

**NEUMANN BUSINESS SCHOOL**  
**ESCUELA DE POSTGRADO**

**MAESTRÍA EN**  
**GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**



**“Elaboración de una propuesta de mejora de la seguridad de la información en una institución financiera basada en la norma PCI DSS. Guayas, Ecuador 2020.”**

**Trabajo de Investigación**  
**para optar el Grado a Nombre de la Nación de:**

Maestro en  
Gestión de Tecnologías de la Información

**Autores:**

Ing. Orellana Vélez, Nathaly Vanessa  
Ing. Tamayo Lamar, Josué Andrés

**Docente Guía:**

Mg. Moscoso Zegarra, Giomar Walter

**TACNA – PERÚ**  
**2020**

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del (los) autor (es)”

## **Dedicatoria**

Primero, antes que nada, dedicamos este trabajo a Dios, quien nos supo guiar al mejor camino desde el principio hasta el fin; nos dio fuerzas para seguir adelante y a no renunciar ante cualquier tipo de obstáculo que se presente en nuestro camino. A nuestra familia quien nos brindó el apoyo y aliento. Nuestros padres por sus consejos, comprensión y amor; quienes nos han sabido educar con buenos valores, carácter, principios y forjar coraje para cumplir con nuestros objetivos planteados.

## **Agradecimientos**

En primera instancia agradecemos a nuestros formadores, guías, personas que han influenciado de alguna forma en llegar al punto en que nos encontramos. También le damos las gracias a familiares, amigos y personas importantes para nosotros, no podríamos sentirnos más agradecidos por la confianza y apoyo brindado. No ha sido fácil, pero hemos logrado importantes objetivos, ahora se suma el culminar con éxito el desarrollo de la tesis y obtener otra valiosa titulación profesional. Y a nuestros tutores quienes nos han apoyado desde el principio hasta el fin para culminar con éxito nuestro trabajo.

## Índice

RESUMEN EJECUTIVO.....	9
INTRODUCCIÓN .....	10
Capítulo I Antecedentes del Estudio.....	11
1.1. Título del Tema.....	11
1.2. Planteamiento del Problema. ....	11
1.3. Objetivos.....	12
1.4. Justificación. ....	13
1.5. Metodología.....	13
1.6. Definiciones.....	14
1.7. Alcances y Limitaciones.....	16
Capítulo II Marco Teórico.....	17
2.1. Conceptualización de la(s) variable(s) o tópico(s) clave.....	17
2.2. Importancia de la(s) variable(s) o tópico(s) clave.....	22
2.3. Análisis comparativo .....	26
2.4. Análisis crítico.....	31
Capítulo III Marco Referencial.....	33
3.1. Reseña histórica.....	33
3.2. Filosofía Organizacional.....	35
3.3. Diseño organizacional.....	38
3.4. Productos y/o servicios.....	43
3.5. Diagnóstico organizacional.....	49
Capítulo IV Resultados.....	51
4.1. Diagnóstico.....	51
4.2. Diseño de la Mejora.....	60
4.2.1. Desarrollar y mantener sistemas y redes seguros .....	60
4.2.2. Proteger los datos del titular de la tarjeta.....	64
4.2.3. Mantener un programa de administración de vulnerabilidad .....	71
4.2.4. Implementar medidas sólidas de control de acceso .....	76
4.2.5. Supervisar y evaluar las redes con regularidad.....	85
4.2.6. Mantener una política de seguridad de información.....	91
4.3. Mecanismos de Control.....	100
Capítulo V Estudio Financiero .....	101
5.1 Presupuesto referencial .....	101

5.2 Entregables.....	102
5.3 Plan de Auditoría Anual .....	103
Capítulo VI Sugerencias. ....	104
Capítulo VII Conclusiones.....	108
Capítulo VIII Bibliografía. ....	110

## Índice de Tablas

Tabla 1.- Definiciones.....	16
Tabla 2.- Comparativo PCI DSS vs. ISO/IEC 27001. ....	29
Tabla 3.- Familia ISO27000. ....	30
Tabla 4.- Descripción de la estructura organizacional. ....	41
Tabla 5.- Estrategias para la reducción del alcance PCI DSS. ....	55
Tabla 6.- Forma de enmascarar el número de tarjeta. ....	56
Tabla 7.- Esquematización de numeración del PAN (Primary Account Number) (Acosta, 2013) .....	57
Tabla 8.- Información de las tarjetas de crédito/débito. (Industria de Tarjetas de Credito PCI, 2018) .....	58
Tabla 9.- Elementos de los datos del titular de tarjeta y datos de autenticación confidenciales (Industria de Tarjetas de Credito PCI, 2018) .....	58
Tabla 10.- Inventario de componentes del sistema.....	64
Tabla 11.- Datos Confidenciales de Autenticación.....	66
Tabla 12.- Tabla de justificación PAN en claro. ....	67
Tabla 13.- Ejemplo de Truncamiento.....	67
Tabla 14.- Ejemplo de Tokenización.....	68
Tabla 15.- Ejemplo de Algoritmo Hashing. ....	68
Tabla 16.- Análisis de vulnerabilidades internos vs externo. ....	89
Tabla 17.- Matriz de Responsabilidades de proveedores .....	97
Tabla 18.- Presupuesto referencial. ....	102
Tabla 19.- Listado de lo que se debe tener como mínimo para la certificación PCI DSS. ....	108

## Índice de Ilustraciones

Ilustración 1.- Pilares fundamentales de Seguridad de la Información.....	18
Ilustración 2.- Seguridad de la Información en todos sus aspectos (Imagen tomada de internet).....	20
Ilustración 3.- Canales financieros.....	22
Ilustración 4.- Ventajas que ofrece el estándar PCI DSS.....	23
Ilustración 5.- Estrategias para abordar el riesgo.....	25
Ilustración 6.- Ventajas por cumplimiento y Desventajas por incumplimiento de norma PCI DSS.....	26
Ilustración 7.- Ecosistema PCI SSC (Gimenes, 2019).....	31
Ilustración 8.- Franquicias o marcas que conforman PCI SSC.....	33
Ilustración 9.- Ciclo de vida PCI DSS (Acosta, 2016b).....	35
Ilustración 10.- Filosofía Organizacional.....	36
Ilustración 11.- Valores dentro de una institución.....	37
Ilustración 12.- Organigrama para una institución financiera.....	39
Ilustración 13.- Diseño conformado en la estructura organizacional.....	42
Ilustración 14.- Formas de documentar los procesos.....	43
Ilustración 15.- Transacción General con Tarjeta de pago.....	44
Ilustración 16.- Transacción mediante tecnología ContactLess.....	45
Ilustración 17.- Diagrama General Cajeros Automáticos.....	47
Ilustración 18.- Diagrama general del uso de una App Móvil Financiera.....	48
Ilustración 19.- Análisis F.O.D.A.....	49
Ilustración 20.- Roles y responsabilidades del cumplimiento de PCI DSS.....	52
Ilustración 21.- Organizaciones participantes en el entorno PCI SSC.....	53
Ilustración 22.- Metodología general para la auditoría.....	54
Ilustración 23.- Estructura del PAN (Primary Account Number).....	56
Ilustración 24.- Estructura de una tarjeta de crédito.....	59
Ilustración 25.- Instalar y mantener una configuración de firewalls.....	61
Ilustración 26.- Ciclo de Vida de los Datos.....	65
Ilustración 27.- Ejemplo de cifrado.....	68
Ilustración 28 Tabla de truncamientos por longitud de PAN. (Acosta, 2020). ...	70
Ilustración 29.- Tipos de malware.....	72
Ilustración 30.- Tipos de remediación.....	74
Ilustración 31.- Matriz o Bitácora de retención de Datos de Tarjetahabiente. ...	77
Ilustración 32.- MFA Multi-Factor de Autenticación. (Imagen tomada de Internet).....	79
Ilustración 33.- Gestión de contraseñas.....	80
Ilustración 34.- Registro de logs.....	85
Ilustración 35.- Alertas y eventos a registrar de las pistas de auditoría.....	86
Ilustración 36.- Protección de los logs de auditoría.....	86
Ilustración 37.- Diagrama NTP.....	87
Ilustración 38.- Programa de concientización.....	95
Ilustración 39.- Matriz de revisión de la lista de proveedores de servicio.....	97
Ilustración 40.- Documentos a solicitar a cada proveedor.....	98
Ilustración 41.- Procedimiento para el Plan de Respuesta ante Incidentes.....	99
Ilustración 42.- Plan de auditoria anual.....	104



## **RESUMEN EJECUTIVO**

En la presente documento se dará a conocer la propuesta de mejora de la seguridad de la información en una institución financiera basada en controles que indica la norma PCI DSS, se plantea un estudio de las mejores prácticas del manejo información dentro de una institución financiera, inculcando o capacitando a todas las personas que participan en el ciclo de mejora de la Seguridad de la Información, pero en esta propuesta de mejora como tema principal se va a conocer la norma PCI DSS en la cual participan personas, procesos y sistemas que almacenen, transmitan o procesar los datos de tarjetahabiente de todos los clientes de alguna institución financiera.

La propuesta de mejora tiene como fin conocer cada requisito que tiene la norma y poder aplicarlas en alguna institución, cabe mencionar que no todas las instituciones aplican todos los requisitos, esto se deberá al alcance que la institución defina y quiera certificar.

## **INTRODUCCIÓN**

El área de las tecnologías de información junto a la directiva de la institución financiera apuesta a integrar de manera radical y precisa la integración de una cultura organizacional de la seguridad de la información acorde a la transformación digital que el mundo está experimentando. La necesidad de ofrecer productos y servicios de alta calidad exige a cualquier institución financiera en invertir, recrear las tácticas y estrategias en materia de seguridad de la información.

Esta propuesta de mejora se apoya con el estudio metodológico de la investigación descriptiva y explicativa donde se enfoca que el recurso más fuerte y a la vez el más vulnerable que es, el recurso humano; los colaboradores deben ser capacitados y concientizados del rol que cumplen, el manejo de la información que tratan, el cuidado y prestigio que la institución representa en el mercado.

La seguridad de la información como cultura laboral se regirá con estándares, lineamientos y cambio cultural en seguridad, desde el más alto rango directivo, procesos internos y de colaboración compartida con las herramientas y tecnologías de la información que darán apoyo al desarrollo productivo de la empresa.