o que proporcionará a Internet. Estas aplicaciones y servicios son vulnerables al mal uso por parte de los usuarios no autorizados que buscan una manera de acceder a los sistemas de la red. Las medidas de seguridad que decida utilizar deberán incluir los riesgos del lado del servidor y del lado del cliente.

2.1.10.4 Seguridad a nivel de transmisión

Las medidas de seguridad a nivel de transmisión protegen las comunicaciones de datos dentro de la red y entre varias redes. Cuando se comunica en una red que no es de confianza como Internet, no puede controlar cómo fluye el tráfico desde el origen hasta el destino. El tráfico y los datos transportados fluyen a través de distintos sistemas que están fuera de su control. A menos que se implementen medidas de seguridad como las de configurar las aplicaciones para que utilicen la capa de sockets segura (SSL), los datos direccionados estarán a disposición de cualquier persona que desee verlos y utilizarlos. Las medidas de seguridad a nivel de transmisión protegen los datos mientras fluyen entre los límites de otros niveles de seguridad.

Una política de seguridad global de Internet, deberá desarrollar individualmente una estrategia de seguridad para cada capa. Asimismo, deberá describir cómo interaccionarán entre sí los distintos conjuntos de estrategias para ofrecer así a su empresa una red de seguridad exhaustiva.

2.2 COBIT 5

Es desarrollado por la Asociación de Auditoria y Control de Sistemas de Información ISACA, provee un marco de referencia completo que ayuda a las empresas a alcanzar sus objetivos para el Gobierno y la Gestión de TI (GEIT) de la empresa. Para decirlo simplemente, ayuda a las empresas a crear un valor óptimo de TI manteniendo un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y uso de recursos. COBIT 5 permite que la TI se gobierne y controle de manera holística en toda la empresa, incorporando el negocio integral y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, ya sean comerciales, sin fines de lucro o del sector público (ISACA, 2017).

2.2.1 Principios de Cobit 5

ISACA explica que COBIT 5 se basa en cinco principios clave para gobierno y gestión de TI empresarial, en la siguiente figura, se muestran los 5 principios del standard:

Ilustración 4. Principios de COBIT 5.

Fuente: ISACA, COBIT 5

COBIT 5 se basa en cinco principios clave para gobierno y gestión de TI empresarial los cuales se presentan a continuación:

2.2.1.1 Principio 1: Satisfacción de las necesidades de las partes interesadas.

Las empresas existen para crear valor para sus grupos de interés, manteniendo un equilibrio entre la realización de beneficios y la optimización del riesgo y uso de los recursos. COBIT 5 proporciona todos los procesos requeridos y otros facilitadores para respaldar la creación de valor del negocio a través del uso de TI. Dado que cada empresa tiene distintos objetivos, una empresa puede personalizar COBIT 5 para que se adecue a su propio contexto a través de la cascada de objetivos, traduciendo los objetivos de alto nivel de la empresa en objetivos manejables,

específicos y relacionados con TI y correlacionándolos con procesos y prácticas específicos. (ISACA, 2017, p.45).

2.2.1.2 Principio 2: Cobertura de toda la empresa.

COBIT 5 integra el gobierno de TI de la empresa dentro del gobierno de la empresa:

Abarca todas las funciones y procesos dentro de la empresa; COBIT 5 no se centra solo en las "funciones de TI", sino que trata la información y las tecnologías relacionadas como activos que todos los miembros de la empresa deben manejar como cualquier otro activo.

Considera que todos los facilitadores de gobierno y gestión relacionados con TI afectan a toda la empresa y son integrales (es decir, incluyen todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de información de la empresa y TI relacionada). (ISACA, 2017, p.47).

2.2.1.3 Principio 3: Aplicación de un marco de referencia único e integrado.

Existen muchos estándares y buenas prácticas relacionados con TI, cada uno de los cuales suministra orientación con respecto a un subconjunto de actividades de TI. COBIT 5 se alinea con otros estándares y marcos relevantes a un nivel alto y, de este modo, puede servir como el marco de referencia global para la gestión y el gobierno de TI de la empresa. (ISACA, 2017).

2.2.1.4 Principio 4: Habilitación de un enfoque holístico.

Una gestión y un gobierno eficiente y eficaz de TI de la empresa requiere un enfoque holístico, que tenga en cuenta varios componentes que interactúan entre sí. COBIT 5 define un conjunto de facilitadores para respaldar la implementación de un sistema integral de gobierno y gestión para la TI de la empresa. Los facilitadores se definen en términos generales como cualquier elemento que pueda ayudar a alcanzar los objetivos de la empresa (ISACA, 2017).

El marco COBIT 5 define siete categorías de facilitadores:

- Principios, políticas y marcos de referencia
- Procesos
- Estructuras organizacionales

- Cultura, ética y comportamiento
- Información
- Servicios, infraestructura y aplicaciones
- Personas, habilidades y competencias

2.2.1.5 Principio 5: Separación de gobierno y gestión.

El marco COBIT 5 hace una distinción clara entre gobierno y gestión. Estas dos disciplinas abarcan distintos tipos de actividades, requieren distintas estructuras organizacionales y sirven a diferentes propósitos. (ISACA, 2017). El punto de vista de COBIT 5 con respecto a esta diferencia clave entre gobierno y gestión está definida en la siguiente sección, es importante mencionar que para efectos de la presente investigación, se han considerado solo los procesos que tienen injerencia en temas de seguridad.

2.2.2 Procesos de gestión

Según COBIT (2012) el dominio de Gestión APO (Alinear, Planificar y Organizar) cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir mejor con los objetivos del negocio. Es importante mencionar que la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas; y finalmente, la implementación de una estructura organizacional y tecnológica apropiada. Este dominio proporciona la dirección para la entrega de soluciones y la entrega de servicios.

2.2.2.1 APO12 Gestionar el riesgo

Descripción del Proceso: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. (COBIT, 2012, p.107).

Declaración del Propósito del Proceso: Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI. (COBIT 5, 2012).

El proceso apoya la consecución de un conjunto de principales metas TI	
Meta TI	**Métricas Relacionadas**
02. Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste del incumplimiento de TI, incluyendo acuerdos judiciales y multas, y el impacto de pérdida de reputación • Número de asuntos de incumplimiento relacionados con TI reportados a la junta que llegan a ser de dominio público o que provocan situaciones de escándalo • Número de asuntos de incumplimiento relacionados con acuerdos contractuales con proveedores de servicio TI • Cobertura de la evaluación del cumplimiento
04. Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
06. Transparencia de los costes, beneficios y riesgo de las TI • Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados.	• Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados. • Encuesta de satisfacción a las partes interesadas clave relativa al nivel de transparencia, comprensión y precisión de la información financiera de TI.
10. Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública • Número de servicios de TI con los requisitos de seguridad pendientes • Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías

El proceso apoya la consecución de un conjunto de principales metas TI	
Meta TI	**Métricas Relacionadas**
13. Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	• Número de programas/proyectos ejecutados en plazo y en presupuesto • Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto • Número de programas que necesitan ser revisados significativamente debido a defectos de calidad • Coste del mantenimiento de aplicaciones respecto al coste total de TI

Tabla 2. APO12 Apoyo de metas de TI.

Fuente: COBIT 5, 2012, p.107

Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. El riesgo relacionado con TI está identificado, analizado, gestionado y reportado	• El grado de visibilidad y reconocimiento en el entorno actual. • Numero de eventos de perdida con características clave, capturados en repositorios. • Porcentaje de auditorías, eventos y tendencias capturados en repositorios
2. Existe un perfil de riesgo actual y completo	• Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado. • Completitud de atributos y valores en el perfil de riesgo.
3. Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control.	• Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado. • Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos.
4. Las acciones de gestión de riesgos están efectivamente implementadas.	• Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados. • Número de medidas que no reducen el riesgo residual.

Tabla 3. APO12 Objetivos y Metricas de Proceso.

Fuente: COBIT 5, 2012, p.107

2.2.2.2 APO 13 Gestionar la seguridad

Descripción del Proceso: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. (COBIT 5, 2012, p. 107)

Propósito: Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa. (COBIT 5, 2012)

El proceso contribuye al logro de un conjunto de objetivos principales relacionados con TI	
Metas TI	**Métricas Relacionadas**
02. Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI • Cobertura de las evaluaciones de conformidad
04. Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
06. Transparencia de los costes, beneficios y riesgo de las TI	• Porcentaje de casos de inversión de negocio, que tienen claramente definidos y aprobados los costes y beneficios esperados relacionados con TI • Porcentaje de servicios de TI que tienen claramente definidos y aprobados los costes operacionales y los beneficios esperados • Encuestas de satisfacción dirigidas a los principales accionistas en relación con el nivel de transparencia, entendimiento y precisión de la información financiera de TI.
10. Seguridad de la información, infraestructura de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública. • Número de servicios de TI con los requisitos de seguridad pendientes.

El proceso contribuye al logro de un conjunto de objetivos principales relacionados con TI	
Metas TI	**Métricas Relacionadas**
	• Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados. • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías.
14. Disponibilidad de información útil y relevante para la toma de decisiones	• Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión. • Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información. • Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa.

Tabla 4. APO13 Apoyo de metas de TI.

Fuente: COBIT 5, 2012, p.113

Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos. • Número de incidentes relacionados con la seguridad.
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa. • Número de soluciones de seguridad que se desvían del plan. • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa.
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad. • Número de incidentes de seguridad causados por la no observancia del plan de seguridad. • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad.

Tabla 5. APO13 Objetivos y Metricas de Proceso.

Fuente: COBIT 5, 2012, p.113

2.2.2.3 DSS06 Gestionar los servicios de seguridad

Descripción de Proceso: Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos. (COBIT 5, 2012, p. 197)

Propósito del proceso: Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados. (COBIT 5, 2012)

El proceso apoya la obtención de un conjunto de objetivos relacionados con las TI	
Metas TI	**Métricas Relacionadas**
04. Riesgos de negocio relacionados con las TI gestionados.	• Porcentaje de procesos de negocio críticos, servicios TI y programas de • Negocio, habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los • riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo
07. Entrega de servicios TI de acuerdo con los requisitos del negocio.	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI • Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados. • Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados.

Tabla 6. DSS06 Apoyo de metas de TI.

Fuente: COBIT 5, 2012, p.197

Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. La cobertura y efectividad de los controles clave para cumplir con los requerimientos de negocio para el procesamiento de la información es completa.	• Porcentaje completado de inventario de procesos críticos y controles clave. • Porcentaje de controles clave cubiertos con los planes de pruebas. • Número de incidentes y evidencias del informe de auditoría indicando fallos de los controles clave
2. El inventario de roles, responsabilidades y derechos de acceso está alineado con las necesidades autorizadas de negocio.	• Porcentaje de roles de proceso de negocio con derechos de acceso y niveles de autorización asignados. • Porcentaje de roles de proceso de negocio con una separación clara de tareas. • Número de incidentes y evidencias de auditoría debido a acceso o violación de segregación de funciones.
3. Las transacciones de negocio son retenidas completamente y según se requiera en registros.	• Porcentaje de completitud de registros de transacciones rastreables • Número de incidentes donde el historial de transacciones no pueda ser recuperado.

Tabla 7. DSS06 Objetivos y Metricas de Proceso.

Fuente: COBIT 5, 2012, p.197

2.2.3 Procesos de Gobierno

Supervisar, Evaluar y Valorar (MEA): La totalidad de los procesos de TI deben de ser evaluados regularmente en el tiempo, para conocer su calidad y cumplimiento de los requerimientos de control. Este dominio incluye la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Con esto se obtendrá de manera oportuna la detección de problemas por medio de la medición del desempeño, se garantiza que los controles internos sean efectivos y eficientes, la

vinculación del desempeño de TI con las metas del negocio, así como la medición y reporte de riesgos, además del control, cumplimiento y desempeño. (COBIT 5, 2012, p.207).

2.2.3.1 MEA02 Supervisar, evaluar y valorar el sistema de control interno

Supervisar, Evaluar y Valorar el Sistema de Control Interno: Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

Propósito del Proceso. Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual. (COBIT 5, 2012, p.207).

El proceso apoya la consecución de un conjunto de principales metas TI	
Meta TI	**Métricas Relacionadas**
02. Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas.	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación. • Número de problemas de no conformidad relativos a TI de los que se ha informado al consejo de administración o que han causado comentarios o bochorno públicos. • Número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI. • Cobertura de las evaluaciones de conformidad.
04. Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos. • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos. • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI Frecuencia de actualización del perfil de riesgo.

El proceso apoya la consecución de un conjunto de principales metas TI	
Meta TI	**Métricas Relacionadas**
15. Cumplimiento de las políticas internas por parte de TI	• Número de incidentes relacionados con el incumplimiento de la política • Porcentaje de partes interesadas que comprenden las políticas. • Porcentaje de políticas soportadas por estándares y prácticas de trabajo efectivas. • Frecuencia de revisión y actualización de las políticas.

Tabla 8, MEA02 Apoyo de metas de TI.

Fuente: COBIT 5, 2012, p.207

Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Los procesos, recursos e información cumplen con los requisitos del sistema de control interno de la empresa.	• Porcentaje de procesos con la seguridad de que las salidas cumplen el objetivo dentro de los márgenes de tolerancia. • Porcentaje de procesos con la seguridad de que son conformes con las metas de control interno.
2. Todas las iniciativas de aseguramiento se planean y ejecutan de forma efectiva.	• Porcentaje de iniciativas de aseguramiento que siguen a programas de aseguramiento aprobados y los estándares de planificación
3. Se proporciona aseguramiento independiente de que el sistema de control interno es operativo y efectivo.	• Porcentaje de procesos bajo revisión independiente
4. El control interno está establecido y las deficiencias son identificadas y comunicadas.	• Número de debilidades identificadas en los informes externos de certificación y cualificación. • Número de brechas mayores en el control interno. • Tiempo transcurrido entre la ocurrencia de la deficiencia del control interno y su comunicación.

Tabla 9. MEA02 Objetivos y Metricas de Proceso.

Fuente: COBIT 5, 2012, p.207

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 la adopción de medidas de seguridad uniformes a nivel mundial. (Security Standards Council, 2018, p.5).

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). (Security Standards Council, 2018).

2.3.1 Aplicabilidad de las PCI DSS

El Consulado de standard de seguridad (Security Standards Council) explica que la norma PCI DSS es aplicable a todas las entidades que participan en el procesamiento, almacenamiento y transmisión información de las tarjetas de pago, entre las cuales se pueden mencionar comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicio. (Security Standards Council, 2018, p.7).

A continuación, se definen cuáles son los datos del titular y los datos de autenticación confidenciales a los cuales se protegen con el uso del estándar PCI DSS:

Datos de Cuentas	
Los datos de titulares de tarjetas incluyen:	Los datos confidenciales de autenticación incluyen:
• Número de cuenta principal (PAN) • Nombre del Titular de la tarjeta • Fecha de vencimiento • Código de servicio	• Contenido completo de la pista (banda magnética o datos equivalentes que están en el chip) • CAV2/CVV2/CVV2/CID • PIN/ Bloqueos de PIN

Tabla 10. Datos de Cuentas.

Fuente: Security, Standards Council, 2018, p.7

Según la normativa, se definen cuáles son los datos que no deben ser guardados incluso si están cifrados, Esto se implementa aun cuando no haya cifrado de la información. Las organizaciones deben comunicarse con sus adquirientes o directamente con las marcas de pago para saber si se puede almacenar los datos SAD (datos de autenticación confidenciales) antes de la autorización y durante cuánto tiempo. (Security Standards Council, 2018).

En la siguiente tabla, se explica cuáles son los datos que no están permitidos almacenar:

		Elementos de datos	Almacenamiento permitido
Datos de cuentas	Datos de la tarjeta	Número de cuenta principal (PAN)	Si
		Nombre del titular de la tarjeta	Si
		Código de servicio	Si
	Datos confidenciales de autenticación	Fecha de vencimiento	Si
		Contenido completo de la pista o chip	No
		CAV2/CVV2/CVV2/CID	No
		PIN/ Bloqueo de PIN	No

Tabla 11. Datos no permitidos de almacenar

Fuente: Security, Standards Council, 2018, p.7

2.3.2 Alcance de los requisitos de las PCI DSS

Los requisitos de seguridad de la PCI DSS se aplican a todos los componentes del sistema que sean incluidos dentro del entorno CDE (entorno de datos del titulas de la tarjeta):

- Servicios de seguridad (servidores de autenticación, firewalls internos)
- Componentes de virtualización como Interruptores/routers virtuales, escritorios virtuales e hipervisores.
- Componentes de red como firewalls, puntos de acceso inalámbricos.
- Tipos de servidores (por ejemplo Web, Aplicación, Bases de datos, autenticación, correo, proxy y DNS)
- Aplicaciones que abarcan otras aplicaciones compradas o personalizadas.

El estándar explica que el primer paso es determinar con exactitud al alcance de la revisión. Y es la entidad evaluada la encargada confirmar el alcance de las PCI DSS al identificar todas las ubicaciones y los flujos de datos del titular de la tarjeta, e identificar todos los sistemas a los que están conectados y que podrían tener injerencia en el riesgo (Security, Standards Council, 2018, p.10).

2.3.3 Normativa PCI DSS v3.2.1

A continuación, encontrará una descripción general de alto nivel de los 12 requisitos de las DSS de la PCI:

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req. 1	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta	1.1. Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. 1.2. Desarrolle configuraciones para firewalls y routers que restrinjan las conexiones entre redes no confiables. 1.3. Prohíba el acceso directo público entre Internet y todo componente del sistema en el entorno de datos de los titulares de tarjetas. 1.4 Instale software de firewall personal o una funcionalidad equivalente en todos los dispositivos móviles.

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req 2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad	2.1. Siempre cambie los valores predeterminados por el proveedor y elimine o deshabilite las cuentas predeterminadas. 2.2. Desarrolle normas de configuración para todos los componentes de sistemas. 2.3. Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido. 2.4. Lleve un inventario de los componentes del sistema que están dentro del alcance de las PCI DSS. 2.5. Asegúrese de que las políticas de seguridad y los parámetros predeterminados del proveedor estén documentados, implementados y que sean de conocimiento para todas las partes afectadas. 2.6. Los proveedores de hosting compartido deben proteger el entorno y los datos del titular de la tarjeta que aloja la entidad.
Req. 3	Proteger los datos del titular de la tarjeta	3.1. Almacene la menor cantidad posible de datos del titular de la tarjeta. 3.2. No almacene datos confidenciales de autenticación después de recibir la autorización (aun cuando estén cifrados). 3.3. Enmascare el PAN (número de cuenta principal). 3.4 Convierta el PAN (número de cuenta principal) en ilegible en cualquier lugar donde se almacene. 3.5 Documente e implemente procedimientos que protejan las claves utilizadas. 3.6. Documente por completo e implemente todos los procesos y procedimientos de administración de claves criptográficas. 3.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para proteger los datos del titular de la tarjeta almacenados estén documentados

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req 4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.	4.1. Utilizar criptografía sólida y protocolos de seguridad. 4.2. Nunca debe enviar PAN no cifrados por medio de tecnologías de mensajería. 4.3. Asegúrese de que las políticas de seguridad y los procedimientos operativos para cifrar las transmisiones de los datos del titular de la tarjeta estén documentados.
Req 5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.	5.1. Implemente un software antivirus en todos los sistemas. 5.2. Asegúrese de que los mecanismos de antivirus estén actualizados, ejecuten análisis periódicos y generen registros de auditoría que se guarden de conformidad con el Requisito 10.7 de las PCI DSS. 5.3. Asegúrese de que los mecanismos de antivirus funcionen activamente. 5.4 Asegúrese de que las políticas de seguridad y los procedimientos operativos estén documentados e implementados.

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req 6	Desarrollar y mantener sistemas y aplicaciones seguros	6.1. Establezca un proceso para identificar las vulnerabilidades de seguridad. 6.2 Asegúrese de que todos los software y componentes del sistema tengan instalados parches de seguridad. 6.3. Desarrolle aplicaciones de software internas y externas de manera segura. 6.4 Siga los procesos y procedimientos de control de todos los cambios en los componentes del sistema. 6.5 Aborde las vulnerabilidades de codificación comunes en los procesos de desarrollo. 6.6. En el caso de aplicaciones web públicas, trate las nuevas amenazas y vulnerabilidades continuamente. 6.7 Asegúrese de que las políticas de seguridad y los procedimientos operativos para desarrollar y mantener seguros los sistemas y las aplicaciones estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.
Req 7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa	7.1. Limite el acceso a los componentes del sistema. 7.2 Establezca un sistema de control de acceso para los componentes del sistema. 7.3. Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso estén documentados e implementados.

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req 8	Identificar y autenticar el acceso a los componentes del sistema.	8.1. Defina e implemente políticas y procedimientos para garantizar la correcta administración de la identificación de usuarios en todos los componentes del sistema. 8.2. Además de asignar una ID exclusiva, asegúrese de que haya una correcta administración de autenticación de usuarios. 8.3. Asegure todo el acceso administrativo individual que no sea de consola y todo el acceso remoto al CDE mediante la autenticación de múltiples factores. 8.4. Documente y comunique los procedimientos y las políticas de autenticación a todos los usuarios. 8.5 No use ID ni contraseñas de grupo, compartidas ni genéricas. 8.6. Los mecanismos de autenticación deben ser asignados a una sola cuenta y se deben implementar controles físicos y lógicos. 8.7. Se restringen todos los accesos a cualquier base de datos que contenga datos del titular de la tarjeta. 8.8. Asegúrese de que las políticas de seguridad y los procedimientos operativos de identificación y autenticación estén documentados

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req. 9	Restringir el acceso físico a los datos del titular de la tarjeta.	9.1. Utilice controles de entrada a la empresa apropiados para limitar y supervisar el acceso físico. 9.2. Desarrolle procedimientos que permitan distinguir, fácilmente, a los empleados y a los visitantes. 9.3. Controle el acceso físico de los empleados a las áreas confidenciales. 9.4. Implemente procedimientos para identificar y autorizar a los visitantes. 9.5. Proteja físicamente todos los medios. 9.6 Lleve un control estricto de la distribución interna o externa. 9.7. Lleve un control estricto del almacenamiento y la accesibilidad de los medios. 9.8. Destruya los medios cuando ya no sea necesario guardarlos. 9.9. Proteja los dispositivos que capturan datos de tarjetas de pago. 9.10. Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta estén documentados, implementados

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req. 10	Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta	10.1. Implemente pistas de auditoría para vincular todo acceso a componentes del sistema con usuarios específicos. 10.2. Implemente pistas de auditoría automáticas en todos los componentes del sistema. 10.3. Registre, al menos, las siguientes entradas de pistas de auditoría: Id de usuarios, tipo de evento, Fecha y Hora. 10.4. Utilizando tecnología de sincronización, sincronice todos tiempos y relojes críticos y asegúrese de que lo siguiente sea implementado para adquirir, distribuir y almacenar tiempos. 10.5. Proteja las pistas de auditoría para que no se puedan modificar. 10.6. Revise los registros y los eventos de seguridad en todos los componentes. 10.7. Conserve el historial de pistas de auditorías durante, al menos, un año. 10.8. Implementar un proceso para la detección y el informe oportunos de fallas de los sistemas. 10.9. Asegúrese de que las políticas de seguridad y los procedimientos operativos estén documentados, implementados.

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req 11	Probar periódicamente los sistemas y procesos de seguridad.	11.1. Implemente procesos para determinar la presencia de puntos de acceso inalámbrico (802.11) 11.2. Realice análisis internos y externos de las vulnerabilidades de la red. 11.3. Implemente una metodología para las pruebas de penetración. 11.4. Use técnicas de intrusión-detección y de intrusión-prevención para detectar o prevenir intrusiones en la red. 11.5. Implemente un mecanismo de detección de cambios. 11.6. Asegúrese de que las políticas de seguridad y los procedimientos operativos para monitorear y comprobar la seguridad estén documentados, implementados.

Normas de seguridad de datos de la PCI: Descripción general de alto nivel		
Numero de requerimiento	**Requisitos de la PCI**	**Procedimiento de Prueba**
Req. 12	Mantener una política que aborde la seguridad de la información para todo el personal.	12.1. Establezca, publique, mantenga y distribuya una política de seguridad. 12.2. Implemente un proceso de evaluación de riesgos que cumpla con lo siguiente. 12.3. Desarrolle políticas de uso para las tecnologías críticas y defina cómo usarlas correctamente. 12.4. Asegúrese de que las políticas y los procedimientos de seguridad definan, claramente, las responsabilidades de seguridad de la información de todo el personal. 12.5. Asigne a una persona o a un equipo responsabilidades de administración de seguridad de la información. 12.6. Implemente un programa formal de concienciación sobre seguridad. 12.7. Examine al personal potencial antes de contratarlo a fin de minimizar el riesgo de ataques desde fuentes internas. 12.8. Mantenga e implemente políticas y procedimientos para administrar los proveedores de servicios con quienes se compartirán datos. 12.9. Los proveedores de servicios aceptan, por escrito y ante los clientes, responsabilizarse de la seguridad de los datos del titular de la tarjeta. 12.10. Implemente un plan de respuesta ante incidentes. 12.11. Realizar revisiones es para confirmar que el personal sigue las políticas de seguridad y los procedimientos operativos.

Tabla 12. Normativa de Seguridad PCI DSS.

Fuente: Security Standards Council, 2018, p.5

La PCI DSS comprende un conjunto mínimo de requisitos para proteger los datos de cuentas y se puede mejorar por medio de controles y prácticas adicionales a fin de mitigar los riesgos, así como leyes y regulaciones locales, regionales y sectoriales. Además, los requisitos de la legislación o las regulaciones pueden requerir la protección específica de la información de identificación personal u otros elementos de datos (por ejemplo, el nombre del titular de tarjeta). Las PCI DSS no sustituyen las leyes locales ni regionales, las regulaciones gubernamentales ni otros requisitos legales.

2.3.4 Mejores prácticas para implementar las PCI-DSS

A fin de garantizar que los controles de seguridad se sigan implementando correctamente, las PCI DSS deberán implementarse en las actividades BAU (habituales) como parte de la estrategia general de seguridad. Esto permite que la entidad supervise constantemente la eficacia de los controles de seguridad y que mantenga el cumplimiento de las PCI DSS en el entorno entre las evaluaciones de las PCI DSS. (Security Standards Council, 2018, p.13).

Ejemplos de cómo incorporar las PCI DSS en las actividades BAU incluyen, pero no se limitan a:

1. Monitorear los controles de seguridad, tales como firewalls, IDS/IPS (sistemas de intrusión-detección o de intrusión-prevención), FIM (supervisión de la integridad de archivos), antivirus, controles de acceso, etc., para asegurarse de que funcionan correctamente y según lo previsto.
2. Garantizar la detección de todas las fallas en los controles de seguridad y solucionarlas oportunamente. Los procesos para responder en caso de fallas en el control de seguridad son los siguientes:
    - Restaurar el control de seguridad.
    - Identificar la causa de la falla.
    - Identificar y abordar cualquier problema de seguridad que surja durante la falla del control de seguridad.
    - Implementar la mitigación (como procesos o controles técnicos) para evitar que la causa reaparezca.

Reanudar la supervisión del control de seguridad, quizás con una supervisión mejorada durante un tiempo a fin de verificar que el control funcione correctamente.

3. Revisar los cambios implementados en el entorno (por ejemplo, incorporación de nuevos sistemas, cambios en las configuraciones del sistema o la red) antes de finalizar el cambio y realizar las siguientes actividades:
   - Determinar el posible impacto en el alcance de las PCI DSS (por ejemplo, una nueva regla para los firewalls que permita la conectividad entre un sistema del CDE y otro sistema puede incorporar sistemas o redes adicionales al alcance de las PCI DSS).
   - Identificar los requisitos de las PCI DSS correspondientes a los sistemas y las redes afectados por los cambios (por ejemplo, si un nuevo sistema está dentro del alcance de las PCI DSS, se deberá configurar de acuerdo con las normas de configuración de sistemas, entre otros, FIM (supervisión de la integridad de archivos), AV (antivirus), parches, registros de auditorías, etc., y se deberá incorporar al programa trimestral de análisis de vulnerabilidades).
   - Actualizar el alcance de las PCI DSS e implementar los controles de seguridad, según sea necesario.
4. Si se implementan cambios en la estructura organizativa (por ejemplo, la adquisición o fusión de una empresa), se debe realizar una revisión formal del impacto en el alcance y en los requisitos de las PCI DSS.
5. Se deben realizar revisiones y comunicados periódicos para confirmar que los requisitos de las PCI DSS se siguen implementando y que el personal cumple con los procesos de seguridad. Estas revisiones periódicas deben abarcar todas las instalaciones y ubicaciones, en las que se incluyen tiendas minoristas, centros de datos, etc., e incluir la revisión de los componentes del sistema (o muestras de los componentes del sistema) a fin de verificar que siguen implementados los requisitos de las PCI DSS; por ejemplo, normas de configuración implementadas, parches y AV (antivirus) actualizados, registros de auditorías revisados y así sucesivamente. La entidad debe determinar la frecuencia de las revisiones periódicas en función del tamaño y de la complejidad del entorno (Security Standards Council, 2018, p.14).

Estas revisiones también se pueden usar para verificar que se mantiene la evidencia correspondiente, por ejemplo, registros de auditorías, informes de análisis de vulnerabilidades, revisiones de firewall, etc., para ayudar a la entidad a prepararse para la siguiente evaluación sobre cumplimiento.

6. Revisar las tecnologías de hardware y software, al menos, una vez al año para confirmar que el proveedor las sigue admitiendo y que pueden satisfacer los requisitos de seguridad de la entidad, incluida la PCI DSS. Si se detecta que el proveedor ya no puede admitir las tecnologías o que no pueden satisfacer las necesidades de seguridad de la entidad, la entidad debe preparar un plan de recuperación que incluya el reemplazo de la tecnología si fuera necesario.

Además de las prácticas anteriores, las organizaciones también deben considerar la opción de separar las tareas de las funciones de seguridad de modo que las funciones de seguridad y auditorías sean independientes de las funciones operativas. En entornos en los que una persona desempeña varias funciones (por ejemplo, operaciones de administración y seguridad), las tareas se deben asignar de manera tal que ninguna persona tenga control completo de un proceso sin un punto de verificación independiente. Por ejemplo, las tareas de configuración y de aprobación de cambios se pueden asignar a dos personas distintas. (Security Standards Council, 2018, p14).

2.3.5 Controles de compensación

Los controles de compensación se pueden tener en cuenta para la mayoría de los requisitos de las PCI DSS cuando una entidad no puede cumplir con un requisito explícitamente establecido, debido a los límites comerciales legítimos técnicos o documentados, pero pudo mitigar el riesgo asociado con el requisito de forma suficiente, mediante la implementación de otros controles, o controles de compensación (Security Standards Council, 2018, p.159).

Los controles de compensación deben cumplir con los siguientes criterios:

1. Cumplir con el propósito y el rigor del requisito original de las PCI DSS.
2. Proporcionar un nivel similar de defensa, tal como el requisito original de PCI DSS, de manera que el control de compensación compense el riesgo para el cual se diseñó el requisito original de las PCI DSS. (Consulte la columna de guía para obtener el propósito de cada requisito de PCI DSS).

3. Conozca en profundidad otros requisitos de las PCI DSS. (El simple cumplimiento con otros requisitos de las PCI DSS no constituye un control de compensación).

Los requisitos de las PCI DSS no se pueden considerar controles de compensación si ya fueron requisito para el elemento en revisión. Por ejemplo, las contraseñas para el acceso administrativo sin consola se deben enviar cifradas para mitigar el riesgo de que se intercepten contraseñas administrativas de texto claro. Una entidad no puede utilizar otros requisitos de contraseña de las PCI DSS (bloqueo de intrusos, contraseñas complejas, etc.) para compensar la falta de contraseñas cifradas, puesto que esos otros requisitos de contraseña no mitigan el riesgo de que se intercepten las contraseñas de texto claro. Además, los demás controles de contraseña ya son requisitos de las PCI DSS para el elemento en revisión (contraseñas). (Security Standards Council, 2018, p.159).

Los requisitos de las PCI DSS se pueden considerar controles de compensación si se requieren para otra área, pero no son requisito para el elemento en revisión.

Los requisitos existentes de las PCI DSS se pueden combinar con nuevos controles para convertirse en un control de compensación. Por ejemplo, si una empresa no puede dejar ilegibles los datos de los titulares de tarjetas según el requisito 3.4 (por ejemplo, mediante cifrado), un control de compensación podría constar de un dispositivo o combinación de dispositivos, aplicaciones y controles que aborden todo lo siguiente: (1) segmentación de red interna; (2) filtrado de dirección IP o dirección MAC y (3) contraseñas de un solo uso. (Security Standards Council, 2018).

4. Sea cuidadoso con el riesgo adicional que impone la no adhesión al requisito de las PCI DSS

El asesor debe evaluar por completo los controles de compensación durante cada evaluación anual de PCI DSS para validar que cada control de compensación aborde de forma correcta el riesgo para el cual se diseñó el requisito original de PCI DSS, según los puntos 1 a 4 anteriores. Para mantener el cumplimiento, se deben aplicar procesos y controles para garantizar que los controles de compensación permanezcan vigentes después de completarse la evaluación (Security Standards Council, 2018, p.159).

2.3.6 Ejemplo Requerimiento 3: Proteger los datos del Titular

A continuación, se detalla el primer requisito de la norma PCI número 3, para ilustrar el contenido de cada norma, dado que las normas PCI son muy extensas y no es práctico incluir todo su contenido en este proyecto. Cada norma PCI incluye los requisitos de la PCI DSS, los procedimientos de prueba y la guía de ejecución.

Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la función de hash son importantes componentes para proteger los datos de los titulares de tarjetas. Si un intruso viola otros controles de seguridad y obtiene acceso a los datos cifrados, sin las claves de cifrado adecuadas, no podrá leer ni utilizar esos datos. También se deberían considerar otros métodos eficaces para proteger los datos almacenados oportunidades para mitigar posibles riesgos. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar datos del titular de la tarjeta, salvo que sea absolutamente necesario; truncar los datos del titular de la tarjeta si no se necesita el PAN (número de cuenta principal) completo y no enviar el PAN (número de cuenta principal) utilizando tecnologías de mensajería de usuario final, como correo electrónico y mensajería instantánea (Security Standards Council, 2018, p.36).

2.3.6.1 Requerimiento de la PCI DSS

3.1 Almacene la menor cantidad posible de datos del titular de la tarjeta implementando políticas, procedimientos y procesos de retención y eliminación de datos que incluyan, al menos, las siguientes opciones para el almacenamiento de CHD (datos del titular de la tarjeta):

- Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio
- Requisitos de retención específicos para datos de titulares de tarjetas
- Procesos para eliminar datos de manera cuando ya no se necesiten
- Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan la retención definida.

2.3.6.2 Procedimientos de prueba

3.1.a. Revise las políticas, los procedimientos y los procesos de retención y eliminación de datos y verifique que incluyen lo siguiente para todo el almacenamiento de los datos del titular de la tarjeta (CHD):

Limitación del almacenamiento de datos y del tiempo de retención a la cantidad exigida por los requisitos legales, reglamentarios y del negocio.

Requisitos específicos para la retención de datos del titular de la tarjeta (por ejemplo, los datos del titular de la tarjeta se deben mantener durante X tiempo por Y razones de la empresa).

Eliminación segura de los datos del titular de la tarjeta cuando ya no son necesarios por motivos legales, reglamentarios o empresariales.

Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan los requisitos de retención definidos.

3.1.b Entreviste al personal y verifique lo siguiente: • Todos los lugares donde se almacenan datos de titulares de tarjetas están incluidos en los procesos de retención y eliminación de datos. • Se implementa un proceso trimestral automático o manual para identificar y eliminar, de manera segura, los datos de titulares de tarjetas almacenados.

El proceso trimestral automático o manual se lleva a cabo en todas las ubicaciones de datos de titulares de tarjetas.

3.1.c Para obtener una muestra de los componentes del sistema que almacenan datos del titular de la tarjeta:

Revise los archivos y los registros del sistema para verificar que los datos almacenados no superen los requisitos definidos en la política de retención de datos.

Observe el mecanismo de eliminación y verifique que los datos se eliminen de manera segura.

2.3.6.3 Guía

Una política formal para la retención de datos identifica los datos que se deben conservar, así como el lugar donde residen los datos, de modo que se puedan destruir o eliminar de manera segura cuando ya no sean necesarios. Los únicos datos del titular de la tarjeta que se pueden almacenar después de la autorización son el número de cuenta principal o PAN (que debe ser ilegible), la fecha de vencimiento, el nombre del titular de la tarjeta y el código de servicio. Es necesario saber dónde se encuentran los datos del titular de la tarjeta para poder conservarlos o

eliminarlos correctamente cuando ya no sean necesarios. A fin de definir los requisitos de retención apropiados, una entidad primero debe entender las necesidades de su negocio, así como cualesquiera obligaciones legales y regulatorias que se apliquen a su industria, y/o que se apliquen al tipo de dato que se retiene (Security Standards Council, 2018).

Identificar y eliminar los datos almacenados que hayan excedido el período de retención especificado evita la retención de datos innecesarios. Este proceso puede ser automático o manual, o una combinación de las dos opciones. Por ejemplo, se podría implementar un procedimiento programático (automático o manual) para encontrar y eliminar datos, o una revisión manual de las áreas de almacenamiento de datos. La implementación de métodos de eliminación seguros asegura que los datos no se puedan recuperar cuando ya no sean necesarios (Security Standards Council, 2018, p.37).

2.4 ISO 27001 INFORMATION SEGURITY MANAGEMENT

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. (ISO 27001, 2013).

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. (ISO 27001, 2013).

2.4.1 Funcionamiento de la Norma ISO 27001

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). (ISO 27001, 2013).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI). (ISO 27001, 2013).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

2.4.2 Ventajas de utilizar la norma ISO 27001

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

Cumplir con los requerimientos legales: cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

Obtener una ventaja comercial: si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

Menores costos: la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

Una mejor organización: en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados. (ISO 27001, 2013).

2.4.3 Gestión de seguridad de la información en una empresa

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información:

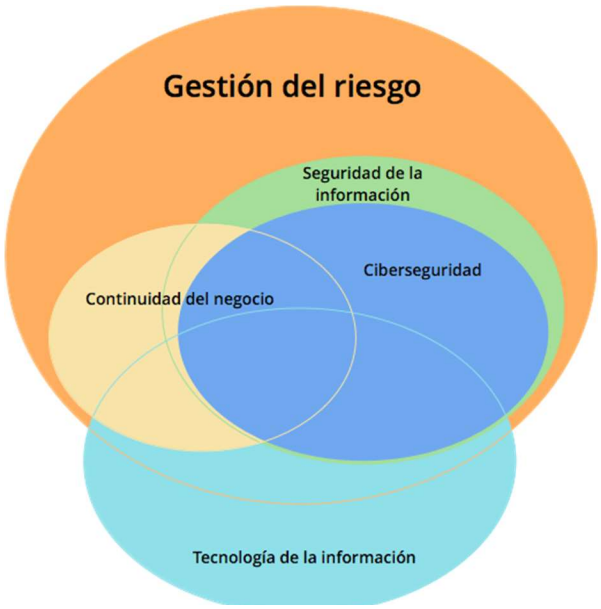


Ilustración 5. Gestion del riesgo segun ISO.

Fuente ISO 27001, 2013

2.4.4 Estructura de la Norma ISO 27001

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas:

- **Sección 0 – Introducción** – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
- **Sección 1 – Alcance** – explica que esta norma es aplicable a cualquier tipo de organización.
- **Sección 2 – Referencias normativas** – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.
- **Sección 3 – Términos y definiciones** – de nuevo, hace referencia a la norma ISO/IEC 27000.
- **Sección 4 – Contexto de la organización** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
- **Sección 5 – Liderazgo** – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
- **Sección 6 – Planificación** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

- **Sección 7 – Apoyo** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
- **Sección 8 – Funcionamiento** – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.
- **Sección 9 – Evaluación del desempeño** – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
- **Sección 10 – Mejora** – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

3 CAPÍTULO III: MARCO METODOLÓGICO

En este capítulo se explica la forma en que se desarrolla la metodología de investigación aplicada en este proyecto de graduación; se detalla la forma en que se obtiene y recopila la información para su posterior análisis y para el planteamiento del modelo que se propondrá en capítulos posteriores.

Sordo, I. en su libro Metodología para elaborar una Tesis, describe el marco metodológico como "el capítulo que explica la metodología, que informa la manera de realizar la investigación y obtener los datos para el análisis; también se describen los instrumentos y las técnicas empleadas para recolectar los datos. En síntesis, corresponde detallar todos los procedimientos ejecutados y con ello demostrar la validez y autenticidad de la investigación." (2016, p. 71).

En esta sección de la tesis se conocerán temas como el tipo de investigación a desarrollar, su alcance, cuáles son las fuentes de información empleadas, técnicas e instrumentos de recolección de datos, procedimientos metodológicos y por último se describirá la operacionalización e instrumentalización de las variables usadas.

3.1 TIPO DE INVESTIGACIÓN

Según el Diccionario de la Real Academia, el significado de la palabra investigar es realizar actividades intelectuales y experimentales de modo sistemático con el propósito de aumentar los conocimientos sobre una determinada materia (RAE, 2019). Por lo tanto, este trabajo se desarrolla en forma ordenada, y a través de la recolección y análisis de información y se elaborará uno o varios modelos en forma experimental hasta lograr el objetivo buscado.

Echeverria define que las investigaciones se clasifican según su dimensión temporal, según su profundidad o según su enfoque. (Barrantes, 2018, p55).

En la siguiente figura, podemos apreciar la clasificación de los tipos de investigación que hace Echeverria:

Ilustración 6. Tipos de Investigación.

Fuente Barrantes, 2018, p.56

3.1.1 Clasificación de Dimensión Temporal

En cuanto a su dimensión temporal, la presente investigación de define como descriptiva, ya que se hace un estudio de la situación actual describiendo las características se hace una exploración de la aplicación en su estado actual y el manejo de la información en cuanto a seguridad y el cumplimiento al estándar PCI DSS.

3.1.2 Clasificación según su profundidad

Referente a su profundidad, se puede definir la presente investigación como experimental, ya que se hace una propuesta de metodología que no ha sido antes implementada en la aplicación en estudio.

3.1.3 Clasificación según su enfoque

En el desarrollo de la presente investigación se utilizarán datos cuantificables, lo que nos lleva a concluir que se utilizarán técnicas de investigación cuantitativa y adicionalmente, se

utilizarán observaciones del comportamiento de una aplicación de tecnología de la información, específicamente de la eficiencia de su diseño, lo que implica que se utilizará también la investigación cualitativa, al usar ambas metodologías califica como una metodología de investigación mixta.

A continuación, se infieren las razones por las cuales se usará cada uno de ellos:

3.1.3.1 Características de Investigación cuantitativa:

El sujeto por analizar es una aplicación y en forma específica, se determinará una metodología para analizar su cumplimiento con un estándar específico, los aspectos de este tipo de investigación que se aplicarán son:

- El contenido del estándar comprende datos precisos y es necesario documentar su cumplimiento.
- Se experimentará con varios ejercicios de análisis antes de plantear el modelo final.
- La matriz de valoración de riesgos que se planteará, aunque se elaborará un modelo sencillo, tiene valoración matemática.
- El foco es específico: cumplimiento con un estándar.
- La teoría está completamente relacionada con el diseño de la investigación a realizar.

3.1.3.2 Características de Investigación cualitativa:

Bajo el mismo entendido de que el objeto de estudio es el cumplimiento de una aplicación con un estándar específico, se identificaron los siguientes aspectos que identifican parte de la investigación a realizar como cualitativa:

- El objetivo es entender un proceso completo, el cual se trata del análisis de riesgos y cumplimiento de una aplicación con un estándar.
- La manipulación de los datos se realizará a partir de la identificación de patrones son significación.
- El modelo que se determinará se realizará de manera inductiva.

3.2 ALCANCE DE LA INVESTIGACIÓN

De acuerdo con el planteamiento de Ulate & Vargas en su libro Metodología para elaborar una Tesis, define que las investigaciones pueden tener un alcance exploratorio, descriptivo, correlacional o explicativo:

- Estudios exploratorios: se realizan cuando se debe examinar un tema poco estudiado o que nunca ha sido abordado en alguna investigación.
- Estudios explicativos: pretenden establecer las causas de cualquier evento o fenómeno estudiado, estudiando dos o más variables de las condiciones manifestadas.
- Estudio descriptivo: tiene como objetivo describir fenómenos, situaciones, contextos o eventos, detallando su significado y como se manifiestan. Su propósito está en especificar las propiedades y características de lo estudiado.
- Estudio correlacional: busca relacionar las definiciones de dos o más variables, buscando conocer la asociación que puede existir en ellas.

Este trabajo de investigación tendrá un alcance básicamente descriptivo en el cual se planteará la problemática de cumplimiento de una aplicación con un estándar y se diseñará una herramienta que ayude a plantear las mejoras necesarias para su cumplimiento.

3.3 FUENTES DE INFORMACIÓN

En este punto del proyecto es necesario establecer cuáles son las fuentes de información que le dan sustento teórico que servirá como base para obtener los conocimientos necesarios para plantear un modelo práctico que se utilizará para lograr los objetivos planteados en este proyecto de investigación. Estas fuentes de información pueden ser variadas, desde libros consultados, entrevistas a personas expertas, revistas, periódicos páginas de internet, etc. En este capítulo no se detallará una lista, debido a que esta información se incluye en las citas bibliográficas; sin embargo, si es necesario explicar su origen.

En su libro Metodología para elaborar una Tesis, Ulate & Vargas afirman que las fuentes de información se clasifican en tres tipos: primarias, secundarias y terciarias; (Ulate & Vargas,

2019, p.71). A continuación, se explica brevemente cada una de ellas e incluyen las fuentes que se usarán en este trabajo.

- Fuentes de información primarias: son aquellas que proporcionan datos de primera mano, es decir, información obtenida directamente de quien la produjo, el autor original. Puede tratarse de libros, antologías, artículos, disertaciones, documentos oficiales, trabajos presentados en una conferencia o un seminario, videocintas, foros, páginas de internet, entre otros.
- Fuentes de información secundarias: son resúmenes de fuentes primarias, compilaciones, comentarios de artículos, de libros o tesis.
- Fuentes de información terciaria: reúnen fuentes de segunda mano, como podría ser un catálogo temático, un directorio, una guía de índice, un catálogo de revistas periódicas.

3.3.1 Fuentes de información primarias:

Con base en la teoría presentada en el apartado anterior se presentan las fuentes de información primarias utilizadas en este trabajo de investigación:

- El estándar PCI-DSS (***P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard*), es la Fuente de información más importante, ya que establece las bases de evaluación de la aplicación de estudio en este proyecto de investigación.
- Bibliografía relacionada con Seguridad de la información.
- Entrevistas a profesionales expertos en el área de auditoría.
- Guías y manuales profesionales de métodologia de investigación.

3.3.2 Fuentes de información secundarias:

En este trabajo solamente se utilizará una fuente de información secundaria, la cual es el Manual para la preparación para el examen CISA; que, aunque es de autoría propia del ISACA, a la vez recoge información proveniente de otras fuentes, como lo es el Marco Conceptual de Instituto de Auditores internos *(The Institute of Internal Auditors*), ISO 27002, PCI DSS, Cobit 5, etc.

3.4 TÉCNICAS Y HERRAMIENTAS DE RECOLECCIÓN DE DATOS

Hernández define explica que para pueden hacer uso de diferentes técnicas y herramientas de recolección de datos según el tipo de enfoque que se le dé a la investigación. (Hernandez, 2014).

A continuación, se presenta una tabla explicativa con las diferentes herramientas de las que se puede hacer uso según el enfoque de la investigación:

Herramientas para Investigaciones cuantitativas	Herramientas para investigaciones cualitativas
Cuestionarios cerrados	Observación
Registro de datos estadísticos	Entrevistas profundas
Pruebas estadísticas	Sesiones de grupo
Diferentes tipos de entrevistas	Biografías
Encuestas	Revisión de archivos
	Etnografías

Tabla 13. Herramientas según enfoque de la investigación.

Fuente: Hernandez et al. (2014).

Dado que la presente investigación tiene un enfoque mixto, se considera que es conveniente el uso de diferentes técnicas y herramientas para la recolección de datos. Esto ayuda a enriquecer el criterio para la comprensión de la situación actual de la aplicación en cuanto el cumplimiento de las mejores prácticas del standard PCI DSS, de la misma forma se hace uso de herramientas que cuantifican riesgos lo que proporciona una valoración y pone en perspectiva la realización de los objetivos del presente trabajo.

3.4.1 Entrevistas

Las entrevistas permiten adquirir información de primera mano y de esta manera generar conocimiento para el desarrollo de la investigación.

Es sumamente importante tener en cuenta los objetivos de la investigación para hacer la selección de los sujetos a los cuales se les hace las entrevistas. (Ulate & Vargas, 2019, p.76). Una vez definidos los sujetos a los que se les somete a las entrevistas, se procede a definir si las entrevistas deben ser estructuradas o no estructuradas, esto con el

fin de poder obtener el mayor conocimiento sobre la situación de la aplicación y siempre teniendo en cuenta los objetivos de la investigación. (Ulate & Vargas).

Para el desarrollo de la presente investigación de hace uso de entrevistas estructuradas y no estructuradas, esto con la intención de poder extraer la mejor información para así apoyar los objetivos de la investigación.

Si bien es cierto que las entrevistas estructuradas son muy recomendables ya que se pueden definir preguntas de respuesta corta lo cual hace el trabajo del entrevistador más sencillo. (Hernandez et al. 2014). Para los efectos de la presente investigación se hace uso de entrevista con un formato no estructurado, dado que mucho de la información a adquirir es sobre procesos de negocio a los cuales apoya la aplicación en estudio, y de la cual se tiene que entender su funcionamiento en cuanto al manejo de datos de métodos de pago.

A continuación de enuncian las entrevistas no estructuradas que serán aplicadas, las cuales pueden ser consultadas en el como parte del registro de documentación de apoyo a la investigación:

a. Entrevista a un Gerente de Auditoria de Tecnológica de la Información: En el Apéndice B.01 se encuentra la presente entrevista donde se entendieron conceptos sobre los análisis de riesgos, procesos de auditoria de TI.
b. Entrevista a Gerente de Auditoria Interna: Durante esta entrevista se aclararon conceptos referentes a auditoria, conceptos de riesgos y aspectos a evaluar en procesos de auditoria. Apéndice B.02.
c. Entrevista a Auditor de Tecnologías de la Información: En esta entrevista se exploraron temas sobre la auditoria de gestión de riesgos y de los procesos de auditoria en este tipo de evaluaciones. Apéndice B.03
d. Entrevista a la Gerente Administrador de la cuenta: En esta entrevista se consultaron temas relacionados a la empresa dueña de la aplicación en estudio, funcionamiento de la aplicación y del flujo de datos. Apéndice C.

3.4.2 Revisión de Documentos

Hernandez (2014) afirma que la revisión documental es fundamental para el investigador, pues facilita el entendimiento del fenómeno central de estudio, le permite al investigador conocer sobre los antecedentes y el contexto del problema que se estudia.

En la presente investigación se hizo la revisión de la siguiente documentación:

a. Revisión bibliográfica: Se consultaron fuentes bibliográficas como libros, guías de certificación, marcos de referencia y mejores prácticas esto con el fin de conocer los parámetros en los que se basa la industria actualmente.
b. Revisión de documentación interna: se consultaron reportes de auditorías pasadas, cartas de aceptación, cartas de aceptación de riesgos, manuales de procedimientos internos, políticas de seguridad, políticas de retención de datos CHD (Datos del portador de tarjeta por sus siglas en ingles).

Con el fin de llevar un registro escrito sobre los documentos y artefactos consultados durante la investigación se hace uso de la plantilla de revisión documental en el Apéndice C.

3.4.3 Variables de Investigación

Ulate & Vargas (2019) mencionan la importancia de la definición y la instrumentalización de las variables en una investigación, ya que esta actividad da la capacidad de asumir el valor que estas tienen para el desarrollo de los objetivos definidos durante la investigación.

De tal manera el estudio de las variables de la investigación se presenta según su función en el cumplimiento con los objetivos, para lo cual se hace uso de un cuadro de variables, en donde

se pone en contraste cada una de las variables y su función en cuanto al cumplimiento de los objetivos de la investigación.

A continuación, se presenta el cuadro de variables en donde se proporciona también sus indicadores y su definición instrumental en donde se mencionan los instrumentos que se utilizaran para mostrar dicha información:

Objetivo específico	Variables de estudio	Definición conceptual	Indicadores	Definición instrumental
Proponer una herramienta de referencia para procesos de auditoria con el fin de asegurar el cumplimiento de las mejores prácticas de la industria en cuanto al manejo de datos de pago y protección de identidad	Herramienta de referencia	Herramienta de referencia para procesos de auditorías para certificación PCI DSS	Efectividad de la herramienta en el cumplimiento de los requerimientos del standard PCI DSS	• Entrevista • Revisión documental
Identificar los riesgos inherentes en la aplicación a través de la implementación de una herramienta que permita hacer una evaluación de fondo en la manera en que información sensitiva es administrada, con el fin de asegurar el cumplimiento con las mejores prácticas según la norma PCI-DSS y Cobit	Riesgos Inherentes	Identificación de los riesgos inherentes que afectan la manera en que se maneja la información sensitiva	El impacto que los riesgos representan en cuanto al buen manejo de información sensitiva	• Revisión Documental • Observación
Valorar los riesgos identificados con base en un modelo cualitativo con escala de medición ordinal, para determinar su importancia dentro de las prioridades de gestión en alineamiento con el estándar	Riesgos Identificados	Valorar los riesgos identificados en un modelo cuantitativo	El impacto que los riesgos tienen en la afectación del cumplimiento del standard	• Revisión documental • Entrevista

Objetivo específico	Variables de estudio	Definición conceptual	Indicadores	Definición instrumental
Identificar los controles diseñados para gestionar eficazmente los riesgos encontrados y a su vez evaluar su efectividad en la mitigación de la vulnerabilidad de la información	Controles para gestión de riesgos	Identificar los controles correctos para gestionar los riesgos antes encontrados	Tener la capacidad de identificar los controles adecuados para la mitigación de riesgos encontrados	• Revisión documental • Entrevistas • Observación
Valorar los riesgos residuales posteriores al proceso de gestión de controles, asimismo determinar sus repercusiones en cuanto al manejo de información sensitiva	Riesgos residuales	Valoración de los riesgos remanentes posteriormente a la implementación de controles.	Valorar los riesgos remanentes para determinar las repercusiones en el cumplimiento de la aplicación con los requerimientos del estándar	• Revisión Documental • Entrevista • Observación

Tabla 14. Definicion de Variables. Fuente: Creacion Propia

3.4.4 Diseño de la Investigación

El diseño de la investigación es un plan estratégico que se desarrolla con el fin de garantizar que la investigación se de en un orden secuencial y para asegurar la cohesión entre temas que se plantean para así propiciar que la investigación genere mejores resultados y proporcione mayor conocimiento. (Hernández R., 2014).

Además de lo mencionado anteriormente, Hernández (2014) afirma que del diseño de la investigación tiene propósitos adicionales que consisten en responder las preguntas planteadas inicialmente en el proyecto de investigación, cumplir con los objetivos planteados y someter la hipotesis a pruebas según lo establecido.

Para el desarrollo del diseño de la presente investigación de toma como referencia los objetivos específicos de la investigación, así mismo, el plan está alineado con las etapas de Auditoria mencionadas en el marco teórico de la presente investigación.

A continuación, se presenta la figura del diseño de la presente investigación:

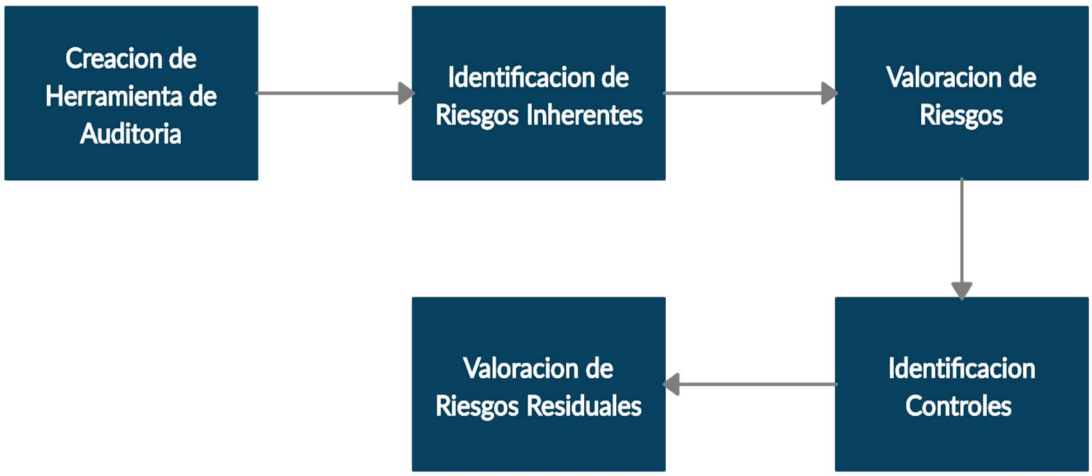


Ilustración 7. Diseño de la Investigación.

Fuente: Creación Propia

3.4.5 Matriz de coherencias

A continuación, se presenta la matriz de coherencia donde se relacionan los objetivos, entregables del proyecto, instrumentos e información del marco metodológico con el fin de conceptualizar todos los elementos que se relacionan entre sí.

Objetivo	Entregable	Etapa de realización del entregable	Técnicas de recolección de la información	Instrumentos	Temas relacionados para marco teórico
Proponer una herramienta de referencia para procesos de auditoria con el fin de asegurar el cumplimiento de las mejores prácticas de la industria en cuanto al	Una hoja de Excel que va a contener varias hojas y en cada una de ellas se podrá hacer cada uno de los análisis que se describen en los	La herramienta completa se proporcionará en el Capítulo V Propuesta del Proyecto.	Se usarán tanto técnicas cualitativas como cuantitativas	• Revisión documental • Entrevistas	Conceptos básicos de auditoría y control interno, objetivos de auditoría, etapas de la auditoría.

Objetivo	Entregable	Etapa de realización del entregable	Técnicas de recolección de la información	Instrumentos	Temas relacionados para marco teórico
manejo de datos de pago y protección de identidad.	objetivos específicos de este trabajo.				
Identificar los riesgos inherentes en la aplicación a través de la implementación de una herramienta que permita hacer una evaluación de fondo en la manera en que información sensitiva es administrada, con el fin de asegurar el cumplimiento con las mejores prácticas según la norma PCI-DSS y Cobit.	Una hoja de Excel en la que se realiza un análisis para identificar los riesgos de una aplicación o proceso.	La herramienta completa se proporcionará en el Capítulo V Propuesta del Proyecto.	Se usarán tanto técnicas cualitativas como cuantitativas	• Revisión documental • Entrevistas	Conceptos básicos de riesgo, análisis y gestión de riesgos.
Valorar los riesgos identificados con base en un modelo cualitativo con escala de medición ordinal, para determinar su importancia dentro de las prioridades de gestión en alineamiento con el estándar.	Una hoja de Excel en la que se realiza una calificación de los riesgos identificados con base en una serie de parámetros relacionados con tecnología de la información.	La herramienta completa se proporcionará en el Capítulo V Propuesta del Proyecto.	Se usarán tanto técnicas cualitativas como cuantitativas	Revisión documental	Conceptos básicos de riesgo, control, análisis y gestión de riesgos.
Identificar los controles diseñados para gestionar eficazmente los riesgos encontrados y a su vez evaluar su efectividad en la mitigación de la vulnerabilidad de la información.	Una hoja de Excel en la que se realiza un análisis para identificar los controles mitigantes de los riesgos previamente identificados.	La herramienta completa se proporcionará en el Capítulo V Propuesta del Proyecto.	Se usarán tanto técnicas cualitativas como cuantitativas	• Revisión documental • Entrevistas	Conceptos básicos de control.

Objetivo	Entregable	Etapa de realización del entregable	Técnicas de recolección de la información	Instrumentos	Temas relacionados para marco teórico
Valorar los riesgos residuales posteriores al proceso de gestión de controles, asimismo determinar sus repercusiones en cuanto al manejo de información sensitiva.	Una hoja de Excel en la que se realiza una calificación de los riesgos, a nivel residual, identificados con base en una serie de parámetros relacionados con tecnología de la información.	La herramienta completa se proporcionará en el Capítulo V Propuesta del Proyecto.	Se usarán tanto técnicas cualitativas como cuantitativas	Revisión documental	Conceptos básicos de riesgo, control, análisis y gestión de riesgos.

Tabla 15. Matrix de Coherencia.

Fuente: Creación propia

4 CAPÍTULO IV: ANALISIS DE LA INFORMACION

Ulate & Vargas (2019) describen el Análisis de resultados como uno de procesos más importantes de la investigación ya que se aplican las técnicas y herramientas adecuadas para la recolección y categorización de la información necesaria para cumplir con los objetivos planteados.

El Análisis de la información permite establecer categorizar, resumir y presentar la información que se ha recolectado a través de los instrumentos de investigación. Además, el análisis de la información permite entender el estado actual del tema en cuestión.

El Análisis de la información con respecto al cumplimiento del Estándar de seguridad en la Empresa Shell se da mediante el uso de los instrumentos de recolección de datos descritos en la sección 3.4.

4.1 RECOPILACIÓN Y ANÁLISIS DE INFORMACIÓN

Siendo las entrevistas uno de los pilares de la recolección de datos, se han tomado personas de interés y/o que tienen condición de expertos en la materia con lo que se ha podido entender muy bien los conceptos y objetivos que se plantearon al hacer las entrevistas.

En el Apéndice C se presenta la entrevista realizada a Deb Deborse quien es la Gerente del departamento de soporte de aplicación y quien tiene mucho conocimiento del entorno de la aplicación y sobre el manejo de temas de seguridad y procesos del servicio que se le provee a Shell.

Fue en dicha entrevista donde se dio a conocer que el equipo de gerencia de soporte a la aplicación como cuenta ha tenido escalaciones no positivas con respecto a incumplimiento de la norma y de eventos repetitivos de incumplimiento, también se han encontrado hallazgos recurrentes que no han sido resueltos.

Otro punto importante es que no se cuenta con un calendario anual de revisión de debilidades y vulnerabilidades como tampoco se cuenta con herramientas y recursos para la documentación y manejo de controles implicados por el Estándar PCI-DSS por lo que se usan las

metodologías de recolección de evidencia y plantillas de los auditores externos, lo cual no permite tener seguimiento ni congruencia entre la documentación de auditorías pasadas.

Durante la entrevista en mención, fue dado a conocer que el equipo de soporte de operaciones de la aplicación no se tiene conocimiento exacto de los modulos en donde es posible acceder a información sensitiva dado que la producción de estos módulos es gestionada por equipos de desarrollo y posteriormente implementada ambientes de producción sin que se dé una transferencia de conocimiento o documentación de este tipo. Otro punto importante de denotar es que no se conocen a fondo los procesos de negocio.

En cuanto al manejo de Información sensitiva que es enviada por correo electrónico y que deben ser impresa para aprobaciones manuales y no existe un proceso escrito ni evidencia sobre del manejo de desperdicio físico seguro

En segunda instancia encontramos en el Apéndice B entrevistas a Profesionales en Auditoria Informática quienes fueron claves en la recolección de información de mejores prácticas en procesos de autoría y que aportaron conocimiento clave para el desarrollo de una metodología que este alineado con el cumplimiento de parámetros actuales, estándar de calidad y uso común en los procesos de auditoria actuales.

4.2 REVISIÓN DOCUMENTAL Y ARTEFACTOS

Se ha observado evidencia provista en auditorias pasadas, documentación corporativa sobre normativas de seguridad, documentación relacionada a seguridad, cartas de aceptación de riesgos, Políticas corporativas de seguridad, políticas de retención de datos.

A continuación, se muestran detallan la documentación existente para el cumplimiento de Algunos requisitos que son considerados de alta importancia como evidencia en procesos de auditoria anteriores. Además, dicha documentación muestra el avance en el cumplimiento con ciertos requerimientos PCI-DSS.

4.2.1 Manejo de Información en Medios Físicos

Las políticas corporativas que existen para el manejo de medios con información sensitiva no se siguen correctamente, En el Anexo 1 podemos ver el documento llamado *DXC Sanitización and Destruction* que aclara que medios físicos deben ser destruidos sin embargo existen aprobaciones de transacciones crediticias que son impresas y de las cuales no se tiene evidencia de destrucción segura siendo esta necesaria para esta en concordancia con la imagen a continuación:

Media Type	Complete Physical Destruction	Degauss	Overwrite	Disk Sanitizer Feature in BIOS	Remote Wipe
Hard Disk Drives	X	X	X	X	
Magnetic Tapes	X	X	X		
Optical Media (CDs/DVDs)	X		X		
USB keys	X		X		
Smartphones	X				X
Physical documents (paper)	X				

Ilustración 8. Métodos de destrucción de datos basados en el tipo de medio.

Fuente: DXC Technology

Tampoco se cuenta con evidencia que apoye las políticas de retención de datos como lo muestra el Anexo 2 en donde se tienen límites temporales de retención y de los cuales no se tiene evidencia como se muestra a continuación:

	A	B	C	D	E	F	G	H	I	J
1	Database Data Retention	Data Type/Category	Database - Online Retention Period				Database - Archive Retention Period			
2			HK	MO	CA	GL3 & GL4	HK	MO	CA	GL3 & GL4
3	Database Data	PCI Transactional Data	4 months	4 months	4 months	4 months	8 years	8 years	8 years	8 years
4	Database Data	PCI Master Data	TEOC/Live Update	TEOC/Live Update	TEOC/Live Update	TEOC/Live Update	N/A	N/A	N/A	N/A
5	Database Data	Non PCI Transactional Data	2 months	2 months	2 months	2 months	N/A	N/A	N/A	N/A
6	Database Data	Non PCI Master Data	TEOC/Live Update	TEOC/Live Update	TEOC/Live Update	TEOC/Live Update	N/A	N/A	N/A	N/A
7										
8	**Note :** For Canada the PCI Transactional Data - Database Online Retention Period will be changed from 7 months to 4 months effective from 30th June 2017 as per re-baseline negotiation.									
9										
10	ABBREVIATIONS									
11	Live Update	Retailer's Master Data - updated every 2 hours from Shell's system.								
12	TEOC	Till End Of Contract								
13										

Ilustración 9. Calendario de retención de datos.

Fuente: DXC Technology

Lo anterior tiene una relación directa con el requerimiento PCI 3.1.b en donde requieren contar con pruebas de comprueben que la información sensitiva es desechada de una manera segura.

4.2.2 Manejo de eventos de seguridad

Otro punto para mencionar es el uso que se le da a eventos de seguridad en acceso a los sistemas de Producción bajo ambientes PCI. El servicio que se le da a Shell incluye un aplicativo automatizado de monitoreo de acceso en donde se generan notificaciones automáticas, sin embargo, el equipo no cuenta con un proceso de seguimiento a estos eventos cuando así lo especifica el Estándar PCI, al no contar con un proceso de seguimiento de alertas de acceso, se está incumpliendo con el requerimiento PCI 10.6.1

En el Anexo 3 se presenta un correo de notificación que le es enviada a personas de soporte o previamente definidas como personas de Interés. A continuación, un ejemplo de notificación de acceso fallido a un servidor de Aplicación en el ambiente de producción PCI:

From: DXC ESS MSS AMS SOC Support
Sent: Monday, March 04, 2019 1:05 AM
To: RCU CCSS Operations <rcuccssoperations@dxc.com>; WSLK_ResourceCenter <wslkresourcecenter@dxc.com>
Cc: RCU Americas <rcu-americas@dxc.com>; DXC ESS MSS AMS SOC Support <hp-ess-mss-ams-soc-support@dxc.com>
Subject: RCU || 292389 || STD003 - Attempt to Exceed User Privileges (KZ83PF sudo KZ83PF) - ustlsrcu625

Hello,

DXC CTAC SECURITY NOTIFICATION
Summary:
The DXC CTAC received a STD003 - Attempt to Exceed User Privileges alert for FRNK account KZ83PF failing to authenticate to the KZ83PF account via sudo on device USTLSRCU625.

Threat Research:
This rule will capture when a user unsuccessfully tries to log into an account which is of a higher privilege level or access a file/process that the user does not have privileges to.

Ilustración 10. Notificación de Acceso Fallido

Fuente: DXC Interna

Lo Anterior, si bien hace el monitoreo y la tarea de notificación de accesos fallidos, el equipo de TI no cuenta con procesos del manejo de estas alarmas. Por lo que no se cumple en totalidad el requerimiento 10.6.1 y 12.10.3 en donde se especifica que los eventos de acceso a sistemas críticos deben ser revisados y se debe mantener un historial y el detalle de las acciones que se tomaran.

4.2.3 Manejo de llaves criptográficas

En cuanto a las llaves criptográficas, se encuentra documentación importante el inventario de llaves, fecha de creación, tipo de algoritmo, pero no se cuenta con fecha de documentación, tampoco se sabe quién es el dueño de la llave y si existe alguna revisión periódica de la llave. En el Anexo 4 se pueden encontrar más detalles sobre la documentación encontrada.

En la siguiente figura podemos encontrar una imagen de consola de administración de las llaves criptográficas, dicha imagen fue provista como parte de las evidencias, y no cuenta con detalle de expiración de las llaves:

Ilustración 11. Consola de Administración de llaves (Vormetric).

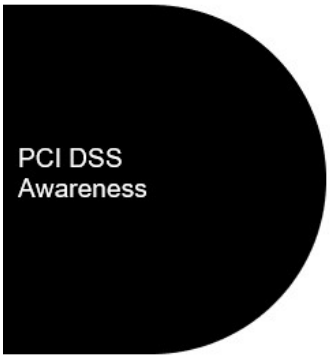
Fuente: DXC Technology

No Contar con un calendario periódico de revisión de llaves y no tener conocimiento de la expiración es una violación a los requerimientos 3.5.1, 3.6.3 y 3.6.4

4.2.4 Procesos de "Onboarding"

Se es conocido que en todo sistema seguro las personas que usan el sistema son las que introducen mayor riesgo ya que conociendo o no, pueden hacer mal manejo de la información. De esta manera el estándar PCI-DSS en el requerimiento 12.6.2 controla que los entrenamientos sobre seguridad sean impartidos a los nuevos usuarios, el requerimiento define que se debe contar con documentación de confirmación por parte de usuarios afirmando y aceptando el compromiso. Lastimosamente no se cuenta con esta información ya que en el equipo no existe un proceso de onboarding global para la cuenta y estos contenidos no se imparte actualmente.

En el Apéndice 5 se muestra la documentación provista como evidencia, en donde se hace referencia de una actualización anual sobre seguridad, Esta iniciativa en global de DXC y no aporta conocimientos específicos sobre el estándar PCI. Es por esta razón que se incumple con el requerimiento 12.6.1 y 12.6.2.



PCI Req 12.6.1: PCI DSS Awareness

- List of personnel in PCIDSS scope
- Evidence of awareness attendance
- Acknowledgement from each PCIDSS personnel that they have read and understood security policies and procedures

Evidence date: 2020-03-13

Personnel:

- Ivonne Cortes
- Jorge Porras

At corporate level, all DXC employees must take periodically the Secure the human training to be updated on the recent security measures (Evidence in 12.10.4), additionally and as part of the monitoring process of this awareness DXC is conducting exercises to confirm employees are following security guidelines.

Ilustración 12. Evidencia de entrenamiento a nuevos empleados.

Fuente: DXC Technology

4.3 IDENTIFICACIÓN DE MEJORAS Y RECOMENDACIONES

A continuación, se describen los puntos en los que se han encontrado posibles mejoras ya sea en la documentación o en los procesos necesarios entorno a la auditoria del sistema en cuestión:

Tabla de Posibles mejoras		
Area de mejora	**Descripcion**	**Puntos de Mejora**
Calendario de revision de vulnerabilidades	No se cuenta con un calendario de seguimiento para el control de vulnerabilidades.	Implementar una herrameinta de control tipo calendario de vulnerabilidades, con esta herramienta se le puede dar seguimiento a las acciones de remediacion que se toman como consecuencia de algun hayazgo posible.
Retencion de datos	No esta muy claro los parametros en donde se eliminan datos de titulares de tarjeta, ni tampoco se conocen los procesos para la eliminacion de medios fisicos.	Hacer una revision de la documentacion y procedimientos en cuanto al borrado de datos sensibles.
Entrenamiento introductorio	No Existe entrenamiento en el proceso inductorio en cuanto standard PCI. O no existe un proceso introductorio definido para la cuenta.	Incluir contenidos del standard PCI en los entrenamientos de seguridad o a los entrenamientos inductorios a la cuenta y garantizar que exista una comprobacion de reconocimiento por parte de los integrantes del equipo. Tambien es importante poder resguardar dichas comprobaciones y asugurar su actualizacion periodica.
Llaves criptograficas	No se conoce la fecha de caducidad de las llaves criptograficas.	Es entendible que la actualizacion de llaves critpgraficas implica impactos en los ambientes de productivos. Sin embargo tiene que existir documentacion de respaldo en donde se definen los parametros bajo los cuales seria necesaria una actualizacion de la emcriptacion de los servidores.

Tabla de Posibles mejoras		
Area de mejora	**Descripcion**	**Puntos de Mejora**
Herramienta de Control de requerimientos PCI	No se cuenta con una herramienta de trabajo para el control de requerimientos PCI, documentacion y candelarizacion de actividades de seguridad.	Implementar una herrameinta de referencia para el manejo de requerimientos y control de actividades con enfasis en el cumplimiento del Standard PCI-DSS

Tabla 16. Tabla de Posibles Mejoras,

Fuente: Creación propia

5 CAPÍTULO V: PROPUESTA DEL PROYECTO

En el presente capitulo se desarrollarán las propuestas que incluyen las mejores prácticas de la industria y que confirman la herramienta de control y mitigación de riesgos, la propuesta a continuación se espera tenga pueda ayudar a otros profesionales en el manejo de riesgos y controles con énfasis en el cumplimiento del estándar PCI.

El entregable principal consta de una plantilla de trabajo que se compone de tres ejes fundamentales en los que se encierra el proceso de principio a fin para la identificación y calificación cualitativa de riesgos inherentes, gestión de controles adecuados y evaluación posterior de riesgos residuales.

5.1 IDENTIFICACIÓN Y CALIFICACIÓN CUALITATIVA DE RIESGOS INHERENTES

La identificación de riesgos inherentes es clave para saber exactamente cuáles de los controles PCI pueden ser aplicados y así poder implementar los controles adecuados con el fin de mantener las operaciones de los aplicativos dentro del marco de referencia PCI.

El entregable presenta una relación directa entre los riesgos y los requerimientos PCI con el fin de posteriormente tener una asignación automática de los controles adecuados para dichos riesgos.

En la figura siguiente se presenta un extracto del Apéndice F.1 donde se muestran cuáles han sido los riesgos que se han identificado para la aplicación Retailer Transaction Settlement Platform (RTSP por sus siglas en Ingles) de Shell:

IDENTIFICACION DEL RIESGO	
PCI Req.	Descripcion del Riesgo
3.1.b	Tener datos del titular almacenados en medios fisicos o digitales y que estos puedan ser accesados por personas ajenas a las operaciones del negocio.
10.6.1	No saber si el ambiente es sujeto de ataques de seguridad, intentos fallidos de acceso, no conocer si existen fallas en los registros de sistema y de componentes criticos del sistema.
12.10.3	No tener la capacidad de responder y dar seguimiento (24/7) a alertas del sistema
12.6.1	tener personal dentro de los equipos de soporte que no conozcan de el standar PCI y sus requerimientos.
12.6.2	No contar con una comprobacion por parte de los colaboradores en cuanto a capacitaciones y actualizaciones de seguridad.

Ilustración 13. Identificación de Riesgos Inherentes.

Fuente: Herramienta de Gestión de Riesgos y Controles PCI

La calificación de los riesgos se ha hecho con base a un modelo cualitativo con escala de medición ordinal, para lo que se han tomado en cuenta cinco criterios en los que los riesgos pueden tener impacto. A continuación, se detallan cada uno de los criterios de evaluación:

- Core del Negocio
- Efecto en la información financiera
- Exposición al fraude
- Dependencia de la tecnología
- Imagen y reputación

Además, se ha definido una escala de medición del 1 al 4, la cual de detalla a continuación:

1- Nada Susceptible
2- Poco susceptible
3- Moderadamente susceptible
4- Muy susceptible

En la figura a continuación es también parte de la misma plantilla de trabajo como parte de los entregables se puede encontrar su detalle en el Apéndice F.1:

CRITERIOS DE EVALUACION										CALIFICACION CUALITATIVA			
Core del negocio y afecta estrategia		Efecto en la información financiera		Exposición al fraude		Dependencia de la tecnología		Imagen y reputación		Totales		Total	Nivel de riesgo inherente
2	2	3	3	3	3	2	2	2	2	2,40	2,40	5,76	Medio
										-	-	-	

Nivel de riesgo	Rangos de calificación	
	De	A
Alto	9	16
Medio	4	8,99

Ilustración 14. Medición cualitativa de riesgos Inherentes.

Fuente: Herramienta de Gestión de Riesgos y Controles PCI

5.2 IDENTIFICACIÓN DE CONTROLES PARA GESTIÓN EFICAZ DE RIESGOS

La identificación de los controles es primordial para la mitigación adecuada de riesgos inherentes, en el caso del estándar PCI, podemos aplicar los controles que el estándar pide para la comprobación de la mitigación de los riesgos anteriormente mencionados.

En la figura a continuación se puede apreciar el detalle del Apéndice F.2 donde se aprecian los controles identificados por la herramienta para mitigación de los riesgos de la aplicación Retailer Transaction Settlement Platform de Shell:

DESCRIPCION DE CONTROLES PCI		
PCI R...	Descripcion del Control	Lista de evidencias a colectar
3.1.b	Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan la retención definida	Todos los lugares donde se almacenan datos de titulares de tarjetas están incluidos en los procesos de retención y eliminación de datos
10.6.1	Revise las siguientes opciones,	Revise las políticas y los procedimientos de seguridadpara verificar que los procedimientos se definen para
12.10.3	Designe a personal específico para	Mediante la observación, revise las políticas yentreviste al personal responsable para verificar que elperso
12.6.1	Capacite al personal inmediatamente	Verifique que el programa de concienciaciónsobre seguridad proporcione diversos métodos parainformar y
12.6.2	Exija al personal que realice, al	Verifique que el programa de concienciaciónsobre seguridad les exija a los empleados realizar, almenos, una

Ilustración 15. Identificación de controles PCI.

Fuente: Herramienta de Gestión de Riesgos y Controles PCI

5.3 IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS RESIDUALES

La herramienta también toma en cuenta los riesgos residuales y tiene la posibilidad de hacer una calificación posterior con el fin de poder valorar las implicaciones del dejar riesgos residuales sin mitigar o si es necesario hacer documentación de aceptación de estos. En el Apéndice F.3 podemos ver el detalle de la evaluación, sin embargo, en este proceso también se usa un modelo cualitativo con escala de medición ordinal pero también se toman parámetros que saber la posibilidad de materialización del riesgo en cuestión.

5.3.1 Criterios de evaluación de riesgos residuales

Los criterios de evaluación para los riesgos inherentes son los siguientes:

- Gestión de Riesgos
- Incumplimiento de la normativa
- Materialidad
- Oportunidad de fraude
- Reincidencia del hallazgo

A cada uno de estos criterios se le califica de dos maneras, en cuanto a la efectividad del control aplicado y en cuanto al potencial de materialización.

A continuación, el detalle de la plantilla de evaluación también se puede ver su detalle en el Apéndice F.4:

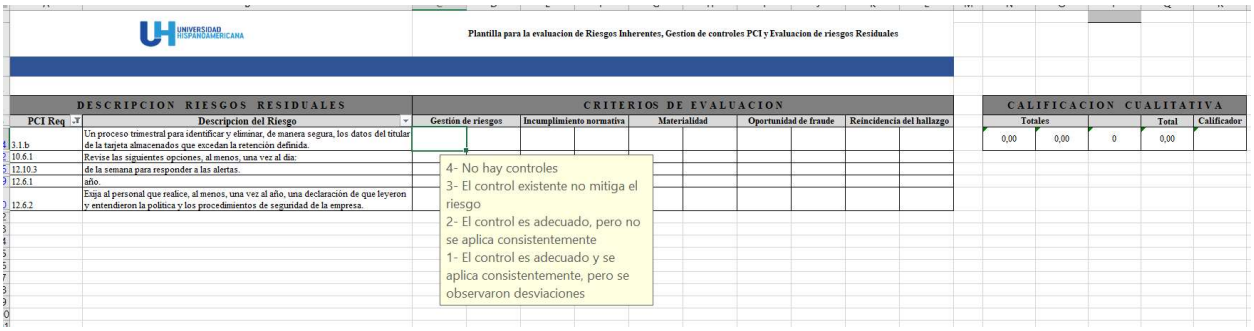


Ilustración 16. Plantilla de evaluación de riesgos residuales (efectividad de controles aplicados).

Fuente: Herramienta de Gestión de Riesgos y Controles PCI

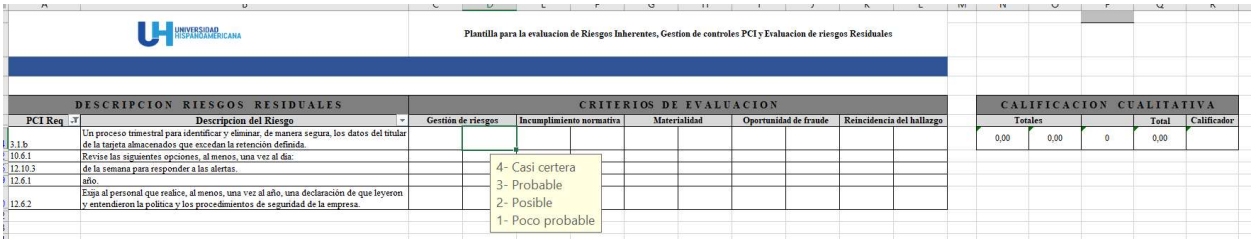


Ilustración 17. Plantilla de evaluación de riesgos residuales (probabilidad de materialización).

Fuente: Herramienta de Gestión de Riesgos y Controles PCI

6 CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

En el presente capitulo, se presentan las conclusiones y recomendaciones obtenidas una vez aplicado la metodología definida a la herramienta como propuesta a un proceso de auditoria dentro del marco de referencia del estándar PCI-DSS.

Durante el desarrollo de este capítulo se presentan las conclusiones y recomendaciones obtenidas en perspectiva con los objetivos obtenidos al inicio de la presente investigación.

6.1 CONCLUSIONES

A continuación, se presentan las conclusiones obtenidas con respecto a cada uno de los objetivos establecidos y a su vez se proporcionan los aportes que resultaron del análisis elaborado.

> Como respuesta al objetivo general: *Crear una propuesta de implementación de una herramienta de referencia para identificar y analizar riesgos como también la gestión de controles oportunos durante el primer semestre del año 2020, usando como marco de referencia las mejores prácticas de la industria con el fin de asegurar el cumplimiento con los estándares PCI-DSS y Cobit.*

Se considera que la plantilla de trabajo creada cumple con el propósito ya que representa una herramienta sencilla de análisis, que permite plantear en un solo documento de trabajo la gestión de riesgos y controles. En la propuesta de implementación, se logró identificar riesgos inherentes y de la misma manera identificar los controles PCI que mitigan dichos riesgos. El valor agregado de la propuesta está en la capacidad de relacionar riesgos inherentes con el control PCI adecuado que pretende mitigar cada riesgo, de la misma manera la posibilidad de evaluar cada riesgo residual, lo cual empodera los administradores de aplicaciones para tomar las mejores decisiones estratégicas.

Con relación a los objetivos específicos, se concluye lo siguiente:

> En relación con el primer objetivo: *Proponer una herramienta de referencia para procesos de auditoria con el fin de asegurar el cumplimiento de las mejores prácticas de la industria en cuanto al manejo de datos de pago y protección de identidad.*

Se logró proponer una herramienta de referencia para procesos de auditoria PCI y de esta forma se logra asegurar el cumplimiento de las mejores prácticas de la industria en cuanto al manejo de datos de pago y protección de identidad, través de una hoja de trabajo. En cuanto al cumplimiento con la normativa es importante mencionar que la recolección de evidencias e implementación de procesos que estén acorde con los controles PCI es un proceso que dependiendo de la organización puede tardar varios meses o años.

> En relación con el segundo objetivo: *Identificar los riesgos inherentes en la aplicación a través de la implementación de una herramienta que permita hacer una evaluación de fondo en la manera en que información sensitiva es administrada, con el fin de asegurar el cumplimiento con las mejores prácticas según la norma PCI-DSS y Cobit.*

Se diseña una hoja de trabajo en la cual se logran identificar los riesgos inherentes en la aplicación. Esto tiene una implicación directa en la manera en que información sensitiva es administrada por parte de los equipos de soporte. De esta tomar las acciones correctas para el cumplimiento con las mejores prácticas según la normativa PCI-DSS y Cobit.

> Sobre el tercer objetivo: *Valorar los riesgos identificados con base en un modelo cualitativo con escala de medición ordinal, para determinar su importancia dentro de las prioridades de gestión en alineamiento con el estándar.*

No solo se aporta un modelo para valorar los riesgos identificados con base en un modelo cualitativo con escala de medición ordinal, indirectamente se provee a los administradores de aplicaciones de una ayuda para definir la estrategia de trabajo y las prioridades en las que asignar sus recursos.

En un escenario perfecto, los gerentes y administradores de aplicaciones podrían gestionar todos controles PCI e implementar nuevos procesos en la solución, sin embargo, la realidad representa muchos retos a los administradores en cuanto la asignación de recursos y los calendarios de entrega, problemática a la cual, la presente propuesta muestra un valor agregado.

En cuanto al cuarto objetivo: *Identificar los controles diseñados para gestionar eficazmente los riesgos encontrados y a su vez evaluar su efectividad en la mitigación de la vulnerabilidad de la información.*

Dentro de la hoja de Excel diseñada se incluye el campo para fácilmente identificar los cuales son controles PCI diseñados para gestionar eficazmente los riesgos encontrados y a su vez evaluar su efectividad en la mitigación de la vulnerabilidad de la información, esta labor se aplica a un caso práctica en forma exitosa.

Finalmente, en cuanto al quinto objetivo: *Valorar los riesgos residuales posteriores al proceso de gestión de controles, asimismo determinar sus repercusiones en cuanto al manejo de información sensitiva.*

Se desarrolla un modelo sencillo para valorar los riesgos residuales posteriores al proceso de gestión de controles, el cual aporta información fiable y sobre las repercusiones de los riesgos que no se encuentran totalmente mitigados, en cuanto al manejo de información sensitiva. Una vez más le herramienta aporta un parámetro de ayuda para la toma de decisiones estratégicas.

6.2 RECOMENDACIONES

Como producto del análisis realizado se aportan las siguientes recomendaciones:

a. Implementar la herramienta proporcionada en este Proyecto de graduación, ya que se considera que puede ser de gran ayuda para gestionar los riesgos relacionados con el cumplimiento de PCI.

b. El cumplimiento con la normativa PCI debe también administrarse proactivamente y se deben tomar decisiones estratégicas que permitan a los equipos administradores de tomar las decisiones adecuadas en la gestión de cambios y mejoras de los sistemas. Herramientas como la presente pueden además de ayudar a la gestión de riesgos y controles, dan información concisa para las acciones estratégicas de los equipos.

c. La calificación de los riesgos inherentes y residuales con las herramientas proporcionadas, servirán de base para valorar el costo – beneficio de la corrección de las oportunidades de mejora que surjan del análisis de los riesgos. También ayuda a los administradores y gerentes a establecer prioridades en cuanto la asignación de recursos.

d. Establecer un procedimiento para rediseñar los controles que resulten ineficientes, del análisis que surja de la aplicación de la herramienta proporcionada en este proyecto. Acorde con la evaluación de riesgos residuales se pueden identificar aquellos controles que se necesitan mejorar.

e. Establecer un proceso revisiones periódicas de vulnerabilidades y escaneos de seguridad y también el respectivo seguimiento de las acciones correctivas, ambos procesos deben tener una calendarización estricta y contar con los recursos para el manejo de cambios e implementaciones que sean pertinentes. En muchos de los casos en donde se ha identificado vulnerabilidades, las mejoras permanentes no infieren una inversión directa en tecnología, sin embargo, se requiere del trabajo de colaboradores en cuanto a cambios de procesos o documentación que respalde las acciones de seguridad.

f. Trasladar las labores de seguimiento a las notificaciones a un equipo operativo como el *Service Desk* o un primer nivel de soporte que pueda dar seguimiento según parámetros y criticalidad de las alertas de seguridad.

Uno de los problemas encontrados en la aplicación del presente caso de estudio, es que la inversión en tecnología y recursos para el monitoreo de acceso no está siendo aprovechado puesto que no se le está dando seguimiento a las notificaciones.

Otro problema es el riesgo que esto implica dado que no se están investigando intentos de accesos. Esto es común en equipos de soporte dado que existen otras prioridades, por lo que se recomienda crear documentación y establecer un parámetro bajo el cual los niveles más operativos de soporte pueden absorber estas tareas tan importantes.

g. Incluir entrenamientos de seguridad con énfasis en el estándar PCI como parte del proceso inducción a los empleados nuevos, así como también impartir entrenamientos anuales de refrescamiento de temas de PCI. En el presente caso de estudio se identificó que los entrenamientos corporativos de seguridad no tenían información específica del estándar PCI, lo cual para la aplicación en cuestión es primordial de impartir.

BIBLIOGRAFÍA

ISACA, (2012). COBIT 5. Illinois, USA.

ISACA, (2017). Manual de Preparación para el examen CISA. Illinois, USA.

ISACA, (2018). Getting Started With Risk Management. Illinois, USA.

ISACA, (2018). How to audit GDPR. Illinois, USA.

López, A. (2005). ISO 27001. Serie 27000. Recuperado de http://www.iso27000.es/index.html

PCI Security Standards Council, (2018). Norma de seguridad de datos de la industria de tarjetas de pago (PCI). Massachusetts, USA

Segovia, A. ISO 27001. 27001 Academy. Recuperado de https://advisera.com/27001academy/es/que-es-iso-27001/

The Institute of Internal Auditors, (2007). GAIT Methodology: A risk-based approach to assessing the scope of IT general controls. Florida, USA.

The Institute of Internal Auditors (2017). Glosario del Marco Internacional para la Práctica Profesional. Florida, USA.

The Institute of Internal Auditors (2019). Dirección de la Auditoria de Tecnologías de la Información. Florida, USA.

The Institute of Internal Auditors (2019). Controles sobre las Tecnologías de la Información. Florida, USA.

The Institute of Internal Auditors (2017). Marco Internacional para la práctica profesional de la auditoría Interna. Florida, USA.

The IIA (2016). Auditoría Interna: Servicios de aseguramiento y consultoría. Florida, USA.

The Institute of Internal Auditors (2019). Gestión de riesgos corporativos Marco Integrado. Florida, USA.

Instituto de Auditores Internos España (2015). Los nuevos conceptos del control interno (Informe COSO). Madrid España.

The Institute of Internal Auditors (2017). Auditoría del gobierno de TI. Florida, USA.

The Institute of Internal Auditors (2017). COSO internal control – Integrates framework. Florida, USA.

RAE. (2018). Real Academia Española. Obtenido de Real Academia Española: https://dle.rae.es/?id=Lgx0cfV

Barrantes E. (2018). A la búsqueda del conocimiento científico. Costa Rica: EUNED.

Barrantes E. (2018). Métodos de estudio a distancia e investigación. Costa Rica: EUNED.

Soto U, Vargas M. (2014). Metodología para elaborar una tesis. Costa Rica: EUNED.

Hernández, R. (2014). Metodología de la Investigación. Mexico D.F: McGraw Hill.

Ulate, I. S., & Vargas, E. M. (2019). Metodología para Elaborar una Tesis. San Jose: EUNED.

Venegas, L., Esparza, F., & Guerron, D. (2017). Evaluación y auditoría de sistemas tecnológicos: estudios de casos resueltos. 3Ciencias.

APÉNDICES

APÉNDICE A. PLANTILLA PARA LAS ENTREVISTAS

Entrevista

Información general de la entrevista					
Entrevista No.		**Fecha**		**Hora**	
Tema					

Personal involucrado en la entrevista		
Nombre	**Rol**	**Condición de la entrevista**

Temas por tratar en la entrevista

Preguntas realizadas en la entrevista
¿Pregunta?
Respuesta

APÉNDICE B. ENTREVISTAS REALIZADAS A PROFESIONALES EN AUDITORÍA

Apéndice B.01. Entrevista a un Gerente de Auditoría de Tecnología de la información

Información general de la entrevista					
Entrevista No.	001	**Fecha**	06/04/2020	**Hora**	7:00 p.m.
Tema	Metodología de Auditoría de tecnologías de la información				

Personal involucrado en la entrevista		
Nombre	**Rol**	**Condición de la entrevista**
Rolando González Montero	Gerente auditoría TI Bac Credomatic Network	Entrevistado
Mauricio Lizano Barahona	Estudiante	Moderador

Temas por tratar en la entrevista
• Aspectos más importantes a evaluar en una Auditoría de tecnología de la información. • Importancia del análisis de riesgos en Tecnología de la Información.

Preguntas realizadas en la entrevista
¿Porqué es importante hacer un análisis de riesgos en una auditoría de tecnología de la información?
Es importante el análisis de riesgos para ver cuántas veces el riesgo se ha presentado, para ver cuáles eventos de riesgos son repetitivos y descubrir la causa raíz, analizar cada producto o servicio y ver la cantidad de riesgos materializados en el último año. Un ejemplo, pueden consistencia en caídas del sistema de planillas; por ejemplo: se cae una vez al mes, tenemos 12 eventos materializados al año, que cada cierto tiempo el servidor se cae, el evento del riesgo solo va a decir caída del servicio y no dice porque, y se tiene un impacto de la imagen que ocasiona la caída del servidor. A un colaborador que no se le pague la planilla dependiendo del servicio es un problema para la empresa, en el

análisis del impacto, lo que dice es que la causa raíz no se había encontrado y el riesgo no se ha mitigado, solo se ve un evento, pero no el conjunto de eventos.

¿Cuáles son los pasos que se realizan en una auditoría de tecnología de la información?

Se debe hacer un análisis de las áreas que intervienen en el proceso, esto para saber si la estrategia del área está alineada con la estrategia de la organización en general, muchas veces TI, quiere tener la última infraestructura en tecnología o los mejores y más caros sistemas de información, pero es probable que la organización no es eso lo que necesita, es probable que la estrategia de la organización esté orientada en optimización de rentabilidad, el ideal es ver la alineación con estrategia en general, para garantizar que los objetivos de la unidad están alineados con el resto de la organización.

Se deben definir y concentrar todos los estándares que aplican a cada proceso o aplicación que se audite, Todo los riesgos legales y regulatorios, estándares, procedimientos internos todo lo que sean controles que deba tener el sistema. Por ejemplo, los depósitos en efectivo mayores a $10.000 de los clientes están regulados por una regulación de legitimación de capitales, el cliente puede hacer el depósito, pero tienen que certificar el origen de los fondos, por lo que los sistemas deben tener los controles necesarios para cumplir con la ley. El propósito es cuando se hace la revisión de los riesgos ver si se tienen controles adecuados o no.

Es importante saber qué se está haciendo, a qué área pertenece y quién lo está haciendo, cuando una actividad y su control lo realiza una sola persona, cómo se gestionan estas labores y si en algún momento del proceso se controlan estas actividades.

Es posible que un riesgo tenga dos controles y que dos riesgos tengan un solo control, eso no es un problema en tanto los riesgos se estén mitigando adecuadamente.

Un caso de evaluación de riesgos puede basarse en los elementos de cumplimiento de la Norma ISO 27005, lo que puede consistir en definir los criterios más relevantes a cumplir de dicha norma y asignarles un puntaje por cumplimiento, de esta forma se puede obtener un valor de peso para el riesgo.

Cuando se habla de un activo tecnológico, también puede incluirse una documentación, porque existe documentación que también requiere custodia adecuada.

¿La evaluación que usted hace con la ISO 27005 se puede convertir en una evaluación PCI?

No, porque los objetivos de ambos estándares son diferentes, PCI lo que busca es la protección de la información de las tarjetas de crédito y débito, ISO 27000 está orientado a activos de información, un computador, un sistema, una base de datos, etc.

Posterior a la revisión, es necesario hacer un informe que resuma todos los aspectos que se identificaron como riesgos no mitigados adecuadamente.

¿Dentro de Universo de riesgos se identifican los riesgos inherentes y los riesgos residuales?

Los riesgos inherentes son todos aquellos riesgos propios de la actividad que se está auditando, sin considerar controles, para clasificar los riesgos desde el más alto, hasta el más bajo, una vez identificados los riesgos críticos, altos y medios, nos concentramos en los riesgos más importantes, usualmente los altos, para llevarlos al apetito de riesgos de la organización, un auditor no puede partir del hecho de que los controles funcionan, el culmen de la revisión es revisar dos cosas en los controles: el diseño y la efectividad y se da cuenta si el riesgo residual está o no a nivel del apetito de riesgo del negocio. Esta metodología está muy alineada con COSO; que, aunque no es una metodología para auditoría de sistemas, es la base de enunciado de riesgos y controles.

¿Qué considera que debería contener una Auditoría de PCI?

PCI en realidad es un estándar que da una seria de controles con los que se deben cumplir, debería de tratarse solamente del cumplimiento con una guía, perfectamente tratarse de un checklist, aunque esto no quita que se pueda hacer alguna prueba sustantiva para revisar ese cumplimiento.

Apéndice B.02. Entrevista a un Gerente de Auditoría Interna

Información general de la entrevista					
Entrevista No.	002	**Fecha**	13/04/2020	**Hora**	4:00 p.m.
Tema	Metodología de Auditoría de tecnología de la información				

Personal involucrado en la entrevista		
Nombre	**Rol**	**Condición de la entrevista**
Manuel Marín Cubero	Consultor en Auditoría Interna, Riesgo y Fraude	Entrevistado
Mauricio Lizano Barahona	Estudiante	Moderador

Temas por tratar en la entrevista

- Importancia del análisis de gestión de riesgos en la auditoría de tecnología de la información.
- Aspectos importantes a considerar en la auditoría de tecnología de la información.

Preguntas realizadas en la entrevista

¿Porqué es importante hacer un análisis de riesgos en una auditoría de tecnología de la información?

El análisis de riesgos es muy relevante en cualquier actividad empresarial, es fundamental hacerlo en tres niveles: a nivel estratégico, evaluando los riesgos que pueden afectar el cumplimiento de los objetivos estratégicos, a nivel de los riesgos de la industria en que se encuentra la empresa y finalmente a nivel de los riesgos que afectan las operaciones y los procesos de la organización.

Entonces, si tomamos en cuenta que la tecnología de la información es una herramienta fundamental para gestionar los procesos de negocio y que dichos procesos son la vía para el cumplimiento de la estrategia, tenemos que el análisis y la mitigación de los riesgos de la tecnología de la información es fundamental para poder encauzar todos los esfuerzos de la administración hacia el cumplimiento de los objetivos de la empresa.

Lo dicho hasta aquí no toca el tema de la auditoría de TI, pero creo que era necesario plantearlo para contestar la pregunta de manera directa: es importante hacer un análisis de riesgos en una auditoría de TI, porque la auditoría está para ayudar a la organización a cumplir con sus objetivos; por lo tanto, al analizar los riesgos y evaluar cómo se mitigan va a aportar un valor importante en su misión.

Aún sabiendo que su perfil de auditor no es de tecnología de la información ¿Cuáles considera usted que son los riesgos más importantes que se deben considerar en una auditoría de tecnología de la información?

Lo veo en dos dimensiones: una dimensión de riesgos técnicos y la otra dimensión es la de los riesgos de negocio. Me explico, la primera dimensión tiene que ver con riesgos que pueden afectar a toda la organización, tanto a nivel estratégico como de procesos, : riesgos de integridad de la data, riesgo de continuidad (que los sistemas de información fallen y no se pueda prestar el servicio, vender, producir, etc.), riesgo de seguridad (robo o hackeo), riesgos de telecomunicaciones y, asociados segunda dimensión, están los riesgos de desarrollo y parametrización de los sistemas, que tiene que ver con la posibilidad de que los sistemas que se utilizan en los diversos procesos del negocio contengan fallas, en su diseño y en su parametrización, que automaticen y, hasta amplifiquen, los errores

Aprovechando su experiencia en una compañía de tarjetas de crédito ¿Cuáles considera usted que son los aspectos más importantes a evaluar en una auditoría a la seguridad de los datos de la tarjeta?

En este caso los aspectos más importantes se relacionan con el resguardo de la información, en el negocio de tarjetas de crédito se procesa una gran cantidad de información muy valiosa, tal como los patrones y volúmenes de consumo de los clientes, si a estos datos se les puede agregar la identificación del cliente, tenemos una base de datos muy valiosa, tanto para la competencia como para estafadores. Por lo tanto, en ese negocio, es fundamental que las bases de datos de consumo y de identificación de los clientes no estén juntas, deben existir bases por separado y tener procesos de unificación, con

controles adecuados, para generar los reportes de gestión y los estados de cuenta de los clientes y no exponer la información consolidada.

Por otra parte, también es importante evaluar aspectos relacionados con el cumplimiento de la legislación de prevención de blanqueo de capitales, ya que por medio de las tarjetas de crédito se pueden dar varios esquemas para el lavado o blanqueo de capitales.

Apéndice B.03 Entrevista a un Auditor de tecnologia

Entrevista

Información general de la entrevista					
Entrevista No.	003	**Fecha**	15/04/20	**Hora**	5:00 p.m.
Tema	Evaluación de riesgos en Auditoría				

Personal involucrado en la entrevista		
Nombre	**Rol**	**Condición de la entrevista**
Henry Vega Rodríguez	Gerente Auditoría Acorde	Entrevistado
Mauricio Lizano Barahona	Estudiante	Moderador

Temas por tratar en la entrevista
Enfoque de auditoría de gestión de riesgos

Preguntas realizadas en la entrevista
¿En qué consiste una auditoría de gestión de riesgos?
Es una metodología que se utiliza para desarrollar las auditorías internas, usualmente se aplica a la revisión de procesos, los procesos se analizan en forma detallada, usualmente por etapas y se identifican los riesgos en cada una de esas etapas, esto con el propósito de evaluar los controles que la administración ha establecido para gestionar y mitigar esos riesgos. A la vez es un modelo que incorpora la relación entre el riesgo con los objetivos y los procesos operativos y se diseña para incrementar la eficiencia y efectividad de la auditoría. Agrega mucho valor, pues identifica riesgos en los procesos del negocio que no se están administrando en forma apropiada, se usa para determinar el nivel apropiado de cobertura de la auditoría y se concentra en evaluar controles críticos o claves. Esta metodología implica un proceso mental e intuitivo.

¿Qué incluye la metodología de la AGR?

Básicamente se deben tomar en cuenta los siguientes aspectos:

- Perfiles de operaciones significativas y su asociación con los riesgos del negocio y elementos de control, bajo la fórmula de Objetivos-Riesgos -Controles, este concepto viene de COSO.
- Uso de mediciones o escalas que ordenen y evalúen los riesgos y controles del negocio, esta escala es más intuitiva que matemática.
- Un procedimiento que regularmente monitoree la evaluación de riesgos y que periódicamente actualice los perfiles, Esto como parte del proceso de planificación y supervisión de los trabajos de Auditoría Interna.
- Requiere un cambio significativo de paradigmas o modelos, pues cambia radicalmente la forma en que los auditores hemos pensado y hemos actuado durante años.

¿Qué es un riesgo?

El riesgo es cualquier evento potencial que pueda afectar adversamente a la consecución de los objetivos, en otras palabras los resultados que se deben cumplir en cada una de las actividades del proceso. Otro concepto importante son los factores de riesgo que son todas aquellas situaciones medibles u observables en un proceso que pueden aumentar la exposición a que un riesgo se materialice. Como parte de este enfoque es necesario tomar en cuenta los controles que son las medidas que se ejecutan para gestionar los factores de riesgo y poder cumplir los objetivos, son los que mitigan los riesgos y de ahí su importancia.

¿Cuáles son las etapas de una metodología de auditoría basada en riesgos?

Como cualquier metodología de auditoría el enfoque de evaluación de riesgos se requiere una planificación exahustiva y el planteamiento de objetivos de auditoría, a continuación describo la que podría ser una metodología por etapas:

1) **Planificación:** en esta estapa se establece el objetivo, la estrategia que se empleará, el alcance de la Auditoría y el área y el personal a auditar.

2) **Análisis de la gestión de riesgos:** puede realizarse a través de un diagrama de flujo o de la elaboración de algún documento que permita el análisis por cada componente del proceso, ya sea por etapas o actividades, en esta etapa se deben identificar los riesgos de cada etapa del proceso y los controles que mitigan esos riesgos, una vez identificados es necesario probarlos.

3) **Ejecución de pruebas a controles:** Se revisan a nivel de diseño, distribución de funciones y posteriormente se hacen pruebas, el objetivo es asegurar que mitigan adecuadamente los riesgos y que realmente pueden asegurar una baja exposición a vulnerabilidades.

4) **Informe de resultados:** Todos los resultados de las ruebas a controles realizadas, ya sean positivos o negativos, a través de oportunidades de mejora. El informe final debe ser expedido en forma oportuna y con un lenguaje completamente asertivo.

APÉNDICE C. ENTREVISTA ADMINISTRADOR DE LA CUENTA

Entrevista

Información general de la entrevista					
Entrevista No.	004	**Fecha**	05/12/19	**Hora**	1:00 p.m.
Tema	Funcionamiento del Equipo de soporte y Funcionalidades de soporte a la aplicación.				

Personal involucrado en la entrevista		
Nombre	**Rol**	**Condición de la entrevista**
Deborah Deborse	Account Delivery Manager	Entrevistado
Mauricio Lizano Barahona	Estudiante	Moderador

Temas por tratar en la entrevista
Área de negocio y segmento de la empresa.

Preguntas realizadas en la entrevista
¿A qué se dedica la empresa DXC Technology Services LLC?
"DXC" es una empresa independiente de servicios de TI de extremo a extremo, que ayuda a las entidades usuarias a aprovechar la innovación para ofrecer resultados beneficiosos para su negocio; adicionalmente, lidera las transformaciones digitales para las entidades de los usuarios al modernizar e integrar su TI principal, y al implementar soluciones digitales a escala para producir mejores resultados comerciales. La independencia tecnológica, el talento global y la extensa red de socios de la compañía permiten a 6,000 entidades de usuarios del sector público y privado en 70 países prosperar ante el cambio.
¿DXC tiene algún modelo para desarrollar su trabajo?

Si, para apoyar su misión, DXC desarrolló un modelo operativo en torno a tres movimientos principales: construir, vender y entregar.

Para cumplir con los siguientes objetivos:

- Impulsar la mejora continua: garantizar que los servicios DXC se entreguen mejor, más rápido y de manera más rentable cada año.
- Reducción de los costos de entrega: reduciendo los costos de la prestación de servicios a una cantidad mínima sin comprometer la calidad de la entrega año tras año.
- Aumentar la responsabilidad de la entrega: minimizar las transferencias en la organización, capacitar a los empleados para que sean dueños de su parte del negocio y produzcan resultados de trabajo que afecten el éxito y las métricas de la entidad usuaria.
- Implementación de estándares globales consistentes: utilizando estándares de la industria y prácticas líderes en toda la empresa dentro de las operaciones de entrega diaria para confirmar un rendimiento óptimo.
- Mejora de la excelencia del servicio de extremo a extremo: garantizar que las entidades usuarias reciban un servicio 24x7 en o por encima de las expectativas del Acuerdo de Nivel de Servicio (SLA) sin interrupción.

DXC ofrece los siguientes servicios:

- Seguridad
- Analítica
- Servicios de nube y plataforma
- Lugar de trabajo y movilidad
- Servicios de aplicación
- Aplicaciones empresariales y en la nube
- Consultoría
- Servicios de procesos comerciales
- Descripción del entorno de control, evaluación de riesgos, información y comunicación, y procesos de monitoreo.

¿DXC tiene una estructura de control interno?

Si, los componentes de control interno de DXC incluyen controles que pueden tener un efecto generalizado en la organización, un efecto en procesos específicos, clases de transacciones o ambos. Algunos de los componentes del control interno incluyen controles que tienen más efecto a nivel de entidad, mientras que otros componentes incluyen controles que están principalmente relacionados con procesos o transacciones específicos. Al evaluar el control interno, DXC considera las interrelaciones entre los siguientes componentes:

- Ambiente de control: Establece el tono de una organización, influyendo en la conciencia de control de su gente. Es la base de todos los demás componentes del control interno, proporcionando disciplina y estructura. Los objetivos de una estructura de control interno son proporcionar una seguridad razonable, pero no absoluta, en cuanto a la integridad y confiabilidad de la información financiera, la protección de los activos contra el uso o disposición no autorizados, y que las transacciones se ejecuten de acuerdo con la autorización y el usuario de la administración instrucciones de la entidad. La gerencia ha establecido y mantiene una estructura de control interno que monitorea el cumplimiento de las políticas y procedimientos establecidos. DXC ha implementado un entorno de servicio basado en procesos diseñado para brindar servicios de calidad a sus entidades usuarias. Los fundamentos de los servicios prestados son la adopción de procesos estandarizados y repetibles, la contratación y el desarrollo de personal altamente calificado y una amplia infraestructura de gestión de entidades de usuarios.
- Prácticas de contratación: DXC ha formalizado prácticas de contratación global diseñadas para determinar si los empleados nuevos, recontratados o transferidos están calificados para su responsabilidad funcional. Donde sea legalmente permitido, se requieren nuevas contrataciones externas para completar con éxito la evaluación de empleo global antes de que inicie el contrato de trabajo. Donde y en la medida legalmente permitida, las verificaciones de antecedentes previas al empleo de DXC incluirán: verificación de la identificación nacional del individuo, verificación de la

educación del individuo (cuando lo requiera el puesto), empleo anterior y una verificación criminal de los cinco años anteriores. Se puede aplicar una evaluación adicional en ciertas situaciones. Los detalles específicos o el alcance de las verificaciones de antecedentes realizadas dependen de la posición para la cual el individuo está solicitando. A los empleados se les asignará una descripción del trabajo por escrito al momento de la incorporación. Los nuevos empleados reciben los procedimientos en forma documental. Se requiere que los nuevos empleados completen la capacitación sobre el Código de Conducta Comercial que establece expectativas duraderas de los compromisos que hacemos entre nosotros y nuestra empresa, con nuestras entidades usuarias y accionistas, y con las comunidades en las que vivimos y trabajamos. El Código de Conducta se aplica por igual a todos los que trabajan en DXC, proporciona a los empleados las pautas de conducta corporativa y requiere que se mantenga la confidencialidad de la información de la entidad corporativa y del usuario. DXC tiene un programa de ética y cumplimiento que incluye la capacitación requerida para que los empleados deben completar, DXC tiene una política de seguridad de la información y estándares asociados que documenta y proporciona orientación al personal de DXC y requiere que los empleados completen la capacitación anual de Conciencia de Seguridad. La confidencialidad y privacidad de la información y los datos de la entidad usuaria se enfatiza en el manual del Código de Conducta Comercial, así como durante la orientación de los nuevos empleados.

- Estándares y procedimientos: Los empleados de DXC utilizan los valores CLEAR de la compañía para guiar sus decisiones y acciones comerciales. Estos valores subrayan la creencia de que DXC es un lugar de trabajo ético, honesto, inclusivo y transparente; lo que es fundamental para el éxito a largo plazo de la empresa. Los valores CLEAR de DXC son un importante diferenciador competitivo e impulsor intangible del éxito de nuestra empresa. Definen lo que hacemos y quiénes somos; nuestros valores CLEAR son los distintivos del rendimiento y la reputación de la compañía.

¿Se mantienen políticas y procedimientos por escrito y claramente definidos?

DXC mantiene un sistema de gestión de calidad para la documentación de políticas y procesos para que los empleados puedan consultarlo fácilmente. Las políticas, procesos e instrucciones de trabajo del Sistema Integrado de Gestión de Calidad (IQMS) están documentados en el Manual de Calidad y en documentos subordinados. Los procesos que resultan directamente en la entrega de productos y servicios a la entidad usuaria están documentados y controlados. La documentación incluye interacciones entre procesos, entidades de usuario y subcontratistas. Una comprensión disciplinada y una aplicación coherente de estos documentos por parte de los asociados ayuda a confirmar que se cumplen los requisitos para entregar productos y servicios de calidad.

DXC tiene un conjunto de políticas y estándares que documentan el marco de políticas de seguridad de la información que utilizan los involucrados en la prestación de servicios para crear e implementar un sistema de gestión de seguridad de la información apropiado y efectivo para la entrega de la entidad de usuario a menos que DXC esté contractualmente obligado a seguir la entidad del usuario específica Políticas de seguridad de la información. Dentro del contenido disponible en ESIS (*Enterprise Security Information Systems*), del cual se asigna a la industria relevante, la legislación relevante, las regulaciones y los estándares globales, hay un conjunto de estándares de control de línea de base definidos. Estas normas de control se dividen en controles generales (administrativos) y técnicos. Los controles generales son aquellos que son básicos para un área operativa, mientras que los controles técnicos tienden a ser de naturaleza específica de la tecnología y se centran en el software compatible con el centro de datos.

¿Se realiza algún proceso de evaluación de riesgos?

El proceso de identificación, evaluación y gestión de riesgos es un componente crítico del sistema de control interno DXC. El propósito del proceso de evaluación de riesgos es identificar, evaluar y administrar los riesgos que afectan la capacidad de la organización para lograr sus objetivos. La administración de DXC también monitorea los

controles para considerar si están operando según lo previsto, y si se modifican según sea apropiado para cambios en las condiciones o riesgos que enfrenta la organización.

La gestión de riesgos es un componente generalizado de los servicios proporcionados por DXC a sus clientes, independientemente de la ubicación o área comercial. El personal de operaciones de DXC dirige programas, proyectos u operaciones y tiene la responsabilidad principal de comprender y gestionar los riesgos asociados con sus actividades.

A nivel corporativo, existen múltiples funciones, incluyendo Legal, Ciberseguridad, Auditoría Interna, Gestión de Riesgos, Adquisiciones, Salud y Seguridad de los Empleados, Contratos y Gobernanza y Cumplimiento de Clientes (GCC), de las cuales brindan apoyo de gestión de riesgos a través de la orientación de políticas y Servicios de consultoría interna. El departamento de Auditoría Interna es responsable de evaluar el entorno de control y riesgo de DXC a través de la evaluación de controles financieros, operativos y administrativos, prácticas de gestión de riesgos y el cumplimiento de las leyes, reglamentos y políticas y procedimientos de DXC. Auditoría interna informa al Comité de Auditoría de DXC y comunica hallazgos significativos y el estado de las acciones correctivas. GCC rige el proceso de evaluación de riesgos para DXC.

¿Podría describir cómo se realiza la información y comunicación de resultados y procedimientos?

La información y la comunicación son un componente integral del sistema de control interno de DXC. Es el proceso de identificar, capturar e intercambiar información en la forma y el marco de tiempo necesarios para llevar a cabo, administrar y controlar las operaciones de la entidad. Este proceso abarca las clases principales de transacciones de la organización, incluida la dependencia y la complejidad de la tecnología de la información. En DXC, la información es identificada, capturada, procesada e informada por varios sistemas de información, así como a través de conversaciones con entidades de usuarios, proveedores, reguladores y empleados.

Para ayudar a alinear las estrategias y objetivos comerciales de DXC con el rendimiento y los controles operativos, DXC ha implementado varios métodos de comunicación a nivel global para confirmar que los empleados comprenden sus roles y responsabilidades individuales y para confirmar que los eventos importantes se comunican de manera oportuna. Estos métodos incluyen programas de orientación y capacitación para empleados recién contratados, reuniones periódicas de administración para actualizaciones sobre el desempeño comercial y otros asuntos, transmisión de videoconferencia, el uso de mensajes de correo electrónico para comunicar mensajes e información urgentes, y la intranet DXC.

¿Cómo es el proceso de supervisión?

La gerencia de DXC se compromete a mantener una comunicación efectiva con el personal. La gerencia de DXC participa en reuniones regulares para discutir el estado del procesamiento actual del cliente, la estructura organizacional y otros asuntos de interés y preocupación. Los problemas o sugerencias identificados por el personal se ponen en conocimiento de la gerencia para que sean abordados y resueltos. Además, el personal de DXC asiste a reuniones para recibir actualizaciones sobre el desempeño comercial reciente y otros asuntos.

El personal de administración y supervisión de DXC monitorea la calidad del desempeño del control interno como parte normal de sus actividades. Para ayudarlos en el monitoreo, DXC ha implementado una serie de informes de gestión que miden los resultados de varios procesos involucrados en la prestación de servicios de procesamiento de transacciones a los usuarios. Además, se ha implementado el proceso seguro del Sistema de excelencia de calidad (QEX) para monitorear y evaluar el cumplimiento de los estándares DXC. Las evaluaciones QEX Secure son realizadas por el personal de DXC y las desviaciones se rastrean y corrigen.

Las excepciones al procesamiento normal o programado a través de hardware, software o problemas de procedimiento se registran, informan y resuelven diariamente. Los niveles apropiados de gestión revisan estos informes diaria y semanalmente y se toman medidas según corresponda.

DXC monitorea los Estándares de Nivel de Servicio (SLS) basados en las pautas establecidas por el cliente y / o la industria. Los estándares incluyen los procesos clave de cambio y gestión de problemas. Los acuerdos específicos de declaración de trabajo se establecen con las cuentas operativas de DXC cuando sea necesario. Estos acuerdos pueden establecer un nivel diferente de servicio que se proporcionará a una cuenta en particular. DXC proporciona 24 horas al día, 7 días a la semana, disponibilidad del sistema y monitoreo del umbral del sistema a través de instalaciones de monitoreo remoto con personal completo.

Con respecto a la seguridad de información, ¿cuáles son las políticas principales?

Se definen los controles mínimos de seguridad de línea de base establecidos en los sistemas de rango medio en el entorno del centro de datos. Cuando DXC no está obligado contractualmente a seguir la política de seguridad del cliente, se implementa el conjunto mínimo de controles de seguridad de ESIS de referencia, a menos que la versión del sistema operativo instalado no admita la configuración. Cuando no se establece un estándar de control en un sistema, la documentación de respaldo, junto con una (s) excepción (es) a la política, debe presentarse, aprobarse y archivarse de acuerdo con los procedimientos de ESIS. La documentación técnica que define los estándares de configuración está disponible en línea para su revisión por los administradores del sistema.

Los procesos de auditoria se hacen con agentes terceros para asegurar la parcialidad, el proveedor de este servicio usa sus metodologías y plantillas por lo que DXC se limita a proveer la información requerida según cada control. DXC también se encarga crear y/o mantener los planes de remediación o documentos de aceptación de riesgos.

La línea de base de cumplimiento DXC establecida incluye, pero no se limita a, las siguientes áreas:

Autenticación / Integridad de la cuenta

- La configuración de la contraseña está establecida para proteger la entrada.
- Las ID de usuario predeterminadas con contraseñas predeterminadas empaquetadas con el software o los componentes del proveedor se deshabilitan, cambian de nombre o se cambia la contraseña predeterminada después de la instalación para evitar el uso no autorizado. Las ID de usuario invitado, si las proporciona el sistema, se controlan de manera similar.

Administración de acceso

- El acceso a los sistemas de rango medio está aprobado y es apropiado para las funciones del trabajo.
- Las cuentas de usuario únicas se asignan a individuos según la función que realizan. Las cuentas compartidas o grupales requieren responsabilidad individual.
- Una sesión que ha permanecido inactiva durante un período de tiempo específico está bloqueada y requiere una nueva autenticación para iniciar sesión
- Las ID de usuario deben bloquearse o deshabilitarse después de un número específico de intentos de inicio de sesión de cuenta si el sistema puede volver a habilitar automáticamente la ID de usuario después de un período de tiempo. Si el sistema no puede volver a habilitar automáticamente, la sesión del usuario no se deshabilita.
- El acceso de usuarios y grupos está restringido adecuadamente para realizar solo las funciones necesarias para realizar el trabajo, de mismo modo, la información sensitiva es enmascarada y solo puede ser vista si el perfil de seguridad del cliente lo permite.
- PowerCARD es una aplicación comercial estándar proporcionada por High Payment Systems (HPS) que ingiere transacciones de pago y tarjetas de fidelización y ejecuta procesos de liquidación basados en las reglas comerciales configuradas en el software En el sistema se procesan millones de dólares globalmente y su buen funcionamiento es de mucha importancia para el negocio de Shell . Los resultados de la liquidación se envían a los adquirentes, los sistemas ERP de Shell y un repositorio de documentación.

Adquisidores y Shell utilizan estos resultados para ejecutar actividades de liquidación financiera.

- Revisión periódica de acceso: El acceso a la aplicación PowerCARD se revisa trimestralmente. Los usuarios internos de DXC son revisados por revisores designados (supervisores / líderes) en el equipo de soporte de aplicaciones de DXC. Las modificaciones para acceder son procesadas por el equipo de soporte de aplicaciones DXC.

Los usuarios a los sistemas del cliente y su acceso relacionado en PowerCARD se proporcionan al solicitante o remitente autorizado de Shell para su revisión. El solicitante o remitente autorizado de Shell proporciona cambios para acceder al equipo de soporte de aplicaciones DXC y el equipo de soporte de aplicaciones DXC modifica el acceso a las aplicaciones según lo solicitado.

¿Cuáles has sido los aspectos en que se puede mejorar los procesos de auditoría por parte de DXC?

En el equipo de soporte ad la aplicación web para el projecto de Shell EVE, hemos tenido algunos problemas para mantener, organizar y dar seguimiento a las revisiones periodicas de vulnerabilidades, especificamente para dar seguimiento a los puntos que han sido resaltado como resultado de estas revisiones. Hemos tenido escalaciones por parte del cliente en cuanto a la remediacion de vulnerabilidades.

Otro punto es el manejo de medios fisicos para procesos de autorizaciones manuales de transacciones. Por necesidad del negocio, las aprovaciones son enviadas por correo electronico y son impresas para su majeno. Y mientras si tenemos un proceso definido para la eliminacion segura, no tenemos evidencia que mostrarle a los auditores, lo cual puede ser considerado como una violacion al estandard.

En cuanto al acceso a informacion sensitiva dentro de la aplicación, tenemos un problema y es que el equipo de soporte no tiene total conocimiento de los procesos de negocio que Shell hace en su herrameinta, tampoco tenemos el control de los modulos en los que se puede acceder a esta informacion. La aplicación PowerCard muestra informacion sensitiva según el perfil de seguridad. Mientras existe documentacion que

mapea los diferentes niveles de seguridad an cuanto al acceso de informacion PCI, tenemos actualizaciones constantes que muchas veces han cambiado el esquema de seguridad inicial hasta el punto de haber tenido incidentes de usuarios finales teniendo acceso a informacion sensitiva sin que su puesto de trabajo asi lo requiera.

Otro dato importante es que el aplicativo y las operaciones contables de la empresa han crecido, de manera tal que se han creado múltiples unidades de negocio y perfiles de seguridad, lo que complica el control sobre el acceso que cada perfil tiene y la manutencion de la documentacion alrededor de este tema.

Repetidamente las auditorías ejecutadas, han evidenciado hallazgos enfocados a las restricciones de los distintos perfiles de seguridad, que han penalizado el servicio del proveedor según los contratos de nivel de servicio (SLA por sus siglas en ingles), sin encontrar la causa raíz del problema. Los esfuerzos de analistas de TI en mejoras del diseño de perfiles de seguridad han sido ineficientes en cumplir con soluciones alineadas con los estándares de calidad PCI y mejores prácticas.

APÉNDICE E. MINUTAS DE ENTREVISTAS

Minuta de Entrevista			
Minuta No.	001	**Fecha**	06/04/2020
Lugar	Reunion en plataforma Virtual	**Hora inicio/ finalización**	7:00pm
Motivo de la reunión	Llevar a cabo la entrevista planeada		

Participantes		
Nombre	**Rol**	**Condición de la entrevista**
Rolando Gonzalez Montero	Gerente de Auditoria de TI	Entrevistado
Mauricio Lizano Barahona	Estudiante	Moderador

Desarrollo de la entrevista
Entrevista para obtener informacion sobre Metodologias de Auditoria de tecnologias de la informacion

Firmas:

Mauricio Lizano Barahona

Rolando Gonzalez Montero

Minuta de Entrevista			
Minuta No.	002	**Fecha**	13/04/2020
Lugar	Reunion en plataforma Virtual	**Hora inicio/ finalización**	4:00pm/
Motivo de la reunión	Llevar a cabo la entrevista planeada		

Participantes		
Nombre	**Rol**	**Condición de la entrevista**
Manuel Marin Cubero	Gerente de Auditoria de TI	Entrevistado
Mauricio Lizano Barahona	Estudiante	Moderador

Desarrollo de la entrevista
Entrevista para obtener informacion sobre Metodología de Auditoría de tecnología de la información

Firmas:

Mauricio Lizano Barahona

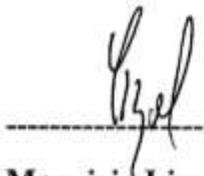
Manuel Marin Cubero

Minuta de Entrevista			
Minuta No.	003	**Fecha**	06/04/2020
Lugar	Reunion en plataforma Virtual	**Hora inicio/ finalización**	7:00pm
Motivo de la reunión	Llevar a cabo la entrevista planeada		

Participantes		
Nombre	**Rol**	**Condición de la entrevista**
Henry Vega Rodriguez	Gerente de Auditoria Acorde	Entrevistado
Mauricio Lizano Barahona	Estudiante	Moderador

Desarrollo de la entrevista
Entrevista para obtener informacion sobre Evaluación de riesgos en Auditoría

Firmas:



Mauricio Lizano Barahona

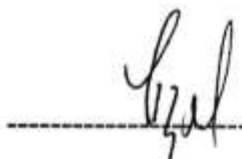
Henry Vega Rodriguez

Minuta de Entrevista			
Minuta No.	004	**Fecha**	06/04/2020
Lugar	Reunion en plataforma Virtual	**Hora inicio/ finalización**	7:00pm
Motivo de la reunión	Llevar a cabo la entrevista planeada		

Participantes		
Nombre	**Rol**	**Condición de la entrevista**
Deborah Deborse	Account Delivery Manager	Entrevistada
Mauricio Lizano Barahona	Estudiante	Moderador

Desarrollo de la entrevista
Entrevista para obtener informacion sobre Área de negocio y segmento de la empresa.

Firmas:



Mauricio Lizano Barahona

***Ver Anexo 6**

Deborah Deborse

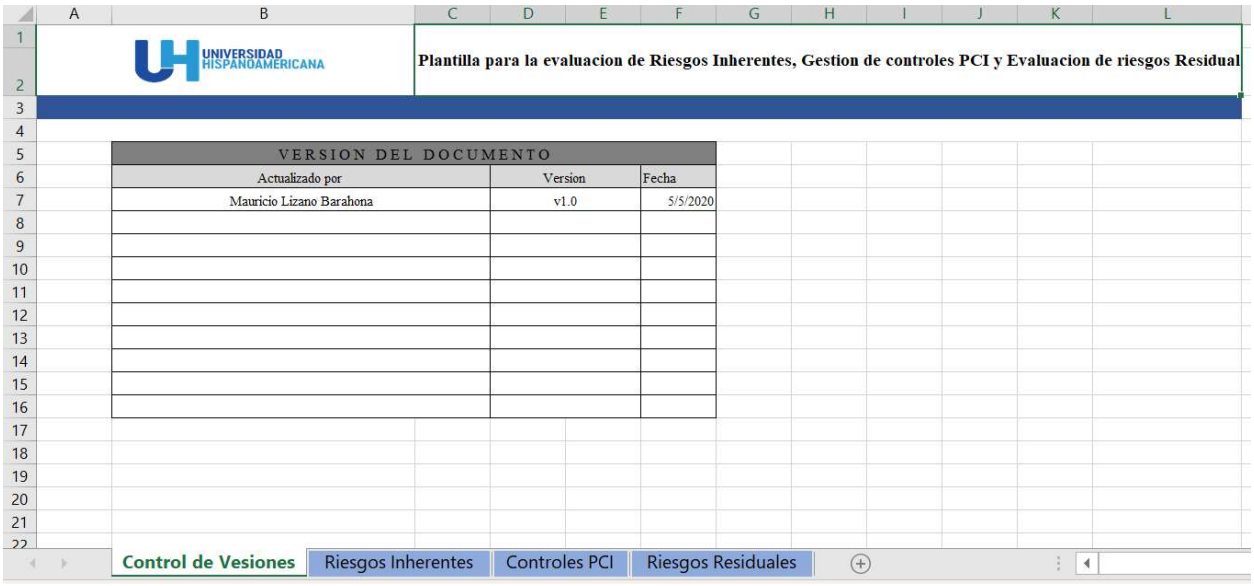
APÉNDICE D. PLANTILLA REVISION DOCUMENTAL

Información Historica de revision de documentos					
No.	**Nombre del Documento**	**Tipo de Documento**	**Autor**	**Fuente**	**Fecha de Revision**

Apéndice D.1. Historial Revision Documental

Información Historica de revision de documentos					
No.	**Nombre del Documento**	**Tipo de Documento**	**Autor**	**Fuente**	**Fecha de Revision**
Anexo 1	DXC Sanitization and Destruction Standard	Corporativo DXC	DXC Technology	DXC Technology	15/04/20
Anexo 2	Shell GRM Data Retention Schedule	Interno de la cuenta	DXC Technology	DXC Technology	10/04/20
Anexo 3	Notificacion de acceso fallido	Correo Interno de notificacion	DXC Technology	DXC Technology	10/04/20
Anexo 4	RCU Shell Cryptographic Keys	Interno de la cuenta	DXC Technology	DXC Technology	05/04/20
Anexo 5	RCU Shell PCI DSS Awareness	Interno de la cuenta	DXC Technology	DXC Technology	20/04/20

APÉNDICE F. HERRAMIENTA DE GESTIÓN DE RIESGOS Y CONTROLES PCI

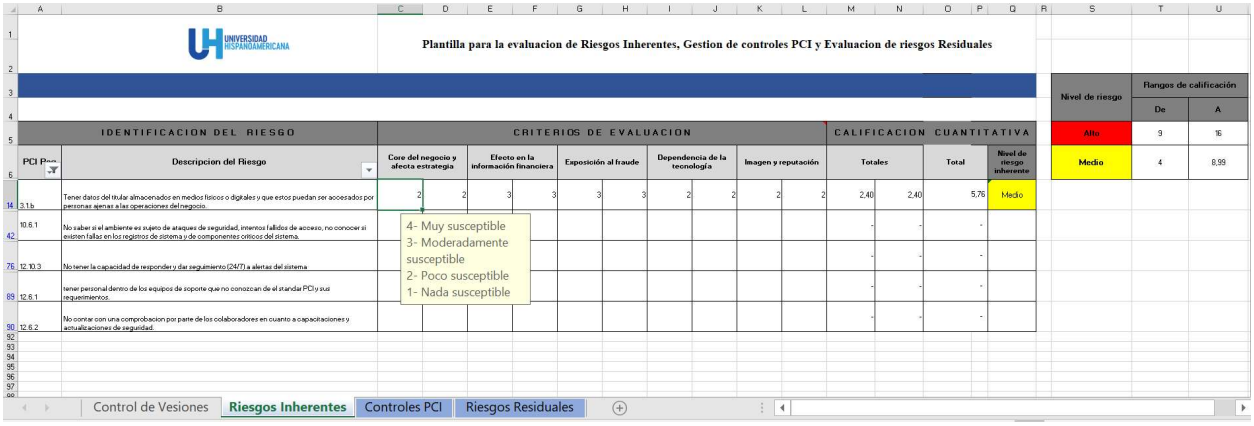


Plantilla para la evaluacion de Riesgos Inherentes, Gestion de controles PCI y Evaluacion de riesgos Residual

VERSION DEL DOCUMENTO		
Actualizado por	Version	Fecha
Mauricio Lizano Barahona	v1.0	5/5/2020

Control de Vesiones | Riesgos Inherentes | Controles PCI | Riesgos Residuales

Apéndice F.1 Identificación y Calificación de Riesgos Inherentes



Plantilla para la evaluacion de Riesgos Inherentes, Gestion de controles PCI y Evaluacion de riesgos Residuales

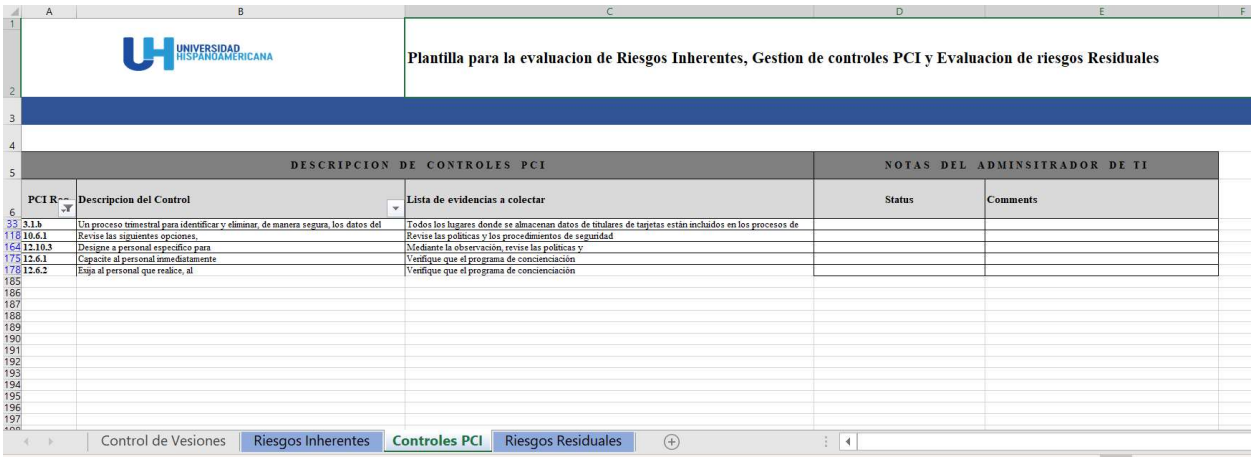
Nivel de riesgo	Rangos de calificación	
	De	A
Alto	9	16
Medio	4	8,99

IDENTIFICACION DEL RIESGO		CRITERIOS DE EVALUACION						CALIFICACION CUANTITATIVA			
PCI Ref.	Descripcion del Riesgo	Core del negocio y afecta estrategia	Efecto en la información financiera	Exposición al fraude	Dependencia de la tecnología	Imagen y reputación		Totales		Total	Nivel de riesgo inherente
3.1.b	Tener datos del titular almacenados en medios físicos o digitales y que estos puedan ser accesados por personas ajenas a las operaciones del negocio.	2	2	3	3	3	3	2	2	2	2	2,40	2,40	5,76	Medio
10.6.1	No saber si el ambiente es sujeto de ataques de seguridad, intentos fallidos de acceso, no conocer si existen fallas en los registros de sistema y de componentes críticos del sistema.											-	-	-	
12.10.3	No tener la capacidad de responder y dar seguimiento (24/7) a alertas del sistema											-	-	-	
12.6.1	tener personal dentro de los equipos de soporte que no conozcan de el standar PCI y sus requerimientos.											-	-	-	
12.6.2	No contar con una comprobacion por parte de los colaboradores en cuanto a capacitaciones y actualizaciones de seguridad.											-	-	-	

4- Muy susceptible
3- Moderadamente susceptible
2- Poco susceptible
1- Nada susceptible

Control de Vesiones | Riesgos Inherentes | Controles PCI | Riesgos Residuales

Apéndice F.2 Identificación de Controles Adecuados con referencia a Estándar PCI

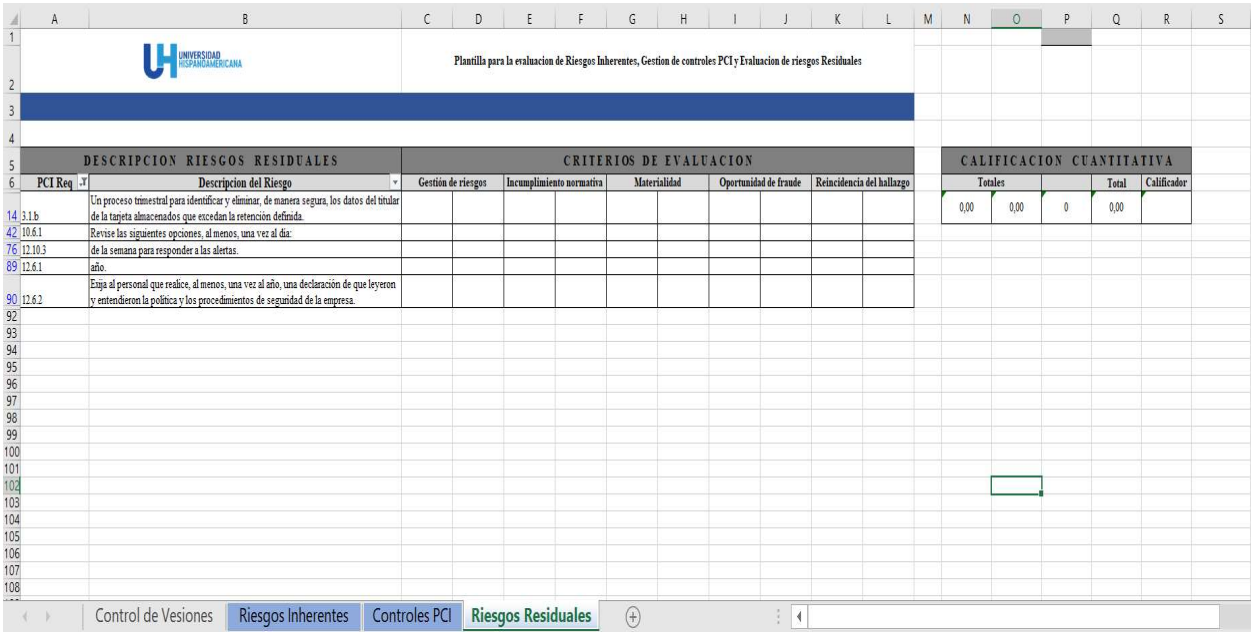


Plantilla para la evaluacion de Riesgos Inherentes, Gestion de controles PCI y Evaluacion de riesgos Residuales

DESCRIPCION DE CONTROLES PCI			NOTAS DEL ADMINSITRADOR DE TI	
PCI R...	Descripcion del Control	Lista de evidencias a colectar	Status	Comments
3.1.b	Un proceso trimestral para identificar y eliminar, de manera segura, los datos del	Todos los lugares donde se almacenan datos de titulares de tarjetas están incluidos en los procesos de		
10.6.1	Revise las siguientes opciones,	Revise las políticas y los procedimientos de seguridad		
12.10.3	Designe a personal específico para	Mediante la observación, revise las políticas y		
12.6.1	Capacite al personal inmediatamente	Verifique que el programa de concienciación		
12.6.2	Exija al personal que realice, al	Verifique que el programa de concienciación		

Control de Vesiones | Riesgos Inherentes | Controles PCI | Riesgos Residuales

Apéndice F.3 Identificación y Calificación de Riesgos Residuales



Plantilla para la evaluacion de Riesgos Inherentes, Gestion de controles PCI y Evaluacion de riesgos Residuales

DESCRIPCION RIESGOS RESIDUALES		CRITERIOS DE EVALUACION									
PCI Req	Descripcion del Riesgo	Gestión de riesgos		Incumplimiento normativa		Materialidad		Oportunidad de fraude		Reincidencia del hallazgo	
3.1.b	Un proceso trimestral para identificar y eliminar, de manera segura, los datos del titular de la tarjeta almacenados que excedan la retención definida.										
10.6.1	Revise las siguientes opciones, al menos, una vez al día:										
12.10.3	de la semana para responder a las alertas.										
12.6.1	año.										
12.6.2	Exija al personal que realice, al menos, una vez al año, una declaración de que leyeron y entendieron la política y los procedimientos de seguridad de la empresa.										

CALIFICACION CUANTITATIVA				
Totales			Total	Calificador
0,00	0,00	0	0,00	

Control de Vesiones | Riesgos Inherentes | Controles PCI | Riesgos Residuales

ANEXOS

ANEXO 1. DXC SANITIZATION AND DESTRUCTION STANDARD

PURPOSE

This standard defines the controls required for the secure sanitization or destruction of Covered DXC Information Systems, Covered DXC Information, Electronic Media or physical documents (paper) when redistributed, transferred, sold, no longer required for business purposes or reached end of useful life.

This standard is published in support of the DXC Information Security Policy.

APPLICABILITY

This standard applies to:

- Covered DXC Employees
- Covered DXC Information
- Covered DXC Information Systems
- Covered DXC Third Parties

DEFINITIONS

"Covered DXC Information" means all DXC, Customer, Supplier, Employee, and other Third Party confidential, proprietary, financial, personal or other sensitive information stored, transmitted, or received using a Covered DXC Information System whose unauthorized disclosure or access can result in harm to DXC Technology or a Third Party to whom that information belongs. The term "Information" applies regardless of whether the Information exists in digital, audio, electronic, facsimile, or other form.

"Covered DXC Information System" means any information system owned or controlled by DXC Technology and used to store, transmit, or receive Covered DXC Information. It also means any customer information systems or acquired services (third party or as a Service (aaS)) to the extent such information systems or services are physically or logically connected to Covered DXC Information Systems or owned, controlled, managed or supervised by DXC. Examples include, but are not limited to:

- Servers
- Personal computers
- Laptops

- Smartphones
- Tablets

"Covered DXC Employee" means any employee of DXC, its wholly-owned subsidiaries, and their affiliates.

"Covered DXC Third Party" means any business partner, supplier, sub-contractor, reseller, distributor, joint venture, consortium, teaming partner, channel partner, lobbyist, law firm or other business partner that will either assist DXC in delivering services, represent DXC's interests to a customer or third party, or provide DXC a service.

"Covered DXC Information Owners" for the purposes of this standard refers to DXC Management, Business Units, and Functions.

"DXC Technology," for purposes of this standard means the DXC Technology company, its parents, subsidiaries, affiliates, and legacy businesses; Covered DXC Third Parties; and Covered DXC Employees.

"Electronic Media" for the purposes of this standard is any electronic storage device that is used to record information, i.e., magnetic storage media (disk, diskette, tape, etc.), and optical media (CD, CD-ROM, CD-RW, DVD-RW, etc.). This includes, but is not limited to hard disks, magnetic tapes, compact disks (CDs), videotapes, audiotapes, and removable storage devices such as floppy disks and zip disks, memory cards, USB drives and memory plug-ins.

"Sanitization" for the purposes of this standard is the secure removal of Covered DXC Information from Covered DXC Information Systems or Electronic Media. It is the process of overwriting and removing any traces of files or file fragments so that the information cannot be recovered.

"Destruction" for the purposes of this standard is the process of destroying Covered DXC Information stored on Electronic Media or physical documents so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.

SANITIZATION AND DESTRUCTION STANDARD

4.1 Requirements

Before Covered DXC Information Systems, Electronic Media or physical documents are redistributed, transferred, sold or disposed of, they must be properly sanitized or destroyed to ensure that any Covered DXC Information present is not recoverable or readable by any means.

If Covered DXC Information and Covered DXC Information Systems are subject to Discovery or a Legal Hold, the requirements outlined in the Records and Information Management Policy supersede this standard.

4.2 Sanitization or Destruction Considerations

The following shall be considered prior to determining the appropriate sanitization or destruction treatment:

- Determine the sensitivity level of the Covered DXC Information to identify whether sanitization or destruction is the appropriate course of action. For more information on identifying, labelling and securing DXC's information assets, refer to the DXC Information Categorization Standard, Records and Information Management Policy, Confidential Information Policy or the Privacy and Data Protection Policy.
- Determine the electronic media type. For example, CDs cannot be sanitized and must be destroyed.
- Determine the operational status of the Covered DXC Information System. If a system is fully functioning, it shall be sanitized allowing the system to be reused.

  Non-functioning systems' electronic storage media must be degaussed or destroyed.

4.3 Sanitization Techniques

When it becomes necessary to reuse, transfer/sell or destroy Covered DXC Information Systems, an approved method for sanitization must be followed to render all Covered DXC Information residing on the systems non-recoverable. Refer to section 4.4 a description of each sanitization method.

The following techniques are approved methods for sanitization or destruction based on media type.

Media Type	Complete Physical Destruction	Degauss	Overwrite	Disk Sanitizer Feature in BIOS	Remote Wipe
Hard Disk Drives	X	X	X	X	
Magnetic Tapes	X	X	X		
Optical Media (CDs/DVDs)	X		X		
USB keys	X		X		
Smartphones	X				X
Physical documents (paper)	X				

4.4 Sanitization Methods

4.4.1 **Specific methods of approved sanitization or destruction include**:

- Completion of a hard drive sanitization if the feature in the PC BIOS.
- Overwriting of information. Overwriting of information means replacing previously stored information on an information system with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. As the

name implies, overwriting uses a program to write 1s, 0s, or a combination onto the media. The DXC standard practice is to overwrite the media three times with random data. Overwriting shall not be confused with merely deleting the pointer to a file (which typically happens when a delete command is used). The overwriting process must be correctly understood and carefully implemented. Sanitization is not complete until three overwrite passes and a verification pass are completed. Note: Client contractual requirements may require different sanitization methods. Consult with the associated client's DXC Account General Manager and Legal/Contracts Representative for guidance. In all cases, the most stringent requirement (e.g., this standard or the more contractual requirement) must be applied.

- Degaussing an information system. Degaussing is a process whereby an information system is erased, i.e., returned to a zero state. Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack. Two types of degassers exist: strong permanent magnets and electric degassers.

- Complete destruction that renders the Covered DXC Information, Covered DXC Information System, media or physical documents (paper) completely unreadable, inaccessible or unusable. Examples include, but are not limited to:
- Shredding with a crosscut shredder or proprietary information shred bin for Covered DXC Information
- Physical force (e.g., pounding CDs/DVDs/hard drives with a sledgehammer)
- Use of an approved metal destruction facility to smelt, disintegrate or pulverize that will disfigure, bend, mangle, or otherwise mutilate Covered DXC Information System, i.e. laptops, PCs, servers

4.5 Destruction of Encryption Keys

Secure deletion of all encrypted keys necessary to recover any clear text on a Covered DXC Information System or Electronic Media is another approved method of sanitization. For example, destruction of the Bitlocker encrypted key.

ROLES AND RESPONSIBILITIES

Role	Responsibility
Covered DXC Employees	• Know and observe the sanitization and destruction requirements and controls specified by this standard. • Provide all the necessary transfer documentation to DXC approved sanitization/destruction vendors and ensure that they contractually adhere to the sanitization and destruction techniques specified herein.
Office of the CIO (OCIO) Information Assurance (IA)	• Publish the DXC Sanitization and Destruction Standard and make available to Covered DXC Employees. • Provide guidance on compliance to this standard.

Covered DXC Information Owners	• Follow the requirements specified herein for proper sanitization and destruction of Covered DXC Information and Covered DXC Information Systems. • Verify that all Covered DXC Information Systems being redistributed or transferred/sold have signed sanitization certificates attached to them before they are processed, unless transfer is to a DXC approved destruction vendor. • Provide assistance in properly performing the sanitization task, and in obtaining approved sanitization tools and/or vendors. • Retain all completed sanitization certificates for a period of one year. • Audit of the sanitization and destruction process when performed by DXC staff to ensure data is no longer retrievable, i.e., a knowledgeable DXC IT person must witness the sanitization process and verify that the electronic storage media (e.g., a hard drive) was sanitized.
Supply Chain Management (SCM) and Legal Contracts Management	SCM and Legal Contracts Management are responsible for ensuring that contracts with Covered DXC Third Parties who handle Covered DXC Information and Covered DXC Information Systems require the application of the relevant controls stipulated by this standard.

EXCEPTIONS AND VARIANCES

Exceptions or variance to this standard must be sought and secured in writing from the Director of OCIO IA or his or her designee. No exception will be approved for longer than one year.

COMPLIANCE

Any Covered DXC Employee who knowingly violates or attempts to violate this standard and associated standards shall be subject to disciplinary action, up to and including termination of employment.

Any Covered DXC Third Party who violate this standard and associated standards may be barred from continued use/access to DXC and any equipment used may be seized, inspected, and images made and retained for further investigation.

REFERENCES

The following references support this standard. Additional supporting documents are maintained in the DXC Centralized Policy Management System.

Reference Title	Relevance
DXC Information Security Policy	Overarching Policy
DXC Information Categorization Standard	Provides requirements for categorization Covered DXC Information based on sensitivity level of that information.
Records and Information Management Policy	Provides requirements on records and information assets management and disposition that supports business goals and legal, regulatory and contractual requirements.
Confidential Information Policy	Provides requirements for identifying, labeling and securing DXC's confidential information assets.
Privacy and Data Protection Policy	Provides definitions and requirements for complying with a global set of standard principles for the protection of Personal Data.

ANEXO 2. RCU SHELL GRM DATA RETENTION SCHEDULE

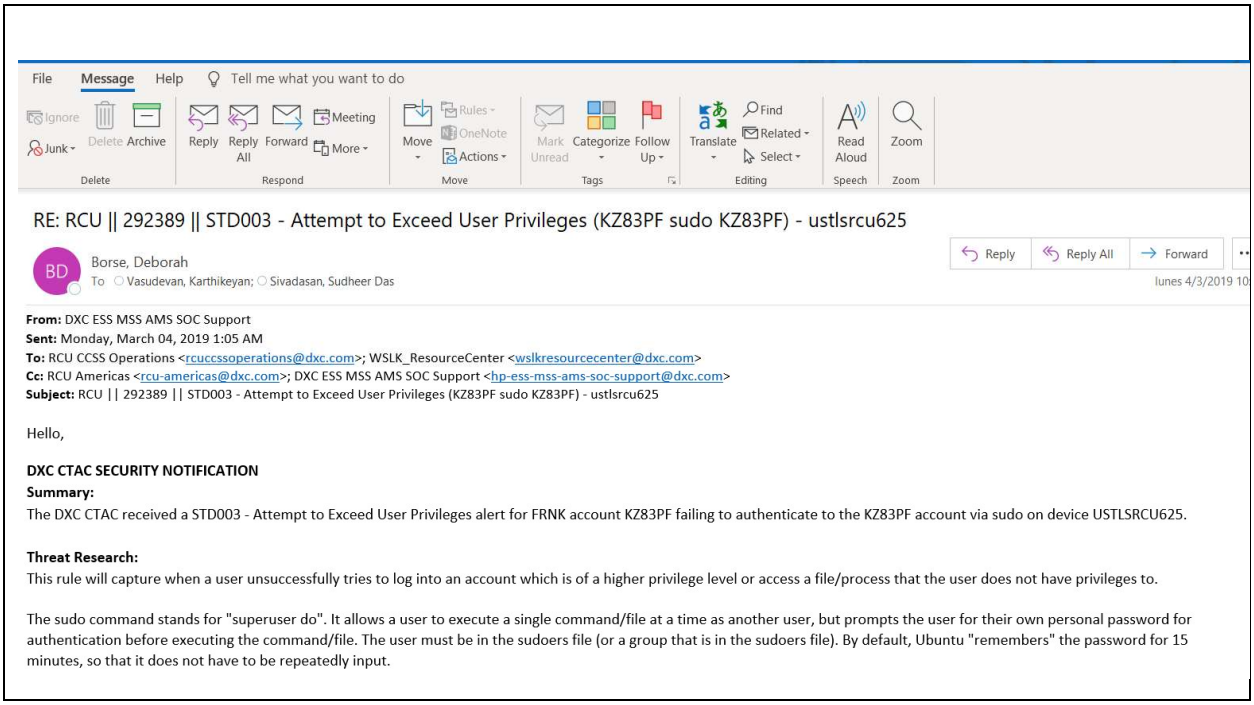
Database Data Retention	Data Type/Category	Database - Online Retention Period				Database - Archive Retention Period				PII		
		HK	MO	CA	GL3 & GL4	HK	MO	CA	GL3 & GL4	HK	MO	CA
Database Data	PCI Transactional Data	4 months	4 months	4 months	4 months	8 years	8 years	8 years	8 years	Yes	Yes	Yes
Database Data	PCI Master Data	TEOC/Live Update	TEOC/Live Update	TEOC/Live Update	TEOC/Live Update	N/A	N/A	N/A	N/A	Yes	Yes	Yes
Database Data	Non PCI Transactional Data	2 months	2 months	2 months	2 months	N/A	N/A	N/A	N/A	No	No	No
Database Data	Non PCI Master Data	TEOC/Live Update	TEOC/Live Update	TEOC/Live Update	TEOC/Live Update	N/A	N/A	N/A	N/A	No	No	No

Note : For Canada the PCI Transactional Data - Database Online Retention Period will be changed from 7 months to 4 months effective from 30th June 2017 as per re-baseline negotiation.

ABBREVIATIONS	
Live Update	Retailer's Master Data - updated every 2 hours from Shell's system.
TEOC	Till End Of Contract

Version | Database Retention_plan

ANEXO 3. NOTIFICACIÓN DE ACCESO FALLIDO



ANEXO 4. RCU SHELL CRYPTOGRAPHIC KEYS

PCI Req 3.5.1, 3.6.3, 3.6.4, 3.6.5: Cryptographic Keys

3.5.1

- Inventory of Keys and Keys storage location (date of creation, strengths, location, usage, expiration date)
    - Proof of review
    - Proof of renewal
    -

3.6.3

- Inventory of Keys and Certificates (date of creation, strengths, location, usage, expiration date)
    - Proof of review
    - Proof of renewal
    -

3.6.4

- Inventory of keys and certificates (date, strengths, location, usage, ...)
- Cryptoperiods for each key type in use and date last time each key was changed
- Tickets showing the keys was changed for those applicable (at the end of the cryptoperiod)

3.6.5

- List of leavers from HR / management (including contractors)
- Inventory of keys and certificates (date, strengths, location, usage, ...)
- Management acknowledgement from concerned teams (application /TLS termination points, ...) if actions were needed or confirmation that no one left that had access to cryptographic keys
- Results of actions taken (Tickets opened to change keys ? Etc…)

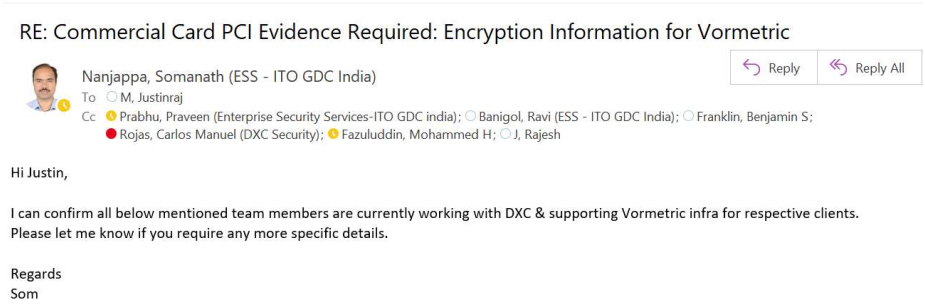
Evidence date: 2020-03-17

Inventory of Keys and Key Storage location: Image of list of Agent Keys. Original document provided separately.

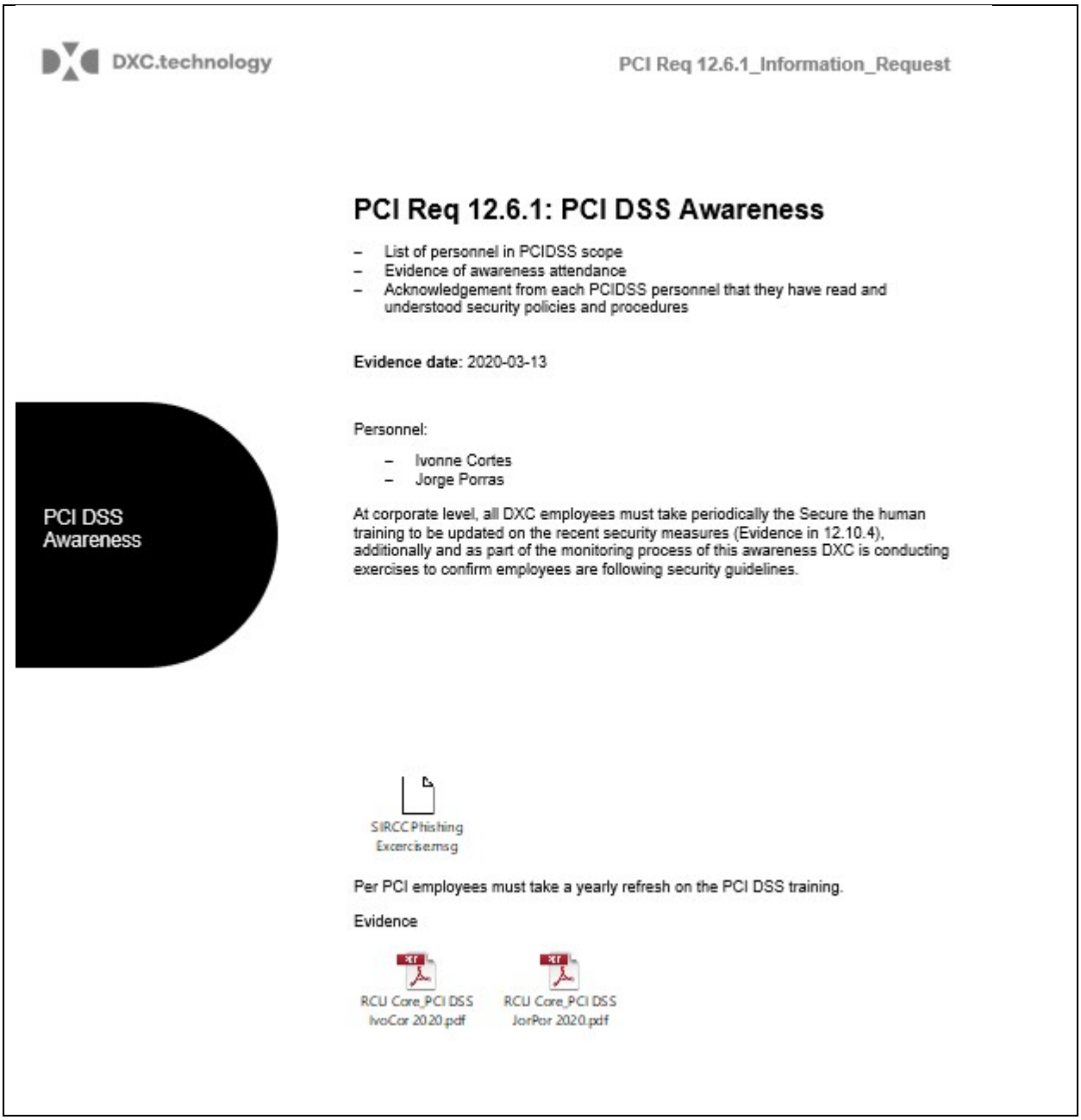
3.5.1, 3.6.3, 3.6.4 Evidence

3.6.5 Evidence

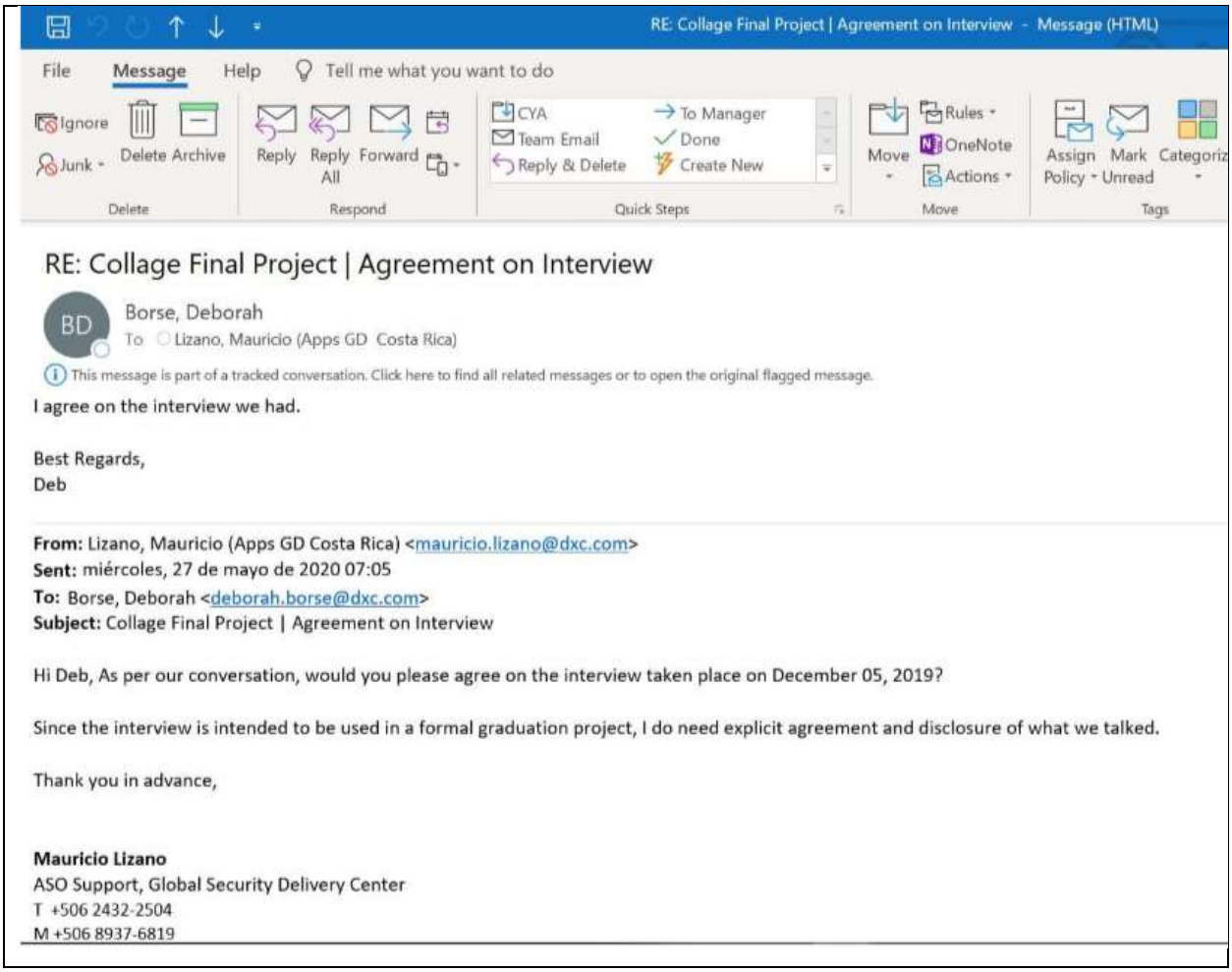
List of leavers from HR / management certification: There were no Key holders that have left the organization



ANEXO 5. RCU SHELL PCI DSS AWARENESS



ANEXO 6. CONFIRMACION DE ENTREVISTA



RE: Collage Final Project | Agreement on Interview - Message (HTML)

File Message Help Tell me what you want to do

Ignore Junk Delete Archive | Reply Reply All Forward | CYA Team Email Reply & Delete To Manager Done Create New | Move Rules OneNote Actions | Assign Policy Mark Unread Categoriz

Delete Respond Quick Steps Move Tags

RE: Collage Final Project | Agreement on Interview

BD Borse, Deborah
To Lizano, Mauricio (Apps GD Costa Rica)

This message is part of a tracked conversation. Click here to find all related messages or to open the original flagged message.

I agree on the interview we had.

Best Regards,
Deb

From: Lizano, Mauricio (Apps GD Costa Rica) <mauricio.lizano@dxc.com>
Sent: miércoles, 27 de mayo de 2020 07:05
To: Borse, Deborah <deborah.borse@dxc.com>
Subject: Collage Final Project | Agreement on Interview

Hi Deb, As per our conversation, would you please agree on the interview taken place on December 05, 2019?

Since the interview is intended to be used in a formal graduation project, I do need explicit agreement and disclosure of what we talked.

Thank you in advance,

Mauricio Lizano
ASO Support, Global Security Delivery Center
T +506 2432-2504
M +506 8937-6819

GLOSARIO

Datos: Son objetos de información en su sentido más amplio, los cuales pueden ser externos o internos, estructurados y no estructurados del tipo gráfico, sonido, imágenes, números, palabras y de otra índole, etc.

Información: Datos que han sido organizados, sistematizados y presentados de manera que los patrones subyacentes resulten claros.

Tecnología: Es un conjunto ordenado de instrumentos, conocimientos, procedimientos y métodos aplicados a las áreas.

Tecnologías de la Información y la Comunicación (TIC): Se refiere al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de la información.

Sistema de Información (SI): Se refiere a un conjunto de procesos y recursos de información organizados con el objetivo de proveer la información necesaria (pasada, presente, futura) en forma precisa y oportuna para apoyar la toma de decisiones en una entidad.

Software de Aplicación: Se refiere a un elemento de los Sistemas de Información, es un conjunto de programas de computador diseñados y escritos para realizar tareas específicas del negocio y que permiten la interacción entre el usuario y el computador.

Sistemas de comunicación: Se refiere a la tecnología que se emplea para el intercambio de información.

Confidencialidad de la información: Se refiere a la protección de la información crítica contra su divulgación no autorizada.

Integridad de la información: Se vincula con la exactitud y la totalidad de la información así como también con su validez de acuerdo con los valores y las expectativas de la entidad.

Confiabilidad de la información: Se vincula con la provisión de la información adecuada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de presentación de reportes financieros y de cumplimiento.

Disponibilidad de la información: Se vincula con el hecho de que la información se encuentre disponible cuando el proceso la requiera. También se asocia con la protección de los recursos necesarios y las capacidades asociadas.

Técnicas de Auditoría Asistidas por Computador (TAAC): Se refiere a las técnicas de auditoria que contemplan herramientas informáticas con el objetivo de realizar más eficazmente, eficientemente y en menor tiempo pruebas de auditoria.

Actividad de auditoría interna: un departamento, división, equipo de consultores, u otro/s profesional/es que proporciona/n servicios independientes y objetivos de aseguramiento y consulta, concebidos para agregar valor y mejorar las operaciones de una organización. La actividad de auditoría interna ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

Alta dirección: grupo de personas que tienen una autoridad delegada del organismo de gobierno para la implementación de estrategias y políticas destinadas a cumplir con el propósito de la organización. Este grupo puede incluir roles que rinden cuentas ante el órgano de gobierno o ante la cabeza de la organización o tienen la responsabilidad general de las funciones principales de presentación de informes, por ejemplo, directores ejecutivos (CEO), directores de organizaciones gubernamentales, directores de TI (CIO) y roles similares.3

Consejo: cuerpo de gobierno de más alto nivel de una organización (por ejemplo: junta directiva, consejo supervisor o administradores, patronato, directorio) que tiene la responsabilidad de dirigir o supervisar las actividades y al que la alta dirección rinde cuentas. Aunque los esquemas de gobierno varían entre jurisdicciones y sectores, generalmente, el Consejo incluye a miembros que no son parte de la dirección. Si no existe un Consejo, la palabra "Consejo" se refiere a un grupo o persona encargada del gobierno de la organización. Además, el "Consejo" en las Normas puede referirse a un comité u otro cuerpo en el que el órgano de gobierno haya delegado ciertas funciones (por ejemplo, un comité de auditoría).

Cumplimiento: adhesión a las políticas, los planes, los procedimientos, las leyes, las regulaciones, los contratos u otros requisitos.

Dirección: ejercicio del control y la supervisión en el contexto de la autoridad y la responsabilidad establecidas por el gobierno. El término "dirección" se usa a menudo como un término colectivo para designar a aquellos que tienen la responsabilidad de controlar una organización o partes de ella.4

Director ejecutivo de auditoría: se refiere a la función de una persona en un puesto de alta jerarquía responsable de la gestión efectiva de la actividad de auditoría interna de acuerdo con el estatuto de auditoría interna y los elementos obligatorios del Marco Internacional para la Práctica Profesional. El director ejecutivo de auditoría y las personas a su cargo tendrán las certificaciones y cualificación apropiadas. El nombre del puesto específico y/o las responsabilidades del director ejecutivo de auditoría pueden variar según la organización.

Gobierno: la combinación de estructuras y procesos implementados por el Consejo para informar, dirigir, gestionar y supervisar las actividades de la organización en pos del logro de sus objetivos.

Gobierno de tecnología de la información (TI): el gobierno de TI se compone del liderazgo, las estructuras de la organización y los procesos que garantizan que la tecnología de la información de una empresa respalde las estrategias y los objetivos de la organización.

Norma: un pronunciamiento profesional promulgado por el Consejo de Normas de Auditoría Interna que describe los requisitos para desempeñar una amplia gama de actividades de auditoría interna y para evaluar el desempeño de la auditoría interna.

Procesos de control: las políticas, los procedimientos (tanto manuales como automatizados) y las actividades que forman parte de un marco de control, que se hayan diseñado y operado para garantizar que los riesgos estén en el nivel que una organización esté dispuesta a aceptar.

Riesgo: la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

Riesgo asumido / apetito de riesgo: el nivel de riesgo que una organización está dispuesta a aceptar.

Servicios de aseguramiento: un examen objetivo de pruebas con el propósito de proveer una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una organización. Por ejemplo: trabajos financieros, de desempeño, de cumplimiento, de seguridad de sistemas y de diligencia debida.

Servicios de consultoría: actividades de asesoramiento y servicios relacionados proporcionadas a los clientes, cuya naturaleza y alcance estén acordados con los mismos y estén dirigidos a añadir valor y a mejorar los procesos de gobierno, gestión de riesgos y control de una organización, sin que el auditor interno asuma responsabilidades de gestión. Algunos ejemplos son la orientación, el asesoramiento, la facilitación y la formación.

Significatividad o materialidad: la importancia relativa de un asunto dentro de un contexto en el cual está siendo considerado, incluyendo factores cuantitativos y cualitativos, tales como magnitud, naturaleza, efecto, relevancia e impacto. El juicio profesional ayuda a los auditores internos cuando evalúan la significatividad de los asuntos dentro del contexto de los objetivos relevantes.

ESIS: Herramienta interna de DXC para el control de vulnerabilidades y documentación de aceptación de riesgos.

RTSP: Retailer Transaction Settlement Platform, es la aplicación web a la que el equipo de Operaciones de aplicación de DXC le da soporte, dicha aplicación también es llamada PowerCard. Esta es la aplicación a la cual se le aplico la herramienta de control creada en la presente investigación.