UNIVERSIDAD
NACIONAL
DE LOJA

PFC- CIS-UNL

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"LEVANTAMIENTO, DEFINICIÓN Y FORMALIZACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA"

Tesis previa a la obtención del título de Ingeniera en Sistemas

AUTOR:

Maritza Lorena Cuenca Capa

DIRECTOR:

Ing. Carlos Miguel Jaramillo Castro, Mg. Sc

LOJA-ECUADOR
2016

CERTIFICACIÓN DEL DIRECTOR

Loja, 16 de diciembre de 2016

Ing. Carlos Miguel Jaramillo Castro, Mg. Sc

DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES DE LA UNIVERSIDAD NACIONAL DE LOJA.

CERTIFICA:

Que la señorita Maritza Lorena Cuenca Capa, egresada de la carrera de Ingeniería en Sistemas y cuyo tema de trabajo de titulación versa sobre **"LEVANTAMIENTO, DEFINICIÓN Y FORMALIZACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA",** ha sido monitoreado, revisado y orientado bajo mi asesoramiento, con pertinencia y con la rigurosidad científica que el trabajo de investigación debe cumplir, por lo cual autorizo su presentación y sustentación.

Ing. Carlos Miguel Jaramillo Castro, Mg. Sc

DIRECTOR DEL TRABAJO DE TITULACIÓN

AUTORÍA

Yo **MARITZA LORENA CUENCA CAPA**, declaro ser autora del presente trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas denominado **"LEVANTAMIENTO, DEFINICIÓN Y FORMALIZACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA"**, y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi trabajo de titulación en el repositorio Institucional-Biblioteca Virtual.

Autor: Maritza Lorena Cuenca Capa

Firma: _____

Cédula: 1104861438

Fecha: 30 de marzo de 2017

CARTA DE AUTORIZACIÓN

CARTA DE AUTORIZACIÓN DEL TRABAJO DE TITULACIÓN POR PARTE DE LA AUTORA, PARA LA CONSULTA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo, **MARITZA LORENA CUENCA CAPA**, declaro ser la autora del trabajo de titulación denominado: **"LEVANTAMIENTO, DEFINICIÓN Y FORMALIZACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA";** autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de titulación que realice un tercero.

Para constancia de esta autorización, en la cuidad de Loja a los treinta días del mes de marzo del dos mil diecisiete.

Firma: 

Autora: Maritza Lorena Cuenca Capa

Cédula: 1104861438

Dirección: Barrio Pucacocha

Correo Electrónico: maritza221cc@gmail.com

Celular: 0969143567

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Carlos Miguel Jaramillo Castro, Mg. Sc.

Tribunal de Grado: Ing. Alex Vinicio Padilla Encalada, Mg. Sc.

Ing. Valeria del Rosario Herrera Salazar, Mg. Sc.

Ing. Jorge Tulio Carrión González, Mg. Sc.

AGRADECIMIENTO

Agradezco de manera especial, a la Universidad Nacional de Loja, noble institución que nos ha alojado, como nuestro segundo hogar y nos ha permitido, tener el prestigio de estudiar en ella y formarnos como profesionales y mejores personas, para bien de nuestro país y toda nuestra colectividad Lojana.

De la misma manera, agradezco a cada uno de los docentes, que conforman la carrera de Ingeniería de Sistemas de la Facultad de Energía las Industrias y los Recursos Naturales no Renovables, quienes con su dedicación, paciencia y empeño supieron inculcar en mí el conocimiento necesario, que hoy me permite culminar con nuestra formación académica e incluirnos en el mundo profesional.

De manera especial, al docente Carlos Jaramillo, por su apoyo brindado en la cristalización del presente trabajo de titulación y tan acertada dirección de la misma.

Por último, contribuyo el siguiente trabajo de titulación, a todas las personas que intervinieron de forma directa e indirecta en el cumplimiento de este trabajo y que gracias a ellos, hoy tengo la oportunidad de lograr un objetivo más en mi vida.

DEDICATORIA

El presente trabajo de titulación, está dedicado a Dios y a la Santísima Virgen del Cisne, por haberme dado la vida y permitirme llegar hasta este momento tan importante de mi formación profesional.

A mis padres, Mercedes y Luis, por el apoyo incondicional que me brindan en todo momento, por sus sabios consejos que me han permitido ser una persona de bien, pero más que nada, por su amor, de igual manera a mis hermanos Karina, Jessica y Rene y a mi cuñado Ángel Omar por su apoyo y comprensión.

Con mucho cariño, a mi esposo Wilman Patricio y a mis dos hermosos hijos, Kiara y Sebastián por su incondicional apoyo, amor y comprensión, que han sido mi motivo de superación, y a todas aquellas personas que participaron directa o indirectamente en la elaboración de este trabajo de titulación.

Maritza Lorena

ÍNDICE DE CONTENIDOS

CERTIFICACIÓN DEL DIRECTOR I

AUTORÍA III

CARTA DE AUTORIZACIÓN IV

AGRADECIMIENTO V

DEDICATORIA VI

ÍNDICE DE CONTENIDOS VII

ÍNDICE DE FIGURAS XVII

ÍNDICE DE TABLAS XIX

a. TÍTULO 1

b. RESUMEN 2

ABSTRACT 3

c. INTRODUCCIÓN 4

d. REVISIÓN DE LITERATURA 6

1. HISTORIA DE LA UNIVERSIDAD NACIONAL DE LOJA 6

1.1. Misión, Visión y Objetivos de la Universidad Nacional de Loja 6

1.2. UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN 7

1.2.1. Misión 7

1.2.2. Atribuciones y Responsabilidades 7

1.2.3. Productos y Servicios 9

1.2.3.1. Desarrollo de Software 9

1.2.3.2. Redes y Equipos Informáticos 10

1.2.3.3. Electrónica y Telecomunicaciones 10

2. SEGURIDAD DE LA INFORMACIÓN 11

2.1. Diferencia entre seguridad de la información y seguridad informática 11

2.2. Importancia y beneficios de la seguridad en las organizaciones 13

2.3. ¿Qué es un fallo de seguridad? 14

3. ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 14

3.1. ISO (Organización Internacional de Estándares) 14
3.2. Norma ISO/IEC 27001:2013 15
3.3. Norma ISO/IEC 27002:2013 15
4. PROCESOS 16
4.1. Definición de proceso 16
4.2. Características de los procesos 16
4.3. Elementos de los procesos 17
4.4. Clasificación de los procesos 18
5. GESTIÓN DE PROCESOS 18
5.1. Metodologías de la gestión de procesos 19
5.1.1. Metodología SIPOC (Suppliers-Inputs-Process-Outputs-Customers) 19
5.1.1.1. SIPOC significa 20
5.1.1.2. Preparando el Sipoc 20
5.1.1.3. Beneficios 20
5.1.1.4. Aplicaciones de la metodología en base al ciclo PHVA 21
5.1.1.5. Empresa que han usado la metodología sipoc en base al ciclo PHVA 21
5.1.2. Metodología TORTUGA 21
5.1.3. Metodología PULPO 22
5.1.4. Ventajas y Desventajas de las Metodologías de gestión 22
5.1.5. Comparativa de las Metodologías de gestión 23
6. MEJORA CONTINUA 24
7. DIAGRAMAS PARA LA MODELACIÓN DE PROCESOS 25
7.1. Diagramas de flujo 25
7.2. Diagramas sipoc 26
7.3. Diagramas Bpmn 26
8. ESTANDAR BPMN 26
8.1. BPMN 26
8.2. Características 27
8.3. Modelación de procesos 28
8.4. Elementos de los diagramas 28
e. MATERIALES Y MÉTODOS 30

1. MATERIALES 30
2. MÉTODOS Y TÉCNICAS 32
2.1. MÉTODOS 32
2.2. TÉCNICAS 33
2.3. METODOLOGÍA SIPOC (*Suppliers-Inputs-Process-Outputs-Customers*) 33
f. RESULTADOS 36
FASE 1: Diagnosticar la situación actual de la unidad de Telecomunicaciones e Información sobre los procesos de seguridad de la información. 36
1.1. Recopilar información mediante la encuesta, referente a los procesos existentes de seguridad de la información 36
1.2. Realizar la tabulación de acuerdo a las encuestas obtenidas 38
1.3. Analizar la información recolectada para la determinación de la situación actual dentro de la UTI, que permite determinar la definición de los procesos de seguridad de la información más primordiales 43
FASE 2: Levantamiento de los procesos de seguridad de la información 47
2.1. Determinar los procesos que se están ejecutando actualmente en la Unidad de Telecomunicaciones e Información 47
2.2. LEVANTAMIENTO DE PROCESOS 48
2.2.1. LEVANTAMIENTO DEL PROCESO CLASIFICACIÓN DE LA INFORMACIÓN 48
2.2.1.1. Requisitos y Documentación 48
2.2.1.2. Actores 48
2.2.1.3. Descripción de Actividades 48
2.2.2. LEVANTAMIENTO DEL SUBPROCESO DIRECTRICES DE CLASIFICACIÓN 49
2.2.2.1. Requisitos y Documentación 49
2.2.2.2. Actores 49
2.2.2.3. Descripción de Actividades 49
2.2.3. LEVANTAMIENTO DEL SUBPROCESO ETIQUETADO Y MANIPULADO DE LA INFORMACIÓN 49
2.2.3.1. Requisitos y Documentación 49
2.2.3.2. Actores 49
2.2.3.3. Descripción de Actividades 49

2.2.4. LEVANTAMIENTO DEL PROCESO GESTIÓN DE ACCESO DE USUARIOS 50
2.2.4.1. Requisitos y Documentación 50
2.2.4.2. Actores 50
2.2.4.3. Descripción de Actividades 50
2.2.5. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DE APLICACIONES INTERNAS 50
2.2.5.1. Requisitos y Documentación 50
2.2.5.2. Actores 51
2.2.5.3. Descripción de Actividades 51
2.2.6. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS DE APLICACIONES INTERNAS 52
2.2.6.1. Requisitos y Documentación 52
2.2.6.2. Actores 52
2.2.6.3. Descripción de Actividades 52
2.2.7. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DE BASE DE DATOS 53
2.2.7.1. Requisitos y Documentación 53
2.2.7.2. Actores 53
2.2.7.3. Descripción de Actividades 53
2.2.8. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS DE BASES DE DATOS 54
2.2.8.1. Requisitos y Documentación 54
2.2.8.2. Actores 54
2.2.8.3. Descripción de Actividades 54
2.2.9. LEVANTAMIENTO DEL SUBPROCESO BLOQUEO DE USUARIOS DE BASES DE DATOS 54
2.2.9.1. Requisitos y Documentación 54
2.2.9.2. Actores 54
2.2.9.3. Descripción de Actividades 55
2.2.10. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DE SISTEMAS OPERATIVOS 55
2.2.10.1. Requisitos y Documentación 55
2.2.10.2. Actores 55

2.2.10.3. Descripción de Actividades 55
2.2.11. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS DE SISTEMAS OPERATIVOS 56
2.2.11.1. Requisitos y Documentación 56
2.2.11.2. Actores 57
2.2.11.3. Descripción de Actividades 57
2.2.12. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DEL SISTEMA DE GESTIÓN ACADÉMICA 58
2.2.12.1. Requisitos y Documentación 58
2.2.12.2. Actores 58
2.2.12.3. Descripción de Actividades 58
2.2.13. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS DEL SISTEMAS DE GESTIÓN ACADÉMICA 59
2.2.13.1. Requisitos y Documentación 59
2.2.13.2. Actores 59
2.2.13.3. Descripción de Actividades 59
2.2.14. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DE CUENTAS DE CORREO ELECTRÓNICO INSTITUCIONAL 60
2.2.14.1. Requisitos y Documentación 60
2.2.14.2. Actores 60
2.2.14.3. Descripción de Actividades 61
2.2.15. LEVANTAMIENTO DEL PROCESO SUSPENSIÓN DE CUENTAS DE USURIOS DE CORREO ELECTRÓNICO INSTITUCIONAL 61
2.2.15.1. Requisitos y Documentación 61
2.2.15.2. Actores 62
2.2.15.3. Descripción de Actividades 62
2.2.16. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS A NIVEL DE SERVIDORES 63
2.2.16.1. Requisitos y Documentación 63
2.2.16.2. Actores 63
2.2.16.3. Descripción de Actividades 63
2.2.17. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS A NIVEL DE SERVIDORES 63
2.2.17.1. Requisitos y Documentación 63

2.2.17.2. Actores 64
2.2.17.3. Descripción de Actividades 64
2.2.18. LEVANTAMIENTO DEL PROCESO GESTIÓN DE CONTRASEÑAS DE USUARIOS 64
2.2.18.1. Requisitos y Documentación 64
2.2.18.2. Actores 64
2.2.18.3. Descripción de Actividades 64
2.2.19. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE LAS CONTRASEÑAS 65
2.2.19.1. Requisitos y Documentación 65
2.2.19.2. Actores 65
2.2.19.3. Descripción de Actividades 65
2.2.20. LEVANTAMIENTO DEL SUBPROCESO RESETEO DE CONTRASEÑAS 65
2.2.20.1. Requisitos y Documentación 65
2.2.20.2. Actores 66
2.2.20.3. Descripción de Actividades 66
2.2.21. LEVANTAMIENTO DEL SUBPROCESO RESETEO DE CONTRASEÑAS ON-LINE 67
2.2.21.1. Requisitos y Documentación 67
2.2.21.2. Actores 67
2.2.21.3. Descripción de Actividades 67
2.2.22. LEVANTAMIENTO DE SUBPROCESO USO DE LAS CONTRASEÑAS 68
2.2.22.1. Requisitos y Documentación 68
2.2.22.2. Actores 68
2.2.22.3. Descripción de Actividades 68
2.2.23. LEVANTAMIENTO DEL PROCESO COPIAS DE SEGURIDAD 68
2.2.23.1. Requisitos y Documentación 68
2.2.23.2. Actores 69
2.2.23.3. Descripción de Actividades 69
2.2.24. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE RESPALDOS 69
2.2.24.1. Requisitos y Documentación 69
2.2.24.2. Actores 69

2.2.24.3. Descripción de Actividades 69
2.2.25. LEVANTAMIENTO DEL SUBPROCESO CODIFICACIÓN DE RESPALDOS 70
2.2.25.1. Requisitos y Documentación 70
2.2.25.2. Actores 70
2.2.25.3. Descripción de Actividades 70
2.2.26. LEVANTAMIENTO DEL SUBPROCESO ALMACENAMIENTO DE RESPALDOS 70
2.2.26.1. Requisitos y Documentación 70
2.2.26.2. Actores 70
2.2.26.3. Descripción de Actividades 70
2.2.27. LEVANTAMIENTO DEL SUBPROCESO PRUEBAS DE RESPALDOS 71
2.2.27.1. Requisitos y Documentación 71
2.2.27.2. Actores 71
2.2.27.3. Descripción de Actividades 71
2.2.28. LEVANTAMIENTO DEL SUBPROCESO PROCEDIMIENTOS DE RECUPERACIÓN 72
2.2.28.1. Requisitos y Documentación 72
2.2.28.2. Actores 72
2.2.28.3. Descripción de Actividades 72
FASE 3: DEFINICIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN 73
3.1. Definir los procesos de seguridad de la información más esenciales dentro de la Unidad de Telecomunicaciones e Información 73
3.2. Propuesta de los procesos de seguridad de la información 73
PROCESO PADRE: GESTIÓN DE ACTIVOS 73
PROCESO 1: CLASIFICACIÓN DE LA INFORMACIÓN 73
1.1. Requisitos y Documentación 73
1.2. Actores 74
1.3. Descripción de Actividades 74
1.4. Diagramas 75
1.5. Documentación 77
PROCESO 2: ENTREGA DE INFORMACIÓN EN MEDIOS DE ALMACENAMIENTO 78

2.1. Requisitos y Documentación ... 78
2.2. Actores ... 78
2.3. Descripción de Actividades ... 78
2.4. Diagramas ... 81
2.5. Documentación ... 83
PROCESO PADRE: CONTROL DE ACCESOS ... 84
PROCESO 3: CONTROL DE ACCESOS FÍSICOS A LAS INSTALACIONES DE LA UTI ... 84
3.1. Requisitos y Documentación ... 84
3.2. Actores ... 85
3.3. Descripción de Actividades ... 85
3.4. Diagramas ... 87
3.5. Documentación ... 89
PROCESO 4: GESTIÓN DE ACCESO DE USUARIOS ... 90
4.1. Requisitos y Documentación ... 90
4.2. Actores ... 91
4.3. Descripción de Actividades ... 91
4.4. Diagramas ... 93
4.5. Documentación ... 95
P4-SUBPROCESO 1: CREACIÓN DE USUARIOS ... 96
4.1.1. Requisitos y Documentación ... 96
4.1.2. Actores ... 96
4.1.3. Descripción de Actividades ... 97
4.1.4. Diagramas ... 99
4.1.5. Documentación ... 101
P4-SUBPROCESO 2: MODIFICACIÓN DE USUARIOS ... 103
4.2.1. Requisitos y Documentación ... 103
4.2.2. Actores ... 103
4.2.3. Descripción de Actividades ... 103
4.2.4. Diagramas ... 105
4.2.5. Documentación ... 107

P4-SUBPROCESO 3: BLOQUEO DE USUARIOS Y SUSPENSIÓN DE CUENTAS DE USUARIOS 108
4.3.1. Requisitos y Documentación 108
4.3.2. Actores 108
4.3.3. Descripción de Actividades 109
4.3.4. Diagramas 111
4.3.5. Documentación 113
PROCESO 5: CONTROL DE ACCESO A SISTEMAS Y APLICACIONES 114
5.1. Requisitos y Documentación 114
5.2. Actores 115
5.3. Descripción de Actividades 115
5.4. Diagramas 118
5.5. Documentación 120
PROCESO PADRE: SEGURIDAD EN LA OPERATIVA 122
PROCESO 6: GENERAR COPIAS DE SEGURIDAD 122
6.1. Requisitos y Documentación 122
6.2. Actores 122
6.3. Descripción de Actividades 122
6.4. Diagramas 124
6.5. Documentación 126
PROCESO PADRE: SEGURIDAD EN LAS TELECOMUNICACIONES 127
PROCESO 7: ENTREGA DE INFORMACIÓN CON PARTES EXTERNAS 127
7.1. Requisitos y Documentación 127
7.2. Actores 127
7.3. Descripción de Actividades 127
7.4. Diagramas 131
7.5. Documentación 133
4.1. Validación de los procesos con sus respectivos responsables 135
FASE 5: FORMALIZACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN POR EL DIRECTOR DE LA UTI Y EL ADMINISTRADOR DE LA SEGURIDAD DE LA INFORMACIÓN 139
g. DISCUSIÓN 140

h. CONCLUSIONES 142
i. RECOMENDACIONES 143
j. BIBLIOGRAFÍA 144

ÍNDICE DE FIGURAS

Figura 1: Seguridad de la información vs seguridad informática……11

Figura 2: Pilares fundamentales de la seguridad de la información……13

Figura 3: Esquema general Sipoc……...17

Figura 4: Esquema general de tortuga…….. 19

Figura 5: Esquema general de pulpo……..22

Figura 6: Elementos del proceso……..22

Figura 7: Ciclo PHVA…… 24

Figura 8: Diagrama de flujo……..25

Figura 9: Diagrama Sipoc…… 26

Figura 10: Formato de proceso……40

Figura 11: Procesos existentes en la UTI……..40

Figura 12: Límite de tiempo por proceso……...43

Figura 13: Circulación de la información……44

Figura 14: Diagrama resumido del proceso definido clasificación de la información…….76

Figura 15: Diagrama detallado del proceso definido clasificación de la información……77

Figura 16: Diagrama resumido del proceso definido entrega de información en medios de almacenamiento…….82

Figura 17: Diagrama detallado del proceso definido entrega de información en medios de almacenamiento…….83

Figura 18: Diagrama resumido del proceso definido control de accesos físicos a las instalaciones de la UTI……..88

Figura 19: Diagrama detallado del proceso definido control de accesos físicos a las instalaciones de la UTI……89

Figura 20: Diagrama resumido del proceso definido gestión de accesos de usuarios……94

Figura 21: Diagrama detallado del proceso definido gestión de accesos de usuarios……95

Figura 22: Diagrama resumido del subproceso definido creación de usuarios…….. 100

Figura 23: Diagrama detallado del subproceso definido creación de usuarios……...101

Figura 24: Diagrama resumido del subproceso definido modificación de usuarios……..106

Figura 25: Diagrama detallado del subproceso definido modificación de usuarios……...107

Figura 26: Diagrama resumido del subproceso definido bloqueo de usuarios y suspensión de cuentas de usuarios……112

Figura 27: Diagrama detallado del subproceso definido bloqueo de usuarios y suspensión de cuentas de usuarios……113

Figura 28: Diagrama resumido del proceso definido control de accesos a sistemas y aplicaciones ……..119

Figura 29: Diagrama detallado del proceso definido control de accesos a sistemas y aplicaciones…….. 120

Figura 30: Diagrama resumido del proceso definido generar copias de seguridad…….. 125

Figura 31: Diagrama detallado del proceso definido generar copias de seguridad……126

Figura 32: Diagrama resumido del proceso definido entrega de la información con partes externas……..132

Figura 33: Diagrama detallado del proceso definido entrega de la información con partes externas……..133

ÍNDICE DE TABLAS

Tabla I: Ventajas y desventajas de las metodologías de gestión……17

Tabla II: Comparativas de las metodologías……...22

Tabla III: Características de los procesos……23

Tabla IV: Elementos de los diagramas BPMN……28

Tabla V: Identificación de actores……35

Tabla VI: Descripción de actividades……...35

Tabla VII: Actividades de seguridad de la información……..41

Tabla VIII: Dominios y objetivos de control a ser definidos……..46

Tabla IX: Controles a ser definidos y controles actuales de la UTI……46

Tabla X: Actores del proceso clasificación de la información……75

Tabla XI: Actores del proceso entrega de información en medios de almacenamiento…..79

Tabla XII: Actores del proceso control de accesos físicos a las instalaciones de la UTI…..86

Tabla XIII: Actores del proceso gestión de acceso de usuarios……92

Tabla XIV: Actores del subproceso creación de usuarios……97

Tabla XV: Actores del subproceso modificación de usuarios……104

Tabla XVI: Actores del subproceso bloqueo de usuarios y suspensión de cuentas de usuarios……..109

Tabla XVII: Actores del proceso control de accesos a sistemas y aplicaciones……..116

Tabla XVIII: Actores del proceso generar copias de seguridad……123

Tabla XIX: Actores del proceso entrega de información con partes externas……128

a. TÍTULO

"LEVANTAMIENTO, DEFINICIÓN Y FORMALIZACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA"

b. RESUMEN

En la actualidad, uno de los bienes más importantes, para cualquier tipo de institución u organización es la información, por lo tanto, su gestión y administración son claves para preservar la confidencialidad, integridad y disponibilidad, lo cual, debe de contar con la protección adecuada que garantice el resguardo de dichas características.

Partiendo de lo mencionado, se ha determinado el enfoque del presente trabajo de titulación, que busca proporcionar medidas de control y gestión para la protección de los activos de información, que son propiedad de la Universidad Nacional de Loja, gestionados desde la Unidad de Telecomunicaciones e Información.

El desarrollo del presente trabajo de titulación, trata sobre el levantamiento, definición y formalización de los procesos de seguridad de la información, en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, usando como marco de referencia, la norma ISO/IEC 27002:2013, la cual, nos permitió ver los procesos más esenciales y críticos dentro de la Unidad de Telecomunicaciones e Información, así mismo, se utilizó la metodología SIPOC (SUPPLIERS, INPUTS, PROCESS, OUTPUTS, CUSTOMERS) para la definición y gestión de los procesos, permitiendo aplicar el ciclo de mejora continua PHVA (Planificar, Hacer, Verificar, Actuar) que se encuentra dentro de la metodología, para poder definir los límites de los procesos, así como su punto de inicio y final de los mismos.

Al finalizar el desarrollo del presente trabajo de titulación, se realizó la respectiva formalización y socialización de los procesos de seguridad de la información, con el director y el administrador de seguridad de la información de la Unidad de Telecomunicaciones e Información, como solución para la mitigación de los riesgos asociados a los activos de información que son de propiedad de la Universidad Nacional de Loja.

ABSTRACT

At present, one of the most important assets for any kind of institution is information, therefore, information management is paramount to preserve confidentiality, integrity and availability, which must be protection to ensure the features.

The approach of the present research seeks to manage the protection of information assets of property of Universidad Nacional de Loja, managed by the Telecommunications and Information Unit.

This investigation deals with the gathering, definition and formalization of information security processes inside the Telecommunications and Information Unit of Universidad Nacional de Loja, ISO / IEC 27002: 2013 standard is used as a reference framework, using the SIPOC methodology (Suppliers, Inputs, Process, Outputs, Customers) to define and manage the processes, allowing the PDCA (Plan-Do-Check-Act) cycle to be applied continuously within regulations.

Finally, e information security processes were formalized with the Unit officials, the director and the information security administrator of the Telecommunications and Information Unit.

c. INTRODUCCIÓN

Hoy en día, muchas empresas e instituciones invierten en tecnología, con el fin de satisfacer sus necesidades y la de sus clientes, y además de tener un mejor control sobre sus operaciones y procesos. Dado que la seguridad de la información es uno de los aspectos críticos, que más preocupa al área de Tecnología de la Información, es por esto, que se necesita tener una gestión clara, para poder definir los procesos en cada una de las diferentes áreas.

Así mismo la mayoría de las empresas e instituciones, toman medidas de protección que garanticen el control de su información y que mitiguen los potenciales riesgos que la puedan impactar. Por ende aparecen una serie de exigencias, que obligan a las instituciones, a definir una serie de procesos de seguridad de la información, puesto que, no llevan un apropiado esquema de sus procesos, así mismo, no tienen un adecuado conocimiento de cómo implementar mecanismo para la seguridad de la información.

Es por ello, que la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, no cuenta con una formalización de procesos, ni gestión de seguridad de la información, impidiendo que se realice la debida gestión de los mismos y así dando lugar a los siguientes problemas:

- No cuentan con procesos formalizados, ni normas de seguridad de información.
- No tienen conocimiento de cómo implementar mecanismos óptimos para el manejo de la seguridad de la información.
- No poseen un lineamiento general para la gestión de procesos.

Así mismo, dando lugar a los siguientes efectos:

- No cuentan con una gestión adecuada de la integridad, disponibilidad y confiabilidad de la información de los servicios que presta la Unidad de Telecomunicaciones e Información.
- No poseen una fuente general formalizada de consulta, acerca de los Procesos de Seguridad de la Información y las actividades de

cada uno de ellos, para que el usuario final pueda conocerlos y cumplirlos.

- El administrador de seguridad de información, no puede realizar la gestión respectiva de los procesos de seguridad de la información a su cargo.
- La falta de procesos formalizados en Seguridad de la Información, impide poder implementar un modelo de Sistema de Gestión de Seguridad de la Información.

En base a la problemática antes mencionada, se elaboró una propuesta formal dirigida al Director de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, para trabajar en los procesos de seguridad de la información donde se levantará, se definirá y se formalizarán los mismos, teniendo como referencia la metodología SIPOC y la norma ISO/IEC 27002:2013.

Dando lugar a los siguientes objetivos:

- Diagnosticar la situación actual de la Unidad de Telecomunicaciones e Información sobre los procesos de seguridad de la información.
- Levantar los procesos de seguridad de la información en la Unidad de Telecomunicaciones e Información.
- Definir los procesos de seguridad de la información en la Unidad de Telecomunicaciones e Información.
- Validar los procesos de seguridad de la información en la Unidad de Telecomunicaciones e Información.
- Formalizar los procesos de seguridad de la información por el Director y el administrador de la Seguridad de la Información de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja.

d. REVISIÓN DE LITERATURA

1. HISTORIA DE LA UNIVERSIDAD NACIONAL DE LOJA

La Universidad Nacional de Loja, es una Institución de Educación Superior, laica, autónoma, de derecho público, con personería jurídica y sin fines de lucro, de alta calidad académica y humanística, que ofrece formación en los niveles: técnico y tecnológico superior; profesional o de tercer nivel; y, de postgrado o cuarto nivel; que realiza investigación científico-técnica sobre los problemas del entorno, con calidad, pertinencia y equidad, a fin de coadyuvar al desarrollo sustentable de la región y del país, interactuando con la comunidad, generando propuestas alternativas a los problemas nacionales, con responsabilidad social; reconociendo y promoviendo la diversidad cultural y étnica y la sabiduría popular, apoyándose en el avance científico y tecnológico, en procura de mejorar la calidad de vida del pueblo ecuatoriano.[1]

1.1. Misión, Visión y Objetivos de la Universidad Nacional de Loja

1.1.1. Misión

Es misión de la Universidad Nacional de Loja: la formación académica y profesional, con sólidas bases científicas y técnicas, pertinencia social y valores; la generación y aplicación de conocimientos científicos, tecnológicos y técnicos, que aporten al desarrollo integral del entorno y al avance de la ciencia; el fortalecimiento del pensamiento, la promoción, desarrollo y difusión de los saberes y culturas; y, la prestación de servicios especializados. [1]

1.1.2. Visión

La Universidad Nacional de Loja tiene como visión, consolidarse como una Comunidad Educativa, con excelencia académica, humanista y democrática, líder en el desarrollo de la cultura, la ciencia y la tecnología. [1]

1.1.3. Objetivos estratégicos

- Formar talento humano de calidad, con sólidas bases científicas, técnicas y humanísticas, que correspondan a las necesidades del desarrollo local, regional y nacional, en el marco de los lineamientos de Sistema de Educación Superior y de un permanente proceso de evaluación.
- Generar conocimientos científicos, innovar tecnologías y potenciar los conocimientos tradicionales, que enriquezcan los procesos de formación y coadyuven a resolver los principales problemas del desarrollo regional y nacional.
- Construir a la Universidad Nacional de Loja, en espacio académico y de interacción social, que produzca pensamientos y propuestas para el desarrollo de la región; que promocione y difunda nuestras culturas y oferte a la colectividad servicios especializados en calidad.[1]

1.2. UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

1.2.1. Misión

Administrar tecnología de información y proveer servicios informáticos y de comunicaciones para el proceso de datos y acceso a información, así como investigar e implementar tecnología de punta que garantice la disponibilidad, integridad y confiabilidad de la información.

1.2.2. Atribuciones y Responsabilidades

- Participar en la elaboración de estudios y diseños de redes.
- Coordinar actividades relacionadas con el mejoramiento de la infraestructura técnica de la Universidad: Redes de portadores, servicios de óptima calidad.
- Coordinar actividades con áreas relacionadas en el mejoramiento de la tecnología y capacitación: Ingeniería en Electrónica y Telecomunicaciones, Ingeniería de Sistemas.

- Actualizar licencias y permisos de operación, tanto de redes de telecomunicaciones como redes informáticas.
- Coordinar y supervisar todos los requerimientos de Software y Conectividad, así como las necesidades de Video Conferencia y Teleducación de la MED.
- Coordinar y supervisar los proyectos TIC's (TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN), en especial de TELEMEDICINA y TELEDUCACIÓN, TELEMETRÍA y VIDEO CONFERENCIAS.
- Realizar la planificación de redes de telecomunicaciones con sus respectivos componentes, memorias técnicas, diseños, detalles constructivos, especificaciones técnicas de cada uno de los proyectos.
- Elaborar estudios de perfeccionamiento del software y redes que brindan servicios de telecomunicaciones e información a la ciudad universitaria, para el ordenamiento e integración, mediante propuestas de conectividad en sus diferentes modalidades: fibra óptica, micro-onda, satelital.
- Planificar y controlar la instalación y el adecuado funcionamiento de los servicios de Internet.
- Elaborar proyectos de expansión de servicios hacia zonas de interés de la Universidad que requieren conectividad: internet, telefonía, telemetría, video conferencia, etc.
- Realizar términos referenciales y pliegos de consultoría para la contratación de estudios de telecomunicaciones y electrónicos.
- Planificación, diseño, implementación y monitoreo para la optimización de los servicios de gestión académica.
- Capacitar a los usuarios en el manejo tanto de software adquirido como del software desarrollado por la sección.
- Establecer las políticas de seguridad y respaldo de los sistemas informáticos de la institución.
- Planificación y distribución adecuada de los diferentes anchos de banda para los servicios de Internet e intranet.
- Proveer de soporte técnico a todas las redes de equipos electrónicos que operan en la Universidad, esto es: sistemas de computación, equipos de

transmisión-recepción (sistemas de micro-ondas, radiodifusión, Televisión), equipos de fibra óptica, ruteadores, switches, etc.

- Realizar la instalación, mantenimiento preventivo y correctivo; y reparación de los sistemas y equipos de telecomunicaciones e informáticos de la UNL.

1.2.3. Productos y Servicios

1.2.3.1. Desarrollo de Software

- Estudio de perfeccionamiento del software que maneja la Universidad en sus diferentes áreas, centros especializados y departamentos.
- Pliegos para la adquisición o contratación de diseños o desarrollos de software especializado, en base a la planificación o proyectos aprobados.
- Planes de diseño, implementación y monitoreo para la optimización de los servicios de gestión académica. Planes de perfeccionamiento y control de los diferentes paquetes de software que manejan cada una de las áreas.
- Diseño de software para la automatización y control de los procesos académicos administrativos de la Universidad: Estadísticas, trámites, archivo.
- Informes de soporte técnico y mantenimiento de software otorgado a todos los sistemas que se encuentran en ejecución en las áreas, centros especializados y unidades universitarias.
- Fichas técnicas del apoyo en software realizado a la Carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, para prácticas educativas.
- Planes de adquisición de software e implementación del hardware adquirido como del software desarrollado por la subunidad. Informes de aplicación de las políticas de seguridad y respaldo de los sistemas informativos de la institución.

1.2.3.2. Redes y Equipos Informáticos

- Planes de diseño y perfeccionamiento de las redes y equipos informáticos de la Universidad en sus diferentes Áreas, Centros Especializados y Departamentos.
- Informes de mantenimiento del servicio de Internet.
- Planes de implementación de nuevas redes informáticas, según los requerimientos universitarios. Planes de distribución adecuada de los diferentes anchos de banda para los servicios de Internet.
- Informes de optimización en la distribución y utilización de redes, subredes y equipos informáticos que presentan servicios de internet.
- Informes de apoyo técnico a la carrera de Ingeniería en Sistemas en la ejecución de prácticas especializadas.
- Planes de cambios o actualizaciones de tecnología en redes computacionales.
- Informes de aplicación de políticas de seguridad para la utilización de la intranet de la universidad.
- Plan de optimización del rendimiento de las redes y equipos informáticos.

1.2.3.3. Electrónica y Telecomunicaciones

- Plan de implementación, mantenimiento y reparación de equipos de telecomunicaciones e información de la Universidad Nacional de Loja.
- Plan de distribución de redes de telecomunicaciones con sus respectivos componentes, memorias técnicas, diseños, detalles constructivos, especificaciones técnicas de cada uno de los proyectos.
- Plan de estudios de perfeccionamiento de las redes que brindan servicios de telecomunicaciones e información a la ciudad universitaria y sus extensiones universitarias, para el ordenamiento e

integración, mediante propuesta de conectividades en sus diferentes modalidades.

- Plan de control de las instalaciones y el adecuado funcionamiento de los servicios de Internet.
- Diseño para la optimización de las redes de telecomunicaciones de las diferentes dependencias de la Universidad: TELEMEDICINA TELEDUCACIÓN, enlaces micro-onda. Fibra óptica y otros.
- Proyectos de expansión de servicios hacia zonas de interés de la Universidad que requieren conectividad: Internet, Telefonía, Telemetría, Videoconferencia y otros.
- Informes de apoyo técnico de las actividades relacionadas a conectividad con los proyectos generados en los Centro de investigación de la Universidad.
- Términos de referencia y pliegos de consultoría para la contratación de estudios de telecomunicaciones y electrónicos.
- Informes de apoyo técnico para la construcción y fiscalización de infraestructura física para informática y telecomunicaciones, principalmente en lo concerniente a casetas, torres, ductos; y, adicionales mecánicos cuando el caso lo requiera.
- Informes de apoyo técnico al Área de Ingeniería Electrónica y Telecomunicaciones, en prácticas pre-profesionales. [2]

2. SEGURIDAD DE LA INFORMACIÓN

2.1. Diferencia entre seguridad de la información y seguridad informática

Fig. 1 Seguridad de la información vs Seguridad Informática[3]

- La Seguridad Informática hace referencia a un enfoque técnico donde se manejan **vulnerabilidades y amenazas** asociadas a los equipos tecnológicos, enfocadas a los ataques más no se habla de riesgos y de su tratamiento.
- La seguridad informática es proteger los activos de acuerdo a sus vulnerabilidades y los ataques que puedan sufrir a partir de mediciones o lecturas tomadas sobre los equipos, sin considerar los riesgos a los que está sometida la organización y el impacto que pudiese ocasionar un incidente de seguridad.
- La seguridad informática se encarga de la implementación de soluciones técnicas para la protección de la información.
- La Seguridad de la Información, incluye la conceptualización de la seguridad informática, incluyendo la responsabilidad del personal que labora en la organización, puesto que sin el involucramiento del personal no puede existir un plan sustentable de seguridad de la información, donde ya se puede hablar de un análisis de riegos, aplicación de buenas prácticas y esquemas normativos.
- El concepto de **Seguridad de la Información** es una extensión de la conceptualización de **Seguridad Informática**, puesto que implica una visión enmarcada en los riegos del negocio, hablando de riesgos organizacionales, operacionales y físicos en los sistemas de información como se puede observar en la **(Figura 1).** [3]
- La seguridad de la Información es la disciplina encargada de diseñar normas, políticas, procesos, técnicas y métodos, orientados a conseguir un sistema de información seguro y confiable, enfocados en los requerimientos del negocio y valor organizacional.[4]
- La seguridad de la información además es la preservación de la confidencialidad, integridad y disponibilidad **(ver Figura 2)** de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización. Definiendo estos pilares fundamentales como:

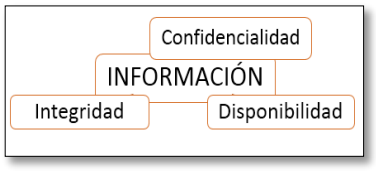


Fig. 2 Pilares fundamentales de la Seguridad de la información [Fuente Propia]

- **Confidencialidad:** Busca limitar el acceso a la información, es decir que esta solo pueda ser utilizada por personas autorizadas.
- **Integridad:** Protección de la información, tanto en su almacenamiento como en su forma de gestión o administración
- **Disponibilidad:** Busca que la información esté disponible y completa a todo momento, para usuarios autorizados [5]

2.2. Importancia y beneficios de la seguridad en las organizaciones

Las organizaciones están tomando conciencia de la aplicación de controles, donde la idea principal es la protección de la información, todo esto mediante aplicaciones de gestión de procesos, que permiten ordenar las actividades y dirigirlas al cumplimiento del objetivo que busca la organización. Lo que se pretende con una gestión de procesos, para la seguridad, es evitar tener que reaccionar ante hechos que se podrían haber sido previstos o gestionados antes que lleguen a ser un problema, ya que evitar problemas es una manera muy barata de ahorrar costos.

Los beneficios que la seguridad de la información, ofrece para las organizaciones son muchos entre los cuales podemos destacar:

- **Aumento de la calidad en los procesos de negocio:** permite obtener una mejora continua de la gestión global de la institución. En definitiva, podemos concluir que todos estos beneficios suponen una nueva ventaja competitiva para la institución, que contribuyen a la viabilidad de la misma a largo plazo.
- **Protección del negocio:** un sistema de seguridad busca mediante planes de contingencia, evitar interrupciones en las actividades o procesos de la

organización, manteniendo la disponibilidad de los activos de información, es decir garantizando la continuidad del negocio.

- **Mantener y mejorar la imagen corporativa:** Se ve reflejada directamente en la imagen de la organización ya que esta se percibe como empresa responsable, comprometida con la mejora de sus procesos, productos y servicios.[6]

2.3. ¿Qué es un fallo de seguridad?

Es cualquier incidente o evento, que pone en peligro cualquiera de los parámetros con los que se valora la seguridad, considerando el crecimiento desmedido de los usuarios que manejan los sistemas de información, cada vez más complejos, mediante el intercambio de información, se vuelve un reto evitar que sucedan diferentes tipos de fallos como son:

- Fallo en las comunicaciones.
- Fallos en el suministro eléctrico
- Fallos humanos de usuarios internos, usuarios externos, administradores, etc.
- Fallos en los sistemas de información: redes, aplicaciones, equipos, etc.
- Virus informáticos, gusanos, troyanos, etc., que inundan la red.
- Accesos no autorizados a los sistemas o a la información.
- Incumplimiento de una ley o reglamento.[6]

3. ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1. ISO (Organización Internacional de Estándares)

Es una organización especializada en el desarrollo y difusión de los estándares a nivel mundial.

Los miembros de esta organización, son organismos nacionales que participan en el desarrollo de Normas Internacionales a través de comités técnicos

establecidos que buscan soluciones en campos de actividad técnica. Los comités técnicos de ISO colaboran en los campos de interés mutuo con la IEC (*International Electrotechnical Commission*), la organización que a nivel mundial prepara y publica estándares en el campo de la electro tecnología. En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (Join Technical Committee Nº1).

Para una Norma Internacional sea aprobada se requiere que del 75% de los organismos internacionales que conforman la organización lo den su voto favorable.[7]

3.2. Norma ISO/IEC 27001:2013

ISO/IEC 27001:2013 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una organización.

La ISO/IEC 27001:2013 considera que la información debe tener sus tres pilares fundamentales como son: confidencialidad, integridad y disponibilidad, estas son fundamentales para garantizar que una organización gestiona de forma adecuada la seguridad de su información.[8]

3.3. Norma ISO/IEC 27002:2013

Las instituciones de todos los tipos y tamaños recopilan, procesan, manipulan y transmiten información de varias formas incluidas las electrónicas, físicas y verbales. Los procesos, los sistemas y el personal involucrado en la operación, manipulación y protección de dicha información son activos que al igual que otros activos comerciales de importancia, resultan valiosos para la organización y por tanto, merecen o requieren protección con diversos peligros.

La seguridad de la información se logra efectuando un conjunto adecuado de registros de seguridad, que incluyen políticas, procesos, procedimientos, estructuras

organizacionales y funciones de software y hardware. Estos controles se deberían establecer, implementar, revisar y mejorar para así garantizar el cumplimento de los objetivos de seguridad de las instituciones.

El estándar ISO/IEC 27002:2013, es una norma que describe controles de seguridad que pueden ser implementados dentro de una institución. Este estándar es una guía de buenas prácticas que constituyen un conjunto de controles recomendables en cuanto a seguridad de la información. Esta norma sigue las directrices de la norma ISO/IEC 27001:2013, está diseñada para que la utilicen las instituciones que tienen la intención de:

- Seleccionar controles de seguridad dentro del proceso de implementación de un SGSI basado en la norma ISO/IEC 27001:2013.
- Implementar controles de seguridad de la información de aceptación común.
- Desarrollar sus propias pautas de gestión de seguridad de la información.

La ISO/IEC 27002:2013 contiene 35 objetivos de control agrupados en 14 dominios.

Para cada dominio de seguridad, la norma detalla un conjunto de controles específicos que las instituciones deberían implementar. El total de controles específicos presentados en la norma son de 114 controles de seguridad, ver (Anexo 5).

Cada institución debería aplicar los controles adecuados para sus necesidades específicas.[9]

4. PROCESOS

4.1. Definición de proceso

Cualquier actividad o grupo de actividades que emplee un insumo, le agregue valor a éste y suministre un producto a un cliente externo o interno. Los procesos utilizan los recursos de una organización para suministrar resultados definitivos.[17]

4.2. Características de los procesos

Las características de los procesos son las siguientes:

TABLA I

CARACTERÍSTICAS DE LOS PROCESOS

Características de los procesos	• Se pueden describir entradas y salidas. • El proceso cruza una o varias veces límites, organizativos funcionales, por lo que puede afectar a varios departamentos. • Son capaces de cruzar vertical y horizontalmente la organización. • Responden a la pregunta qué (se hace), y no al cómo. • Tienen que ser fácilmente comprendidos por cualquier persona de la organización. • Tienen a alguien que se considera responsable del proceso. • Tienen límites bien definidos • Tienen interacciones y responsabilidades bien definidas. • Tienen medidas de evaluación. • Tienen propuestas de cambio. • Son de fácil manejo.

4.3. Elementos de los procesos

Los procesos contienen los siguientes elementos como en la figura 4, los cuales se detallan a continuación.

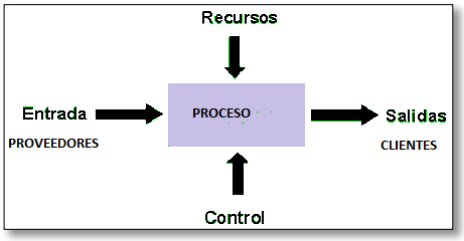


Fig. 3 Elementos del proceso (Fuente Propia)

- **Entrada:** Conjunto de información o elementos que llegan a un proceso.
- **Proceso:** Mecanismos de transformación de insumos en productos o resultados.
- **Recursos:** Sirven para transformar el insumo.
- **Control:** Surgen como una guía o normas en el proceso.
- **Salida:** Es el conjunto de información y elementos que salen de un proceso generado por una actividad.[17]

4.4. Clasificación de los procesos

Hay muchas clasificaciones que se les puede dar a los procesos, pero las principales clases de procesos que son necesarias de identificar en las organizaciones son:

- **Procesos para la gestión de una organización**: Incluyen procesos relativos a la planificación estratégica, establecimiento de políticas, fijación de objetivos y para las revisiones por la dirección.
- **Procesos para la gestión de recursos**: Son aquellos directamente ligados a los servicios que se prestan. Como consecuencia, su resultado es percibido directamente por el cliente/usuario (se centran en aportarle valor). Incluyen todos los procesos que proporcionan los recursos necesarios para los objetivos de calidad y resultados deseados de la organización.
- **Procesos de soporte o apoyo**. Incluyen aquellos procesos necesarios para medir y recopilar datos para realizar el análisis del desempeño y la mejora de la eficacia y la eficiencia. Incluyen procesos de medición, seguimiento, auditoría, análisis del desempeño y procesos de mejora (por ejemplo, para las acciones correctivas y preventivas) [18]

5. GESTIÓN DE PROCESOS

Es conceptualizada, como la forma de gestionar, toda una organización basándose en procesos, siendo definidos estos como una secuencia de actividades orientadas a generar un valor añadido, sobre una entrada para conseguir un resultado y una

salida que a su vez satisfaga los requerimientos del cliente.[10] Para lograr todo esto, es necesario conocer el funcionamiento y estructura del proceso mediante el mapeo de procesos, a través de ciertas herramientas que permiten cumplir con este objetivo. A continuación, se presenta un breve estudio de ciertas metodologías, que se tomaron en consideración desde el inicio del trabajo de titulación.

5.1. Metodologías de la gestión de procesos

Existen diversas metodologías para la gestión de procesos, pero se ha tomado las más convenientes para el desarrollo del presente trabajo de titulación entre las cuales tenemos:

5.1.1. Metodología SIPOC (Suppliers-Inputs-Process-Outputs-Customers)

Se tiene diversas vistas para determinar y analizar un proceso, incluyendo una vista global llamada diagrama PEPSU (proveedores, entradas, procesos, salidas y clientes o usuarios o SIPOC por sus siglas en inglés. Donde su propósito es mostrar las relaciones entre clientes y proveedores y los procesos principales de la organización. Lo cual nos brinda una vista de contexto de la organización.

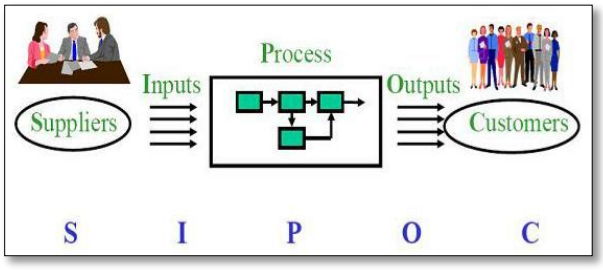


Fig. 4 Esquema general de sipoc[11]

SIPOC muestra las actividades multifuncionales en un diagrama simple, en un diseño total al cual se le puede añadir complementos y se lo considera aplicable a todas las organizaciones. El Diagrama de SIPOC es una herramienta que se emplea en el ámbito de la gestión por procesos en general. [12]

La metodología SIPOC fue desarrollada por William Edwards Deming, quien tiene un gran renombre por todo el mundo por construir las técnicas de control del proceso, como es el caso del ciclo PHVA o PDCA en inglés.[13] Esto permite comprender la estrecha relación entre ambas herramientas y su amplio uso dentro de la gestión de procesos. [14]

5.1.1.1. SIPOC significa

- Supplier= Proveedores: Proporcionan las entradas al proceso.
- Input= Entradas: Recursos que el proceso requiere.
- Process= Proceso: Actividad que transforma las entradas en salidas
- Output= Salidas: Productos o servicios proporcionados
- Customer=Cliente: Inversionistas quienes establecen los requerimientos de las salidas

5.1.1.2. Preparando el Sipoc

- Trabajo en equipo
    - Champion.
    - Propietarios del proceso.
    - Líder de equipo.
    - Green Belt.
- Entradas para preparar el Sipoc
    - Objetivos financieros.
    - Datos de calidad y objetivos.
    - Voz del cliente. [11]

5.1.1.3. Beneficios

- Ayuda a identificar y balancear requerimientos.
- Identificar lagunas en los requisitos.
- Verificar los requerimientos de recursos.
- Da más claridad en cuanto a los procesos involucrados.
- Determinará la métrica correcta para verificar los requerimientos del cliente.
- Establecerá el alcance del proyecto
- Establecerá quien debe de participar en el equipo del proyecto.

5.1.1.4. Aplicaciones de la metodología en base al ciclo PHVA

Es aplicada en:

- Normas ISO 900O Sistema de gestión de calidad.
- Norma ISO 14001 Sistemas de gestión medioambiental.
- Norma ISO 22000 Inocuidad alimentaria.
- Norma OHSAS 18000 Salud y seguridad ocupacional [14]

5.1.1.5. Empresa que han usado la metodología sipoc en base al ciclo PHVA

- Ford y GM
- The Coca-Cola Company
- Empresas japonesas.
- Harley Davison
- Intel
- Colgate Palmolive
- Proctor & Gamble

5.1.2. Metodología TORTUGA

Tortuga es útil para el análisis de procesos. Está compuesta por cuatro preguntas acerca del proceso y dos aspectos relacionados a la entrada y salida. Además es usada tanto para la implementación como la auditoría. La metodología tortuga puede ser usada como una herramienta de descripción y análisis de procesos para facilitar la gestión del negocio. No es una herramienta para identificar el proceso, sino, para entender el proceso. [15]

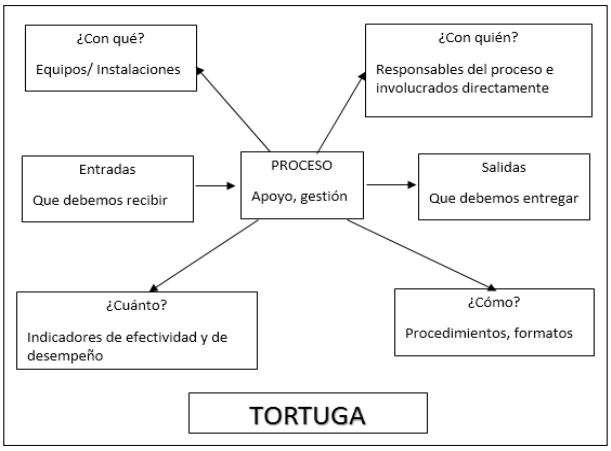


Fig. 5 Esquema general de tortuga [Fuente propia]

5.1.3. Metodología PULPO

Pulpo forma gráficamente las entradas del cliente hacia la organización y las salidas resultantes de la organización al cliente.

Pulpo tiene una interface interna y externa entre una organización y un cliente. Una interface entre la organización y la entrada externa del ambiente (I), así como de una interface entre la organización y la salida externa del ambiente (O). Además, se centra en la aplicación del enfoque de procesos en las auditorías bajo ISO/TS 16949 [16].

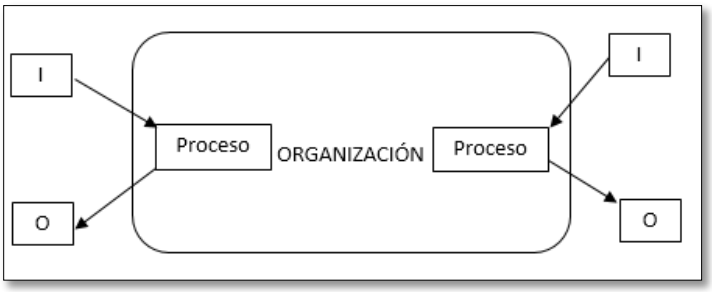


Fig.6 Esquema general de pulpo. [Fuente propia]

5.1.4. Ventajas y Desventajas de las Metodologías de gestión

TABLA II

VENTAJAS Y DESVENTAJAS DE LAS METODOLOGÍAS DE GESTIÓN DE PROCESOS

Metodología	Ventajas	Desventajas
SIPOC	• Mide el rendimiento del proceso. • Identifica las actividades del proceso que aportan valor para el cliente o el negocio y cuáles son inútiles. • Identifica proveedores y clientes. • Permite visualizar como el resultado de un proceso se convierte en la entrada de otro.	• Indican la estructura de la organización a un momento dado, por lo tanto, ante cada cambio producido en las tareas o funciones debe actualizarse.
TORTUGA	• Permite describir y analizar un proceso en cualquier nivel. • Implementa y mantiene un SGC. • Planificación y ejecución de auditorías. • Revisión de la dirección y toma de decisiones.	• Extenso en requerimientos. • Ideal para macro procesos. • No se puede tener una visión clara de la interacción con todos los procesos.
PULPO	• Permite una visión más general de los procesos de una organización. • Analiza la interacción E/S que tiene un cliente con un proceso específico.	• Mayor enfoque hacia el producto final. • Para el análisis y mejora de procesos es necesario incluir auditoría.

5.1.5. Comparativa de las Metodologías de gestión

TABLA III

COMPARATIVA DE LAS METODOLOGÍAS

Metodología	Procesos estratégicos	Procesos para la gestión de recursos	Procesos de soporte o apoyo
SIPOC	X	X	X
TORTUGA	X		X
PULPO		X	

El uso de la metodología SIPOC para el levantamiento de los procesos, asigna la alineación de trabajar en la gestión de estos, independientemente de su tipo, puesto que permite organizarse sin necesidad de cambiar de esquema, por lo tanto, esto

produce uniformidad en la ejecución de cualquier proyecto que se pretenda realizar mediante SIPOC.

6. MEJORA CONTINUA

Cuando se necesite de acciones correctivas, se debería definir el método para poder implementarlas, esto debe incluir la identificación y la eliminación de la causa de los problemas (errores, defectos, falta de controles adecuados en los procesos).

Las acciones tomadas se deben de revisarse y verificar su eficacia de acuerdo con el plan. Cuando se esté logrando con los resultados planificados del proceso y cumpliendo los requisitos, la organización se debe de enfocar en acciones para mejorar el desempeño del proceso a niveles más altos de manera continua.

La metodología PHVA (Planificar-Hacer-Verificar-Actuar) puede ser una herramienta útil para definir, implementar y controlas las acciones correctivas y las mejoras.

Fig. 7 Ciclo PHVA

Planificar: Establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente, legales y reglamentarios y las políticas de la institución.

Hacer: Implementar los procesos.

Verificar: Realizar el seguimiento y la medición de los procesos, productos respecto a las políticas, objetivos y requisitos para el producto.

Actuar: Tomar las acciones para la mejora continua del desempeño del proceso.

Esta metodología es dinámica que puede ser aplicada en cualquier nivel de procesos, puesto que está asociada con la panificación, implementación, verificación y la mejora con el fin de mantener el desempeño de la institución. [19]

7. DIAGRAMAS PARA LA MODELACIÓN DE PROCESOS

7.1. Diagramas de flujo

Son una representación gráfica de una secuencia lógica de procesos de trabajo. Mediante la utilización de diferente simbología, representa operaciones, datos, direcciones de flujo y recursos; para la definición, análisis o solución de un problema. Se caracteriza por su gran facilidad de uso y aporta gran cantidad de información, puesto que muestra la totalidad del sistema, aunque presenta la problemática de su extensión, lo que dificulta la visión global de todo el sistema, así como que los límites del proceso no suelen estar muy claros.[20]

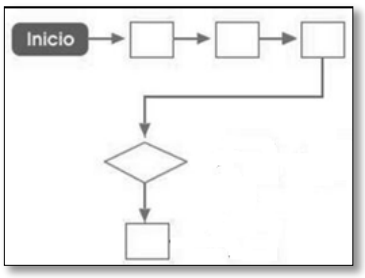


Fig. 8 Diagrama de flujo [Fuente Propia]

- **Ventajas**
  - Muestra las diversas actividades y funciones que se realizan en la organización, sean estas especializadas o no.
  - Al ser una representación gráfica, permite apreciar a simple vista la estructura general y las relaciones de trabajo de una organización, mejor de lo que podría hacerse por medio de una larga descripción.

- **Desventajas**

- No indica el grado en que la organización centraliza, o no, su toma de decisiones
- No indica como fluye la comunicación e información dentro de la organización, más allá de la formalidad en las relaciones que representa.[21]

7.2. Diagramas sipoc

Es un gráfico que permite visualizar al proceso de manera sencilla y general, este esquema puede ser aplicado a procesos de todos los tamaños y a todos los niveles, incluso a una organización completa.[21]

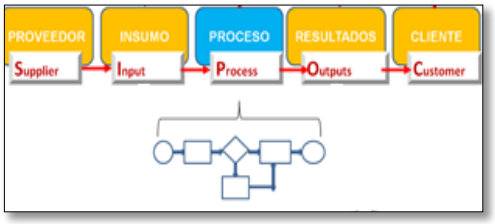


Fig. 9 Diagrama sipoc[22]

- **Ventajas**
  - Permite visualizar el proceso de manera sencilla.
  - Identificar las partes implicadas, como proveedores, entradas, procesos, salidas y clientes[21]

7.3. Diagramas Bpmn

Es un gráfico que permite una estandarización del modelado de los procesos, permitiendo así describir la lógica de los pasos de un proceso.[23]

8. ESTANDAR BPMN

8.1. BPMN

- Por sus siglas en ingles Business Process Model and Notation proporciona un lenguaje común para que las partes involucradas puedan comunicar los procesos de forma clara, completa y eficiente.
- Es el nuevo estándar para el modelado de procesos de negocio y servicios web.
- Es una notación a través de la cual se expresan los procesos de negocio en un diagrama de procesos de negocio.
- Este estándar agrupa la planificación y gestión del flujo de trabajo, así como el modelado y la arquitectura.
- De esta forma, por fin las áreas técnicas y comerciales de una organización pueden hablar en el mismo idioma. Así la comunicación es fluida y pueden satisfacer sus necesidades de precisión y flexibilidad.
- Por lo cual que **BPMN** abre nuevas vías de colaboración y da lugar al desarrollo de aplicaciones nuevas y más flexibles.
- El principal objetivo de **BPMN** es proporcionar una notación estándar que sea fácilmente legible y entendible por parte de todos los involucrados e interesados del negocio. [24]

8.2. Características

- Proporciona un lenguaje gráfico común, con el fin de facilitar su comprensión a los usuarios de negocios.
- Integra las funciones empresariales.
- Utiliza una Arquitectura por Servicios (**SOA**) con el objetivo de adaptarse rápidamente a los cambios y oportunidades del negocio.
- Combina las capacidades del software y la experiencia de negocio para optimizar los procesos y facilitar la innovación del negocio.
- BPMN es independiente de cualquier metodología de modelado de procesos.
- BPMN crea un puente estandarizado para disminuir la brecha entre los procesos
- de negocio y la implementación de estos.
- BPMN permite modelar los procesos de una manera unificada y estandarizada

- permitiendo un entendimiento a todas las personas de una organización.[25]

8.3. Modelación de procesos

Es la captura de una secuencia de actividades de negocio, y de la información de soporte.

Los procesos de negocio describen la manera cómo una empresa u organización alcanza sus objetivos. Existen diferentes niveles del proceso de modelado como son:

- **Mapas de proceso.** Son diagramas de flujo simple de las actividades.
- **Descripciones de proceso.** Conforman una extensión del anterior, y manejan información adicional pero no suficiente para definir completamente el funcionamiento actual.
- **Modelos de proceso.** Son diagramas de flujo extendido con suficiente información para que el proceso pueda ser analizado, simulado, y/o ejecutado

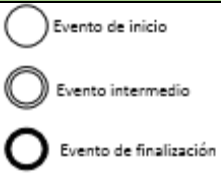
El BPMN soporta cada uno de estos niveles de modelado. [23]

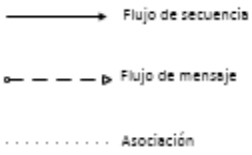
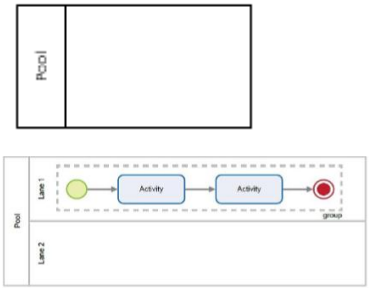
8.4. Elementos de los diagramas

La función del BPMN es crear un mecanismo simple para realizar modelos de procesos de negocio, con todos sus elementos gráficos, y que al mismo tiempo sea posible gestionar la complejidad. El método elegido para manejar estos dos conflictivos requisitos es organizar los aspectos gráficos de la notación en categorías específicas. Las cuatro categorías básicas de elementos son:[25]

TABLA IV

ELEMENTOS DE LOS DIAGRAMAS DE FLUJO BPMN

Elemento	Descripción	Notación
Eventos (events)	Se usan para iniciar o finalizar un proceso y para gestionar acciones específicas durante un flujo de trabajo.	

Actividades (activities)	Tareas que son llevadas a cabo en el proceso, ya sea por personas, automáticamente o mediante subprocesos.	
Compuertas (gateways)	Se usan para separar o unir flujos del proceso.	
Flujos de secuencia	Se usan para mostrar los movimientos del flujo de trabajo.	
Calle (pool)	Contiene un proceso completo. El flujo no puede abandonar un pool se necesita usar los eventos para transferir la acción o los datos de un proceso a otro.	

e. MATERIALES Y MÉTODOS

Para la realización del presente trabajo de titulación titulado “LEVANTAMIENTO, DEFINICIÓN Y FORMALIZACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE LOJA”, se contó con los recursos humanos, económicos y tecnológicos como hardware y software, necesarios para su culminación.

1. MATERIALES

Para la realización del trabajo de titulación fue necesario calcular los recursos humanos, bienes, servicios e imprevistos.

1.1. Talento humano

Recurso Humano	Cantidad	Horas	V. Unitario	V. Total	Nota
Investigadora	1	400	10,00	4,000	
Director de Tesis	1	150	10,00	1,500	El costo del tutor lo asumirá la Universidad Nacional de Loja
			Subtotal	5,500	

1.2. Bienes

Calculo de depreciación a través del método de línea recta. Vida útil de equipos informáticos es de 3 años.

$$Fórmula = \frac{\text{Costo Activo} * \#\text{ meses}}{\text{Vida Útil} * 12\text{ meses}}$$

Equipo	Depreciación		Depreciación	Total
	V. Real	T. Útil / mes		
Computador portátil Toshiba Satellite core i3				886,11
Impresora Cannon MG2200	105	2	5,83	99,17
Memoria 8GB Kingston	8.00	5	1,11	6,89
			Subtotal	992,17

1.3. Servicios

Servicios	Cantidad	V. Estimado	V. Total
Internet/ mes	9	21.00/mes	189.00
Transporte/ mes	5	12.00/mes	60.00
Resma de papel	2	4.50	9.00
Cartuchos de tinta	2	45.00	90.00
Anillados	4	1.50	6.00
		Subtotal	354.00

1.4. Imprevistos

Para la tasa de imprevistos se consideró el 10% de la suma total de talento humano, bienes y servicios.

	Porcentaje costo directo	V. Total
Imprevistos (Talento humano + bienes + servicios)	10%	684.62
	Subtotal	684.62

1.5. Total de recursos

Descripción	V. Total
Talento humano	5,500
Bienes	992,17
Servicios	354.00
Imprevistos	684.62
Total	**7,530.79**

2. MÉTODOS Y TÉCNICAS

Para la ejecución del presente proyecto de titulación fue conveniente y necesario la adopción de métodos que permitieron obtener la información relevante y fiable, para lo cual se utilizó.

2.1. MÉTODOS

- **Método Deductivo**

  Este método va de lo particular a lo general, lo cual fue utilizado al momento de seleccionar los procesos más importantes dentro de la Unidad de Telecomunicaciones e Información, además se tomó como referencia los objetivos para poder concluir y de esta manera recomendar de manera crítica y acorde a cada objetivo.

- **Método Inductivo**

  Este método permitió realizar cada uno de los objetivos específicos para así llegar a cumplir con el objetivo general. De la misma forma, al estudiar la metodología SIPOC, la norma ISO 27002:2013 y el ciclo PHVA, las cuales fueron tomadas como referencia, se procedió al levantamiento de los procesos de seguridad de la información, partiendo de lo general a lo particular.

2.2. TÉCNICAS

- **Análisis de la información**

  Esta técnica nos permitió seleccionar la información más relevante para poder levantar los procesos de seguridad de la información.

- **Observación directa**

  Con esta técnica se pudo constatar la problemática que ocurre en el manejo de la información, infraestructura y recursos tecnológicos que fluyen directamente en la seguridad de la información.

- **Entrevista**

  Esta técnica me permitió obtener mayor información acerca de la ejecución de las actividades, de tal manera que se adquiere toda la información necesaria para iniciar el análisis de la misma.

- **Búsqueda de información científica**

  Se utilizó para sustentar el desarrollo del trabajo de titulación en base a los conocimientos adquiridos de múltiples personas que han hecho uso de la investigación científica, así como para plantear la solución, obtener y generar nuevos conocimientos.

- **Mapeo de procesos**

  Son utilizados en la documentación, evaluación y diseño de los mapas de procesos.

2.3. METODOLOGÍA SIPOC (*Suppliers-Inputs-Process-Outputs-Customers*)

Para la ejecución de este trabajo de titulación, se hizo uso de la metodología SIPOC, el cual nos provee una visión general del flujo de los procesos y sus interrelaciones dentro de la Unidad de Telecomunicaciones e Información, además de definir los límites de los mismos, así como el punto de inicio y final.

Qué significa SIPOC

S= Proveedores: proporcionan las entradas al proceso.

I=Entradas: recursos que el proceso requiere.

P=Proceso: actividad que transforma las entradas en salidas.

O=Salidas: productos a servicios proporcionados.

C=Clientes: establecen los requerimientos de las salidas.

Pasos de SIPOC

1. Identificar las entradas.
2. Identificar el cliente o proveedor de cada entrada.
3. Hacer una lista de los requerimientos de cada entrada.
4. Identificar el proceso y sus límites.
5. Identificar las salidas.
6. Identificar los clientes para cada salida.
7. Hacer una lista de los requerimientos para cada salida.

Luego de haber realizado los pasos anteriores se debe realizar las siguientes actividades:

- **Levantar requerimientos:** Se debe recolectar toda la información necesaria, de lo que ocurre dentro del proceso, para lo cual es necesario recorrer cada departamento y entrevistar a todos los actores participantes de los procesos de manera directa y documentar la información, además es importante tener en consideración las siguientes preguntas:
    - ¿Cuáles son las tareas que desempeña?
    - ¿Cómo realiza o ejecuta cada tarea?
    - ¿Qué información necesita para realizar cada tarea?

Todas estas preguntas entregaran información necesaria para poder diagramar las tareas de un proceso. Además las entrevistas deben tener un formato de conversación más que un cuestionario, la cual debe estar dirigida de manera espontánea por el entrevistador pasa así lograr superar las barreras psicológicas que pueda tener el entrevistado.

- **Elaborar un documento de definición de procesos:** El objetivo principal de elaborar un documento de definición de procesos, consiste en describir en términos generales un determinado proceso. Los pasos a tener en cuenta son:
    - Identificar y describir las actividades que componen un proceso.
    - Especificar la secuencia de las actividades que componen el proceso, de tal forma que se logre cumplir el objetivo u objetivos, para los cuales fue creado dicho proceso.
    - Identificar las entradas y salidas de cada una de las actividades.
    - Establecer el rol responsable de cada actividad del proceso.
- **Identificación de actores:** Identificar los actores que intervienen en el proceso con su respectivo rol y se utilizará la siguiente tabla.

TABLA V
IDENTIFICACIÓN DE ACTORES

Identificación de Actores	
Cargo	**Rol**

- **Descripción de actividades:** Las actividades corresponden a las diferentes tareas que intervienen en la consecución de un proceso. Para identificar las actividades se ponen a consideración la siguiente tabla.

TABLA VI
DESCRIPCIÓN DE ACTIVIDADES

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**

- **Elaborar el diagrama de flujo de los procesos bajo el estándar Bpmn**: El diagrama de flujo del proceso es una representación gráfica del proceso, este diagrama se lo puede realizar con cualquier herramienta de modelamiento.

f. RESULTADOS

El presente trabajo de titulación, estuvo orientado al cumplimiento del objetivo general, conjuntamente con los objetivos específicos, para lo cual, se consideró dividirlo en cinco fases con sus respectivas actividades, las cuales se han cumplido de forma ordenada y optima, a continuación se detalla el desarrollo de cada una de ellas:

FASE 1: Diagnosticar la situación actual de la unidad de Telecomunicaciones e Información sobre los procesos de seguridad de la información.

1.1. Recopilar información mediante la encuesta, referente a los procesos existentes de seguridad de la información

La encuesta, fue realizada con varias alternativas de respuestas (**Ver Anexo 4**), esta fue validada a través de la metodología Sipoc, que permitió conocer la vista macro del flujo de los procesos y sus interrelaciones dentro de la Unidad de Telecomunicaciones e Información, además de definir los límites, el punto de inicio y final de los mismos y la norma ISO/IEC 27002:2013 (**Ver Anexo 5**), donde se tomó en cuenta algunos de los dominios, objetivos de control y controles para la seguridad de la información, entre estos dominios, objetivos y controles tenemos;

- **Gestión de Activos**: su objetivo principal es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos, así mismo tiene algunos objetivos de control como:
    - **Clasificación de la Información:** su objetivo es el de asegurar que se aplica un nivel de protección adecuado a la información.
    - **Manejo de los Soportes de Almacenamiento:** su objetivo es evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.

- **Control de Accesos:** permite controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática, dentro de los objetivos de control que se tomaron en cuenta tenemos:
    - **Requisitos de negocio para el control de accesos:** controla los accesos a la información y las instalaciones utilizadas para su procesamiento.
    - **Gestión de Acceso de Usuarios**: garantiza el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.
    - **Control de acceso a sistemas y aplicaciones:** impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.
- **Seguridad en la operativa:** Su objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada, los objetivos de control que se tomó en cuenta fue:
    - **Copias de seguridad:** alcanzar un grado de protección deseado contra la pérdida de datos.
- **Seguridad en las telecomunicaciones:** Su objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte, el objetivo de control que se tomó en cuenta fue:
    - **Intercambio de información con partes externas:** mantener la seguridad de la información que transfiere una organización internamente o con entidades externas.

Además la Dirección de Telecomunicaciones e Información, supervisa y aprueba, toda acción de incorporación de tecnología y servicios informáticos para la institución, los cuales son realizados, bajo las normativas establecidas en los procesos de adquisición de equipos y recursos informáticos.

En la Unidad de Telecomunicaciones e Información, las políticas institucionales de seguridad informática están basadas en la norma ISO/EC 17799:2000, la cual es un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. (**Ver Anexo 7**).

En el Estatuto por procesos de la Universidad Nacional de Loja (**Ver Anexo 6**) se estipula la organización de la Unidad de Telecomunicaciones e Información, donde consta la distribución de atribuciones y responsabilidades, así como la descripción de los productos y servicios que se ofrecen en la Unidad de Telecomunicaciones e Información. (**Ver sección de la 1.2 de la revisión de literatura**)

Con la ayuda de la metodología Sipoc, la norma ISO/IEC 27002:2013, los estatutos por procesos de la Universidad Nacional de Loja y las políticas de la Unidad de Telecomunicaciones e Información, permitió recopilar información, de que procesos de seguridad de la información se están ejecutando actualmente, en la Unidad de Telecomunicaciones e Información.

Esta encuesta, fue aplicada a todo el personal del departamento de la Unidad de Telecomunicaciones e Información, como son: director, subdirectores, responsable de la seguridad de la información, técnicos de software, técnico de infraestructura, desarrolladores de software, analistas de sistema sección redes y telecomunicaciones.

1.2. Realizar la tabulación de acuerdo a las encuestas obtenidas

Después de haber aplicado las encuestas, la tabulación de los datos obtenidos se presenta en figuras con una distribución porcentual y en tablas.

A continuación en la figura 10 se muestran los resultados de la pregunta ¿Cuentan con algún formato para el levantamiento de los procesos de seguridad de la información? La muestra índico que de los diez encuestados solo uno expresa que si conoce de un formato, cuatro que solo conoce en parte y cinco que no existen un formato definido para los procesos de seguridad de la información .

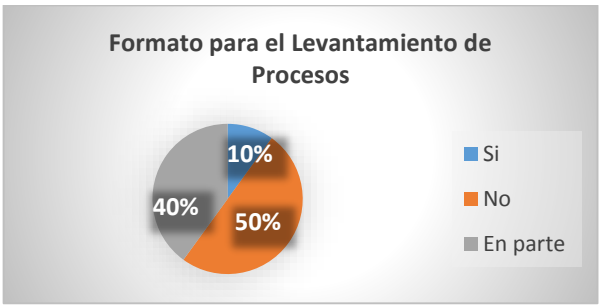


Fig. 10 Formato de procesos

Se determinó que no cuentan con un formato existente, para el levantamiento de los procesos de seguridad de la información, cabe recalcar que el en departamento de desarrollo de software tiene un formato de levantamiento de procesos de tesorería, pero no procesos de la seguridad de la información.

En la figura 11, se muestran los resultados de la pregunta ¿Conoce usted que procesos de seguridad de información, existen actualmente en la UTI? La muestra indica que ocho encuestados, conocen los procesos que se llevan actualmente en la UTI, entre los cuales mencionaron; creación de credenciales, gestión de usuarios, creación de cuantas de usuario de las aplicaciones, creación de usuarios de las bases de datos, creación y validación de usuarios para el accesos a los servidores, gestión de claves de correo, respaldo de la información y administración de equipos tecnológicos de interconectividad.

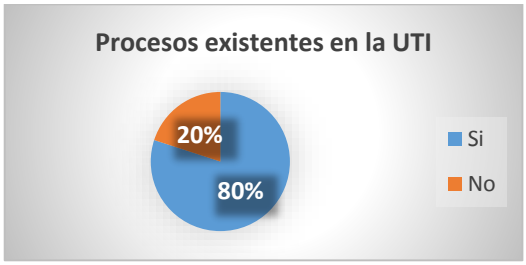


Fig. 11 Procesos existentes en la UTI

Se deduce, que hay muy pocos procesos de seguridad de la información, además los encuestados indican que los procesos actuales, no se encuentran normalizados ni están levantados bajo ninguna metodología de gestión de procesos, estos procesos se realizan de forma rudimentaria atendiendo los requerimientos de forma prioritaria y buscando solucionarios de acuerdo a la naturaleza de los mismos, más no utilizando documentos o plantillas estandarizadas que permitan tener un control

claro y preciso de las actividades que se realizan en cada sección. Cabe considerar que los directivos de cada sección han organizado las actividades y los procesos de acuerdo a su experiencia procurando cumplir con las funciones encomendadas de manera óptima y con los tiempos establecidos.

En la tabla VII se muestran los resultados de la pregunta ¿Qué actividades usted realiza con respecto a procesos de seguridad de la información?

TABLA VII
ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN

Rol	Actividades
Director Unidad	Realiza la creación de credenciales para cada uno de los miembros de la Unidad de Telecomunicaciones e Información. Modificación de datos de cuentas de acceso.
Al administrador de seguridad de la información	Cuentas de correo institucional Gestión de claves de correo Gestión de claves de SGA (Sistema de Gestión Académica) Gestión de claves de evaluación a docentes Gestión de claves de web institucional Gestión de claves de seguimiento a graduados Gestión de claves de otras aplicaciones Creación de usuarios.
El subdirector de redes y equipo informático	Creación y validación de usuarios a nivel de los servidores que brindan diferentes tipos de servicios Supervisar las configuraciones en los servidores, equipos de red sean correctos Velar por el cumplimiento de las políticas de la Unidad de Telecomunicaciones e Información existentes.
El subdirector de desarrollo y	Técnico que atiende requerimientos de la mesa de ayuda.

mantenimiento de software	
El técnico de software	Respaldo de base de datos de aplicaciones es decir solamente para el sistema de gestión académica (SGA) el respaldo se lo hace de manera automática y cada semana, también para el sistema de evaluaciones este respaldo se lo realiza solo en periodo de evaluaciones y por ultimo respaldo de otros sistemas se lo hace manualmente y de manera mensual
Los analistas de redes y telecomunicaciones	Manejo de seguridad en la red a través del firewall, switch y router, administración de credenciales de equipos tecnológicos de interconectividad
Los desarrolladores de sistemas	Indican que no realizan ninguna actividad respecto a procesos de seguridad de la información.
Los técnicos de mantenimiento	Respaldo de la información cuando formatean las máquinas. Mantenimiento preventivo y correcto de equipos.

Se determina que existen muy pocas actividades, con respecto a la seguridad de la información, puesto que no de los inconvenientes es el personal limitado para la ejecución de funciones, donde los directivos de cada sección organizan las actividades, buscando cubrir las necesidades presentes de forma óptima y eficiente con el personal limitado con el que se cuenta.

Se muestran los resultados de la pregunta ¿Qué actividades están previamente establecidas para desarrollar los procesos?, en caso de no contar con alguna actividad que avale alguna o algunas de las actividades indíquelo, respecto a la tercera pregunta. La muestra indica que no cuentan con actividades establecidas para el desarrollo de los procesos, por lo tanto se deduce que, las actividades de los procesos, se los hace de manera rudimentaria de acuerdo a su experiencia para así poder cumplir de manera óptima con las funciones encomendadas.

En la figura 12 se muestran los resultados a la pregunta ¿Cuáles son los límites impuestos de tiempo promedio que se demoran por procesos? La muestra indica que seis de los encuestados expresa que no tienen tiempo promedio definido, tres encuestados indican que se demoran de 5-10 minutos por proceso, uno expresa que se demoran 30 minutos por proceso.

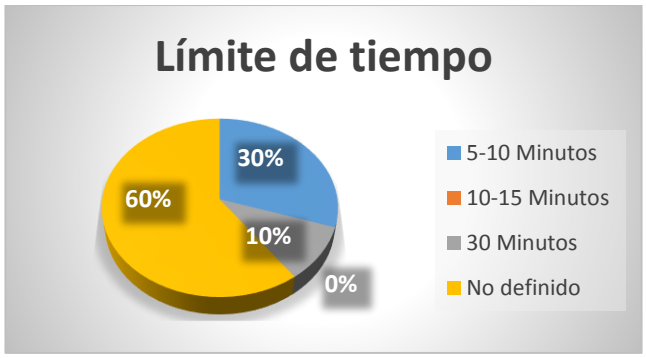


Fig. 12 Límite de tiempo por proceso

Se determina, que no tienen un tiempo definido para la realización de los procesos, es por esto que no hay una rapidez para desarrollar los mismos.

Se muestran los resultados de la pregunta ¿Cómo se valida la eficiencia y eficacia con la que se llevan a cabo cada uno de los procesos? La muestra indica que no existen una validación de la eficiencia y eficacia de los procesos, por lo cual de deduce que los procesos actuales se los realiza de manera cotidiana y en base a la experiencia.

En la figura 13 se muestran los resultados de la pregunta ¿Cómo circula la información y las instrucciones entre las áreas de la UTI referente a los procesos de seguridad de la información? La muestra indica que la información circula mediante oficios y correo electrónico.

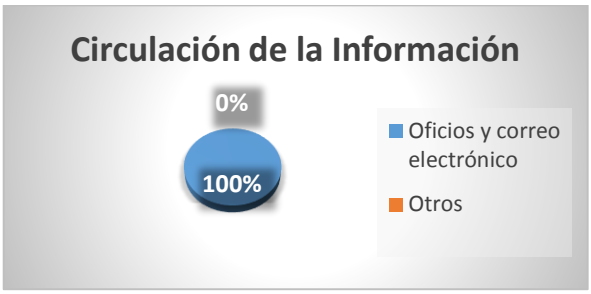


Fig. 13 Circulación de información

Se determina, que hay una buena comunicación en cuanto a la seguridad de la información, puesto que la información, la obtienen todos y así pueden cumplir con sus responsabilidades.

Luego de haber tabulado, los resultados obtenidos de la encuestas aplicadas, al personal de la UTI, se concluye lo siguiente; para el manejo de los procesos de seguridad de la información, que están presentes actualmente en la UTI, estos son ejecutados de manera general, no fueron levantados bajo ninguna metodología de gestión de procesos, ni bajo ninguna norma de seguridad de la información, además no cuentan con un formato para el levantamiento de los mismos. Así mismo, estos procesos, no cuentan con una debida validación de eficacia y eficiencia, dando lugar a que exista, una demora en la ejecución de los mismos, provocando aglomeraciones de usuarios y pérdida de tiempo.

1.3. Analizar la información recolectada para la determinación de la situación actual dentro de la UTI, que permite determinar la definición de los procesos de seguridad de la información más primordiales

A partir de la información recolectada, sugerencias y comentarios del personal se tiene una visión general, de lo concerniente a la seguridad de la información, dentro de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, donde se ha considerado diferentes puntos de importancia que permiten definir los procesos de seguridad de la información.

1. Considerando los controles de seguridad informática, descritos en el documento general que maneja la UTI, se puede decir que este permite a cada departamento mantener un control general sobre las actividades que debe realizarse, pero no se profundiza, en la forma de cómo se realizan los procesos, ni se determina la forma en como estos deben realizarse, por tanto cada departamento realiza sus actividades en base a normativas establecidas por el subdirector de cada departamento de forma extraoficial y de acuerdo a las necesidades, siendo estas adaptadas a las demandas de los usuarios y no de forma estandarizada, lo que dificulta el control de las actividades.

2. Cuando se habla de procesos y flujos de trabajo que se realizan en cada departamento, estos no se encuentran normalizados, donde los procesos se realizan de forma rudimentaria atendiendo los requerimientos de forma prioritaria y buscando solucionarlos de acuerdo a la naturaleza de los mismos, mas no utilizando documentos o plantillas estandarizadas que permitan tener un control claro y preciso de las actividades que se realizan en cada departamento. Cabe recalcar que los directivos de cada departamento, han organizado las actividades y los procesos de acuerdo a su experiencia procurando cumplir con las funciones encomendadas de manera óptima y con los tiempos establecidos. Cabe recalcar que los procesos que se están ejecutando no se han actualizado desde el 2012 hasta presente fecha.

3. En cuanto a los roles y actividades que se realizan en cada departamento, estos se encuentran estipulados en el estatuto por procesos de la Universidad, donde se describen de forma general las funciones y actividades que se realizan en la Unidad de Telecomunicaciones e Información, siendo este el orgánico funcional, a partir del cual se describe el orgánico estructural de la Unidad de Telecomunicaciones e Información (**Ver Anexo 1**), es importante considerar que el personal asignado para el cumplimiento de sus funciones, en algunos casos no está asignado legalmente a sus funciones, sino que realiza las mismas a partir de las disposiciones del director de la UTI.

4. Para un adecuado control de los procesos de seguridad de la información, en la Unidad de Telecomunicaciones e Información, se definen los siguientes dominios, objetivos de control y controles para la seguridad de la información, bajo el anexo de la norma ISO/IEC 27001:2013, este anexo es el de la norma ISO/IEC 27002:2013. Se definirán los procesos más importantes y fundamentales para la UTI, puesto que cuentan con el personal y no se necesita de recursos financieros, ni humanos, para el control de los mismos. A continuación se detallan los mismos.

TABLA VIII
DOMINIOS Y OBJETIVOS DE CONTROL A SER UTILIZADOS BAJO LA NORMA 27002:2013

DOMINIO	OBJETIVOS DE CONTROL	
GESTIÓN DE ACTIVOS	**8.3**	**Manejo de los soportes de almacenamiento**
CONTROL DE ACCESOS	**9.1**	**Requisitos de negocio para el control de acceso**
SEGURIDAD EN LAS TELECOMUNICACIONES	**13.2**	**Intercambio de información con partes externas**

TABLA IX
CONTROLES A SER UTILIZADOS Y CONTROLES QUE ESTÁN PRESENTES EN LA UTI

DOMINIO	OBJETIVOS DE CONTROL		CONTROLES A SER UTILIZADOS	CONTROLES ACTUALES
GESTIÓN DE ACTIVOS	**8.2**	**Clasificación de la información**		X
	8.3	**Manejo de los soportes de almacenamiento**	X	
CONTROL DE ACCESOS	**9.1**	**Requisitos de negocio para el control de acceso**	X	
	9.2	**Gestión de acceso de usuarios**		X
	9.4	**Control de acceso a sistemas y aplicaciones**		X
SEGURIDAD EN LA OPERATIVA	**12.3**	**Copias de seguridad**		X
SEGURIDAD EN LAS TELECOMUNICACIONES	**13.2**	**Intercambio de información con partes externas**	X	

5. Cabe recalcar que no se van a tomar en cuenta todos los dominios de control y controles de la norma ISO/IEC 27002:2013, puesto que el costo económico de personal para la implantación, así como el tiempo sería demasiado elevado, así mismo se necesitaría de capacitaciones especiales para el personal, para el control de los mismos.

   Además se hará una gestión de los procesos que actualmente se encuentran ejecutando, en la Unidad de Telecomunicaciones e Información.

FASE 2: Levantamiento de los procesos de seguridad de la información

2.1. Determinar los procesos que se están ejecutando actualmente en la Unidad de Telecomunicaciones e Información

Después de haber realizado el análisis en el punto 1.3 Tabla IX de la primera fase, se determinó los procesos que se ejecutan actualmente en la UTI (**Ver Anexo 8**), entre los cuales se detallan a continuación.

Procesos	**Subprocesos**
Clasificación de la información	Directrices de clasificación. Etiquetado y manipulación de la información.
Gestión de usuarios	Creación de usuarios de aplicaciones internas Modificación de usuarios de aplicaciones internas Creación de usuarios de bases de datos Modificación de usuarios de bases de datos Bloqueo de usuarios de bases de datos Creación de usuarios de sistemas operativos Modificación de usuarios de sistemas operativos Creación de usuarios del sistema de gestión académica Modificación de usuarios del sistema de gestión académica Creación de usuarios de cuentas de correo electrónico institucional Suspensión de usuarios de cuentas de correo electrónico institucional Creación de usuarios a nivel de servidores Modificación de usuarios a nivel de servidores
Gestión de contraseñas	Creación de contraseñas Reseteo de contraseñas Reseteo de contraseñas on-line Uso de contraseñas
Copias de seguridad	Creación de respaldos Codificación de respaldos Almacenamiento de respaldos Pruebas de respaldos Procedimientos de recuperación

2.2. LEVANTAMIENTO DE PROCESOS

2.2.1. LEVANTAMIENTO DEL PROCESO CLASIFICACIÓN DE LA INFORMACIÓN

2.2.1.1. Requisitos y Documentación

Para la ejecución de la situación actual del proceso, Clasificación de la Información en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja son indispensables los siguientes documentos:

1. Requisitos previos obtenidos por el dueño del proceso:
   a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.1.2. Actores

Las personas que llevan a cabo la situación actual del proceso Clasificación de la Información son denominados actores, puesto que interactúan directamente con el mismo y además son responsables de realizarlo en su totalidad. A continuación, se nombran los actores del proceso Clasificación de la Información.

- Responsable de la seguridad de la información

2.2.1.3. Descripción de Actividades

Se incluye toda la información levantada de acuerdo a cada actividad que pertenece a cada proceso, también se adjunta su número de actividad, dueño de la actividad y el tiempo estimado para su realización.

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 30 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de clasificar la información, para lo cual revisa el documento de políticas institucionales de la UTI (literal 1.a) y clasifica la información de acuerdo a: confidencialidad, integridad y disponibilidad, además deberá revisar los subprocesos de directrices de clasificación y etiquetado de la información y finalmente procederá a clasificar la información.

Para el presente proceso es necesario levantar los siguientes subprocesos:

2.2.2. LEVANTAMIENTO DEL SUBPROCESO DIRECTRICES DE CLASIFICACIÓN

2.2.2.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
    a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.2.2. Actores

- Responsable de la seguridad de la información

2.2.2.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 30 minutos

El responsable de la seguridad de la información, inicia el proceso con la necesidad de ver las directrices de clasificación, para lo cual revisa el documento de políticas institucionales de la UTI (literal 1.a) y ve las directrices para la confidencialidad, integridad y disponibilidad y posteriormente clasifica la información de acuerdo a dichas directrices.

2.2.3. LEVANTAMIENTO DEL SUBPROCESO ETIQUETADO Y MANIPULADO DE LA INFORMACIÓN

2.2.3.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
    a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.3.2. Actores

- Responsable de la seguridad de la información

2.2.3.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 30 minutos

El responsable de la seguridad de la información, inicia el proceso con la necesidad de etiquetar y manipular la información, para lo cual revisa el documento de políticas institucionales de la UTI (literal 1.a) ve el tipo de información y posteriormente etiqueta y manipula la misma.

2.2.4. LEVANTAMIENTO DEL PROCESO GESTIÓN DE ACCESO DE USUARIOS

2.2.4.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.4.2. Actores

- Responsable de la seguridad de la información
- Director UTI

2.2.4.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de gestionar los diferentes usuarios, para lo cual hace uso del documento de políticas institucionales de la UTI (literal 1.a), para luego poderlos clasificar según el tipo de usuario, además deberá revisar los subprocesos de creación, modificación, bloqueo y suspensión de los usuarios, finamente estos registros pasan por el director de la UTI para dar el visto bueno y autorización de los mismos, y así poder realizar la correspondiente gestión.

Para el presente proceso es necesario levantar los siguientes subprocesos:

2.2.5. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DE APLICACIONES INTERNAS

2.2.5.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario

a. Copia de la acción de personal legalizada por los altos directivos de la UNL.

b. Petición del secretario abogado/coordinador de la carrera/administrativo financiero del área, solicitando la creación del usuario de aplicaciones internas

2. Requisitos previos obtenidos por el dueño del proceso

a. Formulario de creación de usuarios de aplicaciones internas.(**Ver Anexo 9**)

b. Acuerdo de confidencialidad de los usuarios (**Ver Anexo 10**)

2.2.5.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo)

2.2.5.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Usuario

Tiempo estimado: 2 días laborables

El usuario inicia el proceso con la necesidad de obtener la creación del usuario de aplicaciones internas, para lo cual adjunta la copia de la acción de personal (literal 1.a) y una petición solicitando la creación del usuario de aplicaciones internas (literal 1.b).

Con todos los requisitos ya obtenidos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad Nro. 01.1

Obtención de requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que los requisitos estén correctos, luego le hace llenar al usuario un formulario de creación de usuarios de aplicaciones

internas (literal 2.a) en este formulario van las firmas del usuario, del jefe inmediato del usuario, del director de la UTI y del responsable de la seguridad de la información y por último le hace firmar al usuario un acuerdo de confidencialidad (literal 2.b) y finalmente crea el usuario de aplicaciones internas.

2.2.6. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS DE APLICACIONES INTERNAS

2.2.6.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario
   a. Oficio autorizado por el jefe superior del usuario para dicha modificación del usuario de aplicaciones internas.
2. Requisitos previos obtenidos por el dueño del proceso
   a. Formulario de modificación de usuarios de aplicaciones internas.(**Ver Anexo 11**)

2.2.6.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo)

2.2.6.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: usuario

Tiempo estimado: 1 hora

El usuario inicia el proceso con la necesidad de pedir la modificación del usuario de aplicaciones internas, para lo cual adjunta un oficio autorizado por el jefe superior del usuario para la modificación del usuario de aplicaciones internas (literal 1.a)

Con todos los requisitos ya obtenidos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad Nro. 01.1

Obtención de requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que los requisitos estén correctos, luego le hace llenar al usuario un formulario de modificación de usuarios de aplicaciones internas (literal 2.a) y finalmente al responsable de la seguridad de la información procede a realizar dicha modificación.

2.2.7. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DE BASE DE DATOS

2.2.7.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
    - **a.** Políticas institucionales de la UTI (**Ver Anexo 7**)
    - **b.** Formulario de creación de usuarios de bases de datos (**Ver Anexo 12**)

2.2.7.2. Actores

- Responsable de la seguridad de la información
- Director de la UTI
- Usuario (Técnico de software de la UTI)

2.2.7.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de obtener la creación del usuario de las bases de datos, para lo revisa el políticas institucionales de la UTI (literal 1.a), para poder darle el tipo de privilegio de accesos a las bases de datos, luego le hace llenar al usuario un formulario de creación usuarios de bases de datos (literal 1.b), este formulario pasa donde el director de la UTI para que dé, la

autorización y visto bueno de dicha creación, si autoriza se crea el usuario, caso contrario se deberá realizar las correcciones correspondientes.

2.2.8. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS DE BASES DE DATOS

2.2.8.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
    a. Políticas institucionales de la UTI (**Ver Anexo 7**)
    b. Formulario de modificación de usuarios de bases de datos. (**Ver Anexo 13**)

2.2.8.2. Actores

- Responsable de la seguridad de la información
- Usuario (Técnico de software de la UTI)

2.2.8.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de obtener la modificación del usuario de bases de datos, para lo revisa el documento políticas institucionales de la UTI (Literal1.a), para poder ver qué tipos de modificación puede hacer, luego procede hacerle llenar al usuario un formulario de modificación de usuarios de bases de datos (literal 1.b) y finalmente procede hacer dicha modificación.

2.2.9. LEVANTAMIENTO DEL SUBPROCESO BLOQUEO DE USUARIOS DE BASES DE DATOS

2.2.9.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
    a. Políticas institucionales de la UTI (**Ver Anexo 7**)
    b. Formulario de bloque de usuarios de bases de datos. (**Ver Anexo 14**)

2.2.9.2. Actores

- Responsable de la seguridad de la información

- Director de la UTI
- Usuario (Técnico de software de la UTI)

2.2.9.3. Descripción de Actividades
Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de bloquear un usuario de bases de datos, para lo cual revisa el documento de políticas institucionales de la UTI (literal 1.a), para ver los tipos de bloqueos que existen, luego le hace llenar al usuario un formulario de bloque de usuarios de bases de datos (literal 1.b), luego se envía este formulario donde el director de la UTI, para que de la debida autorización del bloqueo, si autoriza se realiza el bloqueo, caso contrario debe realizar las correcciones correspondientes.

2.2.10. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DE SISTEMAS OPERATIVOS

2.2.10.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario
   a. Copia de la acción de personal legalizada por los altos directivos de la UNL.
   b. Petición del secretario abogado/coordinador de la carrera/administrativo financiero del área, solicitando la creación del usuario de sistemas operativos
2. Requisitos previos obtenidos por el dueño del proceso
   a. Formulario de creación de usuarios de sistemas operativos (**Ver Anexo 15**)
   b. Acuerdo de confidencialidad de los usuarios (**Ver Anexo 10**)

2.2.10.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo)

2.2.10.3. Descripción de Actividades
Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Usuario

Tiempo estimado: 2 días laborables

El usuario inicia el proceso con la necesidad de obtener la creación del usuario de sistemas operativos, para lo cual adjunta la copia de la acción de personal (literal 1.a) y una petición solicitando la creación del usuario de sistemas operativos (literal 1.b).

Con todos los requisitos ya obtenidos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad Nro. 01.1

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que los requisitos estén correctos, luego le hace llenar al usuario un formulario de creación de usuarios de sistemas operativos (literal 2.a) en este formulario van las firmas del usuario, del jefe inmediato del usuario, del director de la UTI y del responsable de la seguridad de la información y por último le hace firmar al usuario un acuerdo de confidencialidad (literal 2.b) y finalmente crea el usuario de sistemas operativos.

2.2.11. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS DE SISTEMAS OPERATIVOS

2.2.11.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario
   a. Oficio autorizado por el jefe superior del usuario para dicha modificación del usuario de sistemas operativos.
2. Requisitos previos obtenidos por el dueño del proceso
   a. Formulario de modificación de usuarios de sistemas operativos (**Ver Anexo 16**)

2.2.11.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo)

2.2.11.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: usuario

Tiempo estimado: 1 hora

El usuario inicia el proceso con la necesidad de pedir la modificación del usuario de sistemas operativos, para lo cual adjunta un oficio autorizado por el jefe superior del usuario para la modificación del usuario de sistemas operativos (literal 1.a)

Con todos los requisitos ya obtenidos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad Nro. 01.1

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que todos los requisitos estén correctos, luego le hace llenar al usuario un formulario de modificación de usuarios de sistemas operativos (literal 2.a) y finalmente el responsable de la seguridad de la información procede a realizar dicha modificación.

2.2.12. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DEL SISTEMA DE GESTIÓN ACADÉMICA

2.2.12.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario
   - **a.** Copia de la acción de personal legalizada por los altos directivos de los UNL.
   - **b.** Petición del secretario abogado/coordinador de la carrera/administrativo financiero del área, solicitando la creación del usuario del sistema de gestión académica.
2. Requisitos previos obtenidos por el dueño del proceso
   - **a.** Formulario de creación de usuarios del sistema de gestión académica. (**Ver Anexo 17**)
   - **b.** Acuerdo de confidencialidad de los usuarios (**Ver Anexo 10**)

2.2.12.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo.)

2.2.12.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Usuario

Tiempo estimado: 2 días laborables

El usuario inicia el proceso con la necesidad de obtener la creación del usuario del sistema de gestión académica, para lo cual adjunta la copia de la acción de personal (literal 1.a) y una petición solicitando la creación del usuario del sistema de gestión académica (literal 1.b).

Con todos los requisitos ya obtenidos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad N°1.1

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que los requisitos estén correctos, luego le hace llenar al usuario un formulario de creación de usuarios del sistema de gestión académica (literal 2.a) en este formulario van las firmas del usuario, del jefe inmediato del usuario, del director de la UTI y del responsable de la seguridad de la información y por último le hace firmar al usuario un acuerdo de confidencialidad (literal 2.b) y finalmente crea el usuario del sistema de gestión académica

2.2.13. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS DEL SISTEMAS DE GESTIÓN ACADÉMICA

2.2.13.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario
   a. Oficio autorizado por el jefe superior del usuario para dicha modificación del usuario del sistema de gestión académica.
2. Requisitos previos obtenidos por el dueño del proceso
   a. Formulario de modificación de usuarios del sistema de gestión académica (**Ver Anexo 18**)

2.2.13.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo)

2.2.13.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: usuario

Tiempo estimado: 1 hora

El usuario inicia el proceso con la necesidad de pedir la modificación del usuario del sistema de gestión académica, para lo cual adjunta un oficio autorizado por el jefe superior del usuario para la modificación del usuario del sistema de gestión académica (literal 1.a)

Con los requisitos ya listos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad Nro. 01.1

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que todos los requisitos estén correctos, luego le hace llenar al usuario un formulario de modificación de usuarios del sistema de gestión académica (literal 2.a) y finalmente el responsable de la seguridad de la información procede a realizar dicha modificación.

2.2.14. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS DE CUENTAS DE CORREO ELECTRÓNICO INSTITUCIONAL

2.2.14.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario
    a. Copia de la acción de personal legalizada por los altos directivos de la UNL.
2. Requisitos previos obtenidos por el dueño del proceso
    a. Políticas institucionales de la UTI (**Ver Anexo 7**)
    b. Formulario para la creación de cuenta del correo electrónico institucional. (**Ver Anexo 19**)

2.2.14.2. Actores

- Responsable de la seguridad de la información

- Usuario (Puede ser personal docente, administrativo, académico, departamentales, trabajadores, estudiantes, invitados y otros.)

2.2.14.3. Descripción de Actividades

Actividad N° 1

Obtención de los requisitos previos

Dueño de la actividad: Usuario

El usuario inicia el proceso con la necesidad de obtener la creación del usuario de cuentas de correo electrónico institucional, para lo cual adjunta la copia de la acción de personal (literal 1.a), siempre y cuando sea un usuario de tipo docente, administrativo y trabajador.

Con todos los requisitos ya obtenidos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad N°1.1

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que los requisitos estén correctos, luego revisa el documento de políticas institucionales de la UTI (literal 2.a) para saber la nomenclatura del nombre de usuario, luego le hace llenar al usuario un formulario de creación de cuentas de correo institucional (literal 2.b) excepto al usuario estudiante e invitado y procede a la creación del usuario de dicha cuenta.

2.2.15. LEVANTAMIENTO DEL PROCESO SUSPENSIÓN DE CUENTAS DE USURIOS DE CORREO ELECTRÓNICO INSTITUCIONAL

2.2.15.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario

a. Oficio autorizado por el jefe superior de la cuenta del usuario a suspender y además tener el visto bueno del director de la UTI.

2. Requisitos previos obtenidos por el dueño del procesos

a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.15.2. Actores

- Responsable de la seguridad de la información
- Director de la UTI
- Usuario (Puede ser directivo, departamental, académico, administrativo, invitado y otros.)

2.2.15.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: usuario

Tiempo estimado: 1 hora

El usuario inicia el proceso con la necesidad de suspender la cuenta de correo electrónico institucional para lo cual adjunta un oficio autorizado por el jefe superior de la cuenta del usuario a suspender (literal 1.a) y además este oficio debe tener el visto bueno y autorización del director de la UTI.

Con todos los requisitos ya obtenidos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad Nro. 01.1

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que los requisitos estén correctos, luego revisa el documento de políticas institucionales de la UTI (literal 2.a) para saber el tipo de suspensión y posteriormente procede a la suspensión de dicha cuenta.

2.2.16. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE USUARIOS A NIVEL DE SERVIDORES

2.2.16.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso.
   a. Formulario de creación de usuarios a nivel de servidores (**Ver Anexo 20**)
   b. Registro del control de acceso al data center (**Ver Anexo 21**)

2.2.16.2. Actores

- Responsable de la seguridad de la información
- Director de la UTI
- Usuario (Responsable de infraestructura)

2.2.16.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de crear usuarios a nivel de servidores, para lo cual le hace llenar al usuario un formulario de creación de usuarios a nivel de servidores (literal 1.a), este formulario va donde el director de la UTI, para que de su debida autorización, si lo hace también el responsable de la seguridad de la información, le hace llenar un registro de control de acceso al data center (literal 1.b), el registro deben de tener el visto bueno, la firma y sello del director de la UTI, y finalmente crea el usuario a nivel de servidores, caso contrario deberá hacer las correcciones correspondientes.

2.2.17. LEVANTAMIENTO DEL SUBPROCESO MODIFICACIÓN DE USUARIOS A NIVEL DE SERVIDORES

2.2.17.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso.

a. Formulario de modificación de usuarios a nivel de servidores (**Ver Anexo 22**)

2.2.17.2. Actores

- Responsable de la seguridad de la información
- Director UTI
- Usuario (Responsable de infraestructura)

2.2.17.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de modificar usuarios a nivel de servidores para lo cual le hace llenar al usuario un formulario de modificación de usuarios a nivel de servidores (literal 1.a) este formulario debe de tener la autorización del director para realizar la modificación, si la tiene el responsable de la seguridad de la información procede a ser dicha modificación, caso contrario debe realizar las debidas correcciones.

2.2.18. LEVANTAMIENTO DEL PROCESO GESTIÓN DE CONTRASEÑAS DE USUARIOS

2.2.18.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso.

a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.18.2. Actores

- Responsable de la seguridad de la información

2.2.18.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de gestionar las contraseñas de los diferentes usuarios, para lo cual hace uso del documento de políticas institucionales de la UTI (literal 1.a) para poder ver los lineamientos básicos de las contraseñas y proceder a gestionar las mismas.

Para el presente proceso es necesario levantar los siguientes subprocesos:

2.2.19. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE LAS CONTRASEÑAS

2.2.19.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.19.2. Actores

- Responsable de la seguridad de la información

2.2.19.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de crear contraseñas, para lo revisa el documento de políticas institucionales de la UTI (literal 1.a) y ve la sección de creación de contraseñas seguras, además deberá tener ciertas características obligatorias, si la contraseña cumple con las características obligatorias será creada, caso contrario deberá realizar las debidas correcciones.

2.2.20. LEVANTAMIENTO DEL SUBPROCESO RESETEO DE CONTRASEÑAS

2.2.20.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario
   a. Copia de la cédula
2. Requisitos previos obtenidos por el dueño del proceso
   a. Políticas institucionales de la UTI (**Ver Anexo 7**)
   b. Formulario de reseteo de contraseñas (**Ver Anexo 23**)

2.2.20.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo, invitado, estudiantil, trabajador y otros.)

2.2.20.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Usuario

Tiempo estimado: 10 minutos

El usuario inicia el proceso con la necesidad de resetear su contraseña, para lo cual adjunta una copia de su cédula (literal 1.a)

Con todos los requisitos ya obtenidos el usuario acude a la Unidad de Telecomunicaciones e Información y le entrega los mismos al responsable de la seguridad de la información.

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad Nro. 01.1

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 10 minutos

El responsable de la seguridad de la información, verifica que los requisitos estén correctos, luego revisa el documento de políticas institucionales de la UTI (literal 2.a) y ve qué tipo de usuario es, si es un usuario tipo directivo, departamental, académico, trabajador o administrativo, le hace llenar al usuario un formulario de reseteo de contraseñas (literal 2.b); y procede a resetear su contraseña; caso contrario si es un usuario de tipo estudiantil, procede al reseteo la misma.

2.2.21. LEVANTAMIENTO DEL SUBPROCESO RESETEO DE CONTRASEÑAS ON-LINE

2.2.21.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   - **a.** Llenar datos personales en línea.
   - **b.** Adjuntar la cédula en formato PDF.
   - **c.** Formulario de reseteo de contraseñas (**Ver Anexo 23**)

2.2.21.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo, invitado, estudiantil, trabajador y otros.)

2.2.21.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: usuario

Tiempo estimado: 30 minutos

El usuario inicia el proceso con la necesidad de resetear su contraseña, para lo cual envía un correo electrónico a la siguiente dirección soporte.uti@unl.edu.ec

Para la presente actividad hay una subactividad, en la cual el responsable de la seguridad de la información, necesita exponer sus requisitos al usuario, lo cual se muestra en la siguiente subactividad:

Sub-actividad Nro. 01.1

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 20 minutos

El responsable de seguridad de la información revisa el correo soporte.uti@unl.edu.ec, y mira la petición, luego envía un correo pidiendo que adjunte documentos (Literal 1.a,1.b), luego procede a verificar los requisitos, si están completos y correctos, procede a revisa

el documento de políticas generales de usuarios, luego ve que tipo de usuario; si es un usuario directivo, departamental, académico, trabajador o administrativo le envía al usuario un formulario de reseteo de contraseñas para que lo llene, luego el usuario llena el formulario y lo reenvía al formulario a la misma dirección y finalmente procede al reseteo correspondiente de la contraseña y el responsable de la seguridad de la información le envía la contraseña nueva al usuario, si es un usuario estudiantil o invitado y le enviará un correo al solicitante con la contraseña nueva, caso contrario si los requisitos están incorrectos o incompletos se le envía un correo diciendo corregir requisitos.

2.2.22. LEVANTAMIENTO DE SUBPROCESO USO DE LAS CONTRASEÑAS

2.2.22.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   a. Políticas institucionales de la UTI (**Ver Anexo 7)**

2.2.22.2. Actores

- Responsable de la seguridad de la información
- Usuario (Puede ser directivo, departamental, académico o administrativo, estudiantil, trabajador, invitado y otros.)

2.2.22.3. Descripción de Actividades

Actividad Nro. 01

Obtención de los requisitos previos

Dueño de la actividad: Responsable de la seguridad de la información

Tiempo estimado: 15 minutos

El responsable de la seguridad de la información inicia el proceso con la necesidad de hacerles recordar sobre el uso de las contraseñas a los diferentes usuarios que forman parte de la comunidad universitaria, para lo cual revisa el documento de políticas institucionales de la UTI (literal 1.a) y procede a recordarles sobre el uso de las mismas, enviándoles un correo o haciendo una publicación en la página de la UNL.

2.2.23. LEVANTAMIENTO DEL PROCESO COPIAS DE SEGURIDAD

2.2.23.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso

a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.23.2. Actores

- Técnico de software

2.2.23.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: Técnico de software

Tiempo estimado: de 10 minutos hasta 3 horas

El técnico de software inicia el proceso con la necesidad de realizar copias de seguridad de las diferentes bases de datos, para lo cual revisa el documento políticas institucionales de la UTI (literal 1.a) y ve los lineamientos a tomarse en cuenta para poder respaldar la información y así poder gestionar las copias de seguridad.

Para el presente proceso es necesario levantar los siguientes subprocesos:

2.2.24. LEVANTAMIENTO DEL SUBPROCESO CREACIÓN DE RESPALDOS

2.2.24.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.24.2. Actores

- Técnico de software

2.2.24.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: Técnico de software

Tiempo estimado: 10 minutos

El técnico de software inicia el proceso con la necesidad de realizar la creación de respaldos, para lo cual revisa el documento políticas institucionales de la UTI (literal 1.a) y ve los lineamientos a tomarse en cuenta para la creación de los respaldos, si posee todos

estos lineamientos se procederá a la creación de respaldo, y procederá hacer la copia de seguridad pertinente, caso contrario deberá realiza las debidas correcciones.

2.2.25. LEVANTAMIENTO DEL SUBPROCESO CODIFICACIÓN DE RESPALDOS

2.2.25.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.25.2. Actores

- Técnico de software

2.2.25.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: Técnico de software

Tiempo estimado: 10 minutos

El técnico de software inicia el proceso con la necesidad de realizar la codificación de respaldos, para lo cual revisa el documento de políticas institucionales de la UTI (literal 1.a) y ve los lineamientos a tomarse en cuenta, si posee todos estos lineamientos de codificación, se procederá a la codificación de respaldo, caso contrario deberá realiza las debidas correcciones.

2.2.26. LEVANTAMIENTO DEL SUBPROCESO ALMACENAMIENTO DE RESPALDOS

2.2.26.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.26.2. Actores

- Técnico de software

2.2.26.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: Técnico de software

Tiempo estimado: 10 minutos

El técnico de software inicia el proceso con la necesidad de realizar el almacenamiento de respaldos, para lo cual revisa el documento de políticas institucionales de la UTI (literal 1.a) y ve los lineamientos a tomarse en cuenta para el almacenamiento de respaldos, si posee todos estos lineamientos se procederá al almacenamiento de respaldo, además hará uso del formato de eventualidades de respaldos en el cual registrará el control de los almacenamiento de los respaldos, caso contrario si no pose con todos los lineamientos deberá realiza las correcciones pertinentes.

2.2.27. LEVANTAMIENTO DEL SUBPROCESO PRUEBAS DE RESPALDOS

2.2.27.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   a. Políticas institucionales de la UTI (**Ver Anexo 7)**

2.2.27.2. Actores

- Técnico de software

2.2.27.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: Técnico de software

Tiempo estimado: 15 minutos

El técnico de software inicia el proceso con la necesidad de realizar las pruebas de respaldos, para lo cual revisa el documento de políticas institucionales de la UTI (literal 1.a) y ve los lineamientos a tomarse en cuenta para las pruebas de respaldos, si posee todos estos lineamientos se procederá a la realización de las pruebas de respaldo, caso contrario deberá realiza las debidas correcciones.

2.2.28. LEVANTAMIENTO DEL SUBPROCESO PROCEDIMIENTOS DE RECUPERACIÓN

2.2.28.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso

a. Políticas institucionales de la UTI (**Ver Anexo 7**)

2.2.28.2. Actores

- Técnico de software

2.2.28.3. Descripción de Actividades

Actividad Nro. 01

Obtención de requisitos previos

Dueño de la actividad: Técnico de software

Tiempo estimado: 10 minutos

El técnico de software inicia el proceso con la necesidad de realizar los procedimientos de recuperación, para lo cual revisa el documento de Políticas institucionales de la UTI (literal 1.a) y ve los lineamientos a tomarse en cuenta para los procedimientos de recuperación, si posee todos estos lineamientos se procederá a realizar los procedimientos de recuperación, caso contrario deberá realiza las debidas correcciones.

FASE 3: DEFINICIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

3.1. Definir los procesos de seguridad de la información más esenciales dentro de la Unidad de Telecomunicaciones e Información

En esta fase se definieron los procesos de seguridad de la información más fundamentales dentro de la Unidad de Telecomunicaciones e Información (**Ver Anexo 25**). Así mismo se hará una gestión de los procesos existentes, con la ayuda de la norma ISO/IEC 27002:2013 (**Ver Anexo 5**), y la metodología SIPOC.

Procesos definidos

- Gestión de activos
    - Clasificación de la información
    - Entrega de información en medios de almacenamiento
- Control de accesos
    - Control de accesos físicos a las instalaciones de la UTI
    - Gestión de acceso de usuarios
    - Control de accesos a sistemas y aplicaciones
- Seguridad en la operativa
    - Generar copias de seguridad
- Seguridad en las telecomunicaciones
    - Entrega de la información con partes externas

3.2. Propuesta de los procesos de seguridad de la información

PROCESO PADRE: GESTIÓN DE ACTIVOS

PROCESO 1: CLASIFICACIÓN DE LA INFORMACIÓN

1.1. Requisitos y Documentación

Para la ejecución de la situación actual del proceso Clasificación de la Información en la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja son indispensables los siguientes documentos:

1. Requisitos previos obtenidos por el dueño del proceso

a. Documento de políticas generales de la seguridad de la información (Políticas propuestas y no están aprobadas por los altos directivos, por tal motivo no se las ha puesto en anexos).

1.2. Actores

Las personas que llevan a cabo la situación actual del proceso Clasificación de la Información son denominados actores, puesto que interactúan directamente con el mismo y además son responsables de realizarlo en su totalidad. A continuación, se nombran los actores del proceso Clasificación de la Información.

TABLA X:

ACTORES DEL PROCESO CLASIFICACIÓN DE LA INFORMACIÓN

Cargo	**Rol**
Funcionario UTI (Director, subdirector, técnicos, desarrolladores, responsable de infraestructura, administrador de la seguridad de la información, administrador de la base de datos)	Funcionario UTI (Director, subdirector, técnicos, desarrolladores, responsable de infraestructura, administrador de la seguridad de la información, administrador de la base de datos)

1.3. Descripción de Actividades

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**
1. El funcionario de la UTI, obtiene información sin clasificar. 2. Aplica las políticas de la seguridad de la información (**literal 1.a**). 3. Valida si cumple los criterios de seguridad de la información (confidencialidad, integridad, disponibilidad). 3.1. Si no cumple criterios sigue en el paso 3. 3.2. Si cumple criterios sigue en el paso 4 4. Revisar las directrices de clasificación. 5. Obtiene información clasificada con las respectivas directrices.	Funcionario UTI	De 15 a 20 minutos

6. Procede a etiquetar la información de acuerdo a su tipo. 7. Información clasificada. 8. Envía la información clasificada a los funcionarios de la UTI según su nivel de funcionario. 9. Recibe la información según su nivel.		

1.4. Diagramas

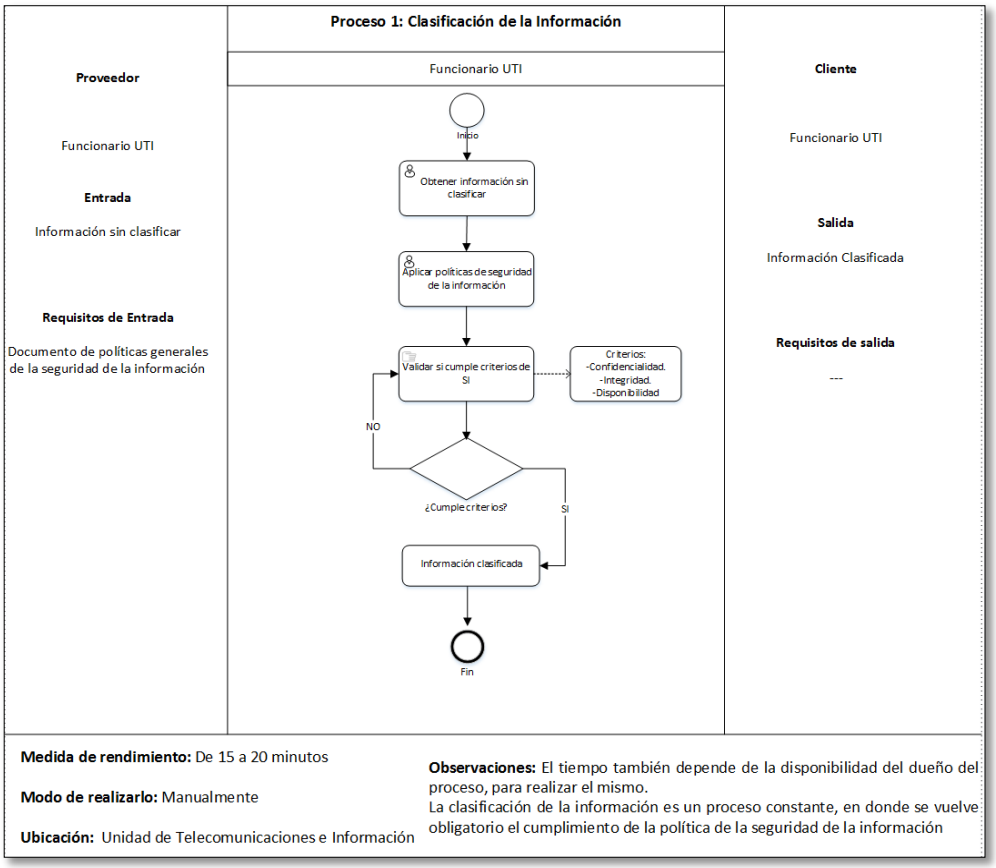


Fig. 14 Diagrama resumido del proceso definido clasificación de la información

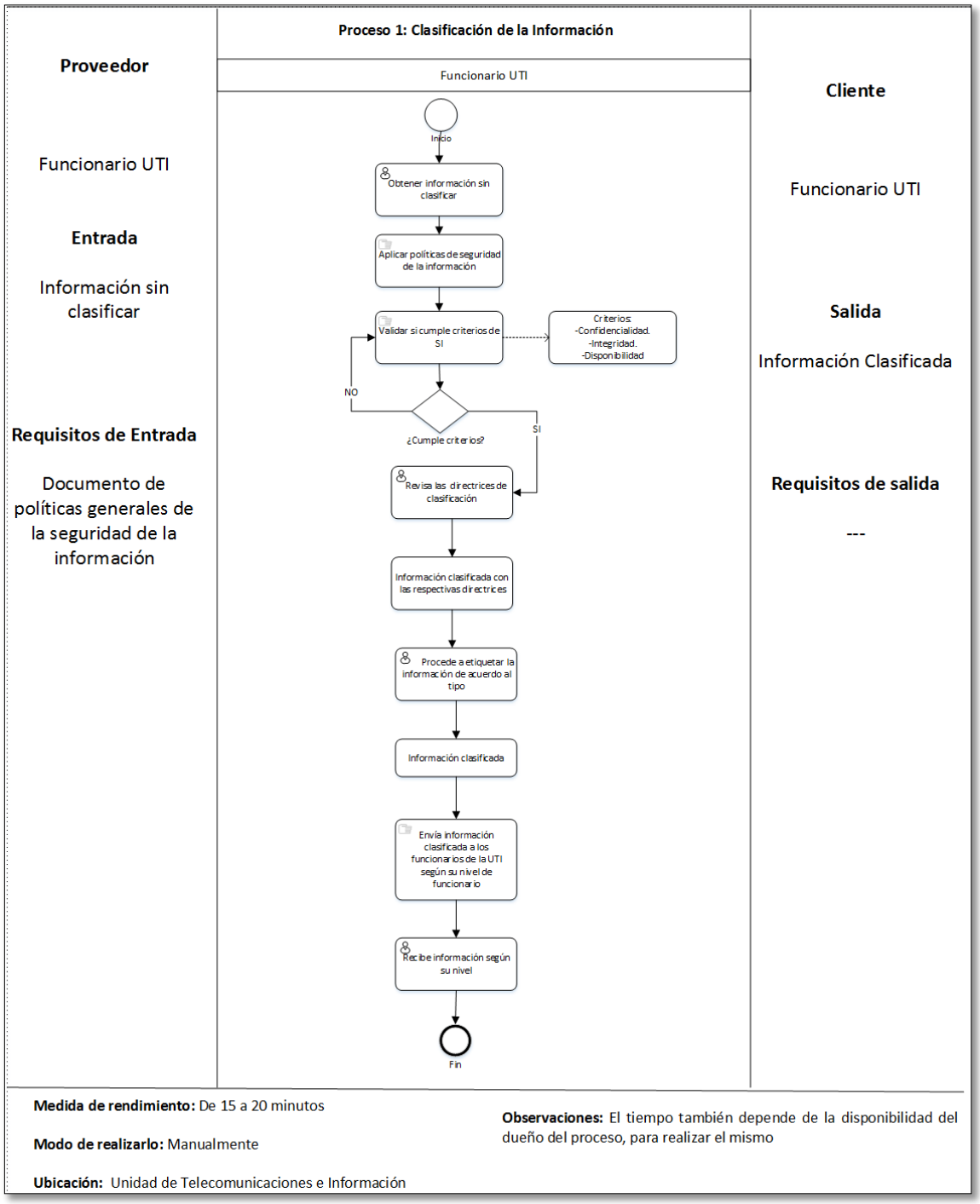


Fig. 15 Diagrama detallado del proceso definido clasificación de la información

1.5. Documentación

	Universidad Nacional de Loja **UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN**		
DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN			
Proceso Padre	Gestión de activos	**Código**	P1
Proceso	Clasificación de la información		
Subproceso			
Objetivo	Asegurar que se aplique un nivel de protección adecuado a la información.		
Responsable (s)	Funcionario UTI		
Entradas			
Proveedor	**Entrada**	**Requisitos de entrada**	
Funcionario UTI	Información sin clasificar	Documento de políticas generales de la seguridad de la información	
Descripción			
1. El funcionario de la UTI, obtiene información sin clasificar. 2. Aplica las políticas de la seguridad de la información. 3. Valida si cumple los criterios de seguridad de la información (confidencialidad, integridad, disponibilidad). 3.1. Si no cumple criterios sigue en el paso 3. 3.2. Si cumple criterios sigue en el paso 4 4. Revisar las directrices de clasificación. 5. Obtiene información clasificada con las respectivas directrices. 6. Procede a etiquetar la información de acuerdo a su tipo. 7. Información clasificada. 8. Envía la información clasificada a los funcionarios de la UTI según su nivel de funcionario. 9. Recibe la información según su nivel.			
Salidas			
Cliente	**Salida**	**Requisitos de salida**	
Funcionarios UTI	Información clasificada		
Medida de rendimiento	De 15 a 20 minutos		
Glosario, siglas y referencias			

PROCESO 2: ENTREGA DE INFORMACIÓN EN MEDIOS DE ALMACENAMIENTO

2.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario

- **a.** Solicitud para el manejo de los soportes de almacenamiento autorizada por el jefe superior del usuario.

2. Requisitos previos obtenidos por el dueño del proceso

- **a.** Formulario de soportes de almacenamiento (**Ver Anexo 26**)
- **b.** Registro de autorización de los soportes de almacenamiento (**Ver Anexo 27**)

2.2. Actores

TABLA XI:
ACTORES DEL PROCESO ENTREGA DE INFORMACIÓN EN MEDIOS DE ALMACENAMIENTO

Cargo	**Rol**
Administrador de seguridad de la información	Administrador de seguridad de la información
Usuario	Usuario

2.3. Descripción de Actividades

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**
1. El usuario solicita información al administrador de la seguridad de la información. 2. El administrador entrega requisitos y documentación.	Administrador dela seguridad de la información	De 8 a 10 minutos

3. El usuario adjunta requisitos y documentación. (**literal 1.a**) 4. El usuario entrega los requisitos al administrador de la seguridad de la información para su verificación. 5. El administrador recibe y valida los requisitos. 5.1. Si no están correctos, el administrador entrega la documentación al usuario para que realiza las modificaciones pertinentes, sigue en el paso 6. 5.2. Si están correctos sigue en el paso 7. 6. El usuario recibe requisitos para corregirlos, sigue en el paso 4. 7. El administrador, entrega al usuario un formulario de soportes de almacenamiento para que lo llene (**literal 2.a**). 8. El usuario recibe formulario y lo llena. 9. El usuario entrega formulario lleno al administrador. 10. El administrador recibe y revisa que esté llenado correctamente. 10.1. Sino esta llenado correctamente, el administrador de la seguridad de la información entrega al usuario para su modificación. Sigue en el paso 11. 10.2. Si está llenado correctamente, sigue en el paso 12.		

11. El usuario recibe formulario para corregirlo, y sigue en el paso 9. 12. El administrador le entrega al usuario un registro de autorización para los soportes de almacenamiento para que lo llene (**literal 2.b**), 13. El usuario recibe y llena el registro de autorización. 14. El usuario le entrega el registro llenado al administrador 15. El administrador recibe y revisa que este llenado correctamente el registro. 15.1. Sino están llenado correctamente, el administrador entrega registro al usuario para su modificación, sigue en el paso 16. 15.2. Si esta llenado correctamente, sigue en el paso 17. 16. El usuario recibe registro para corregirlo, sigue en el paso14. 17. El administrador genera información. 18. Llama al proceso clasificación de la información. 19. Valida y entrega la información 20. Finalmente el usuario recibe información en el soporte.		

2.4. Diagramas

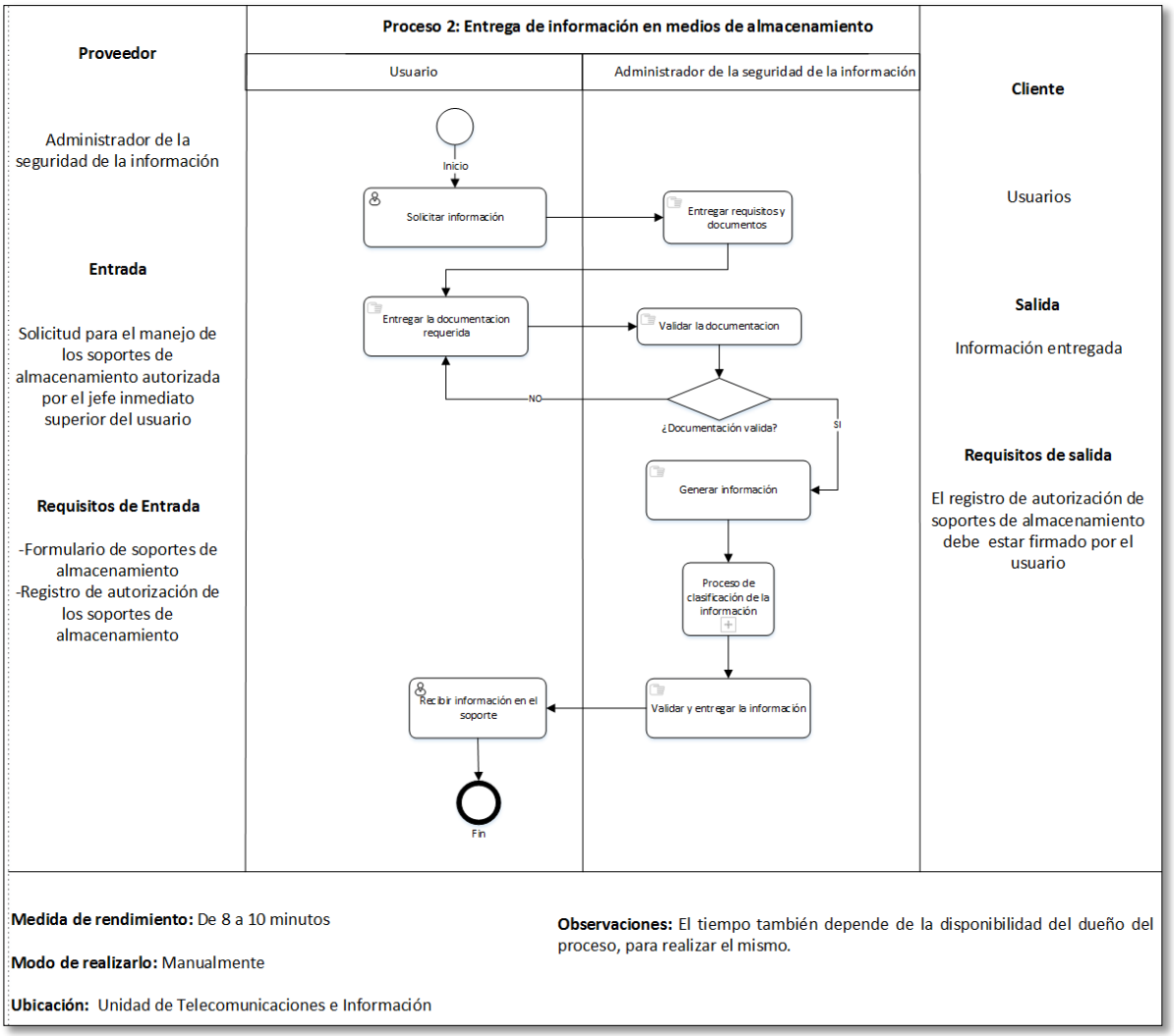


Fig. 16 Diagrama resumido del proceso definido entrega de información en medios de almacenamiento

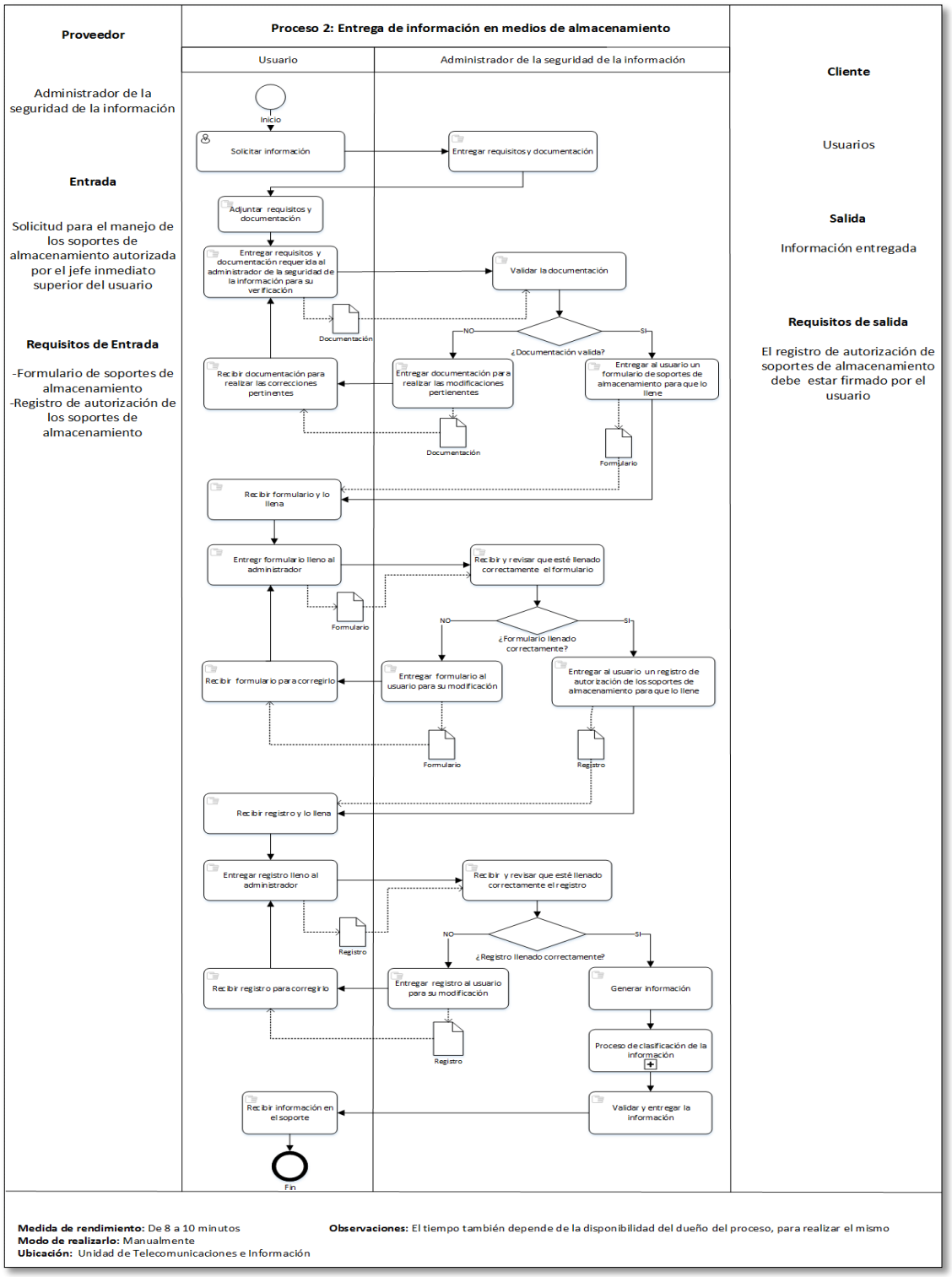


Fig. 17 Diagrama detallado del proceso definido entrega de información en medios de almacenamiento

2.5. Documentación

<table>
<tr><td></td><td colspan="3">Universidad Nacional de Loja

UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN</td></tr>
<tr><td colspan="4">DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>Proceso padre</td><td>Gestión de activos</td><td>Código</td><td>P2</td></tr>
<tr><td>Proceso</td><td colspan="3">Entrega de información en medios de almacenamiento</td></tr>
<tr><td>Subproceso</td><td colspan="3"></td></tr>
<tr><td>Objetivo</td><td colspan="3">Proteger la información almacenada en soportes de almacenamiento.</td></tr>
<tr><td>Responsable (s)</td><td colspan="3">Administrador de la seguridad de la información</td></tr>
<tr><td colspan="4">Entradas</td></tr>
<tr><td>Proveedor</td><td>Entrada</td><td colspan="2">Requisitos de entrada</td></tr>
<tr><td>Administrador de la seguridad de la información</td><td>Solicitud para el manejo de los soportes de almacenamiento, autorizada por el jefe inmediato superior de usuario</td><td colspan="2">-Formulario de los soportes de almacenamiento.
-Registro de autorización de los soportes de almacenamiento.</td></tr>
<tr><td colspan="4">Descripción</td></tr>
<tr><td colspan="4">1. El usuario solicita información al administrador de la seguridad de la información.
2. El administrador entrega requisitos y documentación.
3. El usuario adjunta requisitos y documentación.
4. El usuario entrega los requisitos al administrador de la seguridad de la información para su verificación.
5. El administrador recibe y valida los requisitos.
5.1. Si no están correctos, el administrador entrega la documentación al usuario para que realiza las modificaciones pertinentes, sigue en el paso 6.
5.2. Si están correctos sigue en el paso 7.
6. El usuario recibe requisitos para corregirlos, sigue en el paso 4.
7. El administrador, entrega al usuario un formulario de soportes de almacenamiento para que lo llene.
8. El usuario recibe formulario y lo llena.
9. El usuario entrega formulario lleno al administrador.
10. El administrador recibe y revisa que esté llenado correctamente.</td></tr>
</table>

10.1. Sino esta llenado correctamente, el administrador de la seguridad de la información entrega al usuario para su modificación. Sigue en el paso 11.

10.2. Si está llenado correctamente, sigue en el paso 12.

11. El usuario recibe formulario para corregirlo, y sigue en el paso 9.
12. El administrador le entrega al usuario un registro de autorización para los soportes de almacenamiento para que lo llene.
13. El usuario recibe y llena el registro de autorización.
14. El usuario le entrega el registro llenado al administrador
15. El administrador recibe y revisa que este llenado correctamente el registro.

15.1. Sino están llenado correctamente, el administrador entrega registro al usuario para su modificación, sigue en el paso 16.

15.2. Si esta llenado correctamente, sigue en el paso 17.

16. El usuario recibe registro para corregirlo, sigue en el paso14.
17. El administrador genera información.
18. Llama al proceso clasificación de la información.
19. Valida y entrega la información
20. Finalmente el usuario recibe información en el soporte.

Salidas		
Cliente	**Salida**	**Requisitos de salida**
Usuarios	Información entregada	-El registro de autorización de soportes de almacenamiento debe estar firmado por el usuario
Medida de rendimiento	De 8 a 10 minutos	
Glosario, siglas y referencias		

PROCESO PADRE: CONTROL DE ACCESOS

PROCESO 3: CONTROL DE ACCESOS FÍSICOS A LAS INSTALACIONES DE LA UTI

3.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso

a. Registro de control al data center (**Ver Anexo 21**)

3.2. Actores

TABLA XII:
ACTORES DEL PROCESO CONTROL DE ACCESOS FÍSICOS A LAS INSTALACIONES DE LA UTI

Cargo	**Rol**
Administrador de la seguridad de la información	Administrador de la seguridad de la información
Director UTI	Director UTI
Usuario	Responsable de infraestructura, técnico de telefonía.

3.3. Descripción de Actividades

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**
1. El usuario solicita acceso al director de la UTI. 2. El director de la UTI procede a dar autorización. 2.1. Si no da autorización, sigue en el paso 1. 2.2. Si da autorización, sigue en el paso 3. 3. El director informa al administrador para que realice el registro correspondiente. 4. El administrador hace uso de un registro.(**Literal 1.a**) 5. El administrador revisa que el registro tenga la firma y sello del director de la UTI. 5.1. Si no tiene la firma y sello, el administrador de la seguridad de la información, envía el registro donde el director de la UTI, sigue en el paso 6. 5.2. Si tiene la firma y sello, sigue en el paso 9. 6. El director de la UTI recibe registro. 7. Pone sello y firma en el registro.	Administrador de seguridad de la información	De 5 a 8 minutos

8. Envía el registro al administrador de la seguridad de la información, sigue en el paso 5. 9. El administrador de la seguridad de la información, entrega al usuario el registro para que lo llene. 10. El usuario recibe registro y lo llena 11. El usuario entrega registro lleno al administrador de la seguridad de la información. 12. El administrador recibe y verifica que esté lleno el registro. 12.1. Si no está llenado correctamente el registro, entrega el registro al usuario para su modificación, sigue en el paso 11. 12.2. Si esta llenado correctamente, sigue en el paso 13 13. El administrador informa al usuario que puede ingresar al data center, acompañado del responsable de infraestructura. 14. El usuario realiza los trabajos correspondientes. 15. Acude donde el administrador para registrar su salida. 16. El administrador entrega el registro al usuario para que registre su salida. 17. El usuario recibe registro. 18. Finalmente el usuario registra su salida.		

3.4. Diagramas

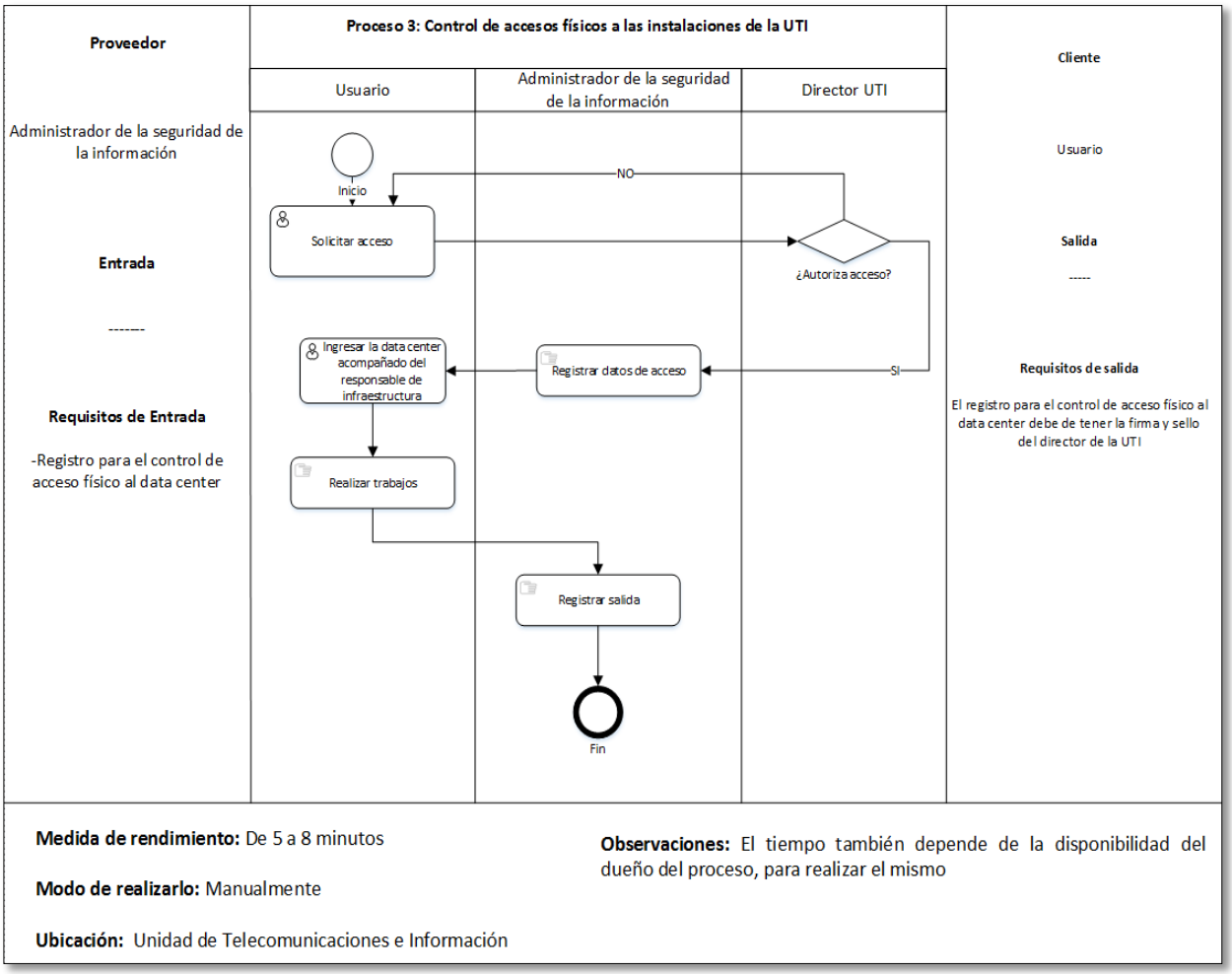


Fig. 18 Diagrama resumido del proceso definido control de accesos físicos a las instalaciones de la UTI

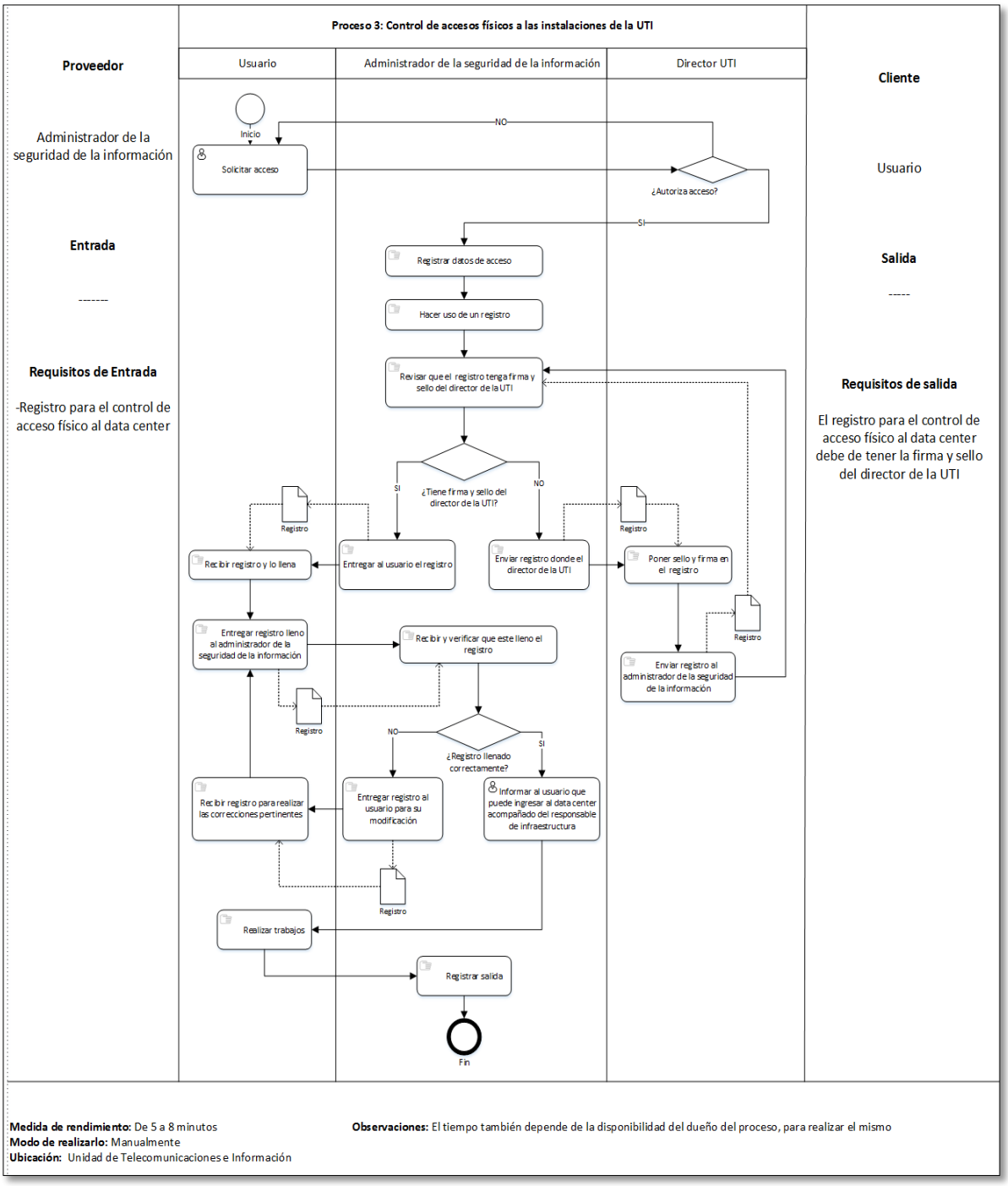


Fig. 19 Diagrama detallado del proceso definido control de accesos físicos a las instalaciones de las UTI

3.5. Documentación

<table>
<tr><td></td><td colspan="4">Universidad Nacional de Loja

UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN</td></tr>
<tr><td colspan="5">DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>Proceso padre</td><td colspan="2">Control de accesos</td><td>Código</td><td>P3</td></tr>
<tr><td>Proceso</td><td colspan="4">Control de accesos físicos a las instalaciones de la UTI</td></tr>
<tr><td>Subproceso</td><td colspan="4"></td></tr>
<tr><td>Objetivo</td><td colspan="4">Controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.</td></tr>
<tr><td>Responsable (s)</td><td colspan="4">Administrador de la seguridad de la información</td></tr>
<tr><td colspan="5">Entradas</td></tr>
<tr><td>Proveedor</td><td colspan="2">Entrada</td><td colspan="2">Requisitos de entradas</td></tr>
<tr><td>Administrador de la seguridad de la información</td><td colspan="2"></td><td colspan="2">-Registro para el control de acceso físico al data center.</td></tr>
<tr><td colspan="5">Descripción</td></tr>
<tr><td colspan="5">1. El usuario solicita acceso al director de la UTI.
2. El director de la UTI procede a dar autorización.
2.1. Si no da autorización, sigue en el paso 1.
2.2. Si da autorización, sigue en el paso 3.
3. El director informa al administrador para que realice el registro correspondiente.
4. El administrador hace uso de un registro.
5. El administrador revisa que el registro tenga la firma y sello del director de la UTI.
5.1. Si no tiene la firma y sello, el administrador de la seguridad de la información, envía el registro donde el director de la UTI, sigue en el paso 6.
5.2. Si tiene la firma y sello, sigue en el paso 9.
6. El director de la UTI recibe registro.
7. Pone sello y firma en el registro.
8. Envía el registro al administrador de la seguridad de la información, sigue en el paso 5.
9. El administrador de la seguridad de la información, entrega al usuario el registro para que lo llene.</td></tr>
</table>

10. El usuario recibe registro y lo llena
11. El usuario entrega registro lleno al administrador de la seguridad de la información.
12. El administrador recibe y verifica que esté lleno el registro.
    12.1. Si no está llenado correctamente el registro, entrega el registro al usuario para su modificación, sigue en el paso 11.
    12.2. Si esta llenado correctamente, sigue en el paso 13
13. El administrador informa al usuario que puede ingresar al data center, acompañado del responsable de infraestructura.
14. El usuario realiza los trabajos correspondientes.
15. Acude donde el administrador para registrar su salida.
16. El administrador entrega el registro al usuario para que registre su salida.
17. El usuario recibe registro.
18. Finalmente el usuario registra su salida.

Salidas		
Cliente	**Salida**	**Requisitos de salida**
Usuario		El registro para el control de accesos físico al data center debe tener la firma y sello del director de la UTI
Medida de rendimiento	De 5 a 8 minutos	
Glosario, siglas y referencias		

PROCESO 4: GESTIÓN DE ACCESO DE USUARIOS

4.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el usuario

- **a.** Copia de la acción de personal legalizada por los altos directivos de la UNL.
- **b.** Petición del secretario abogado/coordinador de la carrera/administrativo financiero del área, o jefe departamental solicitando la creación del usuario.
- **c.** Oficio autorizado por el jefe superior del usuario para dicha modificación.
- **d.** Oficio autorizado por el jefe superior del usuario de la cuenta del usuario a suspender.
- **e.** Oficio autorizado por el jefe superior del usuario para el bloque del usuario.

2. Requisitos previos obtenidos por el dueño del proceso

a. Formularios para cada tipo de usuario

4.2. Actores

TABLA XIII:
ACTORES DEL PROCESO GESTIÓN DE ACCESO DE USUARIOS

Cargo	**Rol**
Administrador de la seguridad de la información	Administrador de la seguridad de la información
Usuario	Puede ser docente, administrativo, académico, departamentales, trabajadores, estudiantes, invitados, administrador de la base de datos, responsable de infraestructura y otros.

4.3. Descripción de Actividades

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**
1. El usuario solicita la creación, modificación, bloqueo o suspensión del usuario. 2. El administrador entrega requisitos y documentos. 3. El usuario adjunta requisitos previamente autorizados ya sean estos por el jefe inmediato superior o jefe departamental. 4. Entrega los requisitos al administrador de la seguridad de la información. (**literal 1.a hasta 1.e**) 5. El administrador recibe y revisa los requisitos.	Administrador de seguridad de la información	De 3 a 5 minutos

5.1. Si no están correctos, el administrador entrega requisitos al usuario para su modificación, sigue en el paso 6. 5.2. Si están correctos los requisitos, sigue en el paso 7 6. El usuario recibe requisitos para su modificación y los realiza, sigue en el paso 4. 7. El administrador hace uso de formularios según los requerimientos de los requisitos. 8. El administrador para gestionar los diferentes usuarios debe realizar los siguientes subprocesos de acuerdo a los requerimientos de los requisitos. 9. Entre los subprocesos tenemos creación de usuarios, modificación de usuarios y bloqueo de usuarios y suspensión de usuarios de cuentas de correo electrónico institucional.		

4.4. Diagramas

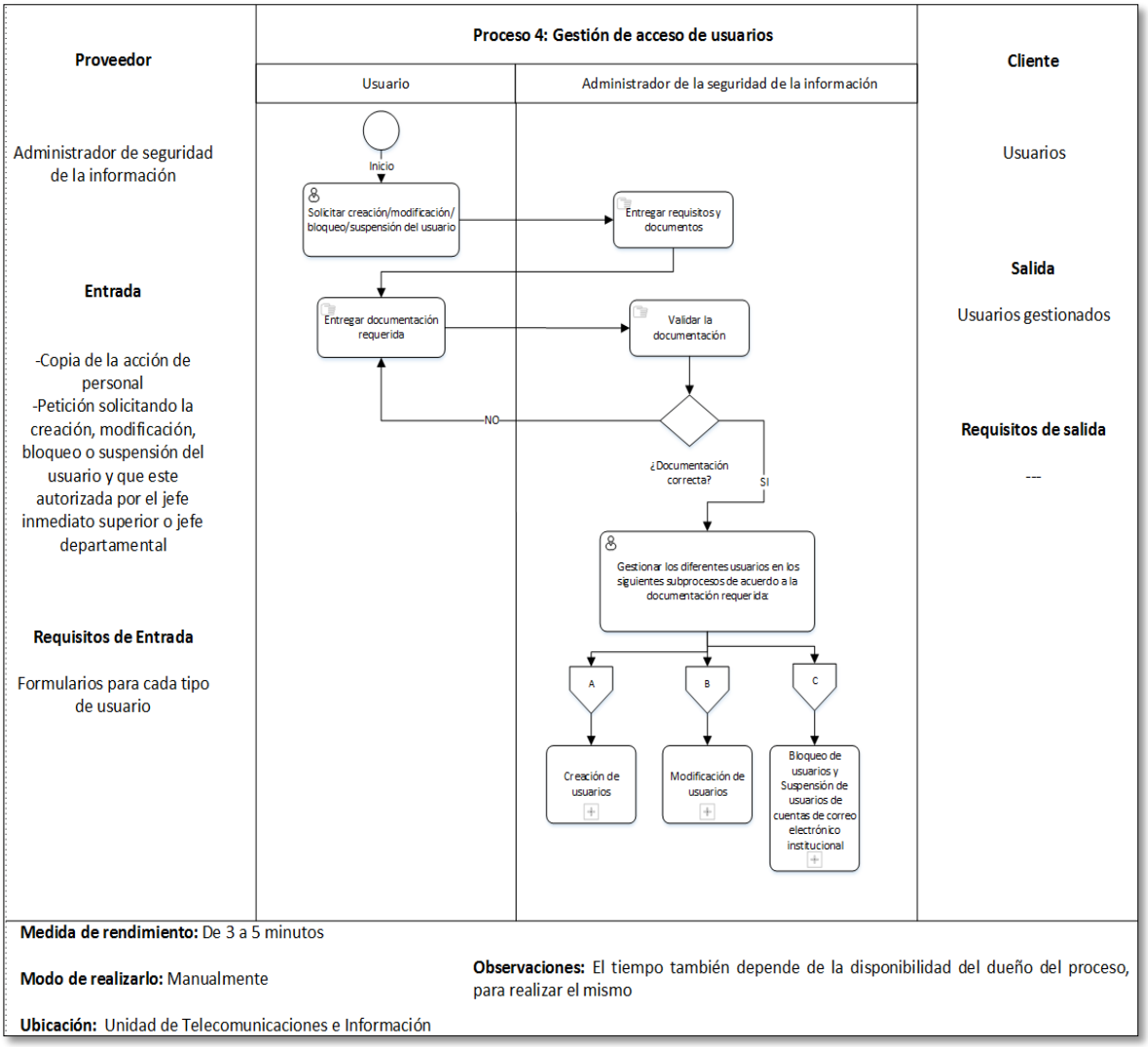


Fig. 20 Diagrama resumido del proceso definido gestión de acceso de usuarios

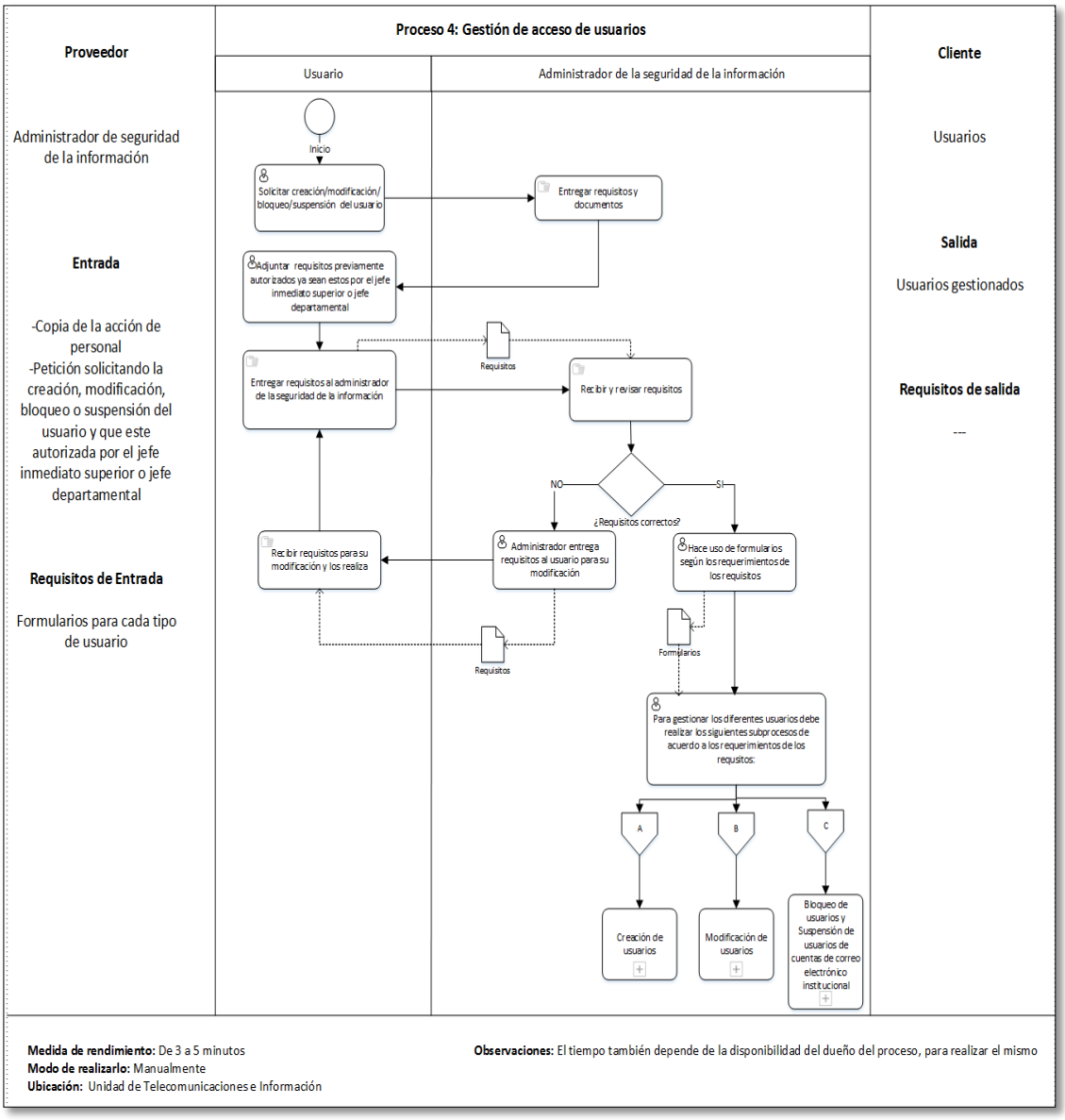


Fig. 21 Diagrama detallado del proceso definido gestión de acceso de usuarios

4.5. Documentación

<table>
<tr><td></td><td colspan="4">Universidad Nacional de Loja

UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN</td></tr>
<tr><td colspan="5">DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>Proceso padre</td><td colspan="2">Control de accesos</td><td>Código</td><td>P4</td></tr>
<tr><td>Proceso</td><td colspan="4">Gestión de acceso de usuarios</td></tr>
<tr><td>Subproceso</td><td colspan="4"></td></tr>
<tr><td>Objetivo</td><td colspan="4">Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.</td></tr>
<tr><td>Responsable (s)</td><td colspan="4">Administrador de la seguridad de la información</td></tr>
<tr><td colspan="5">Entradas</td></tr>
<tr><td>Proveedor</td><td colspan="2">Entrada</td><td colspan="2">Requisitos de entrada</td></tr>
<tr><td>Administrador de la seguridad de la información</td><td colspan="2">-Copia de la acción de personal.
-Petición solicitando ya sea la creación, modificación, bloque o suspensión del usuario, además la petición debe de estar autorizada por el jefe inmediato superior o jefe departamental del usuario</td><td colspan="2">Formularios para cada tipo de usuario.</td></tr>
<tr><td colspan="5">Descripción</td></tr>
<tr><td colspan="5">1. El usuario solicita la creación, modificación, bloqueo o suspensión del usuario.
2. El administrador entrega requisitos y documentos.
3. El usuario adjunta requisitos previamente autorizados ya sean estos por el jefe inmediato superior o jefe departamental.
4. Entrega los requisitos al administrador de la seguridad de la información.
5. El administrador recibe y revisa los requisitos.
5.1. Si no están correctos, el administrador entrega requisitos al usuario para su modificación, sigue en el paso 6.
5.2. Si están correctos los requisitos, sigue en el paso 7
6. El usuario recibe requisitos para su modificación y los realiza, sigue en el paso 4.
7. El administrador hace uso de formularios según los requerimientos de los requisitos.
8. El administrador para gestionar los diferentes usuarios debe realizar los siguientes subprocesos de acuerdo a los requerimientos de los requisitos.</td></tr>
</table>

9. Entre los subprocesos tenemos creación de usuarios, modificación de usuarios y bloqueo de usuarios y suspensión de usuarios de cuentas de correo electrónico institucional.		
Salidas		
Cliente	**Salida**	**Requisitos de salida**
Usuarios	Usuarios gestionados	
Medida de rendimiento	De 3 a 5 minutos	
Glosario, siglas y referencias		

P4-SUBPROCESO 1: CREACIÓN DE USUARIOS

4.1.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso

- **a.** Formulario de creación de usuarios de aplicaciones internas.(**Ver Anexo 9**)
- **b.** Formulario de creación de usuarios de sistemas operativos.(**Ver Anexo 17**)
- **c.** Formulario de creación de usuarios del sistema de gestión académica.(**Ver Anexo17**)
- **d.** Formulario de creación de usuarios de bases de datos.(**Ver Anexo12**)
- **e.** Formulario de creación de usuarios a nivel de servidores. (**Ver Anexo 20**)
- **f.** Formulario de creación de usuarios de cuentas de correo electrónico institucional. (**Ver Anexo 19**)
- **g.** Acuerdo de confidencialidad de los usuarios (**Ver Anexo 10**)

4.1.2. Actores

TABLA XIV:
ACTORES DEL SUBPROCESO CREACIÓN DE USUARIOS

Cargo	**Rol**
Administrador de la seguridad de la información	Administrador de la seguridad de la información
Director UTI	Director UTI
Usuario	Puede ser docente, administrativo, académico, departamentales, trabajadores, estudiantes, invitados, administrador de la base de datos, responsable de infraestructura y otros.

4.1.3. Descripción de Actividades

Descripción	Dueño de la actividad	Tiempo de ejecución
1. El administrador llena formulario según la petición de los requisitos. 2. Si el formulario llenado es de bases de datos o de servidores. 2.1. Envía al director de la UTI para su autorización. 2.2. El director recibe y revisa el formulario para dar autorización 2.3. Si no da autorización, el director envía el formulario al administrador para que realice las modificaciones pertinentes. 2.4. El administrador recibe formulario para realizar las modificaciones pertinentes, sigue en el paso 2.1 2.5. Si da autorización, el administrador recibe formulario autorizado, sigue en el paso 4. 3. Si el formulario llenado no es de base de datos o servidores, sigue en el paso 4 4. El administrador entrega formulario al usuario para que lo legalice. 5. El usuario recibe formulario para legalizarlo. 6. Entrega formulario legalizado al administrador. 7. El administrador recibe y revisa el formulario que este legalizado correctamente. 7.1. Si no está legalizado correctamente el administrador entrega formulario al	Administrador de la seguridad de la información	De 10 a 15 minutos

usuario para que lo firme correctamente. 7.2. Usuario recibe formulario para legalizar correctamente, sigue en el paso 6 7.3. Si está legalizado correctamente, sigue en el paso 8. 8. Entrega acuerdo de confidencialidad al usuario para que lo lea y lo firme. 9. El usuario recibe acuerdo para leer y firmar. 10. Entrega acuerdo firmado al administrador. 11. El administrador recibe y revisa el acuerdo que este firmado correctamente. 11.1. Si no está firmado correctamente el administrador, entrega acuerdo al usuario para que lo firme correctamente. 11.2. El usuario recibe acuerdo para firmar correctamente, sigue en el paso 10. 11.3. Si está firmado correctamente sigue en el paso 12. 12. El administrador crea el usuario. 13. Entrega al usuario su password y nombre de usuario. 14. Finalmente el usuario recibe password y nombre de usuario.		

4.1.4. Diagramas

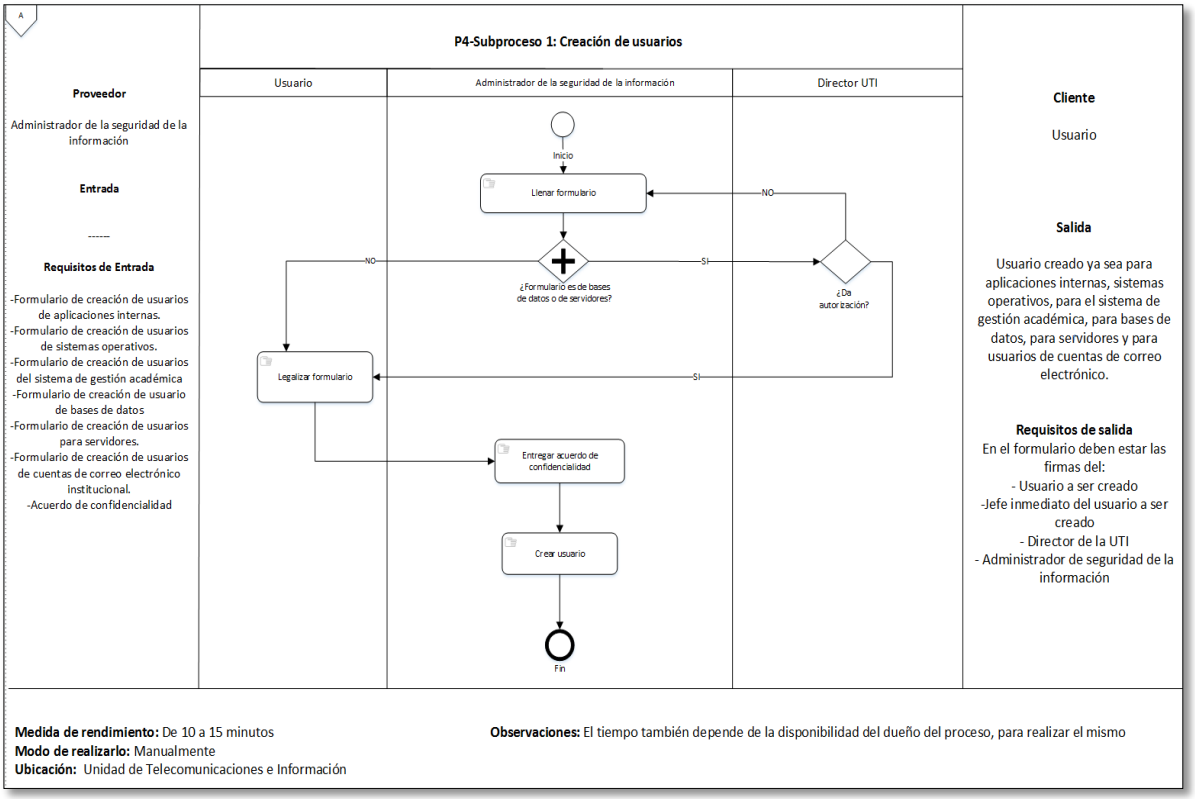


Fig. 22 Diagrama resumido del subproceso definido creación de usuarios

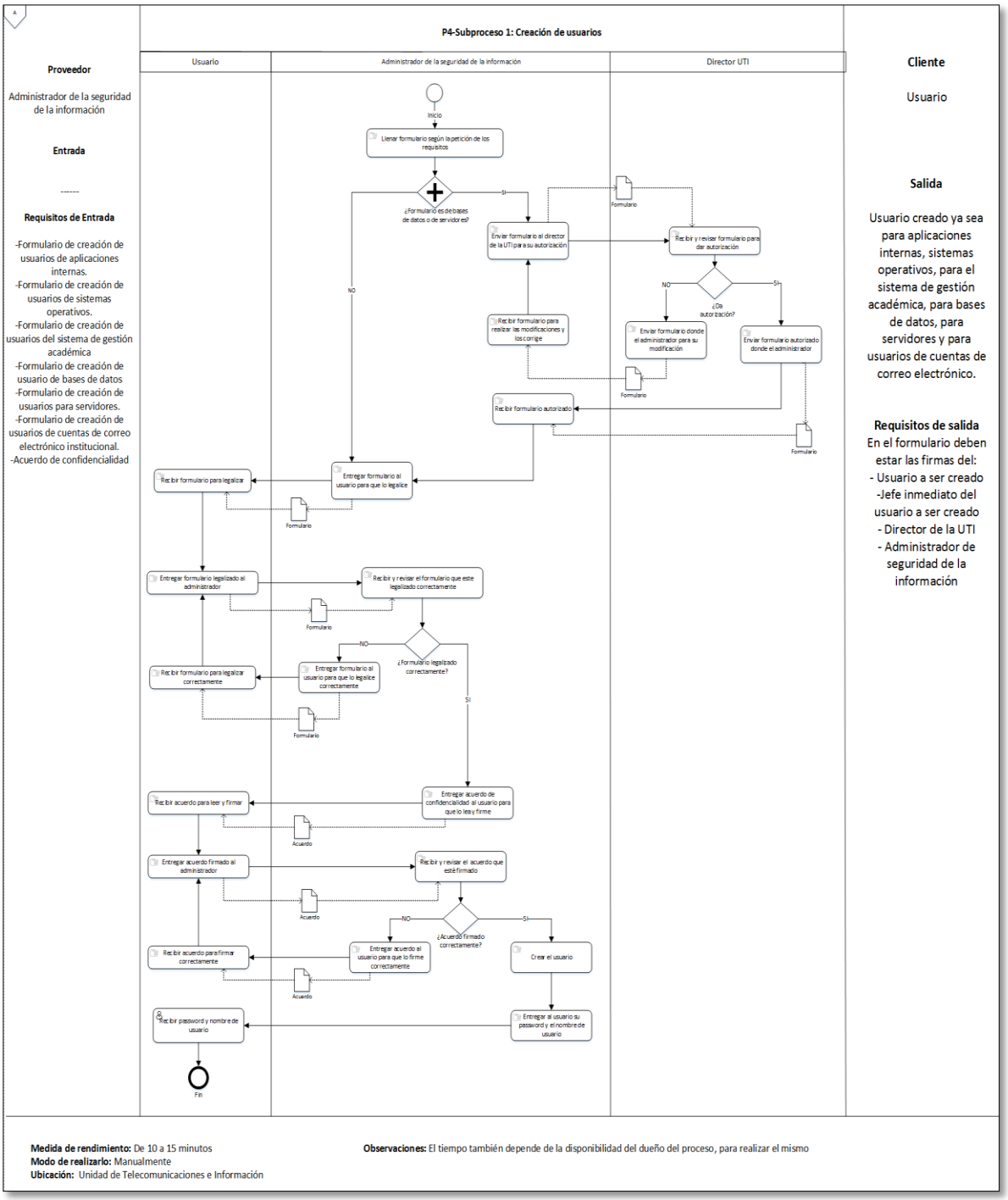


Fig. 23 Diagrama detallado del subproceso definido creación de usuarios

4.1.5. Documentación

	Universidad Nacional de Loja **UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN**		
DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN			
Proceso padre	Control de accesos	**Código**	P4-SP1
Proceso	Gestión de usuarios		
Subproceso	Creación de usuarios		
Objetivo	Crear el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas y aplicaciones.		
Responsable (s)	Administrador de la seguridad de la información		

Entradas		
Proveedor	**Entrada**	**Requisitos de entrada**
Administrador de la seguridad de la información		-Formulario de creación de usuarios de aplicaciones internas. -Formulario de creación de usuarios de sistemas operativos. -Formulario de creación de usuarios del sistema de gestión académica. -Formulario de creación de usuarios de bases de datos. -Formulario de creación de usuarios a nivel de servidores. -Formulario de creación de usuarios de cuentas de correo electrónico institucional. -Acuerdo de confidencialidad de los usuarios

Descripción

1. El administrador llena formulario según la petición de los requisitos.
2. Si el formulario llenado es de bases de datos o de servidores.
   2.1. Envía al director de la UTI para su autorización.
   2.2. El director recibe y revisa el formulario para dar autorización
   2.3. Si no da autorización, el director envía el formulario al administrador para que realice las modificaciones pertinentes.
   2.4. El administrador recibe formulario para realizar las modificaciones pertinentes, sigue en el paso 2.1

2.5. Si da autorización, el administrador recibe formulario autorizado, sigue en el paso 4.

2. Si el formulario llenado no es de base de datos o servidores, sigue en el paso 4
3. El administrador entrega formulario al usuario para que lo legalice.
4. El usuario recibe formulario para legalizarlo.
5. Entrega formulario legalizado al administrador.
6. El administrador recibe y revisa el formulario que este legalizado correctamente.

7.1. Si no está legalizado correctamente el administrador entrega formulario al usuario para que lo firme correctamente.

7.2. Usuario recibe formulario para legalizar correctamente, sigue en el paso 6

7.3. Si está legalizado correctamente, sigue en el paso 8.

8. Entrega acuerdo de confidencialidad al usuario para que lo lea y lo firme.
9. El usuario recibe acuerdo para leer y firmar.
10. Entrega acuerdo firmado al administrador.
11. El administrador recibe y revisa el acuerdo que este firmado correctamente.

11.1. Si no está firmado correctamente el administrador, entrega acuerdo al usuario para que lo firme correctamente.

11.2. El usuario recibe acuerdo para firmar correctamente, sigue en el paso 10.

11.3. Si está firmado correctamente sigue en el paso 12.

12. El administrador crea el usuario.
13. Entrega al usuario su password y nombre de usuario.
14. Finalmente el usuario recibe password y nombre de usuario.

Salidas		
Cliente	**Salida**	**Requisitos de salida**
Usuario	Usuario creado ya sea para: -Aplicaciones internas. -Sistemas operativos. -Sistema de gestión académica. -Bases de datos. -Servidores y -Usuarios de cuentas de correo electrónico institucional.	En el formulario deben de estar las firmas del: -Usuario a ser creado. -Jefe inmediato del usuario. -Director de la UTI. -Administrador de la seguridad de la información.
Medida de rendimiento	De 10 a 15 minutos	
Glosario, siglas y referencias		

P4-SUBPROCESO 2: MODIFICACIÓN DE USUARIOS

4.2.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
   a. Formulario de modificación de usuarios de aplicaciones internas. (**Ver Anexo 11**)
   b. Formulario de modificación de usuarios de sistemas operativos. (**Ver Anexo 16**)
   c. Formulario de modificación de usuarios del sistema de gestión académica (**Ver Anexo 18**)
   d. Formulario de modificación de usuarios de bases de datos (**Ver Anexo 13**)
   e. Formulario de modificación de usuarios para servidores (**Ver Anexo 22**)

4.2.2. Actores

TABLA XV:

ACTORES DEL SUBPROCESO MODIFICACIÓN DE USUARIOS

Cargo	**Rol**
Administrador de la seguridad de la información	Administrador de la seguridad de la información
Director UTI	Director UTI
Usuario	Puede ser directivo, departamental, académico, administrativo, administrador de la base de datos.

4.2.3. Descripción de Actividades

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**
1. El administrador llena formulario según petición de los requisitos.	Administrador de la seguridad	De 8 a 10 minutos

2. Si el formulario llenado es de bases de datos o de servidores 2.1. Envía al director de la UTI para su autorización. 2.2. El director recibe y revisa el formulario para dar autorización. 2.2.1. Si no da autorización envía formulario al administrador para su modificación. 2.2.2. El administrador recibe formulario para realizar las modificaciones y las corrige, sigue en el paso 2.1. 2.3. Si da autorización, sigue en el paso 3 3. Envía formulario autorizado al administrador. 4. El administrador recibe formulario autorizado, sigue en el paso 6. 5. Si el formulario llenado no es de bases de datos ni de servidores. Sigue en el paso 6 6. Realiza la modificación de los accesos de acuerdo a lo solicitado. 7. El administrador informa al usuario que ya está modificado. 8. Finalmente el usuario comprueba los cambios realizados.	de la información	

4.2.4. Diagramas

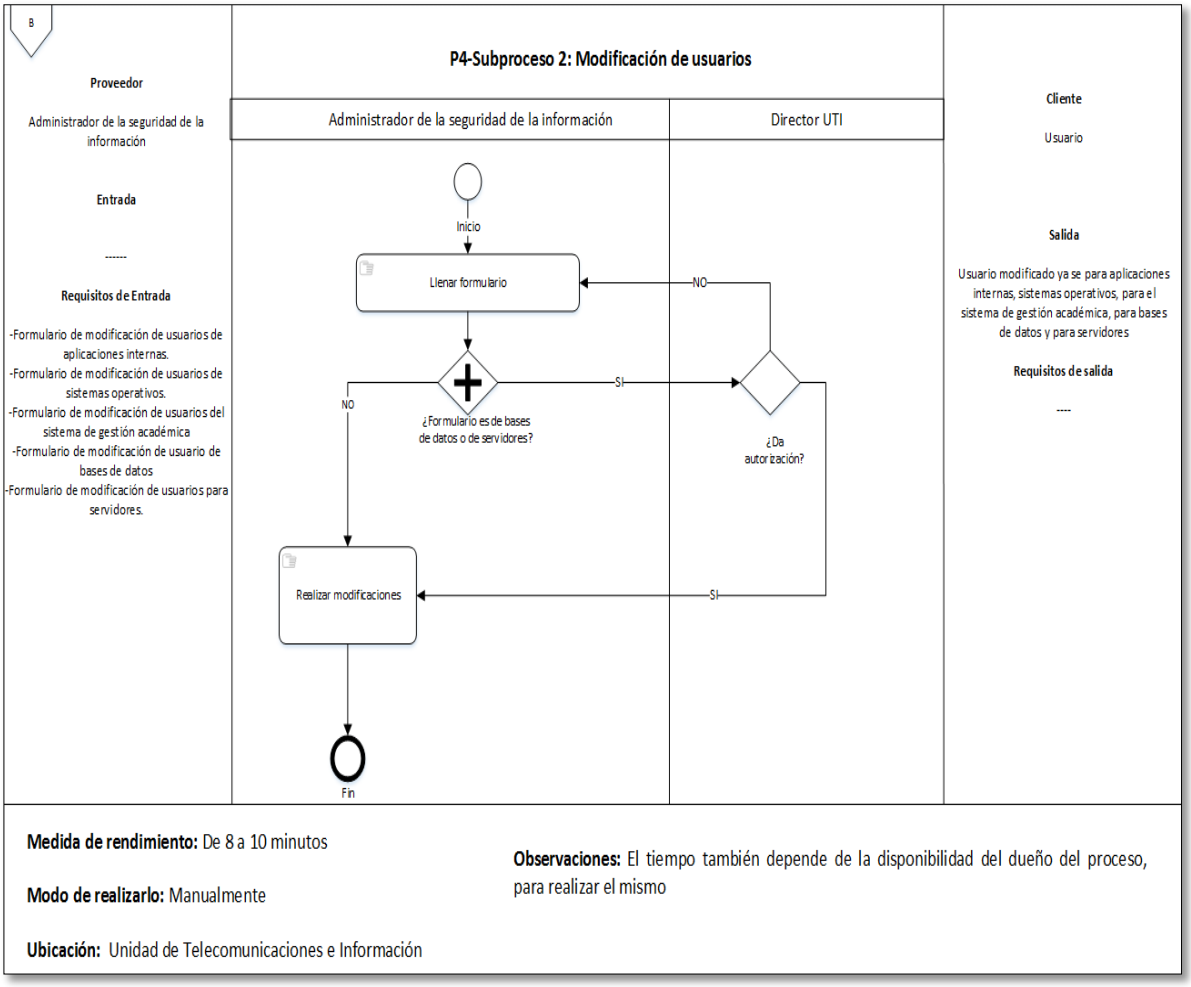


Fig. 24 Diagrama resumido del subproceso definido modificación de usuarios

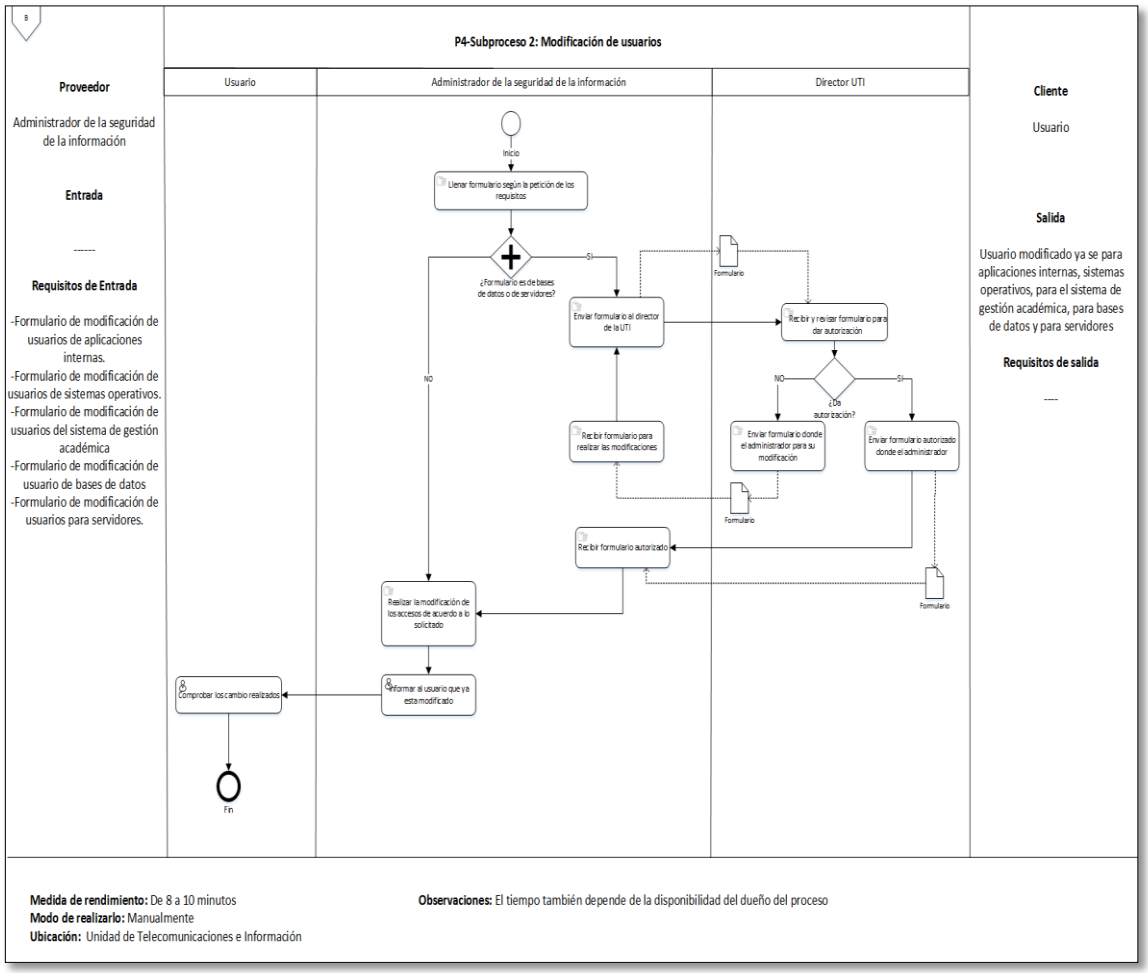


Fig. 25 Diagrama detallado del subproceso definido modificación de usuarios

4.2.5. Documentación

<table>
<tr><td></td><td colspan="3">Universidad Nacional de Loja

UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN</td></tr>
<tr><td colspan="4">DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>Proceso padre</td><td>Control de accesos</td><td>Código</td><td>P4-SP2</td></tr>
<tr><td>Proceso</td><td colspan="3">Gestión de usuarios</td></tr>
<tr><td>Subproceso</td><td colspan="3">Modificación de usuarios</td></tr>
<tr><td>Objetivo</td><td colspan="3">Modificar el acceso de los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.</td></tr>
<tr><td>Responsable (s)</td><td colspan="3">Administrador de la seguridad de la información</td></tr>
<tr><td colspan="4">Entradas</td></tr>
<tr><td>Proveedor</td><td>Entrada</td><td colspan="2">Requisitos de entradas</td></tr>
<tr><td>Administrador de la seguridad de la información</td><td></td><td colspan="2">-Formulario de modificación de usuarios de aplicaciones internas.
-Formulario de modificación de usuarios de sistemas operativos.
-Formulario de modificación de usuarios del sistema de gestión académica.
-Formulario de modificación de usuarios de bases de datos.
-Formulario de modificación de usuarios de servidores.</td></tr>
<tr><td colspan="4">Descripción</td></tr>
<tr><td colspan="4">1. El administrador llena formulario según petición de los requisitos.
2. Si el formulario llenado es de bases de datos o de servidores
2.1. Envía al director de la UTI para su autorización.
2.2. El director recibe y revisa el formulario para dar autorización.
2.2.1. Si no da autorización envía formulario al administrador para su modificación.
2.2.2. El administrador recibe formulario para realizar las modificaciones y las corrige, sigue en el paso 2.1.
2.3. Si da autorización, sigue en el paso 3
3. Envía formulario autorizado al administrador.
4. El administrador recibe formulario autorizado, sigue en el paso 6.
5. Si el formulario llenado no es de bases de datos ni de servidores. Sigue en el paso 6</td></tr>
</table>

6. Realiza la modificación de los accesos de acuerdo a lo solicitado. 7. El administrador informa al usuario que ya está modificado. 8. Finalmente el usuario comprueba los cambios realizados.

Salidas		
Cliente	**Salida**	**Requisitos de salida**
Usuario	Usuario modificado para: -Aplicaciones internas. -Sistemas operativos. -Sistema de gestión académica. -Bases de datos y -Servidores.	
Medida de rendimiento	De 8 a 10 minutos	
Glosario, siglas y referencias		

P4-SUBPROCESO 3: BLOQUEO DE USUARIOS Y SUSPENSIÓN DE CUENTAS DE USUARIOS

4.3.1. Requisitos y Documentación

1. Requisitos previos por el dueño del proceso
    - **a.** Formulario de bloqueo de usuarios de bases de datos. (**Ver Anexo 14**)
    - **b.** Formulario de suspensión de usuarios de cuentas de correo electrónico institucional (**Ver Anexo 28**)

4.3.2. Actores

TABLA XVI:

ACTORES DEL SUBPROCESO BLOQUEO DE USUARIOS Y SUSPENSIÓN DE CUENTAS DE USUARIOS

Cargo	**Rol**
Administrador de la seguridad de la información	Administrador de la seguridad de la información
Director de la UTI	Director de UTI
Jefe departamental	Directivo, departamental, académico, administrativo y subdirector.

4.3.3. Descripción de Actividades

Descripción	Dueño de la actividad	Tiempo de ejecución
1. El administrador llena formulario según petición de los requisitos. 2. Envía formulario donde el director de la UTI para su autorización. 3. El director recibe y revisa el formulario para dar autorización. 3.1. Si no da autorización envía formulario al administrador para su modificación. 3.2. El administrador recibe formulario para realizar las modificaciones y las corrige, sigue en el paso 2. 3.3. Si da autorización, envía formulario autorizado al administrador, sigue en el paso 4. 4. El administrador recibe formulario autorizado 5. Entrega formulario al jefe departamental para que lo firme. 6. El jefe departamento recibe formulario para firmar. 7. Entrega formulario firmado al administrador. 8. El administrador recibe y revisa formulario que este firmado correctamente. 9. Pide al jefe departamental la cédula de identidad para comprobar la autenticidad de la firma. 9.1. Si no está firmado correctamente el formulario, el administrador indica	Administrador de la seguridad de la información	De 10 a 15 minutos

al jefe departamental que la firma no es la misma, sigue en el paso 1. 9.2. Si está firmado correctamente, procederá a bloquear el usuario o a suspender la cuenta del usuario del correo electrónico institucional. Sigue en el paso 10 u 11. 10. Si es para bloquear el usuario. 10.1. Mira el tipo de bloqueo, si es temporal o total. 10.2. Procederá hacer el bloqueo correspondiente, sigue en el paso 12. 11. Si es para suspender la cuenta del usuario 11.1. Mira el tipo de suspensión, si es total o temporal 11.2. Procederá hacer la suspensión correspondiente, sigue en el paso 12. 12. Informa al jefe departamental que ya está bloqueado el usuario o la suspensión de la cuenta del usuario. 13. Finalmente el jefe departamental comprueba los cambios realizados.		

4.3.4. Diagramas

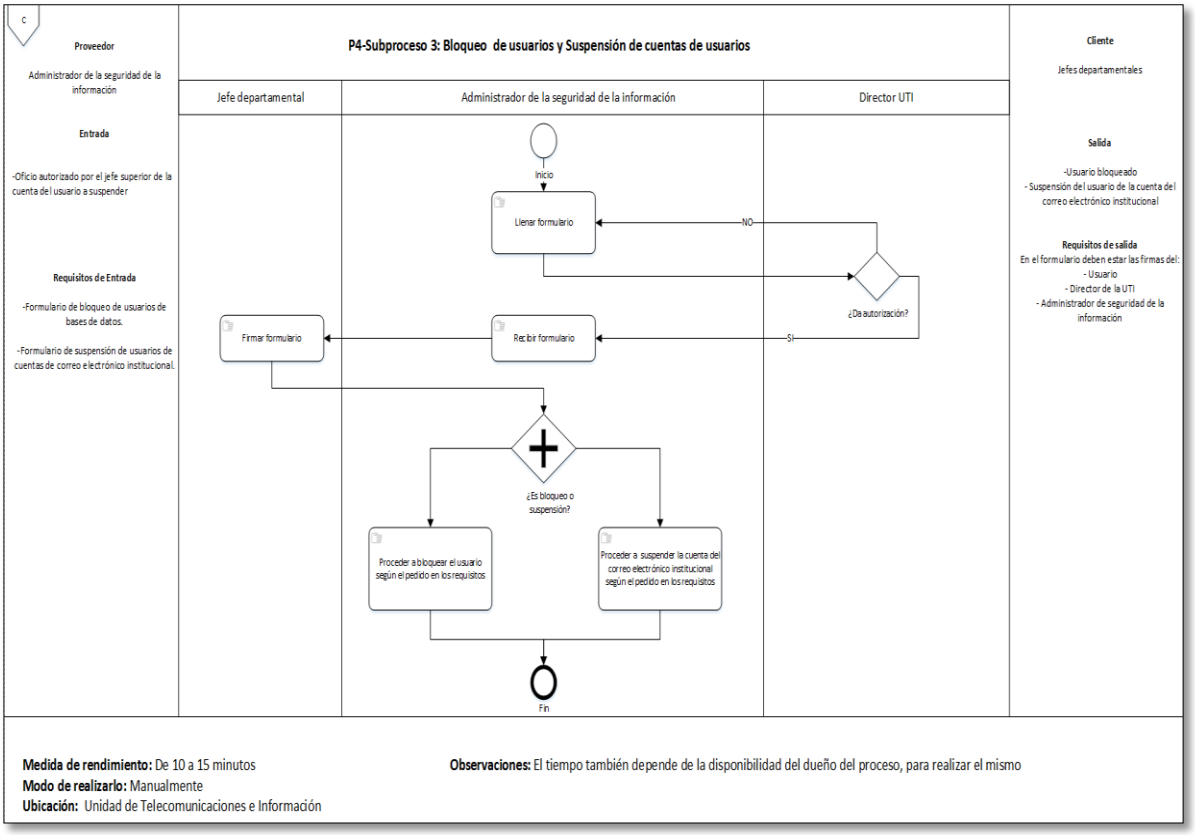


Fig. 26 Diagrama resumido del subproceso definido bloqueo de usuarios y suspensión de cuentas de usuarios.

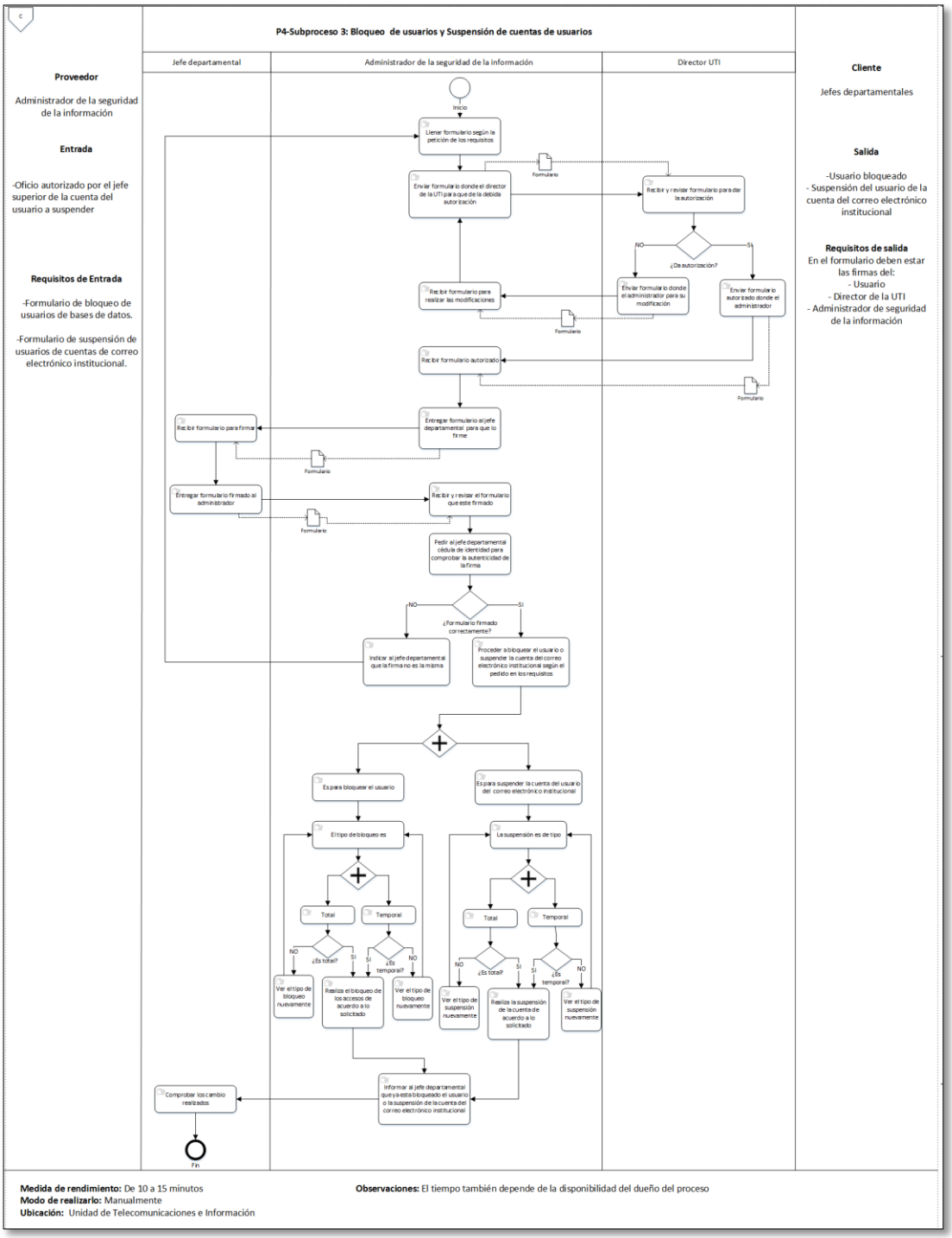


Fig. 27 Diagrama detallado del subproceso definido bloqueo de usuarios y suspensión de cuentas de usuarios.

4.3.5. Documentación

<table>
<tr><td></td><td colspan="4">Universidad Nacional de Loja

UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN</td></tr>
<tr><td colspan="5">DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>Proceso padre</td><td colspan="2">Control de accesos</td><td>Código</td><td>P4-SP3</td></tr>
<tr><td>Proceso</td><td colspan="4">Gestión de usuarios</td></tr>
<tr><td>Subproceso</td><td colspan="4">Bloqueo de usuarios y suspensión de cuentas de usuarios</td></tr>
<tr><td>Objetivo</td><td colspan="4">Bloquear el acceso a los usuarios e impedir los accesos no autorizados a los sistemas de información y servicios, y suspender las cuentas de correo electrónico institucional.</td></tr>
<tr><td>Responsable (s)</td><td colspan="4">Administrador de la seguridad de la información</td></tr>
<tr><td colspan="5">Entradas</td></tr>
<tr><td>Proveedor</td><td colspan="2">Entrada</td><td colspan="2">Requisitos de entrada</td></tr>
<tr><td>Administrador de la seguridad de la información</td><td colspan="2">-Oficio autorizado por el jefe superior de la cuenta del usuario a suspender.</td><td colspan="2">-Formulario de bloqueo de usuarios de bases de datos.
-Formulario de suspensión de cuentas de correo electrónico institucional.</td></tr>
<tr><td colspan="5">Descripción</td></tr>
<tr><td colspan="5">1. El administrador llena formulario según petición de los requisitos.
2. Envía formulario donde el director de la UTI para su autorización.
3. El director recibe y revisa el formulario para dar autorización.
3.1. Si no da autorización envía formulario al administrador para su modificación.
3.2. El administrador recibe formulario para realizar las modificaciones y las corrige, sigue en el paso 2.
3.3. Si da autorización, envía formulario autorizado al administrador, sigue en el paso 4.
4. El administrador recibe formulario autorizado
5. Entrega formulario al jefe departamental para que lo firme.
6. El jefe departamento recibe formulario para firmar.
7. Entrega formulario firmado al administrador.
8. El administrador recibe y revisa formulario que este firmado correctamente.
9. Pide al jefe departamental la cédula de identidad para comprobar la autenticidad de la firma.</td></tr>
</table>

9.1. Si no está firmado correctamente el formulario, el administrador indica al jefe departamental que la firma no es la misma, sigue en el paso 1.

9.2. Si está firmado correctamente, procederá a bloquear el usuario o a suspender la cuenta del usuario del correo electrónico institucional. Sigue en el paso 10 u 11.

10. Si es para bloquear el usuario.

    10.1. Mira el tipo de bloqueo, si es temporal o total.

    10.2. Procederá hacer el bloqueo correspondiente, sigue en el paso 12.

11. Si es para suspender la cuenta del usuario

    11.1. Mira el tipo de suspensión, si es total o temporal

    11.2. Procederá hacer la suspensión correspondiente, sigue en el paso 12.

12. Informa al jefe departamental que ya está bloqueado el usuario o la suspensión de la cuenta del usuario.

13. Finalmente el jefe departamental comprueba los cambios realizados.

Salidas		
Cliente	**Salida**	**Requisitos de salida**
Jefe departamental	-Usuario bloqueado. -Suspensión del usuario de la cuenta del correo electrónico institucional	En el formulario deben de estar las firmas de: -Usuario. -Director de la UTI. -Administrador de la seguridad de la información
Medida de rendimiento	De 10 a 15 minutos	
Glosario, siglas y referencias		

PROCESO 5: CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

5.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
    a. Solicitud de control a sistemas y aplicaciones autorizada por el jefe inmediato superior.
2. Requisitos previos obtenidos por el dueño del proceso
    a. Formulario de acceso/modificación/bloqueo/suspensión a sistemas y/o aplicaciones (**Ver Anexo 29**)

5.2. Actores

TABLA XVII:

ACTORES DEL PROCESO CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Cargo	**Rol**
Administrador de la seguridad de la información	Administrador de la seguridad de la información
Usuario (Funcionarios UTI)	Director, Subdirectores, desarrolladores, secretaria, técnico de software, administrador de la base de datos y responsable de infraestructura.
Director UTI	Director UTI

5.3. Descripción de Actividades

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**
1. El usuario solicita la creación, modificación bloqueo o suspensión de un sistema o aplicación. 2. El administrador entrega requisitos y documentos. 3. El usuario adjunta requisitos y documentación previa. 4. Entrega requisitos al administrador para su verificación. 5. El administrador recibe y revisa requisitos para validar. 5.1. Si no están correctos los requisitos, el administrador entrega requisitos al usuario para su modificación.	Administrador de la seguridad de la información	De 8 a 10 minutos

5.2. El usuario recibe requisitos para corregirlos, sigue en el paso 4. 5.3. Si están correctos los requisitos, sigue en el paso 6. 6. El administrador llena el formulario. 7. Envía formulario donde el director de la UTI para su aprobación. 8. El director recibe y revisa el formulario. 8.1. Si no autoriza, el director envía formulario donde el administrador para su modificación. 8.2. El administrador recibe formulario para realizar las correcciones pertinentes, sigue en el paso 7. 8.3. Si lo autoriza, sigue en el paso 9. 9. El director entrega formulario autorizado al administrador. 10. El administrador recibe formulario autorizado. 11. Entrega formulario al usuario para que lo legalice. 12. Usuario recibe formulario para legalizarlo. 13. Entrega formulario legalizado al administrador. 14. El administrador recibe y revisa que este legalizado correctamente el formulario. 14.1. Si no está legalizado correctamente, el administrador envía formulario al usuario para que lo legalice correctamente.		

14.2. El usuario recibe formulario para legalizar correctamente, sigue en el paso 13. 14.3. Si está legalizado correctamente, sigue en el paso 15 15. El administrador firma el formulario. 16. Procede a crear, modificar, bloquear o suspender el usuario de acuerdo a los requisitos del formulario. 17. El usuario es para: Crear Modificar Bloquear Suspender 18. Realiza la operación de acuerdo a lo solicitado. 19. Informa al usuario que los cambios están realizados de acuerdo a los requisitos. 20. Finalmente el usuario comprueba los cambios realizados.		

5.4. Diagramas

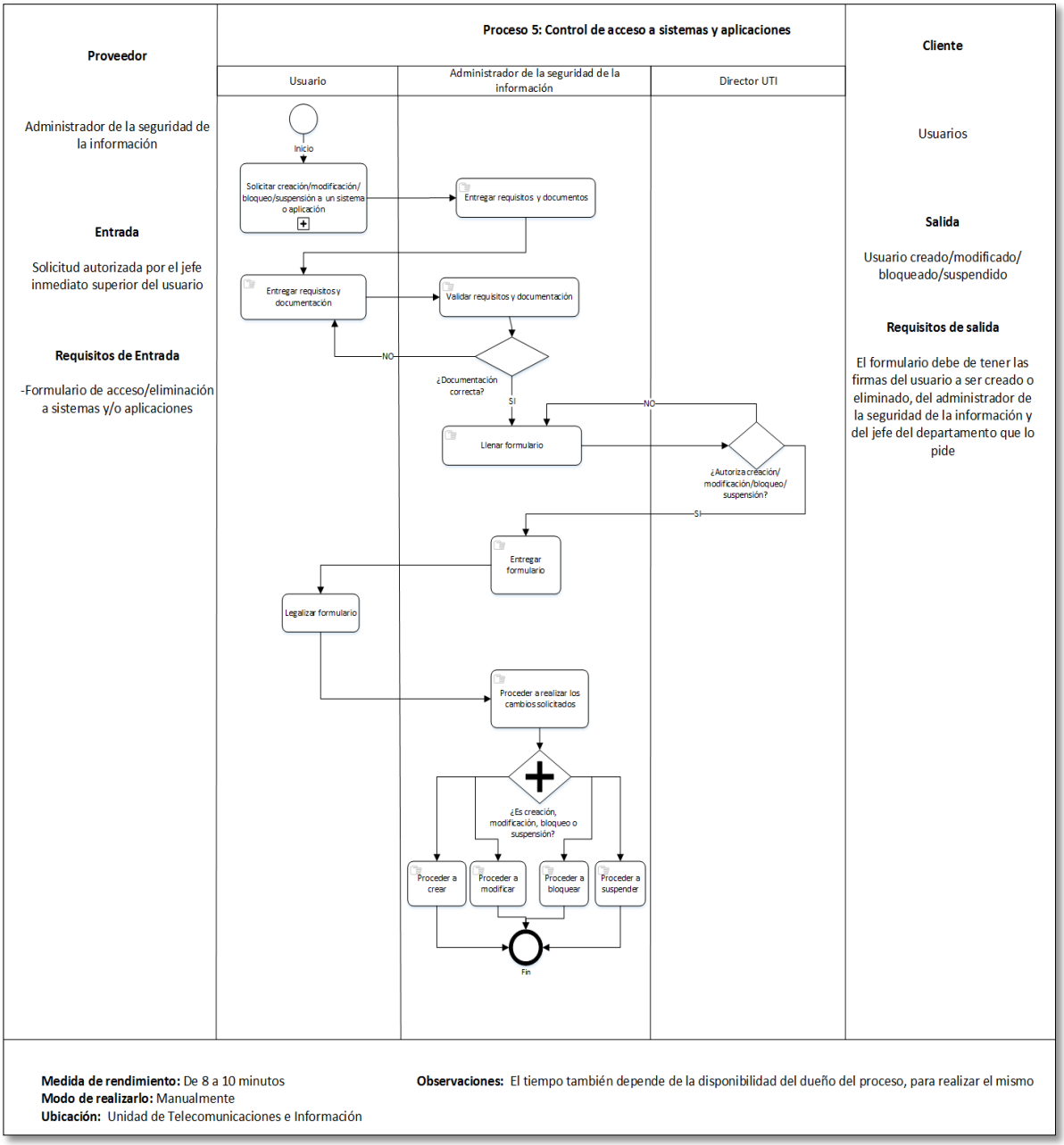


Fig. 28 Diagrama resumido del proceso definido control de accesos a sistemas y aplicaciones

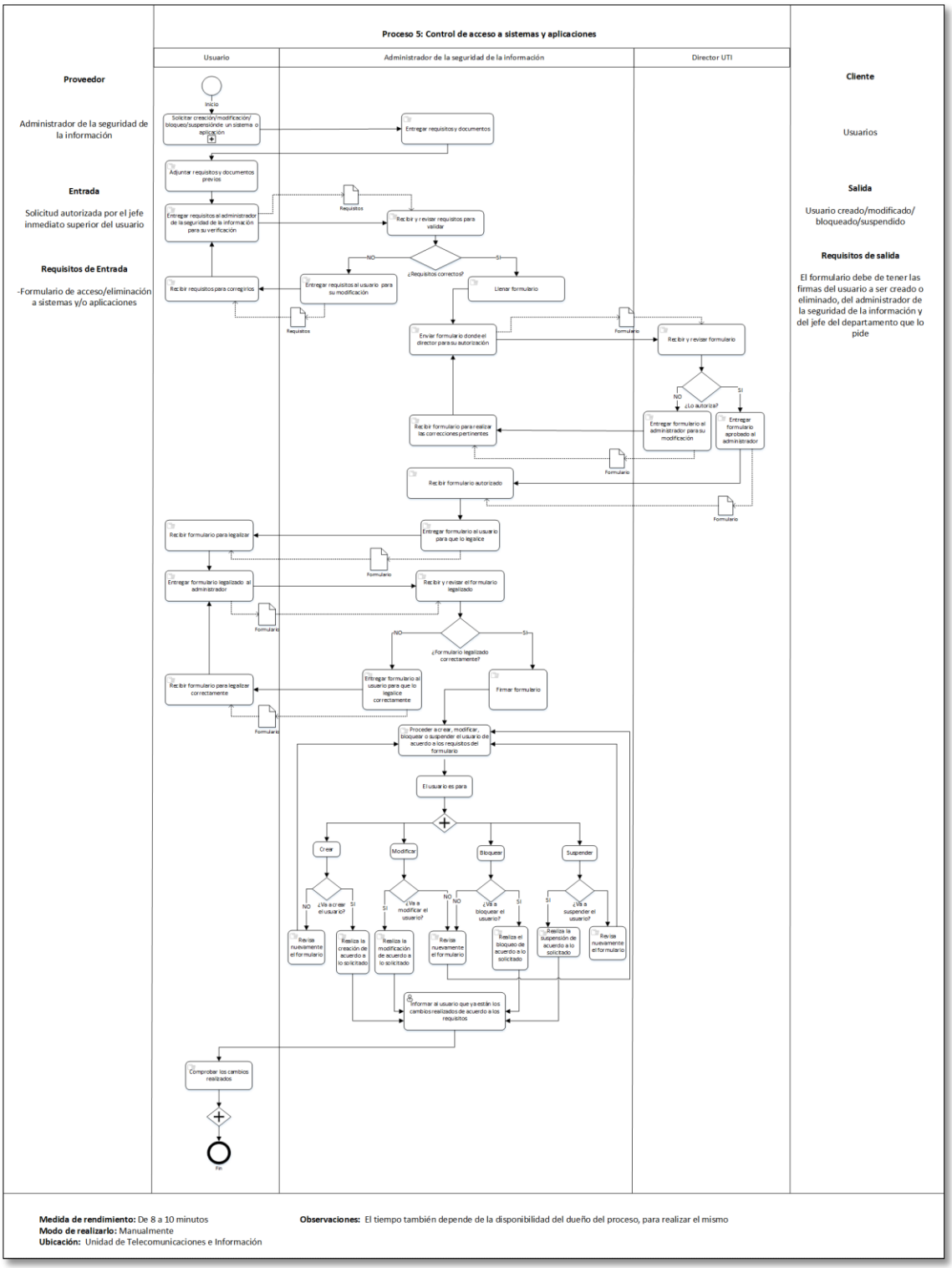


Fig. 29 Diagrama detallado del proceso definido control de accesos a sistemas y aplicaciones

5.5. Documentación

<table>
<tr><td></td><td colspan="3">Universidad Nacional de Loja

UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN</td></tr>
<tr><td colspan="4">DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>Proceso padre</td><td>Control de accesos</td><td>Código</td><td>P5</td></tr>
<tr><td>Proceso</td><td colspan="3">Control de acceso a sistemas y aplicaciones</td></tr>
<tr><td>Subproceso</td><td colspan="3"></td></tr>
<tr><td>Objetivo</td><td colspan="3">Impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.</td></tr>
<tr><td>Responsable (s)</td><td colspan="3">Administrador de la seguridad de la información</td></tr>
<tr><td colspan="4">Entradas</td></tr>
<tr><td>Proveedor</td><td>Entrada</td><td colspan="2">Requisitos de entrada</td></tr>
<tr><td>Administrador de la seguridad de la información</td><td>Solicitud de control a sistemas y aplicaciones autorizada por el jefe inmediato superior del usuario.</td><td colspan="2">-Formulario de acceso/modificación/bloqueo/suspensión de sistemas y aplicaciones</td></tr>
<tr><td colspan="4">Descripción</td></tr>
<tr><td colspan="4">1. El usuario solicita la creación, modificación bloqueo o suspensión de un sistema o aplicación.
2. El administrador entrega requisitos y documentos.
3. El usuario adjunta requisitos y documentación previa.
4. Entrega requisitos al administrador para su verificación.
5. El administrador recibe y revisa requisitos para validar.
5.1. Si no están correctos los requisitos, el administrador entrega requisitos al usuario para su modificación.
5.2. El usuario recibe requisitos para corregirlos, sigue en el paso 4.
5.3. Si están correctos los requisitos, sigue en el paso 6.
6. El administrador llena el formulario.
7. Envía formulario donde el director de la UTI para su aprobación.
8. El director recibe y revisa el formulario.</td></tr>
</table>

8.1. Si no autoriza, el director envía formulario donde el administrador para su modificación.

8.2. El administrador recibe formulario para realizar las correcciones pertinentes, sigue en el paso 7.

8.3. Si lo autoriza, sigue en el paso 9.

9. El director entrega formulario autorizado al administrador.

10. El administrador recibe formulario autorizado.

11. Entrega formulario al usuario para que lo legalice.

12. Usuario recibe formulario para legalizarlo.

13. Entrega formulario legalizado al administrador.

14. El administrador recibe y revisa que este legalizado correctamente el formulario.

14.1. Si no está legalizado correctamente, el administrador envía formulario al usuario para que lo legalice correctamente.

14.2. El usuario recibe formulario para legalizar correctamente, sigue en el paso 13.

14.3. Si está legalizado correctamente, sigue en el paso 15

15. El administrador firma el formulario.

16. Procede a crear, modificar, bloquear o suspender el usuario de acuerdo a los requisitos del formulario.

17. El usuario es para:

Crear-Modificar

Bloquear-Suspender

18. Realiza la operación de acuerdo a lo solicitado.

19. Informa al usuario que los cambios están realizados de acuerdo a los requisitos.

20. Finalmente el usuario comprueba los cambios realizados.

Salidas		
Cliente	**Salida**	**Requisitos de salida**
Usuarios	Usuario creado, modificado, bloqueado o suspendido.	En el formulario debe tener las firmas de: -Usuario. -Jefe departamental. -Administrador de la seguridad de la información
Medida de rendimiento	De 8 a 10 minutos	
Glosario, siglas y referencias		

PROCESO PADRE: SEGURIDAD EN LA OPERATIVA
PROCESO 6: GENERAR COPIAS DE SEGURIDAD

6.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso
    a. Registro de copias de seguridad(**Ver Anexo 30**)

6.2. Actores

TABLA XVIII:

ACTORES DEL PROCESO GENERAR COPIAS DE SEGURIDAD

Cargo	**Rol**
Responsable de copias de seguridad	Responsable de copias de seguridad
Subdirectores	Subdirectores de redes y equipos informáticos Subdirectores de desarrollo de software
Responsable de infraestructura	Responsable de infraestructura
Administrador de la seguridad de la información.	Administrador de la seguridad de la información.

6.3. Descripción de Actividades

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**
1. El subdirector correspondiente, realiza la matriz de inventario de software, base de datos y de configuraciones. 2. Envía la matriz al responsable de copias de seguridad. 3. El responsable de copias de seguridad, recibe la matriz y planifica la obtención de respaldos. 4. Envía la planificación al responsable de infraestructura.	Administrador de la base de datos	De 5 minutos hasta 3 horas

5. El responsable de infraestructura, recibe la planificación para coordinar accesos a los equipos informáticos. 6. Envía la planificación al administrador, para que le otorgue accesos a los equipos informáticos. 7. El administrador recibe la planificación y otorga los accesos a los equipos informáticos. 8. El responsable de bases de datos, genera los respaldos y las etiquetas. 9. Comprueba los respaldos. 9.1. Si no están correctos los respaldos, sigue en el paso 8. 9.2. Si están correctos los respaldos, sigue en el paso 10 10. Registra los respaldos realizados, en su registro de copias de seguridad (**literal 1.a**). 11. Entrega los respaldos al administrador. 12. El administrador recibe los respaldos. 13. Registra los respaldos en su registro de copias de seguridad. 14. Finalmente guarda una copia fuera de las instalaciones de la UTI.		

6.4. Diagramas

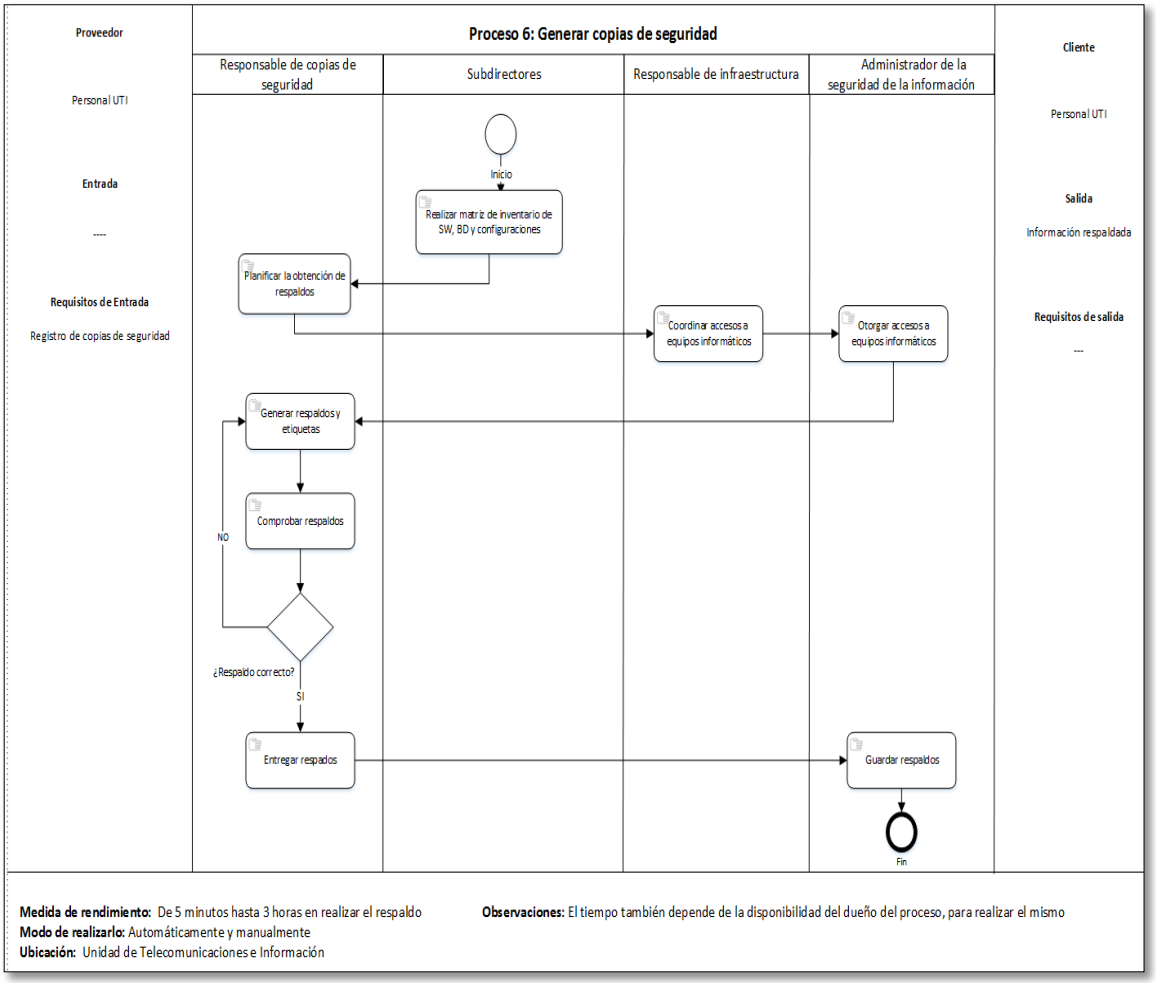


Fig. 30 Diagrama resumido del proceso definido generar copias de seguridad

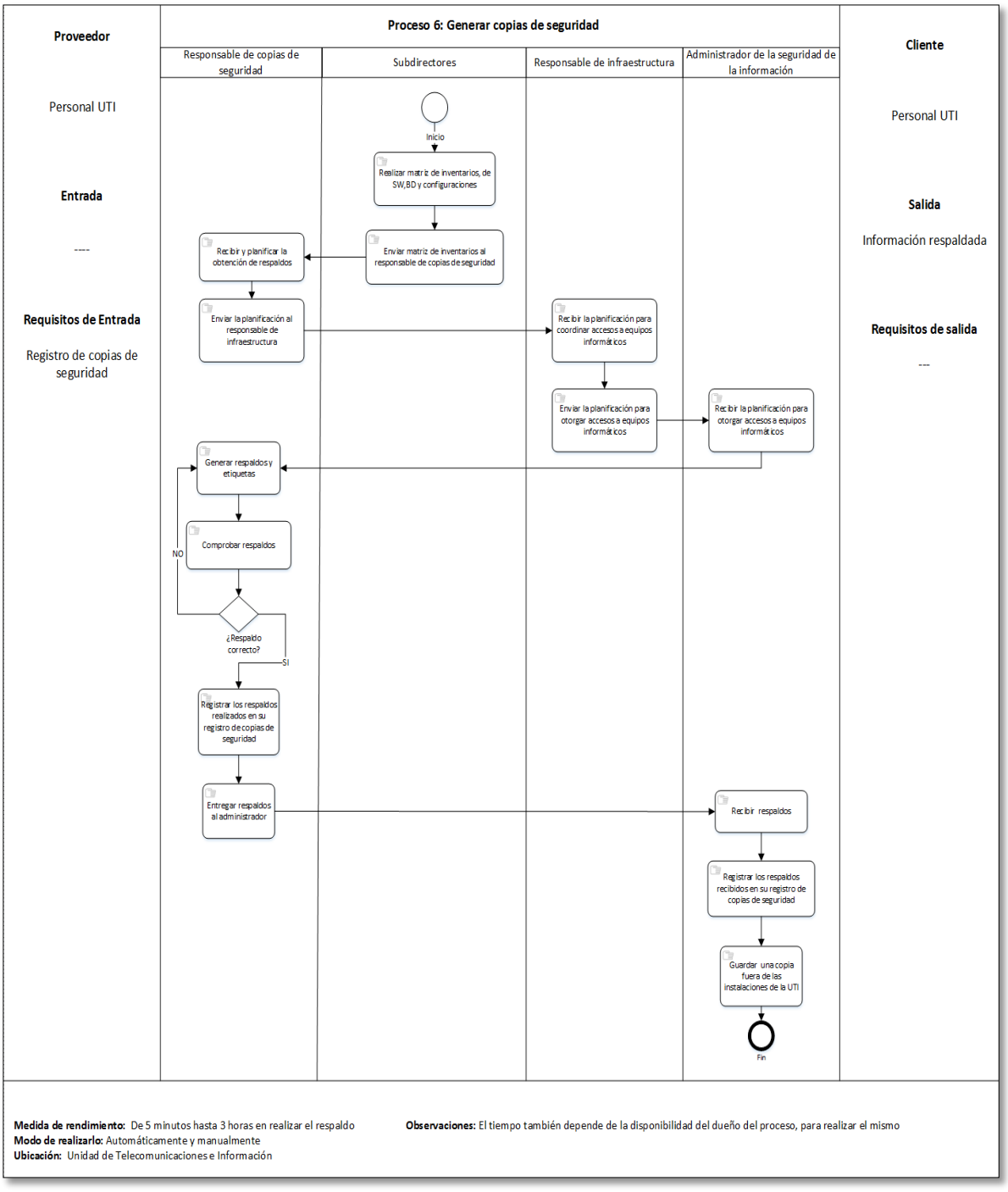


Fig. 31 Diagrama detallado del proceso definido generar copias de seguridad

6.5. Documentación

<table>
<tr><td></td><td colspan="4">Universidad Nacional de Loja

UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN</td></tr>
<tr><td colspan="5">DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>Proceso padre</td><td colspan="2">Seguridad en la operativa</td><td>Código</td><td>P6</td></tr>
<tr><td>Proceso</td><td colspan="4">Generar copias de seguridad</td></tr>
<tr><td>Subproceso</td><td colspan="4"></td></tr>
<tr><td>Objetivo</td><td colspan="4">Alcanzar un grado de protección deseado contra la pérdida de datos.</td></tr>
<tr><td>Responsable (s)</td><td colspan="4">Administrador de la seguridad de la información</td></tr>
<tr><td colspan="5">Entradas</td></tr>
<tr><td>Proveedor</td><td colspan="2">Entrada</td><td colspan="2">Requisitos de entrada</td></tr>
<tr><td>Personal UTI</td><td colspan="2"></td><td colspan="2">Registro de copias de seguridad</td></tr>
<tr><td colspan="5">Descripción</td></tr>
<tr><td colspan="5">1. El subdirector correspondiente, realiza la matriz de inventario de software, base de datos y de configuraciones.
2. Envía la matriz al responsable de copias de seguridad.
3. El responsable de copias de seguridad, recibe la matriz y planifica la obtención de respaldos.
4. Envía la planificación al responsable de infraestructura.
5. El responsable de infraestructura, recibe la planificación para coordinar accesos a los equipos informáticos.
6. Envía la planificación al administrador, para que le otorgue accesos a los equipos informáticos.
7. El administrador recibe la planificación y otorga los accesos a los equipos informáticos.
8. El responsable de bases de datos, genera los respaldos y las etiquetas.
9. Comprueba los respaldos.
9.1. Si no están correctos los respaldos, sigue en el paso 8.
9.2. Si están correctos los respaldos, sigue en el paso 10
10. Registra los respaldos realizados, en su registro de copias de seguridad
11. Entrega los respaldos al administrador.</td></tr>
</table>

12. El administrador recibe los respaldos. 13. Registra los respaldos en su registro de copias de seguridad 14. Finalmente guarda una copia fuera de las instalaciones de la UTI.		
Salidas		
Cliente	**Salida**	**Requisitos de salida**
Personal UTI	Información respaldada	
Medida de rendimiento	De 5 minutos hasta 3 horas en realiza el respaldo	
Glosario, siglas y referencias		

PROCESO PADRE: SEGURIDAD EN LAS TELECOMUNICACIONES

PROCESO 7: ENTREGA DE INFORMACIÓN CON PARTES EXTERNAS

7.1. Requisitos y Documentación

1. Requisitos previos obtenidos por el dueño del proceso

a. Acuerdo de confidencialidad y no divulgación de la información con partes externas y proveedores (**Ver Anexo 31**)

7.2. Actores

TABLA XIX:

ACTORES DEL PROCESO ENTREGA DE INFORMACIÓN CON PARTES EXTERNAS

Cargo	**Rol**
Director UTI	Director UTI
Rector UNL	Rector UNL
Administrador de la seguridad de la información	Administrador de la seguridad de la información
Empresa/Usuario/Cliente	Empresa/Usuario/Cliente

7.3. Descripción de Actividades

Descripción	**Dueño de la actividad**	**Tiempo de ejecución**
1. La empresa envía solicitud de pedido de información, al	Administrador de la seguridad	De 15 a 60 minutos

administrador solicitando información. 2. El administrador recibe y revisa la solicitud de pedido de información de la empresa/usuario/cliente. 3. Revisa el tipo de información requerida 4. La información es de tipo: 4.1. Publica 4.1.1. Si no es información pública ir la paso 4. 4.1.2. Si es información pública ir al paso 5. 4.2. Reservada uso interno 4.2.1. Si no es información reservado uso interno ir la paso 4. 4.2.2. Si es información reservada uso interno, enviar la solicitud al director de la UTI para su aprobación. 4.2.3. El director recibe y revisa la solicitud. 4.2.3.1. Si no la aprueba, envía la solicitud negada al administrador, caso contrario envía solicitud aprobada. 4.2.4. El administrador recibe y revisa la solicitud. 4.2.4.1. Si no fue aprobada, envía comunicado a la empresa/usuario/cliente, sigue en el paso 6.	de la información	

4.2.4.2. Si fue aprobada, sigue en el paso 5. 4.3. Reservada confidencial 4.3.1. Si no es información reservada confidencial ir al paso 4. 4.3.2. Si es información reservada confidencial enviar la solicitud al rector de la UNL para su aprobación. 4.3.3. El rector recibe y revisa la solicitud. 4.3.3.1. Si no la aprueba, envía la solicitud negada al administrador, caso contrario envía solicitud aprobada. 4.3.4. El administrador recibe y revisa la solicitud. 4.3.4.1. Si no fue aprobada, envía comunicado a la empresa/usuario/cliente, sigue en el paso 6. 4.3.4.2. Si fue aprobada, sigue en el paso 5. 4.4. Reservada secreta 4.4.1. Si no es información reservada secreta ir al paso 4. 4.4.2. Si es información reservada secreta enviar la solicitud al rector de la UNL para su aprobación. 4.4.3. El rector recibe y revisa la solicitud.		

4.4.3.1. Si no la aprueba, envía la solicitud negada al administrador, caso contrario envía solicitud aprobada. 4.4.4. El administrador recibe y revisa la solicitud. 4.4.4.1. Si no fue aprobada, envía comunicado a la empresa/usuario/cliente, sigue en el paso 6. 4.4.4.2. Si fue aprobada, sigue en el paso 5. 5. Envía la información solicitada 6. Finalmente la empresa recibe información solicitada o negada.		

7.4. Diagramas

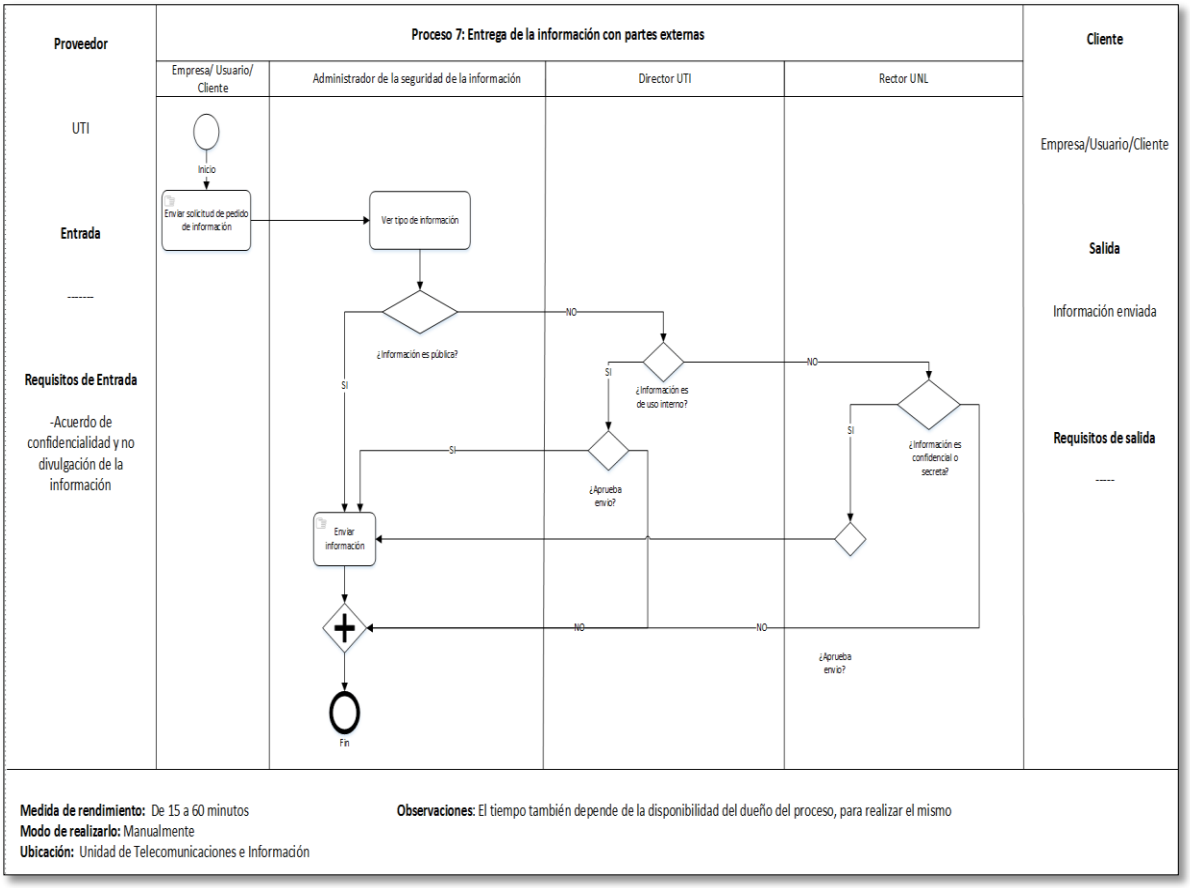


Fig. 32 Diagrama resumido del proceso definido entrega de la información con partes externas

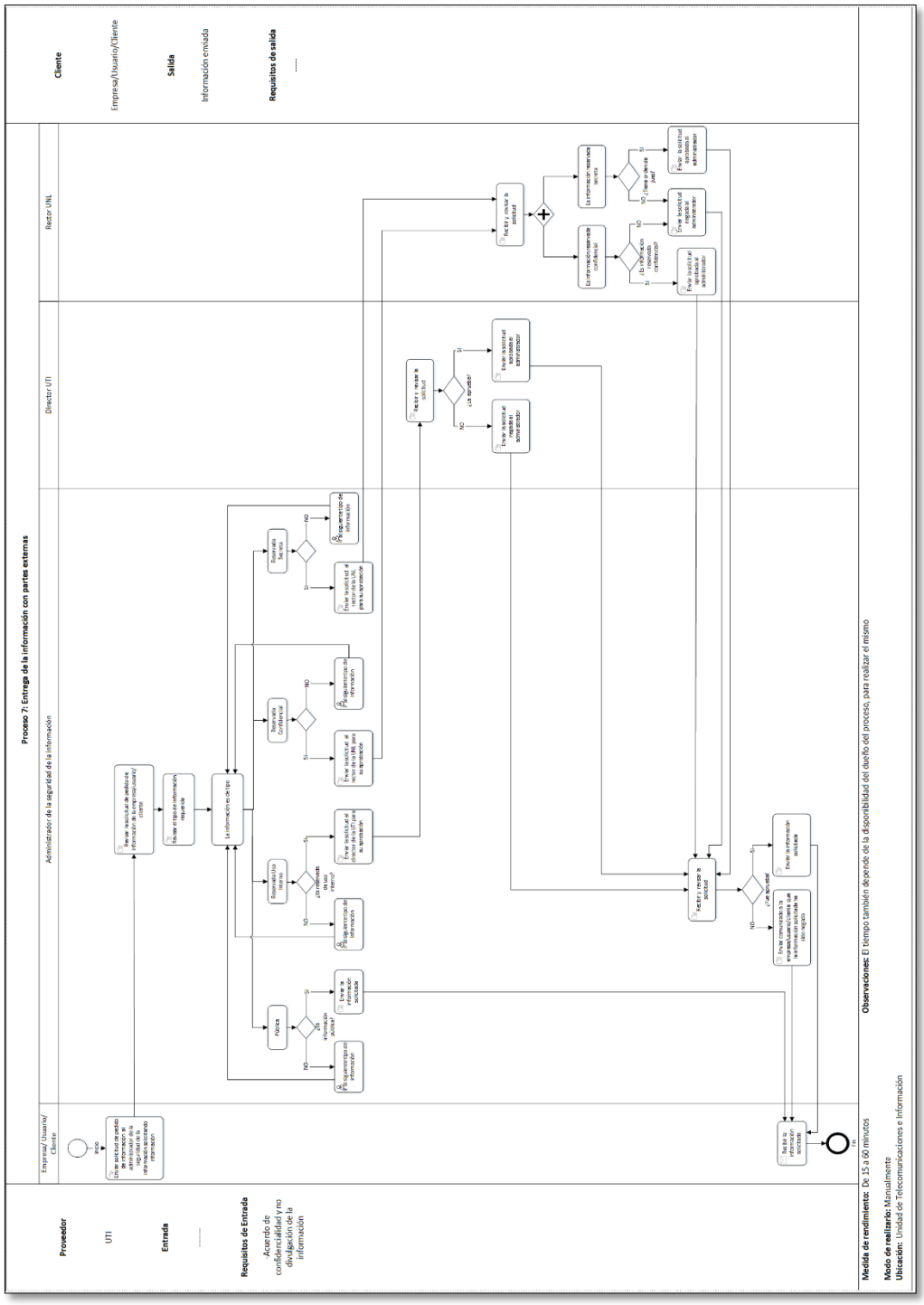


Fig. 33 Diagrama detallado del proceso definido entrega de la información con partes externas

7.5. Documentación

	Universidad Nacional de Loja **UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN**		
DOCUMENTO DE LOS PROCESOS DE LA SEGURIDAD DE LA INFORMACIÓN			
Proceso padre	Seguridad en las telecomunicaciones	**Código**	P7
Proceso	Entrega de información con partes externas		
Subproceso			
Objetivo	Mantener la seguridad de la información que transfiere una organización internamente o con entidades externas.		
Responsable (s)	Administrador de la seguridad de la información		
Entradas			
Proveedor	**Entrada**	**Requisitos de entrada**	
Unidad de Telecomunicaciones e Información		Acuerdo de confidencialidad y no divulgación de la información	
Descripción			

1. La empresa envía solicitud de pedido de información, al administrador solicitando información.
2. El administrador recibe y revisa la solicitud de pedido de información de la empresa/usuario/cliente.
3. Revisa el tipo de información requerida
4. La información es de tipo:

4.1. Publica

4.1.1. Si no es información pública ir la paso 4.

4.1.2. Si es información pública ir al paso 5.

4.2. Reservada uso interno

4.2.1. Si no es información reservado uso interno ir la paso 4.

4.2.2. Si es información reservada uso interno, enviar la solicitud al director de la UTI para su aprobación.

4.2.3. El director recibe y revisa la solicitud.

4.2.3.1. Si no la aprueba, envía la solicitud negada al administrador, caso contrario envía solicitud aprobada.

4.2.4. El administrador recibe y revisa la solicitud.

4.2.4.1. Si no fue aprobada, envía comunicado a la empresa/usuario/cliente, sigue en el paso 6.

4.2.4.2. Si fue aprobada, sigue en el paso 5.

4.3. Reservada confidencial

4.3.1. Si no es información reservada confidencial ir al paso 4.

4.3.2. Si es información reservada confidencial enviar la solicitud al rector de la UNL para su aprobación.

4.3.3. El rector recibe y revisa la solicitud.

4.3.3.1. Si no la aprueba, envía la solicitud negada al administrador, caso contrario envía solicitud aprobada.

4.3.4. El administrador recibe y revisa la solicitud.

4.3.4.1. Si no fue aprobada, envía comunicado a la empresa/usuario/cliente, sigue en el paso 6.

4.3.4.2. Si fue aprobada, sigue en el paso 5.

4.4. Reservada secreta

4.4.1. Si no es información reservada secreta ir al paso 4.

4.4.2. Si es información reservada secreta enviar la solicitud al rector de la UNL para su aprobación.

4.4.3. El rector recibe y revisa la solicitud.

4.4.3.1. Si no la aprueba, envía la solicitud negada al administrador, caso contrario envía solicitud aprobada.

4.4.4. El administrador recibe y revisa la solicitud.

4.4.4.1. Si no fue aprobada, envía comunicado a la empresa/usuario/cliente, sigue en el paso 6.

4.4.4.2. Si fue aprobada, sigue en el paso 5.

5. Envía la información solicitada

6. Finalmente la empresa recibe información solicitada o negada.

Salidas		
Cliente	**Salida**	**Requisitos de salida**
Empresa/usuario/cliente	Información enviada	
Medida de rendimiento	De 15 a 60 minutos	
Glosario, siglas y referencias		

FASE 4: VALIDACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

4.1. Validación de los procesos con sus respectivos responsables

Para la realización de la validación de los procesos de la seguridad de la información se utilizó una matriz de validación de procesos la cual se presenta continuación:

La ponderación de cada pregunta se realizó de acuerdo a la siguiente escala, marcando el ítem correspondiente.

CATEGORÍA	NIVEL DE CUMPLIMIENTO
1	Totalmente en desacuerdo
2	En desacuerdo
3	Ni de acuerdo ni en desacuerdo
4	De acuerdo
5	Totalmente de acuerdo

MATRIZ DE VALIDACIÓN

Proceso	Validación	Escala				
		1	2	3	4	5
P1. Clasificación de la Información	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						
	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					

P2. Entrega de información en medios de almacenamiento	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						
P3. Control de accesos físicos a las instalaciones de la UTI	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						
P4. Gestión de accesos de usuarios.	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						
	¿El diagrama muestra el flujo adecuado para la realización del proceso?					

P4-SP1. Creación de usuarios	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						
P4-SP2. Modificación de usuarios	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						
P4-SP3. Bloqueo de usuarios y suspensión d cuentas de usuarios	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						

P5. Control de acceso a sistemas y aplicaciones	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						
P6. Generar copias de seguridad	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						
P7. Entrega de información con partes externas	¿El diagrama muestra el flujo adecuado para la realización del proceso?					
	¿El diagrama cuenta con los participantes necesarios para la ejecución del proceso?					
	¿El diagrama tiene las actividades necesarias para la ejecución eficiente del proceso?					
	¿Los documentos que se muestran en el diagrama son los necesarios para la ejecución del proceso?					
Observaciones						

Esta validación, la realizó el comité de seguridad de la información, lo cual se puede observar en el **Anexo 33** y además certifican su validación, en el cual se puede observar en el **Anexo 34.**

FASE 5: FORMALIZACIÓN DE LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN POR EL DIRECTOR DE LA UTI Y EL ADMINISTRADOR DE LA SEGURIDAD DE LA INFORMACIÓN

Para la formalización de los procesos, se realizó una reunión con el director y el administrador de la seguridad de la información, en la cual se formalizaron los procesos **Ver Anexo 32** y certifican su formalización **Ver Anexo 35,** y además certifican su conformidad con el trabajo de titulación, en el cual se puede observar en el **Anexo 36.**

g. DISCUSIÓN

El presente trabajo de titulación, cumplió con los objetivos específicos planteados al inicio del mismo, tratando de cumplir los parámetros requeridos y metas propuestas dentro del cronograma estipulado. Las mismas que se detallan a continuación:

DESARROLLO DE LA PROPUESTA

Objetivo 1: Diagnosticar las situación actual de la Unidad de Telecomunicaciones e Información sobre los procesos de seguridad de la información.

Para el cumplimiento adecuado de este objetivo, se realizó una encuesta (Ver anexo 4) a todo el personal de la UTI, determinando la necesidad de los procesos de seguridad de la información institucional, partiendo de ello se realizó el análisis de las políticas actuales implementadas en la UTI y destinadas a cada sección, con la finalidad de determinar la gestión actual sobre los procesos de seguridad de la información, a partir de la información recolectada, se puedo establecer el entorno actual del manejo y gestión de los procesos de seguridad de la información dentro de la UTI, estableciendo con ellos los puntos importantes a ser tratados en el desarrollo del trabajo de titulación.

Objetivo 2: Levantar los procesos de seguridad de la información en la Unidad de Telecomunicaciones e Información.

Para el cumplimiento de este objetivo, se llevaron a cabo varias actividades, que permitieron levantar cada uno de los procesos de seguridad de la información, que actualmente se ejecutan dentro de la UTI (Ver anexo 8), además en base a los resultados obtenidos en la primera fase ayudó a levantar los mismos.

Objetivo 3: Definir los procesos de seguridad de la información en la Unidad de Telecomunicaciones e Información.

El cumplimiento de este objetivo, se basó en la norma ISO/IEC 27002:2013 la cual facilitó la definición de los procesos de seguridad de la información, más críticos y esenciales dentro de la UTI (Ver sección 1.3 de la fase 1 y anexo 25), así mismo se utilizó la metodología Sipoc y el estándar Bpmn 2.0 para la realización de los diagramas de flujo.

Objetivo 4: Validar los procesos de seguridad de la información en la Unidad de Telecomunicaciones e Información.

Para el cumplimiento de este objetivo, se utilizó una matriz de validación de procesos (Ver anexo 33), además estos procesos de seguridad de la información, fueron validados por el comité de la seguridad de la información de la UTI y finalmente se puede observar su certificación (Ver anexo 34).

Objetivo 5: Formalizar los procesos de seguridad de la información por el Director y Administrador de la seguridad de la información de la Unidad de Telecomunicaciones e Información.

Para el cumplimiento de este objetivo, se estableció una reunión con el director de la UTI y el administrador de la seguridad de la información, en el cual certifican la formalización de los procesos de seguridad de la información (Ver anexo 35), además el director de la UTI certifica su conformidad con la formalización y documentación de los procesos de seguridad de la información (Ver anexo 36).

h. CONCLUSIONES

- Actualmente en la Unidad de Telecomunicaciones e Información, manejan documentos de políticas de la seguridad de la información, que no están aprobadas por los altos directivos de la Universidad Nacional de Loja.
- La falta de tener estandarizados o normalizados los procesos, hace que las actividades no tengan un control adecuado.
- La aplicación de la norma ISO/IEC 27002:2013, en la definición de los procesos de la seguridad de la información, permitió ver los procesos más críticos, para poder tener un mejor control de la seguridad de la información.
- El uso de la metodología Sipoc y el ciclo PHVA contribuyó al desarrollo de los procesos, brindando así una vista más amplia de cómo estos actúan.
- La esquematización del documento de los procesos de la seguridad de la información, permitirá a la Unidad de Telecomunicaciones e Información, dar los primeros pasos en la gestión de los procesos de la seguridad de la información a nivel institucional.

i. RECOMENDACIONES

- Es importante para la Unidad de Telecomunicaciones e Información, mantener actualizadas y aprobadas las políticas de seguridad de la información, puesto que, éstas están realizadas bajo la norma ISO/IEC 27002:2005.
- Para la Unidad de Telecomunicaciones e Información es importante considerar la asignación de personal destinado específicamente a la gestión, manejo y aplicación de la seguridad de la información a nivel institucional.
- De realizar los procesos faltantes, una vez que los procesos desarrollados alcance su madurez.
- En el desarrollo de los siguientes procesos y su actualización, se mantenga la metodología SIPOC y PHVA.

j. BIBLIOGRAFÍA

[1] "Universidad Nacional de Loja." [Online]. Available: http://unl.edu.ec/. [Accessed: 19-Jan-2016].

[2] "ESTATUTO POR PROCESOS UNL .pdf." .

[3] I. Carlos Ormella Meyer Asoc and I. Carlos Ormella Meyer, "¿Seguridad informática vs. Seguridad de la información?"

[4] "Seguridad de la información. Redes, informática y sistemas de información - AREITIO J, Javier Areitio Bertolín - Google Libros." [Online]. Available: https://books.google.com.ec/books?id=_z2GcBD3deYC&lpg=PP1&hl=es&pg=PP1#v=onepage&q&f=true.

[5] A. Villal and H. Grupo, "Códigos de buenas prácticas UNE-ISO / IEC Contenidos."

[6] "Seguridad informática - Purificación Aguilera López - Google Libros." [Online]. Available: https://books.google.com.ec/books?id=Mgvm3AYIT64C&lpg=PP1&hl=es&pg=PP1#v=onepage&q&f=true.

[7] E. Por, I. José, and M. Poveda Página, "Módulo 4: Estándares de gestión de la seguridad de la información."

[8] E. Bash, "Definición y validación de proceso," *PhD Propos.*, vol. 1, pp. 1–18, 2015.

[9] "iso27000.es/iso27002.html." .

[10] Q. Edición, V. Resumida, and J. B. Carrasco, "Gestión de procesos (Valorando la práctica)."

[11] pedro leira, "Diagrama SIPOC, herramienta para descubrir las posibles áreas de mejora | El Blog de Pedro Leira." [Online]. Available: https://pedroleira.com/2013/02/04/diagrama-sipoc-herramienta-para-descubrir-las-posibles-areas-de-mejora/.

[12] "SIPOC - Un diagrama de lo más útil para mapeo de procesos." [Online]. Available: http://www.pymesycalidad20.com/sipoc-un-diagrama-de-lo-mas-util-para-mapeo-de-procesos.html. [Accessed: 14-May-2016].

[13] "six_sigma_learning_book.pdf." [Online]. Available: http://6sigma.weebly.com/uploads/1/2/0/7/120786/six_sigma_learning_book.pdf. [Accessed: 14-May-2016].

[14] *The Certified Manager of Quality/organizational Excellence Handbook*. 2005.

[15] L. Tortuga and U. Herramienta, "La Tortuga - Una Herramienta de M ú ltiples Aplicaciones Puerto Vallarta Mayo 2004 Contenido," 2004.

[16] I. P. N. C. Manual, "Mapeo de la cadena de valor 1," pp. 1–110, 2006.

[17] E. Politécnica, D. E. L. Ejército, D. D. E. Ciencias, and D. E. L. A. Computación, "Metodología Para El Análisis , Diseño E Implementación De Procesos Con Tecnología Bpm (Business Process Management) Y," 2013.

[18] D. Iso and T. C. Sc, "Orientación sobre el concepto y uso del ' Enfoque basado en procesos ' para los sistemas de gestión," pp. 1–11, 2004.

[19] Q.-E. Norma, T. Ecuatoriana, and C. Edición, "INSTITUTO ECUATORIANO DE NORMALIZACIÓN SISTEMAS DE GESTIÓN DE LA CALIDAD -REQUISITOS."

[20] L. Diagramas, "Como crear un diagrama de flujo," pp. 1–7.

[21] A. DE CLASE Profesor and A. Ruiz-Falcó Rojas, "HERRAMIENTAS DE CALIDAD," 2009.

[22] paulo ramos, "SIPOC paso por paso . Un método para identificar las entradas (inputs) y variables que pueden afectar el resultado del proceso. | Paulo Ramos | LinkedIn." [Online]. Available: https://www.linkedin.com/pulse/sipoc-paso-por-un-m%C3%A9todo-para-identificar-los-insumos-paulo-ramos?forceNoSplash=true.

[23] J. Freund, B. Rücker, and B. Hitpass, *BPMN 2.0: Manual de Referencia y Guía Práctica*. 2011.

[24] B. Bpmn and S. G. U Í A D E R E F E R E N C I A Y M O D E L, "Guía de Referencia y Modelado BPMN."

[25] ANALITICA, "Manual de diagramación de procesos bajo estándar BPMN," *Man. diagramación procesos bajo estándar BPMN*, p. 16, 2005.