UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN.

TEMA:

"PLAN DE CONTINGENCIA PARA LA COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS CHUCHUQUI LTDA., BASADO EN LA NORMA ISO/IEC 27002"

AUTOR: DONY ANDERSON REINA LÓPEZ

DIRECTOR: MSC. JAIME MICHILENA

IBARRA – ECUADOR

2017

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoya los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

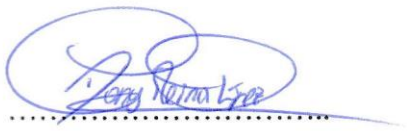
DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD:	040166573-2
APELLIDOS Y NOMBRES:	REINA LÓPEZ DONY ANDERSON
DIRECCIÓN:	IBARRA, AV. LOS GALEANOS (CONJUNTO SAN JORGE I)
E-MAIL:	dareinal1@utn.edu.ec
TELÉFONO FIJO	06-2607925
TELÉFONO MÓVIL:	0980342368
DATOS DE LA OBRA	
TÍTULO:	"PLAN DE CONTINGENCIA PARA LA COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS CHUCHUQUI LTDA., BASADO EN LA NORMA ISO/IEC 27002"
AUTOR:	REINA LÓPEZ DONY ANDERSON
FECHA:	
PROGRAMA:	PREGRADO
TÍTULO POR EL QUE OPTA	INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
DIRECTOR:	MSC. JAIME MICHILENA

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Dony Anderson Reina López, con cédula de identidad No 040166573-2, en calidad de autor y titular de los Derechos Patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad, con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior, Artículo 144.

3. CONCORDANCIA

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los Derechos Patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en la defensa de la Universidad en caso de reclamación por parte de terceros.



Firma

Nombre: Dony Anderson Reina López

Cédula: 040166573-2

Ibarra,

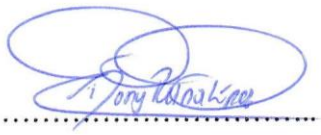
UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Dony Anderson Reina López, con cédula de identidad No 040166573-2, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los Derechos Patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4,5 y 6 en calidad de autor de la obra o trabajo de grado denominado: **"PLAN DE CONTINGENCIA PARA LA COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS CHUCHUQUI LTDA., BASADO EN LA NORMA ISO/IEC 27002"** que ha sido desarrollado para optar por el título de: INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN, en la UNIVERSIDAD TÉCNICA DEL NORTE, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi calidad de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago la entrega del trabajo final en el formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.



.....

Firma

Nombre: Dony Anderson Reina López

Cédula: 040166573-2

Ibarra,

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

MAGISTER JAIME MICHILENA, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN CERTIFICA:

En calidad de Director del presente proyecto de Titulación, Certifico que "PLAN DE CONTINGENCIA PARA LA COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS CHUCHUQUI LTDA., BASADO EN LA NORMA ISO/IEC 27002." Ha sido desarrollado por el señor Dony Anderson Reina López bajo mi supervisión.

Es todo en cuanto puedo certificar en honor de la verdad.

Msc. Jaime Michilena

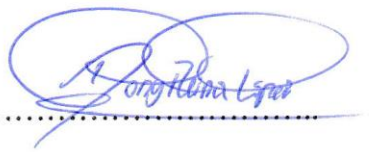
DIRECTOR DE TRABAJO DE GRADO

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, DONY ANDERSON REINA LÓPEZ, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado ni calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.



.....

Firma

Nombre: Dony Anderson Reina López

Cédula: 040166573-2

Ibarra,

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

Dedico este proyecto de titulación a mis padres que con su ejemplo de lucha no me dejaron rendir aun cuando mis fuerzas empezaban a flaquear y constantemente me motivaban para salir adelante, su invaluable apoyo me dio esperanza y me dieron todo lo necesario para ser la persona que hoy soy, algo que siempre marcará mi camino será el gran amor que me demostraron día a día.

A mi hijo, que se encuentra en camino, el regalo más grande que Dios me ha dado, que al acercarse su venida me ayuda a comprender que se debe disfrutar el presente y que cada momento de calidad con la familia es importante y que todo toma sentido cuando se vive con un propósito y con alegría en el corazón, que cuando las cosas se hacen con amor todo sale bien, y que todo es bueno cuando se tiene a Dios y una familia unida.

Dony Anderson Reina López

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco a Dios por el amor que me brinda en cada paso que doy, su infinita misericordia, y su presencia que ha permitido que los problemas se transformen en bendiciones y que lo que parece imposible se haga real en mi vida, por las incomparables obras que ha hecho en mi familia y por ser el sentido de mi vida cuando pierdo de vista los objetivos que me quedan por delante.

Agradezco a mis padres, mis hermanos y mi esposa quienes incansablemente han estado a mi lado en los buenos y malos momentos, dando de su amor que me impulsa a salir adelante y que me ha motivado a ser cada día mejor, a su grandiosa forma de ser y su apoyo a pesar de mis errores.

Don Anderson Reina López

Tabla de contenido

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE II

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE IV

CERTIFICACIÓN V

DECLARACIÓN VI

DEDICATORIA VII

AGRADECIMIENTO VIII

RESUMEN XXVII

ABSTRACT XXVIII

CAPÍTULO I 1

ASPECTOS GENERALES 1

1.1. TEMA O TÍTULO 1

1.2. PROBLEMA 1

1.3. OBJETIVOS 2

1.3.1. Objetivo general 2

1.3.2. Objetivos específicos 2

1.4. ALCANCE 3

1.5. JUSTIFICACIÓN 5

CAPÍTULO II 6

FUNDAMENTO TEÓRICO 6

2.1. Seguridad de la información. 6

2.1.1. Seguridad activa y pasiva. 7

2.1.1.1. Seguridad activa. 7

2.1.1.2. Seguridad pasiva. 7

2.1.2. Seguridad física y lógica. 7

2.1.2.1. Seguridad física. 7

2.1.2.2. Seguridad lógica. 7

2.1.3. Principios de la seguridad. 8

2.1.3.1. Confidencialidad. 8

2.1.3.2. Integridad. 8

2.1.3.3. Disponibilidad. 8

2.1.4. Riesgos en la seguridad de la información 9

2.2. REGLAMENTO A LA LEY ORGÁNICA DE LA ECONOMÍA POPULAR Y SOLIDARIA....9
2.3. ANÁLISIS DE LA NORMA TÉCNICA ISO/IEC 27002....11
2.3.1. Estructura....11
2.3.2. Dominios....11
2.3.3. Categorías principales de seguridad de la información....12
2.3.4. Políticas de seguridad....13
2.3.5. Aspectos organizativos de la seguridad de la información....15
2.3.6. Seguridad ligada a los recursos humanos....15
2.3.7. Gestión de activos....16
2.3.8. Control de accesos....17
2.3.9. Cifrado....18
2.3.10. Seguridad física y ambiental....18
2.3.11. Seguridad en la operativa....18
2.3.12. Seguridad en las telecomunicaciones....19
2.3.13. Adquisición, desarrollo y mantenimiento de los sistemas de información....19
2.3.14. Relaciones con suministradores....20
2.3.15. Gestión de incidentes....20
2.3.16. Aspectos de la seguridad de la información en gestión de la continuidad del negocio....21
2.3.17. Cumplimiento....21
2.4. ANÁLISIS DE LA NORMA TÉCNICA NTC/ISO 27005:2005....22
2.4.1. Estructura....22
2.4.2. Información general....23
2.4.3. Proceso de gestión del riesgo....24
2.5. ITIL V3....26
2.5.1. Descripción general de ITIL....26
2.6. COBIT....27
2.6.1. Descripción....27
2.6.2. Marco COBIT 5....29
CAPÍTULO III....30
ANÁLISIS DE LA SITUACIÓN ACTUAL....30
3.1. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL....30
3.1.1. Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda....31

3.1.2. Servicios prestados por la COAC Chuchuqui Ltda. 32
SERVICIOS PRESTADOS POR LA COAC CHUCHUQUI LTDA. 32
3.1.3. Servicios consumidos por la COAC Chuchuqui Ltda. 32
3.1.4. Activos de Información. 33
3.1.5. Red de datos. 34
3.1.6. Cuarto de Telecomunicaciones. 36
3.1.7. Servicios del Departamento de Tecnología. 38
3.1.8. Controles de seguridad. 39
3.1.9. Estructura organizativa de la COAC Chuchuqui Ltda. 40
CAPÍTULO IV 43
DESARROLLO DEL PLAN DE CONTINGENCIA 43
PLAN DE CONTINGENCIA Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN 44
4.1. PROPÓSITO 44
4.2. INTRODUCCION 45
4.3. METODOLOGÍA 45
4.4. CONCEPTOS PRELIMINARES 46
4.5. ESTRUCTURA 48
4.6. ELEMENTOS INDISPENSABLES EN UN PLAN. 49
4.7. ANÁLISIS DE RIESGOS 50
4.7.1. Identificación del riesgo. 50
4.7.1.1. Identificación de los Activos. 51
4.7.1.2. Identificación de Amenazas. 52
4.7.1.3. Identificación de los controles existentes. 52
4.7.1.4. Identificación de las vulnerabilidades. 53
4.7.1.5. Identificación de los impactos. 54
4.7.2. Estimación del riesgo. 56
4.7.3. Análisis FODA. 60
4.7.3.1. Resultado de Análisis FODA. 63
4.8. TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN 65
4.9. PLAN DE EMERGENCIA 66
4.9.1. Objetivo. 66
4.9.2. Escenarios de incidentes. 66

4.9.2.1. Estimación de los escenarios. 66
4.9.2.2. Características de los escenarios de incidentes de emergencia. 67
4.9.3. Organización institucional de respuesta. 68
4.10. PLAN DE RESTAURACIÓN 72
4.10.1. Objetivo. 73
4.10.2. Estructura. 73
4.10.2.1. Recepción y registro. 73
4.10.2.2. Comparación. 74
4.10.2.3. Clasificación. 74
4.10.2.4. Resolución. 75
4.10.2.5. Seguimiento. 75
4.10.2.6. Cierre. 76
4.10.3. Tiempos de restauración. 76
4.10.4. Escenario 1: no hay comunicación entre cliente-servidor. 77
4.10.5. Escenario 2: falla de un servidor. 79
4.10.6. Escenario 3: ausencia parcial o permanente del personal técnico informático. 84
4.10.7. Escenario 4: interrupción del fluido eléctrico durante la ejecución de los procesos. 87
4.10.8. Escenario 5: corte del servicio de internet. 89
4.10.9. Escenario 6: error humano en la operación (sistema financiero). 91
4.11. PLAN DE RECUPERACIÓN 93
4.11.1. Objetivo. 93
4.11.2. Escenario: indisponibilidad del centro de cómputo (destruccion del sitio de servidores). 93
4.12. PRUEBAS DE VERIFICACIÓN Y EVALUACIÓN 98
4.12.1. Objetivo. 98
4.12.2. Plan de Verificación. 98
4.12.3. Procedimientos para las Pruebas del Plan de Contingencia. 99
4.12.4. Preparaciones PRE Prueba. 100
4.12.5. Alcance del Entrenamiento. 102
4.12.6. Revisión y Actualización. 102
4.13. PLAN DE MANTENIMIENTO 108
4.14. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN 109
4.14.1. Gestión de incidentes en la seguridad de la información y mejoras. 109

4.14.1.1. Responsabilidad y Procedimientos. 109
4.14.1.2. Notificación de los eventos de la seguridad de la información. 110
4.14.1.3. Notificación de los puntos débiles de la seguridad. 111
4.14.1.4. Valoración de los eventos de seguridad de la información y toma de decisiones. 111
4.14.1.5. Respuesta a los incidentes de seguridad. 112
4.14.1.6. Aprendizaje de los incidentes de seguridad y recopilación de evidencias. 113
4.15. POLÍTICAS DE SEGURIDAD. 113
4.15.1. Directrices de la dirección en seguridad de la información 113
4.15.1.1. Conjunto de políticas para la seguridad de la información. 114
4.15.1.2. Revisión de la política para la seguridad de la información. 115
4.16. ASPECTOS ORGANIZATIVOS DE SEGURIDAD DE LA INFORMACIÓN. ..116
4.16.1. Organización Interna. 116
Nivel Directivo 116
4.16.1.1. Asignación de Responsabilidades para la SI y segregación de roles. 117
4.16.1.2. Contacto con las Autoridades. 119
4.16.1.3. Contacto con grupos de interés especial. 120
4.16.2. Dispositivos para movilidad y teletrabajo. 121
4.16.2.1. Política de uso de dispositivos para movilidad. 121
4.16.2.2. Teletrabajo. 122
4.17. SEGURIDAD LIGADA A RECURSOS HUMANOS. 122
4.17.1. Antes de la contratación. 122
4.17.1.1. Investigación de Antecedentes. 123
4.17.1.2. Términos y condiciones de contratación. 124
4.17.2. Durante la contratación 125
4.17.2.1. Responsabilidades de Gestión. 126
4.17.2.2. Concienciación, educación y capacitación en SI. 127
4.17.2.3. Proceso Disciplinario. 127
4.17.3. Cese o cambio de puesto de trabajo 128
4.17.3.1. Cese o cambio de puesto de trabajo. 128
4.18. GESTIÓN DE ACTIVOS 129
4.18.1. Responsabilidad Sobre Los Activos 129
4.18.1.1. Inventario de Activos. 130
4.18.1.2. Uso Aceptable de los Activos. 131

4.18.1.3. Devolución de Activos. 132
4.18.2. Clasificación de la Información 133
4.18.2.1. Directrices de Clasificación 133
4.18.2.2. Etiquetado y Manipulado de la Información. 134
4.18.3. Manejo de los Soportes de Almacenamiento 135
4.18.3.1. Gestión de soportes extraíbles. 135
4.18.3.2. Eliminación de soportes. 136
4.19. CONTROL DE ACCESOS. 137
4.19.1. Requisitos de Negocio para el control de Accesos 137
4.19.1.1. Política de control de accesos. 138
4.19.1.2. Control de accesos a redes y servicios asociados. 139
4.19.2. Gestión de Acceso de Usuario 140
4.19.2.1. Gestión de Acceso de Usuario. 140
4.19.3. Responsabilidades de Usuario 141
4.19.3.1. Uso de información confidencial para autenticación. 142
4.19.4. Control de Acceso a Sistemas y Aplicaciones 143
4.19.4.1. Restricción de Acceso a la información. 144
4.19.4.2. Procedimientos seguros de inicio de sesión. 145
4.19.4.3. Gestión de contraseñas de usuario. 147
4.20. CIFRADO 148
4.20.1. Controles Criptográficos 148
4.20.1.1. Política de uso de gestión de claves. 148
4.21. SEGURIDAD FÍSICA Y AMBIENTAL. 150
4.21.1. Áreas Seguras 150
4.21.1.1. Perímetro de seguridad física. 150
4.21.1.2. Controles físicos de entrada. 151
4.21.1.3. Seguridad de oficinas, despachos y recursos. 152
4.21.1.4. Protección contra amenazas externas y ambientales. 153
4.21.2. Seguridad de los Equipos 154
4.21.2.1. Emplazamiento y protección de equipos. 154
4.21.2.2. Instalaciones de suministro. 155
4.21.2.3. Seguridad del cableado. 157
4.21.2.4. Mantenimiento de los equipos. 158

4.21.2.5. Reutilización o retirada segura de dispositivos de almacenamiento. 159
4.21.2.6. Equipo informático de uso desatendido. 159
4.21.2.7. Política de puesto de trabajo despejado y bloqueo de pantalla. 160
4.22. SEGURIDAD EN LA OPERATIVA. 161
4.22.1. Responsabilidades y procedimientos de operación. 161
4.22.1.1. Documentación de procedimientos de operación. 161
4.22.1.2. Gestión de cambios. 163
4.22.1.3. Gestión de capacidades. 164
4.22.2. Protección Contra Código Malicioso 164
4.22.2.1. Controles contra el código malicioso. 165
4.22.3. Copias de Seguridad 166
4.22.3.1. Copias de seguridad de la información. 167
4.22.4. Registro de Actividad y Supervisión 168
4.22.4.1. Registro y gestión de eventos de actividad. 169
4.22.4.2. Protección de los registros de información. 170
4.22.4.3. Sincronización de relojes. 170
4.22.5. Gestión de la vulnerabilidad técnica 171
4.22.5.1. Gestión de las vulnerabilidades técnicas. 171
4.22.5.2. Restricciones de la instalación de software. 172
4.23. SEGURIDAD EN LAS TELECOMUNICACIONES. 173
4.23.1. Gestión de la Seguridad en las redes. 173
4.23.1.1. Controles de red. 173
4.23.1.2. Mecanismos de seguridad asociados a servicios en red. 174
4.24. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. 175
4.24.1. Requisitos de Seguridad de los Sistemas de Información 175
4.24.1.1. Análisis y especificación de los requisitos de seguridad. 175
4.24.2. Seguridad en los Procesos de Soporte 176
4.24.2.1. Procedimientos de control de cambios en los sistemas. 177
4.24.2.2. Control a los cambios en los paquetes de software. 178
4.25. RELACIÓN CON SUMINISTRADORES 179
4.25.1. Seguridad de la información en las relaciones con suministradores 179
4.25.1.1. Tratamiento del riesgo dentro de acuerdos de suministradores. 179
4.25.2. Gestión de la prestación de servicio por suministradores. 181

4.25.2.1. Supervisión y revisión de los servicios prestados por terceros. 181

4.26. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 182

4.26.1. Continuidad de la seguridad de la información. 182

4.26.1.1. Planificación de la continuidad de la seguridad de la información. 183

4.26.1.2. Implantación de la continuidad de la seguridad de la información. 183

4.26.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 184

4.27. CUMPLIMIENTO 185

4.27.1. Cumplimiento de los requisitos legales y contractuales. 185

4.27.1.1. Identificación de la legislación aplicable. 185

4.27.1.2. Protección de datos y privacidad de la información personal. 186

4.27.1.3. Regulación de los controles criptográficos. 187

4.27.2. Revisiones de la seguridad de la información 187

4.27.2.1. Cumplimiento de las políticas y normas de seguridad. 188

4.27.2.2. Comprobación del cumplimiento. 188

4.28. TIEMPOS PARA REVISIONES Y MEJORAS 188

CAPÍTULO V 190

IMPLEMENTACIÓN Y PRUEBAS 190

5.1. SISTEMAS DE MONITOREO 190

5.1.1. Selección del mejor sistema de monitoreo. 190

5.1.2. Implementación de sistema de monitoreo NAGIOS 192

5.2. CONTROL DE PUERTOS ABIERTOS 196

5.2.1. Cambio de número de puerto SSH. 201

5.2.1.1. Configuración SSH en los servidores. 202

5.2.1.2. Configuración de nuevos puertos en Firewall. 206

5.3. CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y POLÍTICAS DE SEGURIDAD. 209

5.4. IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN EL DATA CENTER 211

5.5. RESUMEN DE IMPLEMENTACIÓN 219

CAPÍTULO VI 223

COSTO BENEFICIO 223

6.1. COTIZACIÓN DE MATERIALES Y MANO DE OBRA 223

6.2. COSTOS DE MATERIALES A UTILIZAR EN LA IMPLEMENTACIÓN DE

LOS CONTROLES DE SEGURIDAD EN BASE A LAS COTIZACIONES. 223
6.3. ANÁLISIS ECONÓMICO 225
6.4. ANÁLISIS DE FACTIBILIDAD ECONÓMICA 232
CONCLUSIONES 233
RECOMENDACIONES 234
REFERENCIAS BIBLIOGRÁFICAS 236
GLOSARIO 238
ANEXOS 240
ANEXO A: FORMATO PARA LEVANTAMIENTO DE INFORMACIÓN DE CONTROLES DE SEGURIDAD 240
ANEXO B: LEVANTAMIENTO DE INFORMACIÓN DE CONTROLES DE SEGURIDAD 241
ANEXO C: TIPOS DE AMENAZAS 246
ANEXO D: TIPOS DE VULNERABILIDADES 248
ANEXO E: LISTA DE TELÉFONOS DE EMERGENCIA 250
ANEXO F: FORMATO DE RECEPCIÓN Y REGISTRO DE INCIDENCIA 250
ANEXO G: FORMATO PARA PRUEBAS Y EVALUACIÓN 252
ANEXO H: DOCUMENTACIÓN DE PRUEBAS Y EVALUACIÓN 254
ANEXO I: POLÍTICAS, REGLAMENTOS Y MANUALES INTERNOS 264
ANEXO J: FORMATO PARA GESTIÓN DE CAMBIOS 267
ANEXO K: CONFIGURACIÓN DE NAGIOS 268
ANEXO L: MANUAL DE USUARIO NAGIOS 270
Interfaz Gráfica NAGIOS 271
Reportes NAGIOS 276
PNP4NAGIOS 280
ANEXO M: MANUAL DE ADMINISTRADOR NAGIOS 283
Personalización de NAGIOS 283
Archivos de configuración 286
Plugins NRPE 291
Ficheros de configuración PNP4NAGIOS 291
ANEXO N: COTIZACIONES Y FACTURAS 294
ANEXO O: CERTIFICADO DE PRESUPUESTO ECONÓMICO 299
ANEXO P: REGISTRO DE ASISTENCIA DE CAPACITACIÓN 300
ANEXO Q: CARTA DE ACEPTACIÓN PARA LA REALIZACIÓN DEL TRABAJO DE GRADO 302

ANEXO R: ACTA DE APROBACIÓN DEL PLAN DE CONTINGENCIA.....303

ANEXO S: CARTA DE FINALIZACIÓN DEL TRABAJO DE GRADO.....307

ANEXO T: RESUMEN DE IMPLEMENTACIÓN AVALADO POR LA COAC CHUCHUQUI LTDA.....308

ANEXO U: CERTIFICADOS DE REUNIONES.....311

ÍNDICE DE FIGURAS

Figura 1: Estructura legal de los organismos de control 10

Figura 2: Proceso de gestión del riesgo en la seguridad de la información 25

Figura 3: Áreas de enfoque de COBIT..... 28

Figura 4: Equipos de conexión intermedia sin protección. 34

Figura 5: Topología de red de la COAC Chuchuqui Ltda. 35

Figura 6: Puerta de Acceso al Data Center..... 36

Figura 7: Ventana en el interior del Data Center de la COAC Chuchuqui Ltda. 37

Figura 8: Fuente de alimentación para equipos en el Data Center de la COAC Chuchuqui Ltda. 37

Figura 9: Organigrama Estructural..... 41

Figura 10: Organigrama Funcional 42

Figura 11: Etapas del Plan de Contingencia..... 48

Figura 12: Riesgo a los cuales se encuentran inmersos los Sistemas de Información 51

Figura 13: Resumen norma ISO/IEC 27002:2013 62

Figura 14. Comité Institucional de Emergencia..... 68

Figura 15: Procedimiento de Gestión de Incidencias..... 73

Figura 16: Categorización de incidencias. 75

Figura 17: Procedimiento de pruebas del plan de contingencia. 101

Figura 18: Servidores de la COAC Chuchuqui bajo monitoreo de NAGIOS. 194

Figura 19: Gráfica pnp4 en NAGIOS del servicio de CPU Load para el servidor Centos Antiguo 195

Figura 20: Selección de varios servicios con la aplicación My basket de pnp4 en NAGIOS 195

Figura 21: Notificaciones de Nagios mediante mensajes de correo electrónico 196

Figura 22: Comando para escaneo de puertos en una red con el software de Kali Linux..... 197

Figura 23: Comando para escaneo de puertos abiertos en la red mediante nmap en Kali Linux 197

Figura 24: Escaneo de puertos abiertos con la interfaz de zenmap. 198

Figura 25: Ventana de acceso remoto SSH mediante el puerto por defecto (22) en Putty. 202

Figura 26: Verificación de inicio de sesión remota ssh mediante el puerto por defecto (22). 203

Figura 27: Comando para la modificación del archivo de configuración del servicio sshd..... 203

Figura 28: Asignación de un nuevo número de puerto para el servicio ssh. 203

Figura 29: Modificación del fichero /etc/services 204

Figura 30: Adición del nuevo número de puerto para el protocolo ssh..... 204

Figura 31: Reinicio del servicio sshd 204

Figura 32: Verificación de bloque del ingreso por el puerto 22 205

Figura 33: Mensaje de error de conexión en el puerto 22 205

Figura 34: Verificación de conexión mediante el nuevo número de puerto asignado 205

Figura 35: Conexión satisfactoria mediante el nuevo número de puerto asignado 206

Figura 36: Ventana de ingreso a la interfaz Zentyal 206

Figura 37: Pestaña de servicios de Zentyal 206

Figura 38: Servicio Secure Shell (SSH) en Zentyal 207

Figura 39: Botón de configuración de Secure Shell 207

Figura 40: Botón para añadir un nuevo puerto para Secure Shell 207

Figura 41: Configuración del nuevo puerto de Secure Shell..... 208

Figura 42: Botón para guardar cambios realizados en Zentyal. 208

Figura 43: Presentación ante el personal de la COAC Chuchuqui Ltda., para dar inicio a la capacitación. 211

Figura 44: Cierre de la capacitación mediante la experiencia del personal de la COAC Chuchuqui. 211

Figura 45: Lectora de huella digital para control de acceso en el Data Center de la COAC Chuchuqui Ltda. 213

Figura 46: Puerta de seguridad del Data Center de la COAC Chuchuqui Ltda. 213

Figura 47: Sistema de aire acondicionado (correspondiente a la parte interior del Data Center). 214

Figura 48: Sistema de aire acondicionado (correspondiente a la parte exterior del Data Center). 215

Figura 49: Detector de humo en el interior del Data Center 216

Figura 50: Extintor implementado en el exterior del Data Center de la COAC Chuchuqui Ltda. 216

Figura 51: Señalética ubicada en las gradas que hacienden a la tercera planta alta de la COAC Chuchuqui Ltda. 217

Figura 52: Señalética y extintor correspondientes a la tercera planta alta de la COAC Chuchuqui Ltda. 217

Figura 53: Señalética correspondiente a la salida de la tercera planta alta de la COAC Chuchuqui Ltda. 218

Figura 54: Señalética y extintor correspondientes a las escaleras que hacienden a la segunda planta alta de la COAC Chuchuqui Ltda. 218

Figura 55: Señalética correspondiente a las rutas de evacuación de la tercera planta alta de la COAC Chuchuqui Ltda. 218

Figura 56: Defensa del Plan de Contingencia ante Consejo Directivo de la COAC Chuchuqui Ltda. 222

Figura 57: Salida de ejemplo de la verificación de instalación Nagios 270

Figura 58: Dominio para el acceso a la interfaz web NAGIOS 271

Figura 59: Ventana de Autenticación de acceso de la Interfaz Web de NAGIOS. 271

Figura 60: Página de inicio de la Interfaz web de NAGIOS. 272

Figura 61: Barra de menú de NAGIOS 272

Figura 62: Listado de host monitoreados por NAGIOS 273

Figura 63: Listado de los Servicios monitoreados para Host CentosAntiguo 273

Figura 64: Información del servicio de Memoria RAM 274

Figura 65: Listado de Servicios monitoreados de Host Zentyal 274

Figura 66: Listado de Servicios monitoreados para Host Localhost 274

Figura 67: Listado de servicios monitoreados para Host Windowsserver 275

Figura 68: Listado de los Servicios de todos los Hosts. 275

Figura 69: Cantidad total de servicios por cada estado. 276

Figura 70: Listado Total de Servicios en Status OK 276

Figura 71: Step 1 de Reportes (Selección de tipo de reporte) 277
Figura 72: Step 2 de reportes (Selección de Host) 277
Figura 73: Step 2 de reportes (selección de servicio) 278
Figura 74: Step 3 de reportes (Selección de opciones de reporte) 278
Figura 75: Reporte de Alertas de estado de los servicios (clasificadas según el tiempo) 279
Figura 76: Reporte de Eventos 280
Figura 77: Acciones de PNP4NAGIOS 281
Figura 78: Rango de Tiempos habituales de PNP4NAGIOS 282
Figura 79: Iconos adicionales para las gráficas de PNP4NAGIOS 282
Figura 80: Fichero contacts.cfg de NAGIOS 283
Figura 81: Comprobación de instalación de NAGIOS 285
Figura 82: Reinicio del servicio Nagios 285
Figura 83: Interfaz Web NAGIOS 286
Figura 84: Archivos de configuración de NAGIOS 286
Figura 85: Archivo de configuración hosts.cfg 287
Figura 86: Archivo de configuración services.cfg 287
Figura 87: Archivo de configuración nagios.cfg 288
Figura 88: Archivo de configuración nrpe.cfg 289
Figura 89: Archivos de configuración de objects de NAGIOS 289
Figura 90: Archivo de configuración commands.cfg 290
Figura 91: Archivo de configuración contacts.cfg 290
Figura 92: Plugins NRPE 291

ÍNDICE DE TABLAS

Tabla 1. Servicios prestados por la COAC Chuchuqui Ltda. 32

Tabla 2. Servicios consumidos por la COAC Chuchuqui Ltda. 33

Tabla 3. Redes de comunicación de la COAC Chuchuqui. 34

Tabla 4. Personal del Departamento de Tecnología de la COAC Chuchuqui Ltda. 38

Tabla 5: Sub-planes de Contingencia 49

Tabla 6. Tabla de escenarios de incidentes con sus respectivas causas e impactos. 55

Tabla 7. Tipos de Impactos de los Riesgos 58

Tabla 8. Tipos de Frecuencia de ocurrencia de una amenaza. 59

Tabla 9. Estimación del riesgo según análisis MAGERIT. 59

Tabla 10. Descripción y valoración de estimación de riesgos 60

Tabla 11. Resultado Análisis FODA 63

Tabla 12. Ejemplos de riesgos de emergencia 67

Tabla 13. Características de los escenarios de incidentes de emergencia 67

Tabla 14. Clasificación de tiempos de restauración 76

Tabla 15. Descripción de Impacto y servicios afectados en escenario 1. 77

Tabla 16. Nivel de Prioridad y tiempos aceptables de caída para el escenario 10.3. 78

Tabla 17. Causas y procedimiento para el escenario 1 79

Tabla 18. Descripción de Impacto y servicios afectados en escenario 2. 79

Tabla 19. Nivel de prioridad y tiempos aceptables de caída para el escenario 2 80

Tabla 20. Impactos y servicios afectados en escenario 3 85

Tabla 21. Nivel de prioridad y tiempos aceptables de caída para el escenario 3 86

Tabla 22. Impactos y servicios afectados en escenario 4 87

Tabla 23. Nivel de prioridad y tiempos aceptables de caída para el escenario 4 88

Tabla 24. Impactos y servicios afectados en escenario 5 89

Tabla 25. Nivel de prioridad y tiempos aceptables de caída para el escenario 5 90

Tabla 26. Impactos y servicios afectados en escenario 6 91

Tabla 27. Nivel de prioridad y tiempos aceptables de caída para el escenario 6 92

Tabla 28. Impactos y servicios afectados en escenario 6 94

Tabla 29. Recursos de contingencia Específicos..... 96

Tabla 30. Resumen de pruebas de verificación del plan de contingencia ejecutadas. 103

Tabla 31. Asignación de roles y responsabilidades..... 118

Tabla 32. Contactos de autoridades..... 120

Tabla 33: Contactos de grupos de interés especial. 120

Tabla 34. Tiempos para revisiones o mejoras del Plan de Contingencia. 189

Tabla 35. Tabla comparativa de las principales características de los sistemas de monitorización. 191

Tabla 36: Puertos abiertos en la red de la COAC Chuchuqui. 199

Tabla 37: de Asignación de números de puerto SSH para servidores del Data Center de la Cooperativa Chuchuqui Ltda. 209

Tabla 38: Materiales a utilizar en la implementación de controles de seguridad. 224

Tabla 39: Costo de mano de obra. 225

Tabla 40: Cálculo del valor de talento humano dependiendo del número de horas para cada tipo

de impacto. 226

Tabla 41: Coste total de restitución según el tipo de impacto. 227

Tabla 42: Valoración total de los impactos al año. 228

Tabla 43: Costos de mantenimiento del Plan de Contingencia. 228

Tabla 44: Estimación de la frecuencia de los impactos con la implementación del Plan de Contingencia. 229

Tabla 45: Costos totales con la implementación del Plan de Contingencia. 229

Tabla 46: Ahorro con la implementación del Plan de Contingencia. 230

Tabla 47: Parámetros de costos. 230

Tabla 48: Flujos operativos (ahorro) 231

Tabla 49: Cálculo de VAN, TIR, ROI y R B/C 232

ÍNDICE DE ECUACIONES

Ecuación 1: Cálculo de la eficiencia neta actualizada. 230

Ecuación 2: Cálculo del Valor Actual Neto 231

Ecuación 3: Cálculo de la TIR 231

Ecuación 4: Cálculo del ROI 232

Ecuación 5: Cálculo de la relación costo beneficio. 232

RESUMEN

Este proyecto se trata de un Plan de Contingencia que tiene su aplicación en la COAC Chuchuqui Ltda. de la ciudad de Otavalo. Para su desarrollo se revisaron las normas internacionales descritas por la unión técnica de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), así como también publicaciones de ITIL (Librería de Infraestructura de Tecnologías de la Información), para tomar un modelo base normalizado y de buenas prácticas que esté relacionado a la seguridad de la información.

En este trabajo se contempló un análisis de riesgos, un plan de emergencia, un plan de restauración, un plan de recuperación, pruebas y evaluación y un plan de mantenimiento, lo cual permitió establecer parámetros sobre los cuales fue necesario la implementación de controles de seguridad.

También dentro de la implementación de controles de seguridad se montó un sistema de monitoreo para los servidores del centro de datos de la COAC en una plataforma de software libre (NAGIOS), se realizó un escaneo de puertos abiertos en la red y las precauciones que se deben tomar para estos, se mejoró la seguridad física de los equipos mediante la implementación de una lectora de huellas para el control de acceso al Data Center al igual que una puerta de seguridad y un sistema de aire acondicionado.

Se realizó una capacitación del personal de la cooperativa sobre la seguridad de la información, lo que ayudó a mejorar los principios de seguridad (confiabilidad, integridad y disponibilidad), también se dio a conocer las nuevas políticas de seguridad instauradas en el último trimestre del año 2016 y una guía de cómo realizar la clasificación de la información.

Finalmente se realizó un estudio de factibilidad técnica y económica basada en cotizaciones de mano de obra y materiales útiles para la implementación de controles de seguridad.

ABSTRACT

This project is a Contingency Plan that has its application in the Chuchuqui Savings and Credit Cooperative of the Otavalo city. For its development, the international standards described by the technical union of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), as well as ITIL (Information Technology Infrastructure Library) publications, were revised to take a standardized model of good practice that is related to information security.

This work included a risk analysis, an emergency plan, a restoration plan, a recovery plan, tests and evaluation and a maintenance plan, which allowed to establish parameters on which it was necessary to implement safety controls.

Also within the implementation of security controls, was set up a monitoring system for the data center servers of the COAC in a free software platform (NAGIOS), a scan of open ports in the network was carried out and precautions were taken. Should be taken for these, the physical security of the equipment was improved by the implementation of a fingerprint reader to control access to the Data Center as well as a security door and an air conditioning system.

A training of the cooperative's personnel on information security was carried out, which helped to improve the principles of security (reliability, integrity and availability), also revealed the new security policies established in the last quarter of the year And a guide on how to perform the classification of information.

Finally, a technical and economic feasibility study was carried out based on labor quotations and useful materials for the implementation of security controls.

CAPÍTULO I

ASPECTOS GENERALES

En este capítulo se explica la problemática, las razones, el justificativo y la importancia del proyecto, así como también se estable el alcance del diseño e implementación del Plan de Contingencia dentro de la COAC Chuchuqui.

1.1. TEMA O TÍTULO

Plan de contingencia para la Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda., basado en la norma ISO/IEC 27002.

1.2. PROBLEMA

La Cooperativa Chuchuqui cuenta con un Data Center en el cual no se han tomado en cuenta las normas de seguridad necesarias, mismas a las que se deben regir todas las entidades financieras, y de las cuales la SEPS (Superintendencia de Economía Popular y Solidaria) en calidad de ente regulador, trata de imponer su cumplimiento dentro del sistema financiero, según lo permite el Reglamento de la Ley Orgánica de la Economía Popular y Solidaria en el Art. 156. La cooperativa tampoco cuenta con un Plan de Contingencia debidamente estructurado; sin embargo, el área de tecnología tiene un borrador que cubre varios aspectos, pero carece de un análisis de impacto de negocio (BIA), planes de recuperación para volver al estado normal de procesamiento y tampoco se han efectuado pruebas para verificar los resultados que se obtienen al ejecutar dicho plan.

Es de gran importancia el cumplimiento de los servicios que la entidad presta a la sociedad en calidad de ser una de las promotoras del equilibrio económico para la población indígena, pero una de sus limitaciones es que la infraestructura de red de la cooperativa no cuenta con las medidas de protección necesarias tanto a nivel de Software como Hardware, por lo cual se ve la necesidad de implementar soluciones que ayuden a mejorar la calidad, capacidad y velocidad del sistema financiero.

Así como las redes de información progresan en su desarrollo y seguridad, también se tiende a encontrar nuevas formas de violar la integridad de las mismas; de igual manera

se ven amenazadas por otros tipos de riesgos que pueden causar daños desfavorables a la red como, por ejemplo: desastres naturales, cortes de energía eléctrica, atentados terroristas o cualquier daño a nivel físico y lógico.

Por todas estas razones es importante que la cooperativa cuente con un plan de contingencia que permita actuar de forma adecuada ante cualquier eventualidad que afecte a la confianza de la institución ya que toda información que se relaciona a finanzas, tiene un grado de importancia muy elevado dentro de cualquier institución y mucho más en una cooperativa de ahorro y crédito cuya estabilidad depende del buen manejo del capital de sus socios, por lo que es una prioridad el implementar medidas de seguridad preventivas, para que la información se encuentre segura y libre de intrusos, además de anticiparse a los sucesos críticos que pueden sufrir los dispositivos de almacenamiento de información que puedan interrumpir en su disponibilidad y fiabilidad o en el peor de los casos, como consecuencia, llegue a perjudicar a sus clientes.

1.3. OBJETIVOS

1.3.1. Objetivo general

Implementar un plan de contingencia empleando mecanismos de control de seguridad informática para el departamento de sistemas de la Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda., basándose en la norma ISO/IEC 27002 con la finalidad de mejorar la confidencialidad, integridad y disponibilidad de la red.

1.3.2. Objetivos específicos

- Analizar la información recopilada sobre la norma de Controles de Seguridad ISO/IEC 27002 y sus respectivos Dominios de Seguridad que en ella se rigen, determinando lineamientos específicos para el desarrollo del plan de contingencia.

- Realizar un análisis de la situación actual del departamento de sistemas de la cooperativa Chuchuqui mediante el levantamiento de información para la identificación de los riesgos que comprometen la seguridad de la información.

- Establecer un plan de recuperación, respaldo y seguridad de la información empleando medidas de protección a nivel de Software y Hardware, las mismas

que también permitan dar solución a las falencias determinadas en el análisis de la situación actual.

- Realizar pruebas de evaluación de los controles de seguridad establecidos en el plan de contingencia, mediante simulaciones de fallos para verificar que se encuentren correctamente aplicados.

- Realizar un presupuesto económico para la implementación de las medidas de seguridad necesarias, empleando cotizaciones de materiales y mano de obra, mediante un estudio de factibilidad técnica-económica, con el fin de evaluar la rentabilidad de las soluciones propuestas.

1.4. ALCANCE

El presente proyecto se desarrollará en la Cooperativa Chuchuqui de la ciudad de Otavalo, cuyo enfoque es el establecer un plan de contingencia, para lo cual se iniciará con la recopilación de los puntos más importantes de la norma ISO 27002, que ayuden en la elaboración de un análisis de la situación actual de la entidad financiera basándose en los controles de seguridad que se rigen en dicha norma, tomando en cuenta los catorce dominios que de ella se desglosan y así poder establecer soluciones adecuadas a las falencias encontradas, para cumplir con los requerimientos que toda institución financiera debe cumplir.

En el análisis de la situación actual se realizará empleando la metodología FODA, identificando las fortalezas, Oportunidades, Debilidades y Amenazas. También se realizará un inventario de los equipos que forman parte de los activos más importantes, especificando sus características esenciales. El análisis permitirá tener una visión de las tecnologías disponibles versus las que se debería implementar.

De acuerdo a las amenazas identificadas se establecerán políticas de seguridad, medidas de mantenimiento de los equipos y procedimientos de control a seguir en caso de que surjan eventualidades inesperadas. Se definirá niveles de responsabilidad que serán repartidos entre el personal disponible y debidamente capacitado para responder a necesidades específicas, tanto para acciones preventivas como para acciones de respuesta inmediata.

Se establecerá medidas para respaldar la información y procedimientos de seguridad a seguir ante cualquier falla en la red que amenace con interrumpir la continuidad de las comunicaciones, tanto a nivel de software como de hardware y de esta forma mantener la fiabilidad y disponibilidad de la información. También se establecerá procedimientos de recuperación y de igual forma para restauración de los servicios de comunicación en el menor tiempo posible.

Se implementará un sistema de monitoreo para hacer seguimiento del estado de los servidores que conforman la red interna de datos, la cual cuenta con los siguientes servidores: Servidor de Producción, Servidor Espejo de Producción, Servidor de Datos Antiguo, Servidor Windows, Servidor Firewall y el mismo servidor donde se desarrollará la monitorización; se realizará una comparativa de software de monitoreo para establecer el más adecuado, poniendo énfasis en los parámetros de estado más importantes, que permiten tener una perspectiva clara del nivel de rendimiento de dichos servidores, de los cuáles el sistema se va a encargar de dar un aviso de alerta el momento en el que los datos resultantes sobrepasen las cuantificaciones establecidas para cada caso. Estas características esenciales son: Espacio de Disco, Memoria RAM, Cantidad de Procesos y Temperatura.

Hay que tomar en cuenta que el sistema de monitoreo ayuda a conocer y anticipar falencias que puedan ocurrir en los servidores de la red, pero no se va dar solución a dichos problemas. El suministrar alguna respuesta a cualquier eventualidad es compromiso de los técnicos encargados.

Se realizarán pruebas de evaluación de los controles de seguridad establecidos en el plan de contingencia, mediante simulaciones de fallos para verificar que se encuentren correctamente aplicados o de ser necesario realizar correcciones o modificaciones.

Se establecerá un presupuesto económico para la implementación de las medidas de seguridad necesarias, empleando cotizaciones de materiales y mano de obra, mediante un estudio de factibilidad técnica-económica contemplando la parte administrativa y legal de la institución, con el fin de evaluar la rentabilidad de las soluciones propuestas.

1.5. JUSTIFICACIÓN

La Cooperativa de ahorro y crédito CHUCHUQUI como institución financiera tiene el compromiso con la sociedad de brindar a sus socios productos y servicios financieros de calidad, generando un crecimiento y rentabilidad sostenida. Uno de los requerimientos para cumplir con este compromiso es el mantener segura la red de información, generando estrategias que ayuden a subsanar los hallazgos identificados en la auditoría realizada por la SEPS según lo expresa el oficio circular N°SEPS-IFPS-2014-03570 del 26 de febrero de 2014.

Debido a las exigencias de la SEPS después de revisar los informes de auditorías como se manifiesta en el Reglamento de la Ley Orgánica de la Economía Popular y Solidaria en el Art. 154 y dada la importancia de la información que maneja diariamente la cooperativa es fundamental la implementación de mecanismos de seguridad en redes, que protejan los datos que se transmiten e interactúan en la red de datos. Implantando recursos de protección para que no se violen las barreras de acceso al Data Center y la información que en ellos se maneja o almacena, que puedan generar pérdidas a la cooperativa.

Es necesario que la entidad intente alcanzar que la SEPS certifique que la cooperativa cuenta con una continuidad de negocio respecto a la tecnología de información y la realización de un plan de contingencia respalda que la cooperativa se encuentre en una etapa de crecimiento tecnológico. Además de proporcionar servicios de calidad para garantizar un mayor nivel de confiabilidad en sus socios y clientes.

Cuando se tiene una transferencia de datos con altos niveles de seguridad informática le permite al beneficiario reducir costos operativos, mejorar su viabilidad, escalabilidad y costo-beneficio de la estructura de la red, obteniendo una gran ventaja para sobresalir en la competitividad con otras entidades del mismo carácter.

CAPÍTULO II

FUNDAMENTO TEÓRICO

En este capítulo se realiza una introducción sobre la Seguridad Informática y se mencionará la norma ISO/IEC 27002 en la cual se basa este anteproyecto, explicando cada uno de sus dominios y objetivos. También menciona algunos detalles de normas (ISO 27005 y COBIT) y manuales de buenas prácticas de ITIL, que tienen relación con la seguridad informática y que forman parte del desarrollo del Plan de Contingencia.

2.1. Seguridad de la información.

En la actualidad los sistemas de comunicación manejan grandes cantidades de información valiosa e importante para las organizaciones, empresas, industrias, y usuarios que requieren preservarla integra, la pérdida de esta o cualquier tipo de manipulación o recepción de personas no autorizadas suponen un peligro inminente, así como perjuicios en recursos económicos, tiempo y disponibilidad. (Alegre Ramos & García Hurtado, 2011, pág. 2)

Toda información personal, así como sistemas de facturación, cuentas bancarias, bases de datos de empresas, sistemas telefónicos, sistemas de control, etc. Se alojan en ordenadores o servidores, conectados a la internet o en una red privada, pero sin duda alguna toda información es valiosa para los usuarios y administradores que la crean y manejan, pero también lo es para aquellos que tienen fines intromisorios o que van en contra de lo legal, lo que hace considerar medidas de prevención, protección y corrección. (Alegre Ramos & García Hurtado, 2011, pág. 2)

En la seguridad de la información, para todo aquello que atente o dé lugar a la pérdida de datos dentro de las redes de comunicación o durante el transporte y recepción de la información, se deben tomar en cuenta varios parámetros definidos como un conjunto de herramientas que brinden seguridad en la información incluso considerando el factor humano. Es decir que no solo se pueden tener planes de prevención ante vulnerabilidades y amenazas técnicas de software (a nivel lógico), sino también de hardware (a nivel físico), y un factor humano o medios humanos que debido a la imprudencia de no tomarlos en cuenta se han convertido en un factor determinante en la

seguridad de la información.

2.1.1. Seguridad activa y pasiva.

2.1.1.1. Seguridad activa.

La seguridad activa es la permanente preparación del sistema ante un ataque o problema que se suscite en la red, es una serie de medidas preventivas que mantienen la seguridad que mantiene como mecanismos más comunes listas de acceso, sistemas de Firewall, establecimiento de contraseñas, diferenciación de niveles de acceso, etc. Este tipo de seguridad tiene por fin evitar problemas en la red de datos. (Alegre Ramos & García Hurtado, 2011, pág. 3)

2.1.1.2. Seguridad pasiva.

La seguridad pasiva tiene lugar una vez que haya sucedido un ataque o fallo en la red, este tipo de seguridad permite reestablecer los servicios y recuperar información, dentro de este tipo de seguridad podemos encontrar Sistemas de Backup, mecanismos de redundancia física, manuales de recuperación de configuraciones, etc. (Alegre Ramos & García Hurtado, 2011, pág. 5)

2.1.2. Seguridad física y lógica.

2.1.2.1. Seguridad física.

Son mecanismos que evitan fallos de carácter físico provocado por la naturaleza o por el humano, estos mecanismos son barreras físicas como soportes, armarios, puertas seguras, seguridad contra incendios, seguridad contra manipulación de todo tipo, sistema de puesta a tierra, equipos organizadores y de sujeción, etc. (Alegre Ramos & García Hurtado, 2011, pág. 6)

2.1.2.2. Seguridad lógica.

Son las medidas que se adoptan para evitar fallos e intrusiones que no son de ámbito físico y que más bien tiene mucho que ver con el software, como programas, sistemas operativos, antivirus, códigos, bases de datos, recursos, protocolos de red, conexiones remotas, en si es todo tipo de información digital. (Alegre Ramos & García Hurtado, 2011, pág. 7)

Este tipo de seguridad es la más vulnerable puesto que la información viaja en forma digital se puede acceder a ella de forma remota. (Alegre Ramos & García Hurtado, 2011, pág. 7)

2.1.3. Principios de la seguridad.

2.1.3.1. Confidencialidad.

Es cuando la información es visible o accesible únicamente para quienes se ha dado la autorización, es decir que solo el propietario o administrador de esa información y los usuarios competentes a ella son los únicos que tienen la capacidad de acceder a dicha información y deberán hacerlo en forma cuidadosa sin ningún tipo de divulgación, difusión o distribución de la información. (Alegre Ramos & García Hurtado, 2011, pág. 10)

2.1.3.2. Integridad.

Cuando la información que circula por un canal de comunicación y llega a su destino sin ser manipulada y alterada se denomina integridad, es decir que en el proceso de entrega de información no se debe hacer cambio alguno a la información puesto que se incurriría en violación de la integridad de la información. (Alegre Ramos & García Hurtado, 2011, pág. 10)

Los intentos de corrupción en la información pueden suceder en cualquier momento y en cualquier lugar o durante el proceso de comunicación entre transmisor y receptor, este problema puede ser consecuencia de las vulnerabilidades a los sistemas o directamente al personal de la empresa, pero también puede ser consecuencia de errores del entorno físico (hardware) de la red de datos.

2.1.3.3. Disponibilidad.

Uno de los grandes problemas a los que se enfrentan los administradores de la red de datos son los tiempos de respuesta en los que se obtiene la información solicitada, esto responde a el concepto denominado disponibilidad, también se relaciona a la facilidad con que se recupera la información solicitada o si dicha información no se encuentra disponible, en todos los casos se depende de la fiabilidad de la red que es la optimización de los recursos tanto físicos como lógicos. (Alegre Ramos & García Hurtado, 2011, pág.

11)

2.1.4. Riesgos en la seguridad de la información

Los riesgos en la seguridad de la información vienen del resultado del análisis de los impactos en distintos escenarios de incidentes y esto es con el fin de identificar ciertas características que nos permitan obtener una valoración de los mismos. De aquí es donde surge el concepto de riesgos aceptables y no aceptables los cuales tiene que ver con la frecuencia en la que estos se presentan y la forma en la estos afectan a las actividades empresariales.

Un riesgo se lo puede describir como una eventualidad o conjunto de eventualidades que pueden llegar a poner en peligro a proyectos de una organización que incluso pueden llegar a evitar el desarrollo de la misma. Hay veces en las que las eventualidades desconocidas pueden ser confundidas con riesgos y esto se debe a que en ocasiones surgen incógnitas en la forma en la que se desenvuelven las operaciones en una organización, pero siempre que se tenga una preocupación se debe realizar un análisis para ver si esas eventualidades afectan o no afectan en los resultados que se desea obtener. (Tejada, 2015)

2.2. REGLAMENTO A LA LEY ORGÁNICA DE LA ECONOMÍA POPULAR Y SOLIDARIA

El Reglamento a la ley orgánica de la economía popular y solidaria tiene su última actualización el 27 de febrero del 2012 en el decreto No. 1061, con el Registro Oficial Suplemento 648. Este reglamento tiene sentido gracias al artículo 283 de la Constitución de la República, en el cual se estable que el sistema económico se integrará por las formas de organización económica pública, privada, mixta, popular y solidaria, y las demás que la Constitución determine. (SEPS, 2012)

El reglamento está conformado por 7 Títulos, los cuales contienen cierto número de capítulos, los cuales a su vez contienen varias secciones y estas secciones pueden contener parágrafos; el reglamento también consta de disposiciones finales, disposiciones transitorias, disposiciones reformatorias y una disposición final. (SEPS, 2012)

Este reglamento tiene como objeto establecer procedimientos de aplicación de la Ley Orgánica de Economía Popular y Solidaria, y para ello determina un orden en la

organización estructural, tanto de la SEPS como de las instituciones financieras asociadas a ella, aclareciendo los requisitos para cada cargo y los roles y responsabilidades que de ellos se amerita.

Hay que tomar en cuenta que la SEPS es la encargada del control de las cooperativas de ahorro y crédito la cual tiene personalidad jurídica de derecho público y autonomía administrativa y financiera que tiene como objetivo la solidez, estabilidad y un buen desarrollo del sector económico popular y solidario. Para mayor entendimiento es necesario conocer la estructura de los organismos de control del sistema financiero ecuatoriano, que se puede observar en la Figura 1. (SEPS, 2015)

Figura 1: Estructura legal de los organismos de control

Fuente: COAC Unión Popular Ltda. (2016). Normativa de la superintendencia de la economía popular y solidaria. Recuperado el 22 de noviembre de 2016 de: http://coacunionpopular.com/coac-union-popular---normativa.html

Los miembros de la SEPS encargados de realizar los controles respectivos a las cooperativas de ahorro y crédito, son personas calificadas para este trabajo en un número no mayor a tres asociados, los cuales tienen la obligación de reunirse por lo menos una vez cada trimestre, para la evaluación de sus tareas designadas como se establece en el Artículo 20 del Reglamento a la ley orgánica de la economía popular y solidaria. (SEPS, 2012)

Estos miembros del órgano de control realizan sus inspecciones de acuerdo a oficios circulares que la SEPS emite para cada caso o institución, basándose en diferentes

reglamentos, códigos o libros que la misma SEPS ha publicado, los cuales se encuentran relacionados con sector económico y financiero y que deben estar vigentes, estableciendo estrategias y procedimientos de hallazgos de auditoría según lo respalda el Reglamento de la Ley Orgánica de la Economía Popular y Solidaria en el Art. 154. (SEPS, 2014)

2.3. ANÁLISIS DE LA NORMA TÉCNICA ISO/IEC 27002

Esta norma es presentada gracias a la ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) que han coordinado comités técnicos para colaborar en los campos de la seguridad de la información, además de estos, se unen otras instituciones gubernamentales y no gubernamentales al desarrollo de este trabajo. (ISO/IEC 27002, 2013)

La norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar una gestión de seguridad de la información en una organización. Los objetivos definidos en esta norma proveen directrices generales sobre las metas generadas para una gestión de la seguridad de la información. (ISO/IEC 27002, 2013)

Los objetivos de los controles de esta norma, tienen como finalidad ser puestos en marcha para socorrer a los requisitos generados por medio del análisis y evaluación de los riesgos. Esta norma puede servir como guía práctica para desplegar los procedimientos de seguridad de la información de la institución y las eficientes prácticas de gestión de seguridad, y para generar una creciente confianza en las actividades que envuelven a los clientes. (ISO/IEC 27002, 2013)

2.3.1. Estructura.

Esta norma cuenta con 14 dominios de seguridad de la información que juntas totalizan 35 categorías principales y 114 controles de seguridad, además de una introducción de análisis y evaluación para el tratamiento de riesgos.

2.3.2. Dominios.

Cada dominio cuenta con un número de categorías principales de la seguridad de la información. Los 14 dominios son (los números en los paréntesis representan la cantidad de categorías para cada dominio los cuáles se detallan en el Plan de Mantenimiento):

- Política de seguridad de la información (1)
- Aspectos organizativos de la seguridad de la información (2)
- Seguridad ligada a los recursos humanos (3)
- Gestión de activos (3)
- Control de Accesos (4)
- Cifrado (1)
- Seguridad física y ambiental (2)
- Seguridad en la operativa (7)
- Seguridad en las telecomunicaciones (2)
- Adquisición, Desarrollo y Mantenimiento de sistemas de información (3)
- Relaciones con suministradores (2)
- Gestión de incidentes de seguridad de la información (1)
- Aspectos de la seguridad de la información en la gestión de continuidad del negocio (2)
- Cumplimiento (2)

Nota: *el orden de los dominios en esta norma no significa su grado de importancia. Dependiendo de las circunstancias, todas las secciones pueden ser importantes. Por lo tanto, conviene que cada organización que utilice esta norma identifique cuáles son los ítems aplicables, que importancia les dan y sus aplicaciones para los procesos específicos de negocio. Todas las alineaciones en esta norma no están ordenadas por prioridades a no ser que se indique.* (ISO/IEC 27002, 2013)

2.3.3. Categorías principales de seguridad de la información.

Cada categoría principal de la información contiene:

- Un objetivo de control que define lo que debe ser alcanzado; y
- Uno o más controles que pueden ser implementados para alcanzar un objetivo de control.

Las descripciones de los controles están estructuradas de la siguiente forma:

Control

Da una definición sobre el control especificando las medidas que se deben tomar para atender un objetivo de control.

Directrices para la implementación del control

Contiene información más específica o detallada para guiar en la implementación del control y brindar atención a un objetivo de control. Algunas de estas guías o directrices no pueden ser adecuadas en todos los casos y así mismo pueda que otras metodologías de implementación de control pueden ser más idóneas. (ISO/IEC 27002, 2013)

Informaciones adicionales

Contiene información adicional que puede ser tomada en cuenta, como, por ejemplo, consideraciones legales o referencias de otras normas. (ISO/IEC 27002, 2013)

2.3.4. Políticas de seguridad.

Un documento que se denomina "política" es aquel que se publica de manera formal por parte del Comité Administrativo de la institución con la intención de establecer instrucciones globales, para su respectivo cumplimiento. (ISO, 2013)

Las políticas se deben basar en el contexto en el que opera una organización y su contenido debe estar bien relacionado a los objetivos, misión, visión, metas de la institución, metodologías adoptadas para alcanzar los objetivos propuestos, procedimientos prestablecidos para los servicios ofrecidos por la institución, así como también deben estar basados en reglamentos de entes reguladores o instituciones de nivel superior a esta que en este caso es la SEPS (Superintendencia de Economía Popular y Solidaria). (ISO, 2013)

La estructura habitual de la documentación de políticas puede ser:

- Resumen: Política Resumen - Visión general de una extensión breve; una o dos frases y que pueden aparecer fusionadas con la introducción. (ISO, 2013)

- Introducción: Breve explicación del asunto principal de la política.

- Ámbito de aplicación: Descripción de los departamentos, áreas o actividades de una organización a las que afecta/aplica la política. Cuando es relevante en este apartado se mencionan otras políticas relevantes a las que se pretende dar cobertura desde ésta. (ISO, 2013)

- Objetivos: Descripción de la intención de la política.

- Principios: Descripción de las reglas que conciernen a acciones o decisiones para alcanzar los objetivos. En algunos casos puede ser de utilidad identificar previamente los procesos clave asociados con el asunto principal de la política para pasar posteriormente a identificar las reglas de operación de los procesos. (ISO, 2013)

- Responsabilidades: Descripción de quién es responsable de qué acciones para cumplir con los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, así como las responsabilidades de las personas con roles designados. (ISO, 2013)

- Resultados clave: Descripción de los resultados relevantes para las actividades de la organización que se obtienen cuando se cumplen los objetivos.

- Políticas relacionadas: Descripción de otras políticas relevantes para el cumplimiento de los objetivos, usualmente se indican detalles adicionales en relación a temas específicos. (ISO, 2013)

Hay que considerar el principio típico en seguridad "lo no está permitido, está prohibido", cada organización debería detectar las necesidades de sus usuarios y valorar los controles de seguridad necesarios que fortalezcan las políticas correspondientes al negocio, aplicando la mejor metodología para su implementación y gestión. (ISO, 2013)

2.3.5. Aspectos organizativos de la seguridad de la información.

El objetivo de éste dominio es establecer la gestión de la seguridad de la información, como parte fundamental de los procesos y servicios de la institución. Para ello se recomienda concretar formalmente una temática de gestión para establecer y delimitar tareas tales como la aprobación de las políticas de seguridad, coordinación de la aplicación de controles de seguridad y la asignación de roles y responsabilidades por parte de los funcionarios. (ISO, 2013)

Cuando se desee realizar cualquier actividad sobre la seguridad de la información, por ejemplo, actualización de las medidas de control, actualización de políticas, nuevo análisis de riesgos, etc., es de suma importancia disponer de fuentes de respaldo confiables que sirvan de guías prácticas o de ser necesario pedir asesoramiento de técnicos especializados.

Existen varios factores que hacen que la protección física se reduzca en las instituciones, por ejemplo, la movilidad constante de los funcionarios que hace que las puertas de acceso permanezcan abiertas, o se descuiden los puestos de trabajo. En estos casos se considera que la información puede ponerse en riesgo si el acceso se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información. (ISO, 2013)

2.3.6. Seguridad ligada a los recursos humanos.

El presente dominio tiene como objetivo cubrir la necesidad de educar e informar al personal desde su ingreso a la institución y en forma continua, dar seguimiento a cualquier actividad que desarrolle dentro de la misma, así como también estar pendiente de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en lo que respecta a la seguridad de la información y asuntos de confidencialidad. (ISO, 2013)

Es muy importante tratar de reducir los riesgos de error humano, uso imprudente de instalaciones y recursos y manipulación no autorizada de la información, haciendo uso del establecimiento de posibles sanciones que se aplicarán en caso de suceda una infracción. (ISO, 2013)

Se recomienda definir responsabilidades en el tema de seguridad de la información en la etapa de incorporación de personal e incluirlas en los contratos de trabajo a firmarse y verificar su capacidad y cumplimiento durante el desarrollo del individuo como empleado, así como, garantizar que el personal esté al tanto de las amenazas y vulnerabilidades en lo que respecta a la seguridad de la información, y se encuentren competentes para respaldar las Políticas de Seguridad de la institución en el desempeño de sus tareas asignadas. (ISO, 2013)

Por lo general, la responsabilidad de incluir las funciones relacionadas a la seguridad de la información en las especificaciones de los roles de los empleados, es del Área de Recursos Humanos, así como, informar a todo el personal que ingresa sobre sus obligaciones, en base al cumplimiento de las Políticas de Seguridad de la Información, verificar y ratificar las responsabilidades de confidencialidad de los funcionarios y coordinar tareas de capacitación de todos los miembros de la institución respecto a los procesos más comunes que ayuden a cubrir las necesidades actuales de seguridad. (ISO, 2013)

2.3.7. Gestión de activos.

El objetivo que pretende alcanzar este dominio es que la organización posea conocimiento puntual sobre los activos que posee como parte necesaria para una correcta administración de riesgos. (ISO, 2013)

Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc. (ISO, 2013)

- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc. (ISO, 2013)

- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios

magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.-), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc. (ISO, 2013)

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.). (ISO, 2013)

Un hábito que las instituciones deben tener es clasificar los activos de información de acuerdo a la sensibilidad y criticidad de la información que contienen o también puede ser de acuerdo a la funcionalidad que cumplen y deben ser etiquetados en función a ello, con el objeto de marcar o indicar cómo han de ser manipulados y protegidos. (ISO, 2013)

Existen varios modelos de clasificación de la información, pero las instituciones deben sujetarse a sus propias políticas o contexto de la organización, pero dicha clasificación no necesariamente debe mantenerse invariable permanentemente, sino que ésta puede cambiar de acuerdo a un nuevo estudio o implementación de nuevas políticas determinadas por la propia institución. (ISO, 2013)

2.3.8. Control de accesos.

Lo que se pretende en este dominio es controlar el acceso por medio de metodologías de restricciones y limitaciones a la información, debido a que ésta es considerada como base de todo sistema de seguridad informática. (ISO, 2013)

Para la restricción del acceso no autorizado a los sistemas de información es necesario la implementación de instrucciones formales para gestionar la asignación de derechos de acceso a los sistemas, bases de datos y servicios de información; estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. (ISO, 2013)

Los procedimientos de gestión de los accesos incluyen a todos los niveles de la estructura organizativa de la institución y estos comienzan desde la incorporación del personal a la organización, hasta que el individuo abandone sus funciones o hasta que el acceso ya no sea necesario por la naturaleza de su trabajo. (ISO, 2013)

La cooperación de los funcionarios es primordial para la eficacia de la seguridad, por lo tanto, es necesario capacitar y concientizar a los mismos sobre sus responsabilidades para el mantenimiento de controles de acceso indicados, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento. (ISO, 2013)

2.3.9. Cifrado.

El presente dominio tiene como objetivo el uso de procedimientos y técnicas criptográficas para la protección de datos dependiendo del análisis de riesgo efectuado para cada clasificación de la información, con la finalidad de garantizar una adecuada preservación de la confidencialidad e integridad. (ISO, 2013)

La implementación de medidas de cifrado se debe desarrollar en base las políticas sobre el uso de controles criptográficos y el establecimiento de una gestión de las claves que cada institución debe poseer para el respaldo de la aplicación de dichas técnicas. (ISO, 2013)

2.3.10. Seguridad física y ambiental.

El objetivo es reducir los riesgos de pérdidas e interferencias a la información y a las operaciones de la organización. Para ello se recomienda el establecimiento de perímetros de seguridad y áreas protegidas, que facilitan la implementación de controles de seguridad de las instalaciones donde se realiza el procesamiento de información crítica o sensible de la institución, contra accesos físicos no autorizados. (ISO, 2013)

El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. La información que se almacena en los sistemas de procesamiento y las copias de seguridad contenidas en diferentes medios de almacenamiento, es susceptible a ser sustraída mientras estos no están siendo utilizados. (ISO, 2013)

2.3.11. Seguridad en la operativa.

El objetivo es gestionar la efectividad de los procedimientos de operaciones y el uso y mantenimiento de documentación actualizada relacionada a cada proceso.

Adicionalmente, se debe realizar una evaluación del posible impacto operativo de cambios que sean necesarios realizar en los sistemas y equipamiento, además de verificar su correcta implementación, asignando los roles y responsabilidades correspondientes. (ISO, 2013)

Con el fin de evitar potenciales amenazas a la seguridad de los sistemas o servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad. (ISO, 2013)

La administración de la realización de las copias de respaldo de información, así como la verificación periódica de su restauración, permiten garantizar el restablecimiento de las operaciones dentro de los tiempos aceptables de caída establecidos. (ISO, 2013)

Finalmente, se debe verificar el cumplimiento de las políticas, procedimientos y controles de seguridad establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para el monitoreo del estado de los sistemas y descubrimiento de nuevos riesgos. (ISO, 2013)

2.3.12. Seguridad en las telecomunicaciones.

Su objetivo es garantizar la protección de la información que se transmite por medio de redes telemáticas y la protección de su infraestructura de soporte. Una gestión confiable de las redes de la institución, requiere de las consideraciones del flujo de datos, implicaciones legales, monitoreo y protección, las cuales pueden comprender límites organizacionales. (ISO, 2013)

La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección. Los intercambios de información por parte de las instituciones se deberían basar en una política formal de intercambio y deben estar alineadas con los acuerdos de intercambio, y cumplir con cualquier legislación relevante. (ISO, 2013)

2.3.13. Adquisición, desarrollo y mantenimiento de los sistemas de información.

Su objetivo es garantizar la aplicación de controles de seguridad y confirmación de datos en la adquisición y el desarrollo de los sistemas de información. Determinar y documentar las normas, políticas, reglamentos internos y procedimientos que se aplicarán

durante el ciclo de vida de los activos y en la infraestructura de base en la cual se apoyan. (ISO, 2013)

En este dominio también se recomienda definir las metodologías de protección de la información crítica o sensible, así como, aplicar a todos los sistemas informáticos, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la institución. (ISO, 2013)

2.3.14. Relaciones con suministradores.

Este dominio tiene como objetivo implementar y conservar el nivel adecuado de la seguridad para la información y la entrega de los servicios contratados alineados con los acuerdos de entrega de servicios prestados por terceros. (ISO, 2013)

La institución debe controlar la implementación de los acuerdos, monitorear su cumplimiento con los estándares y gestionar los cambios para garantizar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas. De ser necesario se debe realizar una capacitación a los terceros para el conocimiento de las normas que se rigen en la institución y así, evitar cualquier inconveniente de errores humanos. (ISO, 2013)

2.3.15. Gestión de incidentes.

Este dominio tiene como objetivo certificar que los incidentes de seguridad de la información y los enflaquecimientos asociados a los sistemas de información sean comunicados inmediatamente de forma tal que se apliquen las acciones correctivas en el tiempo adecuado dependiendo de los tiempos aceptables de caída para cada servicio. (ISO, 2013)

Las instituciones cuentan con múltiples activos de información, cada uno se encuentra expuesto a sufrir cualquier incidente de seguridad. Por lo que resulta necesario contar con una capacidad de gestión de dichos incidentes que permita dar un tratamiento a éstos empezando por su detección y registro, llevando a cabo soluciones y colaborar en la prevención de futuros incidentes similares. (ISO, 2013)

2.3.16. Aspectos de la seguridad de la información en gestión de la continuidad del negocio.

Este dominio tiene como objetivo mantener la seguridad de la información durante los procesos de activación y actualización de los sistemas, desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad. (ISO, 2013)

Se debe integrar dentro de los niveles críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con cuidado especial a la legislación, los servicios, las operaciones, el personal, el transporte y los activos que estén dispuestos de un modo distinto al plan de negocio habitual. (ISO, 2013)

Se debe realizar un análisis de las consecuencias de los incidentes, fallas de seguridad, la disponibilidad del servicio y pérdidas de servicio para desarrollar y aplicar planes de contingencia que ayuden a garantizar que los procesos del negocio se pueden restaurar en los plazos de tiempo aceptable de caída de las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos. (ISO, 2013)

La finalidad de este control es tratar de minimizar los impactos de las posibles interrupciones de las actividades normales de la institución asociadas a desastres naturales, accidentes significativos, fallas en el equipamiento, error humano, falla en la comunicación u otros hechos, velando los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación. (ISO, 2013)

2.3.17. Cumplimiento.

Todo proceso o actividad que esté relacionado con los sistemas de información deben estar regulados y gestionados por disposiciones legales y contractuales. Los requisitos normativos y contractuales correspondientes a cada sistema de información deben estar correctamente definidos y documentados. (ISO, 2013)

La finalidad de este dominio es cumplir con las disposiciones de políticas, normativas, reglamentos y contractuales a fin de evitar sanciones administrativas a la institución o a los funcionarios que incurran en responsabilidad civil o penal como resultado de los incumplimientos. (ISO, 2013)

Se debe realizar una revisión periódica de la seguridad de los sistemas de información para garantizar la adecuada implementación de las políticas, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información. (ISO, 2013)

2.4. ANÁLISIS DE LA NORMA TÉCNICA NTC/ISO 27005:2005

Esta norma está desarrollada gracias a la participación de la ISO (Organización Internacional para la Normalización) e IEC (Comisión Electrotécnica Internacional) que en sí son las que forman el sistema especializado a nivel mundial para la normalización. además de estos existen otros organismos que conforman comités para tratar temas técnicos. Cuando el comité técnico de estos organismos superiores da a conocer una nueva Norma Internacional a todas las organizaciones nacionales, debe cumplir con el 75% de aprobación realizando una votación. (NTC/ISO/IEC 27005, 2008)

La NTC-ISO 27005, proporciona guías o directrices que dan soporte a la gestión del riesgo en la seguridad de la información para una institución, cubriendo los requisitos que conlleva un sistema de gestión de seguridad de la información (SGSI) en relación a la norma ISO 27001. (NTC/ISO/IEC 27005, 2008)

Esta norma sirve como apoyo para la implementación satisfactoria de los controles generales descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 para la seguridad de la información, con su enfoque en la gestión de riesgos, por lo cual es necesario tener conocimientos previos de estas dos normas. Esta norma aplica para cualquier organización que tenga en bien el análisis de riesgos para cubrir las necesidades de la seguridad informática. (NTC/ISO/IEC 27005, 2008)

2.4.1. Estructura.

Esta norma contiene especificaciones de los procedimientos para la gestión del riesgo y las actividades a realizar para la seguridad de la información. Todas estas actividades se presentan en el numeral 6 de esta norma y se detallan posteriormente en los numerales:

- establecimiento del contexto, en el numeral 7;
- evaluación del riesgo, en el numeral 8;
- tratamiento del riesgo, en el numeral 9;

- aceptación del riesgo, en el numeral 10;
- comunicación del riesgo, en el numeral 11;
- monitoreo y revisión del riesgo, en el numeral 12

En anexos se presenta información más específica para la gestión del riesgo y algunos ejemplos de amenazas, vulnerabilidades, activos que pueden ser útiles para su identificación en cada organización.

2.4.2. Información general.

La gestión del riesgo en la seguridad de la información debería ser una parte integral de todas de gestión de seguridad de la información y se deberían aplicar tanto a la implementación como al funcionamiento continuo de un SGSI. La gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. (NTC/ISO/IEC 27005, 2008)

La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable. La gestión del riesgo en la seguridad de la información debería contribuir a: (NTC/ISO/IEC 27005, 2008)

- La identificación de los riesgos;
- La evaluación de los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia;
- La comunicación y entendimiento de la probabilidad y las consecuencias de estos riesgos;
- El establecimiento del orden de prioridad para el tratamiento de los riesgos;
- La priorización de las acciones para reducir la ocurrencia de los riesgos;
- La participación de los interesados cuando se toman las decisiones sobre gestión

del riesgo y mantenerlos informados sobre el estado de la gestión del riesgo;

- La eficacia del monitoreo del tratamiento del riesgo;
- El monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos;
- La captura de información para mejorar el enfoque de la gestión de riesgos;
- La educación de los directores y del personal acerca de los riesgos y las acciones que se toman para mitigarlos. El proceso de gestión del riesgo en la seguridad de la información se puede aplicar a la organización en su totalidad, a una parte separada de la organización (por ejemplo, un departamento, una ubicación física, un servicio), a cualquier sistema de información, existente o planificado, o a aspectos particulares del control (por ejemplo, la planificación de la continuidad del negocio). (NTC/ISO/IEC 27005, 2008)

2.4.3. Proceso de gestión del riesgo.

Así como se indica en la Figura 2, el proceso para gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o de tratamiento del riesgo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos altos se valoren de manera correcta. (NTC/ISO/IEC 27005, 2008)

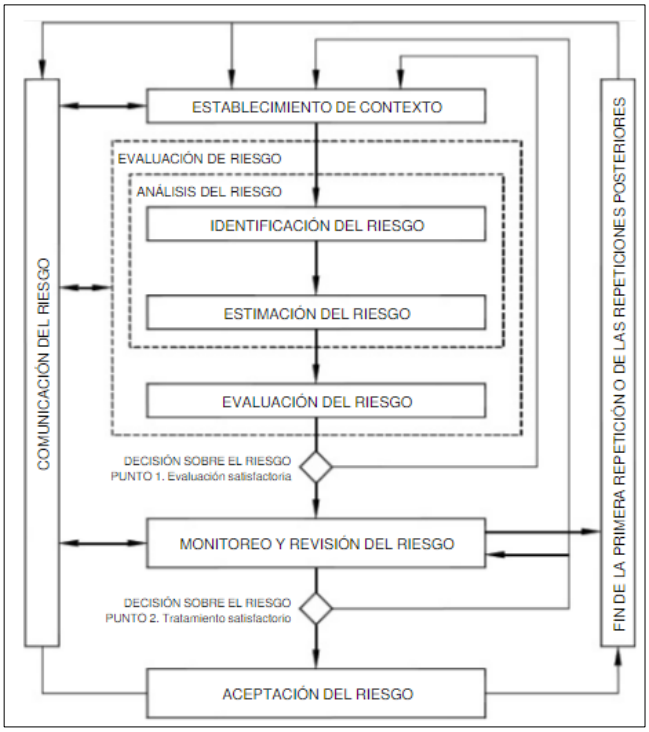


Figura 2: Proceso de gestión del riesgo en la seguridad de la información

Fuente: NTC/ISO/IEC 27005 (2008). Tecnologías de la información: Técnicas de seguridad: Gestión del riesgo en la seguridad de la información. Pereira: Aseuc.

En todo el tiempo que se desenvuelve el proceso de gestión del riesgo en la seguridad de la información es importante que dichos riesgos antes de su respectivo tratamiento sean comunicados los responsables del departamento de tecnología y al personal operativo correspondiente que por lo general son los encargados de gestionar cualquier anomalía en la seguridad de la información. La información obtenida de la identificación de los riesgos puede ser valiosa para la gestión de incidentes y ayuda a la reducción de daños potenciales para la institución. (NTC/ISO/IEC 27005, 2008)

La concienciación por parte de los administradores y el personal encargado de la gestión de riesgos y los controles que se han implementado para evitar los riesgos, facilitan el tratamiento de los incidentes y eventos inesperados de una manera más eficiente. Una recomendación muy necesaria es la documentación los resultados para cada actividad desarrollada durante el proceso de gestión del riesgo. (NTC/ISO/IEC 27005, 2008)

2.5. ITIL V3

2.5.1. Descripción general de ITIL.

ITIL (Information Technology Infraestructure Library o Biblioteca de Infraestructura de Tecnologías de la Información) es un extracto de publicaciones, o libros en sí, que describen de manera sistemática un conjunto de "buenas prácticas" para la gestión de los servicios de Tecnología Informática. (Ríos, 2014)

En vista de que las instituciones cada vez dependen más de las tecnologías de información para el desarrollo de sus actividades diarias, así como también para su control y gestión a través de sistemas de información, y que todo esto a su vez se encuentra dentro de una red que puede estar controlada por otros sistemas informáticos. Por lo tanto, al ver toda esta complejidad que se contiene en las redes y sistemas informáticos, lleva a varias instituciones a recurrir a la necesidad de contar con un modelo de gestión para todo lo que conforma la infraestructura de TI, que sea eficaz y de fácil implementación. (Ríos, 2014)

Es así, como en la década de los 80 nació ITIL por medio de la Agencia Central de Telecomunicaciones y Computación del Gobierno Británico (Central Computer and Telecomunications Agency – CCTA), que pensó e implantó una guía para que las oficinas del sector público británico fueran más eficientes en su trabajo y por tanto se redujeran los costes derivados de los recursos TI. En la actualidad ITIL pertenece al Oficina de Comercio Británico (Office of Government Commerce – OGC), pero puede ser utilizado para su aplicación libremente. (Ríos, 2014)

ITIL descubrió la necesidad de realizar un estudio que contenga una agrupación de libros según conjuntos estructurados en los procesos que estuviesen más relacionados, enmarcando la gran cantidad de publicaciones existente en ocho volúmenes, denominándose desde entonces como ITIL v2. (Ríos, 2014)

Su última versión fue publicada en el año 2007, tildada como ITIL v3. En esta versión se ha realizado un renuevo de la información ya publicada, que agrupa los principales elementos de ITIL en 5 volúmenes, que pueden encontrarse en la actualidad con los siguientes títulos (en inglés original):

- ITIL v3 Service Strategy (SS)
- ITIL v3 Service Design (SD)
- ITIL v3 Service Operation (SO)
- ITIL v3 Continual Service Improvement (CST)
- ITIL v3 Service Transition (ST) (Ríos, 2014)

2.6. COBIT

COBIT (Control Objetives for information and related Technology, Objetivos de Control para Tecnologías de información y relacionadas) es un conjunto de buenas prácticas para la gestión de la información creado por ISACA (Information Systems Audit and Control Association, Asociación para la Auditoría y Control de sistemas de información) con el apoyo del Instituto de Administración de las Tecnologías de la Información (IT Governance Institute), en el año 1992. (Giraldo Martínez, De la Torre Morales, & Villalta Gómez, 2012)

2.6.1. Descripción.

COBIT fue creado con la finalidad de proporcionar una guía que garantice el control y gestión adecuados de las tecnologías de la información, con el objetivo de alcanzar los objetivos del plan de negocio de cualquier organización. Por lo tanto, COBIT es un soporte de apoyo para las instituciones que abarca un conjunto de herramientas que permiten a los administradores cubrir los requerimientos de control, cuestiones técnicas y los riesgos del negocio dentro de todos los niveles de la organización y partes interesadas. (IT Governance Institute, 2007)

COBIT proporciona un marco referencial de soporte que podemos observar en la Figura 3, que garantiza:

- TI está alineada con el negocio
- Permite que el negocio maximice los beneficios de TI

- Los recursos de TI se utilizan de forma responsable
- Los riesgos de TI se manejen de forma adecuada

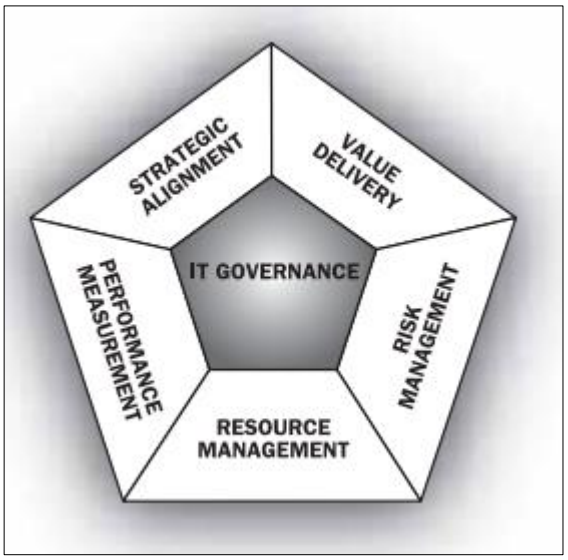


Figura 3: Áreas de enfoque de COBIT

Fuente: IT Governance Institute (2007). COBIT (Control Objetives for information and related Technology). Rolling Meadows: Algonquin Road.

Alineamiento estratégico se centra en:

- garantizar la vinculación de negocio con los planes de TI;
- definir, mantener y validar la propuesta de valor de TI; y
- la alineación de las operaciones de TI con las operaciones de la institución. (IT Governance Institute, 2007)

La distribución de valor se trata de la ejecución de la propuesta de valor a lo largo del ciclo de entrega, asegurando que la tecnología ofrece los beneficios prometidos, concentrándose en la optimización de costos y demostrando el valor intrínseco de TI. (IT Governance Institute, 2007)

Gestión de recursos se trata de la inversión óptima, y la gestión adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. (IT

Governance Institute, 2007)

La gestión del riesgo requiere de la comunicación de los riesgos a los altos funcionarios de la institución, la comprensión de los requisitos de cumplimiento, la transparencia acerca de los riesgos significativos para la institución y la determinación de las responsabilidades de gestión de riesgos en la organización. (IT Governance Institute, 2007)

La medición del rendimiento y monitoreo de las estrategias de implementación, son necesarias para la terminación de proyectos, uso adecuado de recursos, rendimiento del proceso y de prestación de servicios de la institución. (IT Governance Institute, 2007)

2.6.2. Marco COBIT 5.

COBIT 5 se presenta ante las empresas como una ayuda para obtener un valor óptimo en los aspectos de TI, incrementando los beneficios y reduciendo los riesgos.

COBIT 5 tiene un punto de vista que se enfoca en administrar la información y todo aquello que se relacione a tecnologías y sistemas de información. Para lograr sus objetivos estable principios y habilitadores genéricos que guían a los administradores de red en procesos de buenas prácticas para la seguridad de la información.

CAPÍTULO III

ANÁLISIS DE LA SITUACIÓN ACTUAL

En este capítulo se hace un estudio de la estructura física, distribución de departamentos, servicios prestados por la cooperativa, activos de información, red de datos y espacio físico del cuarto de telecomunicaciones para el establecimiento de las fortalezas, amenazas, oportunidades y debilidades.

3.1. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

La COAC Chuchuqui, cuenta con una estructura de red, donde se manejan o funcionan varios sistemas relacionados con bases de datos financieras, por lo cual, en todo el tiempo de atención de la institución, se encuentra realizando distintos tipos de transacciones, lo que hace que las bases de datos varíen considerablemente en un solo día, y que los servidores que conforman la red estén trabajando constantemente. Todo esto hace que surja la necesidad de que todos los elementos principales de la red, deben mantenerse monitoreados y estar respaldados de controles de seguridad, de lo cual carece la cooperativa.

La topología de red no se encuentra bien definida, ya que el personal del departamento de tecnología es nuevo y no existen registros del diseño de la red, lo que dificulta la localización de los puntos de red, además de que no cuentan con el etiquetado de los cables.

También existen ciertas falencias en la parte de la seguridad física para los equipos de red, tanto para los que se encuentran dentro del Centro de Datos, como los equipos de red de conexión intermedia, dejando a los equipos vulnerables para cualquier tipo de amenaza.

La institución se encuentra en un proceso de mejoramiento del Plan de negocio en todos los aspectos, por lo cual la documentación es uno de los principios muy importantes que se debe considerar cuando se en un proceso de cambio, así como también es necesario que se realice una evaluación de riesgos, amenazas y vulnerabilidades de forma periódica.

La implementación de un plan de contingencia informático ayuda a que la institución se encuentre preparada para afrontar cualquier tipo de amenaza, y dar respuesta a cualquier problema con la finalidad de mantener la continuidad del plan de negocio, manteniendo un porcentaje de disponibilidad aceptable, tanto para beneficio de los clientes como de la cooperativa en sí.

Información más específica sobre la situación actual de la cooperativa se ve reflejada en el desarrollo del análisis FODA en la parte de Análisis de riesgos del Plan de Contingencia en el capítulo IV (ver Tabla 11), donde se ha analizado el estado de los controles de seguridad basado en la norma ISO/IEC 27002.

3.1.1. Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda.

La COAC Chuchuqui Ltda. se encuentra ubicada en la ciudad de Otavalo, Parroquia San Luis; ésta es una institución financiera creada con el propósito de participar en la búsqueda de soluciones para problemas sociales y económicos de sus clientes, además de brindar servicios financieros y no financieros de calidad, adaptándose a las necesidades del sector. (COAC Chuchuqui Ltda., 2016)

La cooperativa fue creada en el año 1985 y adquiere valor jurídico en septiembre de 1986 con Acuerdo Ministerial No 86-141-DC Reg # 5259 DGC, gracias a la unión de personas comerciantes, artesanas y panaderas del sector. Actualmente se encuentra ubicada en la calle Bolívar 8-05 y Juan Montalvo de la ciudad de Otavalo con su propia infraestructura. (COAC Chuchuqui Ltda., 2016)

Gracias a la confianza depositada por los ciudadanos no solo del cantón Otavalo sino de las demás provincias adyacentes, la Cooperativa está al servicio de más de 80 comunidades rurales, con un Activo de 13´500.000 hasta la fecha y con 9000 socios. A fin de mejorar el servicio al desarrollo social, la cooperativa ha mejorado su organigrama funcional, dando una mejor atención a las necesidades de sus socios. (COAC Chuchuqui Ltda., 2016)

3.1.1.1. Misión Institucional

“Somos una Cooperativa de Ahorro y Crédito confiable, segura, solidaria con años de experiencia en la prestación de servicios financieros oportunos para el desarrollo

social. Sustentados en principios cristianos, impulsamos el crecimiento económico de socios y grupos emprendedores, con personal eficiente y competente."

3.1.1.2. Visión Institucional

"Ser la mejor opción en el sector financiero popular y solidario de la Provincia de Imbabura, alcanzar un alto reconocimiento y nombramiento por la prestación de servicios de calidad, con personal comprometido y especializado, innovar los servicios de acuerdo a las necesidades de nuestros socios"

3.1.2. Servicios prestados por la COAC Chuchuqui Ltda.

La Cooperativa Chuchuqui Ltda., al tratarse de una institución financiera privada, brinda diferentes servicios con la finalidad de impulsar el crecimiento económico de sus socios y grupos emprendedores, con personal eficiente y competente.

En la Tabla 1 se muestran los distintos servicios que ofrece la cooperativa:

Tabla 1. *Servicios prestados por la COAC Chuchuqui Ltda.*

SERVICIOS PRESTADOS POR LA COAC CHUCHUQUI LTDA.	
Ahorros	**Créditos**
• Ahorro a la vista	• Crédito de consumo
• Ahorro Chuchuquito	• Microcrédito
• Inversiones	• Crédito PYMES

Fuente: http://www.coopchuchuqui.fin.ec

3.1.3. Servicios consumidos por la COAC Chuchuqui Ltda.

Como toda institución, para el desarrollo de las actividades de la COAC es necesario que cuente con la disponibilidad de los servicios que se muestran en la Tabla 2. Dentro de estos servicios se consideran los de primera necesidad como agua potable, luz y teléfono, pero también es necesario nombrar los servicios que la cooperativa consume constantemente ya sea de proveedores, empresas contratistas o terceras personas que se consideren de importancia.

Tabla 2. Servicios consumidos por la COAC Chuchuqui Ltda.

Contacto	Servicio	Número Telefónico
EMELNORTE	Electricidad	062-997100
EMAPA	Agua Potable	062-906 823
IEES	Seguridad Social	062-605592
CNT	Internet	06-2920-040
ECU 911	Emergencias	911
Webcoop	Mantenimiento de Sistemas Financieros	02-2081-266
Seyton	Soluciones Electrónicas y Telecomunicaciones	06-2607-949
Inforc-Ecuador	Seguridad Informática	02-2559-067 / 02-2227-766
Domotik	Ingeniería en Automatización y Seguridad	07-286-1630 / 0993779763
Word Computer	Proveedor de Hardware	06-2608-010
Akross	Soporte y Soluciones Tecnológicas	02-4008-300 / 400 - 8300
Equifax	Estado Crediticio de Socios	26020083 / 0986193984
Banco Central del Ecuador	Servicios Bancarios	Call Center: 1700 153 -153 / 02-3938-600

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

3.1.4. Activos de Información.

En la actualidad para toda institución, la información ha pasado a ser el activo con el valor más significativo, por lo cual deben existir varias metodologías para su adecuado almacenamiento y protección. La información de una organización se la puede encontrar en distintas maneras, puede ser documentos impresos, en unidades digitales de almacenamiento, discos extraíbles, en bases de datos de los servidores etc.

Con la finalidad de evitar pérdidas es necesario contar con controles de seguridad, que garanticen los principios de la información (confiabilidad, integridad y

disponibilidad). La COAC no cuenta con todos los controles necesarios que certifiquen que la información se encuentra segura, por ejemplo, en la Figura 4 se observa la falta de gabinetes para los equipos de conexión intermedia. Se ha realizado un análisis de los controles, basándose en la norma técnica ISO/IEC 27002, el cual se encuentra detallado en el punto 4.7.3. referente al análisis FODA.

Figura 4: Equipos de conexión intermedia sin protección.
Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Con la ayuda del análisis FODA se puede tratar de cubrir los aspectos negativos para la seguridad de la información, sabiendo aprovechar los controles ya existentes, por ejemplo, los discos extraíbles, discos duros y backups de la COAC se encuentran protegidos en la bóveda de la institución, ya que este es el lugar más seguro.

3.1.5. Red de datos.

La COAC Chuchuqui cuenta con una red de datos interna de cableada hacia los distintos departamentos que la conforman, y una inalámbrica únicamente para dispositivos autorizados por el Departamento de Tecnología, el enlace es de 6 Mbps. En Tabla 3 se encuentra una descripción de las redes de comunicación.

Tabla 3. *Redes de comunicación de la COAC Chuchuqui.*

RED	DESCRIPCIÓN
Red Local	Está conformada por la red cableada categoría 5e.
Red Wireless	Está conformada por la red inalámbrica distribuida exclusivamente para la 2da planta alta y la 3ra planta alta.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

La topología de red no se encuentra establecida adecuadamente, incluso es difícil deducir el tipo de topología que está empleando, debido a que no existe etiquetado, la distribución hacia las diferentes plantas de la institución no es adecuada ya que no posee un switch de distribución para cada piso como se muestra en la Figura 5: *Topología de red de la COAC Chuchuqui Ltda.* El proveedor del servicio de internet es CNT EP, que suministra mediante fibra óptica monomodo de 6 hilos.

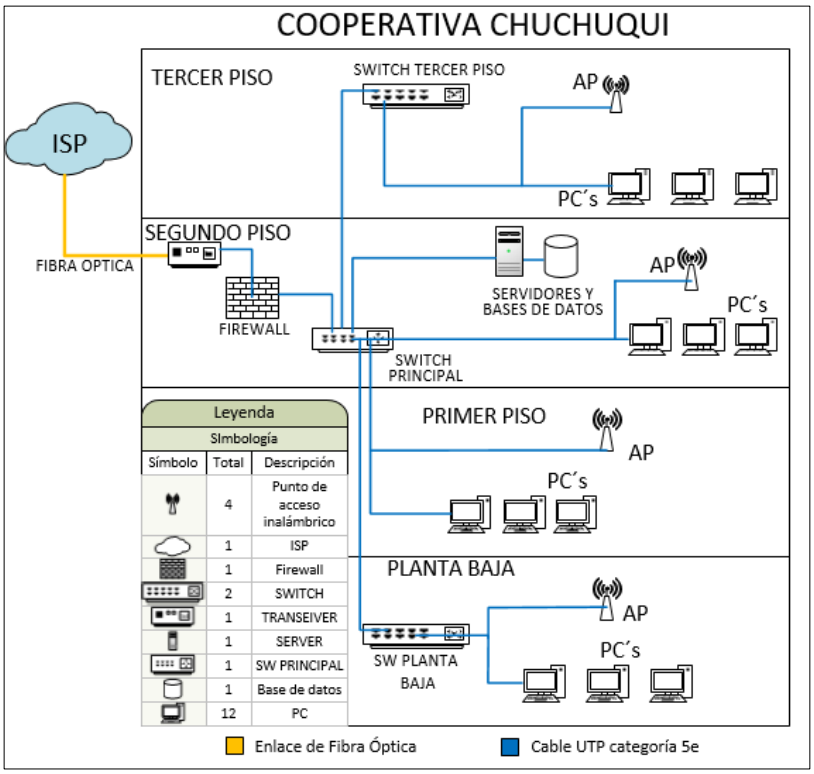


Figura 5: Topología de red de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

La estructura de red y el cableado estructurado lleva varios años sin ser modificado ni renovado, por lo cual existe la necesidad de establecer una nueva topología de red que garantice la seguridad de la información, considerando las diferentes normas de cableado estructurado.

La norma ANSI/EIA/TIA 569 C nos habla sobre el espaciado para el manejo de equipos y es una característica que no se ha tomado en cuenta en la distribución de los equipos en la COAC Chuchuqui Ltda., esta norma nos especifica que se debe proporcionar un espacio libre posterior de 0,6 m (2 pies) para el acceso de servicio en la parte posterior de bastidores y gabinetes, pero es mayormente recomendable tener un

espacio posterior de 1 m (3 pies) para mejor manejo de dispositivos. (ANSI/TIA, 2012)

Otra norma con la que no cumple la COAC Chuchuqui es la ANSI/EIA/TIA 568 C.1-1 la cual especifica como diseñar un sistema de cableado de telecomunicaciones para edificios comerciales, además de los espacios que se deben manejar en áreas de trabajo también se muestra la forma de planificar, distribuir espacios e instalar medios de transmisión. (ANSI/TIA, 2012)

3.1.6. Cuarto de Telecomunicaciones.

El área del Data Center se encuentra ubicado en la 2da planta alta de la COAC y es de $9m^2$. Está conformado por un gabinete de piso donde se alojan los equipos de networking, 4 servidores tipo torre, 1 servidor tipo rack y una central telefónica analógica Panasonic, también contiene un UPS de 6KVA no administrable, 1 servidor tipo PC fuera del gabinete y un sistema de protección eléctrica.

El Data Center carece de un sistema de aire acondicionado, por lo que las temperaturas del cuarto son elevadas, también carece de una puerta de seguridad y un biométrico para acceso sólo a personas autorizadas, como se puede observar en la Figura 6. En este cuarto también existe una ventana, lo cual no es recomendable para un Data Center, en la Figura 7 se muestra la ventana vista desde el interior del Data Center.

Figura 6: Puerta de Acceso al Data Center
Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Figura 7: Ventana en el interior del Data Center de la COAC Chuchuqui Ltda.
Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Además, el Data Center debe mejorar en aspectos de la alimentación de energía eléctrica como se muestra en la Figura 8, también en la pintura empleada en las paredes e incrementar rótulos informativos de seguridad industrial.

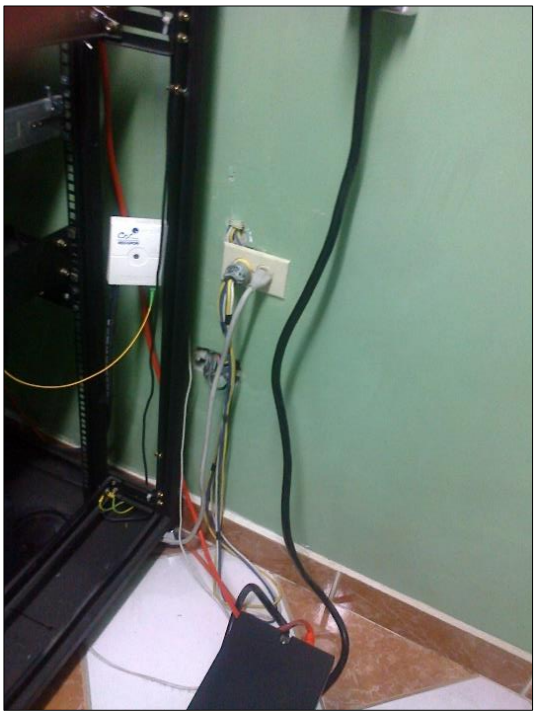


Figura 8: Fuente de alimentación para equipos en el Data Center de la COAC Chuchuqui Ltda.
Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

3.1.7. Servicios del Departamento de Tecnología.

El Departamento de Tecnología está conformado por 2 personas, en la Tabla 4 se puede observar el cargo y las funciones correspondientes.

Tabla 4. *Personal del Departamento de Tecnología de la COAC Chuchuqui Ltda.*

CARGO	ENCARGADO	FUNCIONES
Jefe de Tecnología	Ing. Darío Castañeda	Elaborar, proponer y ejecutar el Plan Estratégico y Operativo de Sistemas como parte integrante del Plan Estratégico Institucional. Identificar, priorizar, especificar y ejecutar los requerimientos funcionales y técnicos de las áreas o departamentos de la Institución, a fin de lograr los resultados esperados de los proyectos del área de Sistemas. Implementar, desarrollar, monitorear y evaluar los proyectos informáticos, del área de Sistemas. Establecer y mantener una estructura óptima de relación, comunicación y coordinación entre la funcionalidad de la Tecnología Informática y otros usuarios dentro y fuera de la Institución. Establecer las relaciones y responsabilidades bilaterales con proveedores calificados de servicios tecnológicos especializados, monitoreando la prestación de estos servicios, para la verificación y aseguramiento del cumplimiento de los convenios adquiridos. Elaborar conjuntamente con el área Administrativa Financiera el presupuesto del departamento. Revisar la correcta elaboración y actualización de los manuales del usuario. Proponer y aplicar, normas y políticas competentes al departamento de sistemas y tecnología. Planear y organizar el mantenimiento, soporte y asesoría técnica requerida por las áreas de la Institución. Atender los requerimientos tecnológicos de entes de control interno y externo. Administrar la infraestructura tecnológica cuidando su integridad y buen funcionamiento. Asegurar el correcto funcionamiento del sistema informático incluyendo los servicios de internet e integrados para transmisión de datos. Asegurar la disponibilidad, integridad y protección (respaldos) oportuna de la información de la institución. Proponer mejoras en el funcionamiento de los sistemas actuales conforme a los requerimientos institucionales. Elaborar y aplicar planes de contingencia orientados al mantenimiento de la continuidad del sistema en el caso de que se presenten emergencias. Realizar evaluaciones periódicas del uso y asignación de los activos de la Tecnología Informática.
Asistente de Tecnología	Ing. Marcelo Yamberla	Apoyar en el seguimiento del Plan Estratégico y Operativo del Sistema como parte integrante del Plan Estratégico Institucional. Monitorear y verificar el buen funcionamiento de los

	equipos de comunicación (Router y switch y las líneas RDSI) de las Oficinas. Apoyar en la administración del Firewall y velar por su buen funcionamiento. Realizar mantenimiento preventivo a los equipos de cómputo de acuerdo al Programa Anual de Mantenimiento. Mantener actualizado el inventario de los equipos de cómputo y comunicaciones, así como del software instalado en las Oficinas de la Cooperativa. Apoyar en los requerimientos tecnológicos de entes de control interno y externo. Apoyar el cumplimiento de las medidas de seguridad establecidas tanto para la seguridad física del personal, instalaciones, equipos, recursos, y contribuir decididamente a la seguridad de la información y recursos informáticos. Coordinar con el proveedor de servicios de comunicaciones y transmisión de datos la reanudación de los servicios, en el caso de interrupciones en los enlaces principales y de contingencia. Atender los requerimientos de los usuarios en el caso de fallas en el funcionamiento estaciones de la red, tanto en hardware y software. Realizar mantenimiento preventivo a los equipos de cómputo de acuerdo al Programa Anual de Mantenimiento. Participar activamente en la implantación, ejecución, prueba y actualización de los planes de contingencia.

Fuente: Departamento Administrativo y de Talento Humano de la COAC Chuchuqui Ltda.

Los servicios que presta el Departamento de Tecnología se ven reflejados en las funciones que realiza el personal. Se reflexiona que todas estas funciones son excesivas para la cantidad de personal de este departamento por lo que se recomienda que se tome en consideración el incremento del personal para esta área, tomando en cuenta que existen otros roles que garanticen la seguridad de la información.

3.1.8. Controles de seguridad.

Para el levantamiento de información sobre los controles de seguridad existentes y no existentes de la COAC Chuchuqui, se lo ha realizado basándose en los controles expuestos en la norma técnica ISO/IEC 27002 y empleando el formato del ANEXO A: FORMATO PARA LEVANTAMIENTO DE INFORMACIÓN DE CONTROLES DE SEGURIDAD, en el cual se establecen algunos parámetros de estado actual y clasificación de estos controles, lo que ayuda al desarrollo del análisis FODA.

Para la clasificación de los controles de seguridad se considera las áreas que se ven afectadas. En el caso de que el control no se encuentre aplicado se analizará si las repercusiones ameritan que se clasifique como una debilidad o como una amenaza, tomando en cuenta los ejemplos que nos brinda la norma técnica ISO/IEC 27005 referente al análisis de riesgos.

En el ANEXO B se muestran 10 ejemplos del levantamiento realizado para los controles de seguridad en la cooperativa, debido a que el total de controles examinados es 69, pero con los ejemplos se puede tener una idea precisa del proceso de levantamiento de información.

3.1.9. Estructura organizativa de la COAC Chuchuqui Ltda.

En la Figura 9 y Figura 10 se encuentra el organigrama estructural y el organigrama funcional de la COAC Chuchuqui Ltda., respectivamente. Esta estructura es necesaria conocerla para el desarrollo del Plan de Contingencia, ya que nos permite conocer las personas responsables para cada área y de esta forma poder asignar responsabilidades que garanticen la seguridad de la información.

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

ORGANIGRAMA ESTRUCTURAL

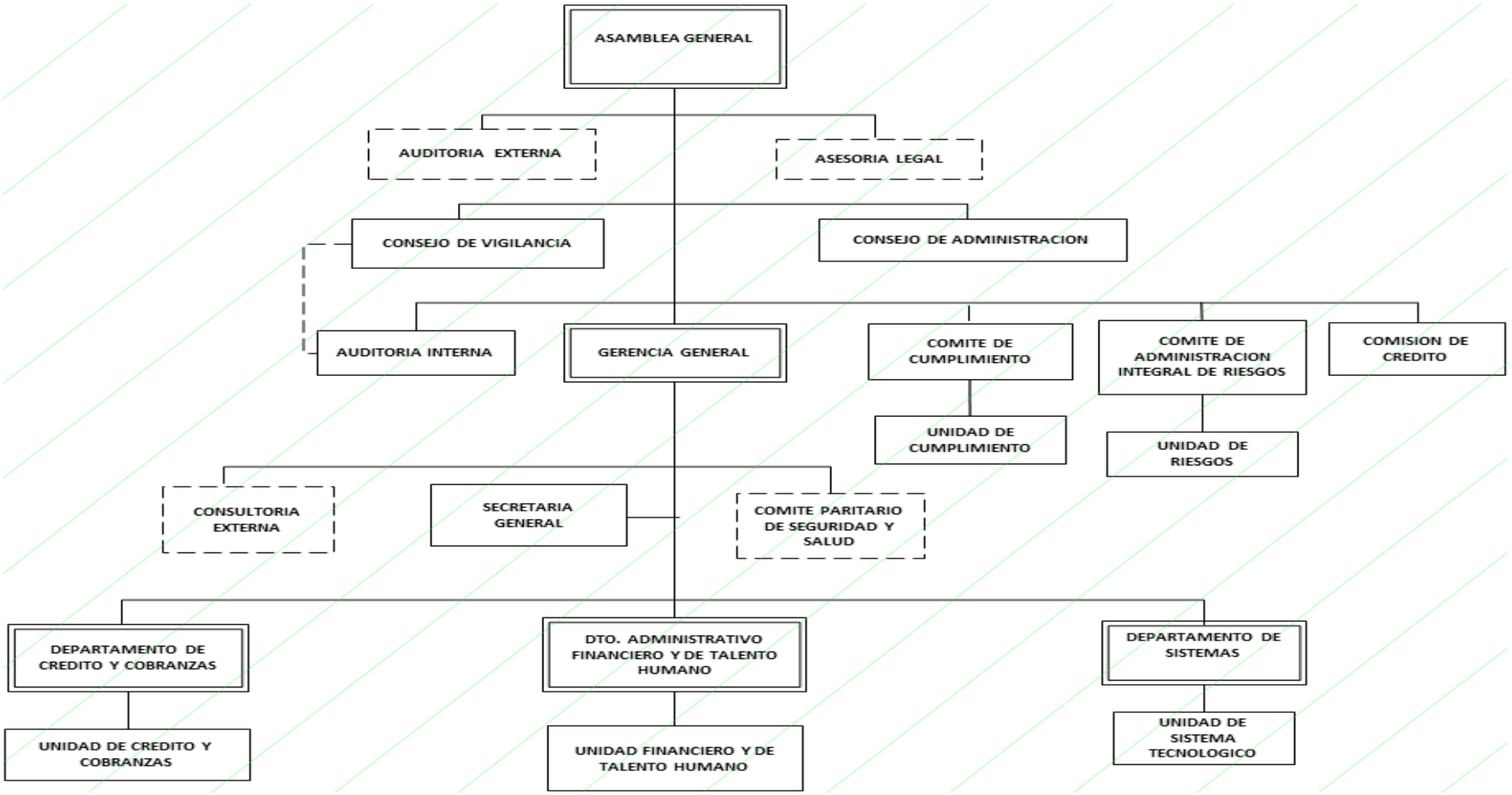


Figura 9: Organigrama Estructural

Fuente: COAC Chuchuqui Ltda.

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

ORGANIGRAMA FUNCIONAL

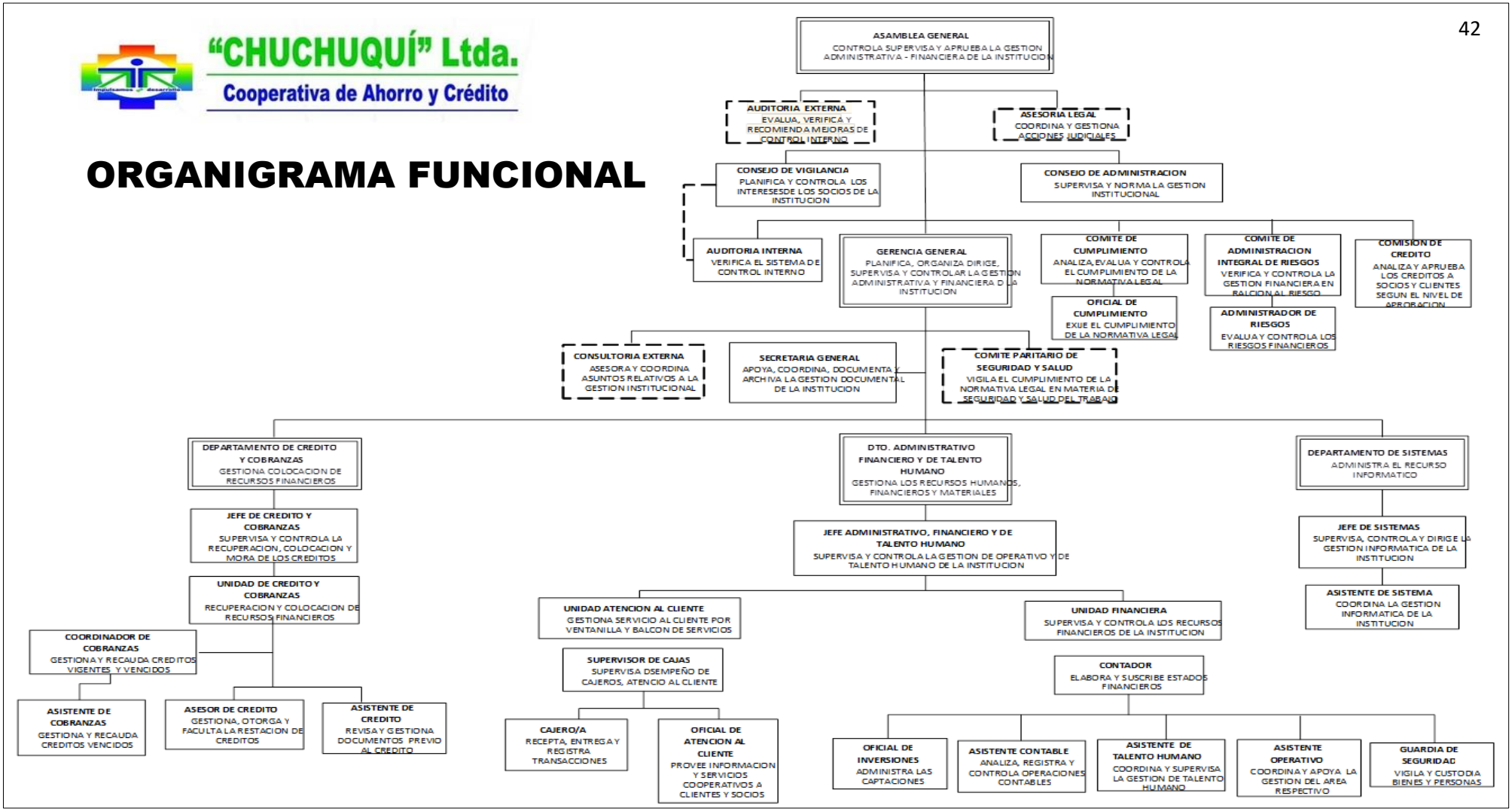


Figura 10: Organigrama Funcional

Fuente: COAC Chuchuqui Ltda.

CAPÍTULO IV

DESARROLLO DEL PLAN DE CONTINGENCIA

En este capítulo se encuentra el desarrollo de la parte teórica del Plan de Contingencia, en que se explica el procedimiento que se debe seguir para la implementación del mismo. Toda la información presentada en este capítulo tiene como finalidad el instaurar parámetros que ayuden al proceso de corregir los aspectos negativos encontrados en el análisis de la situación actual detallada en el capítulo anterior.

"CHUCHUQUÍ" Ltda.

Cooperativa de Ahorro y Crédito

DEPARTAMENTO DE TECNOLOGÍA

PLAN DE CONTINGENCIA INFORMÁTICO

VERSIÓN 1.0
NOVIEMBRE, 2016

COOPERATIVA DE AHORRO Y CRÉDITO DE INDIGENAS "CHUCHUQUI" LTDA.		
PLAN DE CONTINGENCIA Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN		
"CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**Versión:**	1.0
	Revisado por:	Ing. Darío /Jefe Departamento de Tecnología. Ing. Marcelo Yamberla / Asistente de Tecnología
	Aprobado por:	Ing. Darío /Jefe Departamento de Tecnología
	Fecha de aprobación:	24 de septiembre de 2016 - Acta 318 R (31)

4.1. PROPÓSITO

Para la cooperativa de Ahorro y Crédito de Indígenas "CHUCHUQUI" Ltda., es indispensable acudir a los recursos de Tecnologías de la Información y Comunicaciones (TICs) como un medio para proporcionar los servicios que la Cooperativa ofrece a la ciudadanía y es de vital importancia que dicha información sea lo más exacta y explícita posible.

Es importante resaltar que la Cooperativa de Ahorro y Crédito, necesita garantizar tiempos de indisponibilidad lo más breves posibles, tanto en sus equipos informáticos como en el resto de recursos de comunicaciones, para poder alcanzar sus objetivos institucionales; y así de esta manera poder conservar una productividad eficiente en todas las áreas administrativas y de operación.

Por todo lo anteriormente expuesto, el estar fuera de servicio la plataforma informática o el sistema financiero por un lapso mayor de 1 hora origina distorsiones al normal desarrollo de las actividades y funcionamiento de nuestros servicios. De continuar la situación de indisponibilidad por un tiempo mayor, el riesgo al que se expone puede paralizar las operaciones por falta de información para el control y ejecución de servicios financieros de la Cooperativa.

Es de gran necesidad, por tanto, prever cómo proceder y qué recursos emplear ante una situación de contingencia con la finalidad de que su impacto en las

actividades sea lo menos crítico posible.

Nota: Cabe recalcar que la Cooperativa ingresa en una situación de contingencia cuando los equipos de TI o el sistema financiero están fuera de servicio por más de 1 hora según lo que se establece en los tiempos aceptables de caída de los servicios y termina cuando se restablece el ambiente de procesamiento normal y el desarrollo normal de sus actividades.

4.2. INTRODUCCION

El presente documento es el ***Plan de Contingencia Informático*** de la Cooperativa de Ahorro y Crédito "CHUCHUQUI" Ltda., en materia de Riesgos de Tecnología de la Información basado en la norma ISO/IEC 27002.

Establece el objetivo, alcance y metodología utilizada. Además, incluye las definiciones utilizadas, el análisis de la situación, dominios de seguridad, el análisis de sensibilidad de la información manejada, la identificación de los riesgos y controles, y la clasificación de activos IT.

4.3. METODOLOGÍA

El método de investigación que se emplea es el Análisis FODA, tomando en cuenta que, para los procesos de planificación estratégica, esta metodología es muy utilizada debido a su sencillez y además la forma de obtención de la información permite tomar decisiones acertadas en la proyección del desarrollo de las organizaciones.

FODA es el acrónimo de cuatro nociones: Fortalezas, Oportunidades, Debilidades y Amenazas. Esta metodología radica en establecer estrategias en las que la organización emplea las Fortalezas para aprovechar las Oportunidades, reducir las debilidades y afrontar las amenazas. (Orlich, 2013)

Para el análisis de los riesgos y evaluación de los mismos se basa en la metodología de la Norma ISO 27005:2008 y el plan de mantenimiento ha sido elaborado tomando en cuenta los Dominios de Seguridad establecidos en la norma ISO/IEC 27002:2013.

Finalmente, se presentan los anexos como parte complementaria lo cual ayuda a estar preparados frente a cualquier contingencia en los procesos críticos.

4.4. CONCEPTOS PRELIMINARES

- **Contingencia:**

  Anomalía no planificada en la disponibilidad de recursos informáticos.

- **Plan de contingencia:**

  Conjunto de medidas de PREVENCIÓN, DETECCIÓN y de REACCIÓN a poner en marcha ante la presentación de una contingencia.

- **Activo:**

  Cualquier cosa que tenga valor para la organización.

  [ISO/IEC 13335-1:2004]

- **Control**

  Forma de gerenciamiento un riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica de gestión o legal.

  Nota: *control también es tomado como sinónimo de protección o contramedida.*

- **Directriz**

  Descripción que orienta o que deben ser tomados en cuenta, para alcanzar los objetivos establecidos en las políticas.

  [ISO/IEC 13335-1:2004]

- **Recursos de procesamiento de información**

  Cualquier sistema de procesamiento de información, servicio o infraestructura, o las instalaciones físicas que los alberguen.

- **Seguridad de información**

  Preservación de la confiabilidad, integridad o disponibilidad de la información; adicionalmente, otras propiedades como, autenticación, responsabilidad, no repudio y confiabilidad, también pueden estar contenidas.

- **Evento de seguridad de la información**

  Ocurrencia identificada en un sistema, servicio o red, que indica una posible violación de alguna política de seguridad de la información o falla de controles, o una situación previamente desconocida, que pueda ser relevante para la seguridad de la información.

  [ISO/IEC TR 18044:2004]

- **Incidente de la seguridad de la información**

  Un incidente de seguridad de la información está indicado por uno o varios eventos de seguridad de la información inesperados, que tengan una gran probabilidad de comprometer las operaciones de negocio y amenazar la seguridad de la información.

  [ISO/IEC TR 18044:2004]

- **Impacto**

  Cualquier cambio que afecte a los objetivos del negocio de una organización.

  [NTC-ISO 27005:2008]

- **Comunicación del riesgo**

  Hacer un intercambio o compartir información sobre un riesgo de parte de los interesados hacia la persona encargada de tomar decisiones o viceversa.

  [NTC-ISO 27005:2008]

4.5. ESTRUCTURA

En la Figura 11, se puede observar las etapas en las que se encuentra dividido el Plan de Contingencia.

Figura 11: Etapas del Plan de Contingencia

Fuente: Elaboración propia.

- Análisis de riesgos

  Antes de que suceda una eventualidad, cualquier institución debe tratar de mitigar los impactos mediante un análisis de riesgos, este procedimiento es indispensable para empezar a desarrollar un Plan de Contingencia y tener una idea de cómo enfrentarse a un incidente.

  En este punto se analizarán los riesgos de un impacto y dependiendo de estos se otorgará un nivel de prioridad y se establecerá que tipo de sub-plan es el más adecuado para ponerlo en marcha.

En la Tabla 5 se puede observar una descripción de los cuatro sub-planes contenidos en el Plan de Contingencia, los cuales se accionarán dependiendo del tipo de eventualidad y estimación de riesgos.

- Pruebas de verificación y evaluación:

Antes de que un Plan de Contingencia sea aprobado por un consejo directivo, éste debe ser sometido a una serie de pruebas, para comprobar que los procedimientos propuestos en dicho plan, obtengan los resultados esperados, para ello el personal debe estar entrenado en los distintos escenarios de prueba. Al final se realizará un análisis de los resultados y se determinará si el Plan es el adecuado para la institución.

Tabla 5: *Sub-planes de Contingencia*

	EMERGENCIA	**RESTAURACIÓN**	**RECUPERACIÓN**	**MANTENIMIENTO**
OBJETIVO	Limitar los daños	Continuar procesos	Recuperación total de los procesos	Prevenir daños
ACTUACIÓN	Inmediata	Inmediata	A corto plazo	Continuamente
CONTENIDO	Evacuación y evaluación de daños	Alternativas para los procesos significativos	Estrategias para la recuperación de todos los recursos	Reglamentos, normas, políticas de seguridad
RESPONSABILI-DAD PRINCIPAL	Usuarios y empleados de la cooperativa	Departamento de Tecnología y WEBCOOP	Departamento de Tecnología	Usuarios y empleados de la cooperativa

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

4.6. ELEMENTOS INDISPENSABLES EN UN PLAN.

Los elementos indispensables con los que debe contar un Plan de Contingencia se los enlista a continuación:

a. Consenso

- Planes aprobados por el Consejo Administrativo de la Cooperativa.
- Planes elaborados con el apoyo de los empleados de la Cooperativa.
- La asignación de prioridades para las eventualidades debe haber sido tratada con anterioridad por las tres partes implicadas (Consejo Administrativo, Departamento de Tecnología y Empleados).

b. Recursos

- Equipos con "hardware" y "software" adecuados.

- Copias de seguridad actualizadas (Disco Duro externo).

c. Pruebas

- Validación de las copias de seguridad.
- Simulacros de emergencia (una vez por año como mínimo), de preferencia en cooperación con instituciones de apoyo (bomberos, policía nacional).
- Capacitación del personal.

COOPERATIVA DE AHORRO Y CRÉDITO DE INDIGENAS "CHUCHUQUI" LTDA.		
ANÁLISIS DE RIESGOS		
"CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**Revisado por:**	Ing. Darío Castañeda/Jefe Departamento de Tecnología. Ing. Marcelo Yamberla / Asistente de Tecnología
	Aprobado por:	Ing. Darío Castañeda /Jefe Departamento de Tecnología
	Fecha de aprobación:	24 de septiembre de 2016 - Acta 318 R (31)

4.7. ANÁLISIS DE RIESGOS

4.7.1. Identificación del riesgo.

El propósito principal de la identificación del riesgo es que cualquier organización esté en la capacidad de poder anticiparse a lo que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Los pasos que se van a desarrollar a continuación, deberían ayudar a recolectar datos de entrada para la actividad de estimación del riesgo. En la Figura 12 se puede observar los porcentajes de distintos tipos de riesgos a los que se encuentran expuestos los sistemas de información. (NTC/ISO/IEC 27005, 2008)

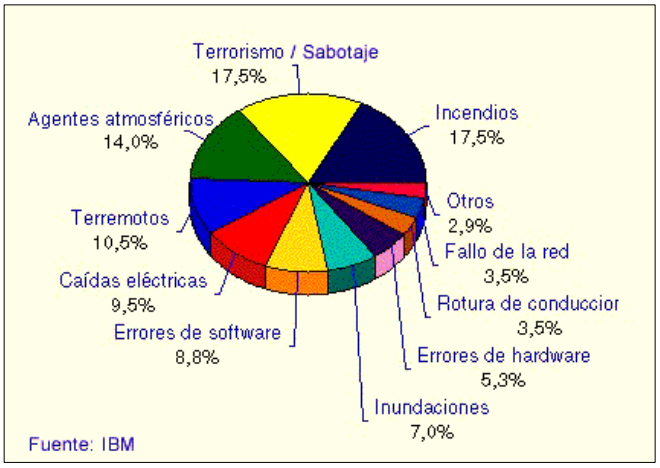


Figura 12: Riesgo a los cuales se encuentran inmersos los Sistemas de Información

Fuente: Sánchez A. (2012). Resguardar Información: Clasificación de respaldos de la información. Recuperado el 24 de noviembre de 2016 de: http://azaleasanchez-resguardarinformacion.blogspot.com/2012/02/clasificacion-de-respaldos-de-la.html

4.7.1.1. Identificación de los Activos.

Un activo se puede deducir como todo aquello que tiene valor para una institución y que, por lo tanto, necesita un cuidado especial. Para la correcta identificación de los activos es recomendable que se tome en cuenta que, los sistemas de información no solo constan hardware y software, sino que contiene más elementos. (NTC/ISO/IEC 27005, 2008)

Un nivel adecuado de detalles es un aspecto muy importante en la identificación de los activos, para ayudar a proporcionar la información necesaria para la valoración del riesgo. El nivel de especificaciones utilizadas en la identificación de los activos tendrá influencia en la cantidad total de referencias recogidas durante la valoración del riesgo. (NTC/ISO/IEC 27005, 2008)

Cada activo debe contar con un propietario o encargado asignado, para establecerle la responsabilidad, compromiso y la rendición de cuentas sobre éste. Dicho propietario puede no tener derechos de posesión sobre el activo, pero tiene la responsabilidad de su producción, progreso, subsistencia, uso y seguridad, según concierna. El propietario del activo con generalmente es la persona más indicada para determinar el valor que el activo tiene para la institución. (NTC/ISO/IEC 27005, 2008)

En el inventario de activos de la cooperativa realizado por el Departamento de Tecnología, se encuentran todas las especificaciones necesarias y actualizadas, que pueden colaborar con el desarrollo del Plan de Contingencia.

4.7.1.2. Identificación de Amenazas.

Para que una eventualidad sea considerada como amenaza, debe tener el potencial de causar daños a activos tales como sistemas, procesos e información y, por lo tanto, a la continuidad de negocio de la institución. Las amenazas pueden proceder de varios orígenes, tales como natural o humano y podrían ser accidentales o intencionales; todas estas deben ser examinadas detalladamente ya que puede tratarse de falsas alarmas que se dan concurridamente. Es necesario identificar tanto los orígenes de las amenazas accidentales como de las intencionales. Una amenaza puede tener su origen dentro o fuera de la organización. (NTC/ISO/IEC 27005, 2008)

Ninguna amenaza debe pasarse por alto, incluidas las inesperadas, aunque después de que sean analizadas y sean descartadas como amenazas potenciales, ya que gracias a sus registros se pueden eliminar vulnerabilidades en la red. Existen amenazas que pueden afectar a más de un activo lo que hace que los impactos sean más graves para la institución. (NTC/ISO/IEC 27005, 2008)

La Norma ISO/IEC 27005 nos brinda una lista de ejemplos de lo que se puede considerar como amenaza dentro de una organización y la se encuentra detallada en el ANEXO C: TIPOS DE AMENAZAS. El resultado de la identificación de amenazas se encuentra plasmado en tabla de resultados del análisis FODA (ver Tabla 11).

4.7.1.3. Identificación de los controles existentes.

La identificación de los controles existentes es muy útil para cualquier organización que se encuentre en un proceso de mejoramiento de la seguridad de la información, ya que evita el trabajo o costos innecesarios, por ejemplo, en la repetición de los controles. Incluso, en el proceso de identificación de los controles existentes se recomienda realizar una verificación para garantizar que los controles propuestos funcionan correctamente. Si el control no cumple con lo esperado, puede que dé lugar al aprovechamiento de las vulnerabilidades. (NTC/ISO/IEC 27005, 2008)

De acuerdo con ISO/IEC 27001, en un SGSI se tiene como herramienta de apoyo a la revisión de la eficacia del control. Una manera de apreciar el efecto del control es ver la forma en que disminuye la probabilidad de ocurrencia de la amenaza y el incremento de dificultad para explotar una vulnerabilidad. En este caso, los reportes de auditoría también proveen información valiosa sobre de la eficacia de los controles. (NTC/ISO/IEC 27005, 2008)

Los controles es algo que requiere una planificación minuciosa, para implementar de acuerdo con las exigencias del tratamiento del riesgo, para ello se debería dar la misma importancia que aquellos ya se encuentran implementados. Hay casos en los que un control existente o planificado se puede considerar como insuficiente, innecesario, ineficiente o injustificado. Por lo cual el análisis debería garantizar la eficacia del control o caso contrario se debe eliminar o reemplazar por uno más eso si siempre tomando en cuenta la relación costo beneficio. (NTC/ISO/IEC 27005, 2008)

El resultado de la identificación de los controles existentes se encuentra plasmado en tabla de resultados del análisis FODA (ver Tabla 11), y se los puede encontrar en el concepto de fortalezas.

4.7.1.4. Identificación de las vulnerabilidades.

Para la identificación de las vulnerabilidades existen varias áreas de estudio:

- distribución;
- tecnologías y procedimientos;
- operaciones de gestión;
- capacidad del personal;
- entorno físico;
- hardware, software o equipo de comunicaciones;
- partes externas o suministradores de servicios.

El hecho de que exista la presencia de una vulnerabilidad no significa que va o

producir algún daño por si misma, dado que los sistemas de información siempre se encuentran bajo alguna debilidad presente para explotarla. Se debe tomar en cuenta que existen vulnerabilidades que no se ven afectadas por una amenaza y esto hace que no sea necesario la implementación de un control, pero si se recomienda identificarla, documentarla y darle seguimiento para determinar cualquier cambio. (NTC/ISO/IEC 27005, 2008)

En muchos casos, los propietarios de los activos son los que hacer que las vulnerabilidades se vean expuestas debido a que su manera de usarlos no es muy adecuada, o son utilizados para propósitos diferentes a los establecidos al momento de ser adquiridos. (NTC/ISO/IEC 27005, 2008)

En el ANEXO D: TIPOS DE VULNERABILIDADES, se han extraído criterios de la Norma ISO/IEC 27005, que se puede emplear como una guía para la identificación de vulnerabilidades dentro de una organización. El resultado de la identificación de vulnerabilidades se encuentra plasmado en tabla de resultados del análisis FODA las cuales se pueden presentar como oportunidades según el concepto que a estos se les atribuye.

4.7.1.5. Identificación de los impactos.

Un impacto puede ser la considerado como pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, etc. Este proceso permite establecer los daños o consecuencias que sufre una organización y que son causados por lo que esta norma lo denomina como un escenario de incidente. Un escenario de incidente se genera a partir de los detalles de una amenaza, la cual puede aprovechar una vulnerabilidad determinada o en algunos casos, un conjunto de vulnerabilidades de una eventualidad en la seguridad de la información (ISO/IEC 27002, 2013). (NTC/ISO/IEC 27005, 2008)

Para el establecimiento del impacto de los escenarios de incidentes se toma en consideración los criterios del impacto que deben ser definidos en la determinación del contexto o, en otras palabras, se debe identificar las causas de estos escenarios. Es necesario que se identifique activos o sistemas se ven afectados en cada escenario. De esta manera, poder determinar el valor de esos activos y los costos financieros a los que se ve sometida la institución. (NTC/ISO/IEC 27005, 2008)

Para la identificación de las consecuencias es necesario primeramente determinar posibles escenarios de incidentes con sus respectivas causas como se muestra en la Tabla 6.

Tabla 6. *Tabla de escenarios de incidentes con sus respectivas causas e impactos.*

CAUSAS	ESCENARIOS	IMPACTO
• Fallas Corte de Cable UTP. • Fallas Tarjeta de Red. • Fallas IP asignado. • Fallas Puerto de Switch. • Fallas Puerto Patch Panel. • Fallas Puerto de Red.	No hay comunicación entre cliente-servidor	• Inactividad de servicios financieros. • Pérdida del modelo de negocio de la institución. • Molestias en los clientes y socios. • Mala reputación de la institución. • Valor financiero del elemento de remplazo
• Fallas de Componentes de Hardware del Servidor. • Falla del UPS (Falta de Suministro eléctrico). • Virus. • Sobrepasar el límite de almacenamiento del Disco	Falla de un servidor	• Corte de servicios financieros. • Mala reputación de la institución ante los socios y clientes. • Incomunicación con los entes de control. • Posible pérdida de datos. • Valor financiero de los elementos de remplazo o de su copia de soporte.
• Enfermedad • Accidente • Renuncia Intempestiva	Ausencia parcial o permanente de personal técnico informático de soporte y/o lineamientos informáticos	• Acumulación de trabajo para el personal de respaldo. • Retraso en las actividades planificadas. • Retraso en soporte técnico. • Desactualización de sistemas. • Desactualización de normas y políticas correspondientes al departamento de tecnología.

• Corte General del Fluido eléctrico • Corte eléctrico en las instalaciones de la cooperativa.	Interrupción del fluido eléctrico durante la ejecución los procesos.	• Daño físico en los equipos • Pérdida de datos • Corte del modelo de negocio. • Mala reputación de la institución. • Valor financiero del remplazo de activos afectados.
• Falla de equipos de comunicación: SWITCH, Fibra Óptica, Módem, Patch Cord. • Perdida de comunicación con proveedores de Internet.	Pérdida del servicio de internet.	• Incomunicación con los entes de control. • Retraso en la entrega y gestión de información con los entes de control. • Costo de adquisición, configuración e instalación del activo nuevo
• Incendio • Sabotaje • Corto Circuito • Terremoto	Indisponibilidad del centro de cómputo (destrucción del sitio de los servidores)	• Caída del modelo de negocio • Pérdida de comunicación con los entes de regulación. • Molestias en los clientes y socios de la institución. • Pérdida de datos. • Daños de los equipos informáticos (servidores). • Nueva inversión para la institución. • Pérdida de Hardware y Software.
• Mala digitación de números de cuentas a la hora de depósitos o retiros • Mala digitación en transferencias • Mala entrega de la cantidad de dinero en caja.	Error humano en la operación (Sistema Financiero)	• Molestias en los clientes y socios de la institución. • Mala reputación. • Descuadre de caja. • Pérdida de dinero.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

4.7.2. Estimación del riesgo.

El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas

y los incidentes anteriores que implicaron a la organización. Una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias. En la práctica, con frecuencia se utiliza la estimación cualitativa en primer lugar para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes. (NTC/ISO/IEC 27005, 2008)

La evaluación y administración de estos riesgos van a permitir a la Cooperativa:

- Desarrollar estrategias de recuperación y respaldo de las decisiones operacionales, tecnológicas y humanas.
- Identificar los controles existentes y los nuevos controles a implementar para minimizar los riesgos, evaluando el costo / beneficio de dichos controles.
- Planificar la seguridad de la información.

Para una correcta estimación de los riesgos es necesario identificar los procesos más importantes, los servicios principales a ser reestablecidos, y la información que debe ser respaldada dentro de la institución, y dependiendo de esta importancia determinar la estimación o criticidad del riesgo.

Principales Procesos Identificados

Software

- WEBCOOP “Sistema Corporativo Web”
- SADFIN “Sistema de Administración financiera y contabilidad”
- ZENTYAL “Administrador de correos, active directory, internet, webserver, firewall, servidor de archivos, etc.”

Principales servicios que deberán ser restablecidos y/o recuperados

- Windows (PC CLIENTE)
  - Internet.

- Herramientas de Microsoft Office.

- Software Base (SERVIDOR)
  - Base de MySQL Server

- Respaldo de la Información (SERVIDOR)
  - Backup de la configuración de CENTOS 5
  - Backup de la Base de Datos de WEBCOOP (SQL)
  - Backup de la WEBSITE
  - Backup del Servidor SADFIN.

En la Tabla 7, se mencionan los tipos de impactos que pueden causar los riesgos con su descripción y valoración asignada. Esto es necesario para saber que prioridad se da al riesgo al proponer una solución.

Tabla 7. *Tipos de Impactos de los Riesgos*

Impacto	Valor	Descripción
Crítico	4	Pérdida de la información confidencial y cuando ocurren daños significativos en los equipos.
Alto	3	Cuando se ven afectadas las operaciones y funciones, información de los usuarios y sistemas de información institucional
Medio	2	Cuando los daños son parciales (solo se dan en ciertos sistemas sin afectar las operaciones)
Bajo	1	Cuando no afectan las actividades ni los sistemas principales

Fuente: NTC/ISO/IEC 27005. (2008). Técnicas de seguridad: Gestión de riesgos para la seguridad de la información. Pereira: Asec.

Así, como los tipos de impactos es importante describir los tipos de frecuencia en la que los riesgos pueden ocurrir. En la Tabla 8 se indica el tipo de frecuencia de ocurrencia de una amenaza.

Tabla 8. *Tipos de Frecuencia de ocurrencia de una amenaza.*

Frecuencia	Valor	Descripción
Crítico	5	Cuando un riesgo o amenaza sucede de una a tres veces al día
Alto	4	Cuando un riesgo o amenaza sucede de una a tres veces a la semana
Medio	3	Cuando un riesgo o amenaza sucede de una a tres veces al mes
Bajo	2	Cuando un riesgo o amenaza sucede de una a tres veces al año
Poco Probable	1	Su valor es bajo ya que es casi improbable que pase o pueda que ocurra una sola vez cada tres años o más.

Fuente: NTC/ISO/IEC 27005. (2008). Técnicas de seguridad: Gestión de riesgos para la seguridad de la información. Pereira: Asec.

Una vez establecido los tipos de impactos y tipos de frecuencia podemos establecer la estimación de los riesgos mediante la metodología MAGERIT, que compara el valor del Impacto y de la Frecuencia, como se indica en la Tabla 9.

Tabla 9. *Estimación del riesgo según análisis MAGERIT.*

RIESGO		FRECUENCIA				
		Crítica	Alta	Medio	Baja	Poco Probable
IMPACTO	Crítico					
	Alto					
	Medio					
	Bajo					

Fuente: Elaboración propia.

En la Tabla 10 se indica la descripción para cada valoración de la estimación de los riesgos.

Tabla 10. *Descripción y valoración de estimación de riesgos*

Estimación	Descripción	Valoración
	La estimación del riesgo es crítica y se deben tomar medidas inmediatas.	1
	La estimación del riesgo es alta y se deben tomar medidas a corto plazo.	2
	La estimación del riesgo es mediana y se deben tomar medidas a largo plazo.	3
	La estimación del riesgo es baja y se deben tomar medidas preventivas.	4

Fuente: Elaboración propia.

4.7.3. Análisis FODA.

El análisis FODA es muy recomendado para el desarrollo de planes estratégicos dentro de organizaciones, con la finalidad de tomar decisiones acertadas en la realización de proyectos o cualquier tipo de propósito que la organización se ha planteado alcanzar. (Ormella, 2014)

Este análisis se ha visto como una evolución dentro de los sistemas de gestión y planificación y a formado parte de los aspectos más importantes de las empresas para la supervivencia y adaptación a nuevos cambios. (Lazzari, 2006, pág. 5)

De este análisis se derivan dos aspectos: externos e internos los cuales se encuentran agrupados bajos los siguientes conceptos:

- **Aspectos externos.** Su análisis se realiza en base a la relación que estos tienen con el ambiente al que se encuentran expuestos o el estado actual en el que se encuentran y los cambios que se espera que tengan en un futuro, tomando en cuenta que, por lo general, estos aspectos no son controlables. Dentro de estos aspectos se encuentran los conceptos de oportunidades y amenazas.

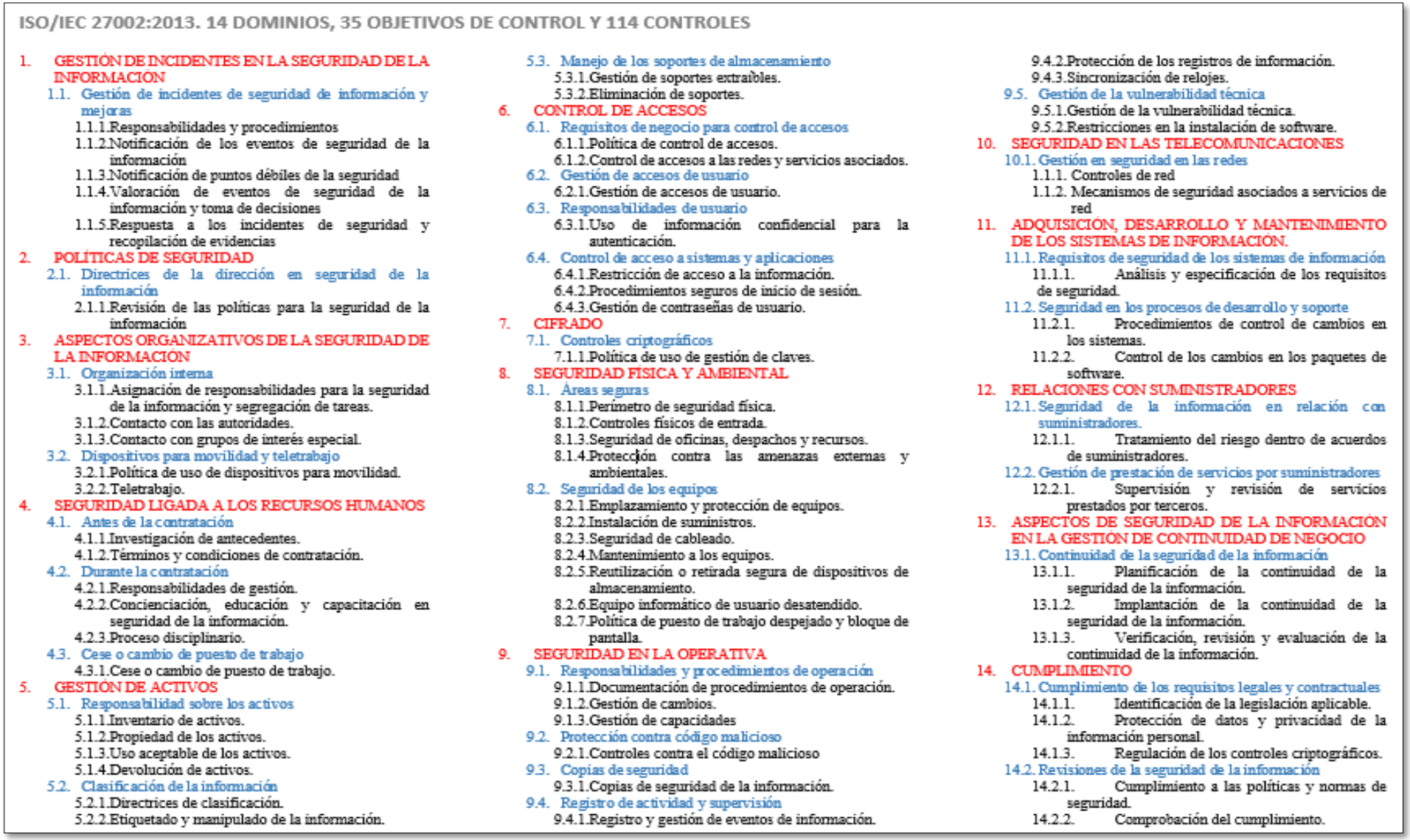
- **Aspectos internos.** Su análisis se realiza en base al estado actual en el que estos se encuentran y las variables en análisis que estos necesitan para mantener la competitividad de toda la institución en general. Ya que según expertos los aspectos internos son los que establecen la sostenibilidad de la competitividad. Dentro de estos aspectos se encuentran los conceptos de fortalezas y debilidades.

A continuación, en la Figura 13 se muestra un resumen de los objetivos y controles

de la norma ISO/IEC 27002 en los cuales se basa este análisis FODA. Para este resumen se eliminaron algunos controles de seguridad, que no se aplican para la COAC CHUCHUQUI, ya que no se encuentran relacionadas con las actividades que en ella se desarrollan.

Para este análisis se ha tomado en cuenta la norma ISO/IEC 27002:2013 de la cual se ha analizado cada uno de los objetivos y controles en relación a la situación actual en la que se encuentra la COAC (Cooperativa de Ahorro y Crédito), y clasificando cada uno respecto a los conceptos de esta metodología. En la Tabla 11 se muestra cada descripción que viene acompañada del literal de la norma al cual se encuentra relacionada.

La finalidad de este análisis es que, al finalizar el proceso de diseño e implementación del Plan de Contingencia, se pueda reducir o eliminar las amenazas y debilidades e incrementar o mantener las fortalezas y oportunidades. Hay que tomar en cuenta que las oportunidades según Ormella (2014), están ligadas a los conceptos que la ISO 27000 da sobre los riesgos, por lo cual se puede decir que, así como las oportunidades pueden aprovecharse para beneficio o también pueden ser oportunidades que se pueden convertir en debilidades según trascurra el tiempo; por lo cual, los riesgos pueden tener resultados positivos como también negativos. Por lo tanto, el FODA nos permite estar pendientes de la evolución de cada aspecto que lo constituye.



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

1. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
   - 1.1. Gestión de incidentes de seguridad de información y mejoras
     - 1.1.1. Responsabilidades y procedimientos
     - 1.1.2. Notificación de los eventos de seguridad de la información
     - 1.1.3. Notificación de puntos débiles de la seguridad
     - 1.1.4. Valoración de eventos de seguridad de la información y toma de decisiones
     - 1.1.5. Respuesta a los incidentes de seguridad y recopilación de evidencias
2. POLÍTICAS DE SEGURIDAD
   - 2.1. Directrices de la dirección en seguridad de la información
     - 2.1.1. Revisión de las políticas para la seguridad de la información
3. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN
   - 3.1. Organización interna
     - 3.1.1. Asignación de responsabilidades para la seguridad de la información y segregación de tareas.
     - 3.1.2. Contacto con las autoridades.
     - 3.1.3. Contacto con grupos de interés especial.
   - 3.2. Dispositivos para movilidad y teletrabajo
     - 3.2.1. Política de uso de dispositivos para movilidad.
     - 3.2.2. Teletrabajo.
4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
   - 4.1. Antes de la contratación
     - 4.1.1. Investigación de antecedentes.
     - 4.1.2. Términos y condiciones de contratación.
   - 4.2. Durante la contratación
     - 4.2.1. Responsabilidades de gestión.
     - 4.2.2. Concienciación, educación y capacitación en seguridad de la información.
     - 4.2.3. Proceso disciplinario.
   - 4.3. Cese o cambio de puesto de trabajo
     - 4.3.1. Cese o cambio de puesto de trabajo.
5. GESTIÓN DE ACTIVOS
   - 5.1. Responsabilidad sobre los activos
     - 5.1.1. Inventario de activos.
     - 5.1.2. Propiedad de los activos.
     - 5.1.3. Uso aceptable de los activos.
     - 5.1.4. Devolución de activos.
   - 5.2. Clasificación de la información
     - 5.2.1. Directrices de clasificación.
     - 5.2.2. Etiquetado y manipulado de la información.
   - 5.3. Manejo de los soportes de almacenamiento
     - 5.3.1. Gestión de soportes extraíbles.
     - 5.3.2. Eliminación de soportes.
6. CONTROL DE ACCESOS
   - 6.1. Requisitos de negocio para control de accesos
     - 6.1.1. Política de control de accesos.
     - 6.1.2. Control de accesos a las redes y servicios asociados.
   - 6.2. Gestión de accesos de usuario
     - 6.2.1. Gestión de accesos de usuario.
   - 6.3. Responsabilidades de usuario
     - 6.3.1. Uso de información confidencial para la autenticación.
   - 6.4. Control de acceso a sistemas y aplicaciones
     - 6.4.1. Restricción de acceso a la información.
     - 6.4.2. Procedimientos seguros de inicio de sesión.
     - 6.4.3. Gestión de contraseñas de usuario.
7. CIFRADO
   - 7.1. Controles criptográficos
     - 7.1.1. Política de uso de gestión de claves.
8. SEGURIDAD FÍSICA Y AMBIENTAL
   - 8.1. Áreas seguras
     - 8.1.1. Perímetro de seguridad física.
     - 8.1.2. Controles físicos de entrada.
     - 8.1.3. Seguridad de oficinas, despachos y recursos.
     - 8.1.4. Protección contra las amenazas externas y ambientales.
   - 8.2. Seguridad de los equipos
     - 8.2.1. Emplazamiento y protección de equipos.
     - 8.2.2. Instalación de suministros.
     - 8.2.3. Seguridad de cableado.
     - 8.2.4. Mantenimiento a los equipos.
     - 8.2.5. Reutilización o retirada segura de dispositivos de almacenamiento.
     - 8.2.6. Equipo informático de usuario desatendido.
     - 8.2.7. Política de puesto de trabajo despejado y bloque de pantalla.
9. SEGURIDAD EN LA OPERATIVA
   - 9.1. Responsabilidades y procedimientos de operación
     - 9.1.1. Documentación de procedimientos de operación.
     - 9.1.2. Gestión de cambios.
     - 9.1.3. Gestión de capacidades
   - 9.2. Protección contra código malicioso
     - 9.2.1. Controles contra el código malicioso
   - 9.3. Copias de seguridad
     - 9.3.1. Copias de seguridad de la información.
   - 9.4. Registro de actividad y supervisión
     - 9.4.1. Registro y gestión de eventos de información.
     - 9.4.2. Protección de los registros de información.
     - 9.4.3. Sincronización de relojes.
   - 9.5. Gestión de la vulnerabilidad técnica
     - 9.5.1. Gestión de la vulnerabilidad técnica.
     - 9.5.2. Restricciones en la instalación de software.
10. SEGURIDAD EN LAS TELECOMUNICACIONES
    - 10.1. Gestión en seguridad en las redes
      - 1.1.1. Controles de red
      - 1.1.2. Mecanismos de seguridad asociados a servicios de red
11. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
    - 11.1. Requisitos de seguridad de los sistemas de información
      - 11.1.1. Análisis y especificación de los requisitos de seguridad.
    - 11.2. Seguridad en los procesos de desarrollo y soporte
      - 11.2.1. Procedimientos de control de cambios en los sistemas.
      - 11.2.2. Control de los cambios en los paquetes de software.
12. RELACIONES CON SUMINISTRADORES
    - 12.1. Seguridad de la información en relación con suministradores.
      - 12.1.1. Tratamiento del riesgo dentro de acuerdos de suministradores.
    - 12.2. Gestión de prestación de servicios por suministradores
      - 12.2.1. Supervisión y revisión de servicios prestados por terceros.
13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DE NEGOCIO
    - 13.1. Continuidad de la seguridad de la información
      - 13.1.1. Planificación de la continuidad de la seguridad de la información.
      - 13.1.2. Implantación de la continuidad de la seguridad de la información.
      - 13.1.3. Verificación, revisión y evaluación de la continuidad de la información.
14. CUMPLIMIENTO
    - 14.1. Cumplimiento de los requisitos legales y contractuales
      - 14.1.1. Identificación de la legislación aplicable.
      - 14.1.2. Protección de datos y privacidad de la información personal.
      - 14.1.3. Regulación de los controles criptográficos.
    - 14.2. Revisiones de la seguridad de la información
      - 14.2.1. Cumplimiento a las políticas y normas de seguridad.
      - 14.2.2. Comprobación del cumplimiento.

Figura 13: Resumen norma ISO/IEC 27002:2013

Fuente: Acoplado de ISO/IEC 27002:2013

4.7.3.1. Resultado de Análisis FODA.

Tabla 11. *Resultado Análisis FODA*

F (Fortalezas)	O (Oportunidades)	D (Debilidades)	A (Amenazas)
Políticas de movilidad y teletrabajo no establecidas. (3.2)	Creación paulatina de políticas de seguridad. (1.1)	Los funcionarios pertenecientes al departamento de tecnología no tienen asignadas responsabilidades y procedimientos relacionados con la seguridad de la información. (1.1.1) y (3.1.1)	Acceso por SSH habilitado y se maneja el puerto por defecto. (11.1)
Contratos establecen puntos de confidencialidad y responsabilidades. (4.1.2)	Existen directrices de clasificación de la información, pero no han puesto en marcha. (5.2)		Equipos de interconexión que se encuentran fuera del Data Center están accesibles. (5.3)
Cuenta con Políticas de control de acceso. (6.1)	Cuenta con sistemas de Detección de incendios y extintores para extinción de incendios. (8.1.3)	No existe un modelo para la valoración de eventos de la seguridad de la información y toma de decisiones. (1.1.4)	No cuentan con sistema de gestión de acceso de usuario, derechos de acceso y de privilegios especiales. (6.2)
Se exige el uso de buenas prácticas de seguridad en la organización. (6.3)	Cuenta con UPS y generados de energía de iniciación manual. (8.2.2)	Aún no se define los contactos de interés y gestión de la seguridad de la información. (3.1)	Los equipos de interconexión se encuentran desprotegidos ante intercepción, interferencia y posibles daños. Y el cableado estructurado necesita do en varios sectores. (8.2.3)
Control de acceso a sistemas y aplicaciones. (6.4)	Falta adaptar adecuadamente la política de puesto de trabajo despejado y bloqueo de pantalla. (8.2.7)	No se realiza capacitaciones continuas sobre la seguridad de la información. (4.2.2)	Carece de una política que permita y restrinja la reutilización o restricción segura de dispositivos de almacenamiento. (8.2.5)
Gestión de claves. (7)	Se está desarrollando un análisis y especificación de los requisitos de seguridad. (11.1.1)	Posee un registro de los equipos activos de red, pero se encuentra desactualizado. (5.1)	No se toman las medidas necesarias para la supervisión y revisión de servicios prestados por terceros. (12.2.1)
Se encuentran bien definidas las áreas de acceso al público. (8.1)	Se aplica el uso de principios de ingeniería en protección de sistemas. (11.2)	No existe etiquetado y manipulado para la información. (5.2.2)	
Los equipos activos como servidores y bases de datos, se encuentran protegidos y aislados de personas no autorizadas. (8.2.1)	Se está desarrollando la gestión de incidentes en la seguridad de la información. (1)	Falta mejor aspectos de Seguridad en oficinas específicamente no existe señalética adecuada en todos los sectores de la institución. (8.1.3)	
Existen procedimientos de información puesta a disposición de los usuarios. (9.1.1)	Conocimiento de las políticas que establecen los proveedores de servicios acerca de la seguridad de la información. (12)		
Se trata de ejecutar un mínimo de cambios posibles en la seguridad de la información, que puedan tener alguna afectación en la información. Los cambios que se realizan es bajo supervisión. (9.1.2)			

Los servidores se encuentran bajo monitoreo y los recursos de red están correctamente distribuidos mediante reglas de acceso. (9.1.3)	La protección contra amenazas externas y ambientales se encuentra sujeta a la construcción arquitectónica actual. (8.1.4)
Todos los dispositivos Móviles (Laptops) conectados a la red cuentan con antivirus licenciado. (9.2)	Los funcionarios carecen de la costumbre para la aplicación de la política de puedto de trabajo despejado. (8.2.7)
Se realizan copias de seguridad de la información ni respaldos de las bases de datos. (9.3)	No existe un control para la gestión de cambios. (9.1.2)
Se controla el registro de actividad del administrador y operador del sistema. (9.4.1)	No existe IDS e IPS de detección y prevención para el control de código malicioso. (9.2)
Todos los sistemas se encuentran sincronizados. (9.4.3)	No se han realizado periódicamente controles de auditorías de los sistemas de información. (9.5)
Existe restricción respecto a la instalación de software. (9.6.2)	No existe gestión de las vulnerabilidades técnicas. (9.5.2)
Están establecidas medidas de seguridad en las telecomunicaciones. (10)	No se realiza periódicamente una verificación, revisión y evaluación de la continuidad de la información. (13.1.3)
Se realiza periódicamente una revisión técnica de las aplicaciones tras efectuar cambios en los sistemas operativos. (11.2.1)	No se realizan comprobaciones periódicas del cumplimiento de las políticas y normas de seguridad. (14.2)
Existe restricción a los cambios en los paquetes de software. (11.2.2)	

Fuente: Elaboración propia.

4.8. TRATAMIENTO DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Para el tratamiento del riesgo existen varias opciones que deberían ser seleccionadas basadas en la eficacia del resultado de las evaluaciones de los riesgos, la relación costo beneficio para la implementación de estas opciones y las ventajas que ellas ofrecen. (NTC/ISO/IEC 27005, 2008)

El costo es un aspecto muy importante que debe ser considerado al igual que garantice que con cualquier opción que se emplee, ayude a reducir los riesgos. Cuando se tome la decisión de realizar mejoras en la seguridad de la información, se debería asegurar de que cualquier cambio o incremento de los controles sea correctamente justificado. (NTC/ISO/IEC 27005, 2008)

Algunas medidas de los tratamientos de los riesgos pueden cubrir eficazmente a más de un riesgo (por ejemplo, la capacitación y concienciación del personal sobre la seguridad de la información). Es conveniente establecer un plan para el tratamiento del riesgo que ayude a determinar el orden de prioridad adecuado para la implementación de los tratamientos en específico. Existen diferentes técnicas para el establecimiento de la prioridad, que incluyen clasificación del riesgo y análisis de costo-beneficio. Por lo cual es también responsabilidad de los administradores de la institución el determinar si es factible la asignación de los presupuestos. (NTC/ISO/IEC 27005, 2008)

El desarrollo del tratamiento de los riesgos se lo despliega en el plan de emergencia, plan de restauración y plan de recuperación en los cuáles se detalla los procedimientos a seguir en cada escenario de incidentes.

Para garantizar la eficiencia de cada uno de estos planes es recomendable, recolectar información acerca de la estructura de la institución para determinar el ambiente en que se pueden desarrollar los riesgos y así poder establecer quienes son los funcionarios adecuados para participar en el proceso de gestión del riesgo y así, conservar la seguridad de la información. En la Figura 9 y Figura 10 presentadas anteriormente se encuentra la estructura organizativa de la cooperativa.

<table>
<tr><th colspan="3">COOPERATIVA DE AHORRO Y CRÉDITO DE INDIGENAS “CHUCHUQUI” LTDA.</th></tr>
<tr><th colspan="3">PLAN DE EMERGENCIA</th></tr>
<tr><td rowspan="3"> 
</td><td>Revisado por:</td><td>Ing. Darío Castañeda /Jefe Departamento de Tecnología.
Ing. Marcelo Yamberla / Asistente de Tecnología</td></tr>
<tr><td>Aprobado por:</td><td>Ing. Darío Castañeda /Jefe Departamento de Tecnología</td></tr>
<tr><td>Fecha de aprobación:</td><td>24 de septiembre de 2016 - Acta 318 R (31)</td></tr>
</table>

4.9. PLAN DE EMERGENCIA

4.9.1. Objetivo.

Garantizar que la institución cuenta con una orientación, equipamiento y preparación suficiente para enfrentar eventos de emergencia, con la finalidad de salvaguardar vidas, brindar seguridad a los activos y estar en la capacidad de restablecer los procesos a la normalidad. (Secretaría general de gestión de riesgos, 2010)

4.9.2. Escenarios de incidentes.

En este plan se considerarán los siguientes escenarios:

- Sismo de tipo tectónico
- Incendio
- Atentado terrorista

4.9.2.1. Estimación de los escenarios.

La estimación de los escenarios de incidentes nos permite determinar los instrumentos necesarios para poder dar priorización y orientación las acciones que van a llevarse a cabo cuando suceda alguno de estos incidentes. Así, como también corregir vulnerabilidades y de esta forma obtener mejores resultados en la prevención y en el proceso de mitigación de los riesgos. En la Tabla 12 podemos ver ejemplos de riesgos de emergencia con sus respectivas medidas y tiempo de implementación. (Secretaría general

de gestión de riesgos, 2010)

Tabla 12. *Ejemplos de riesgos de emergencia*

RIESGO	MEDIDA A IMPLEMENTAR	TIEMPO DE IMPLEMENTACIÓN
Sismo de 6.5° en la escala de Richter, de origen tectónico.	Realización de simulacros de evacuación, para el personal que labora en la cooperativa. Verificación del funcionamiento de alarmas. Comprobación de que no exista estanterías o cuadros no susceptibles a caídas.	Mediano plazo: de 6 a 9 meses.
Incendio	Evaluación de las instalaciones eléctricas para garantizar la reducción de la probabilidad de un cortocircuito.	Corto plazo: de 3 a 6 meses
Aparatos explosivos	Capacitación del personal de seguridad, con la finalidad de establecer medidas de protección en caso de encontrar paquetes sospechosos en las instalaciones de la institución.	Mediano plazo: de 6 a 9 meses.

Fuente: Secretaría general de gestión de riesgos. (2010). Gestión de riesgos: Plan de emergencia institucional. Obtenido de: http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

4.9.2.2. Características de los escenarios de incidentes de emergencia.

En la Tabla 13 se especifican las características para cada tipo de amenaza en los escenarios de incidentes de emergencia.

Tabla 13. *Características de los escenarios de incidentes de emergencia*

AMENAZA	FRECUENCIA	MAGNITUD	INTENSIDAD
Sismo tipo tectónico	Baja	Media	Media
Incendio	Media	Alta	Alta
Atentado terrorista	Media	Media	Alta

Fuente: Secretaría general de gestión de riesgos. (2010). Gestión de riesgos: Plan de emergencia institucional. Obtenido de: http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

4.9.3. Organización institucional de respuesta.

La institución debe establecer una organización o comité institucional de respuesta, el cual será responsable de dirigir el proceso de ejecución del plan de emergencia. A continuación, en la Figura 14 se describe gráficamente la estructura:

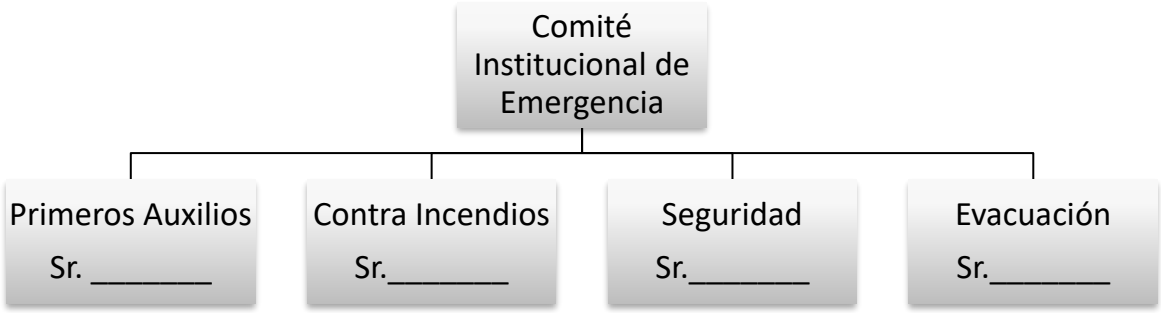


Figura 14. Comité Institucional de Emergencia

Fuente: Elaboración propia.

Primeros Auxilios

La persona encargada de los primeros auxilios tiene la responsabilidad de dar socorro a las personas que necesiten atención inmediata, así como también trasladarlas a un lugar seguro, hasta que algún grupo especial (bomberos, cruz roja, etc.) llegue a dar apoyo. Dentro de sus responsabilidades se incluye (Secretaría general de gestión de riesgos, 2010):

a) Verificación de la existencia de un botiquín de emergencia y abastecimiento de medicamentos y materiales necesarios.

b) Establecer una adecuada prioridad en la atención de personas afectadas.

c) Elaborar una lista de personas afectadas con sus respectivos síntomas y signos.

d) Colaborar en la evacuación de los heridos a establecimientos de salud asignados.

e) Coordinar acciones con los grupos especiales de socorro.

Sus responsabilidades después de acontecido el incidente son:

a) Detallar un informe final de las personas afectadas y los lugares a los que fueron trasladados.

b) Indicar en un informe los materiales utilizados y las tareas que a han desarrollado durante el incidente.

Contra incendios

El responsable deberá verificar continuamente que la institución está en la capacidad de responder ante un incidente de incendio. Entre estas responsabilidades se incluye (Secretaría general de gestión de riesgos, 2010):

a) Verificar periódicamente que los equipos de extinción de incendios se encuentren en estado adecuado para garantizar que estos funcionen correctamente.

b) Solicitar una capacitación al cuerpo de bomberos de cómo batallar contra un incendio para el personal de la institución que vaya a formar parte del grupo de apoyo contra incendios.

c) Revisar periódicamente las instalaciones eléctricas de la institución.

d) Verificar que la institución cuente con el equipo necesario y que su ubicación sea la adecuada.

e) Instruir a todo el personal de la institución sobre las actividades a realizar en un incendio.

f) Coordinar actividades de simulacros.

Durante el incidente su responsabilidad incluye:

a) Combatir el incendio hasta donde se le sea posible o hasta que llegue el grupo de bomberos, procurando proteger las partes más críticas de la institución.

Una vez que ha finalizado el incendio sus responsabilidades incluyen (Secretaría general de gestión de riesgos, 2010):

a) Realizar una evaluación de los daños y necesidades que requiere la institución para su restauración.

b) Elaborar un informe detallando las tareas realizadas y observaciones.

Seguridad

El encargado de seguridad debe garantizar que todo el personal tiene conocimientos sobre las actividades de emergencia. Dentro de sus responsabilidades se incluye (Secretaría general de gestión de riesgos, 2010):

a) Periódicamente debe realizar inspecciones en el interior de la institución para detectar o identificar posibles amenazas o vulnerabilidades.

b) Controlar en ingreso de clientes o visitantes de la institución, así, como también vigilar que no ingresen a áreas restringidas.

c) Brindar seguridad a los funcionarios y clientes de la institución que se encuentren dentro de las instalaciones, así, como también la protección de los bienes.

d) Participar en los ejercicios de simulacros.

Durante el desarrollo de un incidente, sus responsabilidades incluyen (Secretaría general de gestión de riesgos, 2010):

a) Mantener el orden en el momento de la evacuación y controlar de que las áreas críticas de la institución, se encuentren seguras y libres de intrusos.

b) Notificar a la policía sobre novedades importantes que han ocurrido durante el incidente.

c) Dar seguridad a las instalaciones, archivos, bienes, etc., hasta donde se le sea posible sin arriesgar su vida.

d) Coordinar actividades con el resto del comité institucional de emergencia.

Una vez que ha pasado el incidente, sus responsabilidades incluyen:

a) Organizar adecuadamente el retorno del personal a las instalaciones.

b) Realizar una inspección de las instalaciones, tanto internas como externas.

c) Controlar o impedir el ingreso a personas sospechosas.

Evacuación

El encargado de evacuación debe asegurar de que todo el personal ha sido capacitado sobre el procedimiento de evacuación y realizar una asignación de responsables por cada piso. Sus responsabilidades incluyen (Secretaría general de gestión de riesgos, 2010):

a) Informar al personal sobre las rutas de evacuación y asegurar que la institución cuente con la señalización necesaria.

b) Establecer e informar los puntos de encuentro después de la evacuación.

c) Participar en actividades de simulación.

Durante el proceso de evacuación, sus responsabilidades incluyen (Secretaría general de gestión de riesgos, 2010):

a) De ser posible estar identificado con un chaleco o brazalete.

b) Tener a mano un medio de comunicación.

c) Controlar de que la evacuación se realice con el mayor silencio posible y sin correr.

d) Coordinar con los encargados de piso, la evacuación de todas las personas.

e) Conducir al personal a los puntos de concentración determinados.

f) En la zona de concentración se debe realizar una contabilización del personal y realizar un informe de alguna novedad durante el proceso.

Después de finalizada la evacuación su responsabilidad incluye:

a) Coordinar de forma organizada el retorno del personal a las instalaciones.

Nota: En el ANEXO E se puede encontrar los números de emergencia que todos los que conforman el comité institucional de emergencia deben tener conocimiento. Hay que tomar en cuenta que esta lista de contactos es simplemente un respaldo, ya que todos los servicios de emergencia ahora se encuentran unificados a una sola línea telefónica (911).

COOPERATIVA DE AHORRO Y CRÉDITO DE INDIGENAS "CHUCHUQUI" LTDA.		
PLAN DE RESTAURACIÓN		
"CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**Revisado por:**	Ing. Darío Castañeda /Jefe Departamento de Tecnología. Ing. Marcelo Yamberla / Asistente de Tecnología
	Aprobado por:	Ing. Darío Castañeda/Jefe Departamento de Tecnología
	Fecha de aprobación:	24 de septiembre de 2016 - Acta 318 R (31)

4.10. PLAN DE RESTAURACIÓN

Para la propuesta de este plan se consideran los escenarios de incidentes establecidos en el análisis de riesgos, los cuáles se enlistan a continuación:

- No hay comunicación entre cliente – servidor.
- Falla de un servidor.
- Ausencia parcial o permanente del personal de departamento de tecnologías.
- Interrupción del fluido eléctrico durante la ejecución de los procesos.
- Perdida de servicio internet.

Nota: *El escenario de indisponibilidad del centro de cómputo se lo estudiará en el plan de Recuperación.*

4.10.1. Objetivo.

Establecer procedimientos, recursos de contingencia y tiempos aceptables de caída, en respuesta a distintos escenarios de incidentes, con la finalidad de minimizar tiempos de restauración del modelo de negocio de la institución.

4.10.2. Estructura.

Para el desarrollo del plan de restauración se deberá tomar en cuenta la Figura 15, en la que expone un diagrama de flujo que propone una estructura de procedimiento de gestión de incidentes basado en ITIL.

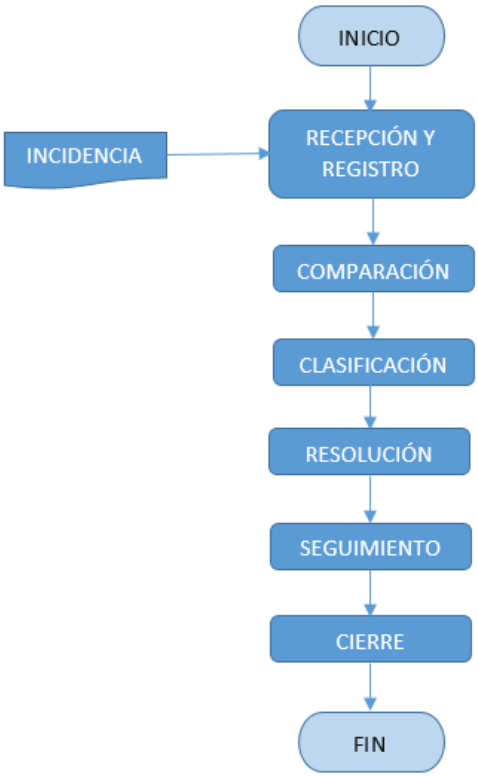


Figura 15: Procedimiento de Gestión de Incidencias

Fuente: Office of Government Commerce (2010). Operación del servicio. Londres, Reino Unido: TSO.

4.10.2.1. Recepción y registro.

En esta sección del procedimiento de gestión se deben considerar las siguientes descripciones (Office of Government Commerce , 2010):

- Descripción de Impactos y consecuencias

- Posibles causas
- Recursos de contingencia
- Nivel de prioridad y tiempo máximo de contingencia

Para la formalización del registro de incidencia se debe seguir el formato del ANEXO F.

4.10.2.2. Comparación.

Si no se tiene una idea muy clara del problema y su solución, se recomienda que previo a buscar una solución por propia cuenta, se realice una búsqueda en la base de datos de incidencias con similares características, para proporcionar una solución rápida y que haya funcionado antes; si no se encuentra el problema o la solución, se pasa a la siguiente etapa, que se trata de la investigación y diagnóstico. (Office of Government Commerce , 2010)

Investigación y diagnóstico. Se analiza si el problema está en las capacidades de los funcionarios de la cooperativa de ser resuelto, o caso contrario se procederá a la asignación del problema a algún grupo especializado que brinde servicios a la institución. (Office of Government Commerce , 2010)

4.10.2.3. Clasificación.

Es importante asignar una clasificación de los incidentes y así, poder determinar los impactos en la institución y la prioridad para dar una solución. Esta clasificación puede estar relacionada con aspectos o elementos comprometidos por la incidencia, también se recomienda que la clasificación cuente con una categorización como lo propone ITIL y que se muestra en la Figura 16. (Office of Government Commerce , 2010)

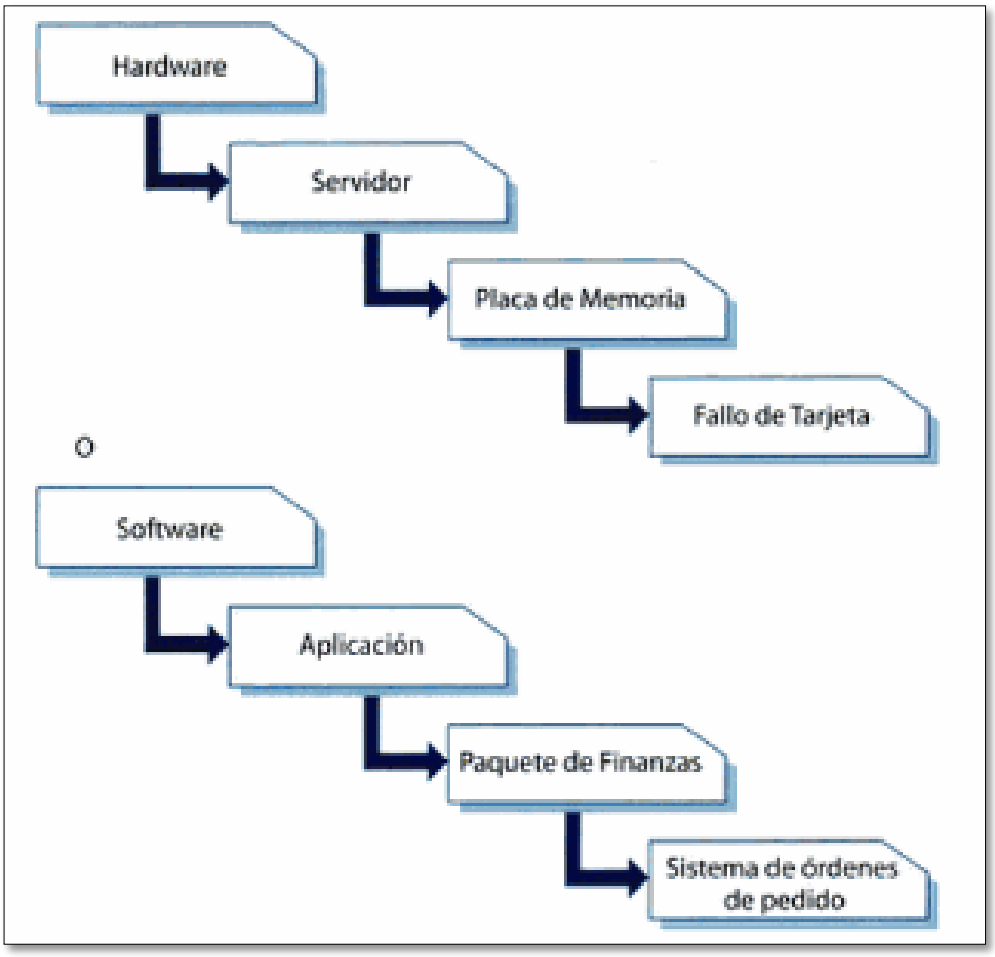


Figura 16: Categorización de incidencias.

Fuente: Ríos S. (2014). ITILv3: Manual íntegro. Recuperado el 10 de octubre de 2016 de: http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf

4.10.2.4. Resolución.

En esta etapa se encuentran todas las acciones o el procedimiento que se va a seguir para dar solución a la incidencia. En este proceso hay que tomar en cuenta que, si es necesario realizar algún cambio significativo en cualquier aspecto de la institución, se debe seguir el procedimiento de gestión de cambios que se encuentra detallada en el plan de mantenimiento en el dominio de "seguridad en la operativa". (Office of Government Commerce , 2010)

4.10.2.5. Seguimiento.

El seguimiento de la incidencia tiene relación directa con el nivel en el que se haya resuelto. Si la solución propuesta por los funcionarios de la institución, será responsabilidad de los mismos el llevar a cabo este seguimiento; sin embargo, si la

incidencia es cedida a grupos especiales porque su resolución necesita de cambios, pasará a ser parte del proceso de gestión de cambios. Estos actores deben actualizar la información almacenada en las correspondientes bases de datos, para que los recursos implicados tengan la información siempre actualizada del estado de la incidencia. (Office of Government Commerce, 2010)

4.10.2.6. Cierre.

Una vez resuelta la incidencia, se deben realizar una serie de acciones que permitan cerrar la incidencia y poner fin al proceso. Estas acciones son: (Ríos, 2014)

- Comunicación al cliente y a los usuarios de la solución establecida.
- Actualización de la base de datos de incidencias.
- Actualización de la CMDB (Change Management Data Base, Base de Datos de Gestión de Cambios), detallando todos los elementos que formaron parte de la gestión de cambios y su correspondiente configuración.

4.10.3. Tiempos de restauración.

Los tiempos de restauración se basan en la publicación de ITIL, la cual también propone un sistema de código de prioridad como se muestra en la Tabla 14.

Tabla 14. *Clasificación de tiempos de restauración*

Código de prioridad	Descripción	Tiempo objetivo de restauración
1	Crítico	1 hora
2	Alto	8 horas
3	Medio	24 horas
4	Bajo	48 horas

Fuente: Office of Government Commerce (2010). Operación del servicio. Londres, Reino Unido: TSO.

Hay que tomar en cuenta que el impacto, prioridad y tiempo, pueden variar a lo largo del análisis de la incidencia como se describe a continuación (Office of Government Commerce , 2010):

- Puede ampliarse debido al aumento de los fallos o al tratarse de una secuencia de fallos.
- Puede reducirse al implementar soluciones temporales que sean eficaces de tal manera que se dé por terminado el incidente.

4.10.4. Escenario 1: no hay comunicación entre cliente-servidor.

Impactos y servicios afectados.

Los impactos y servicios afectados para este escenario se describen en la Tabla 15.

Tabla 15. *Descripción de Impacto y servicios afectados en escenario 1.*

NO HAY COMUNICACIÓN ENTRE CLIENTE-SERVIDOR	
IMPACTOS	SISTEMAS O SERVICIOS AFECTADOS
• Inactividad de servicios financieros • Pérdida del modelo de negocio de la institución • Molestias en los clientes y socios • Mala reputación de la institución • Valor financiero del elemento de remplazo	• Sistema WEBCOOP • Sistema SADFIN • Sistema de información • Servidor de archivos • Servidor de correo • Servidor Web

Fuente: Elaboración propia.

Causas.

- Fallas Corte de Cable UTP.
- Fallas Tarjeta de Red.
- Fallas IP asignado.
- Fallas Puerto de Switch.
- Fallas Puerto Patch Panel.
- Fallas Punto de Red.

Recursos de contingencia.

Componentes de remplazo:

- Tarjeta de Red
- Cables UTP categoría 5e y 6A
- Conectores RJ-45, Jack RJ-45, Probador, herramientas de cableado estructurado, etc.
- Mapa de estructura de la red institucional
- Mapa conceptual modelo Cliente-Servidor

Nivel de Prioridad y tiempos aceptables de Caída.

El nivel de prioridad y los tiempos aceptables de caída para cada recurso involucrado en este escenario se describen en la Tabla 16.

Tabla 16. *Nivel de Prioridad y tiempos aceptables de caída para el escenario 10.3.*

RECURSO	NIVEL DE PRIORIDAD	TIEMPO ACEPTABLE DE CAIDA
Sistema WEBCOOP	CRÍTICO	1 hora
Sistema SADFIN	CRÍTICO	1 hora
Sistema de información	CRÍTICO	1 hora
Servidor de archivos	CRÍTICO	1 hora
Servidor de correo	ALTO	8 horas
Servidor Web	ALTO	8 horas

Fuente: Elaboración propia.

Procedimiento.

Para este escenario se consideran las causas mencionadas en el punto 0, en la Tabla 17 se muestra cada problema y se da un procedimiento de solución, tomando en cuenta que el primer paso siempre es comunicar del incidente al departamento de tecnología o equipo de soporte técnico para la identificación del origen del inconveniente.

Tabla 17. *Causas y procedimiento para el escenario 1*

Causa	**Procedimiento de solución**
Falla por corte en cable UTP	Remplazo del cable UTP
Fallo en la tarjeta de red	Reinstalación del drive Ethernet/WLAN, en caso de que el problema sea del hardware de la tarjeta de red, es necesario realizar un remplazo de la misma.
Fallo en el direccionamiento IP	Comprobar el direccionamiento, de ser necesario realizar una nueva asignación de dirección IP.
Fallo en el puerto de un switch	Verificación de la configuración y habilitación del puerto. Cambio de puerto a uno que se encuentre disponible en el switch. En caso de que el problema sea en el dispositivo, pueda que sea necesario su remplazo.
Fallo en puerto de un patch panel	Verificación de la conexión en el puerto. Realizar un cambio de puerto o de ser necesario el cambio del patch panel.
Fallo en el punto red	Verificación de los conectores de red. Realizar un nuevo ponchado o remplazo de los elementos comprometidos.

Fuente: Elaboración propia.

4.10.5. Escenario 2: falla de un servidor.

Impactos y servicios afectados.

Los impactos y servicios afectados para este escenario se describen en la Tabla 18.

Tabla 18. *Descripción de Impacto y servicios afectados en escenario 2*

FALLA DE UN SERVIDOR	
IMPACTOS	SISTEMAS O SERVICIOS AFECTADOS
• Corte de servicios financieros • Mala reputación de la institución ante los socios y clientes • Incomunicación con los entes de control	• Sistema WEBCOOP • Sistema SADFIN • Sistema de información • Servidor de archivos

• Posible pérdida de datos • Valor financiero de los elementos de remplazo o de su copia de soporte	• Servidor de correo • Servidor Web

Fuente: Elaboración propia.

Causas.

- Fallas de Componentes de Hardware del Servidor
- Falla del UPS (Falta de Suministro eléctrico)
- Virus
- Sobrepasar el límite de almacenamiento del Disco.

Recursos de contingencia.

- Disco duro
- Memorias RAM
- Tarjetas
- Estructura del armario bastidor (servidor)

Nivel de prioridad y tiempo aceptable de caída.

El nivel de prioridad y los tiempos aceptables de caída para cada recurso involucrado en este escenario se describen en la Tabla 19.

Tabla 19. *Nivel de prioridad y tiempos aceptables de caída para el escenario 2*

RECURSO	NIVEL DE PRIORIDAD	TIEMPO ACEPTABLE DE CAIDA
Sistema WEBCOOP	CRÍTICO	1 hora
Sistema SADFIN	CRÍTICO	1 hora
Sistema de información	CRÍTICO	1 hora
Servidor de archivos	CRÍTICO	1 hora
Servidor de correo	ALTO	8 horas
Servidor Web	ALTO	8 horas

Fuente: Elaboración propia.

Procedimiento.

Para el desarrollo del procedimiento que se debe tomar en cuenta algunas posibles causas dentro de las fallas de componentes de hardware de un servidor, que se mencionan a continuación:

Error Físico de Disco de un Servidor (Sin RAID).

En el caso de que el disco presenta fallas críticas, tales que no pueden ser reparadas, se debe tomar los siguientes pasos (Instituto Veracruzano de acceso a la información, 2012):

a) Ubicar el disco con falencias

b) Informar a todos los usuarios que se encuentran en el sistema de que deben cerrar sesión, esto mediante la utilización de mensajes por cualquier medio y llamadas telefónicas a jefes de departamento

c) Dar de baja el sistema y apagar el servidor

d) Retirar el disco con falencias y remplazarlo con otro, formatearlo y darle partición o particiones necesarias

e) Restablecer el último backup en el disco, asegurarse de restaurar todas las modificaciones

f) Verificar los sistemas que se encuentran en dicho disco y verificar su buen estado

g) Habilitar el acceso al sistema para los usuarios.

Error de Memoria RAM

En este caso se dan los siguientes síntomas (Instituto Veracruzano de acceso a la información, 2012):

- El servidor no responde adecuadamente, tiene lentitud de procesamiento o no rinde ante el acceso masivo de usuarios.

- Pueden surgir errores con mapas de direcciones hexadecimales.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la Cooperativa, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes (Instituto Veracruzano de acceso a la información, 2012):

a) Informar a todos los usuarios que se encuentran en el sistema de que deben cerrar sesión, esto mediante la utilización de mensajes por cualquier medio y llamadas telefónicas a jefes de departamento.

b) El servidor debe apagarse correctamente, asegurando que el sistema tubo el tiempo suficiente para cerrarse con normalidad.

c) Ubicar las memorias en mal estado.

d) Extraer las memorias dañadas y reemplazarlas por otras iguales o similares.

e) Extraer la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.

f) Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

g) Probar los sistemas que están en red en diferentes estaciones.

h) Finalmente, luego de los resultados, habilitar el acceso al sistema para los funcionarios.

Error de Tarjeta(s) Controladora(s) de Disco

Para esta falencia se debe considerar que ningún proceso debe ser pausado, debiéndose ejecutar las siguientes acciones (Instituto Veracruzano de acceso a la información, 2012):

a) Informar a todos los usuarios que se encuentran en el sistema de que deben cerrar sesión, esto mediante la utilización de mensajes por cualquier medio y llamadas telefónicas a jefes de departamento.

b) El servidor debe apagarse correctamente, asegurando que el sistema tubo el tiempo suficiente para cerrarse con normalidad.

c) Extraer la tarjeta que se cree que porta la falencia y tener a la mano otra igual o similar.

d) Extraer la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.

e) Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

f) Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar el acceso al sistema para los funcionarios.

Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas (Instituto Veracruzano de acceso a la información, 2012):

- Falla en el suministro de energía eléctrica por mala alimentación del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por una falencia en el chequeo de una debilidad física.

En caso de que se origine alguno de los escenarios descritos anteriormente; se deben realizar las siguientes acciones (Instituto Veracruzano de acceso a la información, 2012):

a) Verificar la correcta alimentación del suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos.

b) Deshabilitar el acceso de usuarios al sistema.

c) Descargar todos los archivos de importancia del servidor, a excepción del volumen raíz.

d) Al término de la operación de reparación se procederá a habilitar el acceso a estaciones para la dirección de soporte técnico, se procederá a verificar que los índices de las bases de datos estén correctos, para ello se debe empezar a ejecutar los sistemas y así poder determinar si el funcionario puede hacer uso de ellos inmediatamente.

Caso de Virus

Dado el escenario de que se presente virus en las computadoras que atente a la seguridad de la información, se procederá a lo siguiente (Instituto Veracruzano de acceso a la información, 2012):

a) Se debe disponer de un antivirus para el sistema, que aísle el virus que ingresa al sistema llevándolo a un directorio donde se pone en cuarentena para su futura examinación.

b) Los antivirus indican el nombre del archivo infectado y que usuario hizo uso de éste.

c) Estos archivos (exe, com, etc.) serán sustituidos del disco original de instalación o del backup.

d) Si los archivos infectados ya han sido aislados y aún se generan mensajes de la existencia de virus en el sistema, lo más probable es que una de las estaciones de la institución es la que está ocasionando la infección, por lo cual, se recomienda retirarla del acceso al sistema y proceder a un análisis.

4.10.6. Escenario 3: ausencia parcial o permanente del personal técnico informático.

Descripción de impactos y servicios afectados.

Los impactos y servicios afectados para este escenario se describen en la Tabla 20.

Tabla 20. *Impactos y servicios afectados en escenario 3*

AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL TÉCNICO INFORMÁTICO	
IMPACTOS	SISTEMAS O SERVICIOS AFECTADOS
• Acumulación de trabajo para el personal de respaldo. • Retraso en las actividades planificadas. • Retraso en soporte técnico. • Desactualización de sistemas. • Desactualización de normas y políticas correspondientes al departamento de tecnología. • Retraso de entrega de información a los entes de control • Administración de bases de datos descuidada. • No hay control y monitoreo de servidores. • Falta de personal para soporte técnico a los usuarios.	• Todas las áreas o servicios corren riesgos de ser afectados.

Fuente: Elaboración propia.

Causas.

- Enfermedad
- Accidente
- Renuncia Intempestiva

Recursos de contingencia.

- Capacitación continua a todo el personal del Dpto. de tecnología (Todo el personal con las mismas capacidades).
- Manual de técnicos del Departo de tecnología.
- Listas de contactos de soporte técnico o afines.

Tiempos aceptables de caída.

El nivel de prioridad y los tiempos aceptables de caída para cada recurso involucrado

en este escenario se describen en la Tabla 21.

Tabla 21. *Nivel de prioridad y tiempos aceptables de caída para el escenario 3*

RECURSO	NIVEL DE PRIORIDAD	TIEMPO ACEPTABLE DE CAIDA
Acumulación de trabajo para el personal de respaldo.	ALTO	8 horas
Retraso en las actividades planificadas.	ALTO	8 horas
Retraso en soporte técnico.	CRÍTICO	1 hora
Desactualización de sistemas.	CRÍTICO	1 hora
Desactualización de normas y políticas correspondientes al departamento de tecnología.	ALTO	8 horas
Retraso de entrega de información a los entes de control	ALTO	8 horas
Administración de bases de datos	ALTO	8 horas
Control y monitoreo de servidores	ALTO	8 horas

Fuente: Elaboración propia.

Procedimiento.

En la ausencia del personal técnico informático lo primero que se debe hacer, es averiguar por cualquier medio posible, si la ausencia es parcial o permanente y según eso se puede tomar las siguientes medidas:

- En caso de que la ausencia sea parcial:

    a) Averiguar las causas, para establecer un tiempo aproximado de ausencia;

    b) Coordinar con el resto de personal, soluciones para cubrir las áreas en las que se desempeña dicho funcionario;

    c) Si no se pueden cubrir todas las funciones, contactar a un especialista que pueda remplazarlo por tiempo de ausencia.

- En caso de que la ausencia sea permanente:

    a) Detallar un informe con los motivos de la ausencia e impactos que esta causaría;

    b) Eliminar las cuentas de acceso a las instalaciones y sistemas del

funcionario que ha abandonado su puesto de trabajo;

c) Realizar una carta formal de renuncia o despido del funcionario;

d) Empezar el procedimiento de contratación de nuevo personal, para cubrir la vacante. El procedimiento debe incluir un concurso de méritos.

4.10.7. Escenario 4: interrupción del fluido eléctrico durante la ejecución de los procesos.

Impactos y servicios afectados.

Los impactos y servicios afectados para este escenario se describen en la Tabla 22.

Tabla 22. *Impactos y servicios afectados en escenario 4*

INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS	
IMPACTOS	SISTEMAS O SERVICIOS AFECTADOS
• Interrupción de las operaciones • Daño físico en los equipos • Pérdida de datos • Corte del modelo de negocio • Mala reputación de la institución • Pérdida de comunicación a Internet • Valor financiero del remplazo de activos afectados.	• Todas las áreas o servicios corren riesgos de ser afectados.

Fuente: Elaboración propia.

Causas.

- Corte General del Fluido eléctrico
- Corte eléctrico en las instalaciones de la cooperativa.

Recursos de contingencia.

- Planta de energía eléctrica.
- UPS (Uninterruptible Power Supply)

Tiempos aceptables de Caída.

El nivel de prioridad y los tiempos aceptables de caída para cada recurso involucrado en este escenario se describen en la Tabla 23.

Tabla 23. *Nivel de prioridad y tiempos aceptables de caída para el escenario 4*

RECURSO	NIVEL DE PRIORIDAD	TIEMPO ACEPTABLE DE CAIDA
PC-Cliente	CRÍTICO	1 hora
Servidor de red	CRÍTICO	1 hora
Servidor Web	ALTO	8 horas
Servidor de correo	ALTO	8 horas
Servicios Institucionales	CRÍTICO	1 hora

Fuente: Elaboración propia.

Procedimiento.

Corte general de fluido eléctrico

Dado el caso se debe tomar las acciones siguientes:

a) Contactar a la empresa eléctrica de la zona, por la información del corte y el tiempo en reparación.

b) Si la reparación persiste mayor a 15 minutos:

- Informar a la gerencia, sobre información recibida de la empresa eléctrica
- Esperar la autorización de la Gerencia sobre el encendido de la planta eléctrica.
- Informar al personal, sobre el inicio de operación.

Corte eléctrico en las instalaciones de la Cooperativa

Dado el caso se debe tomar las acciones siguientes:

a) Ubicar el daño.

b) Realizar un informe técnico sobre el daño y entregar a la Gerencia

c) Informar al personal sobre el daño

d) Solicitar apoyo de un técnico, especialista en energía eléctrica (servicio externo)

e) Solucionar el punto del daño

f) Solicitar mediante un informe técnico a la Gerencia, el análisis de toda la red eléctrica de la institución

g) Avisar a los usuarios sobre la solución, mediante llamadas telefónicas a cada jefe de área. El combustible mantuvo

4.10.8. Escenario 5: corte del servicio de internet.

Impactos y servicios afectados.

Los impactos y servicios afectados para este escenario se describen en la Tabla 24.

Tabla 24. *Impactos y servicios afectados en escenario 5*

CORTE DEL SERVICIO DE INTERNET	
IMPACTOS	SISTEMAS O SERVICIOS AFECTADOS
Incomunicación con los entes de control. Retraso en la entrega y gestión de información con los entes de control. Costo de adquisición, configuración e instalación del activo nuevo	Servidor de correo Servidor Web

Fuente: Elaboración propia.

Causas.

- Falla de equipos de comunicación: SWITCH, Fibra Óptica, Módem, Patch Cord.
- Perdida de comunicación con proveedores de Internet.

Recursos de Contingencia.

- Switch de 24 puertos
- Patch cord
- Módem

Nivel de prioridad y tiempos aceptables de caída.

El nivel de prioridad y los tiempos aceptables de caída para cada recurso involucrado en este escenario se describen en la Tabla 25.

Tabla 25. *Nivel de prioridad y tiempos aceptables de caída para el escenario 5*

RECURSO	NIVEL DE PRIORIDAD	TIEMPO ACEPTABLE DE CAIDA
Pérdida de contacto con entes de control	CRÍTICO	1 hora
Servidor de correo	CRÍTICO	1 hora
Servidor Web	ALTO	8 horas

Fuente: Elaboración propia.

Proceso.

Perdida de comunicación con proveedores de internet

Dado el caso se debe tomar las acciones siguientes:

a) Contactar a la empresa proveedora de internet, mediante llamadas telefónicas.

b) Informar sobre el percance

c) Informar a cada área sobre el tiempo de solución al problema, mediante llamadas telefónicas.

d) Realizar un informe técnico y entregar a la Gerencia General.

e) Avisar a los usuarios sobre la solución, mediante llamadas telefónicas a cada jefe de área.

Falla de equipos de comunicación SWITCH, FIBRA ÓPTICA, MODEM, PATCH CORD

Dado el caso se debe tomar las acciones siguientes:

a) Informar a cada área sobre el tiempo de solución al problema, mediante llamadas telefónicas.

b) Identificar el dispositivo dañado.

c) Realizar cambio del dispositivo

d) Informar a cada área sobre la solución, mediante llamadas telefónicas.

4.10.9. Escenario 6: error humano en la operación (sistema financiero).

Impactos y servicios afectados.

Los impactos y servicios afectados para este escenario se describen en la Tabla 26.

Tabla 26. *Impactos y servicios afectados en escenario 6*

ERROR HUMANO EN LA OPERACIÓN (SISTEMA FINANCIERO).	
IMPACTOS	SISTEMAS O SERVICIOS AFECTADOS
Molestias en los clientes y socios de la institución. Mala reputación. Descuadre de caja. Pérdida de dinero.	Sistema Financiero

Fuente: Elaboración propia.

Causas.

- Mala digitación de números de cuentas a la hora de depósitos o retiros
- Mala digitación en transferencias
- Mala entrega de la cantidad de dinero en caja.
- Descuadre de caja.

Recursos de contingencia.

- Manual de procedimientos del sistema financiero.
- Manual de seguimiento y control de quejas y reclamos.

Nivel de prioridad y tiempos aceptables de caída.

El nivel de prioridad y los tiempos aceptables de caída para cada recurso involucrado en este escenario se describen en la Tabla 27.

Tabla 27. *Nivel de prioridad y tiempos aceptables de caída para el escenario 6*

RECURSO	NIVEL DE PRIORIDAD	TIEMPO ACEPTABLE DE CAIDA
Descuadre de caja	ALTO	8 horas
Digitación de cuentas incorrecta	CRÍTICO	1 hora
Mala entrega del dinero de retiros	CRÍTICO	1 hora

Fuente: Elaboración propia.

Procedimiento.

El procedimiento para este escenario es el siguiente:

a) Identificar el problema y las posibles causas

b) Verificación de los datos a cargo del administrador del sistema comprometido

c) En caso de que la causa sea la falta de dinero en la contabilidad de caja, se debe realizar un levantamiento de evidencias

d) Aplicación del manual Técnico y Operativo del sistema WEBCOOP, para dar solución al inconveniente.

e) Detallar un informe técnico.

COOPERATIVA DE AHORRO Y CRÉDITO DE INDIGENAS "CHUCHUQUI" LTDA.		
PLAN DE RECUPERACIÓN		
	**Revisado por:**	Ing. Darío Castañeda /Jefe Departamento de Tecnología. Ing. Marcelo Yamberla / Asistente de Tecnología
	Aprobado por:	Ing. Darío Castañeda /Jefe Departamento de Tecnología
	Fecha de aprobación:	24 de septiembre de 2016 - Acta 318 R (31)

4.11. PLAN DE RECUPERACIÓN

Para este plan se considerará el escenario de indisponibilidad del centro de cómputo el cual es considerado con un grado de criticidad muy elevado, para lo cual para su compensación es recomendable, que la COAC cuente con un lugar alterno de aproximadamente $6m^2$ de forma rectangular, en el cual se pueda montar los equipos de contingencia haciendo uso de los backups pertinentes.

El proceso de implementación de este lugar alterno de procesamiento de datos se lo considerará en el Plan Estratégico del periodo 2018-2020 en diferentes fases, debido a la situación financiera actual en la que se encuentra la cooperativa.

4.11.1. Objetivo.

Establecer alternativas de recuperación de servicios ante un incidente crítico, tal que obligue a la utilización de equipos de contingencia y backups, para la restitución del modelo de negocio de la institución.

4.11.2. Escenario: indisponibilidad del centro de cómputo (destruccion del sitio de servidores).

Impactos y servicios afectados.

Los impactos y servicios afectados para este escenario se los describe en la Tabla 28.

Tabla 28. *Impactos y servicios afectados en escenario 6*

FALLA DE UN SERVIDOR	
IMPACTOS	SISTEMAS O SERVICIOS AFECTADOS
Caída del modelo de negocio Pérdida de comunicación con los entes de regulación. Molestias en los clientes y socios de la institución. Pérdida de datos. Daños de los equipos informáticos (servidores). Pérdida de Hardware y Software. Nueva inversión para la institución.	Todos los servicios de la institución se ven afectados.

Fuente: Elaboración propia.

Causas.

- Incendio
- Atentado terrorista
- Corto Circuito
- Terremoto

Recursos de contingencia.

Si es necesario, el hardware y software deben activarse o adquirirse. Las estrategias básicas para disponer de equipo de reemplazo son:

- Acuerdos con proveedores: Se establecen acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.
- Inventario de equipos: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa.
- Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación.

- Almacenar un equipo sin usar es costoso, pero permite que la recuperación comience más rápidamente.

- Considerar la posibilidad de un desastre extendido que requiere reemplazos masivos de equipos y retrasos del transporte.

- Mantener listas detalladas de necesidades de equipo y especificaciones dentro del plan de contingencia.

Recursos de Contingencia Generales

- Router (Suministrado por el proveedor de Internet).

- Servidores y Equipos de Comunicación (Switchs, Fibra, etc.).

- Gabinete de Comunicaciones y Servidores.

- Materiales y herramientas para cableado estructurado.

- UPS y Equipos de aire acondicionado.

- Backup de los Sistemas.

- Instaladores de las aplicaciones, de Software Base, Sistema Operativo, Utilitarios, etc.

Recursos de Contingencia Específicos

Dentro de los recursos de contingencia específicos se consideran los equipos y servidores de mayor importancia para el desarrollo de las actividades financieras de la cooperativa, detallando sus características para que en caso de emergencia no se vean afectados los servicios por culpa del hardware de los equipos de respaldo, por lo que se considera que los recursos de contingencia sean de características similares o de mayor capacidad. En la Tabla 29 se enlistan dichos recursos de respaldo.

Tabla 29. *Recursos de contingencia Específicos*

EQUIPOS DE REMPLAZO
HP ProLiant ML310e Gen8 v2 DATA Torre (4 U Rack) / (1)Intel Xeon Quad-Core E3-1240v3 (3.4 GHz 8MB, 80W)/8GB (1x8GB) PC3-12800E DDR3 UDIMM / (1) 2TB Non-hot plug SATA / HP Ethernet 1Gb2-port 332i Adapter / Array Controller B12oi SATA (0/1/1+0)/DVD / TECLADO / Mouse / (1) HP 350W Non-hot plug Power Supply /2 ventiladores Non-hot plug, Non-Redundant
HP 2TB 6G SATA 7.2K 3.5in NHP MDL HDD
HP Hh SATA DVD RW Jb Kit
HP ProLiant DL180 Gen9 SATA / SAS-LFF 2U Rack /Intel Xeon Six-Core: E5-2609v3 (1.9GHz, 15MB, 85W) / 8GB (1x8GB Registered DIMMs, 2.133 MHz)/ No Incluye Discos Duros / HP Ethernet 1Gb 2- port i350 Adapter / HP H240 FIO Smart Host Bus Adapter (0/1/1+0/5) / (1) HP 550W FIO Power Supply /3 ventiladores Hot plug, Non-Redundant. Six-Core Intel Xeon Processor E5-2609v3 (1.19 Ghz, 85 Watts) Discos 500 RAID HP 500GB 6G SATA 7.2k 3.5in SC MDL HDD Memoria RAM adicional HP 8GB 1Rx4 DDR4 2133Mhz – RDIMM Fuentes redundantes HP 800W/900W Gold AC Power Input Module Kit instalador de Fuentes redundantes HP Server RPS Backplane Kit DVD-RWRITER SAMSUNG SE-208DB SLIM 8X USB 2.0-3.0 EXT
Computador ATX Case Kit E Laser Negro Gris WSC 6360 Board Gigabyte H81M S LGA 1150 4ta G Procesador Intel Core i5 4460 32 Ghz 1150 Disco Duro 1TB Sata Toshiba PC 7200RMP Dimm 4Gb DDR3 PC 1600Mhz Kingston DVD RW LG Super Multi SATA 24x DVD 52X CD Lector Multi Card 3.5 Interno Monitor 20 LED LG 20M35A B 1600X900 98 31 Regulador Best Power 1200SM Supresor de picos Omega CDP 6 Tomas
1 UPS APC SMART RT 3000VA ENTRADA 110-120V

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Procedimiento.

La COAC Chuchuqui Ltda., al no contar con un espacio de infraestructura alterno, deberá establecer un lugar apropiado en la misma institución, lo cual aplicaría sólo cuando la indisponibilidad del centro de cómputo no haya afectado al resto de la infraestructura, para lo cual se debe seguir los siguientes pasos:

a) Analizar todas las pérdidas de equipos y materiales con la ayuda de grupos especiales, para mantener las evidencias del incidente.

b) Establecer todos los activos que requieren ser adquiridos, basándose en el inventario de activos.

c) Establecer un lugar alterno dentro de la misma institución.

d) Montar la infraestructura de red dependiendo del mapa de red de estructura institucional.

e) Realizar pruebas de funcionamiento.

f) Restablecer las actividades de la COAC Chuchuqui Ltda.

<table>
<tr><th colspan="3">COOPERATIVA DE AHORRO Y CRÉDITO DE INDIGENAS “CHUCHUQUI” LTDA.</th></tr>
<tr><th colspan="3">PRUEBAS DE VERIFICACIÓN Y EVALUACIÓN</th></tr>
<tr><td rowspan="3"> 
</td><td>Revisado por:</td><td>Ing. Darío Castañeda /Jefe Departamento de Tecnología.
Ing. Marcelo Yamberla / Asistente de Tecnología</td></tr>
<tr><td>Aprobado por:</td><td>Ing. Darío Castañeda /Jefe Departamento de Tecnología</td></tr>
<tr><td>Fecha de aprobación:</td><td>24 de septiembre de 2016 - Acta 318 R (31)</td></tr>
</table>

4.12. PRUEBAS DE VERIFICACIÓN Y EVALUACIÓN

4.12.1. Objetivo.

Verificar y probar ciertos planes o procedimientos que forman parte del Plan de contingencia en general, para garantizar que la metodología utilizada es útil conservar los tres principios de la seguridad de la información (integridad, confiabilidad y disponibilidad).

4.12.2. Plan de Verificación.

Para la verificación de un Plan de Contingencia es de suma importancia que las pruebas de validación de un plan se las lleve a cabo bajo la supervisión de una autoridad independiente. Pero para los sistemas de menor importancia, la verificación puede realizarse de forma interna.

A las pruebas de verificación comúnmente se las denomina pruebas de calidad y estas pueden incluir (Instituto Veracruzano de acceso a la información, 2012):

- Ejecutar pruebas en equipos sometiéndolos a condiciones que simulen las operaciones reales de la institución.
- Comprobar el correcto funcionamiento de los programas para asegurar que se siguen los estándares apropiado.
- Asegurar que siga un procedimiento de documentación adecuado y que se

encuentre bien detallado.

- Garantizar que los sistemas sean capaces de operar bajo condiciones normales, pero también respondan a condiciones de imprevisto.

- Garantizar que se cuente con las medidas correspondientes de seguridad y que estas se encuentren relacionadas con las normas institucionales.

4.12.3. Procedimientos para las Pruebas del Plan de Contingencia.

Introducción

Todos los planes de contingencia deben ser probados para demostrar su habilidad de mantener la continuidad de los procesos críticos de la COAC CHUCHUQUI Ltda.

Objetivos específicos

- Comprobar que el plan de contingencia está adecuado para proporcionar el nivel esperado de ayuda en la confrontación de eventualidades en los procesos críticos de la COAC Chuchuqui Ltda., probando la efectividad de los procedimientos expuestos en el plan.

- Permitir una estimación detallada de la valoración de los costos de operación en el instante que se produzca una contingencia.

Métodos para Realizar Pruebas de Planes de Contingencia

a) Prueba de Escritorio

Esta prueba de escritorio se asemeja a un examen escrito a través de un conjunto de preguntas típicas. Para esta prueba debe haber una capacitación previa, que asegure que los funcionarios tengan el conocimiento necesario para resolver satisfactoriamente todas las preguntas. Por medio de esta prueba se puede analizar las capacidades gerenciales de los funcionarios con cargos principales. (Instituto Veracruzano de acceso a la información, 2012)

El encargado y todo el personal deben tener la facilidad de utilizar el plan de

contingencia para resolver las respuestas a cada situación planteada. Esta prueba también ayuda a comprender el pensamiento de reacción de los funcionarios en caso de una contingencia, lo que permite que pueda que surjan ideas que pueden ser tomadas en cuenta para el mejoramiento del Plan de Contingencia.

b) Simulación en Tiempo Real

Al tratarse de pruebas de simulación real, en una institución, en lo posible se las debe realizar en un tiempo adecuado, en el cual se eviten interrupciones en el desarrollo normal de las actividades de la cooperativa. (Instituto Veracruzano de acceso a la información, 2012)

4.12.4. Preparaciones PRE Prueba.

c) Garantizar que todo el personal tenga acceso al plan de contingencia.

d) Comprobar si se han asignado responsabilidades.

e) Verificar que el plan ya se encuentre aprobado por consejo directivo de la institución.

f) Realizar una capacitación a todo el personal involucrado, incluyendo una guía completa que ayude a cubrir todos los requerimientos para alcanzar los objetivos.

g) Establecer la fecha y hora en la que todo el personal se encuentre disponible para la ejecución.

h) Garantizar la disponibilidad del entorno donde se realizará la prueba.

i) Realizar una documentación de los resultados obtenidos, la finalidad es aprender y descubrir las vulnerabilidades y encontrar una solución eficaz para evitar riesgos críticos.

En la Figura 17 se observa el esquema para la correcta realización de pruebas de verificación del Plan de Contingencia.

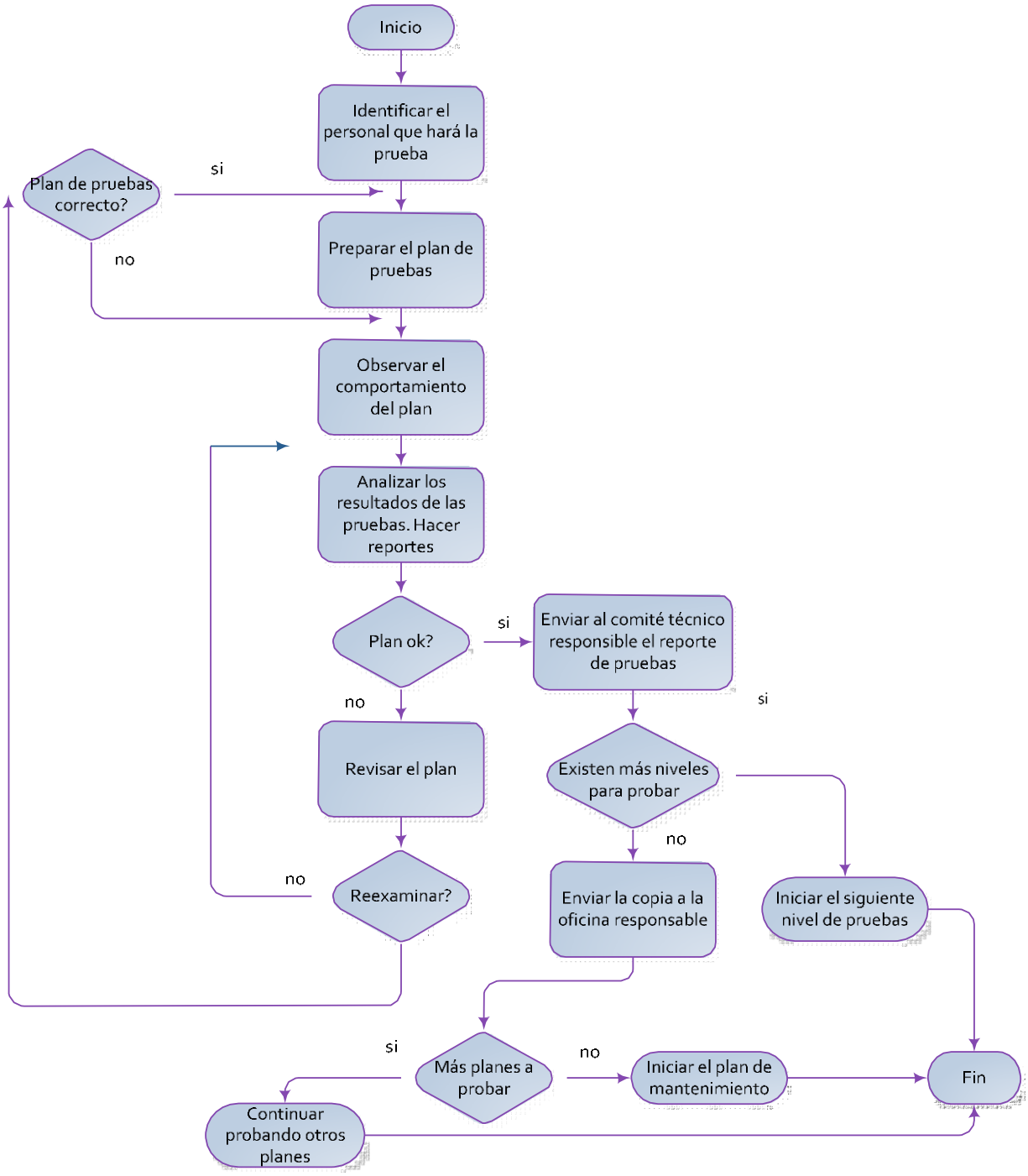


Figura 17: Procedimiento de pruebas del plan de contingencia.

Fuente: Instituto Veracruzano de acceso a la información. (2012). Plan de contingencia Informático. Recuperado el 13 de julio de 2016 de: http://ivai.org.mx/DatosPersonales/Archivos/Interes/Extracto_PLAN_DE_CONTINGENCIA_IVAI.pdf

4.12.5. Alcance del Entrenamiento.

Es importante desarrollar un programa corporativo que cubra las partes esenciales requeridas para comunicar los procedimientos del proceso de recuperación de los procesos de negocio de la Cooperativa. (Instituto Veracruzano de acceso a la información, 2012)

- La capacitación se debe llevar a cabo de manera exhaustiva para que se llegue a estar familiarizado con todos los aspectos del proceso de recuperación.
- La capacitación debe cubrir todos aspectos de la sección de procedimiento de los planes de recuperación dependiendo del escenario que se esté evaluando. (Instituto Veracruzano de acceso a la información, 2012)

4.12.6. Revisión y Actualización.

El seguimiento permanente permite conocer la evolución, los cambios en condiciones actuales, el cumplimiento de metas propuestas y los ajustes requeridos. (Instituto Veracruzano de acceso a la información, 2012)

La evaluación periódica del Plan de Contingencia se realiza a través de:

- Simulacros
- Simulaciones
- Evaluación del desempeño por evento

A continuación, en la Tabla 30 se detalla las pruebas que se han realizado, para la evaluación del plan de contingencia. Para estas pruebas se ha empleado el método de simulación en tiempo real, donde se ha generado algunos escenarios de pruebas, tratando se hacer lo más real posible, para así poder determinar un tiempo aproximado en que se puede dar solución a los incidentes.

Para mayor detalle de los resultados podemos ver las hojas de registro en el ANEXO H. Así, como también el formato para el registro de las pruebas se encuentra en el ANEXO G.

Tabla 30. *Resumen de pruebas de verificación del plan de contingencia ejecutadas.*

PRUEBAS Y EVALUACIÓN EJECUTADAS					
ESCENARIO:	Daño o quemadura del servidor del sistema financiero.				
Objetivo	Aspectos a evaluar	Requerimientos	Procedimiento	Resultados	Observaciones
Recuperar la continuidad del Plan de negocio de la COAC Chuchuqui Ltda., en un tiempo mínimo para el escenario de daño o quemadura del servidor financiero.	Tiempo de respuesta para la continuidad del negocio.	Red de comunicación habilitada. Servidos de respaldo disponible y habilitado. Backup del sistema financiero ejecutado cada 15 días. De ser necesario contar con manuales técnicos (Manual Técnico de carga de backup) y herramientas de software de conexión remota (WinSCP y Putty)	Sacar el respaldo del sistema financiero (10 min y 44 seg). Carga del sistema financiero al servidor de respaldo (8 min y 50 seg). Sacar el backup de la base de datos de sistema financiero (23 seg). Carga del backup de la base de datos en el nuevo servidor (51min y 24seg). Ajustes y corrección para la ejecución del sistema financiero (2 min) Ajustes del direccionamiento del nuevo servidor (1 min). Pruebas del funcionamiento (5 min).	Se implementó el sistema financiero en el servidor de respaldo, con los parámetros de la fecha calendario y se verificó el desarrollo normal del sistema para la continuidad del plan de negocios de la COAC. Para ello se tomó como base, el Manual de Carga de backup. El tiempo de respuesta fue aproximadamente 1 hora con 20 minutos, lo cual no se encuentra dentro del tiempo aceptable de caída del servicio.	El tiempo de recuperación se encuentra elevado, de acuerdo a pruebas que se han realizado anteriormente en el servidor de producción, por lo cual se recomienda analizar los recursos del servidor de respaldo, para mejorar los tiempos de respuesta.

			Restablecimiento de las actividades.		

ESCENARIO: Indisponibilidad de energía eléctrica en la institución.

Objetivo	Aspectos a evaluar	Requerimientos	Procedimiento	Resultados	Observaciones
Recuperar la continuidad del Plan de negocio de la COAC Chuchuqui Ltda., en un tiempo mínimo para el escenario de indisponibilidad de energía eléctrica en la institución.	Tiempo de respuesta para encender el generador eléctrico. Tiempo de disponibilidad del sistema biométrico del Data Center.	Disponibilidad del generador con suficiente combustible para su funcionamiento. Disponibilidad del UPS del Data Center	Consulta del tiempo que demora en regresar el servicio mediante una llamada a la empresa eléctrica. (2 min) Revisión del combustible necesario para el generador eléctrico. Carga d combustible en el generador (3 min) Encendido del generador (5min) Si el tiempo de restablecimiento del servicio es muy extenso, de forma preventiva se recomienda adquirir más combustible para el abastecimiento durante todo el lapso de la incidencia.	Se pudo restablecer la continuidad del plan de negocio, con la ayuda del generador eléctrico que abasteció para el restablecimiento de las actividades con un tiempo de respuesta aproximado de 13 minutos. Se pudo comprobar que el UPS pudo abastecer a los equipos que se encuentran dentro del Data Center y que el biométrico estuvo funcionando todo el tiempo, gracias a sus baterías de backup, que, según las especificaciones del fabricante, tienen una duración de 4 a 5 horas.	El sistema de climatización del Data Center no encuentra alimentado por el UPS por lo cual no entró en funcionamiento, al igual que los ventiladores de los racks, por lo cual se recomienda que estos se conecten directamente al UPS. Hay que tomar en cuenta que entre más dispositivos se conecten al UPS, su capacidad de tiempo de respaldo de energía disminuye.

ESCENARIO: Corte del servicio de internet

Objetivo	Aspectos a evaluar	Requerimientos	Procedimiento	Resultados	Observaciones
Recuperar la continuidad del Plan de negocio de la COAC Chuchuqui Ltda., en un tiempo mínimo para el escenario de corte del servicio de internet.	Tiempo de respuesta por parte de los suministradores del servicio. Tiempo de respuesta para el cambio de un dispositivo en mal funcionamiento.	Teléfonos de contactos con los proveedores de servicio de internet. Disposición de materiales contingencia.	Comunicación con los proveedores del servicio de internet. (2 min) Establecimiento del servicio por parte de proveedores. según el reglamento institucional del suministrador, el tiempo máximo de restablecimiento es de 45 minutos. Si el problema es por causa del mal funcionamiento de un dispositivo, se procede a identificar el elemento afectado. (5 min) Cambio del equipo afectado. (7 min) Pruebas de funcionamiento.	Para la consideración del tiempo de respuesta por parte de los suministradores, se realizó una llamada de simulación al proveedor explicando que se trata de un simulacro, para conocer detalles de cuánto tiempo se tardan en dar solución. Tomando esos aspectos, el tiempo aproxima de restablecimiento del servicio es de 47 min. Para la consideración de falla de un dispositivo se tomó en cuenta que la cooperativa no cuenta con todos los recursos de contingencia para este escenario. Por lo cual se añade un tiempo de adquisición de los dispositivos (2 a 3 horas).	Se pudo establecer tiempos aproximados para el restablecimiento del servicio, y en comparación al tiempo aceptable de caída (8 horas), los tiempos si se encuentran dentro de la meta establecida.

ESCENARIO: Falla de equipo de comunicación.

Objetivo	Aspectos a evaluar	Requerimientos	Procedimiento	Resultados	Observaciones
Recuperar la continuidad del Plan de negocio de la COAC Chuchuqui Ltda., en un tiempo mínimo para el escenario de falla de un equipo de comunicación.	Tiempo de cambio de equipo de comunicación	Mapa de la red de estructura institucional. Equipos de remplazo	Identificar las causas y el equipo de falla de la comunicación. (5 min) Análisis breve sobre si tiene solución o es necesario cambiar el equipo. (2 min) Comprobar la existencia del equipo de remplazo, caso contrario, realizar la adquisición del dispositivo. (Si existe 2 min, si no existe en la institución 2 a 3 horas) Desmontar el equipo dañado y montar el nuevo. (3 min) Cargar la configuración del equipo. (10 min)	Se realizó la simulación con la falla de un switch, donde la institución no cuenta con la existencia de un remplazo, por lo que el tiempo se adquisición se suma. No existen archivos de configuración preparados para los dispositivos de red, por lo que el tiempo de configuración se incrementa un poco. El tiempo aproximado de respuesta es un aproximado de 3 horas con 20 minutos.	Debido a que la institución no cuenta con los equipos de contingencia, el tiempo de respuesta a la incidencia excede el tiempo aceptable de caída del servicio. Por lo cual se recomienda la adquisición de este tipo de dispositivos.

ESCENARIO: Ataque de virus a nivel de software

Objetivo	Aspectos a evaluar	Requerimientos	Procedimiento	Resultados	Observaciones
Mantener la continuidad del Plan de negocio de la COAC Chuchuqui Ltda.,	Tiempo que demora el software antivirus en reaccionar.	Tener actualizado y licenciado el antivirus en todos los dispositivos de	Creación de malware en una máquina virtual con Kali Linux.	Se realizó satisfactoriamente la prueba de ataque de virus	Todo el proceso se realizó con éxito, obteniendo buena respuesta del

en un tiempo mínimo para el escenario de ataque de virus a nivel de software.	la COAC. Malware creado con fines de pruebas.	Pasar el virus al equipo que va a ser sometido a la prueba. Ejecutar el malware y esperar la respuesta del antivirus. Una vez que el antivirus le bloquea la acción del malware, se procede a la eliminación del malware.	o malware, donde al ser ejecutado, la protección que brinda el antivirus ESET NOD32 bloqueó inmediatamente el proceso del malware. Se logró eliminar el malware satisfactoriamente. El procedimiento de detección del virus y eliminación no tardó más de 2 minutos.	antivirus.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

COOPERATIVA DE AHORRO Y CRÉDITO DE INDIGENAS "CHUCHUQUI" LTDA.		
PLAN DE MANTENIMIENTO		
	**Revisado por:**	Ing. Darío Castañeda /Jefe Departamento de Tecnología. Ing. Marcelo Yamberla / Asistente de Tecnología
	Aprobado por:	Ing. Darío Castañeda /Jefe Departamento de Tecnología
	Fecha de aprobación:	24 de septiembre de 2016 - Acta 318 R (31)

4.13. PLAN DE MANTENIMIENTO

Este plan es muy necesario dentro de una institución, debido a que toda organización, sin importar de que tipo sea, se encuentran sometidas a cambios en todos los niveles. Especialmente cuando se habla de cambios, las tecnologías de información son las que más sufren de este fenómeno, por lo cual es necesario tener un plan de mantenimiento que permita a la institución adaptarse a los cambios y no perder la competitividad en el modelo de negocio.

Por lo cual es necesario que todo el Plan de Contingencia se mantenga actualizado continuamente. Cuando se desee hacer cambios en el plan de contingencia, la siguiente guía será de mucha ayuda, ya que se establecen varios parámetros y mediadas que se deben considerar para la gestión de controles de seguridad de la información.

Y para ello se debe seguir un procedimiento formal, el cual se detalla más adelante en el control de **Gestión de Cambios** en el dominio de **Seguridad en la Operativa**.

4.14. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Gestión de incidentes en la seguridad de la información.**
	Control:	**4.14.1. Gestión de incidentes en la seguridad de la información y mejoras.**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Garantizar la existencia de documentos coherentes y eficaces para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades descubiertas en el análisis de riesgos.

4.14.1.1. Responsabilidad y Procedimientos.

Control

Responsabilidades y procedimientos de gestión deben establecerse para garantizar una respuesta más ágil, eficaz y de forma ordenada a los incidentes de seguridad de la información.

Las siguientes directrices para las responsabilidades y los procedimientos de gestión en materia de gestión de incidentes de seguridad de información deben ser considerados:

a) Responsabilidades de gestión deben ser establecidos para asegurar que los siguientes procedimientos se desarrollan y se comunican de manera adecuada dentro de la organización.

- Procedimientos para la planificación de respuesta a incidentes y preparación;
- Procedimientos de vigilancia, detección, análisis y presentación de

informes de eventos de seguridad de la información e incidentes;

- Procedimientos para las actividades de gestión de registro de incidentes;
- Procedimientos para el manejo de las pruebas forenses;
- Procedimientos para la evaluación y decisión sobre los eventos de seguridad de la información y la evaluación de debilidad seguridad de la información;
- Los procedimientos de intervención incluidos los de escalada, una recuperación controlada de un incidente y la comunicación a las personas u organizaciones internas y externas.

b) Procedimientos establecidos deben asegurar que:

- El personal competente maneje los asuntos relacionados con incidentes de seguridad de la información dentro de la organización;
- un punto de contacto para la detección y notificación de incidentes de seguridad se implementa;
- Contacto con las autoridades apropiadas grupos de interés externos o foros que se ocupan de las cuestiones relacionadas con los incidentes de seguridad de la información se mantienen;

4.14.1.2. Notificación de los eventos de la seguridad de la información.

Control

Los eventos de seguridad de la información deben comunicarse a través de medios de gestión apropiados, de la forma más rápida posible.

Todos los empleados deben ser conscientes de su responsabilidad de informar de los eventos de seguridad de la información lo más rápidamente posible. También deben ser conscientes del procedimiento de notificación de eventos de seguridad

de la información y a los puntos de contacto con los que deberían ser reportados los eventos.

Situaciones que se deben considerar para la notificación de eventos:

a) Control de seguridad inefectivo;

b) Incumplimiento de la integridad, confidencialidad y disponibilidad de la información;

c) Errores humanos;

d) Incumplimiento de las normas de seguridad física;

e) Cambios no autorizados de los sistemas de información;

f) Malfuncionamiento del software o hardware de los activos;

g) Violación de accesos.

4.14.1.3. Notificación de los puntos débiles de la seguridad.

Control

Los funcionarios de la institución deben notificar o reportar las vulnerabilidades que ellos piensen que sean sospechas, tras la observación o análisis de la información necesaria de los sistemas de información o servicios.

Todos los empleados tienen la responsabilidad de notificar a las autoridades competentes sobre los que consideren que pueden ser puntos débiles para la institución, para que se lleve a cabo un análisis correspondiente, y en un caso crítico la notificación debe ser los más pronto posible.

4.14.1.4. Valoración de los eventos de seguridad de la información y toma de decisiones.

Control

Las eventualidades dentro de la seguridad de la información deben ser evaluados

y se debe decidir si han de ser clasificados como incidentes de seguridad de la información.

Los profesionales que van a ser los encargados de evaluar cada asunto de seguridad de la información, debe tomar en cuenta la clasificación de incidentes y decidir si el evento debe ser clasificado como un incidente de seguridad informática. La clasificación y priorización de los incidentes pueden ayudar a identificar el impacto y el alcance de un incidente.

4.14.1.5. Respuesta a los incidentes de seguridad.

Control

Los incidentes de seguridad informática deben ser respondidos de acuerdo con los documentos de procedimientos.

Las eventualidades deben ser atendidas por personal capacitado y autorizado para dar alguna respuesta al incidente, ya sea de la misma institución o sea un profesional externo.

La respuesta de control debe incluir lo siguiente:

a) Recolectar evidencia tan pronto como sea posible, después de la eventualidad;

b) Realización de un análisis forense de la seguridad de la información;

c) Asegurar que toda actividad de respuesta implicada, esté correctamente aplicada;

d) Comunicación sobre información relevante que toda la institución o personal específico deba tener conocimiento.

e) Hacer frente a la vulnerabilidad encontrada que causó o contribuyó al incidente;

f) Una vez que el incidente haya sido resuelto, debe existir una documentación que sirva como respaldo para la solución de futuros

incidentes.

4.14.1.6. Aprendizaje de los incidentes de seguridad y recopilación de evidencias.

Control

Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad o impacto de incidentes en el futuro.

La institución debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

4.15. POLÍTICAS DE SEGURIDAD.

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Políticas de Seguridad de la Información**
	Control:	**4.15.1. Directrices de la dirección en seguridad de la información**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Proporcionar orientación y apoyo a la gestión de seguridad de la información, de acuerdo con los requerimientos del negocio y reglamentos pertinentes.

DESCRIPCIÓN

El departamento de Tecnología en conjunto con la Administración, deben establecer una orientación política clara en concordancia con los objetivos de negocio, así como también debe demostrar apoyo y compromiso con la seguridad de la información, mediante la emisión y mantenimiento de una política de seguridad de la información en toda la organización.

4.15.1.1. Conjunto de políticas para la seguridad de la información.

Control

Un documento de políticas de seguridad de la información debe ser aprobado por el Consejo de administración y ser publicado y comunicado a todos los empleados y colaboradores externos.

El documento de política de seguridad de la información debe indicar compromiso de la administración y se establece un enfoque de organización para la gestión de seguridad de la información. El documento de política debe contener declaraciones relativas a:

- Una definición de seguridad de la información, sus objetivos generales y el alcance y la importancia de la seguridad como un mecanismo que permite el intercambio de información (véase la introducción);
- Una declaración de intención de la administración, el apoyo a los objetivos y principios de la información la seguridad en línea con la estrategia y los objetivos de negocio;
- Un marco para el establecimiento de objetivos de control y controles, incluyendo la estructura de riesgo evaluación y gestión de riesgos;
- Una breve explicación de las políticas de seguridad, los principios, las normas y el cumplimiento.

Los requisitos de especial importancia para la organización, incluyen:

- El cumplimiento de los requisitos legales, reglamentarios y contractuales;
- Educación de seguridad, formación y sensibilización de los requisitos;
- Gestión de la continuidad del negocio;
- Una definición de las responsabilidades generales y específicas para la gestión de seguridad de la información, incluyendo la comunicación de

incidentes de seguridad de la información;

- Las referencias a la documentación que puede apoyar la política.

Las políticas de seguridad de la información deben ser comunicadas a toda la organización a los usuarios en una forma que sea relevante, accesible y comprensible para el lector previsto. Si la información de alguna política de seguridad se distribuye fuera de la organización, se debe tener cuidado de no revelar información sensible.

4.15.1.2. Revisión de la política para la seguridad de la información.

Control

La revisión de las políticas de seguridad de la información debe realizarse en intervalos planificados. Los cambios no significativos de los intervalos pueden ocurrir, pero deben asegurar su conveniencia, adecuación y eficacia.

La política de seguridad de la información debe tener un propietario de aprobación, en relación a la responsabilidad de gestión para el desarrollo, revisión y evaluación de la política de seguridad. La revisión debe incluir la evaluación de las oportunidades de mejora de la política de seguridad de la información de la organización y acercarse a la gestión de seguridad de la información en respuesta a cambios en el entorno de la organización, circunstancias del negocio, condiciones legales, o entorno técnico.

La revisión de la política de seguridad de la información debe tener en cuenta los resultados de la gestión críticas. Si se incluye un calendario o un periodo de la revisión, no es necesario definir procedimientos de gestión.

La entrada a la revisión por la dirección debe incluir información sobre:

- Resultados de las revisiones independientes;
- Estado de las acciones preventivas y correctivas;
- Los resultados de anteriores revisiones de la dirección;

- El rendimiento del proceso y cumplimiento de la política de seguridad de la información;
- Cambios que podrían afectar el enfoque de la organización para la gestión de seguridad de la información, incluyendo cambios en el entorno de la organización, circunstancias del negocio, la disponibilidad de recursos y el entorno técnico;
- Las tendencias relacionadas con las amenazas y vulnerabilidades;
- Información de incidentes de seguridad de la información;
- Recomendaciones proporcionadas por las autoridades pertinentes.

Las Políticas, reglamentos y manuales que están puestas en marcha hasta la fecha de presentación de este documento y que han sido analizadas por el personal del Departamento de Tecnología, se encuentran detalladas en el ANEXO I.

4.16. ASPECTOS ORGANIZATIVOS DE SEGURIDAD DE LA INFORMACIÓN.

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Aspectos Organizativos de la Seguridad de la Información**
	Control:	**4.16.1. Organización Interna.**
	Destinatarios:	Nivel Directivo

OBJETIVO

Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización.

DESCRIPCIÓN

La administración debe asignar funciones relacionadas con la seguridad de la información y debe coordinar y examinar la aplicación de la seguridad en toda la organización.

Es necesario tener creada y disponible dentro de la organización una lista de contactos con especialistas o grupos de seguridad externos, incluidos las autoridades pertinentes, en caso de que se requiera una fuente de asesoramiento especialista en seguridad de la información. La lista de contactos también es necesaria para mantenerse al día con las tendencias industriales, supervisión de calidad y métodos de evaluación para proporcionar puntos de enlace adecuados al manipular los incidentes de seguridad de la información.

4.16.1.1. Asignación de Responsabilidades para la SI y segregación de roles.

Control

Se deben asignar y definir claramente las responsabilidades para la Seguridad de la Información, tareas y establecer áreas de responsabilidad ante cualquier eventualidad con la finalidad de reducir cualquier intento alteración no autorizada en sistema y resto de elementos que conforman la red de comunicaciones, así como también el mal uso de los activos de la organización.

Tomando como referente la seguridad de la información; las personas con mayor jerarquía que tengan responsabilidades de seguridad asignadas, están en la capacidad de delegar tareas de seguridad a los demás. Sin embargo, siguen siendo responsables y deben asegurarse de que cualquier tarea delegada se ha realizado correctamente.

La asignación de responsabilidades se lo realizará en consideración de las actividades que se relacionan con la seguridad de la información y basándose en las tareas establecidas en el documento de contrato de cada empleado, también se tomarán en cuenta aspectos definidos en las políticas de seguridad como se muestra en la Tabla 31.

Tabla 31. *Asignación de roles y responsabilidades*

PUESTO	ROLES	RESPONSABILIDADES
Jefe de Tecnología	Coordinador principal del Departamento de Tecnología	Evaluar, diseñar, actualizar e implementar soluciones tecnológicas que posibiliten mayor eficiencia en la ejecución de procesos, minimizando el riesgo informático y respondiendo oportunamente a las exigencias del crecimiento Institucional. Verificar que se realicen reuniones periódicas para revisión de políticas y plan de contingencia y de ser necesario, la actualización de los mismos. Tomar las decisiones significativas en caso de emergencia. Realización de informes sobre incidentes o algún cambio que puede afectar al enfoque de la seguridad de la información. Responsable de los procedimientos a seguir en una contingencia que afecte a las operaciones de la institución que se desenvuelven en el aspecto tecnológico. Coordinar las etapas para la ejecución del Plan de Contingencia Participar en los organismos de seguridad y salud ocupacional conforme a la ley Cumplir y hacer cumplir con las disposiciones contenidas en Reglamentos, Políticas, Manuales, Instructivos y Procedimientos que forman parte de los Documentos Normativos de la Institución, que le sean aplicables al puesto de trabajo Cumplir y hacer cumplir la normativa técnico-legal en materia de seguridad y salud ocupacional

Asistente de Tecnología	Coordinador de Sistemas y soporte técnico	Apoyar en el seguimiento del Plan Estratégico y Operativo del Sistema como parte integrante del Plan Estratégico Institucional. Apoyar en la administración del Firewall y velar por su buen funcionamiento. Apoyar en los requerimientos tecnológicos de entes de control interno y externo. Mantener actualizado un inventario de activos. Establecer listas actualizadas de contactos de autoridades, proveedores y grupos de interés especial. Realización de pruebas en caso de modificaciones en los sistemas. Establecer manuales técnicos y de usuario. Realización de copias de seguridad periódicamente. Monitorear y verificar el buen funcionamiento de los equipos de comunicación (Router y switch y las líneas RDSI) de las Oficinas

Fuente: Departamento de Recursos Humanos de la COAC Chuchuqui Ltda.

4.16.1.2. Contacto con las Autoridades.

Control

Se debe establecer contactos apropiados con las autoridades correspondientes a la zona donde se encuentra la institución, aquí se incluyen los números de emergencia. Para ello en la Tabla 32 se ha establecido una lista de contactos con sus respectivos números telefónicos. Hay que recalcar que para poder contactarse con las autoridades responsables de las instituciones gubernamentales se lo puede realizar a través del número de emergencia 911.

Tabla 32. *Contactos de autoridades*

Contacto	Número Telefónico
Bomberos	911
Policía Nacional	911
Ambulancia	911
Emelnorte	097 927 0745
CNT	06-2920-040
Municipio de Otavalo	06-2920-460 06-2924-566

Fuente: Elaboración propia.

4.16.1.3. Contacto con grupos de interés especial.

Control

Se debe tener una lista de contactos con grupos, foros, empresas o instituciones especializados en seguridad informática como se indica en la Tabla 33.

Tabla 33: *Contactos de grupos de interés especial*.

Contacto	Descripción	Número Telefónico
Webcoop	Sistemas Financieros	02-2081-266
Seyton	Soluciones Electrónicas y Telecomunicaciones	06-2607-949
Inforc-Ecuador	Seguridad Informática	02-2559-067 / 02-2227-766
Domotik	Ingeniería en Automatización y Seguridad	07-286-1630 / 0993779763
Word Computer	Proveedor de Hardware	06-2608-010
Equifax	Estado Crediticio de Socios	26020083 / 0986193984
Banco Central del Ecuador	Servicios Bancarios	Call Center: 1700 153 -153 / 02-3938-600
Greenetics	Seguridad Informática	02-6034-068

Fuente: Elaboración propia.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Aspectos Organizativos de la Seguridad de la Información.**
	Control:	**4.16.2. Dispositivos para movilidad y teletrabajo.**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

DESCRIPCIÓN

Se debe adoptar una política de apoyo y medidas de seguridad para gestionar el riesgo de la vulnerabilidad la red, a través de la intrusión mediante el uso de dispositivos móviles.

Cuando se usa el dispositivo móvil, se debe tener especial cuidado para asegurar que la información de la institución no se vea comprometida. La política de dispositivo móvil debe tener en cuenta el riesgo de trabajar con el dispositivo móvil en ambientes no protegidos.

4.16.2.1. Política de uso de dispositivos para movilidad.

Control

Se debe tener cuidado al usar dispositivos móviles en lugares públicos, salas y otras áreas de reuniones no protegidas. La protección debe estar en lugares en los que se restringe el acceso no autorizado para evitar la divulgación de la información almacenada y procesada por este dispositivo. Se debe usar técnicas de criptografía y cumplir con las responsabilidades de proteger la información de autenticación.

Se debe fomentar la concienciación personal sobre los riegos adicionales que resultan de la utilización de dispositivos móviles, por lo cual los trabajos que se

realizan de esta manera en organización deben ser supervisados.

Los dispositivos móviles son de uso personal y privado, no pueden ser prestados a terceros, para evitar el mal uso de la información que en ellos se encuentran.

4.16.2.2. Teletrabajo.

Al tratarse de una institución financiera, como tal no deben existir tareas o actividades de teletrabajo (a excepción de inspecciones para créditos) debido a que cualquier información es de suma importancia para la cooperativa.

En el caso de inspecciones para créditos financieros, se debe controlar la información que le es permitido llevar consigo al inspector, así como también la información que se le es permitido transmitir a los usuarios que están requiriendo el crédito.

4.17. SEGURIDAD LIGADA A RECURSOS HUMANOS.

Impulsamos el desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Seguridad Ligada a los Recursos Humanos.**
	Control:	**4.17.1. Antes de la contratación**
	Destinatarios:	Nivel Directivo

OBJETIVO

Asegurar que los empleados, contratistas y terceros usuarios a entender sus responsabilidades, que se consideren adecuadas para el cumplimiento de sus funciones, y así, reducir el riesgo de robo, fraude o mal uso de las instalaciones.

DESCRIPCIÓN

Las responsabilidades en relación a la seguridad de la información deberán dirigirse antes del empleo con las descripciones adecuadas del trabajo

establecidas en términos y condiciones de empleo.

Todos los candidatos a empleo, contratistas y usuarios de terceras partes deben ser adecuadamente seleccionados, especialmente para los trabajos delicados.

4.17.1.1. Investigación de Antecedentes.

Control

Se debe realizar controles de verificación a fondo sobre todos los candidatos para el empleo, contratistas y terceros usuarios; pero esto debe llevarse a cabo de acuerdo con las leyes, regulaciones y ética pertinente, proporcional a los requerimientos del negocio. Debe realizarse una clasificación de la información y riesgos percibidos para acceder a ella cuando sea necesario.

Los controles de verificación deben tener en cuenta toda la privacidad relevante, pero con la protección de los datos personales, lo se debería realizar siempre y cuando la legislación laboral lo permita, esto incluye:

a) La disponibilidad de las referencias de caracteres satisfactorios, por ejemplo, una referencia laboral y una referencia personal;

b) Un control del curriculum vitae del solicitante (para la integridad);

c) La confirmación de los títulos académicos y profesionales reivindicados;

d) Control de identidad independiente (pasaporte o documento similar);

e) Controles más detallados, como los controles de crédito o cheques y de los antecedentes penales

Cuando la persona se encuentre en una etapa de prueba de trabajo, ya sea en la cita inicial o en la promoción e implica que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular si éstos están manejando información sensible, por ejemplo, información financiera o información altamente confidencial, la organización también debe considerar, la realización de un control minucioso de las actividades.

Los procedimientos deben definir los criterios y limitaciones de las verificaciones de la información proporcionada por la persona a ser contratada, por ejemplo, quién es elegible para seleccionar la gente, y cómo, cuándo y por qué comprobaciones de verificación se deben llevar a cabo.

4.17.1.2. Términos y condiciones de contratación.

Control

Como parte de sus obligaciones contractuales, empleados, contratistas y terceros usuarios deben estar de acuerdo y firmar los términos y condiciones de su contrato de trabajo, que debe indicar tanto su responsabilidad como la de la institución para la seguridad de la información.

Los roles y responsabilidades de seguridad de los empleados, contratistas y terceros usuarios deben definirse y ser documentados en conformidad con la política de seguridad de la información de la institución.

Los roles y responsabilidades de seguridad deben incluir la obligación de:

- Aplicar y actuar de acuerdo con las políticas de seguridad de la información de la institución;
- Proteger los activos del acceso no autorizado, divulgación, modificación, destrucción o interferencia;
- Ejecutar procesos o actividades particulares de seguridad;
- Garantizar la responsabilidad sobre las acciones tomadas por persona para cumplimiento de sus asignaciones;
- Informe de los eventos de seguridad o eventos potenciales u otros riesgos de seguridad para la organización.
- Las responsabilidades para la clasificación de la información.

La institución debe asegurarse de que los empleados, contratistas y terceros usuarios están de acuerdo con los términos y condiciones relativas a seguridad de

la información apropiadas. También deben tener conocimiento del grado de acceso que tienen permitido en los activos de la organización relacionados con los sistemas y servicios de información.

En su caso, las responsabilidades contenidas dentro de los términos y condiciones de empleo deberían continuar por un período definido después de la finalización del empleo.

Otras consideraciones que se deben tomar en cuenta para el proceso de contratación se establecen el en REGLAMENTO INTERNO, aprobado por consejo administrativo el 09 de noviembre de 2014.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Seguridad Ligada a los Recursos Humanos.**
	Control:	**4.17.2. Durante la contratación**
	Destinatarios:	Nivel Directivo

OBJETIVO

Asegurar que los empleados y contratistas son conscientes de sus responsabilidades a cumplir para la seguridad de la información.

DESCRIPCIÓN

Deben ser definidas responsabilidades de gestión para garantizar que la seguridad se aplica a lo largo del todo el tiempo de empleo del individuo dentro de la organización.

Un nivel adecuado de sensibilización, educación y capacitación en procedimientos de seguridad y el uso correcto de instalaciones de procesamiento de información, se deben proporcionar a todos los empleados, contratistas y

terceros usuarios para minimizar los posibles riesgos de seguridad.

4.17.2.1. Responsabilidades de Gestión.

Control

En departamento de cumplimiento debe exigir a los empleados, contratistas y usuarios la aplicación de políticas y procedimientos de seguridad de acuerdo a lo establecido por la institución.

Los responsables de gestión deben garantizar que los empleados, contratistas y usuarios:

- Estén adecuadamente informados sobre sus roles y responsabilidades de seguridad de la información antes de dar autorización de acceso a los sistemas de información o de información sensible;
- Están dotados de guías de seguridad y expectativas de su papel dentro de la organización;
- Están motivados para cumplir con las políticas de seguridad de la organización;
- Logren un nivel de conciencia en materia de seguridad, pertinentes a sus funciones y responsabilidades dentro de la organización;
- Cumplan con los términos y condiciones de empleo, que incluye la organización en las políticas de seguridad de la información y los métodos adecuados de trabajo;
- Siguen teniendo las capacidades y cualificaciones apropiadas.

La COAC Chuchuqui cuenta con un REGLAMENTO INTERNO aprobado por consejo administrativo el 09 de noviembre de 2014, al cual deben regirse los funcionarios, y cumplir con todas las disposiciones que en este se encuentran.

4.17.2.2. Concienciación, educación y capacitación en SI.

Control

Todos los empleados de la institución y, en su caso, los contratistas y los usuarios pertinentes, deben recibir una formación adecuada sobre la sensibilización y actualizaciones regulares en las políticas y procedimientos de la organización, que sean relevantes para el desempeño de su función de trabajo.

La sensibilización debe comenzar con un proceso de inducción formal diseñado para introducir las políticas de seguridad de la organización y expectativas antes conceder autorización para acceder a la información o los servicios.

La formación continua debe incluir los requisitos de seguridad, responsabilidades legales y controles de negocio, así como la formación en el uso correcto de las instalaciones de procesamiento de información, por ejemplo, el uso de paquetes de software e información sobre el proceso disciplinario.

4.17.2.3. Proceso Disciplinario.

Control

Debe haber un proceso disciplinario formal para los empleados que han cometido una infracción de seguridad. El proceso disciplinario no debe iniciarse sin comprobación previa de que un fallo de seguridad se ha producido.

El proceso disciplinario formal debe garantizar el tratamiento correcto y justo para los empleados que están sospechosos de haber cometido violaciones de la seguridad. El proceso disciplinario formal debe prever una respuesta que tenga en cuenta factores tales como la naturaleza y nivel de gravedad de la infracción y su impacto en los negocios, si es o no es una primera vez o reincidencia, si el infractor fue o no fue debidamente capacitado, los contratos de negocios y otros factores según se requiera. En casos críticos de mala conducta, el proceso debe permitir la retirada inmediata de sus obligaciones, los derechos de acceso y privilegios, y de ser necesario inmediatamente escoltarlo fuera de la institución.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Seguridad Ligada a los Recursos Humanos.**
	Control:	**4.17.3. Cese o cambio de puesto de trabajo**
	Destinatarios:	Nivel Directivo

OBJETIVO

Proteger los intereses de la organización como parte del proceso de cambiar o terminar el empleo.

DESCRIPCIÓN

Para la salida de un empleado, contratista o tercer usuario, se debe asegurar que todas las responsabilidades han sido culminadas y todo se encuentra en orden en su puesto de trabajo, tener en conocimiento las razones por las cuales sale del cargo, organización nueva a la que se dirige, el retorno de todos los equipos y la eliminación de todos los accesos y verificar que las retribuciones se han completado.

4.17.3.1. Cese o cambio de puesto de trabajo.

Las responsabilidades para llevar a cabo la terminación del empleo o cambio de empleo deben ser claramente definido y asignado.

La comunicación de las responsabilidades de terminación debe incluir los requisitos de seguridad en marcha y responsabilidades legales y, en su caso, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad. Por lo general estos acuerdos deben continuar por un periodo definido después de haber finalizado el empleo.

El jefe encargado de Recursos Humanos es generalmente responsable de la terminación del proceso en general y las obras en caso de proyectos con contratistas, junto con el director de la supervisión de la persona, de la cual se

debe gestionar los aspectos de seguridad mediante procedimientos adecuados.

El proceso de terminación debe ser formalizado para incluir el regreso de todos los programas emitidos con anterioridad, documentos de la empresa, y el/los equipo/s que el empleado ha usado durante su tiempo de trabajo. Otros activos de la organización, tales como los dispositivos informáticos móviles, tarjetas de crédito, tarjetas de acceso, software, manuales, y la información almacenada en medios electrónicos también necesitan ser devueltos.

En los casos en que un empleado, contratista o tercer usuario compra un equipo para sus labores dentro de la organización o utiliza su propio equipo personal, se deben seguir procedimientos que garanticen que toda la información transferida de la institución sea eliminada.

Si un empleado que se marcha, contratista o tercer usuario tiene conocimiento de nombres de usuario y contraseñas que generalmente permanecen activas, éstas deben cambiarse después de la terminación del contrato, acuerdo o cambio de empleo.

4.18. GESTIÓN DE ACTIVOS

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Gestión de Activos**
	Control:	**4.18.1. Responsabilidad Sobre Los Activos**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Identificar los activos de la organización y definir las responsabilidades de protección adecuados.

DESCRIPCIÓN

Todos los activos deben ser contabilizados y tener un propietario nominado o responsable. Los propietarios deben ser identificados para todos los activos y la responsabilidad del mantenimiento adecuado tomando en cuenta los controles de seguridad asignados. La ejecución de labores específicas en los equipos puede ser delegadas por el propietario según el caso, pero el propietario sigue siendo responsable de la protección adecuada de los activos.

4.18.1.1. Inventario de Activos.

Control

Todos los activos deben ser claramente identificados para lo cual se debe elaborar y mantener un inventario de todos los activos importantes.

Una organización debe identificar todos los activos y documentar la importancia de estos activos. El inventario de activos debe incluir toda la información necesaria con el fin de recuperarse en caso de un desastre, incluyendo el tipo de activo, formato, ubicación, información de copia de seguridad, e información de la licencia. Los inventarios no deben duplicar innecesariamente otros inventarios que ya se han realizado anteriormente, pero si deben garantizar que la información se encuentre alineada a los activos actuales.

Es necesario conocer algunos tipos de activos antes de realizar in inventario y poder clasificarlos en grupos que a continuación se describen:

- Activos de Datos o Información: son todos aquellos elementos de hardware y de software de procesamiento, almacenamiento y comunicación, bases de datos, procesos y procedimientos.

- Activos de Software o Aplicaciones: Se conforma de aquellas aplicaciones o programas utilizados por la entidad para gestionar, analizar y transformar los datos, permitiendo la explotación de la información para la explotación de los servicios.

- Activos del tipo Equipos Informáticos: Activos físicos destinados a

soportar directa o indirectamente los servicios que presta la organización, con responsabilidades para el procesamiento de datos, soporte de aplicaciones y almacenamiento de datos.

- Activos del tipo Redes de Comunicación: Bienes físicos relacionados directamente con el transporte de datos entre equipos activos y pasivos de la red.

- Activos del tipo Soportes de Información: Dispositivos físicos que la institución utiliza para almacenar su información de forma permanente o en periodos de tiempo considerables.

- Activos del tipo Equipamiento Auxiliar: Elementos físicos que dan soporte a los sistemas de información, sin estar directamente relacionados con los datos.

4.18.1.2. Uso Aceptable de los Activos.

Control

Se debe identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con el procesamiento de la información.

Todos los empleados, contratistas y terceros usuarios deben seguir las reglas para el uso aceptable de información y los activos asociados a las instalaciones de procesamiento de información, incluyendo:

- Creación de correo electrónico y el uso adecuado dispositivos electrónicos para el acceso a internet;

- Directrices para el uso de los dispositivos móviles, especialmente para el uso fuera de las instalaciones de la institución.

La administración correspondiente debe proporcionar normas o directrices específicas a los empleados, contratistas y terceros usuarios que utilicen o tengan acceso a los activos de la organización y fomentar consciencia de los límites existentes para su uso de la información y los activos dentro de las instalaciones

de la institución asociada con el procesamiento de la información. Ellos deben ser responsables de cualquier uso o tratamiento de los recursos de información, y de cualquier tarea llevada a cabo bajo su responsabilidad.

4.18.1.3. Devolución de Activos.

Toda la información y los activos asociados a las instalaciones de procesamiento de información deben ser de propiedad por una parte designada de la organización.

El propietario de los activos debe ser responsable de:

- Garantizar que la información y los activos asociados a las instalaciones de procesamiento de información son una clasificación adecuada;
- Definir y revisar periódicamente las restricciones de acceso y las clasificaciones, teniendo en tener en cuenta las políticas de control de acceso aplicables.

La propiedad puede ser asignado para:

- Un proceso de negocio;
- Un conjunto definido de actividades;
- Una solicitud; o
- Un conjunto definido de datos.

Las tareas de rutina pueden ser delegadas, por ejemplo, a un compañero de trabajo que necesite realizar actividades continuas en el activo, pero la responsabilidad sigue siendo del propietario.

En los sistemas complejos de información puede ser útil realizar grupos de activos para su designación, que actúan juntos para proporcionar una función particular, como servicios. En este caso, el propietario del servicio es responsable de la entrega del servicio, incluido el funcionamiento de los activos, que se le

proporcionen.

Otra información adicional acerca de la responsabilidad sobre los activos, se encuentra en el Manual de Gestión de Activos Informáticos, Norma Internacional ISO/IEC 27002:2005, aprobada el 23 de Julio del 2016.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Gestión de Activos**
	Control:	**4.18.2. Clasificación de la Información**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

DESCRIPCIÓN

La información debe ser clasificada para indicar la necesidad, prioridades, y grado de protección para la manipulación de la información. La información tiene diversos grados de sensibilidad y criticidad. Algunos artículos pueden requerir un adicional nivel de protección o manejo especial. Un esquema de clasificación de la información se debe utilizar para definir un conjunto adecuado de los niveles de protección y comunicar la necesidad de medidas especiales de manipulación.

4.18.2.1. Directrices de Clasificación

La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la institución.

De acuerdo con alguna política de control debe ser la responsabilidad del

propietario del activo definir la clasificación de un activo, revisar periódicamente, y asegúrese de que se mantiene hasta la fecha y en el nivel adecuado. Se debe considerar que el número de categorías de clasificación y los beneficios que pueden obtenerse de su uso.

Esquemas excesivamente complejos pueden llegar a ser embarazoso y poco rentable para utilizar lo que lo convierte en poco práctico. Se debe tener cuidado al interpretar las etiquetas de clasificación de documentos de otras organizaciones, que pueden tener diferentes definiciones para la mismo información o etiquetas nombras de forma similar.

El nivel de protección se puede evaluar mediante el análisis de la confidencialidad, la integridad y la disponibilidad y cualquier otro requisito para la información que se considere.

La información a menudo deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, ya que el exceso de clasificación puede conducir a la aplicación de controles innecesarios que resulta en un gasto adicional.

Las directrices específicas de la clasificación de la información se encuentran en el Manual de Gestión de Activos Informáticos – Norma ISO/IEC 27002:2005, aprobado el 23 de julio del 2016 en el Acta No 314 R (25).

4.18.2.2. Etiquetado y Manipulado de la Información.

Control

Un conjunto apropiado de procedimientos para el etiquetado de información y manejo debe ser desarrollada e implementado de acuerdo con el esquema de clasificación adoptado por la institución.

Los procedimientos para el etiquetado de la información y los activos de información se necesitan cubrir en forma física y electrónica.

El etiquetado y manejo seguro de la información clasificada es un requisito clave

para el intercambio de información. Etiquetas físicas son una forma común de etiquetado; sin embargo, algunos activos de información, tales como documentos en formato electrónico, no puede ser etiquetado físicamente, por lo cual puede ser necesario utilizar medios electrónicos. Por ejemplo, el etiquetado de un informe de notificación puede aparecer en la pantalla.

Las directrices específicas de la clasificación de la información se encuentran en el Manual de Gestión de Activos Informáticos – Norma ISO/IEC 27002:2005, aprobado el 23 de julio del 2016 en el Acta No 314 R (25).

	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Gestión de Activos**
	Control:	**4.18.3. Manejo de los Soportes de Almacenamiento**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación.

4.18.3.1. Gestión de soportes extraíbles.

Control

Debe haber procedimientos establecidos para la gestión de medios extraíbles.

Las siguientes directrices para la gestión de los medios extraíbles deben ser considerados:

- Si ya no es necesario, los contenidos de los medios de comunicación reutilizable que son retirados de la institución, dicha información debería hacerse irrecuperable;

- Cuando sea necesario y práctico, debe exigirse una autorización para

retirar dispositivos de almacenamiento extraíbles en la institución, para poder llevar un registro de dichas expulsiones con el fin de mantener una pista de auditoría;

- Todos los medios de comunicación extraíble deben ser almacenados en un ambiente seguro, de acuerdo con especificaciones de los fabricantes;
- La información almacenada en los dispositivos extraíbles que tiene que estar disponibles por un tiempo más largo que el promedio de vida del dispositivo (de acuerdo con las especificaciones del fabricante), debe ser también almacenada en otro lugar para evitar pérdida de información debido a la degradación de los mismos;
- Se debe considerar tener un registro de los medios extraíbles para limitar la oportunidad de pérdida los datos;
- Unidades de medios extraíbles sólo debe activarse si hay una razón institucional para hacerlo.

Todos los procedimientos y niveles de autorización deben estar claramente documentados. Los medios extraíbles incluyen cintas, discos, memorias flash, discos duros extraíbles, CD, DVD e impresoras.

4.18.3.2. Eliminación de soportes.

Control

Los medios deben ser desechados cuando ya no sea necesario, utilizando procedimientos de extracción de forma.

Los procedimientos de extracción en forma segura de los soportes deben reducir al mínimo el riesgo que corre la información sensible ante la filtración a personas no autorizadas. Los procedimientos para la extracción segura de los soportes que contengan información sensible debe ser proporcional a dicha sensibilidad de la información. Los siguientes elementos deberían ser considerados:

- Los medios de comunicación que contienen información sensible deben

ser almacenados y extraídos de forma segura y con precaución, para evitar que estos se quemen, dañen, o sus datos sean borrados cuando sean usados para otra aplicación dentro de la institución;

- Los procedimientos deben estar en buenas condiciones, para facilitar la identificación de los elementos que podrían requerir la eliminación segura;
- Puede ser más fácil desmontar o extraer los dispositivos multimedia si estos se encuentran bien organizados, en lugar de intentar separar los elementos sensibles de forma manual;
- Los elementos sensibles deben estar conectados el mayor tiempo posible, según lo permita su tiempo de vida con el fin de mantener una pista de auditoría.

4.19. CONTROL DE ACCESOS.

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Control de Accesos**
	Control:	**4.19.1. Requisitos de Negocio para el control de Accesos**
	Destinatarios:	Nivel Directivo

OBJETIVO

Limitar el acceso a las instalaciones de procesamiento de información y de información.

DESCRIPCIÓN

El acceso a la información, instalaciones de procesamiento de información, y procesos de negocio deben ser controlados sobre la base de los requerimientos del negocio y de seguridad. Se deben tener en cuenta reglas de control de acceso,

políticas de difusión de información y autorización.

4.19.1.1. Política de control de accesos.

Control

Se debe establecer una política de control de acceso, documentarla, y revisarla basado en los negocios y requisitos de seguridad para el acceso.

Deben establecerse de forma clara y concisa, reglas de control de acceso y de derechos para cada usuario o grupo de usuarios en una política de control de acceso. Los controles de acceso son a la vez lógica y física. Los usuarios y los proveedores de servicios deben tener conocimiento claro del negocio, los requisitos y los controles de acceso que deben cumplir.

La política debe tener en cuenta lo siguiente:

- Los requisitos de seguridad de las aplicaciones de negocios individuales;
- La identificación de toda la información relacionada con las aplicaciones de negocio y los riesgos que enfrenta la información;
- Las políticas para la difusión de información y autorización, por ejemplo, la necesidad de conocer los principios institucionales, los niveles de seguridad y clasificación de la información;
- La coherencia entre las políticas de control de acceso y clasificación de la información de diferente sistemas y redes;
- La legislación pertinente y las obligaciones referentes a la protección de acceso a los datos o servicios;
- Perfiles de acceso de usuario estándar para los roles de trabajo comunes en la institución;
- La gestión de los derechos de acceso en un entorno distribuido y en red, la cual tiene conocimiento de todos los tipos de conexiones disponibles;

- Requisitos para la autorización formal de las solicitudes de acceso;
- Los requisitos para la revisión periódica de controles de acceso;
- La eliminación de los derechos de acceso.

4.19.1.2. Control de accesos a redes y servicios asociados.

Control

Los usuarios sólo deben contar con acceso a los servicios que han sido específicamente autorizados usar.

Una política debe formularse en relación con el uso de las redes y servicios de red. Esta política debe cubrir:

- Las redes y los servicios de red que están autorizados a acceder;
- Los procedimientos de autorización para determinar quién se le permite el acceso y a qué redes y servicios;
- Los controles y procedimientos para proteger el acceso a las conexiones de red y de gestión servicios de red;

La política sobre el uso de servicios de red debe ser coherente con la política de control de acceso de las instituciones.

Las conexiones no autorizadas e inseguras a servicios de red pueden afectar a toda la institución. Este control es particularmente importante para las conexiones de red a las aplicaciones de negocios sensibles o críticas o para usuarios en lugares de alto riesgo, áreas públicas o externas.

Otra información adicional, se encuentra en la Política de Control de Acceso a la Red/Información, según norma internacional ISO/IEC27002:2005, aprobada el 25 de junio de 2016.

	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Control de Accesos**
	Control:	**4.19.2. Gestión de Acceso de Usuario**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Garantizar el acceso de usuarios autorizados y para evitar el acceso no autorizado a los sistemas y servicios.

4.19.2.1. Gestión de Acceso de Usuario.

Control

Debe haber un registro de usuarios y el procedimiento de cancelación formal de la autorización de sesión y revocar el acceso a todos los sistemas y servicios de información.

El procedimiento de control de acceso para el registro del usuario y la cancelación del registro debe incluir:

- Utilizar los ID de usuario únicas para que los usuarios puedan estar enlazados y responsabilizados de su comportamiento; el uso de identificadores de grupo sólo se permitirá cuando sean necesarias para razones comerciales u operativas, y deben ser aprobados y documentados;

- Comprobación de que el usuario tiene autorización del propietario de la red para el uso del sistema de información o servicio; aprobación por separado para los derechos de acceso de administración puede también ser apropiado;

- Comprobar que el nivel de acceso concedido es adecuado para el propósito del negocio y es coherente con la política de seguridad de la

institución.

- Exigir a los usuarios a firmar declaraciones que indican que entiendan las condiciones de acceso;
- Garantía de que los proveedores de servicios no ofrecen acceso sino hasta que los procedimientos de autorización han sido terminados;
- El mantenimiento de un registro formal de todas las personas registradas para usar el servicio;
- Eliminar de inmediato o el bloqueo de los derechos de acceso de los usuarios que han cambiado de roles o puestos de trabajo;

Debería considerarse la posibilidad de establecer roles de acceso de usuario basado en los requerimientos del negocio, para disminuir el número de derechos de acceso a los perfiles de usuarios típicos. Si se emplean solicitudes de acceso, es más fácil de gestionar nivel de este tipo de papeles que a nivel de los derechos particulares.

Se debería considerar la posibilidad de incluir cláusulas en los contratos de personal y de servicios, que especifiquen las sanciones si el acceso no autorizado se intenta por parte del personal o agentes de servicio.

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Control de Accesos**
	Control:	**4.19.3. Responsabilidades de Usuario**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Fomentar en los usuarios la responsabilidad de salvaguardar su información de

autenticación.

DESCRIPCIÓN

La cooperación de los usuarios autorizados es esencial para la seguridad efectiva. Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso efectivos, particularmente en relación con el uso de contraseñas y la seguridad del equipo de usuario.

Una política clara de escritorio o pantalla transparente deben ser implementados para reducir el riesgo de acceso no autorizado o daños en los documentos, medios e instalaciones de procesamiento de información.

4.19.3.1. Uso de información confidencial para autenticación.

Control

Los usuarios deben estar obligados a seguir las buenas prácticas de seguridad en la selección y uso de contraseñas.

Todos los usuarios deben ser advertidos de:

- Mantener las contraseñas confidenciales;
- Evitar mantener un registro (por ejemplo, papel, archivo de software o dispositivo de mano) de contraseñas, a menos que esto se pueda almacenar de forma segura y el método de almacenamiento ha sido aprobado;
- Cambiar las contraseñas cada vez que hay alguna indicación de la posible contraseña del sistema o compromiso;
- Seleccionar contraseñas de calidad con suficiente longitud mínima que se encuentran:
    1. Fácil de recordar;
    2. No se basa en ninguna otra cosa que alguien podría adivinar

fácilmente u obtener usando persona información relacionada, por ejemplo, nombres, números de teléfono, y las fechas de nacimiento, etc.;

3. No es vulnerable a ataques de diccionario (es decir, no consistir en palabras incluidas en diccionarios);

4. Libre de caracteres idénticos, totalmente numérica o alfabética de todos los consecutivos.

- Cambiar contraseñas a intervalos regulares o en función del número de accesos (contraseñas para cuentas con privilegios deben cambiarse con más frecuencia que las contraseñas normales), y evitar la reutilización de contraseñas o el ciclismo de edad;
- Cambiar las contraseñas temporales en el primer inicio de sesión;
- No compartir las contraseñas de los usuarios individuales;
- No usar la misma contraseña para fines comerciales y no comerciales.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Control de Accesos**
	Control:	**4.19.4. Control de Acceso a Sistemas y Aplicaciones**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Evitar el acceso no autorizado al sistema y las aplicaciones.

DESCRIPCIÓN

Las instalaciones deben contar con la seguridad necesaria para restringir el

acceso a los sistemas operativos para los usuarios no autorizados. Las instalaciones deben ser capaces de lo siguiente:

- La autenticación de usuarios autorizados, de acuerdo con una política de control de acceso definido;
- El registro de intentos de autenticación del sistema correctos y erróneos;
- Registrar el uso de privilegios especiales del sistema;
- La emisión de alarmas cuando se violan las políticas de seguridad del sistema;
- Proporcionar los medios adecuados para la autenticación;
- En su caso, restringir el tiempo de conexión de los usuarios.

4.19.4.1. Restricción de Acceso a la información.

Control

Todos los usuarios deben tener un identificador único (ID de usuario) exclusivamente para su uso personal, y una adecuada técnica de autenticación debe ser elegida para demostrar la identidad citada de un usuario.

Este control debe aplicarse a todos los tipos de usuarios (incluido el personal de soporte técnico, operadores, los administradores de red, programadores de sistemas y administradores de bases de datos).

ID de usuario se deben utilizar para rastrear las actividades de la persona responsable. Las actividades de los usuarios regulares no deben de realice a partir de las cuentas con privilegios. En circunstancias excepcionales, cuando hay un beneficio claro de negocio, el uso de un ID de usuario puede ser compartido para un grupo de usuarios o para un trabajo específico. La aprobación de la gestión debe ser documentada para tales casos.

Controles adicionales pueden ser necesarios para mantener la rendición de cuentas. En ciertos casos algún ID no necesitan ser rastreado (por ejemplo,

acceso de sólo lectura), o donde existen otros tipos de controles, por ejemplo, donde la fuerte autenticación y verificación de identidad se requiere como los métodos de autenticación alternativa a contraseñas, tales como medios criptográficos, tarjetas inteligentes, tokens o biométricos.

4.19.4.2. Procedimientos seguros de inicio de sesión.

Control

El acceso a los sistemas operativos debe ser controlado por un procedimiento de conexión segura.

El procedimiento para iniciar sesión en un sistema operativo debe estar diseñado para reducir al mínimo la oportunidad para el acceso no autorizado. Por consiguiente, el procedimiento de conexión debe revelar el mínimo la información sobre el sistema, con el fin de evitar proporcionar un usuario no autorizado con cualquier asistencia innecesaria. Un buen procedimiento de conexión debe:

- No mostrar los identificadores de sistema o aplicaciones hasta que el proceso de conexión exitosa ha sido terminado;
- Mostrar un aviso general advirtiendo que el equipo debe ser accesible únicamente para personal autorizado;
- No dar mensajes de ayuda durante el procedimiento de conexión que ayudaría a usuarios no autorizados;
- Validar la información de inicio de sesión una vez realizado todos los datos de entrada. Si una condición de error surge, el sistema no debe indicar que parte de los datos es correcta o incorrecta;
- Limitar el número de intentos de inicio de sesión fallidos permitido, por ejemplo, para tres intentos, y considerar:

    1. El registro de intentos fallidos y exitosos;

2. Forzar un tiempo de retraso antes de autorizar cualquier nuevo intento de entrada en el caso de reincidencia de intentos fallidos bloquear cualquier autorización específica;

3. Desconectar las conexiones de enlace de datos;

4. El envío de un mensaje de alarma a la consola del sistema si el número máximo de intentos de inicio de sesión se alcanza;

5. Establecer el número de reintentos de contraseña en conjunción con la longitud mínima de la contraseña y el valor del sistema a proteger;

- Limitar el tiempo máximo y mínimo permitido para el procedimiento de conexión. Si se excede, el sistema debería terminar la entrada de datos en el sistema;

- Mostrar la siguiente información sobre la finalización de un exitoso inicio de sesión:

1. Fecha y hora de inicio de sesión de éxito anterior;

2. Detalles de cualquier intento de inicio de sesión fallidos desde el último inicio de sesión con éxito;

- No mostrar la contraseña introducida o considere la posibilidad de ocultar los caracteres de la contraseña por símbolos;

- No transmite las contraseñas en texto claro sobre una red.

Si las contraseñas se transmiten en texto claro durante la sesión de conexión a través de una red, pueden ser capturado por una red de programas 'sniffer' en la red.

4.19.4.3. Gestión de contraseñas de usuario.

Control

Los sistemas para la gestión de contraseñas deben ser interactivos y deben garantizar la calidad de las contraseñas.

Un sistema de gestión de contraseñas debe:

- Imponer el uso de identificadores de usuario y contraseñas individuales para mantener la rendición de cuentas;
- Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluyen una confirmación para el procedimiento y así prever los errores de inicio;
- Hacer cumplir una elección de contraseñas de calidad;
- Hacer cumplir los cambios de contraseña;
- Los usuarios de la fuerza para cambiar las contraseñas temporales en la primera conexión a la comunicación;
- Mantener un registro de las contraseñas de los usuarios anteriores y evitar su reutilización;
- No mostrar las contraseñas en la pantalla cuando se introduzcan;
- Almacenar archivos de contraseñas por separado de los datos de sistema de aplicación;
- Almacenar y transmitir las contraseñas en forma protegida (por ejemplo, cifrado o hash).

Otra información adicional, acerca de los procedimientos seguros de inicio de sesión y gestión de contraseñas se encuentra en el documento de POLÍTICAS/PROCEDIMIENTOS DE ACCESO A LOS SISTEMAS DE INFORMACIÓN, MÓDULO: ASIGNACIÓN DE CLAVES Y ROLES, aprobado

el 23 de abril del 2016 en el Acta No 308 R (23).

4.20. CIFRADO

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Cifrado**
	Control:	**4.20.1. Controles Criptográficos**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

DESCRIPCIÓN

Una política debe desarrollarse sobre el uso de controles criptográficos. La gestión de claves debe apoyar el uso de técnicas criptográficas.

4.20.1.1. Política de uso de gestión de claves.

Control

Se debe desarrollar una política sobre el uso de controles criptográficos para la protección de la información e implementarla.

En el desarrollo de una política de cifrado se debe considerar lo siguiente:

a) El enfoque de gestión hacia el uso de controles criptográficos para todos quienes conforman la institución, incluyendo los principios generales en las que la información de negocios debe ser protegida;

b) Evaluación de riesgos identificando el nivel requerido de protección teniendo en cuenta el tipo, la fuerza, y la calidad del algoritmo de cifrado

requerido;

c) El uso de cifrado para la protección de la información sensible que puede ser transportada por medios extraíbles, dispositivos o a través de líneas de comunicación;

d) El enfoque de la gestión de claves debe incluir métodos para hacer frente a la protección de claves criptográficas y la recuperación de la información codificada en el caso de pérdida;

e) Normas que deben adoptarse para la aplicación efectiva en toda la organización (Cuál es la solución que se utiliza para los procesos de negocio);

El impacto controles criptográficos se pueden usar para lograr diferentes objetivos de seguridad, por ejemplo:

a) La confidencialidad: mediante el cifrado de la información para proteger la información sensible o crítica, ya sea almacenada o transmitida;

b) La integridad / autenticidad: el uso de firmas digitales o códigos de autenticación de mensajes para proteger la autenticidad y la integridad de la información sensible o crítica almacenada o transmitida;

c) No repudio: el uso de técnicas criptográficas para obtener pruebas de la ocurrencia o no ocurrencia de un evento o acción.

4.21. SEGURIDAD FÍSICA Y AMBIENTAL.

	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Seguridad Física y Ambiental**
	Control:	**4.21.1. Áreas Seguras**
	Destinatarios:	Todos los funcionarios de la institución.

OBJETIVO

Restringir el acceso físico no autorizado para evitar daños y la interferencia en las oficinas y con la información de la institución.

DESCRIPCIÓN

Las instalaciones de procesamiento de información críticas o sensibles deben ser alojadas en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad adecuadas y controles de ingreso. Estos deberían ser físicamente protegidos del acceso, daños, y la interferencia. La protección proporcionada debe ser proporcional a los riesgos identificados.

4.21.1.1. Perímetro de seguridad física.

Control

Perímetros de seguridad (barreras, tales como paredes, puertas de entrada controladas con tarjetas o mostradores de recepción tripulados) se debe utilizar para proteger áreas que contienen las instalaciones de procesamiento de información.

Las siguientes pautas deben ser consideradas y aplicadas en los perímetros de seguridad física:

- Perímetros de seguridad deben estar claramente definidos, y la ubicación y la fuerza de cada uno de los perímetros debe depender de los requisitos de seguridad de los activos dentro del perímetro y los resultados de una

evaluación de riesgos;

- Perímetros de un edificio o sitio que contengan instalaciones de procesamiento de la información deben ser físicamente herméticas (es decir, no debe haber espacios en el perímetro o áreas en las que un robo podría fácilmente ocurrir); las paredes externas del sitio debe ser de construcción sólida y todos puertas exteriores deben estar adecuadamente protegidos contra el acceso no autorizado con el control mecanismos, por ejemplo, alarmas, cerraduras, biométricos, etc; puertas y ventanas deben estar cerradas cuando se desatienda la protección.

- Debe existir una zona de recepción tripulada u otros medios para controlar el acceso físico a las oficinas de la institución; el acceso a los sitios y zonas públicas debe limitarse sólo para el personal autorizado;

- Las barreras físicas deben, en su caso, ser construidos para evitar el acceso físico no autorizado y la contaminación del medio ambiente;

- Debe instalarse adecuadamente sistemas de detección de intrusos o normas internacionales y regularmente probados para cubrir todas las puertas exteriores y ventanas accesibles; las zonas no ocupadas estar monitoreadas en todo momento;

- Las áreas de procesamiento de información deben estar gestionados y físicamente aislados de terceros usuarios.

4.21.1.2. Controles físicos de entrada.

Control

Las áreas seguras deberían estar protegidos por controles de entrada adecuados para garantizar que sólo al personal autorizado se les permite el acceso.

Las siguientes pautas deben ser consideradas:

- La fecha y hora de entrada y salida de los visitantes deben registrarse, y todos los visitantes deben ser supervisados a menos que su acceso ha sido

previamente aprobado; y que sólo se debe conceder el acceso con fines específicos, autorizados y deben ser emitidos los requisitos de seguridad de la zona con instrucciones sobre los procedimientos de emergencia.

- El acceso a zonas en las que la información sensible es procesada o almacenada debe ser controlado y restringido a las personas no autorizadas; se debe utilizar para autorizar y validar todos los accesos, controles de autenticación, por ejemplo, tarjeta de control de acceso, para de esta forma mantener segura una pista de auditoría de todos los accesos;

- Todos los empleados, contratistas, terceros usuarios y todos los visitantes deben estar obligados a llevar alguna forma de identificación visible y se debe notificar inmediatamente al personal de seguridad si algún visitante no lleve identificador visible;

- El personal de servicio de apoyo a terceros debe tener acceso restringido a áreas seguras o instalaciones de procesamiento de información sensible y únicamente puede tener acceso cuando sea requerido y ese acceso debe ser autorizado y controlado;

- Los derechos de acceso a zonas seguras deben revisarse y actualizarse periódicamente, y ser revocados cuando sea necesario.

4.21.1.3. Seguridad de oficinas, despachos y recursos.

Control

La seguridad física de oficinas, salas e instalaciones deben ser diseñadas y aplicadas.

Las siguientes pautas deben ser considerados para asegurar oficinas, salas e instalaciones:

- Deben tenerse en cuenta los reglamentos y las normas de salud y seguridad pertinentes;

- Las principales instalaciones deberían estar situadas para evitar el acceso

por parte del público;

- En su caso, los edificios deben ser discretos y dar una indicación mínima de su propósito, sin signos obvios, fuera o dentro del edificio que puedan indicar la presencia de actividades de procesamiento de la información;

- Los planos y los directorios telefónicos internos que identifican la ubicación de la información sensible instalaciones de procesamiento no deben ser fácilmente accesibles por el público.

4.21.1.4. Protección contra amenazas externas y ambientales.

Control

La protección física contra los daños causados por incendios, inundaciones, terremotos, explosiones, disturbios civiles, y otros tipos de catástrofes naturales o de origen humano deben ser diseñados y aplicados.

Se debe considerar como amenaza de seguridad a cualquier infraestructura vecina presentada, por ejemplo, un incendio en un edificio vecino, filtraciones de agua desde el techo o en el suelo debajo del nivel del suelo o una explosión en la calle.

Las siguientes pautas deben ser consideradas para evitar daños por incendio, inundación, terremoto, explosión, disturbios civiles, y otros tipos de catástrofes naturales o de origen humano:

- Materiales peligrosos o inflamables deben almacenarse a una distancia considerable de un área segura. Suministros a granel, tales como papelería no deben ser almacenados en un lugar que contienen los sistemas de datos;

- El equipo de reserva y medios de respaldo deberían estar situadas a una distancia preventiva para evitar daños de un desastre que afecte el sitio principal;

- El equipo contra incendios adecuado debe ser proporcionado y

adecuadamente colocado.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Seguridad Física y Ambiental**
	Control:	**4.21.2. Seguridad de los Equipos.**
	Destinatarios:	Departamento de Tecnología

OBJETIVO

Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las actividades de la institución.

DESCRIPCIÓN

El equipo debe ser protegido de las amenazas físicas y ambientales. La protección de los equipos es necesaria para reducir el riesgo de acceso no autorizado a la información y para proteger contra la pérdida o daño. También se debe tener en cuenta la ubicación y la posibilidad de eliminación del equipo. Controles especiales pueden ser necesarios para proteger contra las amenazas físicas, y para salvaguardar las instalaciones de apoyo, tales como el suministro eléctrico e infraestructura de cableado.

4.21.2.1. Emplazamiento y protección de equipos.

Control

El equipo debe estar situado o protegido para reducir los riesgos de las amenazas y los riesgos ambientales, y las oportunidades de acceso no autorizado.

Las siguientes pautas deben ser consideradas para proteger el equipo:

- El equipo estará situado de manera que minimice el acceso a las zonas de trabajo innecesarias;

- Las instalaciones de procesamiento de información de gestión de datos sensibles deben ser colocados en ángulo que pueda restringir la visualización, para reducir el riesgo de la información que se está viendo por personas no autorizadas durante su uso y permanencia de las instalaciones;

- Los dispositivos o equipos que requieren una protección especial deben ser aislados para reducir el nivel general de la protección necesaria;

- Los controles deben ser adoptadas para minimizar el riesgo de posibles amenazas físicas, por ejemplo, el robo, fuego, explosivos, humo, agua (o la falta de suministro de agua), los efectos del polvo, vibraciones, químicos, la interferencia por la alimentación eléctrica, interferencia de comunicaciones, la radiación electromagnética, y el vandalismo;

- Se deben establecer dentro de las instalaciones directrices para comer, beber y fumar en la proximidad de procesamiento de la información;

- Las condiciones ambientales, como la temperatura y la humedad, deben ser monitorizados para detectar eventualidades que podrían afectar negativamente al funcionamiento de las instalaciones del procesamiento de la información;

- Protección pararrayos se debe aplicar a todos los edificios y filtros de protección contra rayos debe ser instalado en todas las líneas eléctricas y de comunicaciones entrantes;

- Los equipos de procesamiento de información sensibles deben ser protegidos para minimizar el riesgo de fuga de información por irradiación.

4.21.2.2. Instalaciones de suministro.

Control

El equipo debe estar protegido contra fallos de alimentación y otras

perturbaciones causadas por fallos en el apoyo de los servicios públicos.

Todos los servicios de apoyo, tales como la electricidad, el suministro de agua, alcantarillado, calefacción / ventilación y aire acondicionado deben ser adecuados para los sistemas que están sustentando. La ventaja de que los suministros se encuentren regularmente inspeccionados y comprobados, es que garantiza su correcto funcionamiento y reduce cualquier riesgo de mal desempeño o fallo. Debe establecerse un suministro eléctrico adecuado que se ajuste a las especificaciones del fabricante del equipo.

Es recomendable contar con un sistema de alimentación ininterrumpida (UPS) para apoyar el funcionamiento continuo de los equipos de soporte en operaciones críticas de negocio. El plan de contingencia debería poder cubrir la acción a tomar en caso de fallo de la UPS. Se debe considerar un generador de respaldo si se requiere procesamiento para continuar en caso de un corte de corriente prolongado. Un suministro adecuado de combustible debe estar disponible para asegurar que el generador puede estar en acción durante un periodo prolongado. Los equipos UPS y generadores deben ser revisados regularmente para asegurarse de que tiene la capacidad adecuada y probados de conformidad con las recomendaciones del fabricante. Además, se podría considerar la posibilidad de utilizar múltiples fuentes de energía o, si el sitio es grande una subestación de alimentación independiente.

Los interruptores de desconexión de emergencia deben estar ubicados cerca de las salidas de emergencia y en las salas de equipos, para facilitar el suministro de energía rápida en caso de una emergencia. El alumbrado de emergencia debe proporcionarse en caso falla la energía principal.

El suministro de agua debe ser estable y adecuado para suministrar aire acondicionado, equipo de humidificación y sistemas de detección y extinción de incendios. Los fallos del sistema de suministro de agua pueden dañar al equipo o puede evitar que la extinción de incendios se realice con eficacia. Los sistemas de alarma para detectar fallos de funcionamiento en los servicios públicos de apoyo deben ser evaluados y se implementan si es necesario.

Los equipos de telecomunicaciones deben estar conectados al proveedor de servicios públicos por al menos dos distintas vías, para prevenir una falla en una ruta de conexión y la eliminación de los servicios de voz. Los servicios de voz deben estar adecuados para cumplir con los requisitos legales, locales y para las comunicaciones de emergencia.

4.21.2.3. Seguridad del cableado.

Control

Energía y telecomunicaciones de cableado que transporta datos o el apoyo a los servicios de información deben estar protegidos de la interceptación o daños.

Las siguientes pautas de seguridad para el cableado deben ser considerados:

- Energía y telecomunicaciones líneas en las instalaciones de procesamiento de información deben estar subterránea, siempre que sea posible, o sujetas a protección alternativo adecuado;
- Cableado de la red debe protegerse de la intercepción no autorizada o daño, por ejemplo, mediante el uso de un conducto o evitando rutas a través de las zonas comunes;
- Los cables de alimentación deben estar separados de los cables de comunicaciones para evitar la interferencia;
- Se debe utilizar marcas identificadoras o etiquetados muy claros en los cables y equipos para minimizar los errores de manipulación, tales como emendaciones accidentales en cables de red equivocados;
- Debe utilizarse una documentación de la lista de etiquetado para reducir la posibilidad de errores;
- Para los sistemas sensibles o críticas se debe considerar más controles que incluyen:

    1. La instalación de conductos blindados y bloqueadas las

habitaciones o en las cajas de inspección y puntos de terminación;

2. El encaminamiento alternativo y / o medios de transmisión que proporcionan la seguridad adecuada;
3. El uso de cableado de fibra óptica;
4. El uso de blindaje electromagnético para proteger los cables;
5. La iniciación de barridos técnicos e inspecciones físicas por ser dispositivos no autorizados unido a los cables;
6. El acceso controlado a los paneles de conexión y salas de cable;

4.21.2.4. Mantenimiento de los equipos.

Control

El equipo debe mantenerse correctamente para asegurar su continua disponibilidad e integridad.

Las siguientes directrices para el mantenimiento del equipo deben ser considerados:

- El equipo deberá mantenerse de acuerdo con el servicio recomendado y especificaciones del proveedor;
- Sólo las personas autorizadas para realizar mantenimiento, deben llevar a cabo las reparaciones y verificaciones del servicio del equipo;
- Se deben mantener registros de todos los fallos sospechosos o reales, y todos los mantenimientos preventivos y correctivos;
- Deben aplicarse controles adecuados cuando el equipo está previsto para mantenimiento, teniendo en cuenta si este mantenimiento es realizado por personal de sitio o externo a la organización; en su caso, la información sensible debe ser borrada del equipo o el personal de mantenimiento deben proteger la información adecuadamente;

- Todos los requisitos impuestos por las pólizas de seguro deben ser respetadas.

4.21.2.5. Reutilización o retirada segura de dispositivos de almacenamiento.

Control

Todos los elementos del equipo que contienen medios de almacenamiento deben ser evaluados para verificar que los datos sensibles y software licenciado sean desmontados o sobrescrito de forma segura antes de su extracción.

Los dispositivos que contengan información sensible deben ser destruidos físicamente o la información debe estar eliminada, borrados o sobrescritos utilizando técnicas para hacer que la información original no se recuperable, en lugar de utilizar el formato estándar de eliminación.

Los dispositivos dañados que contienen datos sensibles pueden requerir una evaluación de riesgos para determinar si el artículo debe ser destruido físicamente en lugar de enviar al servicio técnico o desecharlo.

La información puede ser comprometida por descuido en la eliminación o reutilización de los equipos.

4.21.2.6. Equipo informático de uso desatendido.

Control

Los usuarios deben asegurarse de que el equipo desatendido tiene la protección adecuada.

Todos los usuarios deben ser conscientes de los requisitos y procedimientos de seguridad para la protección desatendida equipos, así como sus responsabilidades para la aplicación de dicha protección. Se debe advertir a los usuarios para:

- Terminar las sesiones activas cuando haya terminado, a menos que puedan ser asegurados por un adecuado mecanismo de bloqueo, por

ejemplo, una salvapantalla protegida por contraseña;

- Cerrar sesión (log-off) en ordenadores centrales, servidores y PC de la oficina cuando la sesión ha terminado (es decir, no sólo apagar la pantalla del PC o terminal);

- Los equipos de seguridad o terminales de uso no autorizado deben contar una cerradura con llave o un control equivalente, por ejemplo, la contraseña de acceso, cuando no está en uso.

4.21.2.7. Política de puesto de trabajo despejado y bloqueo de pantalla.

Control

Deben adoptarse una política de escritorio despejado para los documentos y medios de almacenamiento extraíbles y una política de bloqueo de pantalla dentro de las instalaciones de procesamiento de información.

El escritorio despejado y la política de bloqueo de pantalla deben tener en cuenta las clasificaciones de la información, los requisitos legales y los riesgos correspondientes. Las siguientes pautas deben ser consideradas:

- La información comercial sensible o crítica, por ejemplo, en papel o en soporte electrónico, debe ser asegurada (a ser posible en formas de seguros de muebles u otros tipos de seguridad para los muebles o escritorios), aunque se piense que no sea necesario y sobre todo cuando se desocupe la oficina;

- Ordenadores y terminales se deben dejar cerrando sesión o protegidos con bloqueo de pantalla y un mecanismo de teclado controlado por una contraseña de bloqueo;

- Los puntos de correo entrante y saliente y de fax desatendidos deben ser protegidos;

- Debe prevenirse el uso no autorizado de las fotocopiadoras y otras

tecnologías de reproducción (por ejemplo, escáneres, cámaras digitales);

- Los documentos que contengan información sensible o clasificada deben ser retirados de las impresoras inmediatamente.

4.22. SEGURIDAD EN LA OPERATIVA.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Seguridad en la Operativa**
	Control:	**4.22.1. Responsabilidades y procedimientos de operación.**
	Destinatarios:	Departamento de tecnología

OBJETIVO

Garantizar la seguridad y correcto manejo de la disponibilidad de los registros de información de log en los procedimientos de operación.

4.22.1.1. Documentación de procedimientos de operación.

Control.

Los procedimientos de operación deben estar documentados y ponerse a disposición de todos los usuarios que lo necesiten.

Los procedimientos documentados deben estar preparados para las actividades operacionales asociadas a los sitios de la institución donde se realiza el procesamiento de información y comunicaciones, tales como el inicio o arranque y terminación de procesos de equipo, mantenimiento de los equipos de respaldo, manejo de medios, cuarto de informática y gestión de seguridad en la entrega de correos electrónicos.

Los procedimientos de operación deben especificar las instrucciones de uso, incluyendo:

- Instalación y configuración de sistemas;
- Proceso y forma de manipulación de la información tanto automática como manual;
- Copias de seguridad;
- Instrucciones para el manejo de errores y otras condiciones excepcionales que pudieran surgir durante la ejecución del trabajo, incluidas las restricciones en el uso de los recursos del sistema;
- Contactos de soporte y soluciones tecnológicas incluyendo contactos de soportes externos;
- Contactos de interés especial en caso de operaciones inesperadas o dificultades técnicas;
- Instrucciones para la manipulación de información confidencial en documentos físicos y de ser necesario, incluir los procedimientos de eliminación segura para dicha documentación;
- Procedimientos de reinicio y recuperación del sistema para su uso en caso de fallo del sistema;
- Gestión de una pista de auditoria y registro de log de sistemas de información;
- Procedimientos de monitoreo.

Los procedimientos de operación y la documentación de los procedimientos para las actividades de los sistemas deben ser tratados como documentos formales y sus cambios deben ser autorizados por la administración. De ser posible los sistemas de información deben ser monitoreados constantemente, utilizando los mismos procedimientos, herramientas y pautas.

4.22.1.2. Gestión de cambios.

Control

Deben ser controlados todos los cambios de la organización que posiblemente afecte a la seguridad de la información como procesos de negocio, procesos de información y sistemas.

Se debe considerar lo siguiente:

- Identificación y registro de los cambios significativos;
- Planificación y pruebas de cambios;
- Evaluación de los impactos potenciales, incluyendo los impactos a la seguridad de la información de tales cambios;
- Aprobación formal para la ejecución de cambios tomando en cuenta el propósito de los cambios;
- Verificar que los requerimientos para la seguridad de la información se cumplan;
- Comunicación de los detalles de los cambios a todas las personas relevantes;
- Provisión de un proceso de cambio rápido de emergencia controlando la implementación de los cambios necesarios para resolver un incidente.

Para este proceso de gestión de cambios debe existir una CMDB (Change Management Data Base, Base de Datos de Gestión de Cambios), donde se deben almacenar todos los cambios que se han realizado, especificando todos los elementos que formaron parte del procedimiento, su configuración y de ser necesario detallar alguna observación. (Ríos, 2014)

Para la formalización de la gestión de cambios se debe basar en el formato establecido en el ANEXO H

4.22.1.3. Gestión de capacidades.

Control

El uso de los recursos debe ser monitoreado, adecuado y proyectado al futuro sobre la capacidad de los requerimientos para asegurar el performance requerido por los sistemas.

La capacidad de los requerimientos debe ser identificada, teniendo en cuenta la criticidad del negocio de los sistemas en cuestión. El monitoreo de los sistemas debe aplicarse para garantizar, y de ser necesario, mejorar el rendimiento y capacidad de los sistemas. Controles de detección se deben poner en marcha para indicar problemas en su debido tiempo. Se deben tomar en cuenta las proyecciones de necesidades futuras de capacidad considerando nuevos requerimientos del negocio y del sistema, y tendencias actuales para el procesamiento de información.

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Seguridad en la Operativa.**
	Control:	**4.22.2. Protección Contra Código Malicioso**
	Destinatarios:	Departamento de tecnología.

OBJETIVO

Para proteger la integridad d**el software y de la información, s**e deben tomar precauciones para prevenir y detectar la introducción de **código malicioso.**

DESCRIPCIÓN

Las instalaciones de software y procesamiento de la información son vulnerables a la introducción de código malicioso, tales como virus informáticos, gusanos de red, caballos de Troya y bombas lógicas. Los usuarios deben ser conscientes de los peligros de código malicioso. Los gerentes deben, en su caso, introducir

controles de prevenir, detectar y eliminar el código malicioso.

4.22.2.1. Controles contra el código malicioso.

Control

Se debe implementar de sensibilización en usuarios sobre procedimientos adecuados de detección, prevención y recuperación de los controles de protección contra código malicioso.

La protección contra código malicioso debe basarse en la detección y reparación de software, conciencia de seguridad y controles de acceso y sistema de gestión de cambios apropiados. Se debe considerar:

- Establecer una política formal que prohíbe el uso de software no autorizado;
- Establecer una política formal para proteger el software contra los riesgos asociados a la obtención de archivos ya sea desde o a través de redes externas, indicando que medidas de protección deben ser tomadas;
- Implementar controles que previenen o detectan el uso de conocidas o sospechosas páginas web que contienen código malicioso;
- Implementar controles que previenen o detectan el uso no autorizado de los sistemas;
- Reducir las vulnerabilidades que pueden ser explotadas por el malware;
- Realización de exámenes periódicos de todo el contenido del software y los datos de los sistemas de apoyo en el proceso crítico de negocio; la presencia de los archivos no autorizados o modificaciones no autorizadas deben ser investigados formalmente;
- La instalación y la actualización periódica de detección de código malicioso y reparación de software para escanear equipos y medios de comunicación como un control preventivo, o de forma rutinaria; los

controles realizados a cabo deberían incluir:

1) El control de los archivos en medios electrónicos u ópticos y archivos recibidos a través de redes;

2) El control de los archivos adjuntos de correo electrónico y descargas antes de su uso;

3) El control de páginas web de código malicioso;

- Definición de procedimientos y responsabilidades de gestión para hacer frente a código malicioso, protección de los sistemas, capacitación, presentación de informes ante un código malicioso;

- La preparación de planes de continuidad de negocio adecuadas para recuperarse de ataques de código malicioso, incluyendo todos los datos necesarios y el software de copia de seguridad y recuperación de éstos;

- La aplicación de procedimientos para verificar la información relativa al código malicioso, y asegúrese de que los boletines de alerta son precisos e informativos; los gerentes deben asegurar que se usan fuentes calificadas, por ejemplo, revistas de renombre, sitios de Internet confiables o proveedores que producen software de protección contra código malicioso; todos los usuarios deben ser conscientes de las vulnerabilidades que se pueden presentar.

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Seguridad en la Operativa**
	Control:	**4.22.3. Copias de Seguridad**
	Destinatarios:	Departamento de Tecnología.

OBJETIVO

Proteger la información, mantener la integridad y la disponibilidad de

información para evitar la pérdida datos.

DESCRIPCIÓN

Los procedimientos de rutina deben ser establecidos para aplicar la política y la estrategia acordada para la copia de seguridad, para tener un respaldo de la información que puede ser restaurada en el momento oportuno.

4.22.3.1. Copias de seguridad de la información.

Control

Las copias de seguridad de la información y software deben ser tomadas y analizadas periódicamente de acuerdo con la política de copia de seguridad.

Una política de copia de seguridad debe ser implementada dependiendo de los requerimientos de la institución para asegurar que toda la información esencial, software y sistemas pueden ser recuperados después de un desastre o fallo.

Cuando se designa un plan de backup, se debe tomar en cuenta:

- Registros precisos y completos de las copias de seguridad y se debe elaborar una documentación de los procedimientos de restauración.
- El alcance y la frecuencia de backups debe reflejar los requisitos de negocio de la institución, los requisitos de seguridad de la información involucrados y la criticidad de la información para la continuidad de las operaciones de la cooperativa.
- La información de las copias de seguridad se debe mantener con un nivel apropiado de seguridad física y medioambiental conforme a las normas aplicadas en el lugar principal de procesamiento de la información.
- Los medios de backup deben ser regularmente testeados para asegurar que estos pueden ser instaurados en caso de una emergencia en los que sean necesarios; este test puede ser combinado con un test de procedimiento de recuperación y chequeo del tiempo requerido para la

restauración. Para probar la capacidad de restauración de los datos de la copia de seguridad, se debe realizar en medios dedicados para prueba, para no sobrescribir el medio original en caso de que el proceso de copia de seguridad o restauración falle y provoque que los datos sean irrecuperables.

- En casos donde la confidencialidad es de suma importancia, los backups deben ser protegidos mediante encriptación de datos.

Los procesos de ejecución de copias de seguridad deben ser supervisados y direccionar adecuadamente en caso de fracasos, para garantizar que las copias de seguridad siguen manteniendo su integridad de acuerdo a la política de copias de seguridad (POLÍTICAS DE COPIAS DE SEGURIDAD - NORMA INTERNACIONAL ISO/IEC 27002:2005) aprobada el 25 de junio del 2016 según consta en el Acta No. 312 R (25).

Los medios auxiliares de backups para los sistemas y servicios individuales se comprobarán periódicamente para garantizar que se cumplen los requisitos de los planes de continuidad de negocio. En el caso de sistemas y servicios críticos, los medios auxiliares deben cubrir toda la información de los sistemas, aplicaciones y datos necesarios para recuperar el sistema completo en un evento o desastre.

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Seguridad en la Operativa**
	Control:	**4.22.4. Registro de Actividad y Supervisión**
	Destinatarios:	Departamento de tecnología.

OBJETIVO

Registrar acontecimientos y generar evidencia.

4.22.4.1. Registro y gestión de eventos de actividad.

Control

Registrar los eventos de las actividades de los usuarios, errores y eventos de seguridad de la información, que se deben producir, mantener y revisar con regularidad.

Los registros de eventos deben incluir, cuando sea pertinente:

- ID de usuario;
- Actividad en el sistema;
- Fecha, hora y detalles de los eventos importantes, por ejemplo, inicio de sesión y finalización de sesión;
- Identificador de dispositivo o localización si es posible y el identificador del sistema;
- Registro de los intentos satisfactorios y erróneos en la autenticación para el acceso al sistema;
- Cambios en la configuración del sistema;
- Uso de privilegios;
- Uso de recursos y aplicaciones del sistema;
- Archivos de acceso y tipo de acceso;
- Dirección de red y protocolos;
- Alarmas levantadas por el control de acceso del sistema;
- Activación y desactivación de la protección de los sistemas tal como los sistemas anti virus y sistema de detección de intrusos.
- Registro de las transacciones ejecutadas por el usuario en las aplicaciones.

4.22.4.2. Protección de los registros de información.

Control

La disponibilidad de los de registros de log y la información de registro deben ser protegidos contra la manipulación y acceso no autorizado.

Los controles deberían tratar de proteger la información de registros y operaciones, contra problemas de cambios no autorizados, la disposición de los registros debe contemplar:

- Registros de los cambios en los tipos de mensajes;
- Registros de los archivos que han sido modificados o borrados;
- Monitoreo de la capacidad de almacenamiento de los medios de comunicación que contienen los archivos de registro, para evitar que estos superen la capacidad permitido, lo que resulta tanto en la falta de registro de eventos o sobre-escritura de los eventos pasados registrados.

Algunos registros pueden ser necesarios para el desarrollo de auditorías por lo que estos archivos se deben conservar como parte de evidencias o pruebas.

4.22.4.3. Sincronización de relojes.

Los relojes de todos los sistemas de procesamiento de información o de seguridad que tienen más relevancia para la institución, deben estar sincronizados a una única fuente de tiempo de referencia.

Los requerimientos de la institución con respecto a los tiempos que se manejen en ella, deben estar documentados y estos deben ser exigencias legales y reglamentarias para el control interno. Se debe definir un tiempo de referencia estándar para el uso dentro de la institución.

La referencia del tiempo de la institución también debe contar con una referencia externa y estas deben estar en la documentación reglamentaria.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Seguridad en la Operativa**
	Control:	**4.22.5. Gestión de la vulnerabilidad técnica**
	Destinatarios:	Departamento de tecnología.

OBJETIVO

Prevenir la explotación de las vulnerabilidades técnicas que pueden presentar los sistemas de proceso y almacenamiento de información.

DESCRIPCIÓN

La gestión de vulnerabilidades técnicas deberá aplicarse de manera efectiva, sistemática, y manera constante, con las mediciones realizadas para confirmar su eficacia. Estas consideraciones deben incluir sistemas operativos, y cualquier otra aplicación en uso.

4.22.5.1. Gestión de las vulnerabilidades técnicas.

Control

La información sobre las vulnerabilidades técnicas de los sistemas de información debe ser utilizada de manera prudente, la institución debe hacer una evaluación de los riesgos que a los que se expone la cooperativa y debe asociar cada vulnerabilidad a una medida de prevención.

Un inventario de activos competo es un prerrequisito para la adecuada implementación de la gestión de las vulnerabilidades. La información específica de los equipos que brindan los proveedores como el número serie, versión, software instalado, y otras características técnicas en las que los equipos funcionan adecuadamente, es necesaria tomarla en cuenta al momento de tomar medidas correctivas la prevención de falencias en el rendimiento de los equipos.

Las siguientes recomendaciones deben ser implementadas para la adecuada

gestión del proceso para las vulnerabilidades técnicas:

- La organización debe establecer roles y responsabilidades asociadas a la gestión de las vulnerabilidades técnicas, incluyendo el monitoreo de las vulnerabilidades, evaluación de riesgos, toma de medidas, seguimiento de activos y cualquier coordinación de responsabilidades requerida.

- Los recursos de información que sean empleados para la identificación de las vulnerabilidades técnicas deben ser respaldados por técnicas de software o alguna tecnología en específico.

- Un tiempo de reacción debe ser definido para tomar medidas correctivas ante las notificaciones de vulnerabilidades técnicas.

- Una vez identificada una vulnerabilidad técnica que pueda ser crítica, la organización debería identificar los riesgos asociados y las acciones a realizar de forma inmediata.

- Las medidas que se vayan adoptar, deben ser probadas y evaluadas antes de ser instauradas para asegurar que sean efectivas y no dan lugar a efectos secundarios que no pueden ser tolerados;

- un registro de auditoría debe mantenerse para todos los procedimientos realizados;

- El proceso de gestión de vulnerabilidades técnica debe controlarse y evaluarse regularmente con el fin de asegurar su eficacia y eficiencia;

- Los controles de los sistemas con alto riesgo deben dirigirse en primer lugar.

4.22.5.2. Restricciones de la instalación de software.

Control

La cooperativa debe cumplir con el principio de privilegio mínimo, si se concede ciertos privilegios, los usuarios pueden tener hábito de instalar software. La

institución debe identificar qué tipos de software son permitidos instalar y cuáles son prohibidos, por recomendación el software permitido debe ser licenciado para garantizar que no se instale software malicioso. Los privilegios deben estar acorde a los roles de los funcionarios.

Otra información sobre la restricción de la instalación de software, se puede consultar en el MANUAL OPERATIVO DE TECNOLOGÍAS - Políticas y procedimientos del área de Tecnología de Información aprobado el 22 de noviembre del 2014 en el Acta No 286 R (14).

4.23. SEGURIDAD EN LAS TELECOMUNICACIONES.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Seguridad en las Telecomunicaciones**
	Control:	**4.23.1. Gestión de la Seguridad en las redes.**
	Destinatarios:	Departamento de tecnología.

OBJETIVO

Garantizar la seguridad de la información en la red y la disponibilidad de la información de apoyo.

4.23.1.1. Controles de red.

Control

La red debe ser gestionada y controlada para proteger la información de los sistemas y aplicaciones que se desenvuelven en la institución.

Los controles deben ser implementados para garantizar la seguridad de la información en la red y la protección de servicios a los se encuentra conectada, ante posibles accesos no autorizados. Se debe considerar los siguientes ítems:

- Se debe establecer responsabilidades y procedimientos para la gestión de

los equipos de red.

- Se debe establecer controles especiales para garantizar la confiabilidad e integridad de los datos que pasan por la red cableada o redes inalámbricas y para proteger la conexión de sistemas y aplicaciones.

- Implementar mecanismos adecuados para el monitoreo de autenticación para garantizar que existan registros y detección de acciones que pueden afectar o ser relevantes para la seguridad de la información.

- Toda actividad de gestión debe estar coordinada para garantizar el servicio óptimo de la institución y que los controles sean aplicados adecuadamente en todo el procesamiento de la información a través de infraestructura de red.

- Todo sistema en la red de la institución debe contar con el proceso de autenticación.

- La conexión de equipos a la red, debe estar restringida.

4.23.1.2. Mecanismos de seguridad asociados a servicios en red.

Control

Los mecanismos de seguridad, niveles de servicio y la gestión de los requisitos de todos los servicios de red deben ser identificados e incluidos en los acuerdos de servicios (SLA), independientemente de si estos servicios se generan de forma interna o si son externos como los servicios prestados por el Banco Central del Ecuador.

Debe determinarse y controlarse regularmente, la capacidad del proveedor de servicios de red para la administración de servicios acordados de manera segura, y el derecho a la auditoría debe ser acordado.

Se debe identificar las medidas de seguridad necesarias para determinados servicios, tales como características de seguridad, niveles de servicio y los requisitos de supervisión. La institución debe asegurarse de que el proveedor de

servicios, implementa estas medidas.

Los servicios de red deben incluir la provisión de conexiones, servicios de redes privadas y soluciones de seguridad de gestión de red, tales como sistemas de detección de intrusiones y firewall.

4.24. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

Impulsamos su desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.**
	Control:	**4.24.1. Requisitos de Seguridad de los Sistemas de Información**
	Destinatarios:	Departamento de tecnología.

OBJETIVO

Asegurar la introducción de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

DESCRIPCIÓN

Se debe definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan. Definir los métodos de protección de la información crítica o sensible. Esto aplica a todos los sistemas informáticos, tanto propios o de terceros que se desenvuelven dentro de la institución.

4.24.1.1. Análisis y especificación de los requisitos de seguridad.

Control

Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.

Los requisitos de seguridad de la información deben ser identificados mediante diversos métodos, tales como los requisitos derivados del cumplimiento de políticas y regulaciones, identificación de amenazas, revisiones de incidentes o limitando el aprovechamiento de las vulnerabilidades. Resultados de la identificación deben ser documentados y revisados por parte de todos los interesados.

La identificación y administración de los requisitos de seguridad de la información y la asociación de un proceso deben ser integrados en la primera etapa de cualquier proyecto relacionado con los sistemas de información. Los requerimientos de la seguridad de la información deben considerar:

- La información a los usuarios y funcionarios de la institución sobre su rol y responsabilidades.
- Los requerimientos de protección necesaria de los activos, en particular los que tienen más impacto sobre la disponibilidad, confidencialidad e integridad de los servicios.
- Requerimientos derivados del proceso de negocio, tales como la autenticación para el acceso a sistemas, bases de datos y monitoreo de la red.

Impulsamos el desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.**
	Control:	**4.24.2. Seguridad en los Procesos de Soporte**
	Destinatarios:	Departamento de tecnología.

OBJETIVO

Controlar estrictamente los ambientes del proceso de soporte para los sistemas de información.

DESCRIPCIÓN

Los funcionarios responsables de los sistemas de aplicaciones deberían ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deberían garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo.

Se debe incorporar la seguridad de la información al ciclo de vida de desarrollo de sistemas en todas sus fases, desde la concepción hasta la desaparición de un sistema, por medio de procedimientos y métodos de desarrollo, operaciones y gestión de cambios.

4.24.2.1. Procedimientos de control de cambios en los sistemas.

Control

Los procedimientos de control de cambios deben ser documentados y aplicados formalmente con el fin de reducir al mínimo la corrupción de los sistemas de información. La introducción de nuevos sistemas y cambios importantes en los sistemas existentes deben seguir un proceso formal de especificaciones, ensayos y control de calidad.

Este proceso debe incluir una evaluación de riesgos, el análisis de los impactos de los cambios, y la especificación de controles de seguridad necesarios. Este proceso también debe garantizar que la seguridad y el control existente es adecuado para que los procesos de negocio no corran peligro.

Los procesos de cambios deben considerar que:

- La institución puede solicitar a la SEPS una visita de auditoría para el control de los sistemas de información.
- La SEPS emite un informe con la fecha en la que se realizará la visita para la realización de la auditoría informática, para lo cual el personal de la institución debe estar dispuesto. Este informe de auditoría debe indicar si es o no necesario la realización de algún cambio en los sistemas de

información.

- En caso de requerir un cambio en los sistemas informáticos, se debería hacer contrato temporal o permanente de un profesional experto en temas referentes a la auditoría informática, para el control de los procedimientos.

- Se puede solicitar a la WEBCOOP (proveedores del sistema financiero), un informe técnico de forma trimestral en el que detalle las actividades ejecutadas en el sistema, para constancia o evidencia del proceso.

4.24.2.2. Control a los cambios en los paquetes de software.

Control

En la medida de lo posible y factible, paquetes de software suministrados por el proveedor deben utilizarse sin modificación. Cuando un paquete de software tiene que ser modificado los siguientes puntos deben ser considerados:

- Los procesos de los servicios no estén en riesgo y que su integridad no se vea comprometida;

- Si se debe o no, obtener el consentimiento del proveedor;

- La posibilidad de obtener los cambios necesarios que el proveedor asigne como programa estándar de actualizaciones;

Todos los cambios deben ser totalmente probados y documentados, para que se puedan volver a aplicar si es necesario en futuras actualizaciones de software.

Control de los cambios se realiza mediante una solicitud previa, la cual se la puede realizar por medio de un mail, para la aprobación del jefe de tecnología, como se indica en la política de control de acceso. POLÍTICA DE CONTROL DE ACCESO A LA RED/INFORMACIÓN - NORMA INTERNACIONAL ISO/IEC 27002:2005, CAPITULO 3: TELETRABAJO.

4.25. RELACIÓN CON SUMINISTRADORES

	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Relación con suministradores**
	Control:	**4.25.1. Seguridad de la información en las relaciones con suministradores**
	Destinatarios:	Nivel Directivo

OBJETIVO

Garantizar la protección de los activos de la institución que son accesibles para los proveedores de servicios y controlar el acceso de terceros a los dispositivos de procesamiento de información.

DESCRIPCIÓN

Cuando la cooperativa requiera dicho acceso de terceros, se debería realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deberían definirse y aceptarse en un contrato con la tercera parte.

Se debe realizar un inventario de conexiones de red y flujos de información significativos con 3as partes, evaluar sus riesgos y revisar los controles de seguridad de información existentes.

4.25.1.1. Tratamiento del riesgo dentro de acuerdos de suministradores.

Control

Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la institución con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.

Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar,

almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la institución.

Es necesario establecer y documentar acuerdos con proveedores para asegurar que no haya malos entendidos entre la organización y el proveedor respecto a las obligaciones de ambas partes, para cumplir con los requisitos de seguridad de la información relevante.

Los siguientes términos deben ser considerados en los acuerdos con suministradores de servicios, con el fin de satisfacer los requisitos de seguridad de información:

- Descripción de la información que va a ser proporcionada y a la que van a tener acceso los suministradores;
- Clasificación de la información de acuerdo a la clasificación propuesta por el esquema la institución;
- Requerimientos legales y regulatorios, incluyendo la protección de datos y una descripción de cómo hacer que eso se cumpla;
- Obligación de cada una de las partes de implementar controles de seguridad;
- De ser necesario, información sobre políticas de seguridad relevantes deben ser especificadas en el contrato;

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Relación con suministradores**
	Control:	**4.25.2. Gestión de la prestación de servicio por suministradores.**
	Destinatarios:	Nivel Directivo.

OBJETIVO

Verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se ser prestan cumplen con todos los requerimientos acordados con los terceros.

DESCRIPCIÓN

Es necesario revisar periódicamente los acuerdos de nivel de servicio (SLA) y compararlos con los registros de supervisión. En algunos casos puede ser factible un sistema de reconocimiento o castigo. También es recomendable estar atentos a cambios que tengan impacto en la seguridad de la información.

4.25.2.1. Supervisión y revisión de los servicios prestados por terceros.

Control

Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente, para garantizar que las condiciones de seguridad de la información de los acuerdos, están siendo considerados por los suministradores.

Para la supervisión y revisión de los servicios, se deben considerar:

- Mantener informes, notificaciones e investigación de los incidentes o fallos de seguridad, para tener un tratamiento frente a cualquier amenaza.
- Garantizar que los proveedores mantienen la capacidad suficiente de acuerdo al diseño del pan de trabajo y asegurar que los servicios continúan con un nivel adecuado para afrontar cualquier clase de

amenaza.

La institución el suficiente control de las operaciones de los suministradores, una visualización de los controles de seguridad, especialmente para la información sensible o crítica y establecer medidas para la facilidad de acceso a la información necesaria requerida por los suministradores. La institución deberá aclarar las responsabilidades de los suministradores respecto a las actividades de seguridad como la identificación de vulnerabilidades y reporte de los incidentes de seguridad.

4.26. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

Impulsamos el desarrollo "CHUCHUQUÍ" Ltda. Cooperativa de Ahorro y Crédito	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**
	Control:	**4.26.1. Continuidad de la seguridad de la información.**
	Destinatarios:	Nivel Directivo

OBJETIVO

Asegurar la oportuna reanudación de los servicios, contrarrestando las interrupciones a las actividades normales de institución y proteger los procesos críticos de negocio de los efectos de los fallos principales de los sistemas de información o desastres imprevistos.

DESCRIPCIÓN

La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa. Si los controles de seguridad no pueden continuar resguardando la información ante situaciones adversas, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la

información.

Las autoridades deberían verificar la validez y la efectividad de las medidas de continuidad de la seguridad de la información regularmente, especialmente cuando cambian los sistemas de información, los procedimientos y los controles de seguridad de la información, o los procesos y soluciones establecidas para la gestión de la continuidad de negocio.

4.26.1.1. Planificación de la continuidad de la seguridad de la información.

Control

La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o desastres.

La institución debe determinar si la información de la continuidad de la seguridad es idónea dentro del proceso de gestión de la continuidad del negocio o dentro del proceso de gestión de recuperación de desastres. Los requisitos de seguridad de la información deben ser determinados en la planificación de la continuidad del negocio y recuperación de desastres.

Ante la falta de continuidad de negocio formal y la planificación de recuperación de desastres, la gestión de seguridad de la información debe asumir que los requisitos de la seguridad informática siguen siendo los mismos en situaciones desfavorables, en comparación con las condiciones operativas normales. Alternativamente, la institución podría realizar un análisis de impacto en el negocio de los aspectos de seguridad de la información para determinar los requisitos aplicables a situaciones comprometedoras.

4.26.1.2. Implantación de la continuidad de la seguridad de la información.

Control

La institución debe establecer, documentar, implementar y mantener procesos, procedimientos y controles que garanticen el nivel de requerimientos para la continuidad de negocio para la seguridad de la información, durante una

situación desfavorable.

La cooperativa debe asegurar que:

- Se encuentre establecida una adecuada estructura de gestión, apta para mitigar y responder ante un acontecimiento perturbador, utilizando personal con la capacidad, autoridad y experiencia suficiente.

- Formar personal preparado para incidentes, con la responsabilidad, autoridad y capacidad para mantener una eventualidad y conservar la seguridad de la información a la que están nominados.

- Documentación de planes, responsabilidades y procedimientos de recuperación se han desarrollado y aprobado, detallando como la organización podría gestionar un evento desfavorable y podría mantener toda la información crítica asegurada.

4.26.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Control

La institución debe verificar el establecimiento e implementación de los controles de continuidad de la seguridad de la información en intervalos de forma periódica con la finalidad de garantizar que dichos controles son validados y efectivos en caso de que ocurra una eventualidad.

Los cambios organizacionales, técnicos y cambios en los procedimientos operacionales o de los controles de continuidad, puede llevar a un cambio significativo de los requerimientos de seguridad de la información, relacionados con la continuidad de negocio.

La institución debe verificar estos controles por las siguientes razones:

- Probar la funcionalidad del proceso de continuidad seguridad de la información, procedimientos y controles para asegurarse de que son coherentes con los objetivos de continuidad de seguridad de la

información;

- Prueba del conocimiento y de rutina para operar el proceso de continuidad de la información de seguridad, procedimientos y controles para asegurar que su rendimiento es consistente de acuerdo con los objetivos de continuidad de seguridad de la información;

- La revisión de la validez y eficacia de las medidas de continuidad de seguridad de la información.

4.27. CUMPLIMIENTO

	**COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.**	
	Dominio:	**Cumplimiento**
	Control:	**4.27.1. Cumplimiento de los requisitos legales y contractuales.**
	Destinatarios:	Nivel Directivo.

OBJETIVO

Establecer requisitos legales, reguladores y de seguridad convenidos para el diseño, operación, uso y gestión de los sistemas de información.

DESCRIPCIÓN

Los requisitos legales específicos deberían ser anunciados por los asesores legales de la institución o por profesionales adecuadamente cualificados. Se debe obtener asesoramiento legal competente, especialmente si la institución opera o tiene clientes en múltiples jurisdicciones.

4.27.1.1. Identificación de la legislación aplicable.

Control

Se debe identificar, documentar y mantener a la fecha, de forma explícita todos

los requisitos legales y normativos para cada sistema de información y para la institución en general, junto al enfoque para llevar a cabo con esos requisitos o políticas de seguridad.

Las especificaciones de los controles y responsabilidades individuales que satisfacen los requerimientos deberían ser definidos y documentados.

4.27.1.2. Protección de datos y privacidad de la información personal.

Control

Los datos e información privada se deben proteger contra pérdidas, destrucción, accesos no autorizados de acuerdo con los requisitos, reglamentos legales, normas o políticas de seguridad.

Se deben establecer políticas de seguridad que especifique la forma apropiada de protección de datos y privacidad de la información personal. Tomando en cuenta que, si se divulga o se descuida información relevante, puede traer consecuencias para la institución, por ejemplo, la información de usuario y contraseña para la autenticación de los sistemas financieros.

Cada persona es responsable de cumplir con las políticas y manuales que hablan sobre estos principios y que a continuación se mencionan algunos de ellos:

- Manual de procedimientos para la asignación, custodia y conservación de los activos fijos.
- Política de uso y establecimiento de claves de acceso a servicios de información.
- Políticas/procedimientos de acceso a los sistemas de información – Módulo: asignación de claves y roles.
- Manual de procedimientos de destrucción de documentos confidenciales.
- Manual de seguridad física y entorno, Norma ISO/IEC 27002:2005

- Política de copias de seguridad, Norma ISO/IEC 27002:2005

4.27.1.3. Regulación de los controles criptográficos.

Control

Se debe utilizar controles de cifrado de la información en cumplimiento con todos los reglamentos, normas y políticas pertinentes.

Tal y como se estable en la Política de Copias de Seguridad – Norma ISO/IEC 27002:2005, El cifrado se aplicará solo en los ficheros considerados como críticos por el Departamento de Tecnología.

	COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUI" LTDA.	
	Dominio:	**Cumplimiento**
	Control:	**4.27.2. Revisiones de la seguridad de la información**
	Destinatarios:	Nivel Directivo.

OBJETIVO

Realizar revisiones regulares de la seguridad de los sistemas de información de acuerdo a las políticas de seguridad apropiadas y las plataformas técnicas; los sistemas de información deberían ser auditados para el cumplimiento y documentación de los modelos y controles de seguridad adecuados.

DESCRIPCIÓN

Deberían existir controles para proteger los sistemas activos y las herramientas de auditoría, durante el desarrollo de las auditorías de los sistemas de información. De recomendación se debe invertir en auditorías TI capacitadas que utilice ISO 27000, COBIT, ITIL, CMM y estándares o métodos de buenas prácticas similares como referencias.

4.27.2.1. Cumplimiento de las políticas y normas de seguridad.

Control

Los funcionarios del departamento de tecnología de la cooperativa deberían revisar periódicamente el cumplimiento del proceso de la seguridad de la información dentro de su área de responsabilidad respecto a las políticas, normas o cualquier otro tipo de requisito correspondiente a la seguridad de la información.

Si dentro de las revisiones se confirma el incumplimiento de las políticas, normas o requisitos de seguridad, se debería recurrir al reglamento interno, para tomar medidas correctivas y de esta forma garantizar que dichos incumplimientos no se vuelvan a repetir; todo este procedimiento de revisión debe documentarse y notificarse.

4.27.2.2. Comprobación del cumplimiento.

Control

Los sistemas de información se deben revisar periódicamente, para verificar el cumplimiento de las políticas y normas de seguridad dispuestas en la institución. Para lo cual el departamento de tecnología debe realizar informes trimestrales sobre los resultados de las revisiones para cumplimiento de la implementación del POA (Plan Operativo Anual).

4.28. TIEMPOS PARA REVISIONES Y MEJORAS

Para el sostenimiento del Plan de Contingencia se establecen tiempos en los cuales se deben realizar actualizaciones y revisiones, con la finalidad de establecer mejoras que contribuyan a la continuidad del Plan de negocio. A continuación, en la Tabla 34 se detallan los tiempos para cada dominio del plan de mantenimiento según lo que establecen documentos de mejores prácticas.

Se debe tomar en cuenta que cada institución puede establecer sus propios tiempos para

actualización de cada una de las áreas antes mencionadas, dependiendo de políticas internas o requerimientos exigidos por los entes de control.

Tabla 34. *Tiempos para revisiones o mejoras del Plan de Contingencia.*

TIEMPOS PARA EL MANTENIMIENTO DEL PLAN DE CONTINGENCIA	
OBJETIVO	TIEMPO DE MANTENIMIENTO
Gestión de incidentes de seguridad de la información y mejoras	La gestión de incidentes se debe realizar a corto plazo, es decir, se puede realizar un informe trimestralmente.
Políticas de seguridad	Las políticas se deben revisar cada año según disposiciones de reglamento interno.
Aspectos organizativos de la seguridad de la información	Este dominio se debe revisar cada vez que se genere un nuevo suceso en la institución, y de ser necesario se puede establecer una comisión nueva.
Gestión de activos	Cada que la institución realiza la adquisición de activos nuevos, las bases de datos son actualizadas. Para más detalles se puede ver en el manual de Gestión de activos.
Control de Accesos	Según se establece en las **políticas/procedimientos de acceso a los sistemas de información,** debido a la modificación de contraseñas, el dominio de control de accesos se debe revisar cada 30 días.
Cifrado	El dominio de cifrado al igual que el control de accesos se lo debe revisar cada 30 días.
Seguridad física y ambiental	La revisión de la seguridad física y ambiental se debe realizar a mediano plazo, es decir, realizar un informe cada 6 meses.
Seguridad en la operativa	Este dominio se debe revisar previo análisis e informe de auditoría interna, con el involucramiento de recursos humanos.
Seguridad en las telecomunicaciones	Este dominio se lo debe revisar a corto plazo, es decir, se debe realizar un informe trimestralmente.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Los sistemas de información tienen en tiempo variable, ya que depende de los requerimientos de los entes de control y la fecha de cumplimiento del proveedor.
Relaciones con suministradores	Cada que exista un cambio las políticas, reglamentos o normas dentro de la institución se debe revisar y analizar cómo estos nuevos aspectos pueden afectar a la relación con los suministradores.
Aspectos de la seguridad de la información en gestión de la continuidad de negocio	Este dominio se relaciona con el Manual de copias seguridad, ya que cada vez que se realiza un respaldo de backup, el responsable debe garantizar el correcto funcionamiento de las mismas.
Cumplimiento	El dominio de cumplimiento se debe mantener constantemente; se debe realizar revisiones periódicas del cumplimiento de las normas, reglamentos y políticas de seguridad.

Fuente: ISO/IEC 27002:2013. Contenido: Information Technology – Security techniques – Code of practice for information security controls.

CAPÍTULO V

IMPLEMENTACIÓN Y PRUEBAS

En este capítulo se explica el desarrollo de la implementación de los controles de seguridad que se ha considerado de prioridad para el Departamento de Tecnología y sus respectivas pruebas de funcionamiento para dar respuesta a los inconvenientes encontrados en el análisis de la situación actual.

El orden en que se encuentra la implementación es de acuerdo a la prioridad que se ha otorgado por parte de los miembros del Departamento de Tecnología de la COAC Chuchuqui Ltda.

5.1. SISTEMAS DE MONITOREO

La implementación de un sistema de monitoreo cubre la necesidad de mejor el dominio de **seguridad en las telecomunicaciones** según lo que se detalla en la norma ISO/IEC 27002:2013. En este dominio se encuentra el control de red el cual dice o recomienda que es necesario administrar y controlar las redes para que información de los sistemas y aplicaciones se encuentre protegida.

Los sistemas de monitoreo tienen gran importancia dentro de las instituciones, ya que gracias a ellos podemos estar al tanto del estado de los servidores y equipos de comunicación. De esta forma los administradores pueden gestionar de mejor manera la red y poder anticiparse ante cualquier eventualidad previniendo pérdidas de la información.

5.1.1. Selección del mejor sistema de monitoreo.

En la Tabla 35 se realiza una comparativa entre distintos softwares de monitoreo, de los cuales se ha llevado a cabo un análisis en las características que se especifican más adelante, considerando también el distintivo de licencia gratuita extendida.

Tabla 35. *Tabla comparativa de las principales características de los sistemas de monitorización.*

Sistema de monitorización	Software libre	Funcionalidad	Fácil uso	Arquitectura	Soporte	Licencia gratuita extendida
Nagios	●	●	●	●	●	●
Hiperic HQ	●	●	●	●	○	●
Zabbix	●	●	●	○	●	○
Zennos	●	●	○	○	●	○
Ganglia	●	○	○	○	○	○
OpenNMS	●	●	○	●	●	○
Cacti	●	○	○	○	○	●
Munin	●	●	○	○	○	●
BMC Patrol	○	●	●	●	○	○
HP Open view	○	●	●	●	○	○
IBM Tivoli	○	●	●	●	○	○
Pandora FMS	●	●	●	●	●	○

Fuente: Cruz L. (2012). Documento del estado del arte: Sistemas de monitorización. Recuperado de: http://1984.lsi.us.es/pfe/trac/pfe-pandora/raw-attachment/wiki/WikiStart/3-Doc.Estado%20del%20Arte.pdf

● El sistema de monitereo cumple con los requisitos globales de esa característica.

○ El sistema de monitoreo no cumple con por lo menos un requisito de esa característica.

Como se aprecia en la Tabla 35, el sistema de monitoreo de NAGIOS es el único que cumple con todos los requerimientos necesarios para la implementación, por lo cual se determina que éste va a ser adecuado para la institución.

Para la selección de la mejor plataforma de monitoreo se realizó una comparativa entre varias herramientas muy populares en este campo y para ello se consideraron los factores globales que a continuación se van especificar: (Cruz, 2012)

- Funcionalidad. - En este campo se analizará la capacidad de monitorizar servicios, hardware y sistema operativo, así como también la capacidad de generar gráficas, informes, estadísticas, el envío de notificaciones y alarmas.

- Facilidad de uso. – Este campo tiene que ver mucho en la forma y presentación de la interfaz gráfica o interfaz web tomando las consideraciones de configuración, personalización, instalación y puesta en marcha de dicha interfaz.

- Arquitectura. – Las consideraciones para este campo son basadas en las funcionalidades para realizar varios procesos de la aplicación, el consumo y requisitos de hardware y software, sistema con agentes que trabajen en cada nodo o cliente, la posibilidad de monitorear varios clientes o nodos a la vez, estabilidad en los cambios de configuración (reinicio del sistema).

- Calidad de soporte de comunidad o a nivel de empresa. – Se considerará el desarrollo constante de mejoras, actualizaciones o revisiones de la aplicación, la existencia de un foro de preguntas y resolución de problemas para los usuarios, disponibilidad de una versión Enterprise de su herramienta en caso de que los clientes tengan necesidades más específicas.

5.1.2. Implementación de sistema de monitoreo NAGIOS

5.1.2.1. Introducción a NAGIOS

NAGIOS se ha convertido en una herramienta potencial en aspecto de monitoreo en código abierto, su ambiente ofrece una vigilancia más comprensiva, para el mantenimiento y control de equipos, redes, servidores y se lo está empleando tanto en data centers como en laboratorios. Los tiempos, los equipos, los servicios que van a ser monitoreados se los configura dentro de los archivos que forman parte de esta aplicación, los mismos que se van a detallar más adelante.

NAGIOS permite gestionar hosts y servicios de forma remota en una sola ventana. Indica advertencias en los estados de los hosts o servicios y permite establecer alarmas que indica si algo va mal en sus servidores, y finalmente ayuda a los administradores de red detectar problemas antes de que ocurran. En consecuencia, ayuda a reducir el tiempo de indisponibilidad de los servicios y disminuye pérdidas empresariales.

Para acceder a NAGIOS se necesita de un navegador de Internet, en este se mostrarán varias pantallas que nos indicarán y nos ayudarán a comprobar el estado de los sistemas, detalles de los servidores, etc., todo esto por medio de gráficos, informes y listados.

NAGIOS ya cuenta con su versión 4.0.1, que su desarrollo se encuentra totalmente completo y verificado por expertos, por lo cual es muy estable y contiene algunas mejoras en comparación a versiones anteriores. Cabe recalcar que NAGIOS ha ido mejorando de la misma manera que Linux, gracias a la colaboración de varias personas que han aportado con nuevas ideas y modificaciones para mejorarlo.

Algunos de los servicios que nos presta NAGIOS son:

- Monitoreo de los recursos de un host (número de procesos, uso del disco, número de usuarios)
- Notificaciones a contactos cuando un servicio o un host tenga problemas (e-mail, pager o definido por el usuario)
- Interfaz web opcional con gráficas que describen cada uno de los estados en los que está o ha estado un servicio o equipo. Además, un historial de notificación y problemas.

Para relacionarse un poco más con NAGIOS es necesario conocer los archivos que le incluyen con sus especificaciones generales. A continuación, se menciona los más importantes:

- nagios.cfg (archivo principal de configuración)
- cgi.cfg (configuración de cgi’s para ambiente web)
- hosts.cfg (definición de los equipos a monitorear)
- hostgroups.cfg (definición de un grupo de hosts a los que pertenecerán los equipos definidos en host.cfg)
- contacts.cfg (contacto al que se le notifica cualquier problema de los servicios)

- services.cfg (se definen los servicios que se monitorean en cada equipo)

- commands.cfg (en este fichero se encuentran los comandos que se encargan de realizar la comunicación de los distintos servicios que se pueden monitorear en los equipos clientes)

5.1.2.2. Aplicación del sistema de monitoreo de NAGIOS

Los comandos de instalación y configuraciones iniciales de NAGIOS los podemos encontrar en el ANEXO K. Adicionalmente en el ANEXO L y ANEXO M se encuentran los manuales de Usuario y Administrador respectivamente, que hablan sobre la configuración de los ficheros para la personalización de NAGIOS, configuración de servicios, la forma de añadir un nuevo usuario y guías de cómo manipular la interfaz gráfica de NAGIOS.

En la Figura 18 se puede observar la interfaz web de NAGIOS con sus configuraciones correctamente aplicadas, donde los servidores de la COAC Chuchuqui Ltda. se encuentran bajo monitoreo.

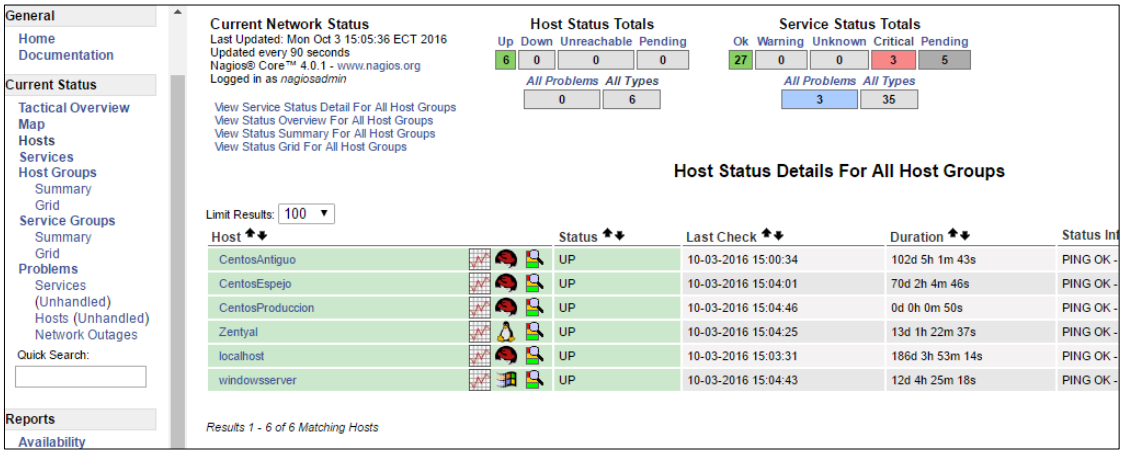


Figura 18: *Servidores de la COAC Chuchuqui bajo monitoreo de NAGIOS.*
Fuente: Elaboración propia.

En la Figura 19 se observa el resultado de la configuración de las gráficas con pnp4 en NAGIOS. Estas gráficas nos indican el estado de los servicios en distintos rangos de tiempo (últimas 4 horas, últimas 25 horas, última semana, último mes y último año), según se desee.

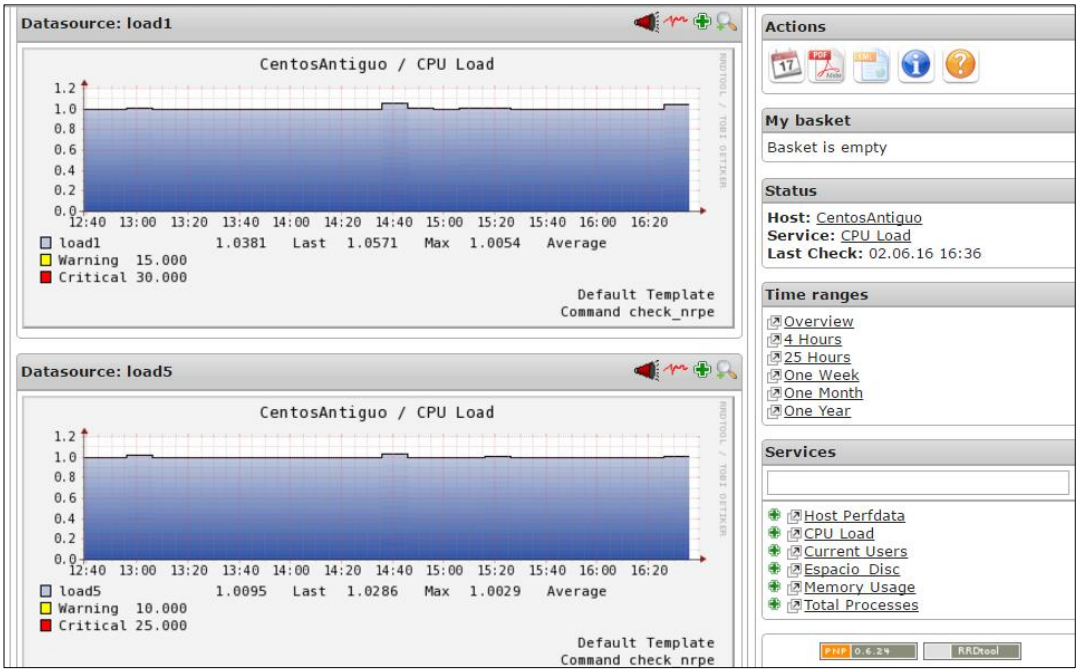


Figura 19: *Gráfica pnp4 en NAGIOS del servicio de CPU Load para el servidor Centos Antiguo*
Fuente: Elaboración propia.

Con la aplicación de **My basket** de pnp4 se puede seleccionar diferentes servicios incluso de diferentes servidores en caso de querer sacar reportes, como se muestra en la Figura 20.

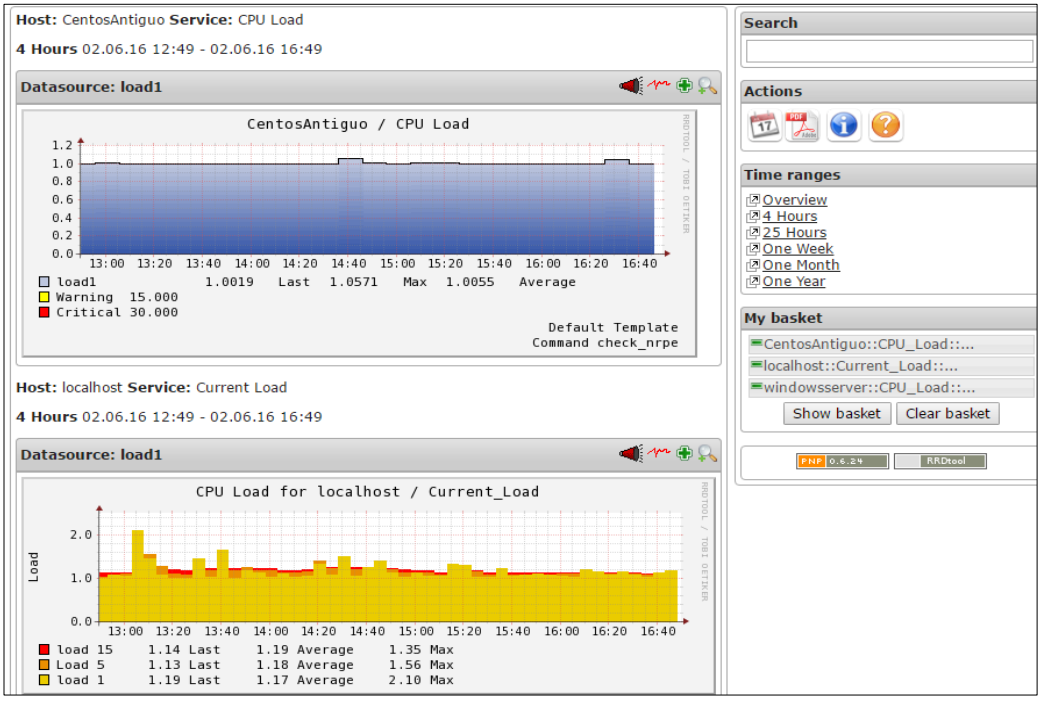


Figura 20: *Selección de varios servicios con la aplicación My basket de pnp4 en NAGIOS*
Fuente: Elaboración propia.

El sistema de monitoreo de Nagios se encuentra configurado de tal modo que las notificaciones de eventualidades se envían mediante mensajes de correo electrónico a los administradores de la red de la COAC Chuchuqui Ltda., como se puede observar en la Figura 21 un ejemplo.

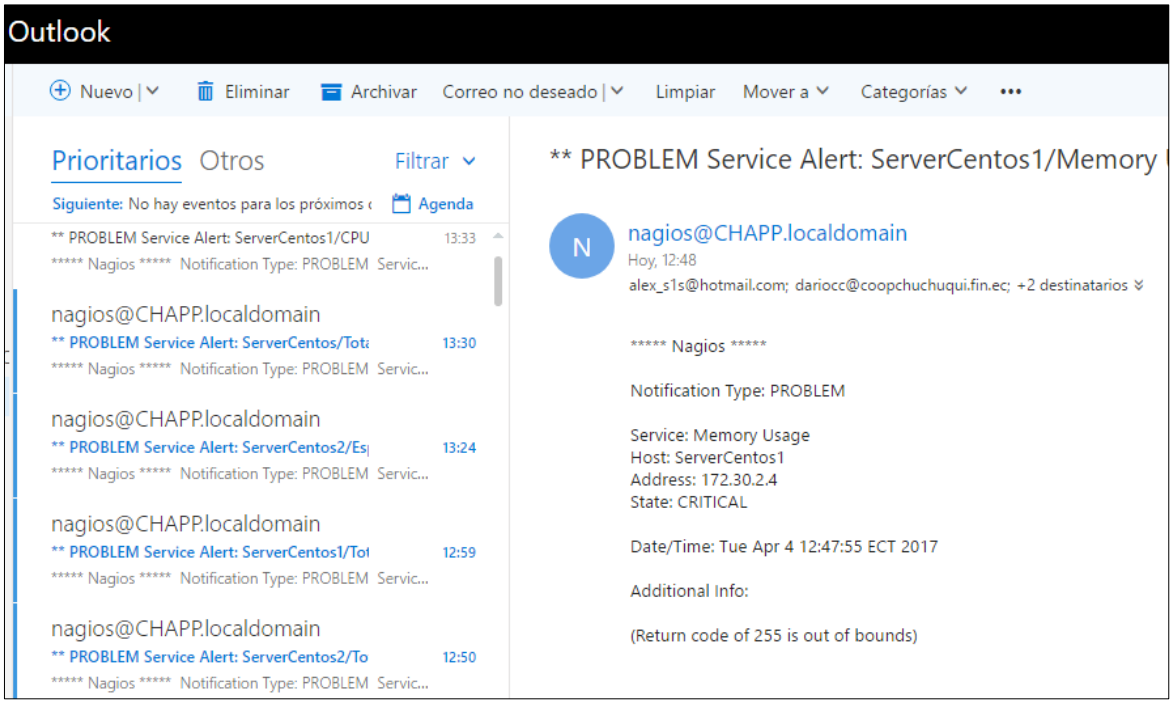


Figura 21: Notificaciones de Nagios mediante mensajes de correo electrónico

Fuente: Elaboración propia.

5.2. CONTROL DE PUERTOS ABIERTOS

Esta implementación mejora el dominio de **control de accesos** de la norma ISO /IEC 27002:2013, asegurando que ningún puerto que permita la conexión remota se encuentre habilitado o de ser el caso, mejorar la seguridad para los puertos habilitados.

Para el control de puertos se realizó un escaneó empleando el sistema operativo de Kali Linux y su herramienta de NMAP (Network Mapper) que es un escaneador de seguridad que permite descubrir host y servicios en la red. El procedimiento para este proceso es sencillo una vez que se cuente con este sistema operativo de Kali Linux, para su ejecución solo se necesita abrir un terminal e introducir el comando con la siguiente estructura:

- **[root@kali]#** nmap -sT networkAddress/netmask

Este comando permite conocer todos los puertos que se encuentran abiertos en toda la red que se especifique, el formato de la dirección de red es de la siguiente forma "192.168.10.0/24", en la Figura 22 se puede observar un ejemplo del formato para escribir correctamente el comando.

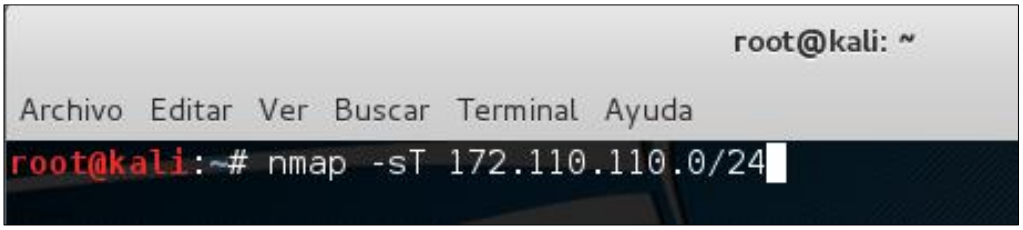


Figura 22: Comando para escaneo de puertos en una red con el software de Kali Linux

Fuente: Elaboración propia.

Para obtener simplemente los puertos que se encuentran abiertos en la red, se puede añadir el comando **grep** como se indica en la Figura 23.

Figura 23: Comando para escaneo de puertos abiertos en la red mediante nmap en Kali Linux

Fuente: Elaboración propia.

Otra forma de realizar el escaneo de puertos es mediante el comando **zenmap** que simplemente es la forma gráfica de nmap. En la Figura 24 se puede observar un ejemplo de escaneo con la interfaz de znmap. La forma gráfica es un poco más fácil de emplear, ya que solo debemos indicar la dirección del servidor o conjunto de direcciones que van a ser analizadas para que el comando de ejecución se autocomplete automáticamente. Incluso podemos especificar algunos detalles adicionales que ofrece zenmap como es el perfil del escaneo, detalles de los hosts, topología, entre otros.

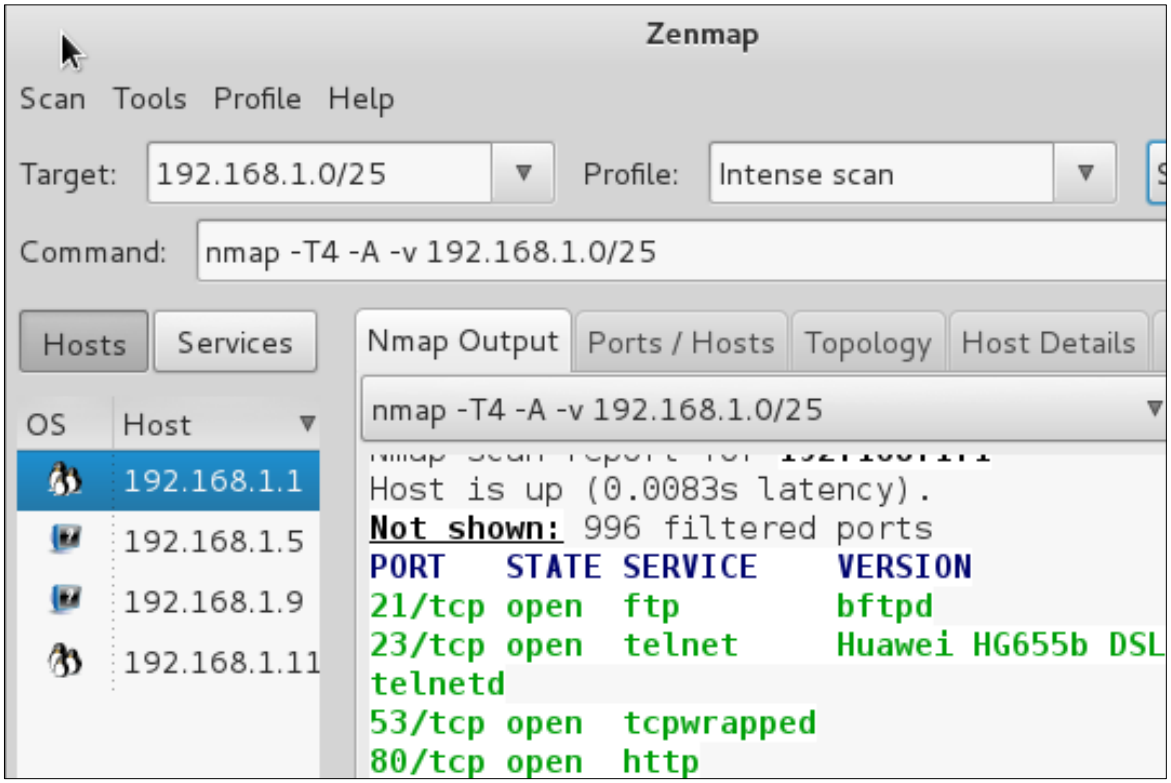


Figura 24: Escaneo de puertos abiertos con la interfaz de zenmap.

Fuente: Elaboración propia.

En la Tabla 36 se muestra un resumen del escaneo realizado en la red de la COAC Chuchuqui Ltda., en el cual se detalla el servicio de cada puerto que se encuentra en estado abierto.

Tabla 36: *Puertos abiertos en la red de la COAC Chuchuqui.*

PUERTOS SCANNER - KALI LINUX	PUERTO TCP/UDP	SERVICIOS	MÁS DETALLES
Discovered open port 22/tcp on 172.110.xxx.xxx	22	Conexión de acceso remoto SSH	
Discovered open port 993/tcp on 172.110. xxx.xxx	993	Servidor de correo entrante IMAP "Internet Message Access Protocol"	
Discovered open port 135/tcp on 172.110. xxx.xxx	135	Servicio RPC (Remote Procedure Call)	win xp para "ASISTENCIA DE ACCESO REMOTO" (telefonica utiliza este puerto para espiar la actividad de sus usuarios y para regular la transferencia de ancho de banda)
Discovered open port 53/tcp on 172.110. xxx.xxx	53	DNS (Domain Name Server) (TCP/UDP) DNS (Servidor de Nombres de Dominio) (TCP / UDP) Bonk (DoS) (TCP) Bonk (DoS) (TCP)	
Discovered open port 80/tcp on 172.110. xxx.xxx	80	Servidor WEB (HTTP)	
Discovered open port 143/tcp on 172.110. xxx.xxx	143	Servidor de correo entrante IMAP "Internet Message Access Protocol"	
Discovered open port 445/tcp on 172.110. xxx.xxx	445	Microsoft-DS (TCP/UDP) Microsoft-DS (TCP / UDP)	Compartir archivos a través de una red TCP/IP Windows.
Discovered open port 139/tcp on 172.110. xxx.xxx	139	NETBIOS Session Service (MS Windows) (TCP/UDP) Servicio de Sesión NetBIOS (MS Windows) (TCP / UDP)	Sirve para compartir archivos e impresoras en Windows. Hace que la red sea vulnerable a los ataques de los piratas informáticos.
Discovered open port 110/tcp on 172.110. xxx.xxx	110	Servidor correo saliente POP3 (Postal Office Protocol)	
Discovered open port 995/tcp on 172.110. xxx.xxx	995	pop3 protocol over TLS | SSL (was spop3) (TCP/UDP) pop3 protocolo sobre TLS | SSL (se spop3) (TCP / UDP)	
Discovered open port 587/tcp on 172.110. xxx.xxx	587	Servidor Correo saliente SMTP	puerto 587 se usa para SMTP (Protocolo de Transferencia de Correo Simple).

Discovered open port 443/tcp on 172.110. xxx.xxx	443	HTTPS Webserver (SSL) Secure HTTP Protocol (TCP/UDP) Servidor web HTTPS (SSL) protocolo HTTP seguro (TCP / UDP)	
Discovered open port 465/tcp on 172.110. xxx.xxx	465	Servidor Correo saliente SMTPS "segura"	smtp protocol over TLS | SSL (was ssmtp) (TCP/UDP) protocolo SMTP sobre TLS | SSL (se ssmtp) (TCP / UDP); SMTPS
Discovered open port 3268/tcp on 172.110. xxx.xxx	3268	Microsoft Global Catalog (TCP/UDP) Microsoft catálogo global (TCP / UDP)	
Discovered open port 389/tcp on 172.110. xxx.xxx	389	Lightweight Directory Access Protocol (TCP/UDP) Directorio de Protocolo ligero de acceso (TCP / UDP)	Servicios de Nombres -- DNS (53/udp) a todas las máquinas que no sean servidores de nombres, transferencias de zona DNS (53/tcp) excepto desde servidores secundarios externos, LDAP (389/tcp y 389/udp)
Discovered open port 3269/tcp on 172.110. xxx.xxx	3269	Microsoft Global Catalog with LDAP | SSL (TCP/UDP) Microsoft catálogo global con LDAP | SSL (TCP / UDP)	
Discovered open port 8443/tcp on 172.110. xxx.xxx	8443	SW Soft Plesk Control Panel, Apache Tomcat SSL, Promise WebPAM SSL, McAfee ePolicy Orchestrator (ePO)	(puerto para controlador GUI / API, como se ve en el navegador web)
Discovered open port 636/tcp on 172.110. xxx.xxx	636	TCP UDP Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	
Discovered open port 1024/tcp on 172.110. xxx.xxx	1024		Accesos remotos, internet y uso de los troyanos
Discovered open port 464/tcp on 172.110. xxx.xxx	464	kpasswd (TCP/UDP) kpasswd (TCP / UDP)	
Discovered open port 3128/tcp on 172.110. xxx.xxx	3128	RingZero (TCP) RingZero (TCP)	Página web, bloqueo de proxy

Fuente: Elaboración propia.

El escaneo muestra que varios puertos se encuentran abiertos en distintos servidores de la red de la cooperativa, para los cuales los miembros del departamento de tecnología, al tener conocimiento de las herramientas necesarias para los sistemas financieros y de aplicaciones, deberán determinar si dichos puertos deben ser bloqueados o deben permanecer abiertos.

En caso de que se decida mantener los puertos abiertos dependiendo de los requerimientos de los sistemas, los encargados de la administración de la red, deben establecer reglas denegación o aceptación en el cortafuegos, para prevenir que estos puertos sean explotados para ataques informáticos.

De los resultados del escaneo se considera de importancia tomar medidas para controlar el estado del puerto 22 correspondiente al protocolo de Secure Shell (SSH). En vista a la necesidad de realizar conexiones seguras hacia los servidores de la cooperativa por parte de los miembros del departamento de tecnología, se decide mantener este protocolo abierto, pero asignándole un número de puerto distinto al que se encuentra por defecto.

5.2.1. Cambio de número de puerto SSH.

SSH es un protocolo que permite establecer comunicaciones seguras entre dos sistemas empleando una estructura cliente/servidor, la cual permite a los usuarios conectarse a un host o servidor de forma remota. SSH usa encriptación al crear sesiones de conexión, haciendo casi imposible que alguien pueda obtener contraseñas en texto plano. (Red Hat Enterprise Linux, 2013)

Sin embargo, SSH maneja un número de puerto asignado por defecto que es 22, el cual es conocido por muchos profesionales que manejan el tema de telecomunicaciones o informática, lo que le transforma en una vulnerabilidad fácil de atacar. Por este motivo es recomendable cambiar este número de puerto. (Red Hat Enterprise Linux, 2013)

La IANA en calidad de autoridad para la asignación de números de internet, realizó una distribución de los números disponibles en tres categorías:

- **Puertos bien conocidos,** que se encuentran comprendidos entre 0 y 1023. Estos 1024 puertos pueden ser representados en 10 bits y se han establecido como reservados para servicios conocidos.
- **Puertos registrados.** Conforman 48127 puertos comprendidos entre 1024 y 49151.
- **Puertos dinámicos y privados.** Están comprendidos entre los números 49152 y 65535. (Castillo & Medina, 2014)

En caso de tener la necesidad de asignar un número puerto a cualquier aplicación (aunque ya tenga asignado uno por defecto), debe seleccionarse un número en el rango 1024 - 65535. Para esta asignación de puertos se puede acceder a la configuración del fichero **/etc/services** presente en los sistemas Linux (Castillo & Medina, 2014)

5.2.1.1. Configuración SSH en los servidores.

A continuación, se muestra un ejemplo:

Paso 1: Ingresar al servidor en el que se desea cambiar de número de puerto. Se lo puede realizar directamente en la interfaz del servidor o de forma remota mediante el mismo protocolo SSH.

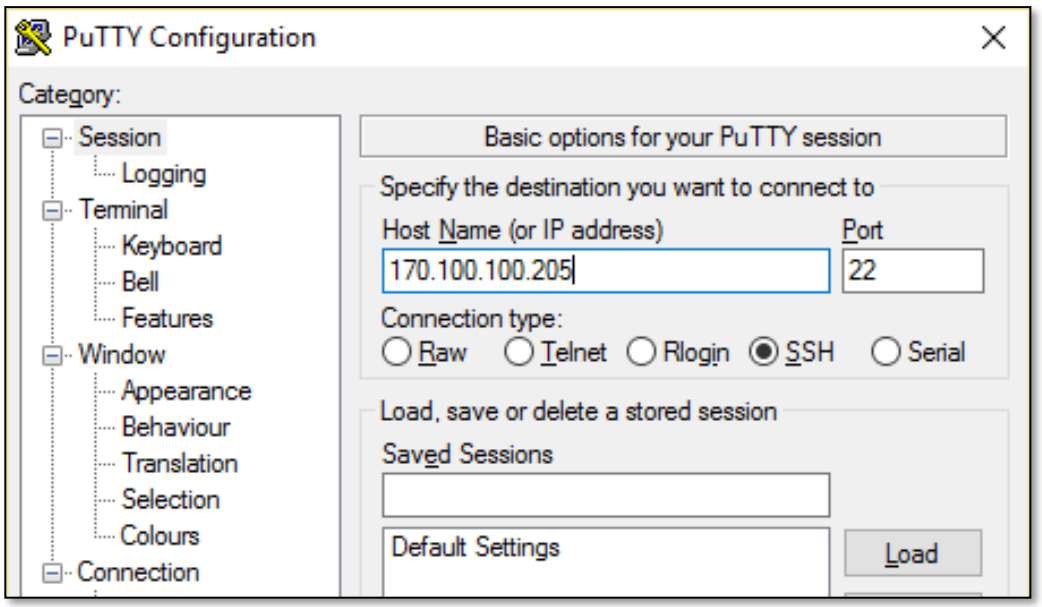


Figura 25: Ventana de acceso remoto SSH mediante el puerto por defecto (22) en Putty.

Fuente: Elaboración propia.

Una vez que se ingresa va a pedir un usuario y una contraseña.

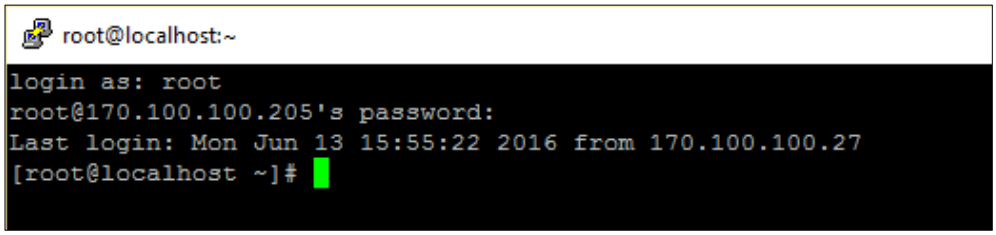


Figura 26: Verificación de inicio de sesión remota ssh mediante el puerto por defecto (22).

Fuente: Elaboración propia.

Paso 2: Configurar el fichero **/etc/ssh/sshd_config** donde se debe ubicar el número de puerto SSH (22).

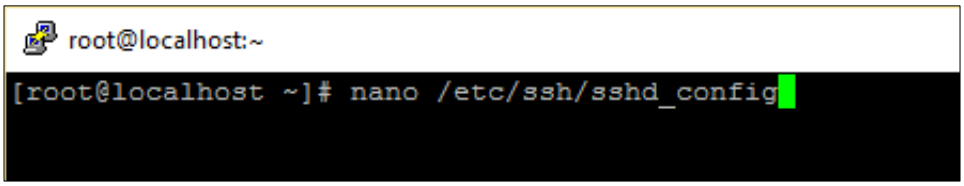


Figura 27: Comando para la modificación del archivo de configuración del servicio sshd

Fuente: Elaboración propia.

Una vez ubicado el número de puerto se va a modificar este número y en caso de que se encuentre comentado, se debe descomentar. Se guarda la configuración antes de salir del fichero.

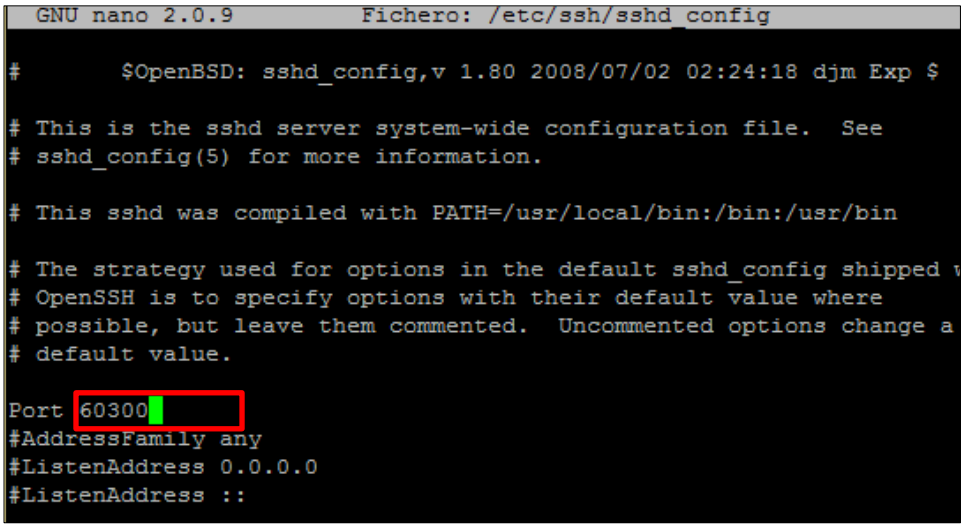


Figura 28: Asignación de un nuevo número de puerto para el servicio ssh.

Fuente: Elaboración propia.

Paso 3: Luego se configura el fichero **/etc/services**. En este archivo de configuración se encuentran todos los servicios disponibles para el equipo con su respectivo número de puerto.

Se debe comentar las líneas que le corresponden al servicio SSH, para deshabilitar el puerto 22.

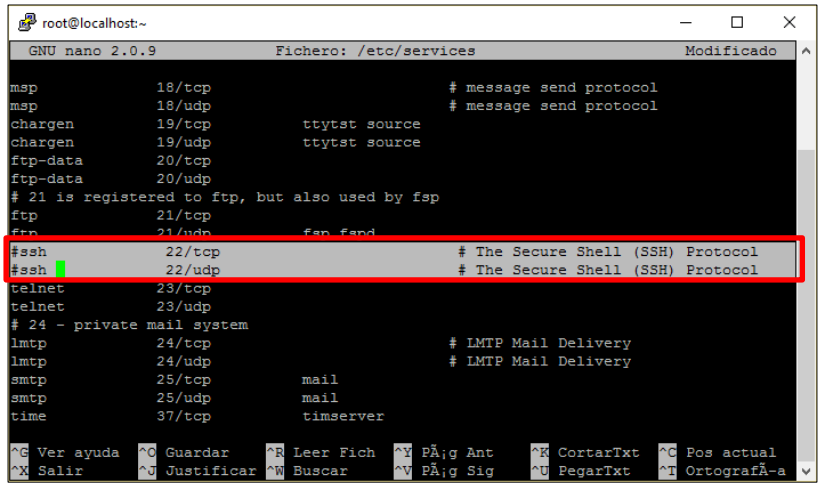


Figura 29: *Modificación del fichero /etc/services*
Fuente: Elaboración propia.

Al final del fichero se añade el número de puerto nuevo para el protocolo SSH, verificando que este número no se encuentre ocupado en algún otro servicio. Guardar la configuración y salir.

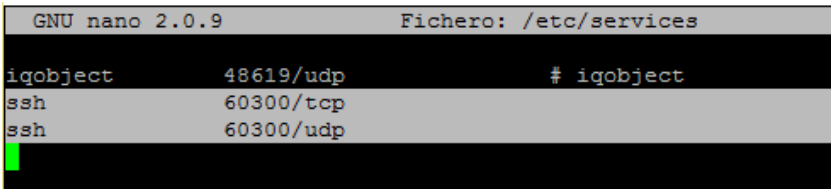


Figura 30: *Adición del nuevo número de puerto para el protocolo ssh*
Fuente: Elaboración propia.

Paso 4: Reiniciar el servicio **sshd** para que hagan efecto los cambios realizados.

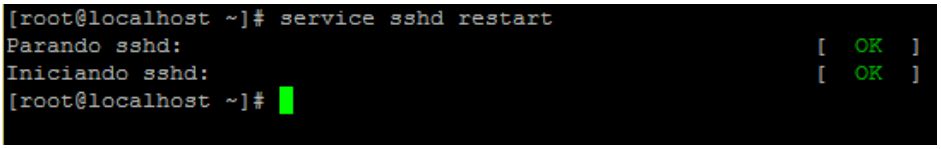


Figura 31: *Reinicio del servicio sshd*
Fuente: Elaboración propia.

Paso 5: Verificar que se ha realizado el cambio satisfactoriamente.

Volver a ingresar al equipo, por el puerto SSH, pero con el número por defecto (22) para comprobar que ya no se puede ingresar.

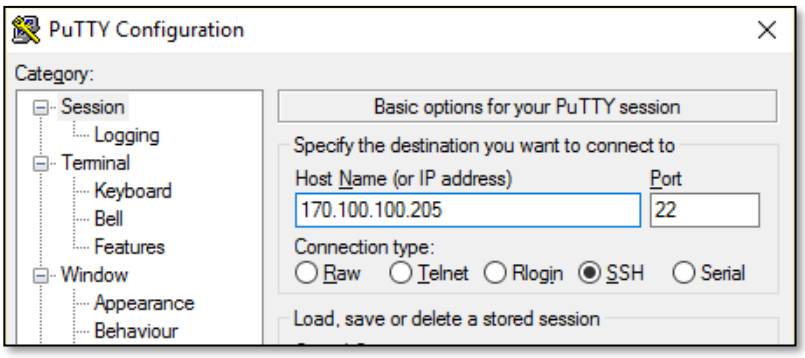


Figura 32: *Verificación de bloque del ingreso por el puerto 22*
Fuente: Elaboración propia.

Debe salir un mensaje de Error, indicando que la conexión ha sido rechazada.

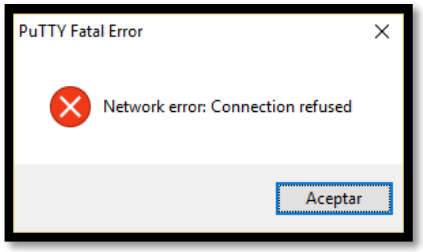


Figura 33: *Mensaje de error de conexión en el puerto 22*
Fuente: Elaboración propia.

Ahora una segunda prueba, ingresando por SSH, pero con el nuevo número de puerto asignado.

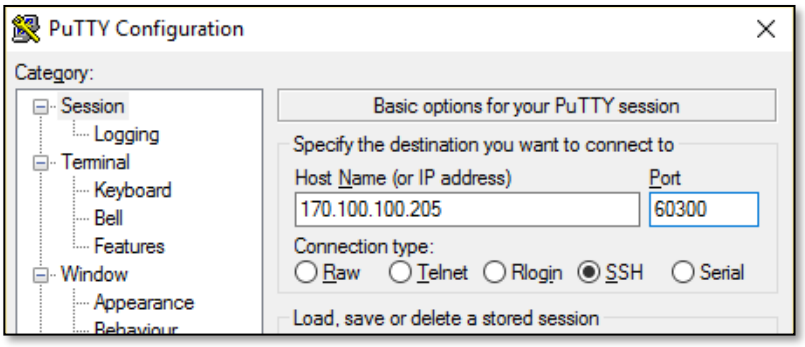


Figura 34: *Verificación de conexión mediante el nuevo número de puerto asignado*
Fuente: Elaboración propia.

La conexión se va establecer y pedirá un usuario y una contraseña para permitir el ingreso.

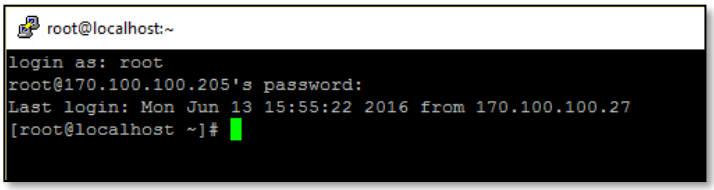


Figura 35: *Conexión satisfactoria mediante el nuevo número de puerto asignado*
Fuente: Elaboración propia.

5.2.1.2. Configuración de nuevos puertos en Firewall.

Paso 1: Ingresar a la interfaz de configuración del firewall que en este caso es Zentyal.

Figura 36: *Ventana de ingreso a la interfaz Zentyal*
Fuente: Elaboración propia.

Paso 2: Ingresar en la configuración de servicios que se encuentra en la sección de red de Zentyal.

Figura 37: *Pestaña de servicios de Zentyal*
Fuente: Elaboración propia.

Paso 2: Buscar la descripción de **Secure Shell** de donde surge el acrónimo SSH. En este servicio es donde se va a realizar la configuración de los nuevos números de puertos para este protocolo.

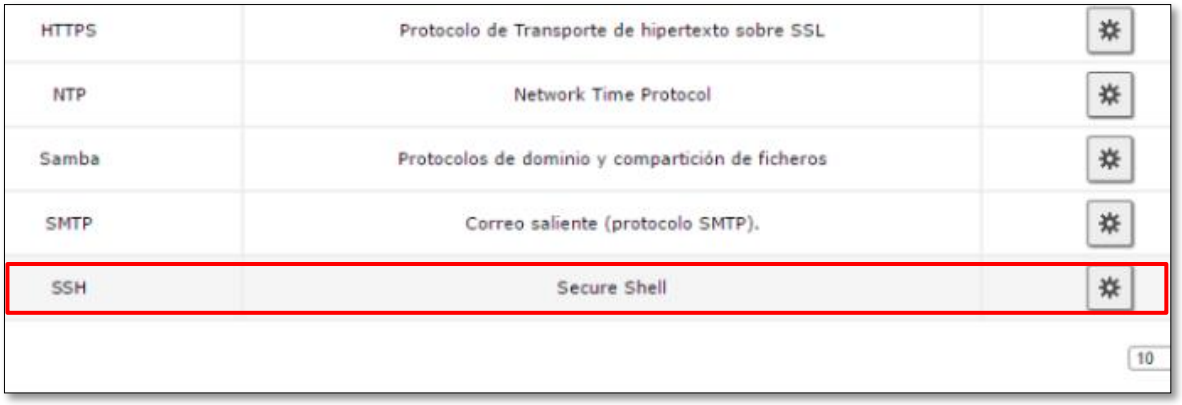


Figura 38: *Servicio Secure Shell (SSH) en Zentyal*
Fuente: Elaboración propia.

Paso 3: Clic en configuración.

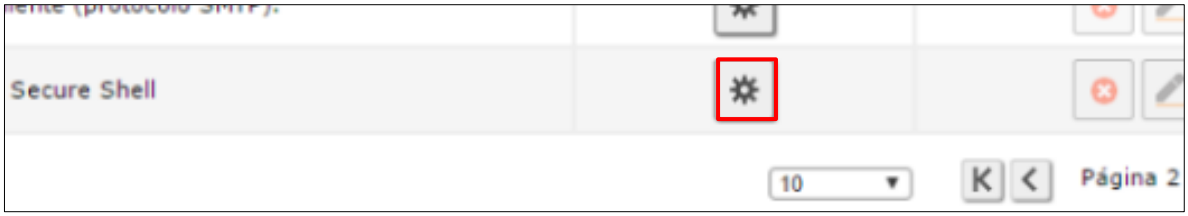


Figura 39: Botón de configuración de Secure Shell
Fuente: Elaboración propia.

Paso 4: Clic en Añadir Nuevo

Figura 40: *Botón para añadir un nuevo puerto para Secure Shell*
Fuente: Elaboración propia.

Paso 5: Completar la configuración del servicio, asignación de nuevo número de puerto y Añadir.

Figura 41: *Configuración del nuevo puerto de Secure Shell*
Fuente: Elaboración propia.

Paso 5: Guardar cambios.

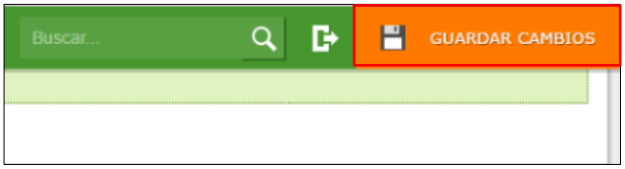


Figura 42: *Botón para guardar cambios realizados en Zentyal.*
Fuente: Elaboración propia.

Este procedimiento se repite para cada servidor, realizando una asignación de número de puerto SSH diferente para cada uno, obteniendo mayor seguridad debido a que ciertos funcionarios tienen autorización sólo para servidores determinados por los administradores. En la Tabla 37 se enlista cada servidor con su respectiva dirección IP y número de puerto SSH asignado.

Tabla 37: *de Asignación de números de puerto SSH para servidores del Data Center de la Cooperativa Chuchuqui Ltda.*

Servidor	Dirección IP	Puerto SSH
Firewall	172.110.xxx.xxx	xxxxx
Producción Antiguo	172.110.xxx.xxx	xxxxx
Producción Espejo	172.110.xxx.xxx	xxxxx
Aplicaciones	172.110.xxx.xxx	xxxxx
Windows Server	172.110.xxx.xxx	xxxxx
Producción	172.110.xxx.xxx	xxxxx

Fuente: Elaboración propia.

5.3. CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN Y POLÍTICAS DE SEGURIDAD.

La realización de una capacitación ayuda a mejorar el dominio de **seguridad ligada a los recursos humanos** en cual se encuentra el dominio de concienciación, educación y capacitación en seguridad de la información, que recomienda que se deben realizar capacitaciones periódicas en esta temática.

La capacitación fue destinada a todo el personal de la COAC Chuchuqui Ltda., con la finalidad de lograr una concienciación y educación en los aspectos de la seguridad de la información, explicando una introducción sobre la importancia de los controles de seguridad y dar conocimiento de las nuevas políticas instauradas por el departamento de Tecnología.

La capacitación se la realizó el día jueves 15 de septiembre de 2016 en el salón de capacitaciones CHUCHUQUI Ltda., con el tema "**SEGURIDAD DE LA INFORMACIÓN**", con una duración de 4 horas. Los puntos a tratarse en la capacitación fueron los siguientes:

- Introducción a la seguridad de la información.
- Formas de ataques informáticos y casos de fraude en el Ecuador.
- Usuarios y contraseñas de los sistemas.
- Controles de conexión a la red.
- Políticas de uso del repositorio centralizado.
- Políticas de control de dispositivos móviles.
- Política de copias de seguridad.
- Política de control de acceso a la red y a la información.
- Clasificación de la información.
- Etiquetado y manipulación de la información.
- Manual de gestión de activos.
- Manual de seguridad física y entorno.
- Formas de protegerse ante ataques informáticos.
- Formas adecuadas de navegación.

Para constancia de la realización de la capacitación en la Figura 43 y Figura 44 se muestra parte de su desarrollo y en el ANEXO P se encuentra el listado de los funcionarios participantes.

Los resultados que se obtuvieron fueron los esperados por el departamento de tecnología cumpliendo con la concienciación del personal mediante ejemplos de ataques

y la forma de como poder actuar ante uno de estos.

Figura 43: Presentación ante el personal de la COAC Chuchuqui Ltda., para dar inicio a la capacitación.

Fuente: Elaboración propia.

Figura 44: Cierre de la capacitación mediante la experiencia del personal de la COAC Chuchuqui.

Fuente: Elaboración propia.

5.4. IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN EL DATA CENTER

En el dominio de seguridad física y ambiental de la norma ISO/IEC 27002, se habla sobre la protección de los equipos contra amenazas externas y ambientales, para lo cual se ha decidido cumplir con este dominio en el Centro de Datos de la COAC Chuchuqui Ltda.

En el levantamiento de la información sobre los controles de seguridad en el Data Center se encontraron las siguientes debilidades:

- No posee una bitácora de acceso y/o cámaras de seguridad para el control de ingreso.
- Los controles ambientales del área no cuentan con control de humedad, temperatura y protección contra la electricidad estática, ni tampoco se monitorean los parámetros adecuados.
- No cuenta con la instalación de equipos de detección de humo, fuego, y movimiento o equipos de control de incendios.
- El UPS que posee esta área no garantiza el respaldo de energía necesario y la planta eléctrica se encuentra fuera de funcionamiento a la fecha de la visita

Hay que recalcar que estas mismas impotencias fueros descritas por la SEPS en un reporte realizado con anterioridad. Para dar respuesta a estos problemas se implementaron los siguientes equipos y accesorios:

- Lectora de huella digital para interior con proximidad

  En la Figura 45 se puede observar la lectora de huella digital para el control de acceso al Data Center de la COAC, este lector permite el acceso de las siguientes formas:

  - Sólo con tarjeta.
  - Con tarja y contraseña de 4 dígitos
  - Contraseña de 4 dígitos y huella digital
  - Huella digital y contraseña de 4 dígitos

Figura 45: Lectora de huella digital para control de acceso en el Data Center de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Características:

Capacidad de 2000 Huellas, 5,000 usuarios, Almacenamiento 50,000 eventos, INCLUYE. SOFTWARE. Sistema de respaldo en caso de pérdida de energía AC.

- Puerta de seguridad para cuarto de comunicaciones

  En la Figura 46 se puede observar la puerta de seguridad implementa en el Data Center de la COAC vista desde el interior del cuarto.

Figura 46: Puerta de seguridad del Data Center de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Características:

Construida en estructura metálica y forrada con tol de 2mm, cortafuego internamente con material termoaislante para resistir 1000 F por 1 hora.

Bisagras especiales de acero de 1" de diámetro x 6 cm de largo, con rodamientos para evitar fricción.

Dimensiones de la Puerta de 1 m x 2 m de alto.

Incluye brazo auto retorno, y barra antipánico.

Mirilla 30x30 cm.

- Sistema aire acondicionado tipo split pared para cuarto de comunicaciones capacidad: 24.000 BTU/h

En la Figura 47 y Figura 48 se puede observar los componentes del sistema de aire acondicionado tipo Split de pared.

Figura 47: Sistema de aire acondicionado (correspondiente a la parte interior del Data Center).

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Figura 48: Sistema de aire acondicionado (correspondiente a la parte exterior del Data Center).

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Característica:

Kit de instalación, incluye tubería de cobre, codos, soldadura de plata, oxiacetilénica.

Base metálica para equipo externo.

Filtros ADK- 163.

Accesorios eléctricos, Caja de Breaker Bifásica.

Acometida eléctrica para alimentación de equipos.

Bomba de condensado para desagüe de equipo interior.

Materiales Varios de instalación (canaleta, manguera, accesorios, material consumible).

- Detector de humo

  En la Figura 49 se muestra el detector de humo implementado en el interior del Data Center de la COAC Chuchuqui Ltda.

Figura 49: Detector de humo en el interior del Data Center

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

- Extintor de fuego

  En la Figura 50 podemos observar el extintor implementado en el exterior del Data Center.

Figura 50: Extintor implementado en el exterior del Data Center de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Todas las instalaciones antes mencionadas se cumplieron según las normativas y exigencias de la SEPS. Adicionalmente para dar cumplimiento a las recomendaciones del Plan de contingencia se implementó señalética se seguridad alrededor de todas las

instalaciones de la COAC Chuchuqui Ltda., incluyendo mapas de rutas de evacuación por cada piso de la institución como se puede observar en la Figura 51, Figura 52, Figura 53, Figura 54 y Figura 55.

Figura 51: Señalética ubicada en las gradas que hacienden a la tercera planta alta de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Figura 52: Señalética y extintor correspondientes a la tercera planta alta de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Figura 53: Señalética correspondiente a la salida de la tercera planta alta de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

Figura 54: Señalética y extintor correspondientes a las escaleras que hacienden a la segunda planta alta de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

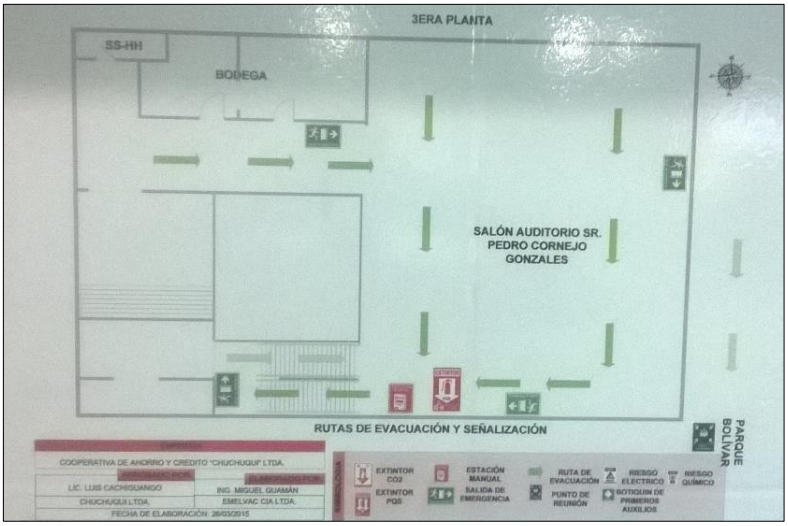


Figura 55: Señalética correspondiente a las rutas de evacuación de la tercera planta alta de la COAC Chuchuqui Ltda.

Fuente: Departamento de Tecnología de la COAC Chuchuqui Ltda.

5.5. RESUMEN DE IMPLEMENTACIÓN

A continuación, se presenta un resumen de los controles de seguridad que han sido implementados o que se han mejorado gracias al presente trabajo en coordinación con los miembros del departamento de tecnología de la cooperativa CHUCHUQUI Ltda. Este resumen se lo realiza especificando los trabajos realizados en cado dominio prescrito por la Norma ISO/IEC 27002 en la cual se encuentra basado este proyecto.

Este resumen se encuentra revisado por los miembros del Departamento de Tecnología de la COAC Chuchqui Ltda., en el ANEXO T se puede observar este mismo resumen sellado y firmado por el asistente de Tecnología para comprobar la veracidad de lo expuesto.

Gestión de incidentes en la seguridad de la información.

Este dominio dio el punto de partida para este trabajo, ya que para dar respuesta a sus directrices se realizó un análisis de riesgos, determinando las fortalezas, oportunidades, debilidades y amenazas según el estado actual de los controles de seguridad en la cooperativa; al igual que se fijaron valoraciones para cada tipo de riesgo dependiendo de la frecuencia con la que estos se presentan.

Políticas de seguridad.

Para el mejoramiento de este dominio se crearon 5 políticas nuevas relacionadas a la seguridad de la información basándose en la norma ISO/IEC 27002, las cuales ya fueron aprobadas por consejo que ya se encuentran puestas en marcha y que se enlistan a continuación:

- Política de Control de Acceso a la Red/Información, según norma internacional ISO/IEC27002:2005
- Políticas de Copias de Seguridad, según norma internacional ISO/IEC27002:2005
- Manual de Gestión de Activos Informáticos, Norma Internacional ISO/IEC 27002:2005
- Manual de procedimientos de Destrucción de Documentos Confidenciales.
- Manual de Seguridad Física y Entorno Norma Internacional ISO/IEC 27002:2005.

Aspectos organizativos de la seguridad de la información.

Se establecieron nuevas responsabilidades y procedimientos relacionados con la seguridad de la información para los miembros del departamento de tecnología de la cooperativa. También se creó una lista de contactos de autoridades y una lista de contactos de grupos de interés especial.

Seguridad ligada a los recursos humanos.

Este dominio se encuentra bien establecido por parte de la cooperativa CHUCHUQUI, pero se hace un llamado de atención en la forma de cómo se realiza el cambio de puesto de trabajo del personal, recomendando tener más seguridad con la información a la que tienen acceso los funcionarios.

Gestión de activos.

En este dominio se actualizó el inventario de activos. También se realizó una capacitación explicando las directrices para la clasificación de la información según el manual adoptado por la institución al igual que se enseñó el procedimiento para el manejo de los soportes de almacenamiento.

Control de accesos.

Para dar respuesta a este dominio se implementó a nivel de hardware una puerta de seguridad en el centro de datos de la cooperativa, junto con un biométrico para el control de acceso y a nivel de software se realizó un escaneo de puertos y se realizó el cambio de número de puerto para el protocolo SSH, para restricción de acceso no autorizado de forma remota.

Cifrado.

En este dominio se realizó una capacitación del personal sobre cómo manejar las claves de accesos a los sistemas.

Seguridad física y ambiental.

Se mejoró este dominio mediante la implementación de señalética alrededor de toda la institución, se mejoró la infraestructura de las oficinas y despachos y además se

planteó una solución para la protección de los equipos, de la cual se implementó un sistema de aire acondicionado en el área del centro de datos, además se realizaron cotizaciones para la implementación de gabinetes de pared para los equipos de conexión intermedia.

También dentro de la capacitación realizada se explicó sobre la política de puesto despejado y bloqueo de pantalla, apara los instantes en los que sea necesario dejar el puesto de trabajo desatendido.

Seguridad en la operativa.

Se establecieron directrices y formatos para la gestión de cambios, y la documentación sobre los procedimientos a seguir en caso de algún incidente.

Seguridad en las telecomunicaciones.

En este dominio se implementó un sistema de monitoreo para los servidores principales de la cooperativa, con la herramienta de NAGIOS. También se planteó el cambio del cableado estructurado de toda la red, debido a la mala distribución de la red, para lo cual el departamento de contabilidad ya dispuso un presupuesto económico para esta propuesta.

Adquisición, desarrollo y mantenimiento de los sistemas de información.

Para este dominio se adquirieron nuevos elementos para distintas áreas que requerían renovación tecnológica, como es la adquisición de un switch Cisco de 24 puertos y un equipo firewall.

Relaciones con proveedores.

En este dominio se establecieron directrices que se deben considerar al momento de gestionar la prestación de servicios por suministradores, empresas contratistas o terceras personas.

Aspectos de seguridad de la información en la gestión de la continuidad de negocio.

El dominio fue respaldado mediante el establecimiento de un plan de emergencia, un plan de recuperación, un plan de restauración, evaluación y pruebas, y un plan de

mantenimiento que nos garantizan la continuidad de la seguridad de la información.

Cumplimiento.

Para este dominio se dejan directrices que ayuden en el cumplimiento de este proyecto, para lo cual Consejo Administrativo aprobó la documentación del Plan de Contingencia en el ACTA No 318 que se encuentra en el ANEXO R. Para dicha aprobación se realizó una defensa del proyecto ante los miembros del Consejo Directivo para explicar detalles y la forma en la que este Plan de Contingencia se debe poner en marcha. En la Figura 56 se observa el desarrollo de la defensa.

Figura 56: Defensa del Plan de Contingencia ante Consejo Directivo de la COAC Chuchuqui Ltda.

Fuente: Elaboración propia.

CAPÍTULO VI

COSTO BENEFICIO

En este capítulo se encuentran las cotizaciones de mano de obra y materiales, factibilidad Técnica-Económica, Análisis Costo-Beneficio, TIR, VAN, ROI, de los cuales se realiza el estudio de factibilidad partiendo de la noción de que el proyecto tiene como finalidad generar un valor de ahorro para la institución.

6.1. COTIZACIÓN DE MATERIALES Y MANO DE OBRA

Todas la cotizaciones y facturas se encuentran en el ANEXO N de este documento.

6.2. COSTOS DE MATERIALES A UTILIZAR EN LA IMPLEMENTACIÓN DE LOS CONTROLES DE SEGURIDAD EN BASE A LAS COTIZACIONES.

Se ha elaborado la Tabla 38 sobre los materiales a utilizar basados en los mejores precios y las mejores herramientas a utilizar en la implementación de controles de seguridad, se ha realizado con una proyección de 5 años, considerando que muchas de las tecnologías utilizadas pueden requerir ser modificadas.

Costo de materiales.

En el listado que se presenta en la Tabla 38, no se consideran en profundidad todos los materiales que se puedan emplear para la implementación del nuevo cableado estructurado ya que este proyecto requiere de un estudio minucioso que permita establecer de forma adecuada todos los elementos necesarios, por lo tanto, en este caso se ha establecido un presupuesto global en el que el Departamento Financiero está en la capacidad de invertir. En caso de que de este presupuesto exista un valor restante, el Departamento de Tecnología tendrá la capacidad de decidir en se lo puede emplear, con la finalidad de continuar con el mejoramiento de la seguridad de la información.

El presupuesto establecido por el área de contabilidad, para inversión en Departamento de Tecnología es de USD 45.000 de los cuales se destinará un máximo de USD 40.000 para el mejoramiento del cableado estructurado y modificación de la topología de red. Y los USD 5.000 restantes serán destinados para la capacitación del personal de Tecnología en temas referentes a la seguridad de la información. Para

constancia de este presupuesto en el ANEXO O se encuentra un certificado emitido por la contadora general de la COAC Chuchuqui Ltda.

Tabla 38: *Materiales a utilizar en la implementación de controles de seguridad.*

DETALLE	COST. UNIDAD	CANT	TOTAL
Rack de pared de 9 UR marca connection	151,54	1	151,54
Rack de pared de 6 UR marca connection	206,28	1	206,28
Lectora de huella digital para interior con proximidad SOYAL AR-837	585	1	585,00
Sistema de respaldo en caso de pérdida de energía AC	150	1	150,00
Tarjetas de proximidad	4,5	10	45,00
Puerta de seguridad para cuarto de comunicación	1997	1	1997,00
Sistema de aire acondicionado tipo Split pared marca LIBERO-LG/ECOX 24000 BTU/h.	2678	1	2678,00
Pintura blanca para Data Center	180	1	180,00
Patch Panel Modular marca nexxt cat. 6A	155	1	155,00
Switch Modelo WSC-fpdl Catalyst Serie 2960-x 48puertos	2980,07	1	2980,07
Firewall 1470 Next Generation Threat Prevention Appliance, Wired, including 3 years of services and Direct Standard support	3260,23	1	3260,23
Instalación, configuración y transferencia de conocimientos de Firewall 1470 Next Generation Threat Prevention Appliance.	840,00	1	840,00
Windows 7 Profesional SPI 64-Bits Español	175	1	175,00
Disco duro 4TB externo WD My Book USB 3.0	255	1	255,00
Copiadora Impresora MPC 4502 MPC 5502	2105,26	2	4210,52
Regulador de Voltaje	114,04	2	228,08
Cableado Estructurado	35087,72	1	35087,72
Capacitaciones del personal de Tecnología	4385,97	1	4385,97
		Subtotal	57570,41
		IVA 14%	7270,96
		IVA 12%	676,20
		TOTAL	**65517,56**

Fuente: ANEXO N: COTIZACIONES Y FACTURAS

Costo de mano de obra.

El costo de mano de obra se basa en el valor establecido por los técnicos para la implementación de los controles de seguridad, también se incluye la mano de obra de un profesional para el mantenimiento del Plan de Contingencia y de la seguridad de la información en sí, en vista de que después del análisis de las funciones de los integrantes del Departamento de Tecnología se llega a la conclusión de que es necesario tener la consideración de incrementar el personal en esta área. Con estas consideraciones, en la Tabla 39 se muestra el listado del costo de mano de obra.

Tabla 39: *Costo de mano de obra.*

Costo de Mano de Obra			
Personal	Número de personas	Mensual o Costo de Obra	Total
Técnico de instalación de control de acceso	1	190,00	190,00
Técnico en posicionamiento de puerta, soldadura eléctrica, nivelación y obra civil	3	150,00	450,00
Técnico en seguridad de redes	1	1200,00	1200,00
		Total	**2440,00**

Fuente: ANEXO N y Departamento de Recursos Humanos de la COAC Chuchuqui Ltda.

6.3. ANÁLISIS ECONÓMICO

Para el análisis económico se debe considerar que la finalidad de este proyecto es mejorar la calidad de servicio y alcanzar un factor de ahorro para la institución en un transcurso de 5 años, aunque este proyecto puede tener valor por un periodo mayor la recomendación para este tipo de organizaciones financieras es actualizar en lo posible los controles de seguridad de la información.

Tabla 40: *Cálculo del valor de talento humano dependiendo del número de horas para cada tipo de impacto.*

CÁLCULO DEL VALOR DE TALENTO HUMANO SEGÚN EL TIPO DE IMPACTO										
			IMPACTO							
			CRÍTICO		ALTO		MEDIO		BAJO	
Funcionarios involucrados	Cantidad	Remuneración	Horas	Valor	Horas	Valor	Horas	Valor	Horas	Valor
Gerente	1	5200,00	10	325,00	7	227,50	4	130,00	1	32,50
Jefe administrativo	1	1750,00	30	328,13	10	109,38	6	65,63	2	21,88
Jefe de sistemas	1	1800,00	40	450,00	16	180,00	8	90,00	4	45,00
Asistente de sistemas	1	1600,00	40	400,00	16	160,00	8	80,00	4	40,00
Supervisor de cajas	1	1200,00	10	75,00	4	30,00	2	15,00	1	7,50
Cajero	2	750,00	10	46,88	4	18,75	2	9,38	1	4,69
				1625,00		**725,63**		**390,00**		**151,56**

Fuente: Departamento de Recursos Humanos de la COAC Chuchuqui Ltda.

Para determinar el factor ahorro del proyecto se lo realiza en base a los tipos de impactos establecidos previamente y la frecuencia con la que estos se presentan. Para cada tipo riesgo se determina un valor aproximado requerido para dar una solución, considerando los requerimientos de talento humano, equipos, infraestructura, sistemas y financieros como se muestra en la Tabla 41.

Para poder calcular el valor del parámetro de talento humano, primeramente, debemos calcular su valor según el número de horas que tardaría dar solución a una eventualidad según su impacto, dependiendo de la remuneración que recibe cada funcionario involucrado en el procedimiento de restitución, como se muestra en la Tabla 40, considerando el caso de que los funcionarios deban cumplir con horas extras, por lo que su valor incrementaría en un 50%.

Tabla 41: Coste total de restitución según el tipo de impacto.

IMPACTO	Parámetro	COSTE	FRECUENCIA
IMPACTO CRÍTICO	Talento humano	1.625,00	1 cada 2 años
	Equipos	10.000,00	
	Infraestructura	5.000,00	
	Sistemas	30.000,00	
	Financiera	3.472,22	
	Total	**50.097,22**	
IMPACTO ALTO	Talento humano	725,63	1 cada año
	Equipos	7.000,00	
	Sistema	15.000,00	
	Total	**22.725,63**	
IMPACTO MEDIO	Talento humano	390,00	3 cada año
	Equipos	30.000,00	
	Sistemas	5.000,00	
	Total	**35.390,00**	
IMPACTO BAJO	Talento humano	151,56	5 cada año
	Sistemas	2.000,00	
	Total	**2.151,56**	

Fuente: Departamento de Tecnología y Departamento de Recursos Humanos de la COAC Chuchuqui Ltda.

En base a la frecuencia con la que se presenta cada tipo de impacto, se calcula la valoración total de los impactos por año como se indica en la Tabla.

Tabla 42: *Valoración total de los impactos al año.*

VALORACIÓN TOTAL DE LOS IMPACTOS AL AÑO			
IMPACTO	FRECUENCIA	COSTO	TOTAL
CRÍTICO	0,50	46.916,67	23.458,33
ALTO	1,00	22.725,63	22.725,63
MEDIO	3,00	8.390,00	25.170,00
BAJO	5,00	2.151,56	10.757,81
		TOTAL	**82.111,77**

Fuente: Elaboración propia.

Para que el proyecto se mantenga vigente se requiere un mantenimiento periódico, para lo cual se debe determinar los costos requeridos. Para este caso se considera la necesidad de contar con un técnico en seguridad de redes, para lo cual se ha determinado que la remuneración para este cargo será de USD 1.200 a lo cual se le añade los beneficios de ley, por lo cual, para obtener el valor anual se multiplica el valor de la remuneración por 14,5. Con esta consideración en la Tabla 43 se realiza el cálculo total del costo de mantenimiento del Plan de Contingencia.

Tabla 43: *Costos de mantenimiento del Plan de Contingencia.*

COSTOS DE MANTENIMIENTO DEL PLAN DE CONTINGENCIA	
Técnico en seguridad informática	17.400,00
Capacitación	3.000,00
Materiales de contingencia	5.000,00
Auditorias	3.500,00
Mantenimiento equipos	800,00
TOTAL	**29.700,00**

Fuente: Departamento de Tecnología y Departamento Financiero de la COAC Chuchuqui Ltda.

La implementación del Plan de Contingencia tiene como finalidad la reducción de la frecuencia con la que se presenta cada tipo de impactos para lo cual en la Tabla se

muestra una estimación de la concurrencia esperada.

Tabla 44: *Estimación de la frecuencia de los impactos con la implementación del Plan de Contingencia.*

IMPACTO	FRECUENCIA
CRÍTICO	1 CADA 5 AÑOS
ALTO	1 CADA 4 AÑOS
MEDIO	1 CADA AÑO
BAJO	2 CADA AÑO

Fuente: Elaboración propia.

Una vez establecido la frecuencia estimada de los impactos con el Plan de Contingencia implementado, se calcula los costos totales que se tendrá cada año como se indica en la Tabla 45.

Tabla 45: *Costos totales con la implementación del Plan de Contingencia.*

COSTOS TOTALES CON LA IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA AL AÑO			
IMPACTO	FRECUENCIA	VALOR	TOTAL
Crítico	0,20	46.916,67	9.383,33
Alto	0,25	22.725,63	5.681,41
Medio	1,00	8.390,00	8.390,00
Bajo	2,00	2.151,56	4.303,13
Costos de mantenimiento	1,00	29.700,00	29.700,00
		TOTAL	**57.457,86**

Fuente: Elaboración propia.

Con los datos obtenidos anteriormente se puede calcular el ahorro anual con la implementación del Plan de Contingencia. Este cálculo se lo realzará para un lapso de 5 años como se puede observar en la Tabla 46.

Tabla 46: *Ahorro con la implementación del Plan de Contingencia.*

	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Costo de los impactos sin el Plan de Contingencia	82.111,77	84.164,57	86.268,68	88.425,40	90.636,03
Costos totales con la implementación del Plan de Contingencia	57.457,86	58.894,31	60.366,67	61.875,84	63.422,73
AHORRO	**24.653,91**	**25.270,25**	**25.902,01**	**26.549,56**	**27.213,30**

Fuente: Elaboración propia.

Para los cálculos de a continuación se requiere conocer de los parámetros de costos que se muestran en la Tabla 47, donde la inversión es el resultado de la suma del costo de los materiales utilizados y el costo de la mano de obra para la implementación del Plan de Contingencia.

Tabla 47: *Parámetros de costos.*

INVERSIÓN	66.157,56
INFLACIÓN	0,025
TMAR	13%
T. REINVERSIÓN	8%

Fuente: Elaboración propia.

Eficiencia neta actualizada

La eficiencia neta actualizada muestra la disminución del valor económico de la eficiencia por año debido a la devaluación de los sistemas. Esto se realiza en base a la tasa de inversión de descuento y de reinversión. Se toma en cuenta la inversión inicial que son todos los costos de mano de obra y los costos de los materiales necesarios para la implementación del Plan de Contingencia. En la Ecuación 1 se indica el cálculo de la eficiencia neta actualiza. (John D, 2000)

$$Eficiencia\ Neta\ actualizada = \frac{Eficiencia\ Neta}{(1+i)^n} - Inversión \qquad \textbf{(1)}$$

En la Tabla 48 se encuentran los flujos operativos de ahorro, donde se realiza el cálculo de la eficiencia neta actualizada en un lapso de 5 años, lo que permite determinar

el periodo de retorno de reinversión (PRRI).

Tabla 48: *Flujos operativos (ahorro)*

FLUJOS OPERATIVOS (AHORRO)			
		EFICIENCIA NETA ACTUALIZADA	PRRI
INVERSIÓN	-66157,5617		
AÑO 1	24.653,91	21.817,62	44.339,95
AÑO 2	25.270,25	19.790,32	24.549,63
AÑO 3	25.902,01	17.951,39	6.598,24
AÑO 4	26.549,56	16.283,34	-
AÑO 5	27.213,30	14.770,29	-
	Total	**90.612,96**	-

Fuente: Elaboración propia.

De la Tabla 48, transformando los datos a días, años y meses aplicando la regla de tres, se obtiene que el PRRI es de 3 años, 4 meses y 26 días.

VAN, TIR, ROI

El VAN muestra le valor económico que se ha logrado ahorrar en función del tiempo transcurrido, y del cual se reducen los valores económicos por concepto de mantenimiento.

La TIR muestra el porcentaje de la tasa interna de retorno realizada en base al tiempo y los costos generados. Se utilizan como datos la eficiencia neta actualizada, la inversión, la tasa de inversión de descuento y la tasa de reinversión. (Guzmán, 2004)

El ROI es el valor operativo en función del ahorro, los valores por encima del 30% en proyectos de empresas que no tienen fines de lucro son comunes y demuestran su eficiencia ante sistemas actuales. En la Ecuación 2 se indica el cálculo del Valor Actual Neto (VAN). (John D, 2000)

$$VAN = Eficiencia\ Neta\ actualizada - Inversión \qquad \textbf{(2)}$$

En la Ecuación 3 se indica el cálculo de la TIR. *(John D, 2000)*

$$TIR = -Io + \sum_1^n \frac{Ef\ Neta\ actualizada}{(1+i)^n} \qquad \textbf{(3)}$$

Donde, Io se refiere a la inversión inicial, n es el número de periodo en años e i hace referencia al interés.

En la Ecuación 4 se indica el cálculo del ROI. (John D, 2000)

$$ROI = \frac{Eficiencia\ neta - Costos\ del\ sistema}{Costos\ del\ sistema} \qquad \textbf{(4)}$$

En la Ecuación 5 se indica el cálculo de la relación costo beneficio. *(John D, 2000)*

$$R\ B/C = \frac{VAN}{Io} \qquad \textbf{(5)}$$

Desarrollando las ecuaciones obtenemos los valores mostrados en la Tabla 49, de donde se puede proporcionar un análisis de factibilidad económica del proyecto.

Tabla 49: *Cálculo de VAN, TIR, ROI y R B/C*

VAN	24.455,39
TIR	18,02%
ROI	37%
R B/C	0,37

Fuente: Elaboración propia.

6.4. ANÁLISIS DE FACTIBILIDAD ECONÓMICA

La eficiencia del Plan de Contingencia se basa el porcentaje de disponibilidad de los servicios, ya que según la información contable la COAC Chuchuqui Ltda., estaría perdiendo un promedio de USD 3.472,22 por cada hora que no se presten los servicios financieros. Puesto que el Plan de Contingencia busca incrementar la disponibilidad y según los indicadores financieros se puede deducir lo siguiente:

- El VAN indica que con el Plan de Contingencia se puede conseguir un ahorro de USD 24.455,39 en el transcurso de 5 años, lo que significa que el proyecto si es viable.

- La TIR muestra un retorno de inversión del 18,02%, el cual es más alto que

algunos proyectos lucrativos, pero que en nuestro caso nos indica un beneficio contabilizado en un porcentaje de ahorro.

- El ROI tiene un valor de 37% el cual es aceptable, ya que los proyectos no lucrativos por lo general se encuentran sobre el 30%, pero esto indica cuan viable es el implementar el proyecto puesto que el ahorro está superando a la inversión y muestra el beneficio operativo del Plan de Contingencia del 37% superior al estado actual en el que se encuentra la institución.

- La relación del costo beneficio indica que por cada dólar invertido en el proyecto se estaría recuperando USD 1,37, por lo que queda demostrado de que es viable la implementación del proyecto.

CONCLUSIONES

- Se implementó y aprobó un plan de contingencia por el Consejo Directivo de la cooperativa de ahorro y crédito de indígenas Chuchuqui Ltda., basándose en la norma ISO/IEC 27002 logrando mejorar los aspectos de confidencialidad, integridad y disponibilidad de la red mediante la implementación de controles de seguridad.

- Se analizó la información sobre la norma ISO/IEC 27002 referente a controles de seguridad, de la cual se alineó dichos controles a las necesidades de la COAC Chuchuqui Ltda., descartando varios de ellos debido a que no se relacionaban a las actividades que se realizan en esta institución.

- Se realizó un análisis de la situación actual mediante el levantamiento de información sobre los controles de seguridad implementados en la COAC Chuchuqui Ltda. y clasificándolos como fortalezas, oportunidades, debilidades y amenazas, lo que permitió dar partida al desarrollo del Plan de Contingencia.

- Se dio respuesta a varios de los problemas encontrados en el análisis de la situación actual, mediante el desarrollo de un análisis de riesgos, un plan de emergencia, un plan de restauración, un plan de recuperación, pruebas de verificación y un plan de mantenimiento, mejorando e implementando

medidas de protección a nivel de Software y Hardware.

- La realización de pruebas de evaluación se las realizó bajo la supervisión de los miembros del Departamento de Tecnología de la COAC Chuchuqui Ltda., las cuales se cumplieron con los requerimientos necesarios obteniendo resultados positivos, lo que demostró que la implementación del plan de contingencia se realizó de forma adecuada.

- Se determinó que el proyecto si es viable según los resultados del análisis de factibilidad económica, el ROI indica que hay un buen desempeño técnico-económico, la rentabilidad económica se muestra con el cálculo del VAN, la relación costo beneficio nos indica que por cada dólar invertido se recupera USD 1,37, llegando a la conclusión de que existe un ahorro para la cooperativa a partir de los 3 años 4 meses y 26 días.

- El realizar el trabajo de grado en la COAC Chuchuqui Ltda., ha sido una experiencia satisfactoria que permitió demostrar los conocimientos adquiridos en clase logrando impartir confianza con los miembros de la institución, además de permitir tener una perspectiva más clara sobre las responsabilidades profesionales que en las instituciones financieras se imponen.

RECOMENDACIONES

- Se recomienda a la COAC Chuchuqui Ltda., considerar la incorporación de una nueva área perteneciente al departamento de tecnología con un profesional en redes de comunicación (Administrador de la red de datos), cuyas capacidades ayuden a cumplir con las tareas relacionadas a la seguridad de información y administración de la red de datos.

- Hacer de conocimiento general el contenido del presente Plan de Contingencia, con la finalidad de instruir adecuadamente al personal de la Cooperativa de Ahorro y Crédito “CHUCHUQUI” Ltda., es deber de la gerencia manifestar su apoyo y compromiso a la seguridad de la información, exigiendo el cumplimiento de las políticas de seguridad que se devuelven a partir de este Plan.

- Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que alteren el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la Cooperativa de Ahorro y Crédito "CHUCHUQUI" Ltda.

- Realizar reuniones periódicas con el personal de tecnología para tratar temas respecto a la seguridad de la información y la comprobación del cumplimiento de las políticas, normas y plan de contingencia establecidos en la institución.

- Se recomienda extender el sistema de monitoreo hacia los equipos de comunicación que se encuentran en cuarto de comunicaciones y rack de cada piso de la institución, como son los switches y routers, ya que estos elementos también son de gran importancia para el correcto desempeño de la red.

- Se recomienda a la Universidad Técnica del Norte mantener la relación con la COAC Chuchuqui Ltda., permitiendo que los estudiantes puedan realizar sus trabajos de grado o prácticas pre-profesionales en esta institución, ya que cuenta con diversos tipos de proyectos en los que se puede aplicar los conocimientos adquiridos en las aulas.

REFERENCIAS BIBLIOGRÁFICAS

Alegre Ramos, M., & García Hurtado, A. (2011). Razones para la seguridad de la información. En *Seguridad informática Ed.11 Paraninfo* (págs. 2-11). Madrid: Paraninfo.

ANSI/TIA. (2012). *Telecommunications Pathways and Spaces.* Arlington.

Castillo, I. G., & Medina, I. M. (2014). *Manual de Practiacas ara la asignatura de seguridad informática.* México.

COAC Chuchuqui Ltda. (Septiembre de 2016). *COAC Chuchuqui.* Obtenido de http://www.coopchuchuqui.fin.ec/

Cruz, L. C. (Septiembre de 2012). *Documento de estado del arte.* Obtenido de http://1984.lsi.us.es/pfe/trac/pfe-pandora/raw-attachment/wiki/WikiStart/3-Doc.Estado%20del%20Arte.pdf

Giraldo Martínez, I. K., De la Torre Morales, M. E., & Villalta Gómez, C. A. (2012). *Dignóstico para la Implantación de COBIT en una Empresa de Producción.* Guayaquil.

Guzmán, C. G. (2004). *Introducción a la Ingeniería Económica.* Bogotá: Faculta de Ingeniería.

Instituto Veracruzano de acceso a la información. (2012). *Plan de contingencia informático.* Veracruz.

ISO. (Octubre de 2013). *El portal de ISO 27001 en Español*. Obtenido de http://www.iso27000.es/iso27002_5.html

ISO/IEC 27002. (2013). *Tecnología de la información - Técnicas de seguridad - Código de prácticas para la gestión de la seguridad de la información.* Geneva: ISO copyright office.

IT Governance Institute. (2007). *COBIT (Control Objetives for Information and related Technology).* Rolling Meadows: Algonquin Road.

John D, F. &. (2000). *Fundamentos de Administración Financiera.* Pearson Eduaction.

Lazzari, L. L. (2006). Control de gestión: una posibleaplicación del análisis foda. Buenos Aires: Red Cuaderno CIBAGE.

NTC/ISO/IEC 27005. (2008). *Técnicas de seguridad: Gestión de riesgos para la seguridad de la información.* Pereira: Aseuc.

Office of Government Commerce . (2010). *Operación del servicio.* Londres: TSO.

Office of Government Commerce. (2010). *Operación del servicio.* Londres: TSO.

Orlich, J. M. (2013). *Universidad para la Cooperación Internacional.* Obtenido de http://www.uci.ac.cr/descargas/AE/FODA(SWOT).pdf

Ormella, C. (16 de Enero de 2014). *Criptografía y Seguridad de la Información: Nuevas versiones de las normas ISO 27001 e ISO 27002.* Obtenido de http://www.criptored.upm.es/descarga/NuevasVersionesISO27001eISO27002.pdf

Red Hat Enterprise Linux. (2013). *Manual de referencia: Protocolo SSH*. Obtenido de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html

Ríos, S. (2014). *B-able.* Obtenido de http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf

Secretaría general de gestión de riesgos. (2010). *Gestión de riesgos: Plan de emergencia institucional.* Obtenido de http://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2012/07/Plan_de_Emergencia_Institucional.pdf

SEPS. (2012). *REGLAMENTO A LA LEY ORGÁNICA DE LA ECONOMÍA POPULAR Y SOLIDARIA.* Quito.

SEPS. (2014). *OFICIO CIRCULAR No. SEPS-IR-DNRFPS-2015.* Quito.

SEPS. (2015). *Super Intendencia de Economía Popular y Solidaria*. Obtenido de http://www.seps.gob.ec/interna?-que-es-la-seps-

Tejada, E. C. (2015). *Auditoría de seguridad informática. IFCT0109.* Málaga: IC Editorial.

GLOSARIO

COAC.- Cooperativa de Ahorro y Crédito

SEPS.- Superintendencia de Economía Popular y Solidaria

ISO/IEC.- Son siglas de organizaciones ISO (Organización Internacional para la Normalización) e IEC (Comisión Electrotécnica Internacional) que regulan, controlan y colaborar en los campos de la seguridad de la información.

NTC/ISO.- Son siglas de organizaciones NTC (Norma Técnica Colombiana) y ISO (Organización Internacional para la Normalización).

ITIL.- Information Technology Infrastructure Library, Biblioteca de Infraestructura de Tecnologías de Información.

COBIT.- Control Objectives for Information and related Technology, Objetivos de Control para Información y Tecnologías Relacionadas.

CCTA.- Central Computer and Telecomunications Agency, Agencia Central de Informática y Telecomunicaciones.

ISACA.- Information Systems Audit and Control Association, Asociación para la Auditoría y Control de sistemas de información.

FODA.- Metodología para el levantamiento de información para el estudio de la situación actual de sus siglas: Fortalezas, Oportunidades, Debilidades y Amenazas.

CNT EP.- Corporación Nacional de Telecomunicaciones Empresa Pública.

PYMES.- Pequeñas y Medianas Empresas.

TI.- Tecnologías de la Información.

UPS.- Uninterruptible Power Supply, Fuente de Poder Ininterrumpible.

WEBCOOP.- Sistema informático para instituciones financieras.

BACKUP.- Copias de seguridad o copia de respaldo de información.

TOPOLOGÍA FÍSICA.- Es la forma en la que se organizan los equipos terminales y equipos activos dentro de una red, las topologías conocidas son en malla, anillo, estrella, bus, estrella extendida, y redes híbridas.

TICs.- Tecnologías de la Información y Comunicaciones.

SGSI.- Sistema de Gestión de la Seguridad de la Información.

SADFIN.- Sistema de Administración Financiera y Contabilidad.

ZENTYAL.- Zentyal Server es un servidor Linux fácil de usar, que es nativamente compatible con Microsoft Active Directory y Zentyal también es una solución de correo electrónico y groupware de código abierto, compatible de forma nativa con Microsoft Outlook.

CMDB.- Change Management Data Base, Base de Datos de Gestión de Cambios

RACK.- Es una estructura metálica que sirve para organizar equipos activos de comunicación, cables, equipos de conexión e interconexión

PATCH PANEL.- Panel de conexiones, es un panel de múltiples puertos que facilita la interconexión de cables, además de evitar el desgaste en los puertos de los equipos principales debido a la conexión y desconexión física.

SSH.- Conexión segura que permite accesos remotos entre equipos activos de la red, mediante uso de claves encriptadas y comunicación ip.

VAN.- procedimiento que permite calcular el valor presente de un determinado número de flujos de caja futuros, originados por una inversión

TIR.- interés en el que el VAN se hace cero. Si el TIR es alto, el proyecto rentable, que supone un retorno de la inversión.

ROI.- es la herramienta económica que compara el beneficio o la utilidad obtenida en relación a la inversión realizada.

MAGERIT.- es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos.

ANEXOS

ANEXO A: FORMATO PARA LEVANTAMIENTO DE INFORMACIÓN DE CONTROLES DE SEGURIDAD

<table>
<tr><td colspan="2">CONTROL:</td><td colspan="2"></td></tr>
<tr><td colspan="4">Descripción:</td></tr>
<tr><td rowspan="2">Estado</td><td>Aplicado</td><td>Se puede mejorar</td><td>No Aplicado</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="4">Clasificado como:</td></tr>
<tr><td>Fortaleza</td><td>Oportunidad</td><td>Debilidad</td><td>Amenaza</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Requerimientos de seguridad Implicados</td></tr>
<tr><td>Integridad</td><td>Confidencialidad</td><td>Disponibilidad</td><td>Otros</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Observaciones:</td></tr>
</table>

ANEXO B: LEVANTAMIENTO DE INFORMACIÓN DE CONTROLES DE SEGURIDAD

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

CONTROL:	Políticas de Seguridad		
Descripción:	Las políticas de Seguridad son documentos en los que se publican de manera formal por parte del comité administrativo de la institución instrucciones globales, para su respectivo cumplimiento en todas las áreas que se crea necesario.		
Estado	Aplicado	Se puede mejorar	No Aplicado
		X	
Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
	X		
Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
X	X		Calidad de Servicio
Observaciones:	Existen características de la seguridad de la información que no se encuentran respaldadas por una política de seguridad y en otros casos la información no se encuentra actualizada.		

CONTROL:	Aspectos organizativos de la seguridad de la información		
Descripción:	Este control tiene la finalidad de incluir dentro de los procesos de servicios de la institución, la seguridad de la información. Uno de estos aspectos es el establecer responsabilidades y funciones que ayuden a mejorar el servicio basado en la seguridad de la información.		
Estado	Aplicado	Se puede mejorar	No Aplicado
		X	
Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
	X		
Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
X		X	
Observaciones:	Dentro del contrato de los empleados existen funciones establecidas pero pocas están referidas a colaborar con la seguridad de la información.		

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

CONTROL:	Contacto con las autoridades

Descripción: Se debe establecer contactos apropiados con las autoridades correspondientes a la zona donde se encuentra la institución, en esta lista se incluyen los números de emergencia.

Estado	Aplicado	Se puede mejorar	No Aplicado
		X	

Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
	X		

Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
		X	

Observaciones: La institución cuenta con los números de contactos con autoridades, pero no se encuentran en una lista de acceso rápido.

CONTROL:	Contacto con grupos de interés especial

Descripción: Se debe contemplar una lista de contactos con grupos, foros, empresas o instituciones especializados en la seguridad informática

Estado	Aplicado	Se puede mejorar	No Aplicado
		X	

Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
	X		

Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
		X	

Observaciones: La institución cuenta con tarjetas de contacto de grupos de interés especial pero no se encuentran plasmados en una lista de acceso rápido.

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

CONTROL:	Uso de dispositivos para movilidad

Descripción: Se debe tener cuidado al usar dispositivos móviles en lugares públicos, salas y otras áreas de reuniones no protegidas.

Estado	Aplicado	Se puede mejorar	No Aplicado
	X		

Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
X			

Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
X	X		

Observaciones: La institución tiene una política para el uso de dispositivos para movilidad, junto con un plan de escaneo de virus de los mismos.

CONTROL:	Teletrabajo

Descripción: Teletrabajo se refiere al uso de dispositivos de institución fuera de la infraestructura, para tareas delegados. Estos dispositivos no deben contener información importante para la organización.

Estado	Aplicado	Se puede mejorar	No Aplicado
	X		

Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
X			

Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
X	X		

Observaciones: La institución tiene restringido la salida de dispositivos perteneciente a la organización, debido al tipo de actividades que desempeñan.

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

CONTROL:	Investigación de antecedentes.

Descripción: Se debe realizar controles de verificación a fondo sobre todos los candidatos para el empleo y contratistas; pero esto se debe llevar a cabo de acuerdo con las leyes, regulaciones y ética pertinente.

Estado	Aplicado	Se puede mejorar	No Aplicado
	X		

Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
X			

Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
X	X		

Observaciones: La institución cuenta con un plan de contratación adecuado para la verificación de la información de los candidatos y una prueba para calificar la capacidad del personal.

CONTROL:	Términos y condiciones de contratación.

Descripción: Como parte de sus obligaciones contractuales, empleados y contratistas deben estar de acuerdo y firmar los términos y obligaciones de su contrato de trabajo.

Estado	Aplicado	Se puede mejorar	No Aplicado
	X		

Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
X			

Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
X	X		

Observaciones: La institución cuenta con un plan de términos y condiciones de contratación adecuados para la seguridad de la información.

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

CONTROL:	Responsabilidades de gestión

Descripción: La administración debe exigir a los empleados y contratistas, la aplicación de políticas y procedimientos de seguridad.

Estado	Aplicado	Se puede mejorar	No Aplicado
	X		

Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
X			

Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
			Disponibilidad, orden

Observaciones: La institución cuenta con un departamento de cumplimiento que se encarga de la gestión basados en un Reglamento interno.

CONTROL:	Concienciación, educación y capacitación en S.I.

Descripción: Todos los empleados de la institución y en su caso contratistas y usuarios pertinentes, deben recibir una formación adecuada sobre la sensibilización y actualizaciones en las políticas y procedimientos de la institución.

Estado	Aplicado	Se puede mejorar	No Aplicado
			X

Clasificado como:			
Fortaleza	Oportunidad	Debilidad	Amenaza
		X	

Requerimientos de seguridad Implicados			
Integridad	Confidencialidad	Disponibilidad	Otros
X	X		

Observaciones: La institución carece de capacitaciones sobre la importancia de la seguridad de la información.

ANEXO C: TIPOS DE AMENAZAS

Tipo	Amenazas
Daño físico	Fuego
	Daño por agua
	Contaminación
	Accidente importante
	Destrucción del equipo o los medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado
	Pérdida de suministro de energía
	Falla en el equipo de telecomunicaciones
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia comprometedoras
	Espionaje remoto
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Falla del equipo
	Mal funcionamiento de equipo

	Saturación del sistema de información
	Mal funcionamiento de software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de datos
	Procesamiento ilegal de los datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal
Pirata informático, intruso ilegal	Piratería
	Ingeniería social
	Intrusión, accesos forzados al sistema
	Acceso no autorizado al sistema
Terrorismo	Bomba/terrorismo
	Guerra de información
	Ataques contra el sistema (por ejemplo, negación distribuida del servicio)
	Penetración en el sistema
	Manipulación del sistema

ANEXO D: TIPOS DE VULNERABILIDADES

Tipos	Ejemplos de vulnerabilidades
Hardware	Mantenimiento insuficiente o instalación fallida de los medios de almacenamiento
	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad.
	Sensibilidad a la radiación electromagnética
	Falta de control de cambio con configuración eficiente
	Susceptibilidad a las variaciones de tensión
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Falta o insuficiencia de la prueba de software
	Defectos bien conocidos en el software
	Falta de la terminación de la sesión cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Falta de pruebas de auditoría
	Distribución errada de los derechos de acceso
	Software de distribución amplia
	Utilización de los programas de aplicación a los datos errados en términos de tiempo
	Interface de usuario complicada
	Falta de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Falta de mecanismos de identificación y autenticación, como la autenticación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de contraseñas
	Habilitación de servicios innecesarios

	Falta de control eficaz del cambio
	Descarga y uso no controlado del software
	Falta de copias de respaldo
Red	Falta de prueba del envío o la recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de falla
	Falta de identificación y autenticación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas autorizadas
	Conexiones de red pública sin protección
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad
	Falta de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos
	Ubicación en un área susceptible de inundación
	Red energética inestable
	Falta de protección física de las puertas y ventanas de la edificación

ANEXO E: LISTA DE TELÉFONOS DE EMERGENCIA

Lista Teléfonos de Emergencia	
CUERPO DE BOMBEROS	**(06)2920-102**
CRUZ ROJA	**(06)2950-888**
HOSPITAL SAN LUIS DE OTAVALO	**(06)2920-444**
HOSPITAL IESS	**(06)2920-428**
SECRETARIA DE GESTION DE	**(06)2953-580**
ECU 911	**911**
POLICIA NACIONAL	**(06)2923-219**

ANEXO F: FORMATO DE RECEPCIÓN Y REGISTRO DE INCIDENCIA

RECEPCIÓN Y REGISTRO DE INCIDENCIA	
Incidencia No	
Categorización de incidencia	
Urgencia de incidencia	
Impactos de incidencia	
Prioridad de incidencia	
Fecha y hora de registro	
Nombre/Cargo de la persona que registra el incidente	
Método de notificación	

Descripción de síntomas del incidente	
Estado de la incidencia (activa, en espera, cerrada, etc.)	
Grupo/persona de soporte para este tipo de incidencia	
Problema asociado/Error conocido	
Acciones o procedimiento que se ha realizado para dar solución a la incidencia	
Fecha y hora de resolución	
Categoría de cierre	
Fecha y hora de cierre	

ANEXO G: FORMATO PARA PRUEBAS Y EVALUACIÓN

PLAN DE CONTINGENCIA DE TI – FORMATO PARA PRUEBAS Y EVALUACIÓN			
Prueba No:		Fecha:	
Escenario de Prueba:			
Responsables:	Nombre		Cargo
Hora de inicio		Hora de finalización	
Objetivo:			
Aspectos a evaluar:			
Requerimientos:			
Técnicas y Procedimiento:			

_____ _____ _____ _____ _____ _____ _____
Resultados: _____ _____ _____ _____ _____ _____ _____
Observaciones: _____ _____ _____ _____

Aprobado por:	Firma:

ANEXO H: DOCUMENTACIÓN DE PRUEBAS Y EVALUACIÓN

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

PLAN DE CONTINGENCIA DE TI – FORMATO PARA PRUEBAS Y EVALUACIÓN			
Prueba No:	1	Fecha:	21 de septiembre de 2016
Escenario de Prueba:	Daño o quemadura total del servidor financiero		
Responsables:	Nombre		Cargo
	Ing. Marcelo Yambería Ing. Darío Castañeda Sr. Dony Reina		Asistente de Tecnología Jefe de Tecnología Tesista
Hora de inicio	10:10 h	Hora de finalización	11:30 h

Objetivo:

Generar la continuidad del plan de negocio de la cosac Chuchuqui Ltda., a través de carga del respaldo del sistema financiero WEBCOOP.

Aspectos a evaluar:

Tiempo de respuesta para la continuidad del negocio

Requerimientos:

1) Red de comunicación habilitada 2) Energía eléctrica al 100% 3) Servidor de respaldo habilitado 4) Back up del sistema financiero ejecutado cada 15 días 5) Back up diario de la base de datos 5) Apoyo de Manual técnico de carga de backups y herramientas software

Técnicas y Procedimiento:

1.- Sacar el respaldo del sistema financiero actual. (10 min. y 44 seg.)
2.- Carga del sistema financiero al servidor de respaldo. (8 min. y 50 seg.)
3.- Sacar el backup de la base de datos del sistema financiero. (23 seg)
4.- Carga del backup en el servidor de la base de datos. (51 min. y 24 seg.)
5.- Ajustes y corrección para la ejecución del sistema financiero. (2 min)
6.- Ajustes de la red de comunicación al sistema financiero (dirección IP). (1 min)

7.- Pruebas del funcionamiento. (5 min)

8.- Ejecución de las actividades en el nuevo servidor del sistema financiero. (inmediato)

Resultados:

Se implementó el sistema financiero de respaldo a la fecha calendario con ejecución y desarrollo normal del sistema para la continuidad del plan de negocios de la COAC.

El tiempo de respuesta total se dio en un aproximado de 1h 20 min, el cual no se encuentra dentro del tiempo aceptable de caída del servicio.

Observaciones:

El tiempo de recuperación está elevado, en comparación a pruebas anteriores realizadas en el servidor de producción del sistema financiero WEBCOOP, por lo cual se recomienda analizar los recursos del servidor de respaldo para tratar de reducir los tiempos de respuesta.

Aprobado por: DARIO CASTAÑEDA

Firma:

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

PLAN DE CONTINGENCIA DE TI – FORMATO PARA PRUEBAS Y EVALUACIÓN			
Prueba No:	2	Fecha:	22 de Septiembre de 2016
Escenario de Prueba:	Indisponibilidad de energía eléctrica		
Responsables:	Nombre		Cargo
	Ing. Dario Castañeda Ing. Marcelo Yambela Sr. Dony Reina		Jefe de Tecnología Asistente de Tecnología Tesista
Hora de inicio	08:22	Hora de finalización	08:35

Objetivo:

Recuperar la continuidad del plan de negocio de la COAC Chuchuqui Ltda. en un tiempo mínimo, para el escenario de indisponibilidad eléctrica.

Aspectos a evaluar:

Tiempo que demora el encendido del generador eléctrico
Tiempo de disponibilidad del sistema biométrico del data center

Requerimientos:

Generador eléctrico con suficiente combustible
Disponibilidad de UPS en el data center

Técnicas y Procedimiento:

1) Consulta mediante una llamada a la empresa eléctrica, sobre el tiempo que demora en volver el servicio. (2 min)
2) Revisión del generador eléctrico. (3 min)

3) Carga de combustible en el generador (3 min)

4) Si el tiempo de demora es corto dependiendo de la llamada, (máximo 10 min), se puede esperar a que vuelva; pero si el tiempo es superior, se procede a encender el generador. (5 min)

5) Si el tiempo de interrupción eléctrica es muy alto, hay que asegurarse que el combustible abastezca para todo ese tiempo, o si es necesario se debe adquirir más combustible.

Resultados:

Se recuperó la continuidad de negocio en un tiempo aproximado de 13 min, el cual esta dentro del tiempo aceptable de caída. La planta eléctrica puede abastecer a toda la institución. El UPS del data center mantuvo los equipos encendidos durante todo el proceso al igual que el biométrico de acceso al data center, estuvo siempre activo.

Observaciones:

Durante el tiempo que demoró en encender la planta eléctrica, el sistema de climatización del data center no estuvo en funcionamiento, ya que se alimenta de la red que se encuentra fuera del UPS. Los ventiladores de rack tampoco funcionaron por lo que se recomienda que estos se conecten directamente al UPS.

Aprobado por: DANIO CASTAÑEDA	Firma:

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

PLAN DE CONTINGENCIA DE TI - FORMATO PARA PRUEBAS Y EVALUACIÓN			
Prueba No:	3	Fecha:	23 de Septiembre del 2016
Escenario de Prueba:	Corte del servicio de internet		
Responsables:	Nombre		Cargo
	Ing. Darío Castañeda Ing. Marcelo Yamberla Sr. Dany Reina		Jefe de Tecnología Asistente de Tecnología Tesista
Hora de inicio	08:30 h	Hora de finalización	10:45 h

Objetivo:

Recuperar la continuidad del Plan de negocio de la COAC Chuchuqui Ltda., en un tiempo mínimo para el escenario del corte del servicio de internet.

Aspectos a evaluar:

- Tiempo de respuesta por parte de los suministradores del servicio
- Tiempo de respuesta para el cambio de un dispositivo en mal funcionamiento

Requerimientos:

- Lista de teléfonos de contactos de proveedores de servicios
- Disposición de materiales de contingencia.

Técnicas y Procedimiento:

1) Comunicación con los proveedores del servicio de internet (2 min)
2) Establecimiento del servicio por parte de los suministradores, según el reglamento institucional del proveedor (CNT), el tiempo máximo que ellos tratan de alcanzar

para dar solución es de 45 minutos, desde la hora que se realizó la llamada
3) Informar al personal sobre el tiempo aproximado de restablecimiento del servicio
4) Si el problema es por causa del mal funcionamiento de un dispositivo, se procede a identificar el elemento afectado (5 min)
5) Cambio del equipo afectado (7 min)
6) Pruebas de funcionamiento
7) Informar al personal sobre el restablecimiento del servicio.

Resultados:

- Para la consideración de respuesta por parte de los suministradores, se realizó una llamada de simulación al proveedor explicando que se trataba de un simulacro, para conocer detalles del tiempo que normalmente se tardan en dar solución. Tomando en cuenta estos aspectos se determina que el tiempo aproximado de recuperación es de 47 min.
- Para la consideración de falla de un dispositivo se tomó en cuenta que la CORE no dispone de todos los recursos de contingencia para este escenario por lo cual se añade un tiempo de adquisición de 2 a 3 horas. A pesar de este incremento de tiempo, para este escenario este tiempo se encuentra dentro del límite de aceptación (8 horas)

Observaciones:

Los tiempos que obtienen para este escenario, están sometidos a margenes de error, por lo que solo se establecen tiempos aproximados, esto se debe a que el tiempo de recuperación por parte de los suministradores puede variar, dependiendo de la gravedad del problema, pero aún así los tiempos aproximados se encuentran dentro del tiempo aceptable de caída (8 horas).

Aprobado por: DANIO CASTAÑEDA	Firma: [signature]

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

PLAN DE CONTINGENCIA DE TI – FORMATO PARA PRUEBAS Y EVALUACIÓN			
Prueba No:	4	Fecha:	23 de Septiembre del 2016
Escenario de Prueba:	Falla de equipo de comunicación (switch)		
Responsables:	Nombre		Cargo
	Ing. Dario Castañeda Ing. Marcelo Yambería Sr. Dony Reina		Jefe de Tecnología Asistente de Tecnología Tesista
Hora de inicio	11:00 h	Hora de finalización	

Objetivo:

Recuperar la continuidad del Plan de negocio de la COAC Chuchuqui Ltda., en un tiempo mínimo para el escenario de falla de un equipo de comunicación.

Aspectos a evaluar:

- Tiempo que demora realizar el cambio de un equipo de comunicación (switch)

Requerimientos:

- Mapa de red de la estructura institucional.
- Equipos de remplazo

Técnicas y Procedimiento:

1) Identificar las causas y el equipo de falla de la comunicación. (5min)
2) Análisis breve sobre si el equipo tiene solución o si es necesario cambiar de dispositivo.

3) Comprobar la existencia del equipo de remplazo, caso contrario realizar la adquisición del dispositivo (Si existe el tiempo es de 2 min y si no existe en la institución el tiempo es de 2 a 3 horas)
4) Desmontar el equipo defectuoso y montar el equipo nuevo. (3 min)
5) Cargar la configuración del equipo. (10 min)

Resultados:

- Se realizó la simulación con la falla de un switch, donde la institución no cuenta con la existencia de un switch de remplazo, por lo que se suma el tiempo aproximado de adquisición.
- No existen archivos de configuración preparados para los dispositivos de red, por lo que el tiempo de configuración se incrementa un poco.
- El tiempo aproximado de respuesta es un aproximado de 3 horas con 20 minutos.

Observaciones:

Debido a que la institución no cuenta con los equipos de contingencia, el tiempo de respuesta a la incidencia excede el tiempo aceptable de caída del servicio. Por lo cual se recomienda la adquisición de este tipo de dispositivos.

Aprobado por: DARIO CASTAÑEDA	Firma:

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

PLAN DE CONTINGENCIA DE TI – FORMATO PARA PRUEBAS Y EVALUACIÓN			
Prueba No:	5	Fecha:	23 de Septiembre de 2016
Escenario de Prueba:	Ataque de virus a nivel de software		
Responsables:	Nombre		Cargo
	Ing. Darío Castañeda Ing. Marcelo Yambería Sr. Dony Reina		Jefe de Tecnología Asistente de Tecnología Tesista
Hora de inicio	14:00 h	Hora de finalización	14:10 h

Objetivo:

Mantener la continuidad del negocio de la COAC Chuchuqui Ltda, en un tiempo mínimo para el escenario de ataque de virus a nivel de software.

Aspectos a evaluar:

- Tiempo que demora el software antivirus en reaccionar a un ataque.

Requerimientos:

- Tener actualizado y licenciado el antivirus en todos los dispositivos de la COAC Chuchuqui Ltda.
- Malware creado con fines de pruebas.

Técnicas y Procedimiento:

1) Creación de malware en una máquina virtual con Kali Linux.
2) Pasar el virus o malware al equipo que va a ser sometido a la prueba.
3) Ejecutar el malware y esperar la respuesta del antivirus.

- Una vez que el antivirus bloquea la acción del malware, se procede a la eliminación del malware.

Resultados:

- Se realizó satisfactoriamente la prueba de ataque de virus o malware, donde al ser ejecutado, la protección del antivirus ESET NOD32 bloqueó inmediatamente el proceso del malware.
- Luego de la detección del virus se procede a la eliminación del malware de forma satisfactoria.
- El procedimiento de detección y eliminación del virus no tardó más de 5 minutos.

Observaciones:

- Todo el proceso se realizó con éxito, obteniendo una buena respuesta del antivirus.

Aprobado por: DARIO CASTAÑEDA	Firma:

ANEXO I: POLÍTICAS, REGLAMENTOS Y MANUALES INTERNOS

ANEXO DE REGLAMENTOS Y MANUALES INTERNOS			
	DENOMINACIÓN	ACTUALIZACIÓNES	
Nº		FECHA	Nº ACTA
1	Estatuto de la cooperativa de ahorro y crédito de indígenas CHUCHUQUI Ltda.	17/03/13	
2	Reglamento interno de administración y servicios	08-feb-2016 14-feb-2016	ACTA Nº 304 R(17) ACTA Nº 72 (ASAM GEN)
3	Reglamento de elecciones	20-may-13	ACTA Nº262 R(07)
4	Reglamento de dietas, viáticos, movilizaciones y gastos de representación	20-may-13	ACTA Nº262 R(07)
5	Reglamento de manejo de caja, ventanilla y procedimientos de control.	17-feb-15	ACTA Nº 289 R(02)
6	Reglamento para guardias de seguridad	24-may-13	ACTA Nº265 R(10)
7	Reglamento de cobranzas	22-may-13	ACTA Nº264 R(09)
8	Reglamento de fondo mortuorio, subvencione de créditos y accidentes personales de la cooperativa	17-feb-15	ACTA Nº 289 R(02)
9	Reglamento de manejo, custodia, y utilización del fondo de caja chica	22-may-13	ACTA Nº264 R(09)
10	Reglamento de crédito de la cooperativa de ahorro y crédito de indígenas CHUCHUQUI Ltda.	20-ago-16	ACTA Nº 316 R(29)
11	Reglamento interno de seguridad y salud ocupacional	31-ene-15	
12	Reglamento de uso, custodia y conservación de activos fijos	17-ene-15	ACTA Nº 288 R(01)
13	Manual de procedimientos para la asignación, custodia y conservación de los activos fijos.	05-dic-15	ACTA nº 300 R(13).

14	Manual de políticas y procedimientos para el área de cajas	16/feb/2015	ACTA Nº 289 R(02)
15	Manual de crédito y cobranzas	20-ago-16	ACTA Nº 316 R(29)
16	Manual de contabilidad	06-sep-14	ACTA Nº 284 R(12)
17	Manual de funciones	16/feb/2015	ACTA Nº 289 R(02)
18	Manual de control interno para la prevención de lavado de activos	29-may-14	ACTA Nº280 R(08)
19	Código de ética para la prevención de lavado de activos	28-mar-15	ACTA Nº 291
20	Manual de código de ética	23-ago-14	ACTA Nº 283 R(11)
21	Manual de seguimiento y control de quejas y reclamos	25-oct-15	
22	Manual operativo de tecnologías	22-nov-14	ACTA Nº 286 R (14)
23	Manual de respaldo de información	22-nov-14	ACTA Nº 286 R (14)
24	Políticas de uso y establecimiento de claves de acceso a servicios de información.	13-dic-14	ACTA Nº 287 R(15)
25	Políticas de Niveles de Operación (OLA's), Acuerdos de Niveles de Servicio (SLA's).	13-dic-14	ACTA Nº 287 R(15)
26	Manual de políticas, procedimientos y normas para la adquisición de sofware, hardware y/o desarrollo de aplicaciones	05-dic-15	ACTA nº 300 R(13).
27	Manual de políticas y procedimientos del área de tecnología de información.	05-dic-15	ACTA nº 300 R(13).
28	Manual de talento humano	28-mar-15	ACTA n.º 291
29	Plan estratégico de sistemas año 2015-2016		
30	Reglamento de fondo de cambio o ventanilla	24/05/13	

31	Manual de Calidad en el Servicio al Socio o Cliente.	09/01/16	ACTA Nº 303 R(16)
32	Manual de captaciones	05-mar-16	ACTA Nº 306 R(19)
33	Políticas/procedimientos de acceso a los sistemas de información módulo: asignación de claves y roles	23-abr-16	ACTA Nº 308 R(21)
34	Manual de usuario: CORREO CORPORATIVO SENTYAL	11/06/2016	ACTA Nº 311 R (24)
35	Manual de usuario: PHD HELP DESK.	11/06/2016	ACTA Nº 311 R (24)
36	Manual de usuario: ADMINISTRADOR ZENTYAL.	11/06/2016	ACTA Nº 311 R (24)
37	Manual de Usuario: CORE FINANCIERO WEBCOOP 2.0, Sistema Aplicacional Financiero para Cooperativas Mediante Programación Web para Plataforma LINUX.	11/06/2016	ACTA Nº 311 R (24)
38	Manual de Procedimientos para Soporte Técnico TI.	11/06/2016	ACTA Nº 311 R (24)
39	Manual Operativo: Respaldo diario/Carga de Respaldos.	11/06/2016	ACTA Nº 311 R (24)
40	Manual técnico: sistema WEBCOOP.	11/06/2016	ACTA Nº 311 R (24)
41	Manual de ADMINISTRADOR DE NAGIOS.	11/06/2016	ACTA Nº 311 R (24)
42	Manual técnico: phd help desk.	11/06/2016	ACTA Nº 311 R (24)
43	Manual Técnico/usuario: ESET ENDPOINT SECURITY 6.	11/06/2016	ACTA Nº 311 R (24)
44	Política de Control de Acceso a la Red/Información, según norma internacional ISO/IEC27002:2005	25/06/2016	ACTA Nº 312 R (25)
45	Políticas de Copias de Seguridad, según norma internacional ISO/IEC27002:2005	25/06/2016	ACTA Nº 312 R (25)
46	Manual de Gestión de Activos Informáticos, Norma Internacional ISO/IEC 27002:2005	23/07/2016	ACTA Nº 314 R (27)
47	Manual de procedimientos de Destrucción de Documentos Confidenciales.	23/07/2016	ACTA Nº 314 R (27)
48	Manual de Seguridad Física y Entorno Norma Internacional ISO/IEC 27002:2005.	20/08/2016	ACTA Nº 316 R (29)

ANEXO J: FORMATO PARA GESTIÓN DE CAMBIOS

PLAN DE CONTINGENCIA FORMATO PARA GESTIÓN DE CAMBIOS	
Cambio Nº.	
Descripción del Cambio	
Justificación para el cambio	
Fecha en que se hace efectivo	
Alternativas consideradas o eliminadas	
Proceso(s) dela institución impactado(s)	
Cronograma de Pruebas	
Entrenamiento Ajustado al cambio	
Solicitado por: **Responsable** **del Plan NOMBRE: _____** **FECHA _____/____/**	**FIRMA:**

Aprobado por: **NOMBRE:**_____ **CARGO:**_____ **FECHA** _____/_____/_____	**FIRMA:**

ANEXO K: CONFIGURACIÓN DE NAGIOS

Instalación de NAGIOS 4.0.1 y Nagios Plugin

[root@localhost]# yum install -y httpd php gcc glibc glibc-common gd gd-devel make net-snmp

[root@localhost]# useradd nagios

[root@localhost]# groupadd nagcmd

[root@localhost]# usermod -G nagcmd nagios

[root@localhost]# usermod -G nagcmd apache

[root@localhost]# mkdir /root/nagios

[root@localhost]# cd /root/nagios

[root@localhost nagios~]# wget http://prdownloads.sourceforge.net/sourceforge/nagios/ nagios-4.0.1.tar.gz

[root@localhost nagios~]# wget https://www.nagios-plugins.org/download/nagios-plugins-2.5.tar.gz

[root@localhost nagios~]# tar –xzvf nagios-4.0.1.tar.gz

[root@localhost nagios~]# tar –xzvf nagios-plugins-2.5.tar.gz

Configuración de Nagios Core

[root@localhost nagios~]# cd nagios-4.0.1

[root@localhost nagios-4.0.1]# ./configure --with-command-group=nagcmd

[root@localhost nagios-4.0.1]# make all

[root@localhost nagios-4.0.1]# make install

[root@localhost nagios-4.0.1]# make install-init

[root@localhost nagios-4.0.1]# make install-commandmode

[root@localhost nagios-4.0.1]# make install-config

Instalación y configuración de la Interfaz Web para Nagios

Al ejecutar la instalación de la interfaz web de Nagios, se crea un usuario por defecto "nagiosadmin".

[root@localhost nagios-4.0.1]# make install-webconf

Asignación de una contraseña para "nagiosadmin".

[root@localhost nagios-4.0.1]# htpasswd -s -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

New password: *******

Re-type new password: *******

Adding password for user nagiosadmin

Reiniciar Apache para que la nueva configuración surta efecto.

[root@localhost]# service httpd start

Compilación Instalación de Nagios Plugin

[root@localhost]# cd /root/nagios

[root@localhost nagios]# cd nagios-plugins-2.5

[root@localhost nagios-plugins-2.5]# ./configure --with-nagios-user=nagios --with-nagios-group=nagios

[root@localhost nagios]# make

[root@localhost nagios]# make install

Verificación de los archivos de configuración de Nagios

[root@localhost nagios]# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Ejemplo de salida:

```
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg
/usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg
/usr/local/nagios/etc/cgi.cfg
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg
/usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-
object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-
object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-
object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-
object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-
object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-
object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-
object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-
object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg
*** Config files installed ***
Recuerde, estos son *Archivos de configuración de EJEMPLO*. Tendrá que leer
la documentación para obtener más información sobre cómo definir realmente servicios,
hosts, etc para satisfacer sus necesidades particulares.
```

Figura 57: Salida de ejemplo de la verificación de instalación Nagios

Fuente: Elaboración propia.

ANEXO L: MANUAL DE USUARIO NAGIOS

Interfaz Gráfica NAGIOS

Para acceder a la interfaz gráfica nos dirigimos a nuestro navegador de preferencia y escribimos la siguiente dirección **http://ip-servidor-nagios/nagios** empleando la dirección ip de nuestro servidor NAGIOS como en ejemplo de la Figura 58.

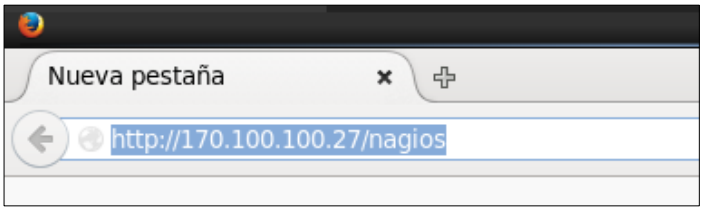


Figura 58: Dominio para el acceso a la interfaz web NAGIOS

Fuente: Elaboración propia.

Al Navegar en esta dirección se mostrará una ventana de identificación para poder acceder a la interfaz web. El nombre de usuario por defecto es **nagiosadmin** y la contraseña es la que se configura el momento de la instalación que en este caso es **admin.**

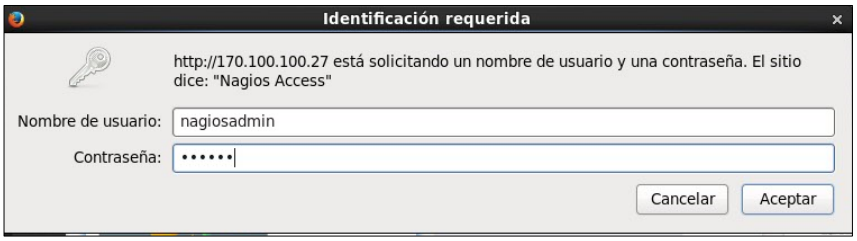


Figura 59: Ventana de Autenticación de acceso de la Interfaz Web de NAGIOS.

Fuente: Elaboración propia.

Una vez que hemos pasado la Autenticación entraremos a la página de inicio de NAGIOS y ya podemos empezar a observar la monitorización de los servidores siempre y cuando toda la configuración se haya realizado correctamente.

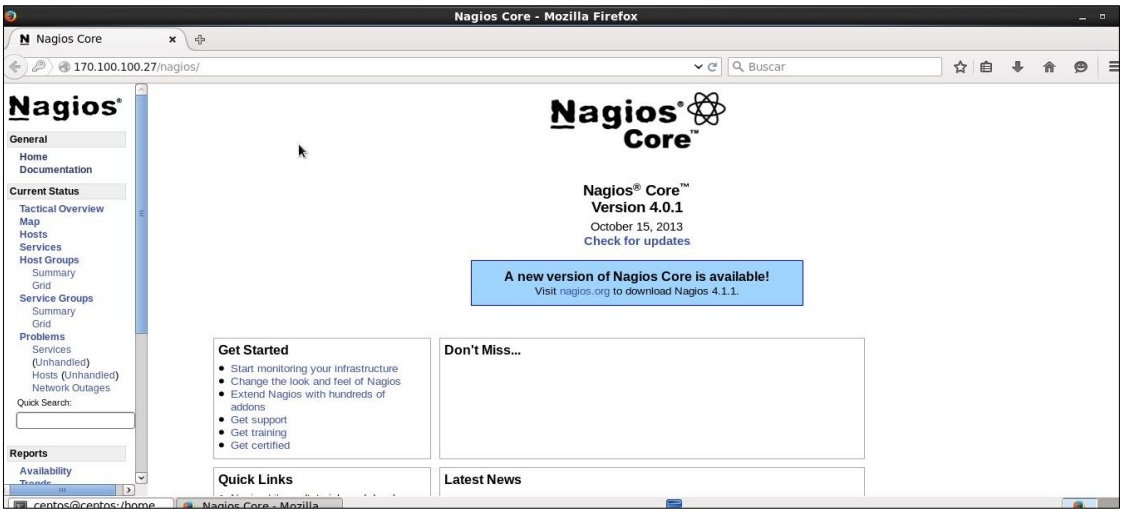


Figura 60: Página de inicio de la Interfaz web de NAGIOS.

Fuente: Elaboración propia.

Ahora para observar los dispositivos de red que se están monitoreando nos dirigimos a la pestaña **Hosts** en el menú de la parte izquierda de la pantalla.

Figura 61: Barra de menú de NAGIOS

Fuente: Elaboración propia.

En esta sección se observa el listado de los Servidores que se están monitoreando y su respectivo estado. Cuando los servidores se encuentran en estado **Up** su casilla va a ser de color verde, esto quiere decir que ese servidor se encuentra trabajando o encendido, pero si se encuentra en estado **Down** su casilla va a ser de color rojo, lo que quiere decir que ese servidor se encuentra fuera de servicio, apagado o que el servidor NAGIOS no puede alcanzar ese host.

Junto con este listado de hosts se puede observar los detalles generales del estado de

los hosts (Estado, Hora de Chequeo anterior, Duración, Información de Estado), para más información se puede hacer clic sobre el nombre.

Como se ve en la Figura 62, junto al nombre del host tenemos una lupa donde vamos a poder observar la información de los servicios que están siendo tomados en cuenta para el monitoreo.

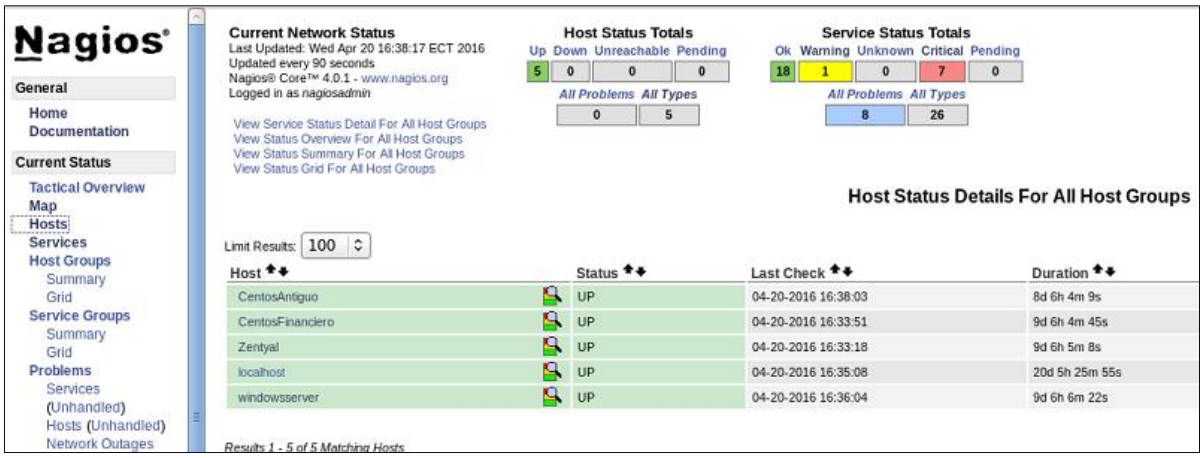


Figura 62: Listado de host monitoreados por NAGIOS

Fuente: Elaboración propia.

En la Figura 63 tenemos un ejemplo del listado de los servicios que están siendo monitoreados en el servidor **CentosAntiguo**. Los servicios que se están desarrollando de forma correcta tendrán en se Status un OK en casillero verde, los servicios que están en peligro tendrán en su Status WARNING en casillero amarillo y los servicios que se encuentran en estado crítico tendrán su Status CRITICAL en casillero rojo.

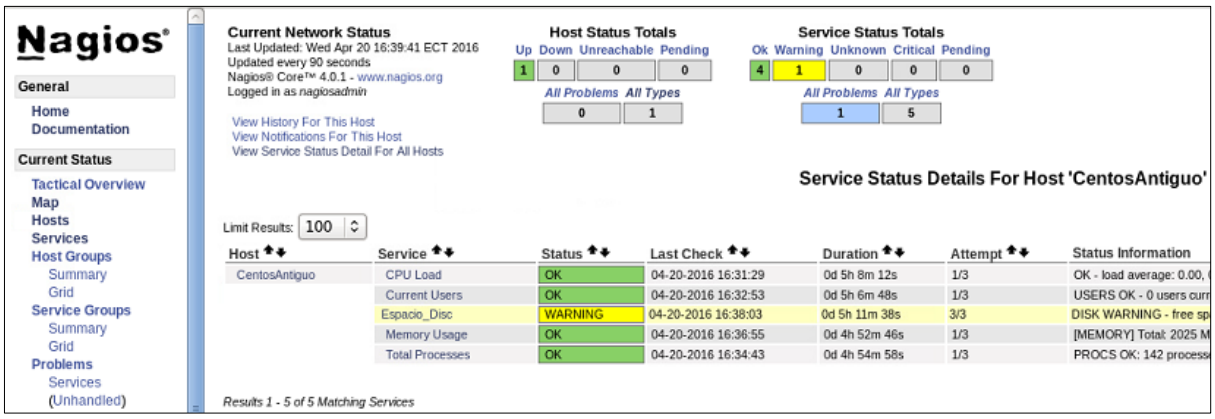


Figura 63: Listado de los Servicios monitoreados para Host CentosAntiguo

Fuente: Elaboración propia.

Si se desea ver detalles de cada servicio, simplemente se da clic en el nombre del

servicio y se mostrará la información como se muestra en la en la Figura 64.

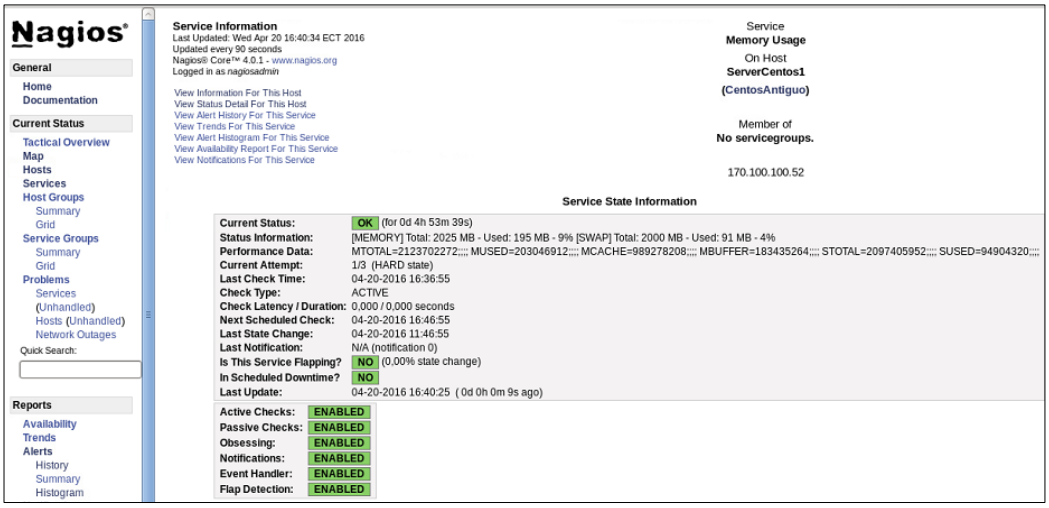


Figura 64: Información del servicio de Memoria RAM

Fuente: Elaboración propia.

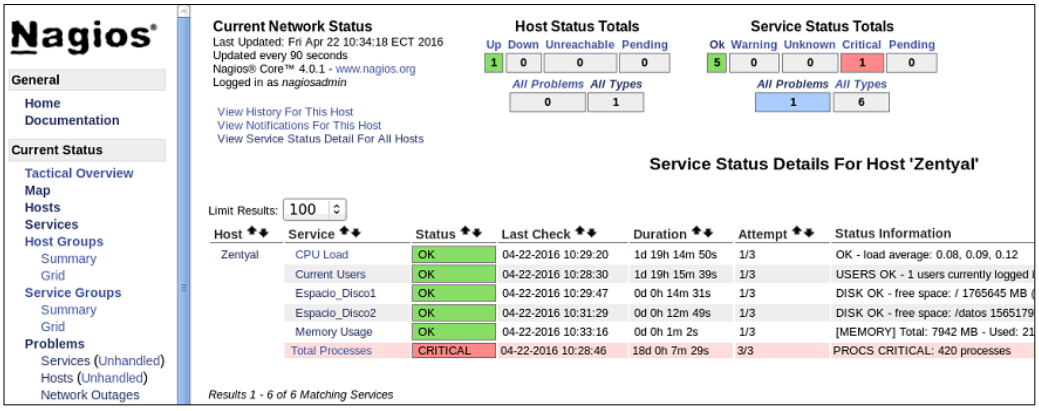


Figura 65: Listado de Servicios monitoreados de Host Zentyal

Fuente: Elaboración propia.

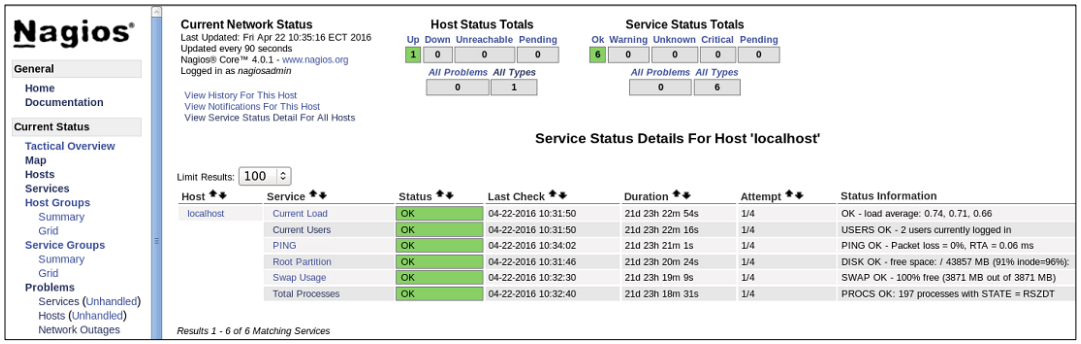


Figura 66: Listado de Servicios monitoreados para Host Localhost

Fuente: Elaboración propia.

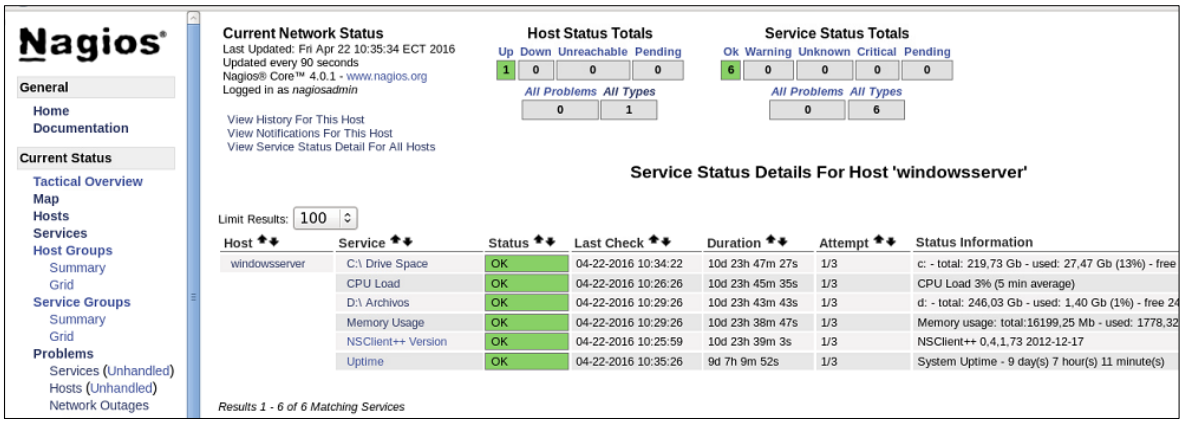


Figura 67: Listado de servicios monitoreados para Host Windowsserver

Fuente**:** Elaboración propia.

Si se desea observar los servicios de todos los hosts a la vez, hacemos clic en **Services** en la barra de menú de la parte izquierda de la pantalla.

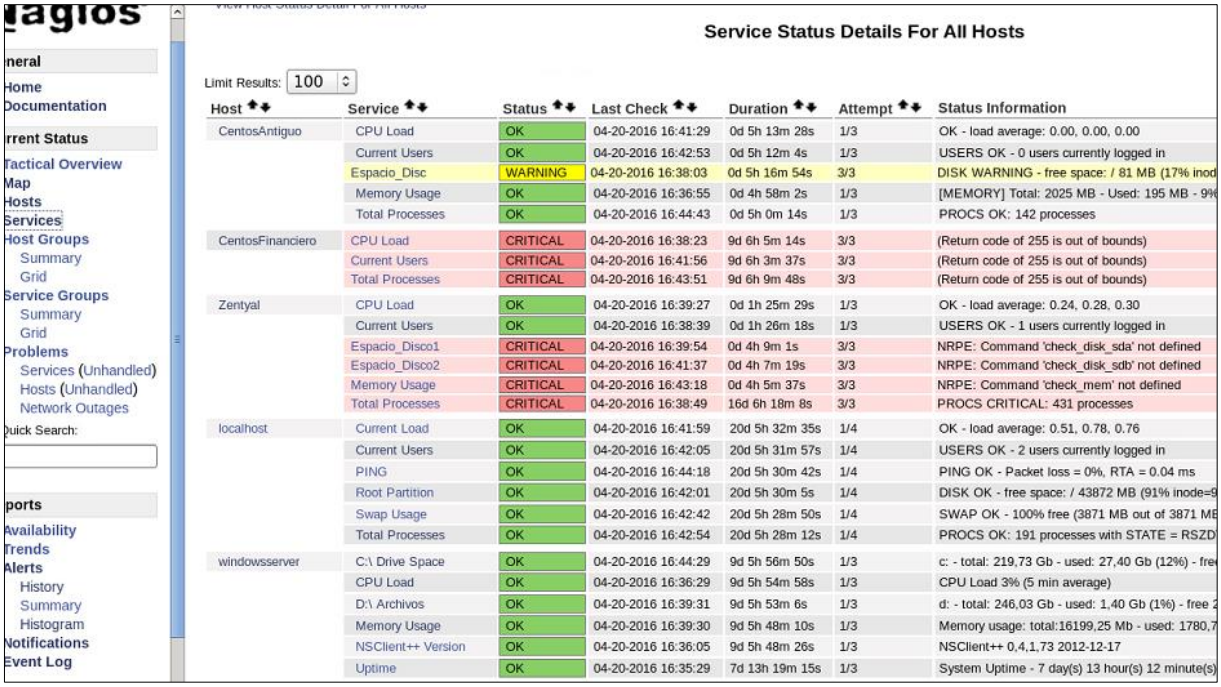


Figura 68: Listado de los Servicios de todos los Hosts.

Fuente: Elaboración propia.

En la parte central superior de la pantalla se puede ver el total de servicios de cada estado. Para ver los servicios dependiendo del estado se da clic sobre el tipo de estado que se desea revisar como se indica en la Figura 69.

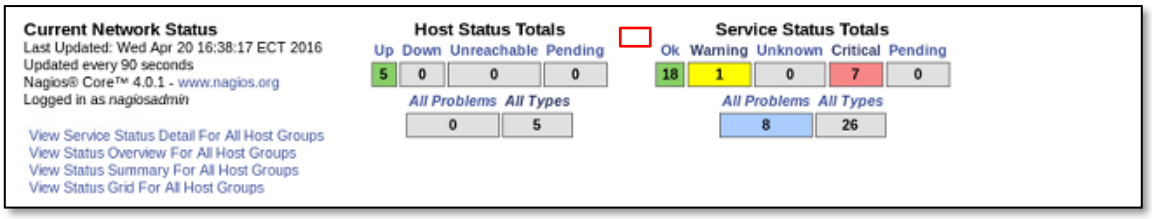


Figura 69: Cantidad total de servicios por cada estado.

Fuente: Elaboración propia.

En la Figura 70 podemos ver un ejemplo con todos los servicios que se encuentran en estado **OK**.

Figura 70: Listado Total de Servicios en Status OK

Fuente: Elaboración propia.

Reportes NAGIOS

Los reportes de los resultados de la monitorización lo podemos encontrar en la interfaz gráfica de NAGIOS, en el menú de la parte izquierda de la pantalla como se indica en la Figura 71

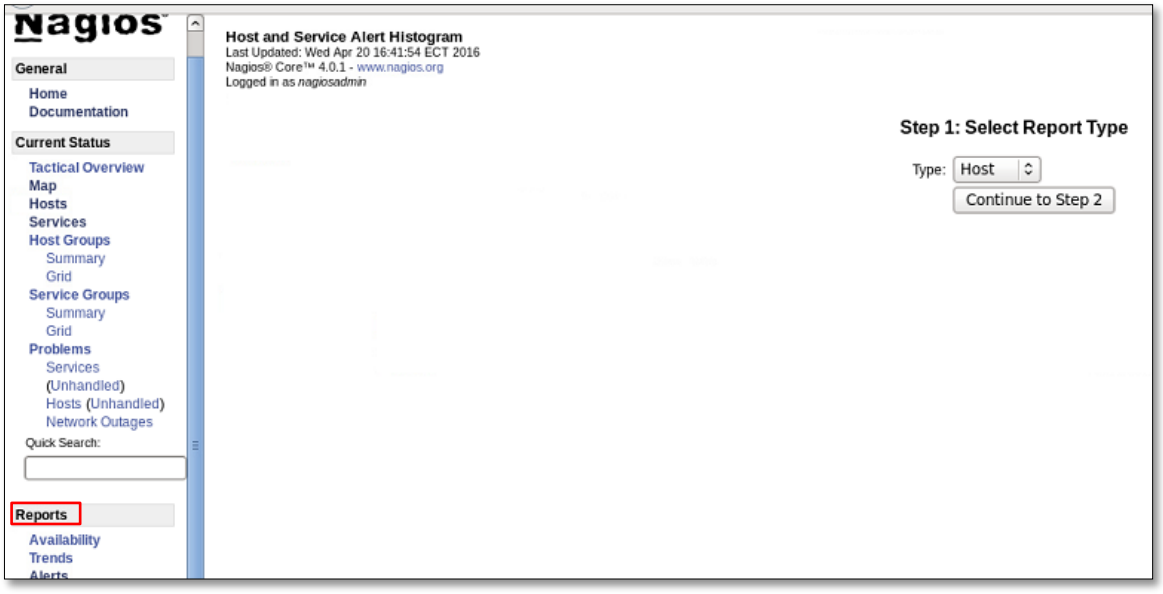


Figura 71: Step 1 de Reportes (Selección de tipo de reporte)

Fuente: Elaboración propia.

Para la obtención de los reportes vamos a pasar por varios Steps donde se va a seleccionar las opciones que se desea obtener en nuestro reporte. El primer set es para seleccionar el tipo de reporte (si se desea el reporte según el host o según el servicio).

Una vez que se ha seleccionado el tipo de servicio se va dar clic en **continuar a Step 2**, en donde el Step 2 se trata de seleccionar el Host (en caso de que el tipo de reporte que se desee sea según el host) o Servicio (en caso de que el tipo de reporte que se desee sea según el servicio).

Figura 72: Step 2 de reportes (Selección de Host)

Fuente: Elaboración propia.

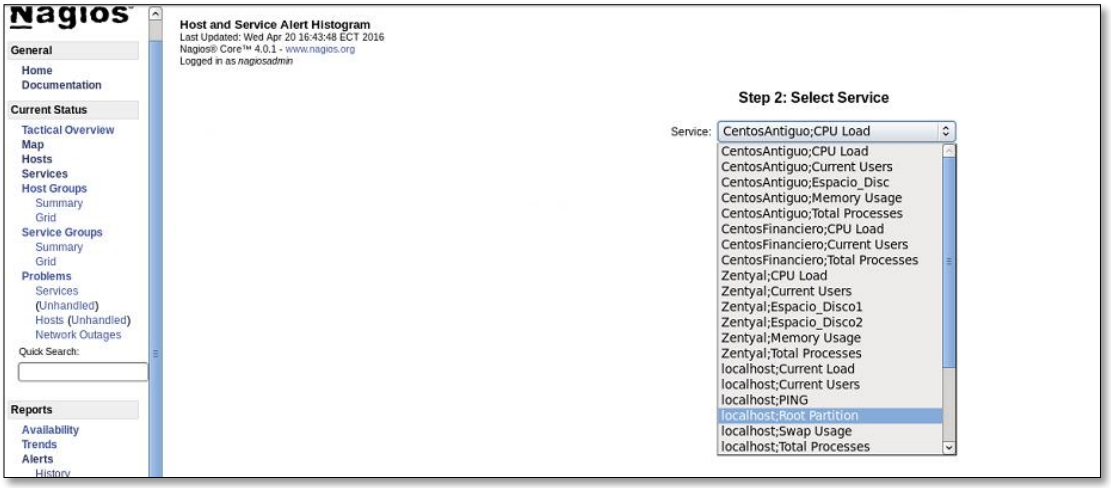


Figura 73: Step 2 de reportes (selección de servicio)

Fuente: Elaboración propia.

Una vez seleccionado el Host o Servicio vamos a pasar al Step 3 donde vamos a seleccionar el periodo de tiempo desde el cual se desea obtener los datos del reporte.

Figura 74: Step 3 de reportes (Selección de opciones de reporte)

Fuente: Elaboración propia.

Una vez que ya se seleccionó el periodo de tiempo vamos a dar clic en **Create Report**, para obtener nuestro reporte, donde vamos a poder analizar las estadísticas del servicio o host que hemos seleccionado, al crear el reporte debe aparecer una gráfica, pero para eso se necesita añadir a la configuración de Nagios otros plugins que se indican más adelante.

Otro de los servicios que nos ofrece NAGIOS es el poder observar las últimas eventualidades que se han producido, indicando la fecha y hora en la que ocurrió un cambio en el estado de uno o varios servicios. Para ello nos dirigimos al menú de Nagios en la sección de reportes, en la opción **Alerts**.

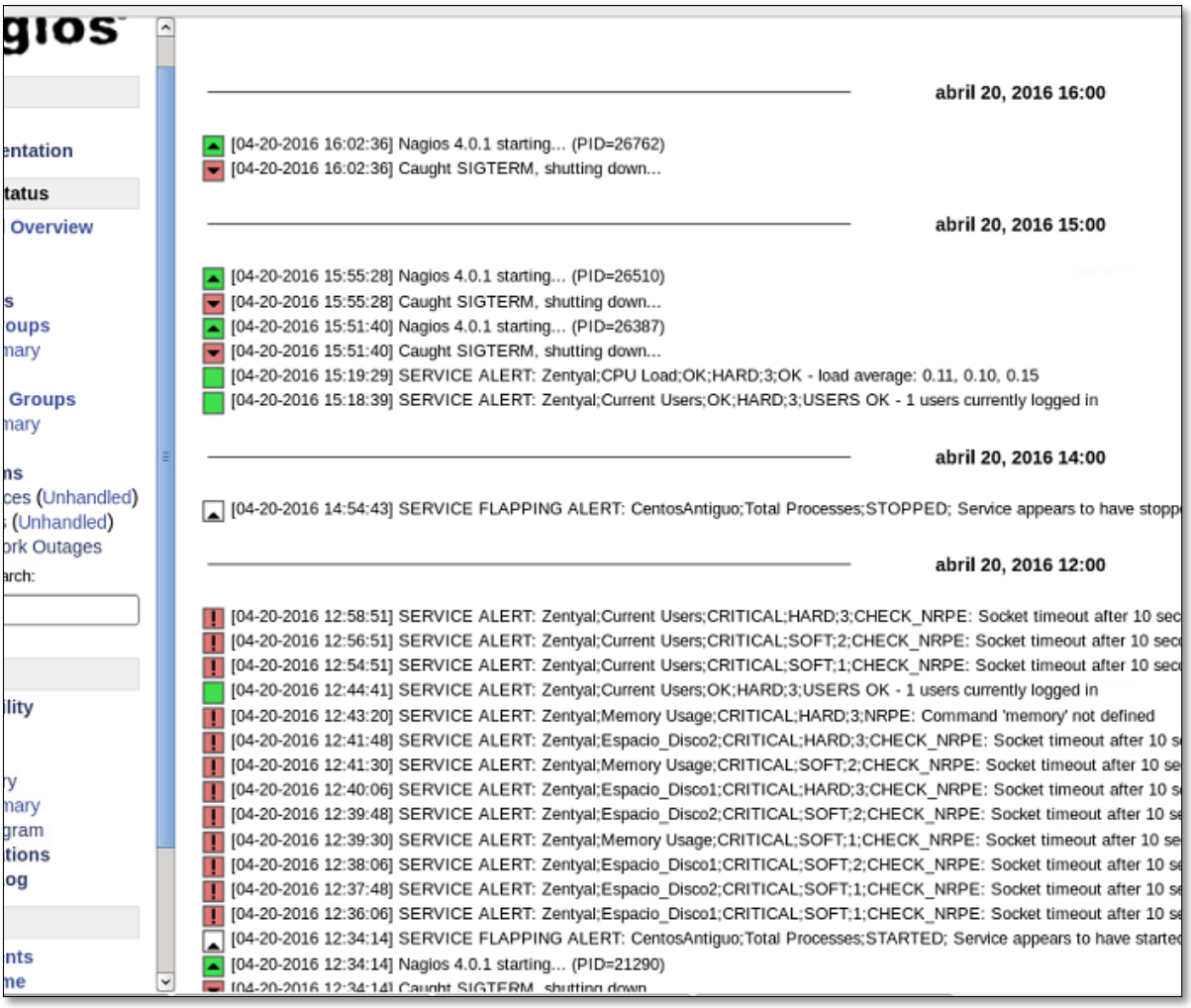


Figura 75: Reporte de Alertas de estado de los servicios (clasificadas según el tiempo)

Fuente: Elaboración propia.

NAGIOS también nos permite obtener un reporte de las últimas eventualidades, cuando ocurre un cambio en alguna característica de los servicios, indicando los detalles de dichas particularidades que se han modificado, esto nos ayuda a analizar el tiempo en el cual un servicio toma distintos valores, y tomar medidas de precaución para los cambios bruscos de la información. Para obtener este reporte nos dirigimos a la opción **Event Log** de la sección de Reportes en el menú de NAGIOS.

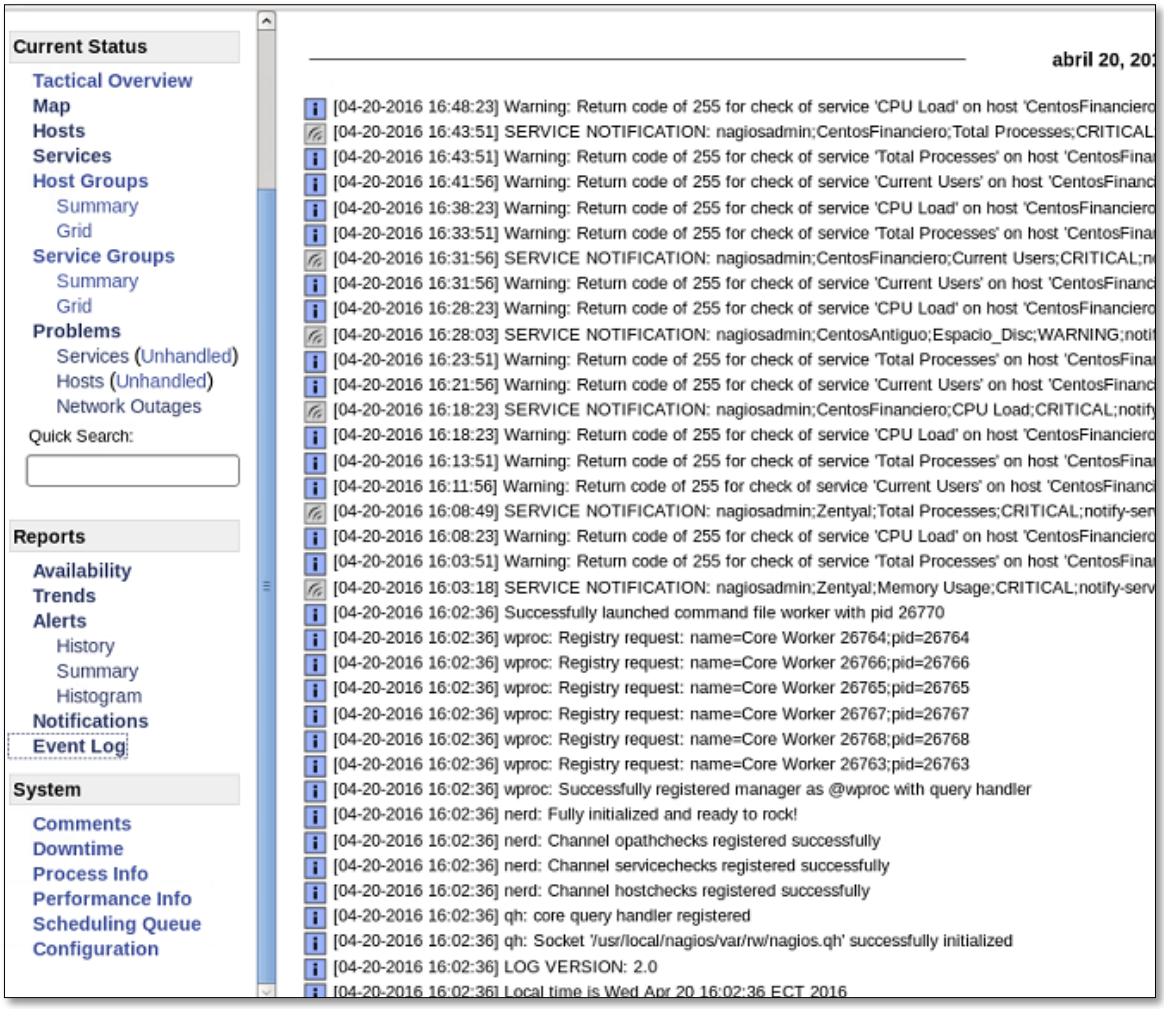


Figura 76: Reporte de Eventos

Fuente: Autoría

PNP4NAGIOS

PNP4NAGIOS es una herramienta adicional que nos permite obtener de forma gráfica los niveles de estado de los Hosts y servicios. Las funcionalidades que nos ofrece en resumen son:

- Visualización de gráficas para intervalos de tiempo predefinidos o especificados.
- Acceso a las distintas gráficas de los servicios del host seleccionado.
- Búsqueda de Hosts.
- Exportación de gráficas a PDF.
- Acceso directo desde un icono en NAGIOS, al lado del servicio / host a sus

gráficas correspondientes.

- Disponibilidad de valores prácticamente reales durante 10 días, a partir de ahí sumarizados en distintos intervalos según el tiempo.

- Personalización de gráficas.

Opciones de PNP4NAGIOS

Acciones

Figura 77: Acciones de PNP4NAGIOS

Fuente: Elaboración propia.

Los iconos de acciones nos proporcionan las siguientes funcionalidades:

- Selección de fechas de visualización en un calendario.

- Exportar la presentación de las gráficas actuales a formato PDF. Si queremos que incluya todas las gráficas de todos los servicios de nuestro host seleccionamos este previamente.

- Ver las estadísticas (gráficas) internas del proceso que usa PNP para generar las gráficas.

- Acceder a la documentación en Internet.

Selección de host o servicios

En la tabla “services” nos muestra los servicios del host seleccionado. Podemos acceder al que queramos. ¿Cómo llegamos a nuestro Host? O bien desde Nagios pinchando en el icono de acceso a PNP4NAGIOS al lado de nuestro Host/Servicio o bien buscándolo en la casilla correspondiente “Search” que nos ayudará gentilmente sugiriéndonos según escribimos.

My basket

Está característica es muy interesante. Nos permite mostrar gráficas de servicios de diferentes hosts juntas en la misma pantalla. Iremos añadiéndolas mediante el icono "+" que hay en las gráficas de servicios.

Time Ranges

Selección de rangos de tiempo más habituales.

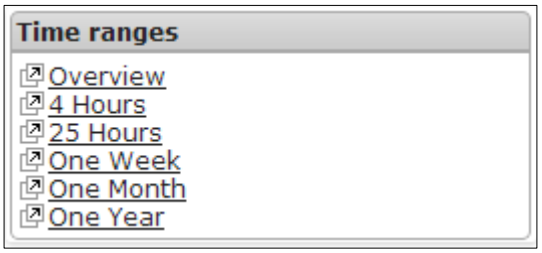


Figura 78: Rango de Tiempos habituales de PNP4NAGIOS

Fuente: Elaboración propia.

Visualización de gráficas en intervalos de tiempo

A la izquierda nos muestra las gráficas en el tiempo del servicio seleccionado con distintos intervalos de tiempo. En el menú de la derecha tenemos ya predefinidos en la tabla "time ranges" los intervalos de tiempo más habituales, pero podemos acotar más mediante el icono del calendario. También sobre las gráficas tenemos unos iconos con funcionalidades interesantes:

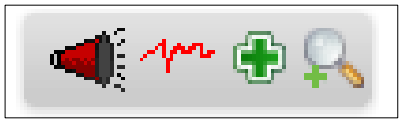


Figura 79: Iconos adicionales para las gráficas de PNP4NAGIOS

Fuente: Elaboración propia.

- Acceso a la página de NAGIOS con las alertas más recientes para este servicio.
- Acceso a la página de NAGIOS con el informe de disponibilidad para este servicio.
- "+". Nos permite añadir esta gráfica a "My basket".

- Zoom. Muy interesante. Abre la gráfica en una ventana aparte y nos permite realizar zoom directamente en el intervalo de tiempo deseado.

ANEXO M: MANUAL DE ADMINISTRADOR NAGIOS

Personalización de NAGIOS

Uno de los archivos de personalización de Nagios es "contacts.cfg", aquí se va a establecer la dirección de correo electrónico asociado a la definición de contacto nagiosadmin para recibir alertas por mail.

[root@localhost]# vi /usr/local/nagios/etc/objects/contacts.cfg

Ejemplo de salida

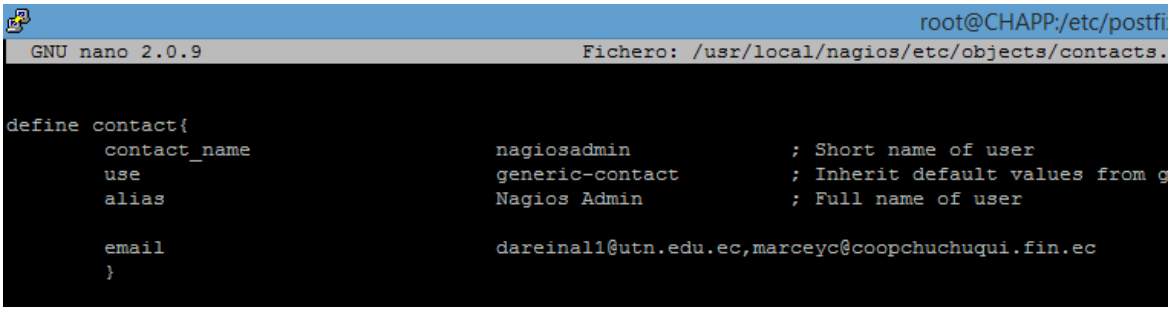


Figura 80: Fichero contacts.cfg de NAGIOS

Fuente: Elaboración propia.

Instalar y configurar la Interfaz Web para NAGIOS

Terminado con toda la configuración en el backend, se debe configurar la Interfaz Web para NAGIOS con el siguiente comando con el que se configura la interfaz y un usuario administrador web por defecto "nagiosadmin".

[root@localhost nagios-4.0.1]# make install-webconf

Ahora se debe asignar una contraseña para el usuario "nagiosadmin", también se pedirá una confirmación de la contraseña la cual se recomienda que sea fácil de recordar para el administrador, porque esta contraseña se utilizará cuando se inicie sesión en la interfaz web de NAGIOS.

[root@localhost nagios-4.0.1]# htpasswd -s -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

New password: *******

Re-type new password: *******

Adding password for user nagiosadmin

Reiniciar Apache para que la nueva configuración surta efecto.

[root@localhost]# service httpd start

Compilar e Instalar Nagios Plugin

Anteriormente se descargó los paquetes de plugins de NAGIOS en /root/nagios, hay que ingresar nuevamente a esa dirección para configurarlos e instalarlos.

[root@localhost]# cd /root/nagios

[root@localhost nagios]# cd nagios-plugins-2.5

[root@localhost nagios-plugins-2.5]# ./configure --with-nagios-user=nagios --with-nagios-group=nagios

[root@localhost nagios]# make

[root@localhost nagios]# make install

Verificar los archivos de configuración de NAGIOS

Ahora se debe realizar una comprobación de la configuración de NAGIOS, para ello se emplea el siguiente comando. Si todo va sin problemas se mostrará algo similar a la a menos a lo de a continuación:

[root@localhost nagios]# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Ejemplo de salida:

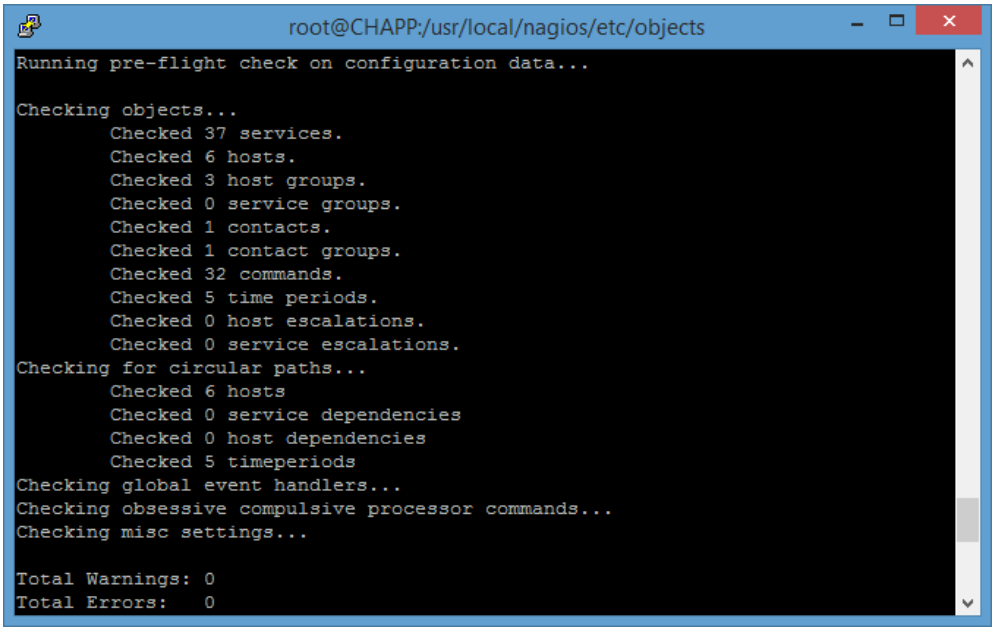


Figura 81: Comprobación de instalación de NAGIOS

Fuente: Elaboración propia.

Añadir Servicios de NAGIOS para el inicio del sistema

Para hacer a NAGIOS funcionar en los reinicios, se necesita agregar **nagios** y **httpd** con el comando **chkconfig**.

[root@localhost]# chkconfig --add nagios

[root@localhost]# chkconfig --level 35 nagios on [root@localhost]# chkconfig --add httpd

[root@localhost]# chkconfig --level 35 httpd on

Reiniciar NAGIOS para que la nueva configuración surta efecto.

[root@localhost]# service nagios start

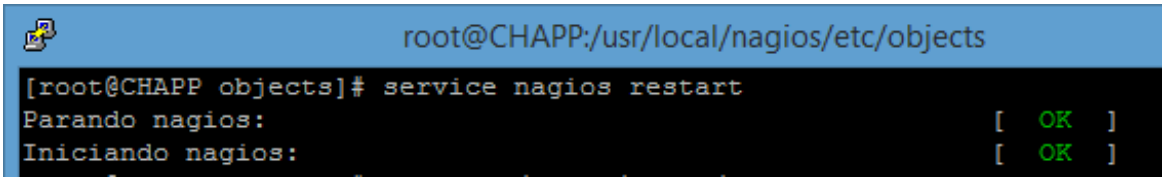


Figura 82: Reinicio del servicio Nagios

Fuente: Elaboración propia.

Inicio de sesión en la interfaz web de NAGIOS

En este punto ya se puede dirigir al siguiente URL "**http://tu-IP-address/nagios**" o http://FQDN/nagios, para poder ver la web de NAGIOS, para ello se iniciará sesión con el nombre de usuario "nagiosadmin" y la contraseña anteriormente asignada.

Figura 83: Interfaz Web NAGIOS

Fuente: Elaboración propia.

Archivos de configuración

Los archivos de configuración de NAGIOS los podemos encontrar en la dirección **/usr/local/nagios/etc**, en esta localización podemos observar los archivos que muestran en la figura 21. Para dirigirnos a esta dirección desde en termina empleamos el comando **cd /usr/local/nagios/etc**

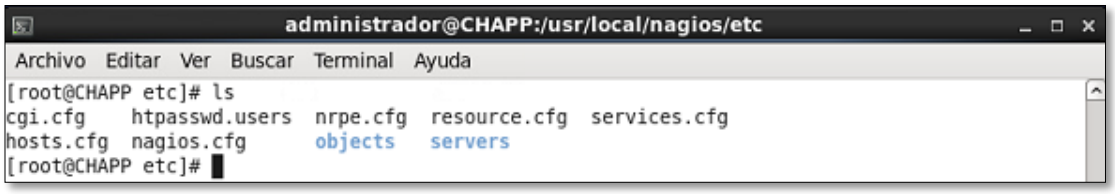


Figura 84: Archivos de configuración de NAGIOS

Fuente: Elaboración propia.

De los archivos de configuración presentados en la figura 21, los de mayor importancia y los cuales podemos realizar modificaciones empleando cualquier comando para editar texto (vim, vi, nano, get, etc.) son los siguientes:

- **hosts.cfg:** Este es un archivo creado por el administrador de NAGIOS, donde se declaran todos los hosts que van a ser monitoreados, si se desea agregar un nuevo host se lo puede realizar siguiendo el formato de la figura 22.

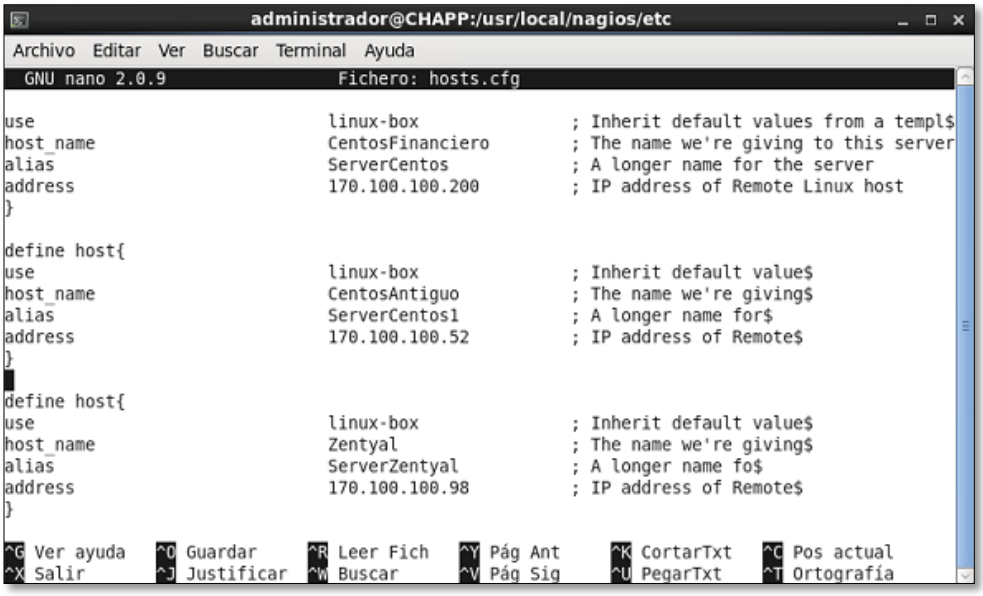


Figura 85: Archivo de configuración hosts.cfg

Fuente: Elaboración propia.

- **services.cfg:** Este es un archivo creado por el administrador de NAGIOS, donde se encuentran los servicios que se desea monitorear para cada host. Si se desea agregar un nuevo servicio se puede guiar en el formato de la figura 23, pero hay que tomar en cuenta que el modelo del check_command para cada servicio es distinto.

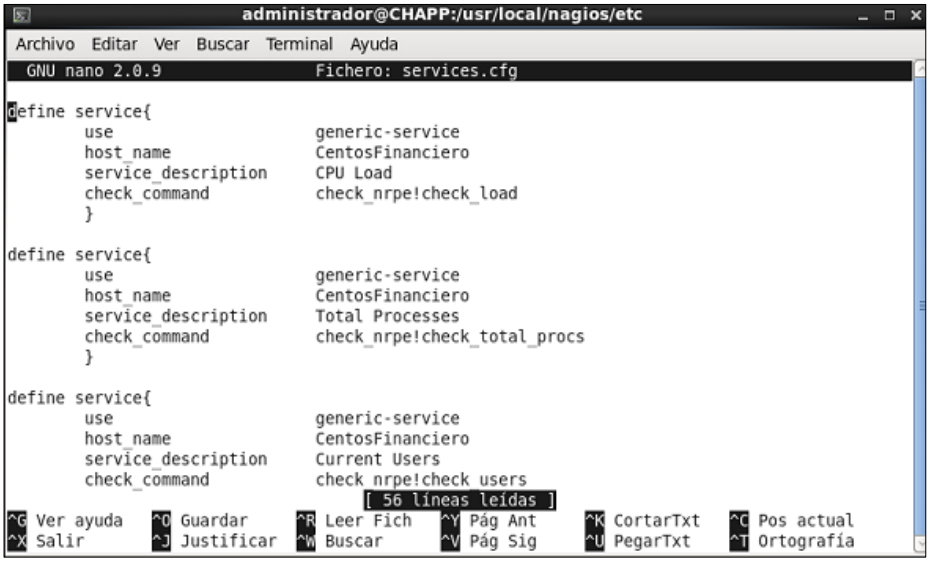


Figura 86: Archivo de configuración services.cfg

Fuente: Elaboración propia.

- **nagios.cfg:** Este es el archivo principal de configuración de NAGIOS, en este podemos encontrar las direcciones de los archivos con los cuales está trabajando

Nagios, en este archivo se agregan las direcciones de los archivos que creamos como hosts.cfg y services.cfg para que NAGIOS pueda obtener la información que en ellos se encuentran.

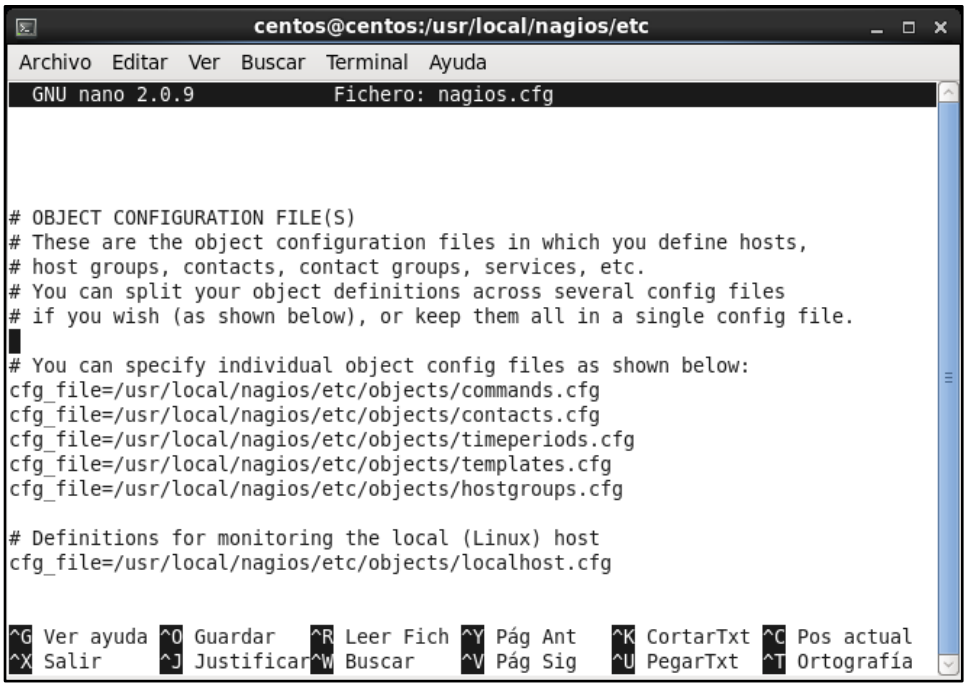


Figura 87: Archivo de configuración nagios.cfg

Fuente: Elaboración propia.

- **nrpe.cfg:** Este archivo pertenece al protocolo NRPE que se debe instalar en el servidor NAGIOS para que pueda tener conectividad con los clientes con sistemas operativos de Linux como Centos, Zentyal, Ubuntu entre otros.

  En este archivo nrpe.cfg se va a encontrar los comandos necesarios para los servicios de los clientes, cada comando va relacionado con un plugin de NRPE (los plugins se los reconoce por su prefijo check_), en caso de que no exista el plugin adecuado para algún servicio hay que descargarlo desde internet y agregarlo en la localización de los plugins.

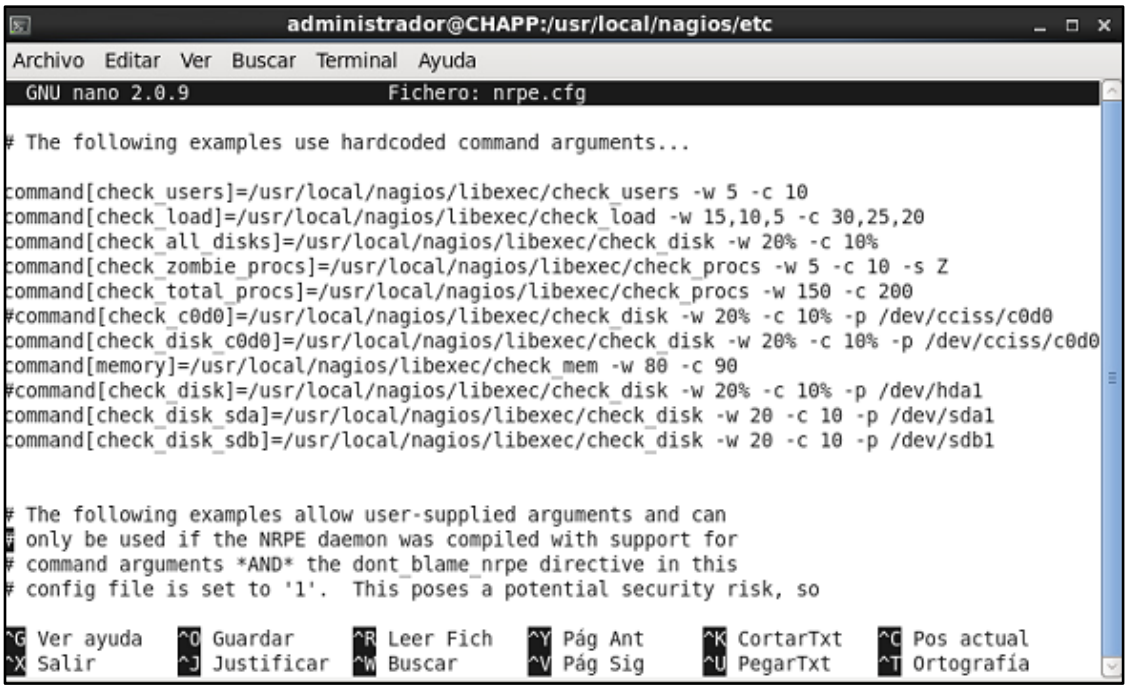


Figura 88: Archivo de configuración nrpe.cfg

Fuente: Elaboración propia.

Otros archivos de configuración de NAGIOS se encuentran en la dirección **/usr/local/nagios/etc/objects** donde se localizan los archivos que se muestran en la Figura 89.

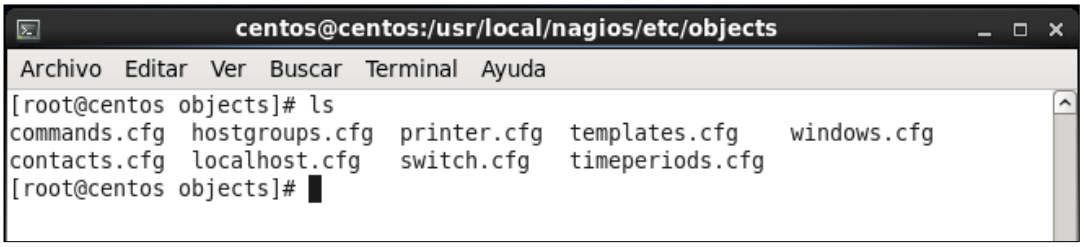


Figura 89: Archivos de configuración de objects de NAGIOS

Fuente: Elaboración propia.

De estos Archivos los más importantes son:

- **commands.cfg:** En este archivo se van a definir los comandos que se van a ejecutar para cada servicio que se va a monitorear de los clientes.

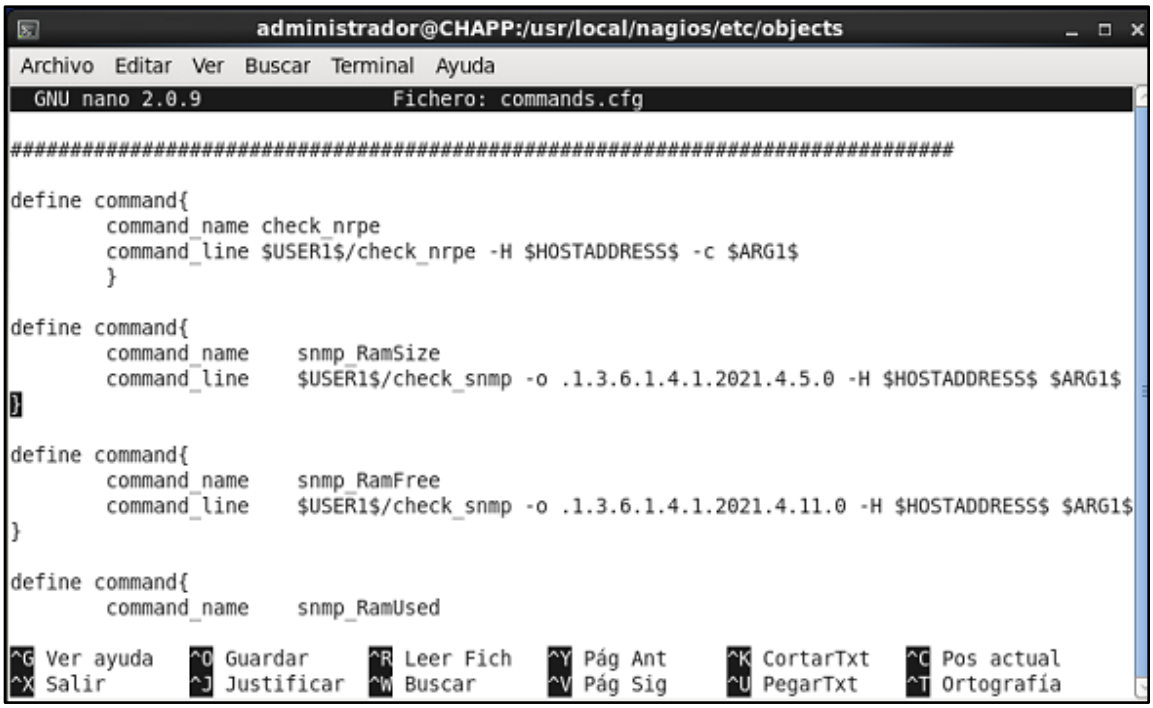


Figura 90: Archivo de configuración commands.cfg

Fuente: Elaboración propia.

- **contacts.cfg:** En este archivo se declara una o varias direcciones de correos electrónicos donde queremos que nos envíen mensajes con las notificaciones de Alertas de NAGIOS.

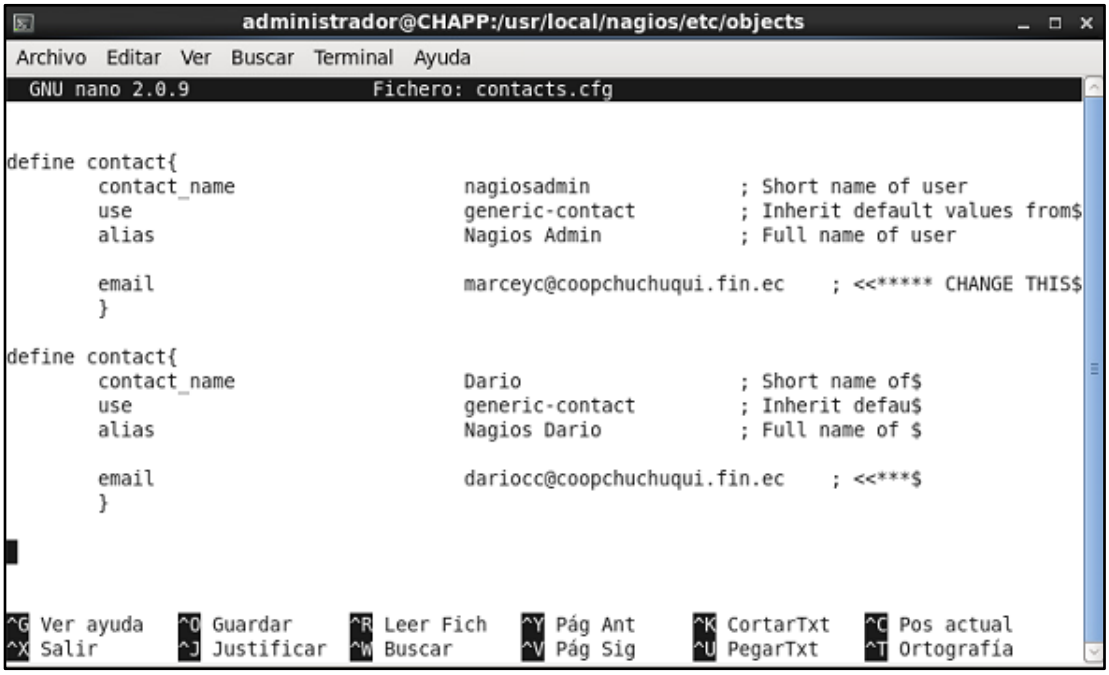


Figura 91: Archivo de configuración contacts.cfg

Fuente: Elaboración propia.

Plugins NRPE

Los plugins NRPE son muy importantes en los clientes NAGIOS ya que nos permiten comunicarnos con el servidor Nagios. Para eso se debe instalar los paquetes del protocolo NRPE en cada cliente y adicionalmente se instalar los plugins en la dirección **/usr/local/Nagios/libexec**, estos plugin son los que extraen la información del estado de los servicios de los clientes y los envía al servidor mediante el protocolo NRPE empleando el puerto 5666. Si no se encuentran todos los plugins necesarios para algún servicio se los puede descargar por separado desde internet y se los agrega en la dirección antes mencionada como se muestra en la Figura 92.

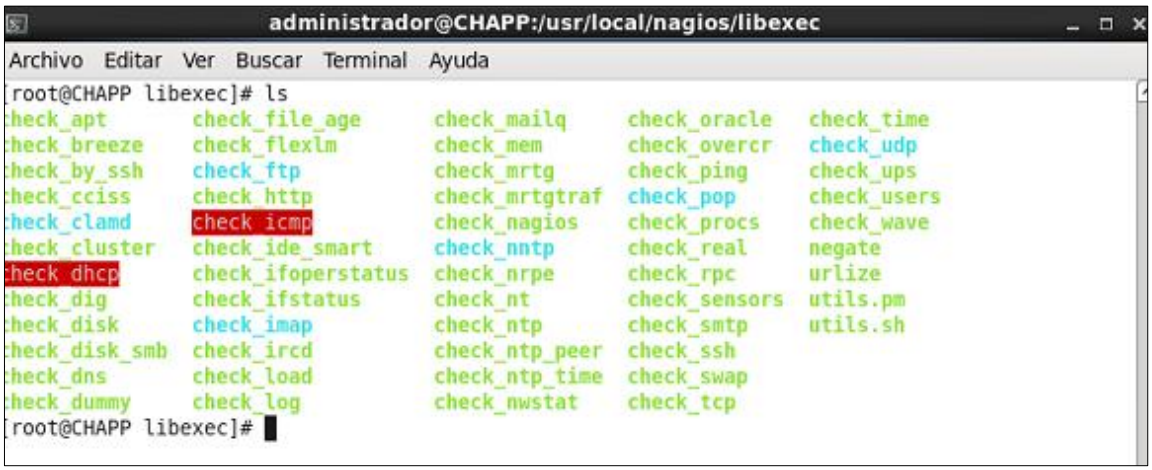


Figura 92: Plugins NRPE

Fuente: Elaboración propia.

Ficheros de configuración PNP4NAGIOS

A continuación, se indicará los ficheros de configuración originarios de NAGIOS, en los que se necesita realizar cambios para el correcto funcionamiento de PNP4NAGIOS y su archivo principal **/etc/httpd/conf.d/pnp4nagios.conf**

En el fichero **/usr/local/nagios/etc/nagios.cfg** se va buscar la línea **process_performance_data=0**, donde remplazaremos el 0 por 1 y también se añadirán las siguientes líneas de configuración.

```
#
# service performance data
#
service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata
service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET
$\tHOSTNAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPER
```

```
FDATA::$SERVICEPERFDATA$\tSERVICECHECKCOMMAND::$SERVICECHEC
KCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATE
TYPE$\tSERVICESTATE::$SERVICESTATE$\tSERVICESTATETYPE::$SERVICES
TATETYPE$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=15
service_perfdata_file_processing_command=process-service-perfdata-file
#
# host performance data starting with Nagios 3.0
#
host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata
host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$TIMET$\tHO
STNAME::$HOSTNAME$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHECK
COMMAND::$HOSTCHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTS
TATETYPE::$HOSTSTATETYPE$
host_perfdata_file_mode=a
host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-file
```

Otro fichero de configuración que se debe configurar es **/usr/local/nagios/etc/objects/commands.cfg**, donde se añadirá las siguientes definiciones de comandos:

```
define command{
command_name process-service-perfdata-file
command_line /usr/local/pnp4nagios/libexec/process_perfdata.pl –
bulk=/usr/local/pnp4nagios/var/service-perfdata
}
define command{
command_name process-host-perfdata-file
command_line /usr/local/pnp4nagios/libexec/process_perfdata.pl –
bulk=/usr/local/pnp4nagios/var/host-perfdata
}
```

También se debe modificar el fichero **/usr/local/nagios/etc/objects/templates.cfg**, donde se añadirá en la definición que contiene la porción "generic-hosts" la siguiente línea:

```
action_url /pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=_HOST_'
class='tips' rel='/pnp4nagios/index.php/popup?host=$HOSTNAME$&srv=_HOST_
```

Y en la definición que contiene la porción "generic-service" se añadirá la siguiente línea:

```
action_url
/pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=$SERVICEDESC$'
class='tips'
rel='/pnp4nagios/index.php/popup?host=$HOSTNAME$&srv=$SERVICEDESC$
```

Un paso muy importante en la configuración de PNP4NAGIOS es el copiar el fichero **status-header.ssi** desde sus paquetes con el siguiente comando:

```
cp /usr/local/src/pnp4nagios-0.6.24/contrib/ssi/status-header.ssi
/usr/local/nagios/share/ssi/
```

Y el último fichero que falta editar es **/etc/httpd/conf.d/pnp4nagios.conf**, donde simplemente se edita la línea AuthUserFile /etc/nagios/htpasswd.users por AuthUserFile /usr/local/nagios/etc/htpasswd.users

Para finalizar debemos resetear los servicios para que comience a funcionar esta herramienta.

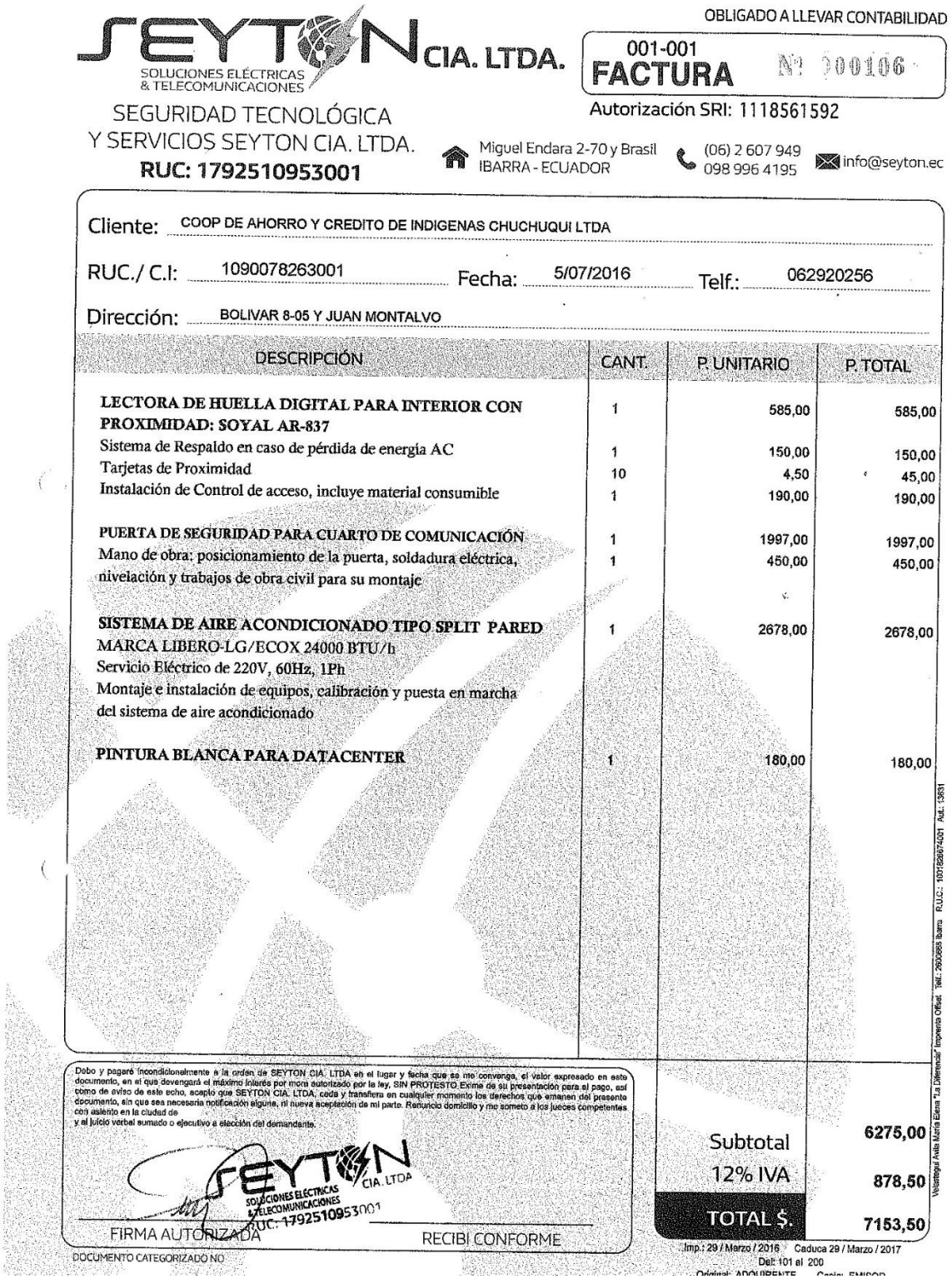
[root@localhost]# service httpd restart

[root@localhost]# service nagios restart

[root@localhost]# service npcd start

[root@localhost]# chkconfig npcd on

ANEXO N: COTIZACIONES Y FACTURAS



SEYTON CIA. LTDA.
SOLUCIONES ELÉCTRICAS & TELECOMUNICACIONES

OBLIGADO A LLEVAR CONTABILIDAD

001-001
FACTURA Nº 000106

Autorización SRI: 1118561592

SEGURIDAD TECNOLÓGICA
Y SERVICIOS SEYTON CIA. LTDA.
RUC: 1792510953001

Miguel Endara 2-70 y Brasil
IBARRA - ECUADOR

(06) 2 607 949
098 996 4195

info@seyton.ec

Cliente: COOP DE AHORRO Y CREDITO DE INDIGENAS CHUCHUQUI LTDA

RUC./ C.I: 1090078263001 Fecha: 5/07/2016 Telf.: 062920256

Dirección: BOLIVAR 8-05 Y JUAN MONTALVO

DESCRIPCIÓN	CANT.	P. UNITARIO	P. TOTAL
LECTORA DE HUELLA DIGITAL PARA INTERIOR CON PROXIMIDAD: SOYAL AR-837	1	585,00	585,00
Sistema de Respaldo en caso de pérdida de energía AC	1	150,00	150,00
Tarjetas de Proximidad	10	4,50	45,00
Instalación de Control de acceso, incluye material consumible	1	190,00	190,00
PUERTA DE SEGURIDAD PARA CUARTO DE COMUNICACIÓN	1	1997,00	1997,00
Mano de obra: posicionamiento de la puerta, soldadura eléctrica, nivelación y trabajos de obra civil para su montaje	1	450,00	450,00
SISTEMA DE AIRE ACONDICIONADO TIPO SPLIT PARED MARCA LIBERO-LG/ECOX 24000 BTU/h Servicio Eléctrico de 220V, 60Hz, 1Ph Montaje e instalación de equipos, calibración y puesta en marcha del sistema de aire acondicionado	1	2678,00	2678,00
PINTURA BLANCA PARA DATACENTER	1	180,00	180,00

Debo y pagaré incondicionalmente a la orden de SEYTON CIA. LTDA en el lugar y fecha que se me convenga, el valor expresado en este documento, en el que devengará el máximo interés por mora autorizado por la ley, SIN PROTESTO. Exime de su presentación para el pago, así como de aviso de este echo, acepto que SEYTON CIA. LTDA, ceda y transfiera en cualquier momento los derechos que emanen del presente documento, sin que sea necesaria notificación alguna, ni nueva aceptación de mi parte. Renuncio domicilio y me someto a los jueces competentes con asiento en la ciudad de
y al juicio verbal sumario o ejecutivo a elección del demandante.

Subtotal	6275,00
12% IVA	878,50
TOTAL $.	7153,50

SEYTON CIA. LTDA SOLUCIONES ELÉCTRICAS & TELECOMUNICACIONES RUC: 1792510953001

FIRMA AUTORIZADA RECIBI CONFORME

DOCUMENTO CATEGORIZADO NO

Imp.: 29 / Marzo / 2016 Caduca 29 / Marzo / 2017
Del: 101 al 200
Original: ADQUIRENTE Copia: EMISOR

Velasteguí Avila María Elena "La Diferencia" Imprenta Offset Tel.: 2600665 Ibarra R.U.C.: 1001526674001 Aut.: 13631

WORLD COMPUTERS
Su inversión inteligente

CORDOVA PALADINES NORMA YOLANDA

Matriz: Pedro Moncayo 353 Y Rocafuerte - Ibarra
Teléfonos: 062640333 - Email: wcfactura@gmail.com

R.U.C.: 0701084121001
Contribuyente Especial Nro.: 466

Nro. Factura: 003-010-000015749

Nro. Autorización: 2007201611204607010841210018954691588
Fec.Autorización: 2016-07-20- 11:20:46

Ambiente: PRODUCCION **Emisión:** NORMAL

CLAVE DE ACCESO:

2007201601070108412100120030100000157491234567810

Cliente: COOP DE AHOORO Y CREDITO CHUCHUQUI LTDA (009324)
R.U.C. / C.I.: 1090078263001
Dirección: BOLIVAR 805 Y JUAN MONTALVO
Ciudad: OTAVALO **Teléfono:** 062920256 **Fecha Emisión:** 2016/07/20
Forma Pago: Credito 001 dias Vence: 2016/07/21 **Vendedor:** ARMAS MUGMAL **Referencia:**
Observación:

Código	Descripción	UM. Bo.	Cant.	Precio U.	%	Dscto.	Total
610120	Windows 7 Profesional SP1 64-Bits Español	UN 01	1.00	175.0000	0.00	0.00	175.0000 *
050222	Disco duro 4 TB Externo WD My Book USB 3.0	UN 01	1.00	255.0000	0.00	0.00	255.0000 *

Total Unidades 2.00

Forma de Pago	Valor
Sin Utilizar El Sistema Financiero	490.20

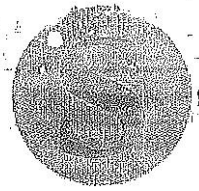
Subtotal	430.00
Descuentos	.00
Otros Descuentos	.00
Base 0%	.00
Base 0I4%	430.00
I.V.A.	60.20
Recargos	.00
Total General:	490.20

WORLD COMPUTERS
Su inversion inteligente
Ibarra - Ecuador

Firma Autorizada
Entregado por

Cliente

Puede descargar su Comprobante Electrónico desde la web: www.worldcomputers.com.ec



SANCHEZ VINTIMILLA OMAR DANILO

OBLIGADO A LLEVAR CONTABILIDAD

Matriz y Establecimiento: Centro, Bolívar 10-96 y Pérez Guerrero Telf.: 2600 656 / 2601 636 Cel.: 099 7380 837

Ibarra Ecuador

www.casacomercialsanhez.com

FACTURA 001-001

Nº 000007071

RUC.: 1710533173001

AUT. SRL.: 1119198189

Com: 19167

Cliente: COOPERATIVA CHUCHUQUI LTDA

Dirección: OTAVALO - BOLIVAR 905 Y JUAN MONTALVO

C.I./RUC: 1090078263001

Fecha: 03-10-2016

Teléfono: 0629830258

Cantidad	Descripción	Precio	Des.	Total
2	COPIADORA IMPRESORA MPC 4502 MPC5502	2,105.36	0.00	4,210.72
2	REGULADOR DE VOLTAJE	114.04	0.00	228.08

BASE IMPONIBLE	4,438.80
I.V.A 14%	621.40
IVA 0%	0.00
TOTAL	5,060.00

Debo y Pagaré a Favor de SANCHEZ VINTIMILLA OMAR DANILO en el plazo aquí estipulado el valor constante en esta factura por la mercadería detallada en la misma recibida en esta factura a total y entera satisfacción. En caso de mora reconoceré además intereses calculados a la época en que se efectúe el pago efectivo.

FIRMA AUTORIZADA

RECIBÍ CONFORME

ORIGINAL ADQUIRIENTE - COPIA EMISOR DOCUMENTO CATEGORIZADO: NO

RIVERA TERAN FAUSTO AMADEO IMPRENTA OFFSET IMPRIMA TELF. 2951588 RUC 1001190543001 AUT. 1431 DEL 6951 A 7150 F.AUTORIZACIÓN IMPR. 27-JULIO-2016 CADUCA 27-OCTUBRE-2016

SEYTON
SOLUCIONES ELECTRICAS & TELECOMUNICACIONES

CONSULTORÍA
IMPLEMENTACIÓN
AUTOMATIZACIÓN
CAPACITACIÓN
SOPORTE TÉCNICO

RUC: 1702510950001

COTIZACIÓN

CLIENTE: Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda
RUC: 1090078150001
DIRECCION: BOLIVAR 805 Y JUAN MONTALVO Otavalo, Ecuador
TELEFONO: 2920256

Nº: C-0017
FECHA: 03/08/2016
CIUDAD: IBARRA

Nº	DETALLE	P. UNITARIO	P.TOTAL
1	RACK DE PARED DE 9 UR MARCA CONNECTION	151,54	151,54
1	RACK DE PARED DE 6 ur MARCA CONNECTION	206,28	206,28
	LOS MODELOS POSEEN UNA BANDEJA Y VENTILADOR		

Sub Total	357,81
IVA 14%	50,09
TOTAL	407,91

FECHA DE ENTREGA: 6 Dias laborables
VALIDEZ DE LA OFERTA: 15 Dias
FORMA DE PAGO: A la entrega del producto
GARANTÍA: 1 Año

Eduardo Puga

Atb:

Ing. Eduardo Puga J.
Asesor Técnico de Proyectos y Negocios
SEYTON

SEYTON CIA. LTDA.

COMUNICACIONES
GOLD PARTNER

Dirección: Pedro Basan N35-87 y Manosca
Teléfono: (593 2)2 443267
RUC: 1792284589001
Web: www.comunicaciones-gp.com

OFERTA COMERCIAL

Cliente:	COAC CHUCHUQUI	**Código:**	GP-01-100001
Ciudad:	OTAVALO	**Telf.:**	
Dirección:	OTAVALO	**Fecha:**	11-ene-2017
Contacto:	ING. DARIO CASTAÑEDA	**Páginas:**	1 de 1
Email:	<dariocc@coopchuchuqui.fin.ec>	**Versión:**	1

DISPONIB.	CODIGO	DESCRIPCION	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
		1470 Next Generation Threat Prevention Appliance, Wired, including 3 years of services and Direct Standard support, vigencia del soporte 3 años	1	$ 3.260,26	$ 3.260,26
		INSTALACION, CONFIGURACION Y TRANSFERENCIA DE CONOCIMIENTOS			
		Incluye: Instalación y configuración de los siguientes equipos: - 1470 Next Generation Threat Prevention Appliance Localidad: Otavalo - Instalación y configuración de los blades: Firewall URL Filtering Threat Prevention	1	$ 640,00	$ 640,00
		Transferencia de conocimientos de la solución instalada. Tiempo: 4 horas Lugar: Otavalo Asistentes: hasta 4 personas	1	$ 200,00	$ 200,00
				SUBTOTAL	$ 4.100,26
				IVA	$ 574,04
				TOTAL	$ 4.674,30

CONFIDENCIALIDAD

La presente cotización está dirigida a la COAC CHUCHUQUI. La información contenida en este documento no debe divulgarse fuera de la COAC CHUCHUQUI y no debe ser duplicada, usada o alterada completamente o de forma parcial con propósitos distintos a su evaluación.

TIEMPO DE ENTREGA

30 dias

FORMA DE PAGO

80% de anticipo, luego de aceptada la propuesta
20% contra entrega de equipos y acta entrega final

VALIDEZ

La presente cotización tiene una validez de 30 días.

Atentamente:

Monica Flores
GERENTE DE CUENTA
mflores@comunicaciones-gp.com

ANEXO O: CERTIFICADO DE PRESUPUESTO ECONÓMICO

Cooperativa de Ahorro y Crédito
De Indígenas "CHUCHUQUÍ" LTDA.
¡Seguridad y experiencia financiera!
Impulsamos el desarrollo

En mi calidad de CONTADORA GENERAL de la Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda, de la cuidad de Otavalo.

Me permito:

CERTIFICAR

Que para el periodo fiscal 2017, se destinará el monto de USD 45.000 al Departamento de Tecnología; mismo que estará predestinado para los diferentes rubros que dicho departamento.

El portador de este documento podrá hacer uso del mismo exclusivamente para asuntos académicos y de investigación científica.

Dado en la ciudad de Otavalo, a los diecisiete días del mes de octubre de 2016.

Atentamente,

Lic. Esthela Males
CONTADORA GENERAL – COAC CHUCHUQUI LTDA.

Fundada el 2 de Septiembre de 1986; controlada por la Superintendencia de la Economía Popular y Solidaria
Dirección: Bolívar 805 y Juan Montalvo • Telf.: 06 2920-256 / 2925 372 / 2926 084 • Telefax: 06 2922-930
E-mail: coac_chuchuqui@hotmail.com Otavalo - Ecuador

ANEXO P: REGISTRO DE ASISTENCIA DE CAPACITACIÓN

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

Departamento de Tecnología

REGISTRO DE CAPACITACIONES IT

Tema: SEGURIDAD DE LA INFORMACIÓN

Fecha: 2016-09-15

Lugar: Salón de capacitaciones CHUCHUQUI Ltda.

CEDULA	NOMBRE/APELLIDO	CARGO	FIRMA
1003620687	Marcelo Velásquez	Secretaria General	
100388772-4	Nelly Yamberla	Asistente Operativo	
1003439878	Maritha Fainango	Aux. Contable	
1002410797	Esthela Males	Contadora	
100247747-7	Anabel Placencia	Auditor	
100321989-4	Jacqueline Chico	Asistente Cumpl.	
100306404-3	Ximena Tituaña	Riesgos	
1003569850	Iván Maldonado	Asesor	
100416604-5	Celia Cachiguango	Asistente Crédito	
100323371-3	Diana Males	JEFE OPERATIVO	
100300965-9	Tania Vásquez	Inversiones	
100403978-8	Sergio Qiona	Cajas	

Capacitadores: Darío Castañeda, Marcelo Yamberla, Dony Reina
Seguridad de la Información – Dpto. Tecnología

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

Departamento de Tecnología

REGISTRO DE CAPACITACIONES IT

Tema: SEGURIDAD DE LA INFORMACIÓN

Fecha: 2016-09-15

Lugar: Salón de capacitaciones CHUCHUQUI Ltda.

CEDULA	NOMBRE/APELLIDO	CARGO	FIRMA
1004003933	Mariela Otavalo	Atención al cliente	
100275711-8	Marco Criollo	Seguridad	
100301846-0	Magdalena Cuacachi Lema	CAJERA	
100339232-9	César Cóndor	Asesor	
100344241-3	Tania Heredia	Crédito	
100242405-5	José Velasquez.	Credito.	

Capacitadores: Darío Castañeda, Marcelo Yamberla, Dony Reina
Seguridad de la Información – Dpto. Tecnología

ANEXO Q: CARTA DE ACEPTACIÓN PARA LA REALIZACIÓN DEL TRABAJO DE GRADO

Impulsamos su desarrollo

Cooperativa de Ahorro y Crédito
De Indígenas "CHUCHUQUÍ" LTDA.
¡Seguridad y experiencia financiera!

Otavalo, 2 de junio del 2016
Oficio Nº CCH-GG-081-2016

Ingeniero
Daniel Jaramillo
DIRECTOR CIERCOM-
UNIVERSIDAD TÉCNICA DEL NORTE
En su despacho.-

De mi consideración:

La Cooperativa de Ahorro y Crédito de Indígenas "CHUCHUQUI" Ltda., **RUC. 1090078263001**, extiende un cordial y afectuoso saludos, deseándoles los mejores éxitos en sus delicadas funciones.

Por medio de la presente, yo, Luis Enrique Cachiguango Cotacachi con C.I. 100124067-8 en calidad de Representante Legal de la Coop. Chuchuqui Ltda, **AUTORIZO** al sr. Dony Anderson Reina López con C.I. 040166573-2 estudiante de la carrera de Ingeniería en Electrónica y Redes de Comunicación de la UTN, para que realice su proyecto de Titulación con el tema: **"Plan de Contingencia para la Cooperativa de Ahorro y Crédito de Indígenas Chuchuqui Ltda, basado en la norma ISO/IEC 27002"** para su efecto tendrá acceso a la información y equipos necesarios, los mismos que utilizará responsablemente y con el debido cuidado.

Particular que pongo en su conocimiento para los fines pertinentes.

Atentamente,

Luis Enrique Cachiguango C.
GERENTE GENERAL
C/copia Archivo

Cooperativa de Ahorro y Crédito "CHUCHUQUI" Ltda. Otavalo - Ecuador

ANEXO R: ACTA DE APROBACIÓN DEL PLAN DE CONTINGENCIA

Viene….

mociona aprobar a que sea remunerada los 15 días adicionales del goce de vacaciones de la Lic. Males, la Sra. Lorena Tuquerrez felicita por los años que viene laborando en la cooperativa, tiempo en el que ha demostrado un alto nivel de profesionalismo al desempeñarse positivamente no solo en este cargo sino también en las coordinaciones generales de cumplimiento de todos los requerimiento de los entes de control, por esta razón apoya la moción, sometida a votación queda aprobada en unanimidad.

7.- Y finalmente en el numeral 7 del orden del día, el Sr. Presidente al no tener más puntos que tratar, da por concluida la presente sesión, siendo las 18H15.

RESUMEN DE RESOLUCIONES

1. En el numeral 1; Se constatación el quórum y se instala de la sesión ordinaria, siendo las 11h15.
2. En el numeral 2; Se aprueba el acta de la sesión anterior con fecha 6 de agosto de 2016.
3. En el numeral 3; Se aprueba la nómina de socios ingresados y retirados desde el 20 de agosto al 9 de septiembre de 2016.
4. En el numeral 4; Se analiza y se aprueba el informe mensual de gerencia
5. En el numeral 5; Se analiza y se aprueba el informe mensual de la unidad de cumplimiento
6. En el numeral 6; Se analiza y se aprueba el pago de vacaciones del periodo 2015 a la Lic. Esthela Males Contadora general.
7. En el numeral 7; Sin más puntos que tratar, se concluye la sesión siendo las 18H15.

Tec. Sebastián Caiza Tocagón
PRESIDENTE

Ing. Maricela Velásquez
SECRETARIA GENERAL

ACTA Nº 318 R (31)

ACTA DE LA SESIÓN EXTRAORDINARIA DEL CONSEJO DE ADMINISTRACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS "CHUCHUQUÍ" LTDA.

"CHUCHUQUÍ" Ltda.
Cooperativa de Ahorro y Crédito

Viene....

En el Salón Pedro Pareja Gonzáles de la Coop. Chuchuqui Ltda., a los veinticuatro días del mes de septiembre del año dos mil dieciséis, siendo las 11h17 (once horas con diecisiete minutos), se reúnen en sesión extraordinaria los miembros del Consejo de Administración, con la presencia de los siguientes señores Directivos: Sra. Lorena Tuquerrez, Ing. Nelly Cabascango, Abg. Cristian Perugachi, Ing. Narcizo Peña bajo la presidencia del Tec. Sebastián Caiza Tocagón, el Sr. Luis Enrique Cachiguango Gerente General y Secretaria quien suscribe a efecto de tratar el siguiente:

ORDEN DEL DÍA

1.- Constatación del Quórum e instalación de la sesión.
2.- Lectura y aprobación de la nómina de socios ingresados y retirados desde el 10 al 23 de septiembre de 2016.
3.- Análisis y aprobación del Plan de Contingencia Informático de la COAC Chuchuqui Ltda.
4.- Análisis y aprobación del Manual Técnico TI "Arquitectura y Procesos de Negocios" de la COAC Chuchuqui Ltda.
5.- Análisis y aprobación de condonaciones de intereses de créditos de las cuentas: 1002449 del Sr. Segundo Peralta Burga y 101114 de la Sra. Burga Bautista Ana Lucia

1.- Iniciando con el numeral 1 del orden del día, el Sr. Presidente Sebastián Caiza solicita que se dé lectura de la nómina del Consejo de Administración a fin de constatar el Quórum, una vez finalizada la lectura se confirma la presencia de todos los miembros del Consejo, siendo así el Sr. Presidente en uso de sus facultades declara instalada la sesión siendo las 11h17.

2.- En el numeral 2 del orden del día, el Sr. Sebastián Caiza Presidente, solicita a la Srta. Secretaria que proceda a dar lectura de los socios ingresados y retirados desde el 10 al 23 de septiembre de 2016, los cuales se presenta en el siguiente cuadro:

HOMBRES	MUJERES	TOTAL CUENTA AHORROS	D. CERTIFICADOS	TOTAL AHORRO
11	10	21	1.050,00	6.265,00

Dando un total en aperturas de 21 cuentas desde el 10 al 23 de septiembre de 2016.

1. CUENTA CHUCHUQUITO TOTAL AHORROS
   3 2.230,80

CIERRES DE CUENTA

Nº	CUENTA	NOMBRES	MOTIVO DE CIERRE	CERTIF.	RETIRO AHORROS	TOTAL RETIRO
1	1002783	Chanalata Maldonado Nancy Amparito	Motivos personales	50,00	21,11	71,11
2	1004676	Concha Chalampuento Laura	Por viaje	30,00	10,31	40,31
3	1005614	Arias Ascanta María Estela	Inmovilizado	30,00	13,74	43,74
4	1008237	Farinango Farinango Lucila	Motivos personales	50,00	384,95	434,95

Viene....

	TOTAL			**160,00**	**430,11**	**590,11**

Fuente: Atención al Cliente "MO"

Culminada la lectura, el Sr. Presidente pone en consideración del Consejo para su respectiva aprobación, toma la palabra la Sra. Lorena Tuquerrez quien manifiesta que en estas semanas hemos tenido buena acogida y felicita a quienes están en esta área por estas nuevas captaciones de socios, y moción a aprobar, esta moción es apoyada por el Ing. Narcizo Peña y sometida a votación es aprobada en unanimidad.

3.- Continuando con el numeral 3 del orden del día, el Sr. Presidente toma la palabra y solicita la intervención de los responsables del área de Tecnología, para que presenten el Plan de Contingencia Informático, por su parte el Ing. Darío Castañeda manifiesta su complacencia por el apoyo que brindan para desempeñarse en esta área cumpliendo con los hallazgos de la SEPS, y cede la palabra la palabra al Ing. Marcelo Yamberla y Sr. Dony Reina (tesista), quienes exponen este instrumento, y manifiestan que para la cooperativa "CHUCHUQUI" Ltda., es indispensable acudir a los recursos de Tecnologías de la Información y Comunicaciones (TICs) como un medio para proporcionar los servicios que la Cooperativa ofrece a la ciudadanía y es de vital importancia que dicha información sea lo más exacta y explícita posible. Además este Plan de Contingencia se basa en la norma ISO/IEC 27002.

Establece el objetivo, alcance y metodología utilizada. Además, incluye las definiciones utilizadas, el análisis de la situación, dominios de seguridad, el análisis de sensibilidad de la información manejada, la identificación de los riesgos y controles, y la clasificación de activos IT.

Culminada la exposición, el Sr. Presidente agradece por la exposición y manifiesta que esta herramienta será muy útil para toda la institución, y pone en consideración del Consejo para su respectiva aprobación, el Ing. Narcizo Peña acota que para el buen funcionamiento de la Cooperativa, es necesario contar con el Plan de Contingencia para poner responder a las posibles situación que se nos presenten a futuro y mociona la aprobación, esta moción es apoyada por la Ing. Nelly Cabascango y sometida a votación es aprobada en unanimidad.

4.- En el numeral 4 del orden del día, el Sr. Presidente toma la palabra y solicita nuevamente la intervención de los responsables del Área de Tecnología a fin de que expongan el Manual Técnico TI "Arquitectura y Procesos de Negocios" de la COAC Chuchuqui Ltda., el Ing. Macelo Yamberla expone que básicamente la arquitectura de Negocio, nos permite tener una visión integral de toda la cooperativa, es decir, da el verdadero norte de cómo mejorar sistemáticamente el funcionamiento de la misma; además plantea el mejor modelo de negocio y su debida configuración de valor, integrando los procesos, la información, aplicativos (sistemas) y la tecnología para

Viene....

Otras costas	
TOTAL DEUDA	1,294.80

En su oficio menciona que por enfermedad de su hija y por su misma salud, al encontrarse en estado delicado, no ha podido cumplir con este crédito, además solicita la condonación de los intereses por mora, y la diferencia del crédito, poder cancelar en su totalidad.

Culminada la exposición, toma la palabra el Sr. Presidente y dejar en consideración de los directivos para su respectiva aprobación, ante esto, el Ing. Narcizo Peña, manifiesta que es importante ayudar a dar solución a los socios y apoyar las gestiones realizadas por el Sr. Gerente, por tanto mociona la condonación de los intereses por mora y recuperar los créditos que se encuentran vencidos, la Ing. Nelly Cabascango apoya esta moción y sometida votación es aprobada en unanimidad.

Una vez tratado todos los puntos de orden del día, el Sr. Presidente en uso de sus facultades declara clausurada la presente sesión extraordinaria, siendo las 18h20.

RESUMEN DE RESOLUCIONES

1. En el numeral 1; Se constata el Quórum y se instala la sesión, siendo las 11H17.
2. En el numeral 2; Se aprueba la nómina de socios ingresados y retirados desde el 10 al 23 de septiembre de 2016.
3. En el numeral 3; Se analiza y se aprueba el Plan de Contingencia Informático de la COAC Chuchuqui Ltda.
4. En el numeral 4; - Se analiza y se aprueba el Manual Técnico TI "Arquitectura y Procesos de Negocios" de la COAC Chuchuqui Ltda.
5.- En el numeral 5; Se analiza y se prueba las condonaciones de intereses de los créditos, de las cuentas: 1002449 del Sr. Segundo Peralta Burga y 101114 de la Sra. Burga Bautista Ana Lucia

Tec. Sebastián Caiza Tocagón
PRESIDENTE

Ing. Maricela Velásquez
SECRETARIA GENERAL

ANEXO S: CARTA DE FINALIZACIÓN DEL TRABAJO DE GRADO

Cooperativa de Ahorro y Crédito
De Indígenas "CHUCHUQUÍ" LTDA.
¡Seguridad y experiencia financiera!
Impulsamos su desarrollo

EN CALIDAD DE JEFE DEL DEPARTAMENTO DE TECNOLOGÍA DE LA COAC CHUCHUQUI LTDA

ME PERMITO

CERTIFICAR

Que, el Sr. DONY ANDERSON REINA LÓPEZ con cédula de ciudadanía No. 040166573-2, culminó satisfactoriamente con sus obligaciones en el desarrollo de su trabajo de grado de tema: **"PLAN DE CONTINGENCIA PARA LA COOPERATIVA DE AHORRO Y CRÉDITO DE INDÍGENAS CHUCHUQUI LTDA., BASADO EN LA NORMA ISO/IEC 27002"**, al igual que su participación en la implementación de controles de seguridad, siguiendo las sugerencias y recomendaciones direccionadas por mi persona.

Se faculta al interesado hacer uso del presente documento como estime conveniente.

Dado en la ciudad de Otavalo a los 31 días del mes de enero de 2017.

Atentamente.

Cooperativa de Ahorro y Crédito Otavalo - Ecuador "CHUCHUQUÍ" Ltda.

Ing. Darío Castañeda

JEFE DEL DEPARTAMENTO DE TECNOLOGIA DE LA COAC CHUCHUQUI LTDA.

ANEXO T: RESUMEN DE IMPLEMENTACIÓN AVALADO POR LA COAC CHUCHUQUI LTDA.

RESUMEN DE MEJORAS DE LA COOAC CHUCHUQUI LTDA., EN BASE A LOS DOMINIOS DE SEGURIDAD DESCRITOS EN LA NORMA ISO/IEC 27002:2013

A continuación, se presenta un resumen de los controles de seguridad que han sido implementados o que se han mejorado en la COAC CHUCHUQUI LTDA., aportando su valor agregado al presente trabajo en coordinación con los miembros del departamento de tecnología. Este resumen se lo realiza especificando los trabajos realizados en cado dominio prescrito por la Norma ISO/IEC 27002 en la cual se encuentra basado este proyecto.

Gestión de incidentes en la seguridad de la información.

Este dominio dio el punto de partida para este trabajo, ya que para dar respuesta a sus directrices se realizó un análisis de riesgos, determinando las fortalezas, oportunidades, debilidades y amenazas según el estado actual de los controles de seguridad en la cooperativa; al igual que se fijaron valoraciones para cada tipo de riesgo dependiendo de la frecuencia con la que estos se presentan.

Políticas de seguridad.

Para el mejoramiento de este dominio se crearon 5 políticas nuevas relacionadas a la seguridad de la información basándose en la norma ISO/IEC 27002, las cuales ya fueron aprobadas por Consejo Directivo y se encuentran puestas en marcha.

Aspectos organizativos de la seguridad de la información.

Se establecieron nuevas responsabilidades y procedimientos relacionados con la seguridad de la información para los miembros del departamento de tecnología de la cooperativa. También se creó una lista de contactos de autoridades y una lista de contactos de grupos de interés especial.

Seguridad ligada a los recursos humanos.

Este dominio se encuentra bien establecido por parte de la cooperativa CHUCHUQUI, pero se hace un llamado de atención en la forma de cómo se realiza el cambio de puesto de trabajo del personal, recomendando tener más seguridad con la

Cooperativa de Ahorro y Crédito Otavalo Ecuador "CHUCHUQUÍ" Ltda.

información a la que tienen acceso los funcionarios.

Gestión de activos.

En este dominio se actualizó el inventario de activos. También se realizó una capacitación explicando las directrices para la clasificación de la información según el manual adoptado por la institución al igual que se indicó el procedimiento para el manejo de los soportes de almacenamiento.

Control de accesos.

Para dar respuesta a este dominio se implementó a nivel de hardware una puerta de seguridad en el centro de datos de la cooperativa, junto con un biométrico para el control de acceso por medio de la empresa SEYTON y a nivel de software se realizó un escaneo de puertos, el cual condujo a la realización del cambio de número de puerto para el protocolo SSH.

Cifrado.

En este dominio se realizó una capacitación del personal sobre cómo manejar las claves de accesos a los sistemas.

Seguridad física y ambiental.

Se mejoró este dominio mediante el incremento de la señalética alrededor de toda la institución, también se mejoró la infraestructura de las oficinas y despachos. También se planteó una solución para la protección de los equipos, de la cual se implementó un sistema de aire acondicionado en el área del centro de datos, además se realizaron cotizaciones para la implementación de gabinetes de pared para los equipos de conexión intermedia.

En la capacitación realizada también se explicó sobre la política de puesto despejado y bloqueo de pantalla, apara los instantes en los que sea necesario dejar el puesto de trabajo desatendido.

Seguridad en la operativa.

Se establecieron directrices y formatos para la gestión de cambios, y la

documentación sobre los procedimientos a seguir en caso de algún incidente.

Seguridad en las telecomunicaciones.

En este dominio se implementó un sistema de monitoreo para los servidores principales de la cooperativa, con la herramienta de NAGIOS. También se planteó el cambio del cableado estructurado de toda la red, para lo cual el departamento de contabilidad ya dispuso un presupuesto económico tentativo para esta propuesta.

Adquisición, desarrollo y mantenimiento de los sistemas de información.

Para este dominio se adquirieron nuevos elementos para distintas áreas que requerían renovación tecnológica, como es la adquisición de un switch Cisco de 24 puertos y un equipo firewall.

Relaciones con suministradores.

En este dominio se establecieron directrices que se deben considerar al momento de gestionar la prestación de servicios por suministradores.

Aspectos de seguridad de la información en la gestión de la continuidad de negocio.

El dominio fue respaldado mediante el establecimiento de un plan de emergencia, un plan de recuperación, un plan de restauración, evaluación y pruebas, y un plan de mantenimiento que nos garantizan la continuidad de la seguridad de la información.

Cumplimiento.

Para este dominio se dejan directrices que ayuden en el cumplimiento de este proyecto, para lo cual Consejo Administrativo aprobó la documentación del Plan de Contingencia en el ACTA No 318. Adicional a esto se recomienda la revisión periódica de las políticas de seguridad y la verificación de su acatamiento.

Atentamente,

Ing. Marcelo Yamberla
ASISTENTE DEL DEPARTAMENTO DE TECNOLOGIA
DE LA COAC CHUCHUQUI LTDA.

Cooperativa de Ahorro y Crédito "CHUCHUQUI" Ltda. Otavalo Ecuador

Recibido
2017-03-21

ANEXO U: CERTIFICADOS DE REUNIONES

Cooperativa de Ahorro y Crédito
De Indígenas "CHUCHUQUÍ" LTDA.
¡Seguridad y experiencia financiera!
Impulsamos su desarrollo

EN CALIDAD DE ASISTENTE DEL DEPARTAMENTO DE TECNOLOGÍA DE LA COAC CHUCHUQUI LTDA
ME PERMITO

CERTIFICAR

Que, el día lunes 1 de agosto de 2016 en el Salón de Capacitaciones CHUCHUQUI Ltda., se reunieron los miembros del Departamento de Tecnología en conjunto con el Sr. Dony Reina (tesista), para establecer un formato para el levantamiento de la información sobre la situación actual de la institución y determinar una estructura adecuada para el Plan de Contingencia.

Se faculta al interesado hacer uso del presente documento como estime conveniente.

Dado en la ciudad de Otavalo a los 21 días del mes de marzo de 2017.

Atentamente

Cooperativa de Ahorro y Crédito
Otavalo Ecuador
"CHUCHUQUÍ" Ltda.

Ing. Marcelo Yamberla
ASISTENTE DEL DEPARTAMENTO DE TECNOLOGIA
DE LA COAC CHUCHUQUI LTDA.

Cooperativa de Ahorro y Crédito
De Indígenas "CHUCHUQUÍ" LTDA.
¡Seguridad y experiencia financiera!
Impulsamos su desarrollo

EN CALIDAD DE ASISTENTE DEL DEPARTAMENTO DE TECNOLOGÍA DE LA COAC CHUCHUQUI LTDA
ME PERMITO

CERTIFICAR

Que, el día martes 9 de agosto de 2016 en el Salón de Capacitaciones CHUCHUQUI Ltda., se reunieron los miembros del Departamento de Tecnología en conjunto con el Sr. Dony Reina (tesista), para analizar el levantamiento de la situación actual de la institución e identificar los escenarios de incidentes que van a ser tratados en el Plan de Contingencia.

Se faculta al interesado hacer uso del presente documento como estime conveniente.

Dado en la ciudad de Otavalo a los 21 días del mes de marzo de 2017.

Atentamente

Cooperativa de Ahorro y Crédito Otavalo Ecuador "CHUCHUQUÍ" Ltda.

Ing. Marcelo Yamberla
ASISTENTE DEL DEPARTAMENTO DE TECNOLOGIA
DE LA COAC CHUCHUQUI LTDA.