ESCUELA DE POSTGRADO NEUMANN

MAESTRÍA EN
ADMINISTRACIÓN DE NEGOCIOS

“Propuesta de mejora de la gestión de la seguridad de información en la Cooperativa de Ahorro y Crédito Fondesurco basado en el estándar ISO 27001 para el año 2020”

Trabajo de Investigación

para optar el Grado a Nombre de la Nación de:

Maestro en:
Administración de Negocios

Autores:
Ing. Zicos Riega, Kelly Beatriz
Ing. Pineda Arratia, Michael Richard

Docente Guía:
Mg. Moscoso Zegarra, Giomar Walter

TACNA – PERÚ

2020

Índice Ilustraciones

Ilustración 1. Metodología OCTAVE 31

Ilustración 2. Metodología MEHARI. 32

Ilustración 3. Metodología MAGERIT. 33

Ilustración 4. Metodología CRAMM. 34

Ilustración 5. Costo Propuesta 40

Ilustración 6. Costo con Certificación. 40

Ilustración 7. Organigrama 44

Ilustración 8. Diagnóstico del Estado de Controles Seguridad en Coop. Fondesurco. 56

Ilustración 9. Análisis del Diagnóstico de Controles de Seguridad. 59

Ilustración 10. Cuestionario. 70

Ilustración 11. Cuestionario. 71

Ilustración 12. Acuerdo de Confidencialidad 72

Ilustración 13. Acuerdo de Confidencialidad 73

Ilustración 14. Acuerdo de Confidencialidad 74

Ilustración 15. Entregables. 75

Índice de Tablas

Tabla 1. Ventajas y Desventajas de la Norma ISO 27001 36

Tabla 2. Resumen del Resultado del Diagnóstico de Controles. 60

Tabla 3. Controles. 62

Índice

Índice Ilustraciones 3

Índice de Tablas 3

Capítulo I: Antecedentes del Estudio 9

1.1. Planteamiento del Problema. 9

1.2. Formulación del problema. 9

1.3. Objetivos. 10

1.3.1. General. 10

1.3.2. Específicas. 10

1.4. Justificación. 11

1.5. Metodología. 11

1.6. Definiciones. 12

1.7. Alcances y Limitaciones. 12

1.7.1. Alcance. 12

1.7.2. Limitaciones. 12

Capítulo II: Marco Teórico 14

2.1. Conceptualización de los tópicos clave. 14

2.1.1. Gestión de la Seguridad de Información. 14

2.1.2. Estándar para la seguridad. 14

2.1.3. ISO/IEC 27001:2013. 15

2.1.4. Servicios Financieros. 16

2.1.4.1. Transacciones bancarias. 16

2.1.4.2. Cuentas bancarias. 16

2.1.4.3. Préstamos o créditos y seguros. 17

2.1.4.4. Depósito a plazo fijo. 18

2.1.5. Estructura de la norma ISO-27001. 18

2.1.5.1. Cláusulas. 18

2.1.5.2. Categorías de control. 18

2.1.6. Gestión de activos. 19

2.1.6.1. Manejo de Medios. 19

2.1.7. Control de accesos. 22

2.1.7.1. Gestión de accesos a usuarios. 23

2.1.8. Seguridad física y ambiental. 24

2.1.8.1. Mantenimiento de equipos. 24

2.1.8.2. Equipos de usuarios sin vigilancia. 24

2.1.8.3. Política de escritorio despejado y pantalla despejada. 25

2.1.9. Seguridad de las operaciones. 25

2.1.9.1. Registro y monitoreo. 25

2.1.9.2. Gestión de vulnerabilidades técnicas. 26

2.1.10. Seguridad en las comunicaciones. 27

2.1.10.1. Gestión de la seguridad de redes. 27

2.1.10.2. Transferencia de información. 28

2.1.11. Gestión de incidentes de seguridad de la información. 30

2.1.11.1. Gestión de incidentes y mejoras de seguridad en la información. 30

2.1.12. Metodologías para el análisis del riesgo. 30

2.1.12.1. OCTAVE. 30

2.1.12.2. MEHARI. 32

2.1.12.3. MAGERIT. 32

2.1.12.4. NIST. 33

2.1.12.5. CRAMM. 33

2.1.12.6. ISM3. 34

2.2. Importancia de los tópicos clave. 35

2.2.1. Gestión de la Seguridad de Información. 35

2.2.2. Principios de la Seguridad de la Información. 35

2.3. Análisis comparativo. 36

2.4. Análisis crítico. 37

2.4.1. ISO/IEC 27001, ¿Es suficiente? 38

2.5. Análisis Costo – Beneficio. 39

2.5.1. Costo de la Propuesta. 39

2.1.1. Costo con Certificación 40

2.1.2. Beneficio. 41

Capítulo III: Marco Referencial 42

3.1. Reseña histórica de la organización. 42

3.2. Filosofía organizacional. 42

3.2.1. Misión. 42

3.2.2. Visión. 43

3.2.3. Valores. 43

3.3. Diseño organizacional. 44

3.3.1. Organigrama Institucional. 44

3.3.2. Descripción de las Funciones de las Áreas. 45

3.4. Productos y/o servicios. 49

3.5. Diagnóstico organizacional. 49

Capítulo IV: Resultados 54

4.1. Diagnóstico. 54

4.1.1. Diagnóstico de controles de seguridad en Coop. Fondesurco. 54

4.1.2. Análisis del Diagnóstico De Controles De Seguridad. 57

4.1.3. Resumen del Diagnóstico de Controles. 60

4.2. Diseño de la Mejora. 60

4.2.1. Controles No implementados. 60

4.3. Mecanismos de Control. 61

Capítulo V: Sugerencias y Conclusiones 63

5.1. Sugerencias. 63

5.2. Conclusiones. 64

Capítulo VI: Bibliografía 66

Capítulo VII: Anexos 70

7.1 Cuestionario. 70

7.2 Acuerdo de Confidencialidad. 72

7.3 Entrega de Documentación. 75

7.4 Anexos Mecanismos de Control. 76

7.4.1 AnexoA-PL-N8-SN03-ME. 76

7.4.2 AnexoA1. 77

7.4.3 AnexoA2. 88

7.4.4 AnexoB-PL-N8-SN03-EM. 88

7.4.5 AnexoC-PL-N8-SN03-TM. 90

7.4.6 AnexoD-PL-N9-SN02-AP. 91

7.4.7 AnexoD1. 92

7.4.8 AnexoE-PL-N9-SN03-IAS. 98

7.4.9 AnexoE1. 100

7.4.10 AnexoF-PL-N9-SN03-RAI. 105

7.4.11 AnexoF1. 106

7.4.12 AnexoG-PL-N11-SN02-ME. 111

7.4.13 AnexoG1. 112

7.4.14 AnexoH-PL-N11-SN02-EUSV. 120

7.4.15 AnexoI-PL-N12-SN04-RAO. 121

7.4.16 AnexoI1. 122

7.4.17 AnexoJ-PL-N12-SN06-GVT. 127

7.4.18 AnexoJ1. 130

7.4.19 AnexoK-PL-N13-SN01-CR. 135

7.4.20 AnexoK1. 136

7.4.21 AnexoL-PL-N13-SN02-PSTI. 141

7.4.22 AnexoL1. 143

7.4.23 AnexoM-PL-N13-SN02-ME. 150

7.4.24 AnexoN-PL-N16-SN01-EDESI. 151

7.4.25 AnexoN1. 153

7.4.26 AnexoN2. 164

7.4.27 AnexoO-PL-N16-SN01-AISI. 165